

JOeSandbox Cloud BASIC



**ID:** 429863

**Cookbook:** browseurl.jbs

**Time:** 21:34:18

**Date:** 04/06/2021

**Version:** 32.0.0 Black Diamond

## Table of Contents

|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| Table of Contents                                                                                 | 2   |
| Analysis Report <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a> | 3   |
| Overview                                                                                          | 3   |
| General Information                                                                               | 3   |
| Detection                                                                                         | 3   |
| Signatures                                                                                        | 3   |
| Classification                                                                                    | 3   |
| Process Tree                                                                                      | 3   |
| Malware Configuration                                                                             | 3   |
| Yara Overview                                                                                     | 3   |
| Sigma Overview                                                                                    | 3   |
| Signature Overview                                                                                | 3   |
| Mitre Att&ck Matrix                                                                               | 4   |
| Behavior Graph                                                                                    | 4   |
| Screenshots                                                                                       | 5   |
| Thumbnails                                                                                        | 5   |
| Antivirus, Machine Learning and Genetic Malware Detection                                         | 6   |
| Initial Sample                                                                                    | 6   |
| Dropped Files                                                                                     | 6   |
| Unpacked PE Files                                                                                 | 6   |
| Domains                                                                                           | 6   |
| URLs                                                                                              | 6   |
| Domains and IPs                                                                                   | 7   |
| Contacted Domains                                                                                 | 7   |
| Contacted URLs                                                                                    | 8   |
| URLs from Memory and Binaries                                                                     | 8   |
| Contacted IPs                                                                                     | 10  |
| Public                                                                                            | 11  |
| General Information                                                                               | 11  |
| Simulations                                                                                       | 12  |
| Behavior and APIs                                                                                 | 13  |
| Joe Sandbox View / Context                                                                        | 13  |
| IPs                                                                                               | 13  |
| Domains                                                                                           | 13  |
| ASN                                                                                               | 13  |
| JA3 Fingerprints                                                                                  | 13  |
| Dropped Files                                                                                     | 13  |
| Created / dropped Files                                                                           | 13  |
| Static File Info                                                                                  | 46  |
| No static file info                                                                               | 46  |
| Network Behavior                                                                                  | 46  |
| Network Port Distribution                                                                         | 46  |
| TCP Packets                                                                                       | 47  |
| UDP Packets                                                                                       | 48  |
| DNS Queries                                                                                       | 50  |
| DNS Answers                                                                                       | 51  |
| HTTP Request Dependency Graph                                                                     | 51  |
| HTTP Packets                                                                                      | 51  |
| HTTPS Packets                                                                                     | 102 |
| Code Manipulations                                                                                | 108 |
| Statistics                                                                                        | 108 |
| Behavior                                                                                          | 108 |
| System Behavior                                                                                   | 108 |
| Analysis Process: iexplore.exe PID: 6628 Parent PID: 800                                          | 108 |
| General                                                                                           | 108 |
| File Activities                                                                                   | 109 |
| Registry Activities                                                                               | 109 |
| Analysis Process: iexplore.exe PID: 6680 Parent PID: 6628                                         | 109 |
| General                                                                                           | 109 |
| File Activities                                                                                   | 109 |
| Registry Activities                                                                               | 109 |
| Disassembly                                                                                       | 110 |

# Analysis Report <http://www.tonhc.org/coronavirus/>

## Overview

### General Information

Sample URL:

http://www.tonhc.org/coronavirus/

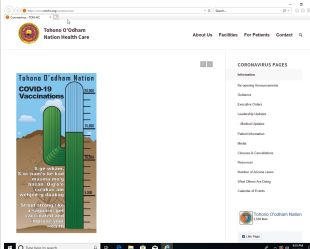
Analysis ID:

429863

Infos:



Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

0

Range:

0 - 100

Whitelisted:

false

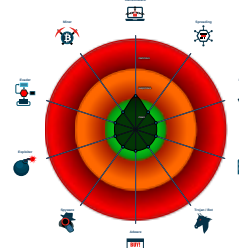
Confidence:

80%

### Signatures

No high impact signatures.

### Classification



## Process Tree

■ System is w10x64

 iexplore.exe (PID: 6628 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)

 iexplore.exe (PID: 6680 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6628 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

■ cleanup

## Malware Configuration

No configs have been found

## Yara Overview

No yara matches

## Sigma Overview

No Sigma rule has matched

## Signature Overview

- Compliance
- Networking
- System Summary



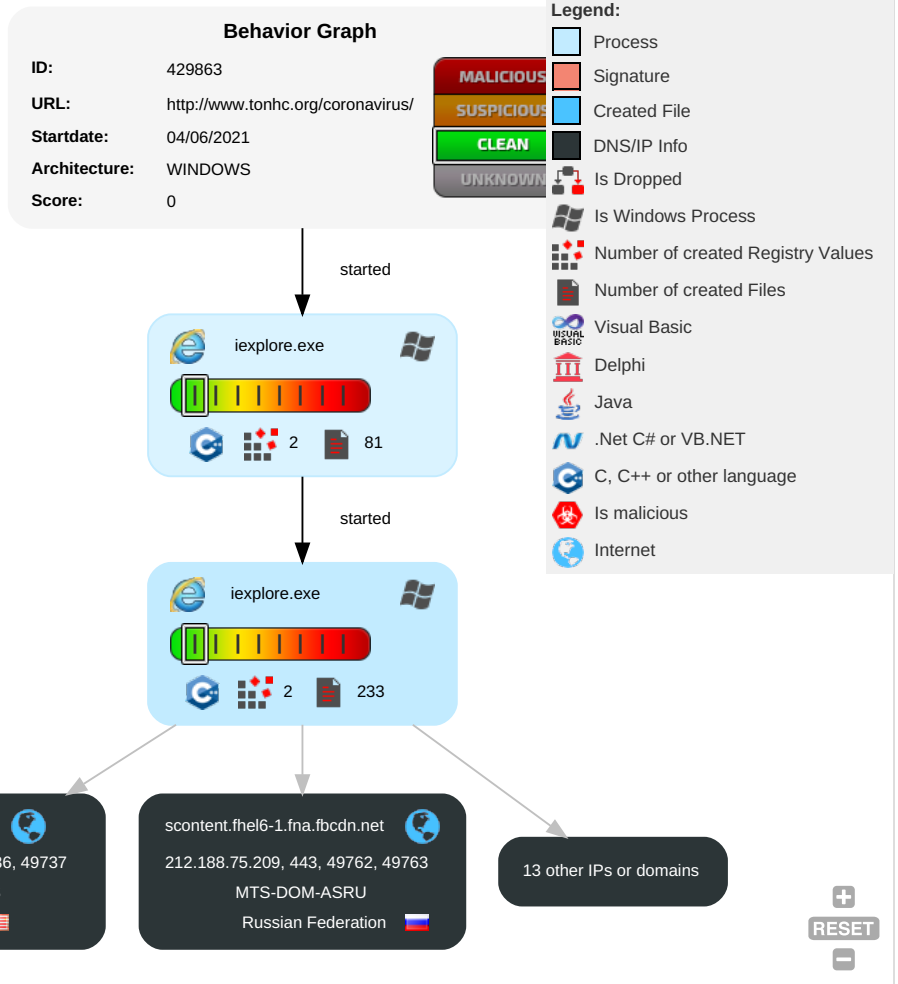
💡 Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

### Mitre Att&ck Matrix

| Initial Access   | Execution                          | Persistence                          | Privilege Escalation                 | Defense Evasion                 | Credential Access        | Discovery                              | Lateral Movement                   | Collection                     | Exfiltration                           | Command and Control              | Network Effects                             | Remote Service Effects                      | Impact                   |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|---------------------------------|--------------------------|----------------------------------------|------------------------------------|--------------------------------|----------------------------------------|----------------------------------|---------------------------------------------|---------------------------------------------|--------------------------|
| Valid Accounts   | Windows Management Instrumentation | Path Interception                    | Process Injection 1                  | Masquerading 1                  | OS Credential Dumping    | File and Directory Discovery 1         | Remote Services                    | Data from Local System         | Exfiltration Over Other Network Medium | Encrypted Channel 2              | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partitions |
| Default Accounts | Scheduled Task/Job                 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1             | LSASS Memory             | Application Window Discovery           | Remote Desktop Protocol            | Data from Removable Media      | Exfiltration Over Bluetooth            | Non-Application Layer Protocol 3 | Exploit SS7 to Redirect Phone Calls/SMS     | Remotely Wipe Data Without Authorization    | Device Lockdown          |
| Domain Accounts  | At (Linux)                         | Logon Script (Windows)               | Logon Script (Windows)               | Obfuscated Files or Information | Security Account Manager | Query Registry                         | SMB/Windows Admin Shares           | Data from Network Shared Drive | Automated Exfiltration                 | Application Layer Protocol 4     | Exploit SS7 to Track Device Location        | Obtain Device Cloud Backups                 | Delete Device Data       |
| Local Accounts   | At (Windows)                       | Logon Script (Mac)                   | Logon Script (Mac)                   | Binary Padding                  | NTDS                     | System Network Configuration Discovery | Distributed Component Object Model | Input Capture                  | Scheduled Transfer                     | Ingress Tool Transfer 2          | SIM Card Swap                               |                                             | Carrier Billing Fraud    |

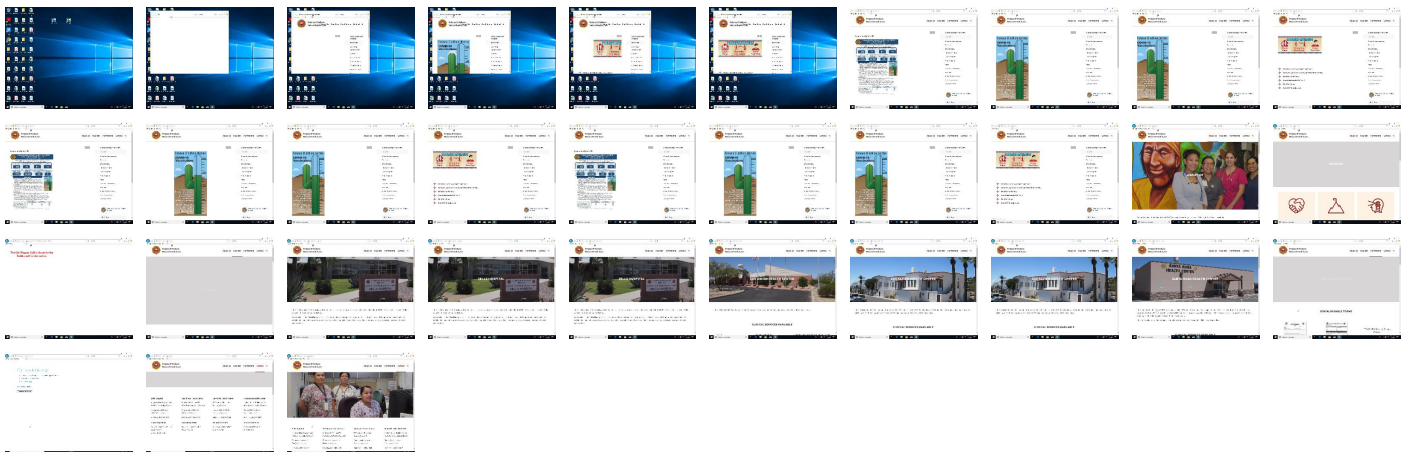
### Behavior Graph

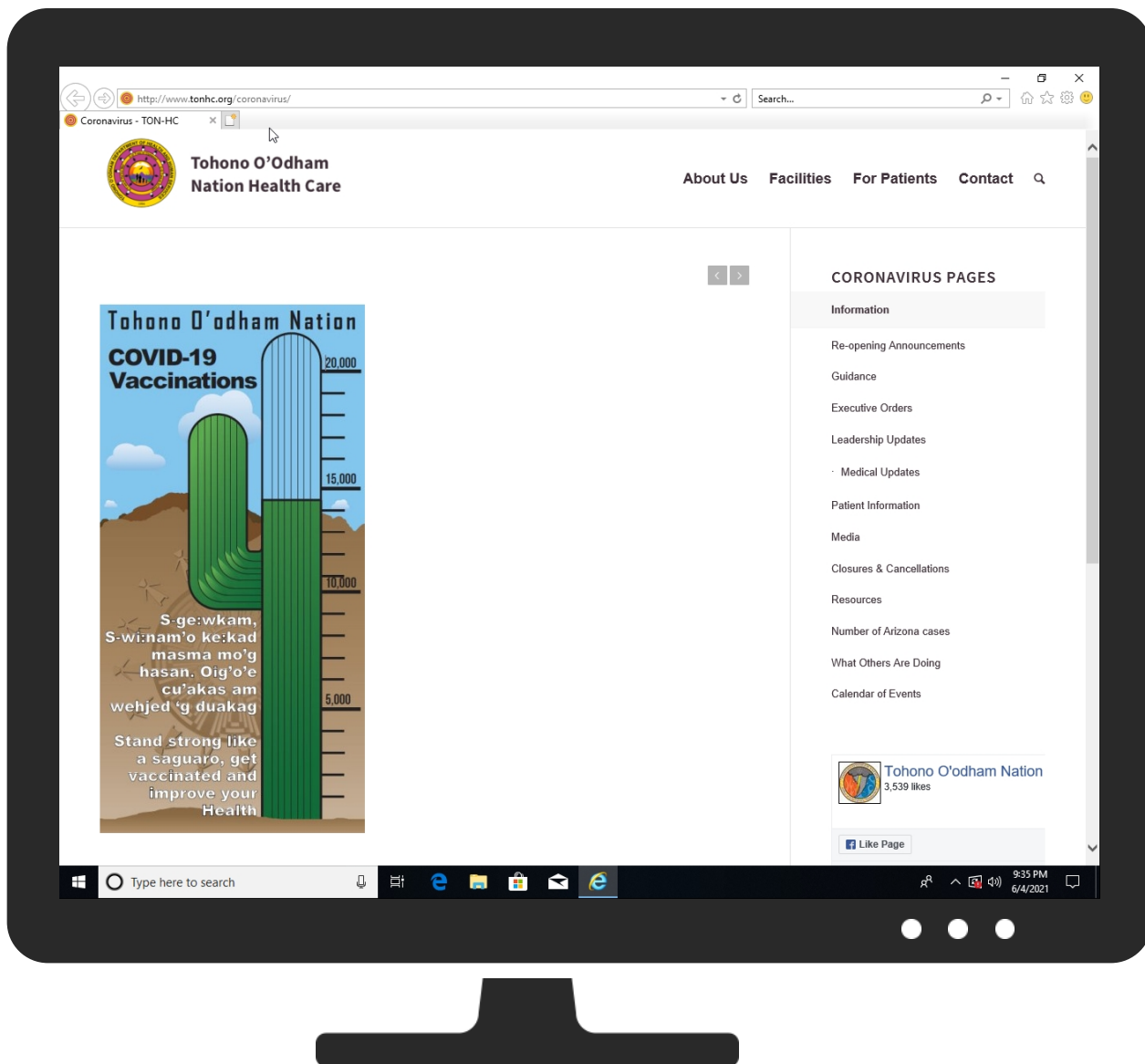


## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source                                                                            | Detection | Scanner         | Label | Link                   |
|-----------------------------------------------------------------------------------|-----------|-----------------|-------|------------------------|
| <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a> | 0%        | Virustotal      |       | <a href="#">Browse</a> |
| <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a> | 0%        | Avira URL Cloud | safe  |                        |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| Source    | Detection | Scanner    | Label | Link                   |
|-----------|-----------|------------|-------|------------------------|
| tonhc.org | 0%        | Virustotal |       | <a href="#">Browse</a> |

### URLs

| Source                                                                                            | Detection | Scanner         | Label | Link |
|---------------------------------------------------------------------------------------------------|-----------|-----------------|-------|------|
| <a href="http://www.tonhc.org/coronavirus/#webpage">http://www.tonhc.org/coronavirus/#webpage</a> | 0%        | Avira URL Cloud | safe  |      |

| Source                                                                                                                                                                                                                  | Detection | Scanner         | Label | Link |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------|-------|------|
| <a href="http://www.tonhc.org/wp-content/plugins/the-events-calendar/common/src/resources/css/common-skeleton">http://www.tonhc.org/wp-content/plugins/the-events-calendar/common/src/resources/css/common-skeleton</a> | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus-guidance/">http://www.tonhc.org/coronavirus-guidance/</a>                                                                                                                     | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus/Root">http://www.tonhc.org/coronavirus/Root</a>                                                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/magnific-popup.css?ver=1">http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/magnific-popup.css?ver=1</a>                                   | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsan-xavi">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsan-xavi</a> | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4">http://www.tonhc.org/wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4</a>                                           | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/xmlrpc.php">http://www.tonhc.org/xmlrpc.php</a>                                                                                                                                           | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-admin/admin-ajax.php">http://www.tonhc.org/wp-admin/admin-ajax.php</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/116">http://www.tonhc.org/wp-json/wp/v2/pages/116</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://https://www.internalfb.com/intern/invariant/">http://https://www.internalfb.com/intern/invariant/</a>                                                                                                   | 0%        | URL Reputation  | safe  |      |
| <a href="http://https://www.internalfb.com/intern/invariant/">http://https://www.internalfb.com/intern/invariant/</a>                                                                                                   | 0%        | URL Reputation  | safe  |      |
| <a href="http://https://www.internalfb.com/intern/invariant/">http://https://www.internalfb.com/intern/invariant/</a>                                                                                                   | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/130">http://www.tonhc.org/wp-json/wp/v2/pages/130</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/w">http://www.tonhc.org/w</a>                                                                                                                                                             | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffor-patients%2F">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffor-patients%2F</a>             | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=5.5.5">http://www.tonhc.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=5.5.5</a>                                       | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/mediaelement/skin-1/mediaelementplayer.css?ver=1">http://www.tonhc.org/wp-content/themes/enfold/js/mediaelement/skin-1/mediaelementplayer.css?ver=1</a>       | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc">http://www.tonhc</a>                                                                                                                                                                         | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://artsy.github.io/blog/2012/10/18/so-you-want-to-do-a-css3-3d-transform/">http://artsy.github.io/blog/2012/10/18/so-you-want-to-do-a-css3-3d-transform/</a>                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5">http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5</a>                           | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/facilities/sells-hospital/.Sells">http://www.tonhc.org/facilities/sells-hospital/.Sells</a>                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/uploads/2017/09/Favicon-3-300x300.png">http://www.tonhc.org/wp-content/uploads/2017/09/Favicon-3-300x300.png</a>                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.Root">http://www.tonhc.Root</a>                                                                                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus-patient-information/">http://www.tonhc.org/coronavirus-patient-information/</a>                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/css/base.css?ver=2">http://www.tonhc.org/wp-content/themes/enfold/css/base.css?ver=2</a>                                                                         | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fo">http://www.tonhc.org/wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fo</a> | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131">http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131</a>     | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsells-ho">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsells-ho</a> | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.5.5">http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.5.5</a>                             | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus/#primaryimage">http://www.tonhc.org/coronavirus/#primaryimage</a>                                                                                                             | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/avia-compat.js?ver=2">http://www.tonhc.org/wp-content/themes/enfold/js/avia-compat.js?ver=2</a>                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus/(Coronavirus">http://www.tonhc.org/coronavirus/(Coronavirus</a>                                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0">http://www.tonhc.org/wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0</a>                             | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/jquery.magnific-popup.min.js?ver=2">http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/jquery.magnific-popup.min.js?ver=2</a>               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/uploads/2017/09/TONHC-Website-Logo-2-300x106.png">http://www.tonhc.org/wp-content/uploads/2017/09/TONHC-Website-Logo-2-300x106.png</a>                                         | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/coronavirus-media/">http://www.tonhc.org/coronavirus-media/</a>                                                                                                                           | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4">http://www.tonhc.org/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4</a>                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/103">http://www.tonhc.org/wp-json/wp/v2/pages/103</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/346">http://www.tonhc.org/wp-json/wp/v2/pages/346</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/events/?ical=1">http://www.tonhc.org/events/?ical=1</a>                                                                                                                                   | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/221">http://www.tonhc.org/wp-json/wp/v2/pages/221</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001">http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001</a>                 | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.tonhc.org/#website">http://www.tonhc.org/#website</a>                                                                                                                                               | 0%        | Avira URL Cloud | safe  |      |

## Domains and IPs

### Contacted Domains

| Name                           | IP             | Active | Malicious | Antivirus Detection                                                                      | Reputation |
|--------------------------------|----------------|--------|-----------|------------------------------------------------------------------------------------------|------------|
| stats.wp.com                   | 192.0.76.3     | true   | false     |                                                                                          | high       |
| star-mini.c10r.facebook.com    | 157.240.9.35   | true   | false     |                                                                                          | high       |
| scontent.fhel6-1.fna.fbcdn.net | 212.188.75.209 | true   | false     |                                                                                          | high       |
| scontent.frx5-1.xx.fbcdn.net   | 185.60.216.19  | true   | false     |                                                                                          | high       |
| scontent.xx.fbcdn.net          | 31.13.92.14    | true   | false     |                                                                                          | high       |
| pixel.wp.com                   | 192.0.76.3     | true   | false     |                                                                                          | high       |
| scontent.frt3-2.xx.fbcdn.net   | 157.240.20.19  | true   | false     |                                                                                          | high       |
| tonhc.org                      | 64.25.66.82    | true   | false     | <ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> </ul> | unknown    |
| i1.wp.com                      | 192.0.77.2     | true   | false     |                                                                                          | high       |

| Name                         | IP          | Active  | Malicious | Antivirus Detection | Reputation |
|------------------------------|-------------|---------|-----------|---------------------|------------|
| i0.wp.com                    | 192.0.77.2  | true    | false     |                     | high       |
| scontent-frt3-1.xx.fbcdn.net | 31.13.92.14 | true    | false     |                     | high       |
| i2.wp.com                    | 192.0.77.2  | true    | false     |                     | high       |
| www.facebook.com             | unknown     | unknown | false     |                     | high       |
| connect.facebook.net         | unknown     | unknown | false     |                     | high       |
| www.tonhc.org                | unknown     | unknown | false     |                     | unknown    |

## Contacted URLs

| Name                                                                                                                                                                                                                                                                                                                                                                                        | Malicious | Antivirus Detection                                                     | Reputation |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------|------------|
| <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=130&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7339871367483555">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=130&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7339871367483555</a>   | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a>                                                                                                                                                                                                                                                                                                           | false     |                                                                         | unknown    |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/magnific-popup.css?ver=1">http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/magnific-popup.css?ver=1</a>                                                                                                                                                                                                       | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4">http://www.tonhc.org/wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4</a>                                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/uploads/2021/02/Cafe-Closed.png">http://www.tonhc.org/wp-content/uploads/2021/02/Cafe-Closed.png</a>                                                                                                                                                                                                                                               | false     |                                                                         | unknown    |
| <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=89&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7034506522366686">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=89&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7034506522366686</a>     | false     |                                                                         | high       |
| <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=159&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.08588111661636594">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=159&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.08588111661636594</a> | false     |                                                                         | high       |
| <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=221&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7699525934342165">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=221&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7699525934342165</a>   | false     |                                                                         | high       |
| <a href="http://connect.facebook.net/en_US/sdk.js">http://connect.facebook.net/en_US/sdk.js</a>                                                                                                                                                                                                                                                                                             | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/facilities/sant-rosa/">http://www.tonhc.org/facilities/sant-rosa/</a>                                                                                                                                                                                                                                                                                         | false     |                                                                         | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=5.5.5">http://www.tonhc.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=5.5.5</a>                                                                                                                                                                                                           | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=203&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7936902269709519">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=203&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7936902269709519</a>   | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/mediaelement/skin-1/mediaelementplayer.css?ver=1">http://www.tonhc.org/wp-content/themes/enfold/js/mediaelement/skin-1/mediaelementplayer.css?ver=1</a>                                                                                                                                                                           | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5">http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5</a>                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/uploads/2017/09/Favicon-3-300x300.png">http://www.tonhc.org/wp-content/uploads/2017/09/Favicon-3-300x300.png</a>                                                                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/css/base.css?ver=2">http://www.tonhc.org/wp-content/themes/enfold/css/base.css?ver=2</a>                                                                                                                                                                                                                                             | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131">http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131</a>                                                                                                                                                                         | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.5.5">http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.5.5</a>                                                                                                                                                                                                 | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/avia-compat.js?ver=2">http://www.tonhc.org/wp-content/themes/enfold/js/avia-compat.js?ver=2</a>                                                                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0">http://www.tonhc.org/wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0</a>                                                                                                                                                                                                 | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://phr.ihs.gov/phr/PHRLogin">http://https://phr.ihs.gov/phr/PHRLogin</a>                                                                                                                                                                                                                                                                                               | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/facilities/">http://www.tonhc.org/facilities/</a>                                                                                                                                                                                                                                                                                                             | false     |                                                                         | unknown    |
| <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a>                                                                                                                                                                                                                                                                                                           | false     |                                                                         | unknown    |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/jquery.magnific-popup.min.js?ver=2">http://www.tonhc.org/wp-content/themes/enfold/js/aviapopup/jquery.magnific-popup.min.js?ver=2</a>                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/uploads/2017/09/TONHC-Website-Logo-2-300x106.png">http://www.tonhc.org/wp-content/uploads/2017/09/TONHC-Website-Logo-2-300x106.png</a>                                                                                                                                                                                                             | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4">http://www.tonhc.org/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4</a>                                                                                                                                                                                                                                     | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001">http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001</a>                                                                                                                                                                                     | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |

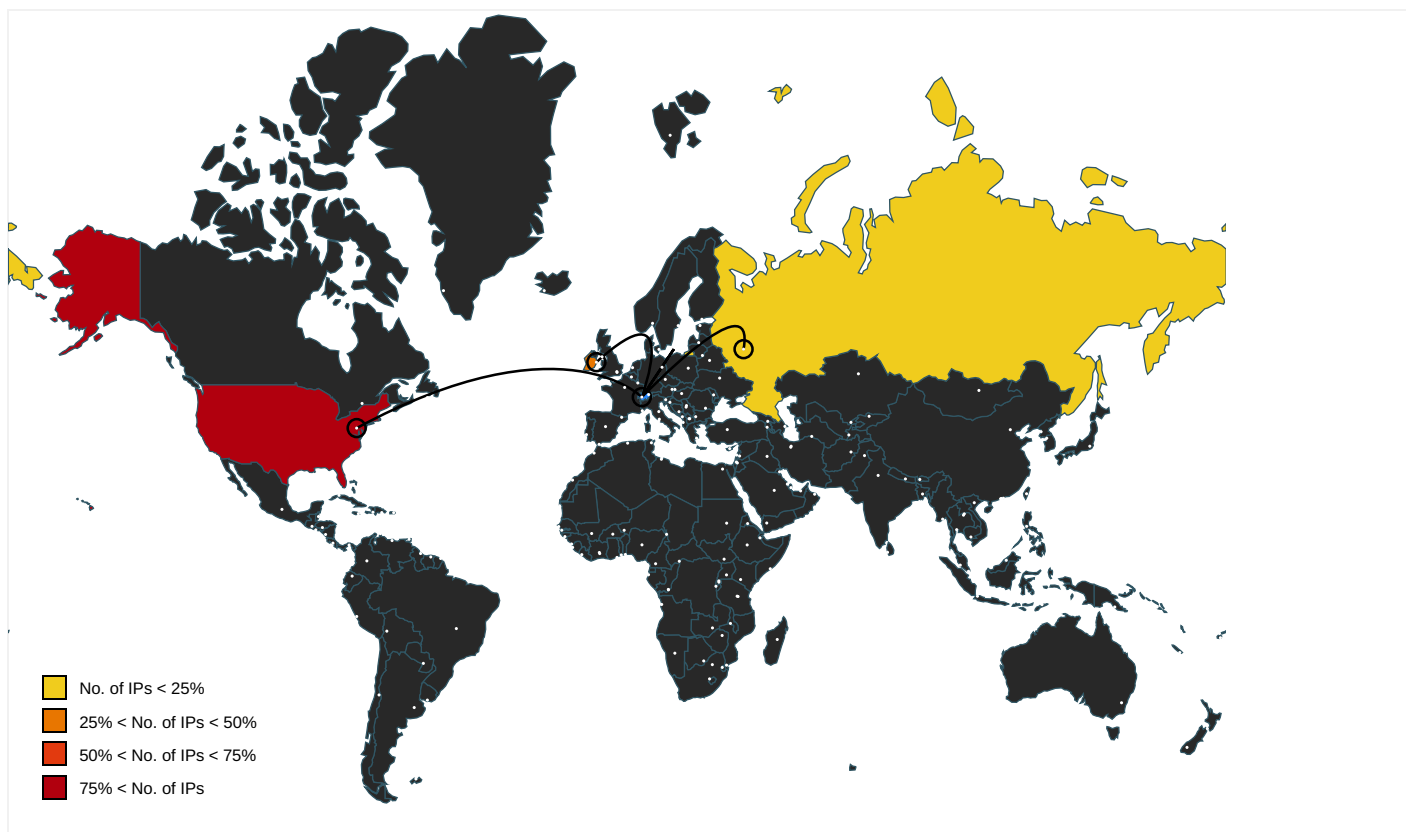
## URLs from Memory and Binaries

| Name                                                                                                                                                                                                                    | Source                                                                                          | Malicious | Antivirus Detection                                                     | Reputation |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------|------------|
| <a href="http://https://phr.ihs.gov/phr">http://https://phr.ihs.gov/phr</a>                                                                                                                                             | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr                                                | false     |                                                                         | high       |
| <a href="http://https://wp.me/P9uvL4-4a">http://https://wp.me/P9uvL4-4a</a>                                                                                                                                             | for-patients[1].htm.2.dr                                                                        | false     |                                                                         | high       |
| <a href="http://https://wp.me/P9uvL4-5A">http://https://wp.me/P9uvL4-5A</a>                                                                                                                                             | san-simon[1].htm0.2.dr                                                                          | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus/#webpage">http://www.tonhc.org/coronavirus/#webpage</a>                                                                                                                       | coronavirus[1].htm.2.dr                                                                         | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://wp.me/P9uvL4-3z">http://https://wp.me/P9uvL4-3z</a>                                                                                                                                             | sant-rosa[1].htm.2.dr                                                                           | false     |                                                                         | high       |
| <a href="http://https://phr.ihs.gov/phr/PHRLogin">http://https://phr.ihs.gov/phr/PHRLogin</a>                                                                                                                           | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr, mission[1].htm.2.dr, for-patients[1].htm.2.dr | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/wp-content/plugins/the-events-calendar/common/src/resources/css/common-skeleton">http://www.tonhc.org/wp-content/plugins/the-events-calendar/common/src/resources/css/common-skeleton</a> | mission[1].htm.2.dr                                                                             | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2021/05/LU-65.jpg?w=673">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2021/05/LU-65.jpg?w=673</a>                                       | coronavirus[1].htm.2.dr                                                                         | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus-guidance/">http://www.tonhc.org/coronavirus-guidance/</a>                                                                                                                     | coronavirus[1].htm.2.dr                                                                         | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/coronavirus/Root">http://www.tonhc.org/coronavirus/Root</a>                                                                                                                               | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr                                                | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://stackoverflow.com/questions/11979156/mobile-safari-back-button">http://stackoverflow.com/questions/11979156/mobile-safari-back-button</a>                                                               | avia[1].js.2.dr                                                                                 | false     |                                                                         | high       |
| <a href="http://https://theeventscalendar.com/">http://https://theeventscalendar.com/</a>                                                                                                                               | mission[1].htm.2.dr                                                                             | false     |                                                                         | high       |

| Name                                                                                                                                                                                                                                  | Source                                           | Malicious | Antivirus Detection                                                                                                                | Reputation |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------|------------|
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsan-xavi">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsan-xavi</a>               | san-xavier[1].htm.2.dr                           | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.tonhc.org/xmlrpc.php">http://www.tonhc.org/xmlrpc.php</a>                                                                                                                                                         | mission[1].htm.2.dr                              | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.tonhc.org/wp-admin/admin-ajax.php">http://www.tonhc.org/wp-admin/admin-ajax.php</a>                                                                                                                               | mission[1].htm.2.dr                              | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://github.com/jquery/jquery-color">http://https://github.com/jquery/jquery-color</a>                                                                                                                             | effect.min[1].js.2.dr                            | false     |                                                                                                                                    | high       |
| <a href="http://api.jqueryui.com/jquery.widget/">http://api.jqueryui.com/jquery.widget/</a>                                                                                                                                           | widget.min[1].js.2.dr                            | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/116">http://www.tonhc.org/wp-json/wp/v2/pages/116</a>                                                                                                                               | about[1].htm.2.dr                                | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://www.internalfb.com/intern/invariant/">http://https://www.internalfb.com/intern/invariant/</a>                                                                                                                 | sdk[1].js0.2.dr                                  | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/130">http://www.tonhc.org/wp-json/wp/v2/pages/130</a>                                                                                                                               | mission[1].htm.2.dr                              | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2021/05/LU-65.jpg?resize=232%2C300">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2021/05/LU-65.jpg?resize=232%2C300</a>                               | coronavirus[1].htm.2.dr                          | false     |                                                                                                                                    | high       |
| <a href="http://https://schema.org/WPSideBar">http://https://schema.org/WPSideBar</a>                                                                                                                                                 | coronavirus[1].htm.2.dr                          | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc.org/w">http://www.tonhc.org/w</a>                                                                                                                                                                           | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffor-patients%2F">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffor-patients%2F</a>                           | for-patients[1].htm.2.dr                         | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://wp.me/P9uvL4-2z">http://https://wp.me/P9uvL4-2z</a>                                                                                                                                                           | contact[1].htm.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://https://github.com/gabceb/jquery-browser-plugin">http://https://github.com/gabceb/jquery-browser-plugin</a>                                                                                                           | avia[1].js.2.dr                                  | false     |                                                                                                                                    | high       |
| <a href="http://https://wp.me/P9uvL4-3h">http://https://wp.me/P9uvL4-3h</a>                                                                                                                                                           | sells-hospital[1].htm.2.dr                       | false     |                                                                                                                                    | high       |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Privacy-Practice-1.png?fit=235%2C300">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Privacy-Practice-1.png?fit=235%2C300</a>           | for-patients[1].htm.2.dr                         | false     |                                                                                                                                    | high       |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells_Hospital-History.jpg?resize=1000%2C">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells_Hospital-History.jpg?resize=1000%2C</a> | about[1].htm.2.dr                                | false     |                                                                                                                                    | high       |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sansimon.jpg?fit=1500%2C704);">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sansimon.jpg?fit=1500%2C704);</a>             | san-simon[1].htm0.2.dr                           | false     |                                                                                                                                    | high       |
| <a href="http://https://secure.gravatar.com/images/grav-share-sprite.png);background-repeat:no-repeat;width:16px;hei">http://https://secure.gravatar.com/images/grav-share-sprite.png);background-repeat:no-repeat;width:16px;hei</a> | jetpack[1].css.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc">http://www.tonhc</a>                                                                                                                                                                                       | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-santarosa.jpg?fit=1500%2C735);">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-santarosa.jpg?fit=1500%2C735);</a>           | sant-rosa[1].htm.2.dr                            | false     |                                                                                                                                    | high       |
| <a href="http://artsy.github.io/blog/2012/10/18/so-you-want-to-do-a-css3-3d-transform/">http://artsy.github.io/blog/2012/10/18/so-you-want-to-do-a-css3-3d-transform/</a>                                                             | avia-compat[1].js.2.dr                           | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.tonhc.org/facilities/sells-hospital/.Sells">http://www.tonhc.org/facilities/sells-hospital/.Sells</a>                                                                                                             | ~DF91B0334891952890.TMP.1.dr                     | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.reddit.com/">http://www.reddit.com/</a>                                                                                                                                                                           | msapplication.xml4.1.dr                          | false     |                                                                                                                                    | high       |
| <a href="http://api.jqueryui.com/size-effect/">http://api.jqueryui.com/size-effect/</a>                                                                                                                                               | effect-size.min[1].js.2.dr                       | false     |                                                                                                                                    | high       |
| <a href="http://www.mediaelementjs.com/">http://www.mediaelementjs.com/</a>                                                                                                                                                           | mediaelement-and-player.min[1].js.2.dr           | false     |                                                                                                                                    | high       |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Facilities-Map-1.png?fit=2000%2C784">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Facilities-Map-1.png?fit=2000%2C784</a>             | contact[1].htm.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc.Root">http://www.tonhc.Root</a>                                                                                                                                                                             | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2021/05/TONHC_VChart-2.jpg?w=436">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2021/05/TONHC_VChart-2.jpg?w=436</a>                                   | coronavirus[1].htm.2.dr                          | false     |                                                                                                                                    | high       |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-staff-photo.jpg?resize=1500%2C630);">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-staff-photo.jpg?resize=1500%2C630);</a> | contact[1].htm.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc.org/coronavirus-patient-information/">http://www.tonhc.org/coronavirus-patient-information/</a>                                                                                                             | coronavirus[1].htm.2.dr                          | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://www.tonhc.org/wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fo">http://www.tonhc.org/wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fo</a>               | mission[1].htm.2.dr                              | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells-Hospital-Map.png?fit=2000%2C659);">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells-Hospital-Map.png?fit=2000%2C659);</a>     | sells-hospital[1].htm.2.dr                       | false     |                                                                                                                                    | high       |
| <a href="http://www.kriesi.at/support/topic/next-previous-blog-post-bug/">http://www.kriesi.at/support/topic/next-previous-blog-post-bug/</a>                                                                                         | layout[1].css.2.dr                               | false     |                                                                                                                                    | high       |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/TODHHS-Logo.png?resize=36%2C36">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/TODHHS-Logo.png?resize=36%2C36</a>                       | mission[1].htm.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsells-ho">http://www.tonhc.org/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fwww.tonhc.org%2Ffacilities%2Fsells-ho</a>               | sells-hospital[1].htm.2.dr                       | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                            | unknown    |
| <a href="http://api.jqueryui.com/category/ui-core/">http://api.jqueryui.com/category/ui-core/</a>                                                                                                                                     | core.min[1].js.2.dr                              | false     |                                                                                                                                    | high       |
| <a href="http://https://github.com/imakewebthings/waypoints/blog/master/licen">http://https://github.com/imakewebthings/waypoints/blog/master/licen</a><br>ses.txt                                                                    | avia[1].js.2.dr                                  | false     |                                                                                                                                    | high       |

| Name                                                                                                                                                                                                                                  | Source                                                                                                                                                                                                                                    | Malicious | Antivirus Detection                                                     | Reputation |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------|------------|
| <a href="http://https://schema.org">http://https://schema.org</a>                                                                                                                                                                     | mission[1].htm.2.dr, san-simon[1].htm0.2.dr, sells-hospital[1].htm.2.dr, sant-rosa[1].htm.2.dr, san-xavier[1].htm.2.dr, contact[1].htm.2.dr, about[1].htm.2.dr, for-patients[1].htm.2.dr, facilities[1].htm.2.dr, coronavirus[1].htm.2.dr | false     |                                                                         | high       |
| <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?resize=1030%2C411">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?resize=1030%2C411</a> | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     |                                                                         | high       |
| <a href="http://gmpg.org/xfn/11">http://gmpg.org/xfn/11</a>                                                                                                                                                                           | mission[1].htm.2.dr                                                                                                                                                                                                                       | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus/#primaryimage">http://www.tonhc.org/coronavirus/#primaryimage</a>                                                                                                                           | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Tohono-Nation-Logo.png?resize=120%2C120">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Tohono-Nation-Logo.png?resize=120%2C120</a>     | mission[1].htm.2.dr                                                                                                                                                                                                                       | false     |                                                                         | high       |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-patient-photo.jpg?fit=1500%2C817">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-patient-photo.jpg?fit=1500%2C817</a>       | for-patients[1].htm.2.dr                                                                                                                                                                                                                  | false     |                                                                         | high       |
| <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?fit=1585%2C632">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?fit=1585%2C632</a>       | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus/(Coronavirus">http://www.tonhc.org/coronavirus/(Coronavirus</a>                                                                                                                             | {F3ABF0DE-C56B-11EB-90EB-ECF4B BEA1588}.dat.1.dr                                                                                                                                                                                          | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?resize=705%2C281">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?resize=705%2C281</a>   | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     |                                                                         | high       |
| <a href="http://https://schema.org/WPHeader">http://https://schema.org/WPHeader</a>                                                                                                                                                   | mission[1].htm.2.dr                                                                                                                                                                                                                       | false     |                                                                         | high       |
| <a href="http://https://wp.me/P9uvL4-h1">http://https://wp.me/P9uvL4-h1</a>                                                                                                                                                           | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     |                                                                         | high       |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=300%2C109">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=300%2C109</a>                                   | for-patients[1].htm.2.dr                                                                                                                                                                                                                  | false     |                                                                         | high       |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Our-Facilities.jpg?resize=1500%2C630">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Our-Facilities.jpg?resize=1500%2C630</a>           | facilities[1].htm.2.dr                                                                                                                                                                                                                    | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/coronavirus-media/">http://www.tonhc.org/coronavirus-media/</a>                                                                                                                                         | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://api.jqueryui.com/transfer-effect/">http://api.jqueryui.com/transfer-effect/</a>                                                                                                                                       | effect-transfer.min[1].js.2.dr                                                                                                                                                                                                            | false     |                                                                         | high       |
| <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2021/05/TONHC_VChart-2.jpg?resize=326%2C651">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2021/05/TONHC_VChart-2.jpg?resize=326%2C651</a>             | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/103">http://www.tonhc.org/wp-json/wp/v2/pages/103</a>                                                                                                                               | san-xavier[1].htm.2.dr                                                                                                                                                                                                                    | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/346">http://www.tonhc.org/wp-json/wp/v2/pages/346</a>                                                                                                                               | san-simon[1].htm0.2.dr                                                                                                                                                                                                                    | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/events/?ical=1">http://www.tonhc.org/events/?ical=1</a>                                                                                                                                                 | mission[1].htm.2.dr                                                                                                                                                                                                                       | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=413%2C150">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=413%2C150</a>                                   | for-patients[1].htm.2.dr                                                                                                                                                                                                                  | false     |                                                                         | high       |
| <a href="http://www.tonhc.org/wp-json/wp/v2/pages/221">http://www.tonhc.org/wp-json/wp/v2/pages/221</a>                                                                                                                               | sant-rosa[1].htm.2.dr                                                                                                                                                                                                                     | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://www.tonhc.org/#website">http://www.tonhc.org/#website</a>                                                                                                                                                             | coronavirus[1].htm.2.dr                                                                                                                                                                                                                   | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Tohono-Nation-Logo.png?resize=36%2C36">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Tohono-Nation-Logo.png?resize=36%2C36</a>         | mission[1].htm.2.dr                                                                                                                                                                                                                       | false     |                                                                         | high       |

## Contacted IPs



## Public

| IP             | Domain                         | Country            | Flag | ASN   | ASN Name     | Malicious |
|----------------|--------------------------------|--------------------|------|-------|--------------|-----------|
| 212.188.75.209 | scontent.fhel6-1.fna.fbcdn.net | Russian Federation |      | 49154 | MTS-DOM-ASRU | false     |
| 157.240.20.19  | scontent-frt3-2.xx.fbcdn.net   | United States      |      | 32934 | FACEBOOKUS   | false     |
| 185.60.216.19  | scontent-frx5-1.xx.fbcdn.net   | Ireland            |      | 32934 | FACEBOOKUS   | false     |
| 157.240.9.35   | star-mini.c10r.facebook.com    | United States      |      | 32934 | FACEBOOKUS   | false     |
| 64.25.66.82    | tonhc.org                      | United States      |      | 19356 | TOUA-NOCUS   | false     |
| 31.13.92.14    | scontent.xx.fbcdn.net          | Ireland            |      | 32934 | FACEBOOKUS   | false     |
| 192.0.77.2     | i1.wp.com                      | United States      |      | 2635  | AUTOMATTICUS | false     |
| 192.0.76.3     | stats.wp.com                   | United States      |      | 2635  | AUTOMATTICUS | false     |

## General Information

|                                                    |                                                                                                                     |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 32.0.0 Black Diamond                                                                                                |
| Analysis ID:                                       | 429863                                                                                                              |
| Start date:                                        | 04.06.2021                                                                                                          |
| Start time:                                        | 21:34:18                                                                                                            |
| Joe Sandbox Product:                               | CloudBasic                                                                                                          |
| Overall analysis duration:                         | 0h 5m 25s                                                                                                           |
| Hypervisor based Inspection enabled:               | false                                                                                                               |
| Report type:                                       | light                                                                                                               |
| Cookbook file name:                                | browseurl.jbs                                                                                                       |
| Sample URL:                                        | <a href="http://www.tonhc.org/coronavirus/">http://www.tonhc.org/coronavirus/</a>                                   |
| Analysis system description:                       | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 11                                                                                                                  |
| Number of new started drivers analysed:            | 0                                                                                                                   |
| Number of existing processes analysed:             | 0                                                                                                                   |
| Number of existing drivers analysed:               | 0                                                                                                                   |
| Number of injected processes analysed:             | 0                                                                                                                   |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technologies:         | <ul style="list-style-type: none"> <li>• HCA enabled</li> <li>• EGA enabled</li> <li>• AMSI enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Analysis Mode:        | default                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Analysis stop reason: | Timeout                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Detection:            | CLEAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Classification:       | clean0.win@3/186@14/8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Cookbook Comments:    | <ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Browsing link: <a href="http://www.tonhc.org/about/">http://www.tonhc.org/about/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/mission/">http://www.tonhc.org/mission/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/wp-content/uploads/2021/02/Cafe-Closed.png">http://www.tonhc.org/wp-content/uploads/2021/02/Cafe-Closed.png</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/facilities/">http://www.tonhc.org/facilities/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/facilities/sells-hospital/">http://www.tonhc.org/facilities/sells-hospital/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/facilities/san-simon/">http://www.tonhc.org/facilities/san-simon/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/facilities/san-xavier/">http://www.tonhc.org/facilities/san-xavier/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/facilities/sant-rosa/">http://www.tonhc.org/facilities/sant-rosa/</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/for-patients/">http://www.tonhc.org/for-patients/</a></li> <li>• Browsing link: <a href="https://phr.ihs.gov/phr/PHRLogin">https://phr.ihs.gov/phr/PHRLogin</a></li> <li>• Browsing link: <a href="http://www.tonhc.org/contact/">http://www.tonhc.org/contact/</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Warnings:             | <p>Show All</p> <ul style="list-style-type: none"> <li>• Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe</li> <li>• HTTP Packets have been reduced</li> <li>• TCP Packets have been reduced to 100</li> <li>• Created / dropped Files have been reduced to 100</li> <li>• Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 92.122.145.220, 52.255.188.83, 88.221.62.148, 142.250.201.202, 142.250.185.131, 104.43.193.48, 52.147.198.201, 20.50.102.62, 152.199.19.161, 67.26.83.254, 8.241.9.254, 8.253.204.249, 8.253.204.120, 8.248.119.254, 92.122.213.247, 92.122.213.194, 52.155.217.156</li> <li>• Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypeataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fonts.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypeataprdcolcus15.cloudapp.net, skypeataprdcoleus16.cloudapp.net, skypeataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypeataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net</li> <li>• Not all processes were analyzed, report is missing behavior information</li> <li>• Report size exceeded maximum capacity and may have missing behavior information.</li> <li>• Report size getting too big, too many NtCreateFile calls found.</li> <li>• Report size getting too big, too many NtDeviceIoControlFile calls found.</li> </ul> |

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASN

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F3ABF0DC-C56B-11EB-90EB-ECF4BBEA1588}.dat

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                  |
| File Type:      | Microsoft Word Document                                                                                                          |
| Category:       | dropped                                                                                                                          |
| Size (bytes):   | 30296                                                                                                                            |
| Entropy (8bit): | 1.8557330867588426                                                                                                               |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 192:rVZuZK2ZWYdtliifl6nc+zMO06JWBO56hQDO5cDsfO5c3cvjX:rb6poYnLI66O06gO560O5cuO5cw                                                |
| MD5:            | 1FE07A28FC58ACB4EB242FF9436C16AF                                                                                                 |
| SHA1:           | BCB888B292954EA59208E37C6478376990E12BCF                                                                                         |
| SHA-256:        | 937321691E565B3E3A78A3E40F368EBC20EE77E16A6C06A1D1DF8643A7099724                                                                 |
| SHA-512:        | 29173C771AB1D3FD5D66575658CE6EA401AF19DFA470E910CA40F160850043F75CFD927BF5F0C4FECDC37F7A5C5CD6257FCB89EB0491D7F852E42341BBD17AE4 |
| Malicious:      | false                                                                                                                            |
| Reputation:     | low                                                                                                                              |
| Preview:        | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>.....                                                                              |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F3ABF0DE-C56B-11EB-90EB-ECF4BBEA1588}.dat

|                 |                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                            |
| File Type:      | Microsoft Word Document                                                                    |
| Category:       | dropped                                                                                    |
| Size (bytes):   | 201494                                                                                     |
| Entropy (8bit): | 2.5450016046745105                                                                         |
| Encrypted:      | false                                                                                      |
| SSDEEP:         | 384:rBdLHAcUyGl8+yK+yo+yj8+yK+yo+y5DLdnCnmS/RBe2pqOP8M+89Z904QURTYV6:zsuGsuM+Kfbz+gvPYoljZ |

|                                                                                                                                |                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F3ABF0DE-C56B-11EB-90EB-ECF4BBEA1588}.dat</b> |                                                                                                                                 |
| MD5:                                                                                                                           | 03C6E97D20B478D35AD754C6B6E26B33                                                                                                |
| SHA1:                                                                                                                          | B45CD134EEA6A04CCC9CC34712C8A83E33B74447                                                                                        |
| SHA-256:                                                                                                                       | E6BF9610DA140F9C9201C359FD2CAFB8526F0B5981D8658DE7EC4CD771A52181                                                                |
| SHA-512:                                                                                                                       | BCFEC04687EBEAA68D0A391CB4D2594158BF0D0D28FFFD9824B84ADA5F6AE4896B73A7BB32838C1D3915DBFB0D2D9C244A786A79BC53EA5110435DE285E9C4A |
| Malicious:                                                                                                                     | false                                                                                                                           |
| Reputation:                                                                                                                    | low                                                                                                                             |
| Preview:                                                                                                                       | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>.....                                                                             |

|                                                                                                                                |                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FBEA4EDE-C56B-11EB-90EB-ECF4BBEA1588}.dat</b> |                                                                                                                                 |
| Process:                                                                                                                       | C:\Program Files\internet explorer\iexplore.exe                                                                                 |
| File Type:                                                                                                                     | Microsoft Word Document                                                                                                         |
| Category:                                                                                                                      | dropped                                                                                                                         |
| Size (bytes):                                                                                                                  | 16984                                                                                                                           |
| Entropy (8bit):                                                                                                                | 1.5658584487055516                                                                                                              |
| Encrypted:                                                                                                                     | false                                                                                                                           |
| SSDEEP:                                                                                                                        | 48:lwMGcprRGwpap0G4pQdGrapbSwZGQpKiG7HpRpaTGlpG:rQZLQq69BScANTkA                                                                |
| MD5:                                                                                                                           | 54CAE29F061C76FCBE3C2809B8B5B442                                                                                                |
| SHA1:                                                                                                                          | F841185BA330048DA2DA215B23A276674D7F97E2                                                                                        |
| SHA-256:                                                                                                                       | 256D9976BB57608F0C93BA87F07CEA2E93F390EFDDBC734314FDACD463C259CBD                                                               |
| SHA-512:                                                                                                                       | D019FEE542064CB12ACF7B13A6C0329DDAB3F12500D5DD08F4AC0CC7C5968C107CFE00535B5957853356A06C7A14A34CD686727B873323B954EC80DB9FA3ED8 |
| Malicious:                                                                                                                     | false                                                                                                                           |
| Reputation:                                                                                                                    | low                                                                                                                             |
| Preview:                                                                                                                       | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>.....                                                                             |

|                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Process:                                                                                               | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| File Type:                                                                                             | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Category:                                                                                              | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):                                                                                          | 656                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Entropy (8bit):                                                                                        | 5.077347775228598                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:                                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:                                                                                                | 12:TMHdNMNxOE/4q94CGCnWimI002EtM3MHdNMNxOE/4q94CGCnWimI00OYGVbkEtMb:2d6NxO+4E4CGCSZHKd6NxO+4E4CGCSZ2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MD5:                                                                                                   | 10A34D83401FC4B4C3C90F7708D7D873                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:                                                                                                  | D2BD6F2DCDDC394659F87A0480DFD4332555BBEB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:                                                                                               | 29AE7B3EA610F42EDB63DA7B4901356253540E60CB8C20F66719D2604CF23BC2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-512:                                                                                               | 2D4DF8BF246A007D1EB0E79BB59E6BEAC0CB3FC73BD152584DBD6DB02CE52FA56A29E2E744C3919B2A8F754034EA9A52FE96D7E8E325B8E8985458A56083DC31                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Malicious:                                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:                                                                                            | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:                                                                                               | <?xml version="1.0" encoding="utf-8"?>..<br><browserconfig><msapplication><config><site src="http://www.twitter.com/"><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<br><?xml version="1.0" encoding="utf-8"?>..<br><browserconfig><msapplication><config><site src="http://www.twitter.com/"><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>.. |

|                                                                                                        |                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml</b> |                                                                                                                                 |
| Process:                                                                                               | C:\Program Files\internet explorer\iexplore.exe                                                                                 |
| File Type:                                                                                             | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                  |
| Category:                                                                                              | dropped                                                                                                                         |
| Size (bytes):                                                                                          | 653                                                                                                                             |
| Entropy (8bit):                                                                                        | 5.135601278573843                                                                                                               |
| Encrypted:                                                                                             | false                                                                                                                           |
| SSDEEP:                                                                                                | 12:TMHdNMNx2kPpdJGCnWimI002EtM3MHdNMNx2kPpdJGCnWimI00OYGkak6EtMb:2d6Nxr4GCSZHKd6Nxr4GCSZ7Yza7b                                  |
| MD5:                                                                                                   | 7EBA67DAD0D857238595EBF09DEF37AA                                                                                                |
| SHA1:                                                                                                  | 0D00E327031306A4D5568302F6BB830A6F379D33                                                                                        |
| SHA-256:                                                                                               | 9600E2F7A62427A6220D3ADE000110134A069D7D0E32B189FA4B35D0635E9040                                                                |
| SHA-512:                                                                                               | EB563982D9ABF880DC522EA31025959CB37601B2CEFDA0D5184F00698DB7F6465EF55C1FD3CF54FE638455ACE6F1226C6502163DFB4BE61BEE740F536C147DC |
| Malicious:                                                                                             | false                                                                                                                           |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reputation: | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:    | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcd2ebe48,0x01d75978</date><accdate>0xcd2ebe48,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcd2ebe48,0x01d75978</date><accdate>0xcd2ebe48,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Size (bytes):   | 662                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Entropy (8bit): | 5.093568416398742                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:         | 12:TMHdNMNxxvL/4q94CGCnWiml002EtM3MHdNMNxxvL/4q94CGCnWiml00OYgmZEtMb:2d6NxvD4E4CGCSZHKd6NxxvD4E4CGCSZy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:            | 76F74B12FEAC326EFD65130C3E7BA3E4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:           | 509EE624A2F62EB2E0CD3BCFE9C481E0E1E57D36                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:        | 0C5ECE7D922E62EF7B6F932AB3474E3247DC4882FC6F0AFBE2037BC2C8581187                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:        | 712128D9E671E51AE874D08C4F0C787AB47ECD1D9FF68BAF2E53AD642BBCCFFCD30D2A77E3B5A0ED5BA7A776CA6137091B200F617B3070B229F7C634014503F55                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:        | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):   | 647                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy (8bit): | 5.081007858360016                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:         | 12:TMHdNMNxiFdvLdDGCnWiml002EtM3MHdNMNxiFdvLdDGCnWiml00OYGd5EtMb:2d6Nx8JNGCSZHKd6Nx8JNGCSZ7YJeb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5:            | 7559DBD8B757C3571AD431DA9B6965AD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:           | E0FA7494A172215167D0BD6105D0A88A2F04B5F3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:        | 99EE3F65D76C8D473B0421548FBA09169C2B714D721DF53135DCE5A9C24EC5A5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:        | 4550619B966BA3EBDF7A77D3F95F4D8BC40A498AD2C77199075564247AC9016C321F09B3BF77C1CE9FEB5082E76D40E1F7D99B3262A1AD0EFEC1ED1B97558C1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Preview:        | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd3d0c88,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd3d0c88,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                  |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                   |
| Category:       | dropped                                                                                                                          |
| Size (bytes):   | 656                                                                                                                              |
| Entropy (8bit): | 5.107987241577909                                                                                                                |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 12:TMHdNMNxxhGw/4q94CGCnWiml002EtM3MHdNMNxxhGw/4q94CGCnWiml00OYg8K07/:2d6NxQ64E4CGCSZHKd6NxQ64E4CGCSZw                           |
| MD5:            | 05F903F8B73F8F4D6EDD2185E946386F                                                                                                 |
| SHA1:           | ABD040CACE9C10B193B6A83B0A7E407B9CB9E178                                                                                         |
| SHA-256:        | 447ECBEC5B24398DD8A28C6282288E48EE12586342AF8DCCB35AB18BC8E76C0C                                                                 |
| SHA-512:        | 1DD6BA7D0F65C3F566D69B931FF83E536654C1A5AB89A3E50315824FA1D6F522177B243CC9817846E17498221F61B54975A955E2BB2100FFEA55747E5E0A84D6 |
| Malicious:      | false                                                                                                                            |
| Reputation:     | low                                                                                                                              |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0xcd4dbd0d,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>.. |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):   | 653                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit): | 5.072725828942823                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:         | 12:TMHdNMNx0nFdvLdDGCnWiml002EtM3MHdNMNx0nFdv94CGCnWiml00OYGxEtMb:2d6Nx0FJNGCSZHKd6Nx0FL4CGCSZ7Ygb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MD5:            | 5B043B39389F30CFFA73DC6330AC4455                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA1:           | 91BD03CEB4EEDF095FD94ACFE4A89B029065CF85                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:        | 1699006AE97C71BB946769E6ADD4216148390508081B3E2184EDC6A7383D017D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-512:        | E08DA266516F434E3952F0885B5057C8000334E27F762EFF338C3A3D8F31EC1B16F9EDDC91480CC7E3ACEAC40A85A3100FAD81F01D64CADE6AC678BC1FFEEFA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Preview:        | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/" /><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd3d0c88,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/" /><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd4dbd0d,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Size (bytes):   | 656                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Entropy (8bit): | 5.1055705243164295                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:         | 12:TMHdNMNxxFdvLdDGCnWiml002EtM3MHdNMNxxFdvLdDGCnWiml00OYgKq5EtMb:2d6NxXJNGCSZHKd6NxXJNGCSZ7Yhb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:            | C3A58875319324DD555FDE7A58A154C8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:           | 03FD7D83F7C587F1D5E07CEB1ED4AB3D2303180D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:        | 8F0B47FEA4C51D3E32A878D6C8A3389C55AAA61F4FD42AD7C9E070027A74D64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-512:        | BE09D1412BC17688DD17FC9567D8E043BE44C3FE02CFEFD8A9877FFBCAA42137D1201CB3DC9A25918E4F9D38EC428D2BDA0F7D29A57AE738F96EE73A55CC9E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/" /><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd3d0c88,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/" /><date>0xcd3d0c88,0x01d75978</date><accdate>0xcd3d0c88,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| File Type:      | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 659                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit): | 5.094333978841497                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SSDEEP:         | 12:TMHdNMNxcNzbZGcNWiml002EtM3MHdNMNxcNzbZGcNWiml00OYGVetMb:2d6NxqdZGCSZHKd6NxqdZGCSZ7Ykb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | 2E53011F49F19145605C7ABD017BB0DC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA1:           | 794A6C50E4DD9A1A302ABF910B335C172278C177                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-256:        | 635DDDB1168A0CE48EE39EBCA38C34B3F4AB349D8C7B63B69253958F941AACAE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-512:        | F02828CC59C84DD45C9C88625D258517500C752297EEB8D12C81B9C83DF46D1751E7EC890883896463A14DCC13BE2B411554C86572C5EA7A8D1942D6C73FD89                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preview:        | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/" /><date>0xcd35e571,0x01d75978</date><accdate>0xcd35e571,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/" /><date>0xcd35e571,0x01d75978</date><accdate>0xcd35e571,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Process:                                                                                       | C:\Program Files\internet explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Type:                                                                                     | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Category:                                                                                      | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):                                                                                  | 653                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit):                                                                                | 5.074573182444342                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:                                                                                        | 12:TMHdNMNxfnNZbZGCnWiml002EtM3MHdNMNxfnNZbZGCnWiml00OYGe5EtMb:2d6Nx1dZGCSZHKd6Nx1dZGCSZ7YLjb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| MD5:                                                                                           | 51E45EBC9FF073F29CC5D482989D85F2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:                                                                                          | F90FCA34F1932537E29426185FB733E2209CFC51                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:                                                                                       | 9F7BA9B5DCC9ED1A2BEB4951915F09315128FC47F0CE6B11723A65D74A9F2C8B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:                                                                                       | F925F574FC52BE0BD0DEAA46EF1C87A1F327914995EC8E6213A69F8BCBB028B047863B2D5475E8A0A623E86C74BE6B3B6159E4A9C0D6C6557A389110740DE52C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Malicious:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reputation:                                                                                    | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:                                                                                       | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcd35e571,0x01d75978</date><accdate>0xcd35e571,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcd35e571,0x01d75978</date><accdate>0xcd35e571,0x01d75978</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Google.url"/></tile></msapplication></browserconfig>.. |

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):   | 35206                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit): | 7.985052726182913                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:         | 768:+cM/8+liAg9TsTN1Mu0BHSIKL9thJt+0qkRhK6hWr5JwS8bB:+csv5ITN1MPBHS7L/d9Rk6UrfwSOB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | 0B3C270A0B3A62FA4FA228E5F1A8BD59                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:           | 51C04FB467FE6D1C0B12A5822231C36041FDF6FD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:        | B7D8801626923DD0C8832A27FA0B96DAC1D78B7A0DD0FB4D434919DCFDFA1CBC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:        | 0D9BECA11D84ED7830F998E3C7C6EEB63040FF0ED2BBB82EEBCC7B939D54A1E7A2F03FD8176CD4D37B62CD7566AEAA5424391C77587772683EC580E71BF24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:        | E.h.t.t.p.:.//.w.w.w...t.o.n.h.c...o.r.g./w.p.-c.o.n.t.e.n.t./u.p.l.o.a.d.s/.2.0.1.7./0.9./F.a.v.i.c.o.n.-3.-3.0.0.x.3.0.0...p.n.g.Yx...PNG.....IHDR.....y}.u....gAMA....a.....sRGB.....cHRM..z&.....u0...`.....p..Q<...bKGD.....pHYs...H...H.F.k>..wNIDATx..w.\$gy.....'.MT.....Y..J.,k.a.5.q.....^'.5...cr...<....M.'..9V..x{...P...v.....sFs.....y..j.....@..{..wA....g..5.@.5G...?s@.....&...*.+.Q..5..J..\......D..Z...Q<..X.....U.M.E.M.U.U....^..l0-g.....j...g.G..{...c.Hh...g..vKk.U..Z. ...XU.....@...rh....(. 'jC...".B( ~..?.....pj.t.C+...lN@7....n.?..u.d!..D.....8...:ia.&abY..`.....A`.8S..(Fq`.....a.P..lS1BZ.l...=.)..(>..M.....]m.....A?..]r.r.....Z..^\$.....\$.01...0:.cS0...qAfs...`.6.b...F.C....bt6WK-k.UCuDP...X.l.l/FN=F....C]...`...tAo...5Cs=....U:t.q.j...Y....cp,..A4!....2Mf..6....N.....jG..UL....uM/X%-k....^p.E...i..0M.^.....\$.:.....0L.a..9Dj]....../...u..j.U...S\$.... |

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUUI0U\BOGz5uZCI[1].css

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:      | ASCII text, with very long lines                                                                                                 |
| Category:       | dropped                                                                                                                          |
| Size (bytes):   | 25410                                                                                                                            |
| Entropy (8bit): | 5.3849178317989805                                                                                                               |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 384:sPVycB4IITlvAn8nAUZWFvbcYUliSHki7:sPctlNlvA8ngvCYZJ4                                                                         |
| MD5:            | CA390CEFF7FDEEEC3E02911BB6BA4F25                                                                                                 |
| SHA1:           | C0913365A3FACE622D6F559792C26725DA957D8C                                                                                         |
| SHA-256:        | 4F1F49980C51348FC971FD53F6DC03A486D7698F348A9FD01EF5DF4E2B5AD251                                                                 |
| SHA-512:        | 97199490581E9C2937FE5060FB68F0C694CE08DC2677D1793770F6F6C2D9FF37AF1E989E766EF7C5791D31500A2CFE1F22E1ED00FD2C749D9C6BF0E1FB5E170F |
| Malicious:      | false                                                                                                                            |
| Reputation:     | low                                                                                                                              |



C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\16486968\_419413705060919\_4560230974885411816\_o[1].jpg

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | .....JFIF.....Photoshop 3.0.8BIM.....g..7FvjXg6QDiFlobJfGk4i..(bFBMD0a000a87010000fd010000a1020000f8020000650300006f04000080050000c005000017060000840600000e080000...C.....%...#... , #&)*).-0-(0%)(...C.....{.....((((((((((((((((((((((((((((((((((((((((((((((((((((((((2.2.".....S.8H.....<.....Z.n.1.....V..B.2..(&'...u.R .)!.....O.....!.....\$. 4.....)..l6a.30...CE...y..l..bE...  X.Zc+..YX1...D.....?F...o...i[.Y.e.n....X(,DD.t....=B..*e..&Mt@.J.?MZ:_P.....!12.....?Jz.d:W.g....T....\$.l.Y.Eu..4.7.....~o...\$.....1.!2Q.....?.{.r....9.w7(_%...h.Jl.d.S.uG.....3.....!1Q."2Aaq.#B...R... br.....?.%.@#.:6].....3-_ET7.aO...*.y..4~....l...?.Z...p2w.dvN.k.....c:wN,..5.....f.1.....!2.E-.Mq...#.....Y..S..r |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\16486968\_419413705060919\_4560230974885411816\_o[2].jpg

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| File Type:      | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 50x50, frames 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Size (bytes):   | 2062                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 7.281621708763654                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SSDEEP:         | 48:K/vumiWGPVWsF1pwNhU1RwypSLkRi/OX/7SOjxTSYCPX2:omrYhU1Rhk8GOXmOjtCu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| MD5:            | 39A9957B73D2E99943BBD1A107BCA1AC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA1:           | C75305A07B14E0F668A91BB1835A8194A8D751C5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-256:        | D9822D50D8A2C98184EFA311238697DFF17C7473A308AD03CD8B7330455A0099                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-512:        | F7453E05FA8C2409693C673F9685B51407EE252F17F1057B19CF6DBAE83F056F8995605C11D8EA6C851DBA2DF1E346F707DE1B72C0494E75A3E2277EB99C9CF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IE Cache URL:   | <a href="http://https://scontent-frx5-1.xx.fbcdn.net/v/t1.18172-1/cp0/p50x50/16486968_419413705060919_4560230974885411816_o.jpg?_nc_cat=105&amp;ccb=1-3&amp;_nc_sid=dbb9e7&amp;_nc_ohc=eSS5Wlk3618AX868K1s&amp;_nc_ht=scontent-frx5-1.xx&amp;tp=27&amp;oh=9681efb9d92047f2724e248cec7c94e7&amp;oe=60E12194">http://https://scontent-frx5-1.xx.fbcdn.net/v/t1.18172-1/cp0/p50x50/16486968_419413705060919_4560230974885411816_o.jpg?_nc_cat=105&amp;ccb=1-3&amp;_nc_sid=dbb9e7&amp;_nc_ohc=eSS5Wlk3618AX868K1s&amp;_nc_ht=scontent-frx5-1.xx&amp;tp=27&amp;oh=9681efb9d92047f2724e248cec7c94e7&amp;oe=60E12194</a>                                                                                                           |
| Preview:        | .....JFIF.....Photoshop 3.0.8BIM.....g..7FvjXg6QDiFlobJfGk4i..(bFBMD0a000a87010000fd010000a1020000f8020000650300006f04000080050000c005000017060000840600000e080000...C.....%...#... , #&)*).-0-(0%)(...C.....{.....((((((((((((((((((((((((((((((((((((((((((((((((((((((((2.2.".....S.8H.....<.....Z.n.1.....V..B.2..(&'...u.R .)!.....O.....!.....\$. 4.....)..l6a.30...CE...y..l..bE...  X.Zc+..YX1...D.....?F...o...i[.Y.e.n....X(,DD.t....=B..*e..&Mt@.J.?MZ:_P.....!12.....?Jz.d:W.g....T....\$.l.Y.Eu..4.7.....~o...\$.....1.!2Q.....?.{.r....9.w7(_%...h.Jl.d.S.uG.....3.....!1Q."2Aaq.#B...R... br.....?.%.@#.:6].....3-_ET7.aO...*.y..4~....l...?.Z...p2w.dvN.k.....c:wN,..5.....f.1.....!2.E-.Mq...#.....Y..S..r |

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\175403742\_1478406012495011\_3389624806742482905\_n[1].png



|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| File Type:      | PNG image data, 331 x 414, 8-bit/color RGB, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):   | 162350                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit): | 7.990600535312483                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Encrypted:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:         | 3072:FwxMqP2AUbrGiYxTuc0uzBrW5rTKgaraJr2qH166RUnpimddcS7W79C+f+l:eleAEGZxTuc0uzBMmaWQqHw6qnpNcef                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| MD5:            | 02942497A15FB2DFF31D30173655DCFA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA1:           | 751E7C5CA789B2971B128EFD30BBE4336FC0B7B3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-256:        | FAEDEF98B472F2B8B3925585EE02CC73F191F53AB98C8AB7B98402D50F26AE84                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA-512:        | 32BAB23C696F6154942EFE08057A34CF82E6BB3A062160D2FE34EFE1C0027F7A3F4A4ECC212CC649534FA12307951F55754E6703283F1254BC8019862A1B9C70                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IE Cache URL:   | <a href="http://https://scontent-frt3-2.xx.fbcdn.net/v/t1.6435-0/s552x414/175403742_1478406012495011_3389624806742482905_n.png?_nc_cat=101&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=8C3fvUape_kAX8vCajH&amp;_nc_ht=scontent-frt3-2.xx&amp;tp=30&amp;oh=8d7db26c827bddf0c4531805f704c48b&amp;oe=60E1039A">http://https://scontent-frt3-2.xx.fbcdn.net/v/t1.6435-0/s552x414/175403742_1478406012495011_3389624806742482905_n.png?_nc_cat=101&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=8C3fvUape_kAX8vCajH&amp;_nc_ht=scontent-frt3-2.xx&amp;tp=30&amp;oh=8d7db26c827bddf0c4531805f704c48b&amp;oe=60E1039A</a>                                                                                                                                                                                                                                                                                  |
| Preview:        | .PNG.....IHDR...K.....&U.....sRGB.....SzTtRaw profile type iptc.....P.....#Kx.^`].O..y..l.....l.....H8..r.Y.-.....#1O....!DATx..w.U.7 ...{zz..0dT0...%.PT.5cZ....b.u.k..b,kND.9..ab.t...{..G..0.....[ _=-vW...N.....wY..P.....@ .....O.....).....a.&".....C.. [ @.(l..l..F.S.l.....!1....2%C.Bw.y_.mv.&R.7..\$}.#R.R8\$.."U.....w.....).Q..8....`n.9." J...x...O.dL1<.%!.^+.E".....=,!%oQ~9..1d.9..0.L.%.....\.,Y.k.R..H2..d..t.H..e....@RX..m..q..li.J.L.v.?A../.E..l.OE.j.L.H....A.#....\$.RR)EL..0.....\.....^..9T.....S....r_qs..`L..UT..L@.z.....y.85uDB...../L...x...lJ ...e....EyC[...f.....t1.....J.7]C.l.^.....0.....U.l.lw.!1.....-E ..J.)C..D....&.l.n...+!..d\....".B@.F..3...R.! ...L.....B.mTz. ...!..R...*Pl..a...X.F.v.....].....a>2..ji.....9.....*SZ&..."d.....]....glR..`~. W..pO..&E'.....t)....t.E.[>d.....le.r.yz.HJ.B""2FB.s1..)'...AN.....Q..~...a.a.... G.V...L.....1.. |

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\188888692\_1505957103073235\_1769118996642174241\_n[1].jpg

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| File Type:      | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 331x414, frames 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 34236                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Entropy (8bit): | 7.978104305061718                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SSDEEP:         | 768:uRgH1P466gsedAMpRDrMWumq9Z/fmwkndDUBtfoe2:sgHV466gseuWrq9lmDCCb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:            | FE648EFE6D1C5FE7AFE91D21ACBABCAD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA1:           | 0F063B4A22355B86F03C4167513CFBA0AD0339FB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:        | ED2248E76A60D223C8E0723FB3189DE2EE4BA35AF3DA3937C4DA87C64AC7EFAD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-512:        | BD9BDC3006EF5882DC86751CFB8E667C2046C7164EAFE13213049AE9F4E1934F8179F33BC0AF84B4AC196EDB3B7920210FC58DD6F51817094F532533E82969C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IE Cache URL:   | <a href="http://https://scontent-frt3-1.xx.fbcdn.net/v/t1.6435-0/s552x414/188888692_1505957103073235_1769118996642174241_n.jpg?_nc_cat=107&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=ybjL_eiQ2fYAX8yQHwg&amp;_nc_oc=AQlwvCrNPd7NiiDledlfpXj11AJTGPWCNs9YYENvV9tze_SqZEvw6TPQGUBJzyuUU&amp;_nc_ht=scontent-frt3-1.xx&amp;tp=7&amp;oh=f99d4b2d88f1653acbfdb74d67926a3a&amp;oe=60DF0DEF">http://https://scontent-frt3-1.xx.fbcdn.net/v/t1.6435-0/s552x414/188888692_1505957103073235_1769118996642174241_n.jpg?_nc_cat=107&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=ybjL_eiQ2fYAX8yQHwg&amp;_nc_oc=AQlwvCrNPd7NiiDledlfpXj11AJTGPWCNs9YYENvV9tze_SqZEvw6TPQGUBJzyuUU&amp;_nc_ht=scontent-frt3-1.xx&amp;tp=7&amp;oh=f99d4b2d88f1653acbfdb74d67926a3a&amp;oe=60DF0DEF</a> |

|                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\188888692_1505957103073235_1769118996642174241_n[1].jpg</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preview:                                                                                                                          | .....JFIF.....Photoshop 3.0.8BIM.....h..(bFBMD0a000a710100003909000046150000701d0000a02100009a370000df500000c2520000d85a0000a75f0000bc850000....C.....%...#... , #&)*)..0-(0%)(..C.....(..((((((((((((((((((((((((((((((((((((((((((((((((((((((((.....K..\".....1..s.KG....K .b.#9.B.....U.QP^..`ju.T.B..^k<.ZR...Y4..R\%.U.b.....{.v.~.N.*\$.w...j.j.km.4<.m).j.r.Q..G8ZS~@-.....(=M...3.Z#(F.... V.4.....(..j2..3..9'7.s"{.). ...f4...y.2....cP..8.H..WaR.w.>...>.....,m."...0...yf.J...@.T2.\$2...!~y.....?.py.....[^.h.}.HUd.%[...E,...6.,L9be.ih.a.X..F..q.6..F.....^.....x!.....~y+vn..EBN.t.MzHh.>(t....Q.X.Z..n.z:.....3..0.....8}.6.....ws..>...SiX..o..G0..U.\$..Y;3...&_W.....7G.....3.ud....?!.=...1...@a..4...Q...u..+..U.....%W.+Q.C.,\.[...-0.....G..R...Z...W.n |

|                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\191433657_1504648103204135_8784403890329073815_n[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Process:                                                                                                                          | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:                                                                                                                        | PNG image data, 261 x 326, 8-bit/color RGB, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:                                                                                                                         | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                                                                                     | 81944                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Entropy (8bit):                                                                                                                   | 7.964381904102698                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:                                                                                                                        | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:                                                                                                                           | 1536:6NRkum0W6hqMyntEb+AvNUBUkcSOXK5/xZwBd5VudSsaoLGJf/KJGX1:6L1W61yttEb+Av+Bo6VxZwB71IGpSJO1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:                                                                                                                              | F672AADB45358D8502FD23B77929633C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:                                                                                                                             | E6A5C90F752F392A809910F1CF31540D1AC060BD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:                                                                                                                          | D0121870A3644FC49A47BB42E28B1E6CF2AA9158FF92BEA4D45D9D92AB72223C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:                                                                                                                          | 0365325BE423B8CB9ACA2D72BA981FB8E4B832FB2B603C361D118A438D5299F2F7608FF34B2552929BDBCCF621B1E78E75A1B3A9197BEAEEB8BAF6D7C4AC720F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Malicious:                                                                                                                        | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:                                                                                                                       | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IE Cache URL:                                                                                                                     | <a href="http://https://scontent-frx5-1.xx.fbcdn.net/v/t1.6435-0/p261x260/191433657_1504648103204135_8784403890329073815_n.png?_nc_cat=105&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=naQZ5QNBrgYAX_i8B7V&amp;_nc_ht=scontent-frx5-1.xx&amp;tp=30&amp;oh=a4d3b7856eee2594a2f199ca60073480&amp;oe=60DFE0F5">http://https://scontent-frx5-1.xx.fbcdn.net/v/t1.6435-0/p261x260/191433657_1504648103204135_8784403890329073815_n.png?_nc_cat=105&amp;ccb=1-3&amp;_nc_sid=8024bb&amp;_nc_ohc=naQZ5QNBrgYAX_i8B7V&amp;_nc_ht=scontent-frx5-1.xx&amp;tp=30&amp;oh=a4d3b7856eee2594a2f199ca60073480&amp;oe=60DFE0F5</a>                                                                                                                                                                                                                                                                                   |
| Preview:                                                                                                                          | .PNG.....IHDR.....F.....8.....sRGB......IDATx..}w \.....j.dK.{7n8.C. (qp..%\$...K~@.H....%.!.....6.w.{.%.IKV.Z.....f~\QL.66....g}.w...9s.s.B...<.}:....8C..^.....;... B...../s.....3.#n...s...&.c.F.r.cY..Bt\[{ ..:X.EB.\$..B..(.!(D.....9Q.+z ..L\$("R.....[[...a.{X.RD\$.,fk~qy..StZ.. .2D.R.../p./+...".\$.x,...2...j.6...h...4.X..@...R..1&...e.%X.8G.,.....O..9T.N_>..{.%.&.....'YY.F.zG-2S.,^p.s.T..dQD4.... .@\$..p ....5.r..q9...P~...y..BC.R...p.( hY.b.h.f.1&.. ..)2.....!..2E...=.G..9)2..3..PK.....O4..\$.k.w.i.X....tA .2.=...1.?...R\$.g...QA%..r... BH.e.@DD..*\$.....*q.T.82s4Z.&B....1..CD=...w.]].7.k;Q...M... .1..liQ<E....."u...V.u.....!.....!1.@.._(. ....h(tff.....e)..!.`B...B. ....L\$.b<G...t.efg.-&...O.O@!.....M.W....G[.uXJ&fO.M..`j.!CY.*6.l.N..../.=F..k.a.7..h.].#...Q..D_P%..P.!J..\.t.DW..J.%3X..0...%b...ld.,2@4.c.)\$%j..S...a.N..-z.r..gO.D&...8.....b...C.. |

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\3PPD5qbge6n[1].css</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                     | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                                   | assembler source, ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:                                                                                    | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):                                                                                | 21734                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                              | 5.362169381432253                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                      | 192:0gz/kitOmrLPeHNn123U096AAD/IplPNunlFdsak7dSAGMDFbSI9eDBz9U0azYV:0okit5rdU0963/lbPNuz+LS/eF4/Y4Rf                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:                                                                                         | 1AAB40013DFF7FA699E5ACC9642EE4A4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                        | 54510FFA332A26D29A99163980D9E5D450DDF377                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                     | 572C0C04A8128FBD4A8818BCE476FB47737FDA001514D40BAF570FBE1A601BFE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                     | FC8B2DDFAEC732C1A1DE3C734F4498CB836C9C39D03147377630FFE6457C265CDC829D0D732383DDD478AB2C105BDFE4118B637F3B4DDB9545E96B28C77A2/8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:                                                                                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Preview:                                                                                     | .fbEmuTracking{position:absolute;visibility:hidden}..text_exposed_root{display:inline}.text_exposed .text_exposed_show{display:inline}.text_exposed .text_exposed_show .text_exposed_link{display:inline !important}.text_exposed_show..text_exposed .text_exposed_hide{display:none}.text_exposed_link{white-space:nowrap}.text_exposed .text_exposed_link{display:none !important}..._605a . _4ooo: not( _1ve7).. _5eit . _4ooo: not( _1ve7){border-radius:50%;overflow:hidden}._605a . _7mi5: not( _1ve7){border-radius:8px;height:40px;overflow:hidden;width:40px}._6y97{border:2px solid #bec3c9;border-radius:50%;box-sizing:border-box;padding:2px 2px}._6_ut._6y97{border-color:#3578e5}..._38vo{position:relative}._605a . _38vo: not( _1x2_):after, _5eit . _38vo: not( _1x2_):after{border-radius:50%}._605a . _7mi8: not( _1x2_):after{border-radius:8px} _38vo:after{border:1px solid rgba(0, 0, 0, .1);bottom:0;content:";left:0;position:absolute;right:0;top:0}._44ma{display:block}._354z{background-color:#42b72a;border:2px solid # |

|                                                                                                    |                                                                                                                                  |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Favicon-3-300x300[1].png</b> |                                                                                                                                  |
| Process:                                                                                           | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:                                                                                         | PNG image data, 300 x 300, 8-bit/color RGBA, non-interlaced                                                                      |
| Category:                                                                                          | downloaded                                                                                                                       |
| Size (bytes):                                                                                      | 30809                                                                                                                            |
| Entropy (8bit):                                                                                    | 7.987134417812598                                                                                                                |
| Encrypted:                                                                                         | false                                                                                                                            |
| SSDEEP:                                                                                            | 768:XM/8+liAg9TsTN1MuobHSIKL9thJt+OqkRhK6hWr5Jr:Xsv5ITN1MPBHS7L/d9Rk6Urrf                                                        |
| MD5:                                                                                               | 882C6E098F2F6F863FD66747DC208A37                                                                                                 |
| SHA1:                                                                                              | 62EC4D93EF856CBF9F965BC38846EA3F893FF83D                                                                                         |
| SHA-256:                                                                                           | FF3713EE5DC955E2C32B4FDB5226E65F73D780CAD0293E712035E1A05EC945C8                                                                 |
| SHA-512:                                                                                           | 1A15D6601EFD935CF4E810BB555DEA6C14378BFF5336820794ABC4A9E2DF6467CF403D6EC894348710E9BAA4A5B49A43F5AD01D8F60A92F58655A4531A322734 |
| Malicious:                                                                                         | false                                                                                                                            |
| Reputation:                                                                                        | low                                                                                                                              |



|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\IPHR[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:                                                                           | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:                                                                          | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IE Cache URL:                                                                        | <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=413%2C150">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/PHR.png?resize=413%2C150</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:                                                                             | .PNG.....IHDR.....2.....PLTE...\$.REB.....R.....2.....D;8.....L@;...<75...=.....y.....~.O.....H..m..[...U.....f.....0\$.`.....t.....310.....8.....C.....+)(.....&\$".....[LD.....Fa~.e=+.....t...cSJ...5,&.lJ...?3*.iTX9(..j).>{(.....v.h.....L1".....t.j.0.....a....TC.....aOQNN.yxQ<z.s\.....}i"..EEE...egfhJ6..[...sH5YE8...^=.K1.....^ZY....Y..U8.bd.oN...wS. ^...vH.kCu?).].....xqnm..mB..r_kR.....~.....rWJyv...q.iX..ub-aL...~..n`Y.sg.L.8>@N.../..#]u.....].....z...~NY..2k.i..MY[...ZK}.....Js.....V....p..^..vM....Dbp...yh^].....c..f.....dx}\$*..*.Gp.....l.....E.;.....Sa.....J..wL...l-IDATx...K"m.....6#....G..JL..)*%.. ....0x..C2....{ .....g.B.B.o.".....^.=.....>5.... .\\....BSdY.hW...`h.r.jl)Y..Z\$*;Y..y.IJ..Z..+X.r%...+*WP.3....k]....r1r....`W. |

|                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\San-Simon-Map[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                      | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                                    | PNG image data, 2000 x 659, 8-bit colormap, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:                                                                                     | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):                                                                                 | 35593                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                               | 7.925903152323706                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                                    | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                       | 768:Uw5QLirfNNkCZYsINiOcYsxz85+4ds3WfaPu2gmw3416e3:UwbjkOOi5YCz85+4dhkPmG4a                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:                                                                                          | B37B15BD52D07F52061C681665C101D1                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                         | 7D165AAEB54D475F5BC19BE56D3D35CE37C83321                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                      | D7FE2F53AFB4466F35215B260A3018C53CACD8D8A4EEF5D512FAD04F40E00BDC                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                      | 0F809904CE07F25855B989059FD28C0FF856584A0698B24F0940E20598BF74D8CE36971E2350EBB68EA5CD8C5269A1FAE0DA436C80DF5E2F805485C2622443B9                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:                                                                                    | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:                                                                                   | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IE Cache URL:                                                                                 | <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/San-Simon-Map.png?fit=2000%2C659">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/San-Simon-Map.png?fit=2000%2C659</a>                                                                                                                                                                                                                                                                    |
| Preview:                                                                                      | .PNG.....IHDR.....v.c.....PLTE.....g.X....P..`.....g.....q:...vB.....p..... l.o.q.j].....v....e*.k3.....nR...www...><...w.....}.....^".....}.10.....ro.....W...x_...~.LK.....cF,'...db.....}z.#.....M.....iL...94....}d.tY.! ....l.....r.....XU..{.JE.....}Z;.....83..aZ...kf. u....`>.PL.^Y...D?jjjKM... ..x.....T.).....IDATx...1O[Y.....7p...6fm.D. ."D..b.b.a.f.2.i.&? .).f.FZ....S..2...n..l6.gw`...SE,.....q...`^ .B.i...Oo..1..(..^.._<...kC.U4.7.....m...{...@...z..!..@..X..U |

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\San-Xavier-Map[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Process:                                                                                       | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:                                                                                     | PNG image data, 2000 x 659, 8-bit colormap, non-interlaced                                                                                                                                                                                                                                                                                                                                                            |
| Category:                                                                                      | downloaded                                                                                                                                                                                                                                                                                                                                                                                                            |
| Size (bytes):                                                                                  | 111226                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit):                                                                                | 7.972617027851128                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:                                                                                        | 1536:NMCAWw/60sx8y8LvqHB1TOppAsFfSCyo2O1rgYNj7tDuXe0nwWfXRNIDSrpAo+0+:Ndw/6048Gh1zkxj1v5e7vrv+h                                                                                                                                                                                                                                                                                                                       |
| MD5:                                                                                           | 2F451F8D09F119228459824305431F0C                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:                                                                                          | 3F04188AC81BD6903B7C5AF8C2BB61FFC899DA5C                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:                                                                                       | 923068230F9980E9610E95D9BC5567C5FD8D4714C99F4323511356ED82BED4A6                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:                                                                                       | FE2BF01014EA46E0A190FA0B7EB4271DCE30A1B39D65BD07A95951EBB7B6B9FBC32DB2DF1240462264478F7E318B8260BC142EFF45B5A3D87DA6ACE973A2E1B1                                                                                                                                                                                                                                                                                      |
| Malicious:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:                                                                                    | low                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IE Cache URL:                                                                                  | <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/San-Xavier-Map.png?fit=2000%2C659">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/San-Xavier-Map.png?fit=2000%2C659</a>                                                                                                                                                                                                 |
| Preview:                                                                                       | .PNG.....IHDR.....v.c.....PLTE.....w.L.....h.....l.....bE...A.....{.....s.....iL.....nS.x`..~f.PA.sY.....x.....}.....sP.....DA...y.ny.ND...l.52.....ja...~[<...ys].....^U...?5..',...ec.{x^k....d.JX.RP...#!.w...z.....nj.vn...ZU... ...bU.D8MR.....8IDATx...[Li.....e.....q.6.@8.....3N...nV.l(g....Kl..."...V.4.Z....n.hl..Q..f...l]7...~..6...eb...;...7.....N.....,G*.G...w.....o.8.....g..^{....u..qnQ...o...y.g |

|                                                                                                    |                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\Sells-Hospital-Map[1].png</b> |                                                                                                                                                                                                                               |
| Process:                                                                                           | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                         |
| File Type:                                                                                         | PNG image data, 2000 x 659, 8-bit colormap, non-interlaced                                                                                                                                                                    |
| Category:                                                                                          | downloaded                                                                                                                                                                                                                    |
| Size (bytes):                                                                                      | 82351                                                                                                                                                                                                                         |
| Entropy (8bit):                                                                                    | 7.985323845723327                                                                                                                                                                                                             |
| Encrypted:                                                                                         | false                                                                                                                                                                                                                         |
| SSDEEP:                                                                                            | 1536:mFDsAp5q3vZqQeFFK90qndCmf+2DZPW7VkQo2iec2hVN+qPkp5:mKApA3khFFK90gCmlZ6V2iHhPk3                                                                                                                                           |
| MD5:                                                                                               | 67327FC9968F9E76614D74D660717F24                                                                                                                                                                                              |
| SHA1:                                                                                              | 21F7201B94724FE93683F74C2134F7144138E028                                                                                                                                                                                      |
| SHA-256:                                                                                           | FAD9D6D164380DADD2918711334897055C41B88A4D2217CBF4397F466A1AF758                                                                                                                                                              |
| SHA-512:                                                                                           | 746C823966762FB6AD69E5C9455DFF8EA4C04475D9AC80DA2E6463CD2932EAA92D1C44E13EA509BD378F16709731D794683E55790EDB6B0B92AE408C6A02E67                                                                                               |
| Malicious:                                                                                         | false                                                                                                                                                                                                                         |
| Reputation:                                                                                        | low                                                                                                                                                                                                                           |
| IE Cache URL:                                                                                      | <a href="http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells-Hospital-Map.png?fit=2000%2C659">http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Sells-Hospital-Map.png?fit=2000%2C659</a> |



C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\U\core.min[1].js

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <pre>/*! * jQuery UI Core 1.11.4. * http://jqueryui.com. * * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jquery.org/license. * * http://api.jqueryui.com/category/ui-core/. */.function(e){function(e){function(e){var e,t,n,i;function r(e,t){var n,i,r=e.nodeName.toLowerCase();return"area"===r?(i=(n=e.parentNode).name,!(!e.href  !i)"map"!==n.nodeName.toLowerCase())&amp;&amp;(!i  (i=a("img[usemap=#"+i+""]")[0])&amp;&amp;o(i));}/*(input select textarea button object)\$/.test(r)?e.disabled:"a"===r&amp;&amp;e.href  t)&amp;o(e)}function o(e){return a.expr.filters.visible(e)&amp;&amp;!a(e).parents().addBack().filter(function(){return"hidden"===a.css(this,"visibility")}).length}a.ui=a.ui  {},a.extend(a.ui,{version:"1.11.4",keyCode:{BACKSPACE:8,COMMA:188,DELETE:46,DOWN:40,END:35,ENTER:13,ESCAPE:27,HOME:36,LEFT:37,PAGE_DOWN:34,PAGE_UP:33,PERIOD:190,RIGHT:39,SPACE:32,TAB:9,UP:38}}),a.fn.extend({scrollParent:function(e){var t=</pre> |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\U\coronavirus[1].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Size (bytes):   | 64363                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Entropy (8bit): | 5.366765051010803                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:         | 1536:WkHVUUr+er+elr+ei+es858DtA1CZ1Om9te7SSaMeajVd6uNAS2OJmcEA1koUUU+:tLN+rg98Z7bPSaMeajVd6uNAS2OQcE8L                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:            | B04F8C630A995DC63D0CC05649A55850                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:           | 66EE1FAAA118127EF5A4DC79A0E04ACC8AA7948B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:        | 97551DDC1CF498785B222C5A6F43AB0E0B00A078655BBE1158E13CDAF3EB1CB7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:        | E614D4FEC71444314E9108458811867BC2E41DD1CD0CD28182E2836EA4AEE020FE08B37DB0DEEB887BE7DC371C2CE551C4A5016DA6348F4966F84152D83227                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:        | <p>&lt;!DOCTYPE html&gt;.&lt;html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_1055 av-no-preview "&gt;.&lt;head&gt;.&lt;meta charset="UTF-8" /&gt;... mobile setting --&gt;.&lt;meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"&gt;.. Scripts/CSS and wp_head hook --&gt;... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ --&gt;..&lt;title&gt;Coronavirus - TON-HC&lt;/title&gt;..&lt;meta name="robots" content="index, follow" /&gt;..&lt;meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" /&gt;..&lt;meta name="bingbot" content="index, follow, max-snippet:-1, max-image-preview:large, max-vi</p> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\U\css[1].css

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:      | ASCII text                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):   | 611                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy (8bit): | 5.210344271248717                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:         | 12:jFuNO6ZRoT6pvuYqFuNO6ZO/T6pld0FqFuNO6ZN76plTWY:5cOYsHrcOYUT0VcOYN7o7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:            | 9394398516DBAD2E51BB639E432BADE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:           | 2A95843169D93250E21AEB3BFEB9A257CC69D6BD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:        | 98B74ED31411C18648EB1C5E303CB12A98FAD87208E3AB626CD4F37A7018EEF1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:        | B78B793D680A2CEA8C5830489E6517BD1ED851CC37FEF60893C972CAF1E91DE7AE6E65732CF82B9108B244575D385576EDEE4FF2C6CBFC51CE9A9962C99BCF41                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IE Cache URL:   | http://https://fonts.googleapis.com/css?family=Source+Sans+Pro%3Aregular%2C700%2C600&subset=latin%2Call&ver=5.5.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Preview:        | <pre>@font-face { font-family: 'Source Sans Pro'; font-style: normal; font-weight: 400; src: url(https://fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3aPA.woff) format('woff'); }.@font-face { font-family: 'Source Sans Pro'; font-style: normal; font-weight: 600; src: url(https://fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3i54rAkw.woff) format('woff'); }.@font-face { font-family: 'Source Sans Pro'; font-style: normal; font-weight: 700; src: url(https://fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3ig4vAkw.woff) format('woff'); }.</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\U\css[2].css

|                 |                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type:      | ASCII text                                                                                                                      |
| Category:       | downloaded                                                                                                                      |
| Size (bytes):   | 203                                                                                                                             |
| Entropy (8bit): | 5.206367642924882                                                                                                               |
| Encrypted:      | false                                                                                                                           |
| SSDEEP:         | 3:0SYWFFWIIYCdGgylIRI5XwDKLRIHDFRwDFTtqzrZqcd8WJhZB28uGUM3xuSPLBy:0IFFE0i+56ZRWHtZlpdRfnVhNin                                   |
| MD5:            | 3F9B532C4E0BB98A6B270F466E3BB339                                                                                                |
| SHA1:           | 53ABE84BE49F53DEC5D83F52E384A410634E8A22                                                                                        |
| SHA-256:        | D9C0984700CF3587571B497508E67E09D8B4F43917463EC7414D447B8ABD29BC                                                                |
| SHA-512:        | 1586406E815842CD18FDAAA8D424B716B003DE609D2EE9C750FE9A52C07CA34328B70149FD66DF3396E35A6E2AD77FAC2EF108115C236AFBFB1FBD8FCD23E46 |
| Malicious:      | false                                                                                                                           |
| Reputation:     | low                                                                                                                             |
| IE Cache URL:   | http://https://fonts.googleapis.com/css?family=Source+Sans+Pro&ver=5.5.5                                                        |



C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\le-202122[1].js

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <pre>window.wpcom=window.wpcom  {};window._stq=window._stq  [];function st_go(a){window._stq.push(['view',a]);};function linktracker_init(b,p){window._stq.push(['cli ckTrackerInit',b,p]);};window.wpcom.stats=(function(){var _clickTracker=(function(){var _blog,_post;var _addEvent=function(el,t,cb){if('function'===typeof el.addEventList ener){el.addEventListener(t,cb);}else if('object'===typeof el.attachEvent){el.attachEvent('on'+t,cb);};var _getClickTarget=function(e){if('object'===typeof e&amp;&amp;e.target){return e.target;};else{return window.event.srcElement;}};var _clickTrack=function(e){var d=0;if('object'===typeof InstallTrigger)d=100;if(7===_getIEver())d=100;_processLin k(_getClickTarget(e),d);};var _contextTrack=function(e){_processLink(_getClickTarget(e),0);};var _isSameHost=function(a){var l=document.location;if(l.host===a.h ost)return true;if(''===a.host)return true;if(l.protocol===a.protocol&amp;&amp;l.host===a.hostname){if('http:'===l.protocol&amp;&amp;l.host+':80'===a.host)return true;if('https:'===l.pro</pre> |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\leffect-scale.min[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):   | 1109                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit): | 5.116483826366515                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:         | 24:NfKzhbkYISHHb90712i+WDGp6g0ZWHfDdbMf4NB+y+9NcU:NSz2YISHHb9RWDGp6pWNU4z+y+9mU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:            | 99DD1A11F49DB0BC9B8A6AD749AC1BE8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA1:           | 976E7C5C4AF5A0970A1AA16168036DD7EBC19AA6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:        | 981273245F40043B454460F0F3BC7686CA73C05246AC7AC924F491086431E361                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-512:        | 30AB3AFC70A341425ADB843342547B182585D15A5E071BD505AB5CDB96762EA6AE166901CC7C0438DE561C6C35874F7B58EEC3FC9A95EC309C16E91A7201CE16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| IE Cache URL:   | http://www.tonhc.org/wp-includes/js/jquery/ui/effect-scale.min.js?ver=1.11.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:        | <pre>/*! * jQuery UI Effects Scale 1.11.4. * http://jqueryui.com. * * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jquery. org/license. * * http://api.jqueryui.com/scale-effect/. *!.function(e){"function"===typeof define&amp;&amp;define.amd?define(["jquery","./effect","./effect-size"],e):e(jQuery)}(function(u) {return u.effects.effect.scale=function(e,t){var i=u(this),o=u.extend({l:0,},e),h=u.effects.setMode(i,e.mode)  "effect",f=parseInt(e.percent,10)  ((0===parseInt(e.percent, 10))?"hide"===h?0:100),r=e.direction  "both",c=e.origin,d={height:i.height(),width:i.width(),outerHeight:i.outerHeight(),outerWidth:i.outerWidth(),n="horizontal"!==r?f/1 00:1,f="vertical"!==r?f/100:1;o.effect="size",o.queue=!1,o.complete=t,"effect"!==h&amp;&amp;(o.origin=c  ["middle","center"],o.restore=l),o.from=e.from  (("show"===h?{height:0,wi dth:0,outerHeight:0,outerWidth:0}:d),o.to={height:d.height*n,width:d.width*f,outerHeight:d.outerHeight*n,outerWidth:d.outerWidth*f},o.fade&amp;&amp;</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\leffect-transfer.min[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 857                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Entropy (8bit): | 5.117158975393317                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SSDEEP:         | 24:Nikzhbk+OSHH40TqKQsv9havC5qQ0tKJO1zn:Nrz2+OSHHTuC3aUqjtSsn                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MD5:            | E81B0A5F159DD53D9304015ED097366                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA1:           | 18EB17BD3C34275F779694808BC73CC75DABBC90                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:        | 9E20A504411A4D12E6A44C59CB44D87BCF2EE78A8C73397EB68B24D3A9B8512D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-512:        | 4844115143261C3F806A5DBAFC649C9769E2A542D9FC8A5B5133F0D65B7EC62507368620C8EDE36D3118F1201EAA22BB62928D0A2D04E7F735C3E78478DDAD8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IE Cache URL:   | http://www.tonhc.org/wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Preview:        | <pre>/*! * jQuery UI Effects Transfer 1.11.4. * http://jqueryui.com. * * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jque ry.org/license. * * http://api.jqueryui.com/transfer-effect/. *!.function(e){"function"===typeof define&amp;&amp;define.amd?define(["jquery","./effect"],e):e(jQuery)}(function(c){return c .effects.effect.transfer=function(e,t){var i=c(this),n=c(e.to),f="fixed"===n.css("position"),o=c("body"),s=f?o.scrollTop():0,d=f?o.scrollLeft():0,o=n.offset(),o={top:o.top-s,left:o .left-d,height:n.innerHeight(),width:n.innerWidth()},n=i.offset(),r=c("&lt;div class='ui-effects-transfer'&gt;&lt;/div&gt;").appendTo(document.body).addClass(e.className).css({top:n. top-s,left:n.left-d,height:i.innerHeight(),width:i.innerWidth(),position:f?"fixed":"absolute"}).animate(o,e.duration,e.easing,function(){r.remove().t()}});</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\lentypo-fontello[1].eot

|                 |                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type:      | Embedded OpenType (EOT), entypo-fontello family                                                                                 |
| Category:       | downloaded                                                                                                                      |
| Size (bytes):   | 47528                                                                                                                           |
| Entropy (8bit): | 6.563936291146135                                                                                                               |
| Encrypted:      | false                                                                                                                           |
| SSDEEP:         | 768:pKq9s+YdSmb2OFTvkvAvh+zAx9KpNUBatpizgp/t9RBj:pKq9s7SmbNTth+zAx9KpN6aTtVp                                                    |
| MD5:            | 593E51E1AC27F455D80B4B971B0408EC                                                                                                |
| SHA1:           | 8CC8D22D4AC8077870AC37CACB021893FE520C5F                                                                                        |
| SHA-256:        | 00FE586A55D55C99AF90F506FC1E3E06597FE5C312A8F1430CCED6F73E416D64                                                                |
| SHA-512:        | 7E10B4C6F0CD341B7B16268167C1396FCDA74187CEB5E551DAC9572B92DD39F554908EF7E25833397EAF51004E086C16E5DDCDA3D24A8B13BE8C8C5A3506E5  |
| Malicious:      | false                                                                                                                           |
| Reputation:     | low                                                                                                                             |
| IE Cache URL:   | http://www.tonhc.org/wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fonts/entypo-fontello.eot?v=3 |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\entypo-fontello[1].eot

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <pre> .....LP.....r).....e.n.t.y.p.o.-f.o.n.t.e.l.l.o.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. 1.....e.n.t.y.p.o.-f.o.n.t.e.l.l.o.....OS/2&gt;QJ/..( ..Vcm.ap&lt;...4..JgJylf.....Hhead.....6hhea..T.....\$hmtxf.....loca.g.pX.....lmaxp.E.....name.....\$!post.7\...H.....R.j.Z.....)r_&lt;...c... ..c...A...Z.....M.....z.....z.....1.....PfEd@...+..R.j.Z.z.....F.....\..l..p..p.....X.....H.....D. ..H.....D...H.....D.....R.....h...&amp;.....l.....H..... ..[.....t.....0..... </pre> |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\event-mod[1].css

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:      | ASCII text                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):   | 18047                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 4.844957288974339                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 384:XDgrcjAU6tWTiQALNlM3XimwNEbZYUQLvRcnk1eclxm5ALX+guR+KOLCP:XDgrztaWN6wNEFOYcnk1eclxm5ALX+Hb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MD5:            | 508BF3A062B7274296721E41BC714D1F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | 48E94EEEE3D9B5B47DE060BDD85CBC0B90B82825                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:        | 9584F0C675182B1378BF2B3AACB1B775F912414A444BC92AE7A285A6D343F81E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | 9A76B32238DCA2B78CD8A3C53D3CD4D80A95EF09E1DF7CE3A6B851C3F0A1D7777AF25C1C5DFC3324E30C0813840A527014D20E42D72AA98FA2D2157B1E96B0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IE Cache URL:   | http://www.tonhc.org/wp-content/themes/enfold/config-events-calendar/event-mod.css?ver=5.5.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:        | /*Custom Template Builder Elements*/...av-upcoming-events{.av-upcoming-event-entry{clear: both; padding:0 0 25px 0; overflow: hidden; display:block;}.av-upcoming-event-entry:hover{text-decoration: none; color: inherit;}.av-upcoming-event-entry:last-child {padding-bottom: 0;}.av-upcoming-event-image{border-radius: 400px; width:60px; float:left; margin: 0 20px 0 0; }.av-upcoming-event-data{ display:block; overflow: hidden; }.av-upcoming-event-meta{ display:block; position: relative; top:-1px; font-size: 12px;}.av-upcoming-event-schedule{display:block;}.av-upcoming-events .pagination-meta{display:none;}.../*TRIBE CALENDAR*/.#top #tribe-events-pg-template{ max-width: 100%; padding:0;}.#top #tribe-events-pg-template .tribe-events-notice{border:none; border-radius:0; padding:14px; text-align: center; font-size: 15px; font-weight:normal; text-shadow: none;}.../*events bar*/.#tribe-events-bar{margin-top: 50px; position: relative; border-bottom-style: solid; border-bottom-width:1px; |

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ewd-ufaq-js[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| File Type:      | ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):   | 15270                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit): | 5.34589312557428                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SSDEEP:         | 192:5BOxW+//22L1wiauawdCHC6h8GzFCA51ZYV:5BO9/22L6iauawQiKrJCA51ZYV                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MD5:            | 5A6999A011C22BBC138E38FCD3FC67EC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA1:           | 2DDD70A952813B6745FBB6E434E2BDC2C036934A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-256:        | 3A8EB49E16813B319C5730AC7D147DCBAED4736F9A0C2B7482EB03C383334B62                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA-512:        | FFE00BDA699AC3D5C55EE4B9142AD1BE387CEBF0A605B1518D1223A36F22448DD96504BF8C3DACB5BDE9F3C1E24DACB2D2CC21CE9D4317AAAC5E519794B961                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IE Cache URL:   | http://www.tonhc.org/wp-content/plugins/ultimate-faqs/js/ewd-ufaq-js.js?ver=1.9.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preview:        | <pre>var filtering_running = 'No';var wpforms_search_running = 'No';...jQuery(function() { //DOM Ready..  ufaqSetClickHandlers();..  UFAQSetAutoCompleteClickHandlers();..  UFAQSetRatingHandlers();..  UFAQSetExpandCollapseHandlers();..  UFAQSetPaginationHandlers();...  UFAQWPFormsHandler();..});...function runEffect(display, post_id) {..  var selectedEffect = reveal_effect;..  // most effect types need no options passed by default..  var options = {};..  // some effects have required parameters..  if ( selectedEffect === "size" ) {..    options = { to: { width: 200, height: 60 } };..  }..  // run the effect..  if (display == "show") {jQuery( "#ufaq-body-"+post_id ).show( selectedEffect, options, 500, handleStyles(display, post_id) );}...if (display == "hide") {jQuery( "#ufaq-body-"+post_id ).hide( selectedEffect, options, 500, handleStyles(display, post_id) );}..};....// callback function to bring a hidden box back..function handleStyles(display, post_id) {</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\for-patients[1].htm

|                 |                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                         |
| Category:       | dropped                                                                                                                         |
| Size (bytes):   | 57656                                                                                                                           |
| Entropy (8bit): | 5.350167165190069                                                                                                               |
| Encrypted:      | false                                                                                                                           |
| SSDEEP:         | 1536:+HVcuR+er+el3+ei+eX0xNp25ihRXuOTKIEgdzJvoOmSSaMeajVd6uNAS2OJrc2y:ArN+3gFEgdzJvjSaMeajVd6uNAS2O9cr                          |
| MD5:            | 2D8AAEDC6B6929AE9ABD0F3F85412D90                                                                                                |
| SHA1:           | 42D65079B3B3133E298DB4FABE5E0B81806B640C                                                                                        |
| SHA-256:        | E5F3CFE74FC71CFCFF1F9415CAD18A3D9557733A97ECF26A305BF2B2FE1C9EA9                                                                |
| SHA-512:        | 221FF21E0FE4C197CCA64557F7EB38F720E46F8EB5E68F05CA0D77580DBF72475421C733C20BD3F6BD6B57E0DFBC969E38F8E3B39E3482CC9F4075F57399273 |
| Malicious:      | false                                                                                                                           |
| Reputation:     | low                                                                                                                             |



C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\jetpack-carousel.min[1].js

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <pre>/* Do not modify this file directly. It is compiled from other files. */./* global jetpackCarouselStrings, DocumentTouch */.jQuery(document).ready(function(e){var t,a,i,o,s,r,n,l,c,d,p,u,m,h,f,g,j,v,w,_=110,x=e("body").css("overflow"),b=e("html").css("overflow"),y=""-.window.innerWidth&lt;=760&amp;&amp;(_=Math.round(window.innerWidth/760*110))&lt;40&amp;&amp;("ontouchstart"in window window.DocumentTouch&amp;&amp;document instanceof DocumentTouch)&amp;&amp;(_=0),void 0===Date.now&amp;&amp;(Date.now=function(){return(new Date).getTime());},var k=function(e){switch(e.which){case 38:e.preventDefault(),o.scrollTop(o.scrollTop()-100);break;case 40:e.preventDefault(),o.scrollTop(o.scrollTop()+100);break;case 39:e.preventDefault(),i.jp_carousel("next");break;case 37:case 8:e.preventDefault(),i.jp_carousel("previous");break;case 27:e.preventDefault(),o.jp_carousel("close")};},S=function(){clearTimeout(d),d=setTimeout(function(){i.jp_carousel("slides"),jp_carousel("fitSlide",!0),i.jp_carousel("updateSlidePositions",!0),i.jp_carousel("fitMeta")</pre> |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\mediaelement-and-player.min[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Size (bytes):   | 160453                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Entropy (8bit): | 5.283279853648975                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SSDEEP:         | 3072:5Lhh0Kn+zzegf1R52Z7p6aUXbIPMPdRLjqdgB0UmATDHZ5JDDnWtNWNKERysXD5:5sKbRLjPZPt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:            | C6D1F8E334DED732E83231A64DE3FD3F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA1:           | 05F7E36A68B6C5595A5E1C1908C5BEEDE4EE12BE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-256:        | 282C86DB3FC6CEDCC79B172069BA09831CE0E6BA235D13BFF382F57F0D3977FF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-512:        | 3EBABBD6598757E55C74BA83600DFB6978757DF0961A79E119749139A954C4C7A8CB750518EB55FFB90A93965CBE5D911936C5D43ADDBB0475757A5B535FCFB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IE Cache URL:   | http://www.tonhc.org/wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:        | <pre>/*! * MediaElement.js * http://www.mediaelementjs.com/. * * Wrapper that mimics native HTML5 MediaElement (audio and video). * using a variety of technologies (pure JavaScript, Flash, iframe). * * Copyright 2010-2017, John Dyer (http://j.hn/). * License: MIT. * */.function r(a,s,l){function d(t,e){if(!s[t]){if(!a[t]){var n="function"===typeof require&amp;&amp;require;if(!e&amp;&amp;n)return n(t,!0);if(u)return u(t,!0);var o=new Error("Cannot find module '"+t+"'");throw o.code="MODULE_NOT_FOUND",o}var i=s[t]={exports:{}},a[t][0].call(i,exports,function(e){return d(a[t][1][e])  e}),i.i.exports,r,a,s,l)}return s[t].exports}for(var u="function"===typeof require&amp;&amp;require,e=0;e&lt;l.length;e++)d(l[e]);return d}({1:[function(e,t,n){},{}],2:[function(i,r,e){function d(i,r,e){var t,n=void 0!==e?e:"undefined"!==typeof window?window:{},o=i(1),"undefined"!==typeof document?t=document:(t=n["__GLOBAL_DOCUMENT_CACHE@4"])](t=n["__GLOBAL_DOCUMENT_CACHE@4"])=o,r.exports=t)}.call(this,"undefined"!==typeof global?global:"undefi</pre> |

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\mission[1].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Size (bytes):   | 47578                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Entropy (8bit): | 5.35753790333006                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:         | 768:NrvHViuUt+em+eIUq+ei+eqLPm8OOY1nMA/wgVyXKYEGdzNfMyAukOmSSaM7u/Ba:dHViuM+em+elr+ei+eb1nMA/wgVyXzEJ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MD5:            | F71C7D988B64F5CA2DDB3EB3CADFFBCE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:           | D8D1053E51ACACF3B9B697F1131FD08E2DA72F19                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:        | 95C0349A4C64AF11B3C24EB8879513D79EA9AE62DF9F893BAFADE660FC6229F2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:        | 2B322FDDCD66A53B98343285709FAC47A38C1918AA5484A75755BC77B5BD140B5D82B7B98F7D4181C8B172B0A8DF29A1037FE79C9C3840B568D5B314C4C9F39                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | <pre>&lt;!DOCTYPE html&gt;.&lt;html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_130 av-no-preview "&gt;.&lt;head&gt;.&lt;meta charset="UTF-8" /&gt;... mobile setting --&gt;.&lt;meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"&gt;.. Scripts/CSS and wp_head hook --&gt;... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ --&gt;..&lt;title&gt;Mission - TON-HC&lt;/title&gt;..&lt;meta name="robots" content="index, follow" /&gt;..&lt;meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" /&gt;..&lt;meta name="bingbot" content="index, follow, max-snippet:-1, max-image-pr</pre> |

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\page[1].htm

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:      | HTML document, ASCII text, with very long lines                                                                                  |
| Category:       | dropped                                                                                                                          |
| Size (bytes):   | 60518                                                                                                                            |
| Entropy (8bit): | 5.789184503490911                                                                                                                |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 1536:CUIEu1rHO13CV1nAc7Lon0m2/EIMJqCvFrXRYB:CGEu1rHO13CVJAn0m2MWJqCvFFYB                                                         |
| MD5:            | 6067C480562416DAAEA11DF55684DC00                                                                                                 |
| SHA1:           | 38F56A92EF706C0AB779274A3C56D53E3E1CC9B7                                                                                         |
| SHA-256:        | 6ECF782D689EE93F7D4AB0097E5691848226BC57739C0A6184FB614B90AE294E                                                                 |
| SHA-512:        | FFC678C96B259B36F551245860F00DB3C58F96D3DFFE81F3977A20B5C0A3F72497B0DEA645C9991532E6B03310A14662101785F695284F0EE4F2BC2F064B9873 |
| Malicious:      | false                                                                                                                            |
| Reputation:     | low                                                                                                                              |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\page[1].htm

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <!DOCTYPE html>.<html lang="en" id="facebook" class="no_svg no_js">.<head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script nonce="qmTkcPi6">window._cstart+=new Date();</script><script nonce="qmTkcPi6">function envFlush(a){function b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env  {}).b(window.Env))}envFlush({"ajaxpipe_token":"AXiXm-MkMnAhF01cTpo","no_cookies":1,"timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":{"requestAnimationFrame":true,"Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,"Event listenHandler scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_categories":{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,"gk_requirelazy_mem":true,"stack_trace_limit":30,"timesliceBufferSize" |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\page[2].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | HTML document, ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):   | 61010                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Entropy (8bit): | 5.79113553381053                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:         | 1536:CU8h3oyGXo2DIAnALWLDt0N2/EIMJq6w0vFTQhKf:Cdh3oyGXo2DIlut0N2MWJq6w0vFuKf                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| MD5:            | 7CD527E14F9C6A5A7F3045A964C1363C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:           | C793C5D7B9A7A8D8DFC93F1D44FE0D8F075CA7F8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:        | 92AACED963FF30315F39DEBCE7F89D796481FBE0F13CC97D4FADEB39A67B8983                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-512:        | 0645B0FB2D514614C1C6E89C82F80BB69E795C01EF693ACA4F431EE317D555F3E1F5379516EA95212744525CBD5B3F018BAE816F9AEEF7EB6714E0056652E64                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:        | <!DOCTYPE html>.<html lang="en" id="facebook" class="no_svg no_js">.<head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script nonce="RCyJaVRO">window._cstart+=new Date();</script><script nonce="RCyJaVRO">function envFlush(a){function b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env  {}).b(window.Env))}envFlush({"ajaxpipe_token":"AXiXm-MkMnAhF01cX6k","no_cookies":1,"timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":{"requestAnimationFrame":true,"Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,"Event listenHandler scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_categories":{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,"gk_requirelazy_mem":true,"stack_trace_limit":30,"timesliceBufferSize" |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\san-simon[1].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Size (bytes):   | 47555                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Entropy (8bit): | 5.361805291150674                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:         | 768:cZYHV9uUL+eE+el8q+ei+eqLP08O+1LOgC4TE/EgdzNfMyAukOmSSaM7u/BajVd9:PHV9u0+eE+elT+ei+eq9TUEgdzJvoOml                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MD5:            | CBC454D1A92FFEB4A599932B5F8A653F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:           | 5E3A05E3D0C6A8022E5BFC1A501E635C0E4A30A9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:        | 3568954877AB63BD0F1871D82683ADA8EF8094CEF6ECEA1E0B6227168B768B1D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:        | FE1A8DF51B261541336F8DF3A7A3675881CFABCD2318B17F4F1D05CC0E67E67838CCA6EBA84B8B9EE147AC9AEFDEFD708C518EB4DA18905AD32008FE9AE35C16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | <!DOCTYPE html>.<html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_header html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_346 av-no-preview ">.<head>.<meta charset="UTF-8" />... mobile setting -->.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">... Scripts/CSS and wp_head hook -->... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ -->...<title>San Simon - TON-HC </title>...<meta name="robots" content="index, follow" />...<meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" />...<meta name="bingbot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMUU\spin.min[1].js

|                 |                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type:      | ASCII text, with very long lines                                                                                                |
| Category:       | downloaded                                                                                                                      |
| Size (bytes):   | 4510                                                                                                                            |
| Entropy (8bit): | 5.260095422457841                                                                                                               |
| Encrypted:      | false                                                                                                                           |
| SSDEEP:         | 96:ep0Xogatn2MzqbCYN0uWHOnUqPEtjIFqk6s:ANga17qbqSjs                                                                             |
| MD5:            | 3498DB8D3BE2F39F4C346CFFDB8318C5                                                                                                |
| SHA1:           | FD71863F2FC61E239CEB0DA1915BD0CFE7328D50                                                                                        |
| SHA-256:        | A5307DA44321773C9F46B34D756DCBD6CD427238E5CBAD91CD2CF151513EC283                                                                |
| SHA-512:        | E016C72604AA7FD0A60BAB28BA9BDC7F26CBE244958DB6909AF6B8A9164041A0CA9D4CFF0757DF1BFEE16CA507164DC58A0CAB2E788CA1F2C1AEB8710310A75 |
| Malicious:      | false                                                                                                                           |
| Reputation:     | low                                                                                                                             |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\spin.min[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IE Cache URL:                                                                            | <a href="http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/spin.min.js?ver=1.3">http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/spin.min.js?ver=1.3</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:                                                                                 | <pre>/* Do not modify this file directly. It is compiled from other files. */.//fgnass.github.com/spin.js#v1.3./**. * Copyright (c) 2011-2013 Felix Gnass. * Licensed under the MIT license. */.!function(t,e){"object"==typeof exports?module.exports=e():"function"==typeof define&amp;&amp;define.amd?define(e):t.Spinner=e()}(this,function(){"use strict";var t,e=["webkit","Moz","ms","O"],i={};function o(t,e){var i,o=document.createElement(t  "div");for(i in e)o[i]=e[i];return o}function r(t){for(var e=1,i=arguments.length;e&lt;i;e++)t.appendChild(arguments[e]);return t}var n,s=(n=o("style",{type:"text/css"}),r(document.getElementsByTagName("head")[0],n),n.sheet[0].styleSheet);function a(e,o,r,n){var a=["opacity",o,~(100*e),r,n].join("-"),l=.01+r/n*100,f=Math.max(1-(1-e)/o*(100-l),e),p=t.substring(0,t.indexOf("Animation")).toLowerCase(),d=p&amp;&amp;"-p+-"  "";return i[a]  (s.insertRule("@@+d+keyframes "+a+"{0%{opacity:"+f+"}"+l+"%{opacity:"+e+"}"+(l+.01)+"%{opacity:1}"+(l+o)%100+"%{opacity:"+e+"}100%{opacity:"</pre> |

|                                                                                                |                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\tonhc-mission[1].jpg</b> |                                                                                                                                                                                                                     |
| Process:                                                                                       | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                               |
| File Type:                                                                                     | [TIFF image data, little-endian, direntries=0], progressive, precision 8, 1500x852, frames 3                                                                                                                        |
| Category:                                                                                      | downloaded                                                                                                                                                                                                          |
| Size (bytes):                                                                                  | 699878                                                                                                                                                                                                              |
| Entropy (8bit):                                                                                | <b>7.99021939528463</b>                                                                                                                                                                                             |
| Encrypted:                                                                                     | <b>true</b>                                                                                                                                                                                                         |
| SSDEEP:                                                                                        | 12288:DJVyxDJfc60tsP8JmjqBWd+woS0r+xfw09wAdwpR3X/adugdCj91mtiOrnk:tVODJfcb3GjqBWdHoUal09x45CFCb6rk                                                                                                                  |
| MD5:                                                                                           | C07B8FF6486E541080524BAB53B71819                                                                                                                                                                                    |
| SHA1:                                                                                          | E29898B828FCA50CCEE6C646FD8D82B36C33549A                                                                                                                                                                            |
| SHA-256:                                                                                       | 36C8637CC547C5913866176DA31C4284F93D1273DE71C800A811155DC20DBEB1                                                                                                                                                    |
| SHA-512:                                                                                       | D7B02D164CC443D90CDED7F6261F2A1EE3A21971AB1D68EBF3986FE02DA4C8A5F91B3A5BA940941713D989B5A6D091FD77F09E88BB770321EE1C7B0D3C46C9                                                                                      |
| Malicious:                                                                                     | false                                                                                                                                                                                                               |
| Reputation:                                                                                    | low                                                                                                                                                                                                                 |
| IE Cache URL:                                                                                  | <a href="http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-mission.jpg?fit=1500%2C852">http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-mission.jpg?fit=1500%2C852</a> |
| Preview:                                                                                       |                                                                                                                                                                                                                     |

|                                                                                                           |                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\tonhc-sanxavier-location[1].jpg</b> |                                                                                                                                                                                                                                           |
| Process:                                                                                                  | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                     |
| File Type:                                                                                                | [TIFF image data, little-endian, direntries=0], progressive, precision 8, 1500x710, frames 3                                                                                                                                              |
| Category:                                                                                                 | downloaded                                                                                                                                                                                                                                |
| Size (bytes):                                                                                             | 175584                                                                                                                                                                                                                                    |
| Entropy (8bit):                                                                                           | 7.974748879528137                                                                                                                                                                                                                         |
| Encrypted:                                                                                                | false                                                                                                                                                                                                                                     |
| SSDEEP:                                                                                                   | 3072:vhYOq+wPQHfENpdvXpONKk0cyjMeW2OTnVhfGdUjAGakqnnj6SW:vhYiweENTfpON5mBOHf6MadneSW                                                                                                                                                      |
| MD5:                                                                                                      | 925AA90EF423DED9722E82BE9321DDC7                                                                                                                                                                                                          |
| SHA1:                                                                                                     | EC863F0D15290922E0FCFCF53FD95ECA0042E1F5                                                                                                                                                                                                  |
| SHA-256:                                                                                                  | C9FA52FD725586ADBFB8A325682521EC0728C7DE7979DAD75DEDD1B1B982954D                                                                                                                                                                          |
| SHA-512:                                                                                                  | 91309A52572AD0224167CF168C4B35D020FF455AAFAA483DBCE2C1603A94DEA2CF7A7324F3E54CB569B2E78F4F70B78DD07FF2BC2AEF5D3F32AE44958BB28769                                                                                                          |
| Malicious:                                                                                                | false                                                                                                                                                                                                                                     |
| Reputation:                                                                                               | low                                                                                                                                                                                                                                       |
| IE Cache URL:                                                                                             | <a href="http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sanxavier-location.jpg?fit=1500%2C710">http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sanxavier-location.jpg?fit=1500%2C710</a> |
| Preview:                                                                                                  |                                                                                                                                                                                                                                           |

|                                                                                                       |                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\tonhc-sells-location[1].jpg</b> |                                                                                                                                  |
| Process:                                                                                              | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:                                                                                            | [TIFF image data, little-endian, direntries=0], progressive, precision 8, 1500x826, frames 3                                     |
| Category:                                                                                             | downloaded                                                                                                                       |
| Size (bytes):                                                                                         | 274026                                                                                                                           |
| Entropy (8bit):                                                                                       | 7.988361649602213                                                                                                                |
| Encrypted:                                                                                            | false                                                                                                                            |
| SSDEEP:                                                                                               | 6144:thLoVNgF4UVNn2lgRBIQRfSOssZLz72e:t5oVNuLbAKBIQR6Z272e                                                                       |
| MD5:                                                                                                  | AC8CA6C7B2CE7B155446B5CB5950498E                                                                                                 |
| SHA1:                                                                                                 | 8B4757726C81503BEDCD15BE70A6653053188D70                                                                                         |
| SHA-256:                                                                                              | AFE5DCC2CB84529DB8B1338218580C33A42FF1E15522569A8C3D68CF49D43492E                                                                |
| SHA-512:                                                                                              | A61E9DA864FE11B74E864C3BF607FE6B84CF57AE5DC1AFA691D4D060947215826922B426FD544A6B84AEF4BC6FAADF37EB14143002EB081F390D5F4A3EAECD2F |
| Malicious:                                                                                            | false                                                                                                                            |
| Reputation:                                                                                           | low                                                                                                                              |

|                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\tonhc-sells-location[1].jpg</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IE Cache URL:                                                                                         | <b>http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sells-location.jpg?fit=1500%2C826</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Preview:                                                                                              | <div>.....JFIF.....Exif..II*.....HPhotoshop 3.0.8BIM.....Z...%G.....8BIM.%.....x/4b4.Xw...C.....C.....&amp;.....+-:...m"t:...T[]..4....f...ZU\$#.jCL..3.WY.WV. .t~./&gt;..s.+.....".....&amp;..2..R7a.J".<br/>.X.z.....O&gt;...C..AD.L..X.d....J.P.....(..[.....@...(..+.....!.....]y.Y.n.]2g..KU.UV..B.N.jeU.(,...m...l.5.....lp.J.Y[\$..T.WW...'.Q..l8.V..../L:..r.Z\$.Rh.....7.....0..@..<br/>...\$.@...(.9U...1...(..y.=~..\$0...T.(...(..[...l..T...t...8..Y"q8.Y3..]Z..Y..N.)N...[...u.4.6e9.*.#.....y.....H....lF.....k..cZ.Yl...VRk..t...l\.....H..U...+.%5.....#;<br/>^s..._n@.....*..P..P.....!...~..X.%.*.T@T.d..2c.&lt;./..fY.....Fr..9.....s%.U..3..~..~:</div> |

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\wp-mediaelement.min[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Process:                                                                                            | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| File Type:                                                                                          | HTML document, ASCII text, with very long lines, with no line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Category:                                                                                           | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Size (bytes):                                                                                       | 906                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit):                                                                                     | 5.026818215220488                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Encrypted:                                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SSDEEP:                                                                                             | 24:ck/l7q5yEwf9ga/9WpqElfayrXac89Wpq9WRpVod91p0yDn:3kF9gw9WsEISy2c89WE9WRpk9P0yD                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MD5:                                                                                                | 2C6D3B562A48E0DF5474999DD47E58FB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA1:                                                                                               | 945220E990EB176C14E53CC663FB01E04E31B59F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-256:                                                                                            | 3E6131330963C472B950B8AAF544BA3829735B8CCB103D614BA7793E3A786550                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-512:                                                                                            | 024CE74A723BF2797AA50D957F4E0C6431F04D1AC9AD6B5A45A17835FEBBEC4557AAD95A01AD0D147C8EC0E68DDBD0732E308C529255F266DC5ED7B98C52BAAE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:                                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Reputation:                                                                                         | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| IE Cache URL:                                                                                       | <b>http://www.tonhc.org/wp-includes/js/mediaelement/wp-mediaelement.min.js?ver=5.5.5</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:                                                                                            | <div>!function(e,n){e.wp=e.wp  {},e.wp.mediaelement=new function(){var e={};return{initialize:function(){if(e="undefined"!=typeof _wpmejsSettings?n.extend(!0,{},_wpmejsSettings):e).classPrefix="mejs-",e.success=e.success  function(e){var n,t,e.rendererName&amp;&amp;!1==e.rendererName.indexOf("flash")&amp;&amp;(n=e.attributes.autoplay&amp;&amp;"false"==e.attributes.autoplay,t=e.attributes.loop&amp;&amp;"false"==e.attributes.loop,n&amp;&amp;e.addEventListener("canplay",function(){e.play(),!1),t&amp;&amp;e.addEventListener("ended",function(){e.play(),!1))),e.customError=function(e,n){if(!1==e.rendererName.indexOf("flash")  !1==e.rendererName.indexOf("flv"))return'&lt;a href="'+n.src+'"'&gt;+mejsL10n.strings["mejs.download-file"]+"&lt;/a&gt;",n("wp-audio-shortcode, .wp-video-shortcode").not(".mejs-container").filter(function(){return!n(this).parent().hasClass("mejs-mediaelement")}).mediaelementplayer(e)}}},n(e.wp.mediaelement.initialize)}(window,jQuery);</div> |

|                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\2WF3MMU\wp-polyfill-dom-rect.min[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                                 | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                                               | ASCII text, with very long lines, with no line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:                                                                                                | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):                                                                                            | 867                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy (8bit):                                                                                          | 4.865638392619301                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                                  | 24:ECXMtJBGqlwqkoXql7qnTlnqBFqlMqpheql1h7sqliKLqICGYPCql3bGvb6f:E1JBGn6IOBBYCPjODQTIfx2ST6f                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:                                                                                                     | A2B965A62D7B2742CA11C0FEA1C55161                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                                    | DF8B9962F6DFCECD19BC917A4DE55C3EAE53F0E3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                                 | ED7451C7B440A859EBA9CA183E9F40D68E36B79C77BE75B1DE08060090AC706B1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:                                                                                                 | 50D5626808C2590CE7833BDC47D486C367694E9F93CA7A2863FE335E5D9AC31526784F36D388DDC8058B0FBAAE6AC9828FB602E70F27427642A2048F87FA854                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:                                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:                                                                                              | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IE Cache URL:                                                                                            | <b>http://www.tonhc.org/wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                                                                                 | <div>!function(e){function d(e){return void 0===e?0:Number(e)}function g(e,t){return!(e===t  !isNaN(e)&amp;&amp;isNaN(t))}e.DOMRect=function(e,t,n,i){var u,r,o,c,f=d(e),a=d(t),m=d(n),b=d(i);Object.defineProperties(this,{x:{get:function(){return f},set:function(e){g(f,e)&amp;&amp;(f=e,u=r=void 0)},enumerable:!0},y:{get:function(){return a},set:function(e){g(a,e)&amp;&amp;(a=e,o=c=void 0)},enumerable:!0},width:{get:function(){return m},set:function(e){g(m,e)&amp;&amp;(m=e,u=r=void 0)},enumerable:!0},height:{get:function(){return b},set:function(e){g(b,e)&amp;&amp;(b=e,o=c=void 0)},enumerable:!0},left:{get:function(){return u=void 0===u?f+Math.min(0,m):u},enumerable:!0},right:{get:function(){return r=void 0===r?f+Math.max(0,m):r},enumerable:!0},top:{get:function(){return o=void 0===o?a+Math.min(0,b):o},enumerable:!0},bottom:{get:function(){return c=void 0===c?a+Math.max(0,b):c}},enumerable:!0}})(this);</div> |

|                                                                                                       |                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026IKNJ\2020-10-06_15-43-59[1].jpg</b> |                                                                                                                                  |
| Process:                                                                                              | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:                                                                                            | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1030x411, frames 3  |
| Category:                                                                                             | downloaded                                                                                                                       |
| Size (bytes):                                                                                         | 85545                                                                                                                            |
| Entropy (8bit):                                                                                       | 7.9826619649416335                                                                                                               |
| Encrypted:                                                                                            | false                                                                                                                            |
| SSDEEP:                                                                                               | 1536:QC5kpFs1ReI8kqHQQI89Gii5PR2gWzDUOj/Bkkxs/Zw9dlhr:QC5o6ReI8kUleo5PbWzrj+ks/Kfr                                               |
| MD5:                                                                                                  | D35FEAD0B823BA3B67F51DD44C39343C                                                                                                 |
| SHA1:                                                                                                 | C96D0402F6DF2C04F429959124043030816F0373                                                                                         |
| SHA-256:                                                                                              | 17F09329A25BF50A015A85DCE8921AF7039CB4282727FB69F1461108CCC6DFA                                                                  |
| SHA-512:                                                                                              | E88C2BBCE643335288EE3699983373A40D6D123EE57579C298B40B0FB84C1A10928D7940D0822D58B146DD52B3BE454F2A5D37EB4FAB64AB397D9AEFED4F3D52 |
| Malicious:                                                                                            | false                                                                                                                            |
| Reputation:                                                                                           | low                                                                                                                              |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\2020-10-06\_15-43-59[1].jpg

IE Cache URL: [http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06\\_15-43-59.jpg?resize=1030%2C411](http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2020/10/2020-10-06_15-43-59.jpg?resize=1030%2C411)

Preview:

.....JFIF.....C.....C.....".....9.y^..V'.  
{H..wG..U.f..Y.C.n.m.;O\....\.....G@B3.r.y...N..."[.k.....J.....>....h.k...yiE.WG.....ipy.P.YC.t>F].....L...C..3.....S.Y..R\$G...'.j...'.Q=E.....6.y):0...y...z].5..z...M.9..'..  
Q=Bv.9R|...K.....Z.....5.....?N.As.z.....=e.g.<.....%Z;U.4.<U(@...:#>.....Zg7E6w...>\*.YW.q...5..w.....|nkM....2...S.J...X..f.K.y.....{'\_w\_M..7[f.....K.zE1.z.s...g....  
.S.k...l..a|~+....7....R....p..3....y.....>...Z.....h.=^.#..0i...<z3.g/pu.....O5+w..bR.Vm..o.{.....Y..Y....~J.....4.c.k.....\_.....O..l...y.1;^;.....d].S.e.r=N.`zm{aC...[...=\_5E+k.)....  
..A..q...k.G....6..M.....2.\$"<...B#...Y\$e.\*,...k.)i.[...c-F.i.a.2.3i.d....cS(<nE.{h.~.{Tp...1K.>..J.....FM..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\6xK3dSBYKcSV-LCoeQqfX1RYOo3aPA[1].woff



Process: C:\Program Files (x86)\Internet Explorer\iexplore.exe

File Type: Web Open Font Format, TrueType, length 81008, version 1.1

Category: downloaded

Size (bytes): 81008

Entropy (8bit): 7.993486350271994

Encrypted: true

SSDEEP: 1536:HzhinwCfTB/rwLUQqH9iJobMmbuKobplhXqzQKXq:fkUfl/rWg9JFbHCIVTKa

MD5: C3D4F5BBD42B7F543A608ECA53A41E01

SHA1: 0511399FA735751F817A4E71130730C761204BDA

SHA-256: D3FB72451B66A1A370D8706C725A304E270C1CB5E46EA8B28DE8810FF7B13619

SHA-512: 1DEA52F16BB86738D4C02C7A1A9CADF3751C3B5C9E9D4B5A02C5C417575AFC57D9AFF15F0824EA9E647F6546237007DE81D03DB806347E7766C7991A3626D35

Malicious: false

Reputation: low

IE Cache URL: <http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xK3dSBYKcSV-LCoeQqfX1RYOo3aPA.woff>

Preview:

wOFF.....<p.....GDEF.....d.MGPOS...d..0....FN...GSUB..3.....J..OS/2..=...W...`|.cmap.=X...D..2..~.cvt ..T....\*...\*"..fpgm..T.....s.Y.7gasp..U.....  
glyf..U...q...N..head...@...6...6...hhea...x...\$...Dhmtx.....t...v..loca.....L.amaxp..{.... ..zname..{....A...[s.post.\*.....1.Q...prep.<...S...V.c.x...3..@..@..Ml...m..  
...m...Y..wg..."\*%\*...8..2.j2..Cv...|y.....Ks.ii-M..V..E.`cm.M.....L...g..L...Y.k...xRO.Y=...^\*..xG..C)...%...V...%j.1.K...,\$X:K...f.L..r`..y-/...X..Yl+...(je...rX.\*'5..5...X.c.klf..  
.5..Rb..l.^KcU.\*^c].....v.v...`7.=...>8.....#)\$..8.g...\_}1..e..W.j\_..|n....N.{|/.x..)?..."...&.l.#.)#%...!..t.....3..\$?:2.F..Y#...+ra... ..X4.b.(.%\$&F"...X6\*b..j..v...3zc...  
?...88.....c8...8:F.....c<c...dv.x..sxe.....d.N.v.:V.l^q..`m.v.=j;o...o...OU... ..p..B..m./..lqa5r&l8..gT.....uu.....z...^..D ..j...ua.z.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\6xKydSBYKcSV-LCoeQqfX1RYOo3i54rAkW[1].woff



Process: C:\Program Files (x86)\Internet Explorer\iexplore.exe

File Type: Web Open Font Format, TrueType, length 80556, version 1.1

Category: downloaded

Size (bytes): 80556

Entropy (8bit): 7.99192700798433

Encrypted: true

SSDEEP: 1536:zzjZPE5DptXxfzBHMfS9oHhUraBdpV2GzgxFXtW/MeLwM7dbCnx:Xjy9tfFHYcr8x2GzgjXw/zb7d+x

MD5: 89B96BBA0B783B75B544AE79EBDAFA3C

SHA1: 27179F16CBF61D09137B9329D414837555796268

SHA-256: 675C781CD8E680D29D91D4CAE91A022A926D9591A94BB23BD438A9111A6C46B2

SHA-512: 274DD0318B01C2B5F209F0E6173D7A5320CD3B322276A484EC73A130A3C1B321CE5D230C7A8C42AF7F9E0C0B28B16386257ED624F5C62C685C3C40978F84BA4

Malicious: false

Reputation: low

IE Cache URL: <http://https://fonts.gstatic.com/s/sourcesanspro/v14/6xKydSBYKcSV-LCoeQqfX1RYOo3i54rAkW.woff>

Preview:

wOFF.....GDEF.....d.MGPOS...d.../.....\_G<GSUB..2.....J..OS/2..<d...V...^..cmap.<...D..2..~.cvt ..T....\*...\*X..fpgm..T.....s.Y.7gasp..U(.....  
glyf..U0...J...%Fi.head...|...6...6...hhea.....\$...Bhmtx.....loca...X.....%...maxp.&.....pname.'.....@...X.qEpost..(H.....1.Q...prep..X...S...VS..8x...3..@..@  
..Ml...m.....m...Y..wg..."\*%\*...8..2.j2..Cv...|y.....Ks.ii-M..V..E.`cm.M.....L...g..L...Y.k...xRO.Y=...^\*..xG..C)...%...V...%j.1.K...,\$X:K...f.L..r`..y-/...X..Yl+...(je...rX  
\*5..5...X.c.klf..5..Rb..l.^KcU.\*^c].....v.v...`7.=...>8.....#)\$..8.g...\_}1..e..W.j\_..|n....N.{|/.x..)?..."...&.l.#.)#%...!..t.....3..\$?:2.F..Y#...+ra... ..X4.b.(.%\$&F"...  
X6\*b..j..v...3zc....?...88.....c8...8:F.....c<c...dv.x...\$K.....Y.z\*..v...==.....l.m...m{z#....'N|....Rd.....-...#.."'..l0j..O.v.d.G.....W.pL("...a...=D!..1.F].....|0].

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\8zxpfb5cm1Q[1].js

Process: C:\Program Files (x86)\Internet Explorer\iexplore.exe

File Type: ASCII text, with very long lines

Category: downloaded

Size (bytes): 63625

Entropy (8bit): 5.421702254679076

Encrypted: false

SSDEEP: 1536:d9Da72VF9InUTJOoOlX3iTDGFmgB2c/vtEA+S4Jk/MWJJr/tOt76tqtcm:7+rOM

MD5: F8EF817E0B96AF9BCA0310DF7D3C3E60

SHA1: D6710844D38DE40693BAEF32E94A3F5FFA107B77

SHA-256: FA50447F38E14580EA8BD2047698D6BACE11F5631EA3E5980E8A96E5FF3BEF38

SHA-512: 56CBDOEA5031E9AA3D74EC757A3F9AA9DDEDC13050D423DBBDFa536CE34C181F5F6CB448421EE5E35EEFFC8CC7F408B7298617403EF3D287A1A8F8108959D

Malicious: false

Reputation: low

IE Cache URL: [http://https://www.facebook.com/rsrc.php/v3/yA/r/8zxpfb5cm1Q.js?\\_nc\\_x=lj3Wp8lg5Kz](http://https://www.facebook.com/rsrc.php/v3/yA/r/8zxpfb5cm1Q.js?_nc_x=lj3Wp8lg5Kz)

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\8zxfB5cm1Q[1].js

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | <pre>if (self.CavalryLogger) { CavalryLogger.start_js(["4UdTPam"]); };__d(["SearchResultPageLoggingInlineActionFalcoEvent",["FalcoLoggerInternal","getFalcoLogPolicy_DO_NOT_USE"],(function(a,b,c,d,e,f){"use strict";a=b("getFalcoLogPolicy_DO_NOT_USE")("1744351");c=b("FalcoLoggerInternal").create("search_result_page_logging_in_line_action",a);e.exports=c}),null);__d(["SearchResultPageLoggingItemClickedFalcoEvent",["FalcoLoggerInternal","getFalcoLogPolicy_DO_NOT_USE"],(function(a,b,c,d,e,f){"use strict";a=b("getFalcoLogPolicy_DO_NOT_USE")("1744352");c=b("FalcoLoggerInternal").create("search_result_page_logging_item_clicked",a);e.exports=c}),null);__d(["SearchCometResultsLoggerUtil",["SearchResultPageLoggingInlineActionFalcoEvent","SearchResultPageLoggingItemClickedFalcoEvent","gkx"],(function(a,b,c,d,e,f){"use strict";a=function(a,c){b("SearchResultPageLoggingItemClickedFalcoEvent").logImmediately(function(){var b={click_type:"graph_search_results_module_tapped",common:{logging_unit_id:a,session</pre> |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\Disclosure-1[1].png

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File Type:      | PNG image data, 235 x 300, 8-bit colormap, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):   | 16568                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Entropy (8bit): | 7.98315171154593                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:         | 384:k9UPUkWXHJPQYTDI+Sw1ryjXfbsWyHfng3Xn9YyloF:ZUkgYSwEjX/3tYxoF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MD5:            | F6AE0325F67375F6B7759DA59AF9E132                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA1:           | 2FD46491FE198B4D5E4BE7573D452B2829CD0020                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:        | E4074E8505BB9A49063A628CDC1C0D854A62E2F7BD87C5F991C0BD97FF56C8A4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-512:        | 54077E0BB24020D3141B5FEF56A3E678A51F9790703125BBC90081C1B7D804273D264DA5F0F39137A11E484C735E26D11460F380288626FE889FA27A84742F02                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| IE Cache URL:   | http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Disclosure-1.png?fit=235%2C300                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | <pre>.PNG.....IHDR.....N.....PLTE.....GpL.....hhh...???...lll..... .....ZZ[....."\$%.....bba.....rsu.....NSY.....~.....]... .....YSL...zx.....777.. .....h^Q...AIPrj_Xaj....HECTI?vy}....yto{....}....gos.....%.....}.....sA...g].4...ft.m^.....;....p}.....5024A7-...jlt...dR-rc..H...K..zm .Nu...\$1?...S^..R..L..I.....b.4E...D.x=.....-.gq:XL...XD....y.Ej.a...k55#.....tRNS.^..6#...K...../...@LC.....=OIDATx..}L.i...f....K#;1.....nX.d\$.{Z]1..l....".k*KP&lt;=v. X...n..1U.... !^..q*4...W(W....*r9e...?...t:y....{-.....G'o...`N..\p.l6.7.....s</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\Facilities-Map-1[1].png

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | PNG image data, 2000 x 784, 8-bit colormap, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):   | 178812                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy (8bit): | 7.970347546563482                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:         | 3072:CymuzWfchFRH5dcKkyqUHvp1H3/ii1OeokEtm9lfb4mid9nHJTadBMMyCfFLvLc0:Cy/afcHR9k8HXFsjmfvb4jznpmMybnc0                                                                                                                                                                                                                                                                                                                                                                    |
| MD5:            | 81627450BF58D37BFE4D2CC748D03AA0                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:           | B409B6C4BE630D56D6E9BD8A3982D4066EE8FAA6                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:        | 837B30EACAFa2E7BA7C58BE1ECC5837067353365E189CABA2A03587494EC63E8                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-512:        | 02D87C180A9511BC81008FFDB1410A38D6F97A1B7D31853FB1CC58D2B2DEE31066D4ECEB8AF0948F2607415EBBB82627F3AF33C92759B6AF573289AC4DE7D9F3                                                                                                                                                                                                                                                                                                                                          |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IE Cache URL:   | http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Facilities-Map-1.png?fit=2000%2C784                                                                                                                                                                                                                                                                                                                                                                     |
| Preview:        | <pre>.PNG.....IHDR.....HA.....PLTE.....&gt;.7..... .....x.....xr].p-we.....u.&gt;.....}j.....f)..... .....rkW.....dW...jcMW.....)\$.t.....^...O@H..}}...iYJQ..O...bZCrjm.....XP6{vw@.....E6&gt;..... w....k^a;6?6'uss..NNF-.B=YT...ww.e_UO..p....z ..UM&gt;s...F..\jFO....h....&amp;-...7IDATx...{PSy...R3..C.@V.....+HBR..HB.[a.....&amp;rs@8..". .....R5..8cyc.Uy....5.3...X.k.y.-....&gt;..Z.An\...A...Vn..Z...j...9.....o.y...."N..2..5.... ..5%...\$.B.....@.%</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\EOQM8FL8ot[1].js

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                            |
| File Type:      | ASCII text, with very long lines                                                                                                 |
| Category:       | downloaded                                                                                                                       |
| Size (bytes):   | 5377                                                                                                                             |
| Entropy (8bit): | 5.237958461920356                                                                                                                |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 96:vAbG7AKxAoAmAkAkJAljwAbECr/is73JwwVUsmt5FDWfK/REZKm8pkskxZ:obGMN3db5LjfoCrqJ3yE8pb4Z                                          |
| MD5:            | 242C5D0DC231DF1879F0DE3CC299D4B6                                                                                                 |
| SHA1:           | C138DF34BFF8CCD39405E4ADA231DD6D6CA5C389                                                                                         |
| SHA-256:        | 908EDFA9F7EC9FD5C6B62159B5CB305D9C2C88601C8BF00A23BB0E96FCEA1E21                                                                 |
| SHA-512:        | 3B9E5800C3C2C68862B12B19B4DA2841A5750A51572FF8BF2386C2DA4E505BABC6A8F128D8A10BE6E00681EC487633D352F47B496B320964708DD2CE163C82B: |
| Malicious:      | false                                                                                                                            |
| Reputation:     | low                                                                                                                              |
| IE Cache URL:   | http://https://www.facebook.com/rsrc.php/v3/yr/r/EOQM8FL8ot.js?_nc_x=lj3Wp8lg5Kz                                                 |





C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\Tohono-Nation-Logo[1].png

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | .PNG.....IHDR.....PLTEGpL...5...\$....0.*....T.....#.....W.....#. " . #!!..... . \$. ..."!...% .<br>.W.X...(. ...)\$.W/).7,&...+. ....:2.+&.1+....aS.2(\$'-'=/'V.bE1?.f.\$+%""".B2(x.C...V7/.'+\$">6.p.....{.k.....&#B8...s.4-.hH2...Q...sa.G...w.....T]O.V...ji.....s...b>jZ....<br>{..R...e?.S...o.b..E;.\$&#...S<-G5'.....U.....1..o].xe.]B/ZL.K@.VJ....H=..h@X?...R(D/.kB%1(.VO...[.]U8...'?..sE...+^;)K2.L'+K7+....M.I.J...qD';...O.nC\...^<.)JzS73....<br>mL4O9..X9.N..SG_..)O4&6)Y..5.....7..qN5+Y8(H1.xG.KL...c<...MA..vF.qB-m@.{ l-h>....*T6....r...;!!\$)QE..yH_F+.8F.. *2~..8...z..i..AT....})tP6./9.LdOC.vQ6.Tp.rC.rB.. .....7<br>A....69+.]7.sC.h.....tRNS...].2....i=.E.'.sQ.....~y....qFTP..G)]DATx.XKL.....E.....7...993...2qp&..B.Q!.@B ..D.%P"..(.D.ES/..+V.L....il@W&].E....vs...f.jW....2\..<br>...y.o...B...k7[o]ok |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\Uf-73aw922e[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Type:      | C source, ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Size (bytes):   | 15628                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Entropy (8bit): | 5.525555044677657                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:         | 192:McOaZmZciy4p4rItSUua5y5nK8C1HPlymDD+JmCQNjs+1nVDutDjocHU6:vOemZHy4pRQUUa05KhymDDDCQ6qDudt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| MD5:            | 01E5FB170D66BF5010B0C781E58B84E7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:           | 083CC1DBB2C119B8B76226FB67791A25A0C55FC6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:        | 4EEF62C77A19B7D9FB6F894CFA0E7757E0A3BF2936C1AF0D330A9E409914BDE0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:        | 996006AB31F6F6C605754C12958B62F07E9977A4E8C1038178B25B4E19355D3F0853835E4E4676B774D0BE6CE83974417370022A093D5FEEEC2AA4B9F2299882                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IE Cache URL:   | http://https://www.facebook.com/rsrc.php/v3/yl/r/Uf-73aw922e.js?_nc_x=lj3Wp8lg5Kz                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:        | if (self.CavalryLogger) { CavalryLogger.start_js(["7V7daTM"]); }.__d__("ChannelConstants",[],(function(a,b,c,d,e,f){var g="channel/";a=[CHANNEL_MANUAL_RECONNECT<br>_DEFER_MSEC:2e3,MUTE_WARNING_TIME_MSEC:25e3,WARNING_COUNTDOWN_THRESHOLD_MSEC:15e3,ON_SHUTDOWN:g+"shutdown",ON_INVALID_HI<br>STORY:g+"invalid_history",ON_CONFIG:g+"config",ON_ENTER_STATE:g+"enter_state",ON_EXIT_STATE:g+"exit_state",ATTEMPT_RECONNECT:g+"attempt_reco<br>nnect",RTI_SESSION:g+"new_rti_address",CONSOLE_LOG:g+"message:console_log",GET_RTI_SESSION_REQUEST:g+"rti_session_request",SKYWALKER:g+"skyw<br>alker",CHANNEL_ESTABLISHED:g+"established",OK:"ok",ERROR:"error",ERROR_MAX:"error_max",ERROR_MISSING:"error_missing",ERROR_MSG_TYPE:"error_m<br>sg_type",ERROR_SHUTDOWN:"error_shutdown",ERROR_STALE:"error_stale",SYS_OWNER:"sys_owner",SYS_NONOWNER:"sys_nonowner",SYS_ONLINE:"s<br>ys_online",SYS_OFFLINE:"sys_offline",SYS_TIMETRAVEL:"sys_timetravel",HINT_AUTH:"shutdown auth",HINT_CONN:"shutdown conn",HINT_DISABLED:"shutdown<br>disabled",HINT_INVALID_ST |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\Vision[1].png

|                 |                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                           |
| File Type:      | PNG image data, 180 x 180, 8-bit colormap, non-interlaced                                                                                                                                                                                                                                                       |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                      |
| Size (bytes):   | 5719                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit): | 7.790531810642579                                                                                                                                                                                                                                                                                               |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                           |
| SSDEEP:         | 96:94F+2Hb29C0lp1TfHsTf0UKB2zs7Ldb4qbcCC1nhBltiYAXEOBM:hG4XIRHxr2zs7dqH1hBzDH                                                                                                                                                                                                                                   |
| MD5:            | 5878DCCCE857497B3BD97C45180CCCE9E                                                                                                                                                                                                                                                                               |
| SHA1:           | E0B10C4D10B3DB82721531825C561FA12E88E3E9                                                                                                                                                                                                                                                                        |
| SHA-256:        | 134303F28C957A94F633460CF605F3F7251B6FDE07910A005A1803F25600CBE7                                                                                                                                                                                                                                                |
| SHA-512:        | 4847789D9EA4D96B477BB4F74CC5F16219F75A256AB7BB555A7461331DCFC53D51A3EA54D3C36BD6E74BE84FEDBB8264BEBD8290BB6933B83FB1A3457EEEF3<br>93                                                                                                                                                                            |
| Malicious:      | false                                                                                                                                                                                                                                                                                                           |
| Reputation:     | low                                                                                                                                                                                                                                                                                                             |
| IE Cache URL:   | http://https://i0.wp.com/www.tonhc.org/wp-content/uploads/2017/09/Vision.png?resize=180%2C180                                                                                                                                                                                                                   |
| Preview:        | .PNG.....IHDR.....PLTEGpL.3)...!.....#.....**...\$\$.....".....'.....!.....!<br>.....U.....@!....."<br>'.....\$. .....&.....!<br>.....@@.....m\$\$.....-.....tRNS.../.....X.....D.....T.....B#).h.0.'...M\$J..8...<P... ..u.*....=.4.....U..W..6z....!+...H.G.....Lq_]d..(.lR5...).Es...r.x.&.1.tj<br>..f....Q. |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\\_0FMPEc0nGG[1].png

|                 |                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                               |
| File Type:      | PNG image data, 64 x 204, 8-bit colormap, non-interlaced                                                                            |
| Category:       | downloaded                                                                                                                          |
| Size (bytes):   | 3241                                                                                                                                |
| Entropy (8bit): | 7.574519172893556                                                                                                                   |
| Encrypted:      | false                                                                                                                               |
| SSDEEP:         | 48:SutiOxAiSVq2Mml0WqtYyYQiocrFP7w0xiF2fvbxWBhoM4znXOLk:SyfxAiSohml0PVQirrD8F8vbxfbZ4k                                              |
| MD5:            | D3B63E5A2751EB4859D45D5012220858                                                                                                    |
| SHA1:           | 8DE1DB85A32181F35DD7DA868343BC0BC1D03B74                                                                                            |
| SHA-256:        | 413DF42B0BC720E5A3EBDE9068FB24D838F9920D120386C7CF86B254F9F0AFF1                                                                    |
| SHA-512:        | CDC3AEC465C54ADD244AF2495C9CC765FFC0FC5487C2CC56ABF18A6112D293EC02EC2425E12AD94A6F9E7EF265636EFB8919EF937C2A3C30B4518F5FCE248<br>C6 |
| Malicious:      | false                                                                                                                               |



|                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\errorPageStrings[1]</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IE Cache URL:                                                                                 | res://ieframe.dll/errorPageStrings.js                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:                                                                                      | <pre>//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";...var L_REFRESH_TEXT = "Refresh the page.";...var L_MOREINFO_TEXT = "More information";...var L_OFFLINE_USERS_TEXT = "For offline users";...var L_RELOAD_TEXT = "Retype the address.";...var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";...var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";...var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";...var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";...//used by invalidcert.js and hstserror.js...var L_CertUnknownCA_TEXT = "Your PC doesn't trust this website's security certificate.";...var L_CertExpired_TEXT = "The website's security certificate is not yet valid or has expired.";...var L_CertCNMismatch_TEXT = "The hostname in the website's security certificate differs from the website you are trying to visit.";...var L</pre> |

|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\ewd-toggle-icon[1].woff</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Process:                                                                                          | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:                                                                                        | Web Open Font Format, CFF, length 2400, version 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Category:                                                                                         | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Size (bytes):                                                                                     | 2400                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Entropy (8bit):                                                                                   | 7.661332138618158                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:                                                                                        | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:                                                                                           | 48:UqV0JbsrbeQFH2I99qsGdZxI/8La4JPJWGHb3tXI7JFVa73+a:UqqGrK2W199qscxIELaWP4GhB3I7tax                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:                                                                                              | 23A98DE91E6A8C03624F46C2054758D8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:                                                                                             | 0302CCBAD2D83D2A9B041B5C6D950E31DCD5AE2B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:                                                                                          | 83CC753A48CD26CDDBECA4C4EA9252332572530F67EBCA7007E49AA73E7574CC7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:                                                                                          | B920E8381065CA472BC476B393BEBE63C95C4C037BDF22181D9C19C59A375AFE3130DB1F03BF139693D260BBCB2844948D98CAE2B45E949C9B3448D9CFD849                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Malicious:                                                                                        | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reputation:                                                                                       | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IE Cache URL:                                                                                     | http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/fonts/ewd-toggle-icon.woff                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                                                                          | <pre>wOFFOTTO...`.....CFF.....=Q...FFTM.....s.GDEF..... L.OS/2.....K...`Q^cmap...\......~WbMhead...../...6....hhea.....\$.hmtx...8...+...B. ).vmaxp...d.....P.name...l.....post...P.....X.VmL.G..9no..r..5...F[R..4j...j.b.....'.wi...;.....%..J..B..6..L!.4411.6A.G...Kmg...t.t.df.y.y.\$... ..\$....4...A....Q. ...1.b.`{k.D.....RNQ.1.....&gt;&amp;.x...../k.`.....P.....L...".z.S.ax.V.....{W....fx.m8a(v.G%.O...%&amp;t0...M.{S.....%`.l.l.1[.....c[.y...".B.l.6B?.@..l.....6... ';...v..x.....^.....u.....'.....i0...3....`3....6f.;...V.VN.K.*.h...+.....&lt;...7.b.;Cv.Z..Y...Ai.(-eY.5Rvj.e.5V%Kd...LF.U.j)... ..y.&amp;5...Q....+/QTBY.).Y. R].0l.1.`-Q2Y.R3..g... ...j....e..2...yi...3..~.g.....8j]..%..`O...&gt;....Y.....D....h.)8.MX.&lt;Na1O&amp;&gt;:R.j..+....t3y....ey.oV.....yy..yy</pre> |

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\ewd-ufaq-styles[1].css</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                         | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                                       | ASCII text, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Category:                                                                                        | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):                                                                                    | 13201                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                                  | 5.144273178727                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:                                                                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                          | 192:Cw0uLkUIf6JkqT9D1o9fP7k9X6Jrbq0u1:RPLNJkqhD21jMx                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:                                                                                             | 8B54F0822E48BCAE1897087A524149AC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                            | 8BB291F2D92864BAEB8F05D971EEE67D6E09DB29                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                         | D4E4F37120FD559331E37E0E1B779CE9B54EDBB1A16DD72079ED22485B6997CB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                         | B8D29D6BD1010A54AF4AC8587CC78EFB14754DB19CE2D55C15B018296CE87F8022683D3C856225FC52541CB2E1B2D357CFFA7673C7733894AC62DE3E6C248F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Malicious:                                                                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:                                                                                      | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IE Cache URL:                                                                                    | http://www.tonhc.org/wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preview:                                                                                         | <pre>.ewd-ufaq-hidden {.. display:none;..}.....ufaq-faq-category-title-toggle {.. cursor: pointer;..}.....ufaq-faq-category-body-hidden {.. display: none;..}.....ewd-ufaq-clear {.. clear:both;..}.....ufaq-permalink {.. margin: 24px 0;..}.....ufaq-permalink-image {..background: url("/.images/insert_link.png");...height: 21px;...width: 30px;...margin-top: -32p x;...margin-left: 112px;..}.....ewd-ufaq-author-date {..}.....ewd-ufaq-author {.. font-weight: 600;..}...ewd-ufaq-date {.. font-weight: 600;..}...ufaq-faq-categories, .ufaq-faq-t ags{..}.....ufaq {}/*..ufaq-faq-title {.. cursor:pointer;..}*/...ufaq-faq-category-title {.. width: 100%;.. clear: both;..}.....ufaq-faq-category{.. margin-bottom: 20px;..}.....ufaq-faq- category-inner {.. margin-bottom: 48px;..}.....ufaq-faq-body {.. padding:10px 25px;.. padding-left: 55px;..}...ufaq-faq-search{.. margin:5px 0 !important;..}...ufaq-search-hig hlight {.. background: #f7ff00;..}...ewd-otp-field-label{..width: auto !important;..}...u</pre> |

|                                                                                     |                                                                                                                                 |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\lg[1].gif</b> |                                                                                                                                 |
| Process:                                                                            | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type:                                                                          | GIF image data, version 89a, 6 x 5                                                                                              |
| Category:                                                                           | downloaded                                                                                                                      |
| Size (bytes):                                                                       | 50                                                                                                                              |
| Entropy (8bit):                                                                     | 3.8488255736198                                                                                                                 |
| Encrypted:                                                                          | false                                                                                                                           |
| SSDEEP:                                                                             | 3:CN+ltRPQEsJen2sSX:xvQEsJ42sSX                                                                                                 |
| MD5:                                                                                | E4D673A55C5656F19EF81563FB10884C                                                                                                |
| SHA1:                                                                               | 1F2D8ED221D39329251AD3A6FF1EDB20B7219443                                                                                        |
| SHA-256:                                                                            | F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1                                                                |
| SHA-512:                                                                            | E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B18479D027016D5BEB148403EF185430DB35F5AED362F36CE2C8ECAD0E6D8E30CEA97E4 |
| Malicious:                                                                          | false                                                                                                                           |
| Reputation:                                                                         | low                                                                                                                             |

**C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\g[1].gif**

|               |                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IE Cache URL: | <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=116&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7313772066002118">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=116&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7313772066002118</a> |
| Preview:      | GIF89a.....!.....bx..j....;                                                                                                                                                                                                                                                                                                                                                               |

**C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\g[2].gif**

|                 |                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                   |
| File Type:      | GIF image data, version 89a, 6 x 5                                                                                                                                                                                                                                                                                                                                                      |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 50                                                                                                                                                                                                                                                                                                                                                                                      |
| Entropy (8bit): | 3.8488255736198                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                   |
| SSDEEP:         | 3:CN+lrPQEsJen2sSX:xvQEsJ42sSX                                                                                                                                                                                                                                                                                                                                                          |
| MD5:            | E4D673A55C5656F19EF81563FB10884C                                                                                                                                                                                                                                                                                                                                                        |
| SHA1:           | 1F2D8ED221D39329251AD3A6FF1EDB20B7219443                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:        | F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1                                                                                                                                                                                                                                                                                                                        |
| SHA-512:        | E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B1B479D027016D5BEB148403EF185430DB35F5FAED362F36CE2C8ECAD0E6D8E30CEA97E4                                                                                                                                                                                                                                                        |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                   |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                     |
| IE Cache URL:   | <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=89&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7034506522366686">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=89&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7034506522366686</a> |
| Preview:        | GIF89a.....!.....bx..j....;                                                                                                                                                                                                                                                                                                                                                             |

**C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\g[3].gif**

|                 |                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | GIF image data, version 89a, 6 x 5                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):   | 50                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 3.8488255736198                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:         | 3:CN+lrPQEsJen2sSX:xvQEsJ42sSX                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | E4D673A55C5656F19EF81563FB10884C                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:           | 1F2D8ED221D39329251AD3A6FF1EDB20B7219443                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:        | F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1                                                                                                                                                                                                                                                                                                                          |
| SHA-512:        | E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B1B479D027016D5BEB148403EF185430DB35F5FAED362F36CE2C8ECAD0E6D8E30CEA97E4                                                                                                                                                                                                                                                          |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                       |
| IE Cache URL:   | <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=221&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7699525934342165">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=221&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.7699525934342165</a> |
| Preview:        | GIF89a.....!.....bx..j....;                                                                                                                                                                                                                                                                                                                                                               |

**C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\g[4].gif**

|                 |                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | GIF image data, version 89a, 6 x 5                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):   | 50                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 3.8488255736198                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:         | 3:CN+lrPQEsJen2sSX:xvQEsJ42sSX                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | E4D673A55C5656F19EF81563FB10884C                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:           | 1F2D8ED221D39329251AD3A6FF1EDB20B7219443                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:        | F3A8992ACB9AB911E0FA4AE12F4B85EF8E61008619F13EE51C7A121FF87F63B1                                                                                                                                                                                                                                                                                                                          |
| SHA-512:        | E0B03411282A979CF772F700D9E5634B0C25C612E380AD33C0D59059B1B479D027016D5BEB148403EF185430DB35F5FAED362F36CE2C8ECAD0E6D8E30CEA97E4                                                                                                                                                                                                                                                          |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                     |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                       |
| IE Cache URL:   | <a href="http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=258&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.6413604959210941">http://pixel.wp.com/g.gif?v=ext&amp;j=1%3A8.6.2&amp;blog=140258946&amp;post=258&amp;tz=-7&amp;srv=www.tonhc.org&amp;host=www.tonhc.org&amp;ref=&amp;fcp=0&amp;rand=0.6413604959210941</a> |
| Preview:        | GIF89a.....!.....bx..j....;                                                                                                                                                                                                                                                                                                                                                               |

**C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\grid[1].css**

|               |                                                       |
|---------------|-------------------------------------------------------|
| Process:      | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type:    | ASCII text                                            |
| Category:     | downloaded                                            |
| Size (bytes): | 9064                                                  |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\grid[1].css

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entropy (8bit): | 5.075396685069554                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:         | 96:pYN4fYeJ7ldtQu7ssNiTfwhS0RbVvdmjerkWLR0qKS9ldUBZptosk/CFCIUZXOt:0eJ7ytQu4ssEZbCjeoWLCTCuQM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| MD5:            | 07EBF81EEE8D9A44213E6A8D3632C232                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:           | A63D87C7911104530DDAE00D1F281B9AB3E08B2B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:        | D9E3F45179711015AA2DCAC0689784AD76FD2055A3B13DA58A88A1590057B719                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:        | 162E61C2C3762D75D56D9F8BC544C4DA994F39F017D18124090B0065169FEFFA37EF6B79E850F11CC747305BD58919DAEF5A46092467EDC0E06DEC8F7ED397A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IE Cache URL:   | http://www.tonhc.org/wp-content/themes/enfold/css/grid.css?ver=2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Preview:        | <pre>/* Table of Contents.===== #Base 960 Grid. #Tablet (Portrait). #Mobile (Portrait). #Mobile (Landscape). #Clearing */./* #Base 960 Grid.===== */.html { min-width: 910px; }.html.responsive { min-width: 0px; }.boxed#top { margin: 0 auto; overflow: visible; /* position:relative; z-index: 3; */...container { position: relative;. width: 100%;. margin: 0 auto;. padding: 0px 50px;. clear: both;}.inner-container{ position: relative; height:100%; width:100%; }./*no z-index for container_wrap or fixed bgs start disapearing when other elements transition -&gt; weird chrome bug*/.container_wrap { clear: both;. position: relative;. /* z-index: 1; */. border-top-style: solid;. border-top-width: 1px;}.unit,.units { float: left;. display: inline;. margin-left: 50px;. position: relative;. z-index: 1;. min-height: 1px;}.row { position: relative;. margin-bottom: 20p</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\jetpack[1].css

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):   | 74986                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 5.033945086500054                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 1536:aMSPADZpQ8l2V9aW0kPQlV0G/oJ7ozUA2J3nQJtQZS:CV0+oJ7c2J3nQJtQZS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MD5:            | 6A95FB13F75DBD3EAD545C3472B1EFC0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | 3A17C602F00401108DC19E8415B046854F963412                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:        | 7002BD7E9131EC2B5D12C24A2CC181F046F5237ADDF358A93921055D3EDA73A9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | FE95313B0BCBAFFDDAA2D7C514173F55AC1B499357C0D64AF674D0BCB2631A5F332978F239EF6F7AEF0C8BDFE1457DDD71549D42CB0054E5B3B082B4485EA8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IE Cache URL:   | http://www.tonhc.org/wp-content/plugins/jetpack/css/jetpack.css?ver=8.6.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Preview:        | <pre>/*!.* Do not modify this file directly. It is concatenated from individual module CSS files.*/.[data-carousel-extra]{cursor:pointer}.jp-carousel-wrap *{line-height:inherit}.jp-carousel-overlay{background:#000}div.jp-carousel-fadeaway{background:-moz-linear-gradient(bottom,rgba(0,0,0,.5),rgba(0,0,0,0));background:-webkit-gradient(linear,left bottom,left top,from(rgba(0,0,0,.5)),to(rgba(0,0,0,0)));position:fixed;bottom:0;z-index:2147483647;width:100%;height:15px}.jp-carousel-next-button span,.jp-carousel-previous-button span{background:url(../modules/carousel/images/arrows.png) no-repeat center center;background-size:200px 126px}.jp-carousel-msg{font-family:"Open Sans",sans-serif;font-style:normal;display:inline-block;line-height:19px;padding:11px 15px;font-size:14px;text-align:center;margin:25px 0 2px;background-color:#fff;border-left:4px solid #ffba00;box-shadow:0 1px 1px 0 rgba(0,0,0,.1)}@media only screen and (-webkit-min-device-pixel-ratio:1.5),only screen and (-o-min-device-</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\jquery.spin.min[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):   | 1806                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit): | 5.008108638193758                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 48:23QpP2wGkdJ/C7LOK/rXBTiBdpdP8y+I+aUuX+JlgskkJlg1kSksH/sHWkalDaJ:FYc/oL9/rXBmBXdZ+I+fuX+JlgHkJlgs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:            | F51BEB5A11ED192A3794D90B048CC7A3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | 59419CEA82CB0D5DE1772D7135F21399260A8C1C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:        | 36AD0EDAF88CB19E7CBDAE22470C1F124F02FD5673BF6144C0A7A9F0A8FEF987                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | 05BB31BD8E5AD9E14C7639895ABC81A3BFF8CABE344D13EAEAEAC763786060665AFF7AB0602A21866C8076C402636A610E14AF7DC67EC2A7E0BD245727AC6E36B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IE Cache URL:   | http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/jquery.spin.min.js?ver=1.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Preview:        | <pre>/* Do not modify this file directly. It is compiled from other files.*/./*.* Copyright (c) 2011-2013 Felix Gnass. * Licensed under the MIT license. */.!function(e){if("object"===typeof exports)e(require("jquery"),require("spin"));else if("function"===typeof define&amp;&amp;define.amd)define(["jquery","spin"],e);else if(!window.Spinner)throw new Error("Spin.js not present");e(window.jQuery.window.Spinner)}}(function(e,n){e.fn.spin=function(s,i){return this.each(function(){var t=e(this),r=t.data();if(r.spinner&amp;&amp;(r.spinner.stop(),delete r.spinner),!1!==s){if(void 0!==(s=e.extend({color:i  t.css("color")},e.fn.spin.presets[s]  s)).right&amp;&amp;void 0!==(s.length&amp;&amp;void 0!==(s.width&amp;&amp;void 0!==(s.radius){var p=t.css("padding-left");p=void 0===p?0:parseInt(p,10),s.left=t.outerWidth()-2*(s.length+s.width+s.radius)-p-s.right,delete s.right}r.spinner=new n(s).spin(this))}),e.fn.spin.presets={tiny:{lines:8,length:2,width:2,radius:3},small:{lines:8,length:4,width:3,radius:5},large:{lines:10,length:8,width:4,radiu</pre> |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\jquery[1].js

|            |                                                       |
|------------|-------------------------------------------------------|
| Process:   | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines                      |
| Category:  | downloaded                                            |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\jquery[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):                                                                            | 96873                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Entropy (8bit):                                                                          | 5.372169393547772                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:                                                                                  | 1536:HYE1fGBiByJsbfXxERJ/shgWcELccJdZVhK04ssx+/mvaSIFSet43tpXJlGVyp3:fsAg0psxTva/FSeKy2bDD5a98Hrq                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:                                                                                     | 49EDCCAE2E7BA985CADC9BA0531CBED1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:                                                                                    | F8747F8EE704D9AF31D0950015E01D3F9635B070                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:                                                                                 | 1DB21D816296E6939BA1F42962496E4134AE2B0081E26970864C40C6D02BB1DF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:                                                                                 | F766DF685B673657BDF57551354C149BE2024385102854D2CA351E976684BB88361EAE848F11F714E6E5973C061440831EA6F5BE995B89FD5BD2D4559A0DC4A6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Reputation:                                                                              | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IE Cache URL:                                                                            | <a href="http://www.tonhc.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp">http://www.tonhc.org/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:                                                                                 | <pre>/*! jQuery v1.12.4   (c) jQuery Foundation   jquery.org/license   WordPress 2019-05-16 */!function(a,b){("object"===typeof module&amp;&amp;"object"===typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a))("undefined"!==typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^(?![\s\uFEFF\xA0]+)\$/g,p=/^ms- q=-(?!da-z)/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?a&lt;0?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,fun</pre> |

|                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\In-uOOobFC9i[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Process:                                                                                        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:                                                                                      | PNG image data, 12 x 12, 8-bit/color RGBA, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category:                                                                                       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                                                   | 3249                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Entropy (8bit):                                                                                 | 7.929663426617602                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:                                                                                      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:                                                                                         | 48:+XWdV9rAZyAbLssK8o8n9TBDaLoieWrfvAtqslu8gGPzMum3EkPyvS7N33FzGmyl:h5cZjAy9nzDaMieWrf9sMnGPzMLYES1/                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| MD5:                                                                                            | 171A063C73F992E71492C4D26605EEE3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:                                                                                           | 690AA01695C908EC153D4900E81F6FAA3E16FBCC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:                                                                                        | 33C09AD5541630DDD97336563AB0C8C13396DCE0075375A15A370BB90B29E6E7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:                                                                                        | 44D57F3FC0F5B63E2D71650B86B0733B71C78162D35C318E88E520EF76A20DB3762AB21CFE80B1D7DA416A2FF33F44E0CC245180EAFBFDDBC687BA83EA98B1E17                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Malicious:                                                                                      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:                                                                                     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IE Cache URL:                                                                                   | <a href="http://https://www.facebook.com/rsrc.php/v3/y3/r/In-uOOobFC9i.png">http://https://www.facebook.com/rsrc.php/v3/y3/r/In-uOOobFC9i.png</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:                                                                                        | <pre>.PNG.....IHDR.....Vu.....iCCPICC Profile..H...wTS...{-tB.H. ....@h1....."(X...b.6(&gt; ...l.....;k.s.k..6...'d.j.9.lith.kFb...p..4@@...GEM..n...[.k.....?Uu.0...Da.TA.?...X/.K...86.....9.cM)6A.%rN...9.q.....y....&lt;4.....~:V.v.c'. C.@'c.....al..3W...S.V'.o.*k.x.J.[.O..A.y.l.]...-.K.....!b{V.....H...B...D.sF&gt;7v.E...q.e...s.....:-r\...b{?V.H..0.aP.8K.F+.y.1J.H.8m.....bn&lt;)F.fav...(&lt;...kl..(=.....OQ3...e.p.u.4L.K.wZ....).P..R..-B..A.9.....f...Y.....b..=.....V[.} ...k...8.JE.k...r.....01o{_-&amp;P...A.*.&amp;...58....7p...!b!f..D. .0...2(rX.....)p.Z....sp...M...0./'.... \$.0.]...@....."\$\$.IDR.tD...r...@...H.r.9..B..=]...D..Q.JG5QC.....Q.4.Eg..h.Z.....*.....K.M.)....G.i.Lp.86...K...2!%...k.u..zq/q..D&lt;...;a.8&lt;..._...[.g...].!7..`@.#x....t.&lt;B)....p.p.p.0@xO\$.VD.b.1..l@lE.BI&amp;v{...a...K.#..!"&lt;R&gt;.....t.t.4@.H.....r.YL.&amp;W...O.....G(j....%.".....S.P.(#</pre> |

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\onuUJj0tCqE[1].png</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Process:                                                                                       | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:                                                                                     | PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category:                                                                                      | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                                                  | 3944                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Entropy (8bit):                                                                                | 7.942659052942245                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:                                                                                        | 96:ZH5cZjAy9nzDaMieWrf9sMnGPzMLYcyQ7IjZKf:DtWnrSp6QmJZKf                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:                                                                                           | 38AD1D995A5599DA0C46928C3FD78372                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA1:                                                                                          | E01AF1AAEA5B36B8D8BAE8EC18814F2FCE02E5CF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-256:                                                                                       | 5F71FCC2D00D22FFD4D9A07B64C435F88DE80893F838FA64A45C386CBBA0C601                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:                                                                                       | 3ED0F3A9FC7C5FA6EEACA1A3DE1E6B1A618A1C2065D61FD6BEBB35C0F888B1FF4144816BA63E66DB780C64470AC71AE731AA1CBE3380F41E8EE8F130E5882B1D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Malicious:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Reputation:                                                                                    | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IE Cache URL:                                                                                  | <a href="http://https://www.facebook.com/rsrc.php/v3/y2/r/onuUJj0tCqE.png">http://https://www.facebook.com/rsrc.php/v3/y2/r/onuUJj0tCqE.png</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:                                                                                       | <pre>.PNG.....IHDR.....w=.....iCCPICC Profile..H...wTS...{-tB.H. ....@h1....."(X...b.6(&gt; ...l.....;k.s.k..6...'d.j.9.lith.kFb...p..4@@...GEM..n...[.k.....?Uu.0...Da.TA.?...X/.K...86.....9.cM)6A.%rN...9.q.....y....&lt;4.....~:V.v.c'. C.@'c.....al..3W...S.V'.o.*k.x.J.[.O..A.y.l.]...-.K.....!b{V.....H...B...D.sF&gt;7v.E...q.e...s.....:-r\...b{?V.H..0.aP.8K.F+.y.1J.H.8m.....bn&lt;)F.fav...(&lt;...kl..(=.....OQ3...e.p.u.4L.K.wZ....).P..R..-B..A.9.....f...Y.....b..=.....V[.} ...k...8.JE.k...r.....01o{_-&amp;P...A.*.&amp;...58....7p...!b!f..D. .0...2(rX.....)p.Z....sp...M...0./'.... \$.0.]...@....."\$\$.IDR.tD...r...@...H.r.9..B..=]...D..Q.JG5QC.....Q.4.Eg..h.Z.....*.....K.M.)....G.i.Lp.86...K...2!%...k.u..zq/q..D&lt;...;a.8&lt;..._...[.g...].!7..`@.#x....t.&lt;B)....p.p.p.0@xO\$.VD.b.1..l@lE.BI&amp;v{...a...K.#..!"&lt;R&gt;.....t.t.4@.H.....r.YL.&amp;W...O.....G(j....%.".....S.P.(#</pre> |

|                                                                                              |                                                       |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\photon.min[1].js</b> |                                                       |
| Process:                                                                                     | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type:                                                                                   | ASCII text, with very long lines                      |
| Category:                                                                                    | downloaded                                            |

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\photon.min[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):                                                                                | 758                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Entropy (8bit):                                                                              | 4.985035613324602                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:                                                                                      | 12:UUIJ3l19KkktvWKAoFEWq2sTujlF5Y3wwSC6g5V9jQXEegHAAp9PSuzeYwQ:VIJ3CHktOpoFEWq2slY3AC64C0EgHAYR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:                                                                                         | C29857EEB45DA2DC95F2D0EEE1BA065A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:                                                                                        | 4A26F361D82EB6A4070B13BB569D3A7B971B6FE7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:                                                                                     | E1B0066BC1972444C0A15E1778BE06ED7BF36C55D597C065B5E79041BCDA291E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:                                                                                     | 308A38B9AF4289EB0F9704D2C991C7C7A49DB9CE5909758901867D2F3F71AA0F60AF0D58A63F96610BA5DB1696B6EE290596A621742E63E51BC1E28CBF80C2D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Malicious:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Reputation:                                                                                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IE Cache URL:                                                                                | <a href="http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001">http://www.tonhc.org/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Preview:                                                                                     | <pre>/* Do not modify this file directly. It is compiled from other files. */.!function(){function t(){if(this.complete){var e=this.getAttribute("data-lazy-src");if(e&amp;&amp;this.src==e)this .addEventListener("onload",t);else{var d=this.width,n=this.height;d&amp;&amp;d&gt;0&amp;&amp;n&amp;&amp;n&gt;0&amp;&amp;(this.setAttribute("width",d),this.setAttribute("height",n),i(this))}}else this.addEvent Listener("onload",t)}var e=function(){for(var e=document.querySelectorAll("img[data-recalc-dims]"),i=0;i&lt;e.length;i++)t.call(e[i])}.i=function(t){t.removeAttribute("data-recalc- dims"),t.removeAttribute("scale")};"undefined"!=typeof window&amp;&amp;"undefined"!=typeof document&amp;&amp;"loading"===document.readyState?document.addEventListener(" DOMContentLoaded",e):e(),document.body.addEventListener("is.post-load",e)}();</pre> |

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\position.min[1].js</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Process:                                                                                       | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| File Type:                                                                                     | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Category:                                                                                      | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Size (bytes):                                                                                  | 6438                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit):                                                                                | 5.236400049384502                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SSDEEP:                                                                                        | 192:bu2o9mX7JvbUjgls3F/yqbdkJhsmCariGf:bu2o9mdDUkThyqsswri6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| MD5:                                                                                           | D1C2E97EECA08CA067CCF2C5736F0390                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA1:                                                                                          | 5281985542FCC8C5A651D1991296E12C39BFCB82                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-256:                                                                                       | 0CE51090B148A45A0E3D652719ED6EF7F1A38E5D272DBF874F86A49664E897A3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-512:                                                                                       | 5CF6AF1E1F0F73884D6B5614ED57FDCB6FB850CCDA298133E3F2916EE5119FB34320700882F17934983E31159011821EC56F5AF8D18239A61E96BF22789B9451                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Malicious:                                                                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Reputation:                                                                                    | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IE Cache URL:                                                                                  | <a href="http://www.tonhc.org/wp-includes/js/jquery/ui/position.min.js?ver=1.11.4">http://www.tonhc.org/wp-includes/js/jquery/ui/position.min.js?ver=1.11.4</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Preview:                                                                                       | <pre>/*!. * jQuery UI Position 1.11.4. * http://jqueryui.com. * * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jquery.org/license. * * http://api.jqueryui.com/position/. */.!function(t){"function"==typeof define&amp;&amp;define.amd?define(["jquery"],t):(jQuery)(function(){return function(){l.ui=l.ui  {};var o,H,x=Ma th.max,T=Math.abs,L=Math.round,n=/left center right , =top center bottom/,f=/[+ -] d+/,s=/^lw+/,h=/%\$/,e=l.fn.position;function P(t,i,e){return(parseFloat(t[t[0]]* (h.test(t[0])?1/100:1),parseFloat(t[1]))*(h.test(t[1])?e/100:1))}function D(t,i){return parseInt(l.css(t,i),10)}l.position={scrollbarWidth:function(){if(void 0===o)return o;var t,i=l(" &lt;div style='display:block;position:absolute;width:50px;height:50px;overflow:hidden;'&gt;&lt;div style='height:100px;width:auto;'&gt;&lt;/div&gt;&lt;/div&gt;"),e=i.children()[0];return l("bod y").append(i),t=e.offsetLeft,i.css("overflow","scroll"),t===(e=e.offsetWidth)&amp;&amp;(e=[0].clientWidth),i.remove(</pre> |

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\san-simon[1].htm</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Process:                                                                                     | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| File Type:                                                                                   | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Category:                                                                                    | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Size (bytes):                                                                                | 47555                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Entropy (8bit):                                                                              | 5.361805291150674                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Encrypted:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SSDEEP:                                                                                      | 768:cZYHV9uUL+eE+elq8+ei+eqLP08O+1LOgC4TE/EgdzNfMyAukOmSSaM7u/BajVd9:PHV9u0+eE+elT+ei+eq9TUEgdzJvoOml                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MD5:                                                                                         | CBC454D1A92FFEB4A599932B5F8A653F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA1:                                                                                        | 5E3A05E3D0C6A8022E5BFC1A501E635C0E4A30A9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-256:                                                                                     | 3568954877AB63BD0F1871D82683ADA8EF8094CEF6ECEA1E0B6227168B768B1D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-512:                                                                                     | FE1A8DF51B261541336F8DF3A7A3675881CFABCD2318B17F4F1D05CC0E67E67838CCA6EBA84B8B9EE147AC9AEFDEFD708C518EB4DA18905AD32008FE9AE35C16                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Reputation:                                                                                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Preview:                                                                                     | <pre>&lt;!DOCTYPE html&gt;.&lt;html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_346 av-no-preview"&gt;.&lt;head&gt;.&lt;meta charset="UTF-8"/&gt;... mobile setting --&gt;.&lt;meta nam e="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"&gt;.. Scripts/CSS and wp_head hook --&gt;... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ --&gt;..&lt;title&gt;San Simon - TON-HC&lt;/title&gt;..&lt;meta name="robots" content="index, follow" /&gt;..&lt;meta name="googlebot" co ntent="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" /&gt;..&lt;meta name="bingbot" content="index, follow, max-snippet:-1, max-image- preview:large, max-video</pre> |

|                                                                                               |                                                                                         |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\IKNJ\san-xavier[1].htm</b> |                                                                                         |
| Process:                                                                                      | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                   |
| File Type:                                                                                    | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators |
| Category:                                                                                     | dropped                                                                                 |
| Size (bytes):                                                                                 | 47433                                                                                   |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\san-xavier[1].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entropy (8bit): | 5.364638341775209                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 768:a+vHVjuUs+eE+eldq+ei+eqLkSq4NnfC6lEIEgdzNfMyAukOmSSaM7u/BajVd6uh:VHVjuD+eE+elk+ei+eAxlREgdzJvoOmb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5:            | D5B0AE46D16CA704E1CA3EF0AC12825D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | 15CE1164157D96639EDCF8476EF864D48E76887F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:        | 089A78FAF390C451E0D4C55704B98FB9421FA9F6377A138A8016D1C2E5B46A56                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | 17EB27D25DA52A656B6169890F6B0B15268B78672C007BD3506661B26B75D3078E1ACA58CB2BD3C4F29038DD2DB000E888BAC6C91CF176056397DD4489D62FB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:        | <!DOCTYPE html>.<html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_103 av-no-preview ">.<head>.<meta charset="UTF-8" />... mobile setting -->.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">.. Scripts/CSS and wp_head hook -->... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ -->..<title>San Xavier - TON-HC</title>..<meta name="robots" content="index, follow" />..<meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" />..<meta name="bingbot" content="index, follow, max-snippet:-1, max-image-preview:large, max-vide |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\sant-rosa[1].htm

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Size (bytes):   | 47382                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 5.3602722385406505                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 768:6AZHVauUD+eE+el0q+ei+eqLPb8OuVRk4AcglESEgdzNfMyAukOmSSaM7u/BajVf:JHVau4+eE+eL+ei+eQzIVIEgdzJvoOmh                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5:            | BF432FBB87891584D7697E5D87F2342F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | FA81954A5B398F692ADB7DB75B399B225993230                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:        | 34F1745762F980953AD4B4EE12051A2E765F72B6E8DFB4A7775D044303F842EB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | A5BD87A87F3CACE35272540750F5B748370C98BA6488EAB2B52306121FDBAC581F7C867B7700F2710B4363971D334593D03582438738A57810980367EDF5B0C7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:        | <!DOCTYPE html>.<html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_221 av-no-preview ">.<head>.<meta charset="UTF-8" />... mobile setting -->.<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">.. Scripts/CSS and wp_head hook -->... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ -->..<title>Santa Rosa - TON-HC</title>..<meta name="robots" content="index, follow" />..<meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" />..<meta name="bingbot" content="index, follow, max-snippet:-1, max-image-preview:large, max-vide |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\sdk[1].js

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 3224                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Entropy (8bit): | 5.608939230407891                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SSDEEP:         | 48:SLA+y/clUyAQHWs5+TaoROFzyHOgeEh7z5jFqxv4tx5YHlekZ462X+wNjyoDuExo:IA+5AQHARay48f5JJYHlh4PJN+oDu9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:            | 9D743430D831FF90A09728221BCA338D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA1:           | 7A1C4BFDABE4FDFB07A91A05F8986077B6235BBF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-256:        | EDDA4C222D6186F7EE05F36FA7D195D0F91D631152E37EFD75A27952A1015C82                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-512:        | 2A12934AE914C880407297AFB2D50D94F3D1FDE05278A894F873CD01DA86A6626CEEE55A7C7A63FCC1BD76E811844EDB1DDDD760836FF0FDF6391CF957CF2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preview:        | /*1622834962,,JIT Construction: v1003908653,en_US*/./**. * Copyright (c) 2017-present, Facebook, Inc. All rights reserved.. * * You are hereby granted a non-exclusive, worldwide, royalty-free license to use,. * copy, modify, and distribute this software in source code or binary form for use. * in connection with the web services and APIs provided by Facebook.. * * As with any software that integrates with the Facebook platform, your use of. * this software is subject to the Facebook Platform Policy. * [http://developers.facebook.com/policy/]. This copyright notice shall be. * included in all copies or substantial portions of the software.. * * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR. * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS. * FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR. * COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER. * IN AN ACTION OF CO |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\sells-hospital[1].htm

|                 |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                   |
| File Type:      | HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators |
| Category:       | dropped                                                                                 |
| Size (bytes):   | 47908                                                                                   |
| Entropy (8bit): | 5.359594634931315                                                                       |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\sells-hospital[1].htm

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encrypted:  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:     | 768:metHVwuUL+eE+eIUq+ei+eqLPp8OkL7hYI+HE2EgdzNfMyAukOmSSaM7u/BajVdV:/HVwuk+eE+eIr+ei+eZrTEgdzJvoOm9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:        | 3B022A6C60D64DA61E79BF11273274F5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:       | 61F1255A822F16883D42916E7149EDF6D1BA9A70                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:    | 504C1E46CA0BE0741C576A1D4A7154AF2A7F5AF69EB5573D7D2B5DC81D7FB9C5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:    | 441019B03069336D89FFC594819CBAA57275E60A7A31BFB3DC7A7D3F5433191579CD1A3E027E51AD29F908D6E4DA35F3EF46D9BC95731FC80594CD94573B8C2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reputation: | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:    | <!DOCTYPE html>.<html lang="en-US" class="html_stretched responsive av-preloader-disabled av-default-lightbox html_header_top html_logo_left html_main_nav_head er html_menu_right html_custom html_header_sticky html_header_shrinking html_mobile_menu_phone html_disabled html_header_searchicon html_content_align_center html_header_unstick_top_disabled html_header_stretch_disabled html_entry_id_203 av-no-preview ">.<head>.<meta charset="UTF-8" />... mobile setting -->.<meta nam e="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">.. Scripts/CSS and wp_head hook -->... This site is optimized with the Yoast SEO plugin v14.3 - https://yoast.com/wordpress/plugins/seo/ -->..<title>Sells Hospital - TON-HC</title>..<meta name="robots" content="index, follow" />..<meta name="googlebot" content="index, follow, max-snippet:-1, max-image-preview:large, max-video-preview:-1" />..<meta name="bingbot" content="index, follow, max-snippet:-1, max-image-preview:large, max- |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\style.min[1].css

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:      | ASCII text, with very long lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Size (bytes):   | 53907                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit): | 4.940786840491388                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:         | 384:F5tku7HBZDO/KRUEqXMXRLrO+AwlVHI+vg7LKclyvNSX2GVX5Ttfr:0RXMXRLrO+Awlxl+vg7LKNcF5Bfr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5:            | 2E7E1D1C1D4D446A1B6B63295757D859                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:           | 27A1D9DCBDC4AFF486016B5C9F3ECE6AD0C028C1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:        | 8C626F0F9B5C109539B256B73E72C02B300A184F46B4535C2EB86599215C78AF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:        | 7526B0ADCE5C1751D3E55BA5077C4BB5F334FAE6A73CB519E2BE07AA602ED25C307A8462AF380DA0550F56AE29C871A663F9A01E523462DFB9A378E8F26888A3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IE Cache URL:   | http://www.tonhc.org/wp-includes/css/dist/block-library/style.min.css?ver=5.5.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | :root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-20:#005a87}#start-resizable-editor-section{display:n one}.wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em}.wp-block-audio audio{width:100%;min-width:300px}.wp-block-button__link{color:#fff;background-c olor:#32373c;border:none;border-radius:28px;box-shadow:none;cursor:pointer;display:inline-block;font-size:18px;padding:12px 24px;text-align:center;text-decorati on:none;overflow-wrap:break-word}.wp-block-button__link:active,.wp-block-button__link:focus,.wp-block-button__link:hover,.wp-block-button__link:visited{color:#fff}.wp-blo ck-button__link.aligncenter{text-align:center}.wp-block-button__link.alignright{text-align:right}.wp-block-button.is-style-squared,.wp-block-button__link.wp-block-button.is-style-squared{border-radius:0}.wp-block-button.no-border-radius,.wp-block-button__link.no-border-radius{border-radius:0!important}.is-style-outline .wp-block-button__l ink,.wp-bl |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\tonhc-patient-photo[1].jpg

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Type:      | [TIFF image data, little-endian, direntries=0], progressive, precision 8, 1500x817, frames 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Size (bytes):   | 248445                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Entropy (8bit): | 7.989720071816527                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:         | 6144:+jU/Io7Qtrl0yqldwffSkGWlmqYYT3Nlx:/l1QtriyhwfkmbYYxIx                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:            | CA74F58265E22041EC9D2D4B2A642530                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:           | 4C9077E9B360BE7FAC4536C4FD12D7AF4E4E562E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:        | 9F34DBC36D4E54603DB87C2758E684C1037DAADC9A2E520A361027592853077A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:        | DF16009389B6B00C1EB5DD9C20659F4D65D581E14FCBA82EFA38436BA4B72A9DA5CECE18254558560B6D4EB3B0E4A4010CAE0F60538C474D487B316692E859E4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Reputation:     | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IE Cache URL:   | http://https://i2.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-patient-photo.jpg?fit=1500%2C817                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Preview:        | .....JFIF.....Exif..IIf*.....HPhotoshop 3.0.8BIM.....Z...%G.....8BIM.%.....x/4b4.Xw...C.....C.....<br>.....1.....^(.5.w.-.Vq.s...IZD.1.....P1.S:...A.R...@!l..R.IT"\$DD..a...H..F.....T.C.2C..1.@<br>c...).r....B...b.....t.c...B...*.&.:l%.;&W...lbf.z.2%.....s.kd..v..l.D...C4...W.N.L\$.L.*t...@....1+D:CR@.T..R.*....P.B.%B.F.".5.1.Q..D...Q"!...DB\$2P.1`1`1....0.0..%tC..b..<br>E.XV.g...U.Z...l.Kyx9...5.l.....[.q]..x.....93...\$p.tH.."D.VL...T.P1.....)U..B.@!.....DEH.D!.#J..bDDDDQ...!Tbc.t.c.t.8...@.t@.C...7.i.YaZ...2X.DaR*..Z...BZ.....<br>..>.....K(y..5.p.t\$.....Z....4.2.\$...K...h.....V0.U\$d.D.C.\$:).l..J""..B.@.T!.Q.Di...).Dj1..H.""(DH....H.H..Z.t.....0 |

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\tonhc-sanxavier-location[1].jpg

|            |                                                                                                                                 |
|------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:   | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                           |
| File Type: | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1500x630, frames 3 |
| Category:  | downloaded                                                                                                                      |

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\tonhc-sanxavier-location[1].jpg |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Size (bytes):                                                                                       | 147466                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Entropy (8bit):                                                                                     | 7.9887140236913545                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:                                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SSDEEP:                                                                                             | 3072:taZBXB9pal0TdyDBKK0+vSCQjL6TKM2KWVKE8Tpw4tCoUUz1U3L:+BzeTEb0+vJQjOTKKWiECJtClol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| MD5:                                                                                                | 84DCC0BB8ED5D0CAE3F70403FC35A090                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA1:                                                                                               | 38F76A64229575A62894CB15E2C554ABA286DB6C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-256:                                                                                            | F6246FD3966B2ECF46887D04DA36454BF9A034F9E30F7EC9BDF9676BBA90B89E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-512:                                                                                            | 166EC69E48BD243404F8216D243538CEB222FED5AF2FF271CB4CCE186A0836F4EC76B4BD47E3FE98A0372E35AED1FE02BBF5AF98D0433312D2CF0988E6003AC1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:                                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Reputation:                                                                                         | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| IE Cache URL:                                                                                       | http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-sanxavier-location.jpg?resize=1500%2C630                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:                                                                                            | .....JFIF.....C.....".....C.....V.....".....0CB<br>m`...I`...`.(b.i@i.....F`.....H..u.\$!.....De!...L.O....5.#...b.e..6.1A..D4.E.\$H".D0CP)!T0@..CT.!(D...a.{d.3...R.=.5.F...._t;....4.<.x.Zx{o.d...aR]p.....-RDd3\$.x.....u.o <br>...a....^Z.....?.. t0M.b.hD.*HM..".E.C.0C.I.m.\$I.H.e!..%!.1..."ID.)\$.I.n.2..Ql...I.`-...T.\$....`...!..!L,C%@Rc.#-CR.IE\$.d.a.j.. "0JA...C.'j]3....-Yy..d...v..!..W.K.....}m..S<br>.....v..V/F...4.@4..L...../_v.>n.j..}?.;.....; ?A..`RB"A.\$..... 4...C@.@.2,bL.\$&....#.....#.....P...&a.ED.Dmb.\$!.....R...0.dD.....B!..P..eE.JA. @.-.L!.2..C*#!).I0.....ix.5.W<br>.....C[.IA....bV....e....n8u.5..j..%....t\...jY..y.....A.B)...6a.e}.8..{~w...rx.C...>..>b!.!.....dX.l..0.a...!#.0CdT...#H"H"2. |

|                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9026\KNJ\tonhc-staff-photo[1].jpg |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Process:                                                                                     | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:                                                                                   | JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1500x630, frames 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Category:                                                                                    | downloaded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Size (bytes):                                                                                | 192777                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit):                                                                              | 7.990509634281373                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:                                                                                   | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                      | 3072:i5xFX6tzlfaGW71ivkK9WqybJgwAnl3BIE7zW2CxmADwpr1KzgzqMCVLvFDXv15F:WxwtzUZW7+dybSwyIMPNuzTtHCNtICu/                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:                                                                                         | A33457848729F12EBA7FB0AF2924B568                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:                                                                                        | 35E5EFD7CED32699E6D1B6514252B77596A39725                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:                                                                                     | E76D5F55279C0ED9E6E553DD3C938EC479D51CF4CADA64FA3F6A48280B90BD63                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:                                                                                     | 129EEEA044BD815038962D3B168CC626F7D6112537E1C2F5BBCA0A71F51FB595BD0E5B22B82B0576078BEA48BD0A5558BB829701EE8B9DFC4F01D8334B88C4C6C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Malicious:                                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:                                                                                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IE Cache URL:                                                                                | http://https://i1.wp.com/www.tonhc.org/wp-content/uploads/2017/09/tonhc-staff-photo.jpg?resize=1500%2C630                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Preview:                                                                                     | .....JFIF.....C.....".....C.....V.....".....b..HR.]}*.<br>.I.....DT..@o.. .#u.1.{...<bc4lb<A....)}!..-p.#jd.c]e..K.../d.'...v...K*'#M.=ms.}....m.8..4T)r.....s.GUkT.6.!!...J8d.e+....y.G+c.u..h...%...../.....<M#.T9.9..!.....& .].F<br>G.8.E.....f...4....A...B....i.._..h.H...&....1`....P....L.P.-....]...h.D..%F.C.6.8.N...XbzM.2c"K....IK.V.d<....*. j!!m.....p.p.;.&)...(B{.6..k..h.....f.1..Y.f..Lm...-.K.Q;...v{EA..H.Lz.<br>i...w]XS....U.c.-.o}.0..Mq.0...?rus8Bm).....'1...o.PUZ....D...(.I( Wz.)...s.0....zd.....?aN.O...<...Ki.d.mSpG.5...;..sT!..K..>m..o....@0.A..d()('.....P.....!mylq.....0...* [pD<br>b.*)/.Q....V..*..um..J*..4..p]h.nZ(...Y3";O..S.%S....,IV..U.+f\$-sf..0wl.O.C.@4HD...@\$t!O...9..})...../..%)* |

## Static File Info

No static file info

## Network Behavior

### Network Port Distribution

Total Packets: 100

- 53 (DNS)
- 80 (HTTP)



## TCP Packets

| Timestamp                           | Source Port | Dest Port | Source IP   | Dest IP     |
|-------------------------------------|-------------|-----------|-------------|-------------|
| Jun 4, 2021 21:35:03.447963953 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:03.448036909 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:03.633620024 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:03.633804083 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:03.633934975 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:03.633990049 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:03.635761976 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:03.821471930 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.110780001 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.110807896 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.110872984 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.110909939 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111067057 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111129045 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111188889 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111238956 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111351967 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111402035 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111438990 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111486912 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111578941 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111625910 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111664057 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111711025 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111736059 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111779928 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.111860991 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.111907005 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.180651903 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.181721926 CEST | 49737       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.182498932 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.183546066 CEST | 49739       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.184804916 CEST | 49740       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.294794083 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.294902086 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.295178890 CEST | 80          | 49735     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.295234919 CEST | 49735       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.364255905 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.366235971 CEST | 80          | 49737     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.366342068 CEST | 49737       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.367932081 CEST | 80          | 49739     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.368014097 CEST | 49739       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.368954897 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369003057 CEST | 80          | 49740     | 64.25.66.82 | 192.168.2.4 |

| Timestamp                           | Source Port | Dest Port | Source IP   | Dest IP     |
|-------------------------------------|-------------|-----------|-------------|-------------|
| Jun 4, 2021 21:35:04.369019032 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369023085 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369066000 CEST | 49740       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369077921 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369085073 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369117975 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369160891 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369199038 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369342089 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369358063 CEST | 80          | 49736     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.369384050 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.369404078 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.370754957 CEST | 49737       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.390271902 CEST | 49740       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.390578985 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.390867949 CEST | 49736       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.391630888 CEST | 49739       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.426549911 CEST | 49744       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.437903881 CEST | 49743       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.468148947 CEST | 443         | 49744     | 192.0.77.2  | 192.168.2.4 |
| Jun 4, 2021 21:35:04.468250990 CEST | 49744       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.475478888 CEST | 49745       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.477334023 CEST | 49746       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.479765892 CEST | 443         | 49743     | 192.0.77.2  | 192.168.2.4 |
| Jun 4, 2021 21:35:04.479849100 CEST | 49743       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.517313004 CEST | 443         | 49745     | 192.0.77.2  | 192.168.2.4 |
| Jun 4, 2021 21:35:04.517420053 CEST | 49745       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.518970966 CEST | 443         | 49746     | 192.0.77.2  | 192.168.2.4 |
| Jun 4, 2021 21:35:04.519054890 CEST | 49746       | 443       | 192.168.2.4 | 192.0.77.2  |
| Jun 4, 2021 21:35:04.554171085 CEST | 80          | 49737     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.557161093 CEST | 80          | 49737     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.557295084 CEST | 49737       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.573534966 CEST | 80          | 49740     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.573566914 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.575679064 CEST | 80          | 49740     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.575752020 CEST | 80          | 49740     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.575825930 CEST | 49740       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577243090 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577326059 CEST | 49740       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577353001 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577410936 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577450991 CEST | 80          | 49739     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577476025 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577665091 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577723980 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577800989 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577858925 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.577935934 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.577997923 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.578061104 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.578089952 CEST | 80          | 49738     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.578125954 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.578141928 CEST | 49738       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.578500986 CEST | 80          | 49739     | 64.25.66.82 | 192.168.2.4 |
| Jun 4, 2021 21:35:04.578564882 CEST | 49739       | 80        | 192.168.2.4 | 64.25.66.82 |
| Jun 4, 2021 21:35:04.578680038 CEST | 80          | 49739     | 64.25.66.82 | 192.168.2.4 |

## UDP Packets

| Timestamp                           | Source Port | Dest Port | Source IP   | Dest IP     |
|-------------------------------------|-------------|-----------|-------------|-------------|
| Jun 4, 2021 21:34:55.408909082 CEST | 53097       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:55.451004028 CEST | 53          | 53097     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:34:56.715245008 CEST | 49257       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:56.757534027 CEST | 53          | 49257     | 8.8.8.8     | 192.168.2.4 |

| Timestamp                           | Source Port | Dest Port | Source IP   | Dest IP     |
|-------------------------------------|-------------|-----------|-------------|-------------|
| Jun 4, 2021 21:34:57.108453989 CEST | 62389       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:57.153328896 CEST | 53          | 62389     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:34:57.481251001 CEST | 49910       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:57.523855925 CEST | 53          | 49910     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:34:58.592163086 CEST | 55854       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:58.635709047 CEST | 53          | 55854     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:34:59.708915949 CEST | 64549       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:34:59.752119064 CEST | 53          | 64549     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:00.668858051 CEST | 63153       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:00.712069988 CEST | 53          | 63153     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:02.109211922 CEST | 52991       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:02.153420925 CEST | 53          | 52991     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:02.393438101 CEST | 53700       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:02.435462952 CEST | 53          | 53700     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:03.344840050 CEST | 51726       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:03.383270979 CEST | 56794       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:03.425668001 CEST | 53          | 56794     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:03.435532093 CEST | 53          | 51726     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:04.241322041 CEST | 56534       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:04.284513950 CEST | 53          | 56534     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:04.377651930 CEST | 56627       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:04.408720016 CEST | 56621       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:04.419912100 CEST | 53          | 56627     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:04.450781107 CEST | 53          | 56621     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:05.330096960 CEST | 63116       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:05.372107983 CEST | 53          | 63116     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:05.661222935 CEST | 64078       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:05.703010082 CEST | 53          | 64078     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:05.732160091 CEST | 64801       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:05.774377108 CEST | 53          | 64801     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:06.212768078 CEST | 61721       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:06.261270046 CEST | 53          | 61721     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:06.688049078 CEST | 51255       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:06.729989052 CEST | 53          | 51255     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:06.737818003 CEST | 61522       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:07.738056898 CEST | 61522       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:07.767791033 CEST | 52337       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:07.780293941 CEST | 53          | 61522     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:07.809990883 CEST | 53          | 52337     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:08.227566957 CEST | 55046       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:08.272543907 CEST | 53          | 55046     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:10.381120920 CEST | 49612       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:10.391675949 CEST | 49285       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:10.426181078 CEST | 53          | 49612     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:10.435765028 CEST | 53          | 49285     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:10.505065918 CEST | 50601       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:10.549053907 CEST | 53          | 50601     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:10.727109909 CEST | 60875       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:10.771599054 CEST | 53          | 60875     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:12.522723913 CEST | 56448       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:12.564641953 CEST | 53          | 56448     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:13.440354109 CEST | 59172       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:13.482742071 CEST | 53          | 59172     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:18.236584902 CEST | 62420       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:18.278539896 CEST | 53          | 62420     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:21.117503881 CEST | 60579       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:21.159674883 CEST | 53          | 60579     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:23.163810015 CEST | 50183       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:23.206687927 CEST | 53          | 50183     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:24.994079113 CEST | 61531       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:25.037815094 CEST | 53          | 61531     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:26.032618046 CEST | 49228       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:26.076862097 CEST | 53          | 49228     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:26.666762114 CEST | 59794       | 53        | 192.168.2.4 | 8.8.8.8     |

| Timestamp                           | Source Port | Dest Port | Source IP   | Dest IP     |
|-------------------------------------|-------------|-----------|-------------|-------------|
| Jun 4, 2021 21:35:26.723215103 CEST | 53          | 59794     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:26.975179911 CEST | 55916       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:27.017407894 CEST | 53          | 55916     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:32.150345087 CEST | 52752       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:32.193967104 CEST | 53          | 52752     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:32.823801041 CEST | 60542       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:32.866400003 CEST | 53          | 60542     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:33.734107018 CEST | 52752       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:33.777146101 CEST | 53          | 52752     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:33.831665993 CEST | 60542       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:33.873959064 CEST | 53          | 60542     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:34.725321054 CEST | 52752       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:34.767482996 CEST | 53          | 52752     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:34.831527948 CEST | 60542       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:34.881439924 CEST | 53          | 60542     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:36.723413944 CEST | 52752       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:36.765645027 CEST | 53          | 52752     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:36.832159996 CEST | 60542       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:36.875395060 CEST | 53          | 60542     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:39.474136114 CEST | 60689       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:39.516129971 CEST | 53          | 60689     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:40.780369043 CEST | 52752       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:40.822482109 CEST | 53          | 52752     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:40.866729975 CEST | 60542       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:40.910332918 CEST | 53          | 60542     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:35:49.794117928 CEST | 64206       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:35:49.837310076 CEST | 53          | 64206     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:36:06.468359947 CEST | 50904       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:36:06.526874065 CEST | 53          | 50904     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:36:19.916460037 CEST | 57525       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:36:19.961296082 CEST | 53          | 57525     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:36:28.085572958 CEST | 53814       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:36:28.225306988 CEST | 53          | 53814     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:36:28.633610010 CEST | 53418       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:36:28.741719961 CEST | 53          | 53418     | 8.8.8.8     | 192.168.2.4 |
| Jun 4, 2021 21:36:29.549509048 CEST | 62833       | 53        | 192.168.2.4 | 8.8.8.8     |
| Jun 4, 2021 21:36:29.689325094 CEST | 53          | 62833     | 8.8.8.8     | 192.168.2.4 |

## DNS Queries

| Timestamp                           | Source IP   | Dest IP | Trans ID | OP Code            | Name                           | Type           | Class       |
|-------------------------------------|-------------|---------|----------|--------------------|--------------------------------|----------------|-------------|
| Jun 4, 2021 21:35:03.344840050 CEST | 192.168.2.4 | 8.8.8.8 | 0x21b3   | Standard query (0) | www.tonhc.org                  | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:04.377651930 CEST | 192.168.2.4 | 8.8.8.8 | 0x1e1a   | Standard query (0) | i2.wp.com                      | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:04.408720016 CEST | 192.168.2.4 | 8.8.8.8 | 0xe91d   | Standard query (0) | i0.wp.com                      | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:05.330096960 CEST | 192.168.2.4 | 8.8.8.8 | 0x5c2b   | Standard query (0) | stats.wp.com                   | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:06.212768078 CEST | 192.168.2.4 | 8.8.8.8 | 0x5642   | Standard query (0) | connect.facebook.net           | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:06.737818003 CEST | 192.168.2.4 | 8.8.8.8 | 0x9506   | Standard query (0) | www.facebook.com               | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:07.738056898 CEST | 192.168.2.4 | 8.8.8.8 | 0x9506   | Standard query (0) | www.facebook.com               | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:07.767791033 CEST | 192.168.2.4 | 8.8.8.8 | 0xc4e7   | Standard query (0) | pixel.wp.com                   | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:08.227566957 CEST | 192.168.2.4 | 8.8.8.8 | 0x6c88   | Standard query (0) | scontent.fhel6-1.fna.fbcdn.net | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:10.381120920 CEST | 192.168.2.4 | 8.8.8.8 | 0x3a90   | Standard query (0) | scontent-frt3-1.xx.fbcdn.net   | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:10.391675949 CEST | 192.168.2.4 | 8.8.8.8 | 0xc90f   | Standard query (0) | scontent-frx5-1.xx.fbcdn.net   | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:10.505065918 CEST | 192.168.2.4 | 8.8.8.8 | 0x55db   | Standard query (0) | scontent-frt3-2.xx.fbcdn.net   | A (IP address) | IN (0x0001) |
| Jun 4, 2021 21:35:10.727109909 CEST | 192.168.2.4 | 8.8.8.8 | 0x41cf   | Standard query (0) | scontent.xx.fbcdn.net          | A (IP address) | IN (0x0001) |

| Timestamp                           | Source IP   | Dest IP | Trans ID | OP Code            | Name      | Type           | Class       |
|-------------------------------------|-------------|---------|----------|--------------------|-----------|----------------|-------------|
| Jun 4, 2021 21:35:39.474136114 CEST | 192.168.2.4 | 8.8.8.8 | 0x9e04   | Standard query (0) | i1.wp.com | A (IP address) | IN (0x0001) |

DNS Answers

| Timestamp                           | Source IP | Dest IP     | Trans ID | Reply Code   | Name                           | CName                       | Address        | Type                   | Class       |
|-------------------------------------|-----------|-------------|----------|--------------|--------------------------------|-----------------------------|----------------|------------------------|-------------|
| Jun 4, 2021 21:35:03.435532093 CEST | 8.8.8.8   | 192.168.2.4 | 0x21b3   | No error (0) | www.tonhc.org                  | tonhc.org                   |                | CNAME (Canonical name) | IN (0x0001) |
| Jun 4, 2021 21:35:03.435532093 CEST | 8.8.8.8   | 192.168.2.4 | 0x21b3   | No error (0) | tonhc.org                      |                             | 64.25.66.82    | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:04.419912100 CEST | 8.8.8.8   | 192.168.2.4 | 0x1e1a   | No error (0) | i2.wp.com                      |                             | 192.0.77.2     | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:04.450781107 CEST | 8.8.8.8   | 192.168.2.4 | 0xe91d   | No error (0) | i0.wp.com                      |                             | 192.0.77.2     | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:05.372107983 CEST | 8.8.8.8   | 192.168.2.4 | 0x5c2b   | No error (0) | stats.wp.com                   |                             | 192.0.76.3     | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:06.261270046 CEST | 8.8.8.8   | 192.168.2.4 | 0x5642   | No error (0) | connect.facebook.net           | scontent.xx.fbcdn.net       |                | CNAME (Canonical name) | IN (0x0001) |
| Jun 4, 2021 21:35:06.261270046 CEST | 8.8.8.8   | 192.168.2.4 | 0x5642   | No error (0) | scontent.xx.fbcdn.net          |                             | 31.13.92.14    | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:07.780293941 CEST | 8.8.8.8   | 192.168.2.4 | 0x9506   | No error (0) | www.facebook.com               | star-mini.c10r.facebook.com |                | CNAME (Canonical name) | IN (0x0001) |
| Jun 4, 2021 21:35:07.780293941 CEST | 8.8.8.8   | 192.168.2.4 | 0x9506   | No error (0) | star-mini.c10r.facebook.com    |                             | 157.240.9.35   | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:07.809990883 CEST | 8.8.8.8   | 192.168.2.4 | 0xc4e7   | No error (0) | pixel.wp.com                   |                             | 192.0.76.3     | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:08.272543907 CEST | 8.8.8.8   | 192.168.2.4 | 0x6c88   | No error (0) | scontent.fhel6-1.fna.fbcdn.net |                             | 212.188.75.209 | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:10.426181078 CEST | 8.8.8.8   | 192.168.2.4 | 0x3a90   | No error (0) | scontent-frt3-1.xx.fbcdn.net   |                             | 31.13.92.14    | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:10.435765028 CEST | 8.8.8.8   | 192.168.2.4 | 0xc90f   | No error (0) | scontent-frx5-1.xx.fbcdn.net   |                             | 185.60.216.19  | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:10.549053907 CEST | 8.8.8.8   | 192.168.2.4 | 0x55db   | No error (0) | scontent-frt3-2.xx.fbcdn.net   |                             | 157.240.20.19  | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:10.771599054 CEST | 8.8.8.8   | 192.168.2.4 | 0x41cf   | No error (0) | scontent.xx.fbcdn.net          |                             | 31.13.92.14    | A (IP address)         | IN (0x0001) |
| Jun 4, 2021 21:35:39.516129971 CEST | 8.8.8.8   | 192.168.2.4 | 0x9e04   | No error (0) | i1.wp.com                      |                             | 192.0.77.2     | A (IP address)         | IN (0x0001) |

HTTP Request Dependency Graph

|                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>www.tonhc.org             <ul style="list-style-type: none"> <li>connect.facebook.net</li> <li>pixel.wp.com</li> </ul> </li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

HTTP Packets

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 0          | 192.168.2.4 | 49735       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|-----------|--------------------|-----------|------|
|-----------|--------------------|-----------|------|

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:03.635761976 CEST | 1095               | OUT       | GET /coronavirus/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Jun 4, 2021<br>21:35:04.110780001 CEST | 1107               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:03 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Set-Cookie: PHPSESSID=a5ulen80fecc1vdmhk7ti8kb4; path=/<br>Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>Cache-Control: no-store, no-cache, must-revalidate<br>Pragma: no-cache<br>Link: <http://www.tonhc.org/wp-json/>; rel="https://api.w.org/"<br>Link: <http://www.tonhc.org/wp-json/wp/v2/pages/1055>; rel="alternate"; type="application/json"<br>Link: <https://wp.me/P9uvL4-h1>; rel=shortlink<br>X-TEC-API-VERSION: v1<br>X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br>X-TEC-API-ORIGIN: http://www.tonhc.org<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 14977<br>Keep-Alive: timeout=5, max=100<br>Connection: Keep-Alive<br>Content-Type: text/html; charset=UTF-8<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d db 72 1b 39 b2 e0 b3 15 31 ff 00 d3 d1 a6 74 9a 55 ac 22 45 5d 28 8b 1e b5 6c 1f 7b 8e 2f 3a 96 3c 7d 66 4d 07 03 64 81 64 49 c5 aa ea ba 88 62 ab 15 31 11 e7 13 76 5f 36 62 37 62 ce 46 ec 2f ec d3 ee cf cc 07 cc 37 6c 66 02 75 23 29 8a 92 28 db 73 62 fa 22 a2 80 44 22 01 24 12 89 04 90 78 f6 f8 c5 87 c3 93 3f 1d bd 64 c3 68 e4 b4 d6 9e e1 0f 73 b8 3b d8 2f 09 57 fb 74 5c 62 3d 87 87 e1 7e 09 13 3a 61 14 88 a8 37 14 16 0b 44 e8 7b 6e 68 9f 0b c6 cf 35 3f 10 8e c7 2d 11 68 96 1d f2 ae 03 00 10 6b 89 3e 8f 9d 48 73 ec c1 30 ea 7a 17 8c 0a e9 0c 05 42 76 22 cf 97 df 8e 37 f0 3a 8e e8 47 f2 73 c4 6d b7 e3 f2 73 05 a7 22 85 1b 77 02 c4 23 bf 7b 71 18 79 a3 02 be 30 b2 7b 67 93 62 d4 30 b0 dd 33 db 1d 28 24 5e d7 76 84 c4 e5 0f 3d 57 c8 e8 94 e4 42 56 c1 83 de d0 ee 79 ae 2a d0 73 23 e1 46 1d 0e 95 71 3b 3d 08 26 a4 a9 0c b1 4b 04 60 b5 ae c1 28 db 6e 2a 11 10 05 93 8e 6d 75 4c a3 d1 c0 46 73 3d 6c cd 73 5b 8c 59 09 fb 03 32 c3 cf 48 44 9c f5 86 3c 08 45 b4 5f fa 74 f2 4a db 29 b1 6a 6b 6d 6d ed d9 63 4d 63 b2 66 0c 12 23 ac ad a6 25 59 5c 3e 12 fb 25 c4 e6 7b 41 04 9d 29 ab b1 5f 1a db 56 34 dc b7 a0 a0 9e d0 e8 a3 c2 6c d7 8e 6c ee 68 61 8f 3b 62 df ac b0 11 bf b0 47 f1 28 89 00 7a 64 71 c7 bd c0 f6 a3 b0 7a 78 7c cc b8 6b b1 b1 4f 95 64 43 cf 3b a3 c2 d7 1e 11 dc c9 d0 0e 59 68 47 82 c1 af e7 47 f6 c8 fe 15 2a 3e b6 a3 21 8b 86 82 fd c9 e3 61 c4 8e 5f 7e 60 be 13 0f 6c 97 9d 9b 9b 7a 9d 69 d0 34 91 1f 36 ab d5 09 02 e8 3d 6f 54 1d 7b 81 05 ed 12 86 55 09 1a 56 43 e1 55 a9 b0 47 cf 22 3b 72 44 eb d0 0b 3c e0 1b 3b 88 43 40 71 f2 e1 bd f6 fa f0 59 55 a6 01 50 ae 3d 02 af eb 45 61 ae 35 6c d7 12 17 15 d6 f7 1c c7 1b 53 c3 16 e0 07 9e 37 70 04 e4 b9 2e 0b 35 95 16 ba b6 ef 8b a8 a9<br>Data Ascii: }r91tU"E](k{/<}fMddlb1v_6b7bF/7lfu#)(sb"D"\$x?dhs;Wt/bb=:a7D{nh5?-hk>Hs0zBv"7:Gsms"w#{qy0{qb03(\$^v=WBVy*s#Fq;=&K'(n*muLFs=ls[Y2HD<E_tJ)jkmMcMcf#%Y\>%(A)_V4llha;bG(zdqzx kOdC;YhGG*>la_~lzi46=oT{UVCUG";rD<;C@qYUP=Ea5IS7p.5 |
| Jun 4, 2021<br>21:35:05.201380968 CEST | 1283               | OUT       | GET /wp-content/themes/enfold/config-events-calendar/event-mod.css?ver=5.5.5 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80fecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.391221046 CEST | 1297               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:44:32 GMT<br>ETag: "467f-55c7790196400-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 4007<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 b5 5c 79 6f dc 36 16 ff bb f3 29 b8 0e 8c 26 a9 25 6b 2e db 99 41 8b 4d 5b 77 11 20 e8 2e 92 6c 8b 45 51 14 9a 11 3d e2 46 17 74 8c ed 08 de cf be 8f 97 44 52 94 2c b9 6e 5b 17 d6 c1 c7 c7 1f 1f df 2d 9f bf fe a1 2a ca 34 46 9f 70 9c 45 7e 89 d1 f7 15 89 02 9c a3 eb 08 c7 38 29 8b d7 e7 b3 99 eb 1f 9d 2a db a7 31 49 0e 0e 3e d2 db f5 83 e5 ae 03 3f f9 7d bd 8f b0 9f 6f d0 2e 2d c3 2d ca fc 20 80 17 36 1e f2 d0 62 9d dd 21 6f 8b d2 23 ce 6f a2 f4 76 83 42 12 04 38 d9 a2 80 14 30 fd fd 66 17 a5 fb cf db 7e da 9b 90 8e ad 4b 7c 57 3a 01 de a7 b9 5f 92 34 d9 a0 24 4d f0 16 ed d3 28 85 89 49 12 e2 9c 94 43 64 22 bf 28 9d 7d 08 4b 45 b5 e0 d0 01 7e 01 89 0d 30 68 1d 48 62 ff 80 eb 5d 9a 03 3a 4e ee 07 a4 2a 36 68 e5 79 d9 dd 16 dd 92 a0 0c 37 17 ec 77 58 98 5f 6e 22 7c 53 6e 51 ec e7 07 02 ec c1 d2 3d ba 74 ba 78 2b f1 c0 2f fd da 40 c1 02 93 75 6c 8c 2d 63 b3 b4 20 1c 9a 1c c3 be 92 23 c0 53 a6 d9 c6 99 33 1e 53 18 57 90 2f 78 83 e6 0b b8 61 a5 5b ec 43 1c 54 11 ae 1f df 9c 02 b9 99 0f 2b 65 bb c1 19 92 83 d8 ce 3c cc e0 9f f3 d7 9f 3e bc fb fe 1a fd f0 f6 fd f5 cf 3f be fd 00 92 f5 02 58 42 2f ca 9c ec b0 20 e4 64 07 a7 14 b2 58 03 7e 77 0e c7 16 cd 3d ef 54 91 26 20 39 3c 18 b9 da 93 24 2d c9 1e 17 62 ff 38 57 48 df 4c af 25 3f 5f 51 94 98 94 f9 11 39 00 8a 7b a0 82 73 1d b9 75 03 e5 2d 26 87 b0 04 aa 79 ec 47 62 60 11 fa 01 dd bb 06 80 f3 d7 02 ab 9d 9f b3 b5 ab fc c1 bd 9a 4b 8b c3 b6 69 cd 64 c9 b6 8b 82 69 2e ad 4e 51 de 47 c0 4b 91 46 24 30 9f 71 e4 e6 76 a1 6c c4 7d b5 66 02 d0 61 47 42 0b bf 3a 37 b0 30 c1 1e 85 49 a1 06 0b eb 8c dc ec 30 0c c0 67 a8 fb c4 bf 01 14 eb d9 1e 40 83 7b 1b 74 e2 9e 6c 67 ed 2a fd 1d 2c a4 2a f1 76 16 72 44 d9 ae cf 84 42 16 1e 3b 6c 33 3a ef c6 91 57 0c 6b 92 04 8c 1c 87 6d d6 39 38 b3 a7 80 36 b3 ae 4d ac 80 31 c1 b9 6b 5f 6b a0 da f9 fb cf 87 3c ad 92 60 83 ca dc 4f 8a cc cf 81 c2 16 7d 61 ac de 51 71 b6 4b 30 05 9e 24 59 55 52 f4 ac 4f 0b 1c e1 7d d9 ee c6 83 39 3b 1f ff 5b 79 9f e1 6f bf a6 f0 7c fd 7b 2d 56 c5 ce 50 7b a8 f8 35 17 69 0e 89 94 60 79 10 d0 7c 49 c5 c7 d0 7a 5c 65 74 e6 55 ae 8f 04 df 16 b5 aa fb 41 05 2e b9 a6 31 de 02 44 12 40 b4 9d 52 a8 ca 0b 8f 1b 0b 31 37 05 dc be 71 ec 89 d4 12 2a b7 54 82 ec 43 f8 23 75 8c e5 a4 69 c0 32 56 51 87 f7 88 14 65 cd 64 81 9f 57 45 3d 29 ef 16 60 0f f7 a1 73 43 22 2a 3b f2 25 8a 07 5d a0 38 8f 8c 0a c3 48 98 93 c5 fa 54 27 03 46 02 f7 10 d1 a7 ab 76 31 29 9b 57 96 0c 48 f8 61 bf f0 19 f8 09 66 30 34 56 8a 52 e9 d9 1d 54 cf da ed a1 bb 3f 03 dd ef 88 33 0a b2 bc 6a 8e 8b 55 64 37 1b d0 90 bb cf 84 1e 54 10 4d 07 14 f4 1e 87 29 f3 33 be aa 6d f2 d7 7b 36 80 54 9c 7e d1 29 7c 35 95 86 13 17 36 4e fa c8 08 3a b7 b9 9f fd e1 47 91 61 59 76 15 e8 8d a4 9e a9 86 40 0e 9e 19 07 87 61 2f 60 f3 ab 32 9d ae 98 98 b4 b6 9b 41 ad 37 9a 5f d0 7b 12 62 a6 6f a4 3e 05 6e 3d 77 55 20 ec 17 d8 49 ab 12 5e a3 f0 a9 ef 7c 65 79 49 7b 6e 7b e1 81 9a 33 2a 8f 19 d9 7f c6 d4 9c b9 ed 15 2a fd 1d b8 0d 92 7f 50 7e 7b ce ac 72 38 c1 55 8b fc ac a0 8b c5 a0<br>Data Ascii: \yo6)&%k.AM[w .!EQ=FtDR,n[~*4FpE~8)*1!>?}o.-- 6b!o#ovB80f~K]W:_4\$M(ICd'')(KE~0hHb):N*6hy7 wX_n"]SnQ=tx+/@ul-c #S3SW/xa[CT+e<>?XB/ dX~w=T& 9<\$~b8WHL%?_Q9{su-&yGb`Kidi.NQGKF\$0qvl}faGB:70l0g@{t lg*,*vrDB;I3:Wkm986M1k_k<'O}aQqK0\$YURO}9:[yo {-VP{5i`y lzletUA.ID@R17q*TC#ui2VQedWE=)'sC"*;:%)8HTFv1 )WHaf04VRT?3jUd7TM}3m{6T~})j56N:GaYv@a/'2A7_{bo>n=wU l^ eyl{n{3**P~{r8U |
| Jun 4, 2021<br>21:35:05.395149946 CEST | 1301               | OUT       | GET /wp-content/themes/enfold/js/shortcodes.js?ver=3 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.593955040 CEST | 1388               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:47:41 GMT<br>ETag: "24d6d-55c779b5d4d40-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 35569<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed bd 7b 7f 1b 37 92 28 fa 37 f5 29 60 8e 33 24 2d be 24 c7 79 50 91 73 1c 27 73 c6 e7 26 e3 6c ec 99 d9 59 c7 cb 5f 93 6c 49 1d 53 6c 0e 9b b4 ac c8 ba 9f 65 3f cb 7e b2 5b 2f 00 05 74 37 45 39 b6 67 f6 dc f1 ee 44 52 03 28 14 80 42 a1 50 a8 47 fb 64 b3 98 ae b3 7c d1 be db d9 bb 6a ec 19 f8 d7 dc 14 a9 29 d6 ab 6c ba 6e 1e ed d1 a7 bb ed 59 3e dd 9c a7 8b 75 a7 bf 4a 93 d9 65 db b5 eb 50 05 69 da 18 0c 4e e7 f9 24 99 9b d7 c9 2a 4b 26 f3 b4 30 eb b3 64 6d 92 55 6a 00 ec cc e4 0b 53 a4 af d3 15 54 c9 a7 49 51 00 88 82 9b de ed 27 af b3 64 bc 59 67 f3 6c 9d 41 c3 63 53 fa f4 f6 ad b9 ba 3e e2 fa fc df ec a4 6d 06 8f 16 b3 55 9e cd de 5e a4 93 a7 cf de 66 3f 9e e5 8b 14 7e 24 33 f8 4f 3e 7b fb cd 3c 99 be fa 26 5d ad 2e df 3e f9 ee 87 7c 92 cd d3 b7 4f 97 80 83 f9 21 5b 64 83 ac bf 4e 8b 75 7b 01 7d 9d 26 eb 7c d5 07 44 57 8f 4e 71 b0 e6 f7 bf 37 ad 7c b1 ce 37 d3 b3 62 9d ac d6 2d 93 2d 8c 9d 8b be fd e5 bb 79 4a 73 c3 28 5d f1 8f d2 80 fa 59 c1 9d c3 c8 cc 7a b5 49 65 20 d7 fc 23 9d 17 e9 2d 00 9c 24 50 3f 80 60 57 20 81 85 79 9d ac 53 73 92 bd 81 19 9f 9c 62 dd f9 04 e6 c0 9c e4 2b 73 4e 20 dc ec dd ed 9f 2c b8 1f 2e 18 53 ab ce 1e 74 df 6e 51 41 6f 72 da 2b d6 97 f3 b4 47 45 ad 4e b9 7a bb 13 2c 8a c2 61 99 c0 52 cf 93 37 a6 98 ae f2 f9 3c 5b 9c 12 12 88 cd e9 2a df 2c 66 45 bf 02 15 db ca a3 d1 b3 9f 6c f7 f6 ef 52 d7 d3 64 3e dd cc b1 ef f5 59 6a 26 ab fc 02 96 d3 9c a5 d9 e9 19 d0 e1 62 66 92 e5 32 c5 1f 66 5a 14 66 b5 81 e9 5c e7 54 f7 0c 28 1b 3a 0c 30 91 f6 63 6e af f0 39 07 d2 39 df 9c f7 b8 a0 6b 78 aa 4e 36 f3 39 8c 34 4d 17 bd 62 9e cd d2 15 15 f4 a6 e9 7c 8e 2d a4 b6 1d 43 08 1c 47 d2 68 c0 ff c7 63 10 dc f3 13 93 26 d3 33 f3 1a e0 e6 b0 8b 68 ff c5 f8 52 e1 58 0a 11 5d 23 f8 ca a7 de 45 b6 3e eb 51 2d 58 57 8b 48 d0 4a e3 01 9b 7d 8d 7b 38 4d ce 4d 91 4f 33 d8 b6 d9 14 f6 f0 3a cf e7 eb 6c 49 73 8e ff 16 e9 05 ec d6 47 00 eb 39 97 b4 af 5a d3 39 ec ef d6 c8 34 69 66 a4 45 b3 6b 66 c9 3a a9 f8 9a ce 93 cb d1 b0 0b 84 92 2f 53 28 9f e4 b3 cb e6 75 19 17 ea 3f e5 1d e7 f0 68 34 76 c6 c0 d0 1f 08 a5 06 a7 b8 a8 16 31 37 7a 4b ed e3 e2 2c 5f ad a7 f9 0c 7e 9b ae b2 e5 ba b0 d4 e9 f6 27 fe 1b 0c 00 22 d0 24 53 88 5d de b3 74 0e 3c c9 55 72 bb 8f ea 72 55 58 2e fa 6b cc 7f 0a dd 8c b9 65 4d 57 cd e4 97 e4 4d d3 2c 01 b1 93 7c 9e e5 41 07 a7 ab 6c d6 83 4d f9 aa e8 61 35 b7 b7 6c e5 f1 72 95 be ce d2 8b 1a d8 34 f0 e4 b5 90 e9 79 52 e4 8b d5 a5 e1 a1 8f 80 5e 56 6b d8 ef 83 79 9e cc f0 67 ba 9e c6 d4 2a 4d f4 b6 e2 2f 8e c9 f0 9f 8a 24 1d 67 c1 2e 93 e9 34 5f cd ca db c0 7e d6 6c cc 7e 13 d0 f6 4f 07 7a 77 e8 e3 75 fa 66 bd ca d7 78 58 28 d4 e5 4b 0f c8 67 9d 64 0b 5 a ae b8 7a c5 40 0a ea 6b 9d 4c ec 96 36 8e 8a e2 7e 8b e9 18 ea e9 dd 7d 05 ff b3 fd 43 91 db e5 0e 07 63 91 08 db 32 1 e d7 bf 01 17 da 16 e9 6c 9c 00 1b 4c b0 ea 38 5b 8c 5d b7 31 6e ae 56 8f da 95 e7 68 3b b8 00 5d 22 40 da 7f f8 0f a8 b0 f7 e1 fe 21 f8 47 8f 9f 3f 9b cb a3 e7 df 99 47 df 7f 6f 9e fd<br>Data Ascii: {7(7)`3\$-\$yPs's&I_Y_IIISle?~[/t7E9gDR(BPGdIj)]nY>uJePiN\$*K&0dmUjSTIQ'dYglAcS>mU'f?~\$3O>{<&}.> O! [dNu{&}&DWNq7 7b--yJs(QYzle #- \$P?' W ySsb+sN .,StnQAor+GENz,aR7<[*;fElRd>Yj&bf2fZfT(:0cn99kxN694Mb)-CGhc &3hRX]#E>Q-XWHJj}{8MMO3:lsG9Z94ifEkf:/S(u?h4v17zK,-~""\$S)t<UrrUX.keMWM, Alma5lr4yR^Vkyg*M/\$g.4_-l-Oz wufxX(KgdZz@kL6-}Cc2lL8[]1nVh;)"@!G?Go |
| Jun 4, 2021<br>21:35:05.807198048 CEST | 1559               | OUT       | GET /wp-content/plugins/ultimate-faqs/js/ewd-ufaq-js.js?ver=1.9.0 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifeccl1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.994012117 CEST | 1966               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Mon, 15 Jun 2020 15:21:49 GMT<br>ETag: "3ba6-5a820fc563eb1-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 3449<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 e5 1b 6b 6f db 46 f2 b3 02 e4 3f 6c 19 c0 a4 62 49 b6 13 dc a1 b0 ea 16 ad dd<br>a2 3d 34 49 1b 27 57 1c 7a 3d 81 12 57 16 1b 8a 64 c8 a5 6d 5d aa ff 7e 33 fb e2 2e b9 a4 24 a7 45 0b 5c d1 d6 b6 76 76<br>de 33 3b 33 bb ba 0d 0b b2 8c 13 46 8b 38 bd 99 15 55 9a c2 4f 72 41 fc 97 99 3f 7d fc e8 16 96 ef f2 65 56 ac cb 59 49 c3<br>62 b1 6a c3 3c 7e f4 eb 8f 15 2d 36 c1 b2 4a 17 2c ce d2 60 f8 81 9c 9c 5c bd 7a 41 5e d3 30 da 3c 7e 44 e0 9f 6a 19 be<br>bf a6 ec 32 89 17 ef be 0d d3 28 a1 45 19 0c a7 62 f1 ed 37 5f fe 08 8b 5f 56 2c bb cc d6 79 42 19 ed 05 7c 1d 32 60 a1<br>6b f5 eb fb 1c 56 2e b3 24 09 f3 92 76 41 fd 10 de c4 69 88 fc 5a 10 35 cc 4f 3f 7c 83 72 cb 55 be b8 15 10 4a 50 02 ba f8<br>7a b9 a4 0b 16 44 71 99 27 e1 66 44 f2 ac 64 b3 38 1a 92 0f 02 13 6a b0 a4 09 c0 d0 48 c0 82 e6 0a 7a 4b c3 64 46 f9 df<br>92 ad 93 13 b2 86 bd 44 7c 48 d8 26 a7 25 49 29 8d 48 9a 91 2c 47 7a 25 c9 c3 b2 84 4f e6 1b 12 d1 65 58 25 ac 26 a2 40<br>2e c8 87 6d 8d b2 cc d6 54 a2 2c c9 2a bc a5 40 fb 7d 15 17 80 24 0f 8b 70 0d 9a 2e 4a 01 1d 2f 49 d0 62 f5 e2 82 78 65<br>fc 5f ea 11 2d 11 31 49 11 96 9d c3 ff ef e2 88 ad ce c9 b3 d3 d3 11 59 d1 f8 66 c5 ce c9 df 4f c9 96 28 56 b6 9a 23 d0 19<br>61 2b c5 54 4d 5a 6a 90 70 8a ab ec ce 03 82 d2 b1 88 f7 04 dd 67 3c cf a2 cd d8 3b 96 2a 26 c3 09 c2 35 79 1e 29 f6 46<br>e4 6f 9c 1d 6e bf 6b b6 49 68 e9 30 d3 70 0a ac 0d 9a 0c ac e2 88 ee c3 00 c2 fd 1e 0c 6c b9 5f 81 76 16 61 92 cc c3 c5<br>3b a2 7d 8c 65 64 8e c1 49 42 02 d4 22 9a 92 79 76 4f 10 c6 70 c4 1d 34 3e 38 44 54 3a 2e 29 7b 13 af 69 56 31 23 80 b5<br>e4 be 21 b8 af 04 1f 4e 0a ba ce 6e 21 46 c1 1d 03 8f de 45 63 0e 25 f8 f3 86 53 b2 e5 b2 ef 50 ee 83 28 87 51 d4 49 d6<br>a4 ba b5 23 d5 9d 7e b8 62 14 bd 09 47 86 ff b1 ec e6 26 a1 fe 70 92 2d 97 81 bf c0 3d f8 47 aa 7e 1f 69 eb 04 10 c8 29<br>13 78 06 18 85 ca 35 2e 88 44 cb 56 71 09 5c 33 56 04 5e 14 b2 70 8c 10 71 e4 89 4c 32 18 b4 c1 fc b0 88 c3 31 e5 49 8c<br>46 06 31 12 c4 23 82 20 92 de a0 a0 ac 2a 52 fe 11 2a d6 67 45 45 7d f2 05 f1 97 61 52 c2 6f e7 f2 23 04 de 2a 82 9c e3<br>49 5e f0 9f 57 22 8b f0 e4 36 18 28 21 94 3f 7f 77 75 cd 0a 99 eb 1d c6 d0 7b d0 c0 da 6a fe 71 73 3b 84 49 58 76 19 4d c9<br>f2 f5 4f 57 33 cc ba b3 d7 22 37 c2 af 81 a4 33 6a 31 24 d8 dd 72 71 40 d2 26 8a 6f c1 c1 4c 04 35 b8 d2 42 db e6 8b 90<br>d1 9b ac d8 8c 59 cc 12 fa 31 2e a0 30 f5 bb 81 82 92 ae 20 b7 26 19 a6 77 bd 4b c6 80 c5 9f b4 81 41 c5 d4 6f 07 bc 0e<br>11 e1 03 86 c1 04 63 1a 81 df a5 90 70 b1 c8 8a 08 e4 f5 b5 c9 7a 94 18 a7 29 2d 7c 33 5a 77 33 26 0d aa f8 13 ba 68 d2<br>da 53 21 56 7e da 9b b4 e1 4b 07 d2 3b 5c 4e b7 27 62 5a 07 df 83 7f f3 71 12 a7 ef 0e 76 c0 ce e8 36 72 8d bf 62 eb 64<br>44 90 2f 34 51 1a af 81 d5 e0 43 b9 28 a0 64 7a 93 e5 e7 ca fd bc 5a fa 24 2e 99 c7 99 81 ac 1d 0c 27 c0 20 19 7f 7a 0a<br>19 f7 ec f4 94 4b d5 1d 5a 2b a8 02 69 f1 07 c8 83 21 03 04 be bb 6a c6 19 46 58 e0 19 99 b6 91 a3 cc 64 c6 11 98 11 d0<br>48 51 b5 bf ef 93 1a 39 b6 69 67 46 e3 cb bd f9 ec 81 36 42 59 a1 32 91 c2 d8 66<br>Data Ascii: koF?lbi=4l'Wz=Wdm]-3.\$Elvv3;3F8UOrA?)eVYljb<~-6j,`lZA^0<~-Dj2(Eb7__v_yBj2'kV.\$vAiZ5O?)rUJ<br>PzDq'fDd8jHzKdFD H&%!)H,Gz%OeX%&@.mT,*@}\$p.J/lbxe_-1YfO(V#m+TMZjpg<:*&5y)FonkIh0pl_va;jedIB"yvOp4>8<br>DT:.){iV1#lNn!FEc%SP(Ql#-bG&p=G-)x5.DVq3V^pqL21f1# *R*gEE)aRo#*l^W"6(!?wu[jqs;IXvMOW3"73j1\$rq@&o<br>L5BY1.0 &wKAocpz)-j3Zw3&hS!V~K;N'bZqv6rbdD/4QC(dzZ\$. ' zKZ+iljFXdHQ9igF6BY2f |
| Jun 4, 2021<br>21:35:06.004292011 CEST | 2037               | OUT       | GET /wp-includes/js/comment-reply.min.js?ver=5.5.5 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.191903114 CEST | 2404               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "ba8-5c007b469ca7c-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1346<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 85 56 51 8f da 38 10 7e bf 5f 01 79 88 ec d6 b8 ac ee 8d d4 5a b5 2c d5 a1 76 5b e9 76 a5 9e 54 55 95 89 07 62 6d b0 39 c7 c9 5e 0e f8 ef 37 4e c2 12 28 f4 f6 85 65 66 70 66 be f9 be cf 79 f3 6a 38 78 cc 74 31 58 ea 1c 06 f8 29 4b 6f 47 2b 30 e0 a4 07 35 78 f5 e6 b7 67 6d 94 7d e6 52 a9 a5 5d af c1 78 b1 2c 4d ea b5 35 a4 a2 db 4a ba c1 9c 4d 59 c6 66 a2 e2 ca a6 65 28 61 0b b1 4d db ea 3f 61 93 d7 d3 5c 16 c5 24 ea 42 23 17 62 a3 5c 9b a7 88 f5 cb 1e b5 cf 61 ae 26 51 5b e0 c3 57 ac 90 26 85 bc 29 08 b9 f6 eb e8 17 67 7d b0 6e dd 54 b6 5f 97 f8 35 62 1e d6 1b eb a4 ab 0f d9 e7 cd 28 c4 46 21 3d 52 ba 8a d8 46 3a 2c 9f ab 0f 1a 72 d5 3b e0 47 9b c0 02 5b 5c 4c 63 f8 c7 fc 2e da 33 40 0c ee 4b 2f 03 3a 5f 16 05 b8 0a dc 6e 57 f1 af b0 f8 a8 fd a5 cc bd fd f7 3c cc 9c 88 fe 2e c1 d5 0f 90 43 ea ad 8b b4 19 cc e2 38 c2 15 cc 2a 7c e0 27 5d f8 b0 a1 10 af 98 11 c3 e1 ec 05 f9 59 0e e1 83 2b e9 65 01 3e 39 ec 6a e0 09 dd 2a 42 19 c4 b1 81 e7 01 10 4b b9 6d 9f 48 66 7c 61 55 cd b6 69 a6 73 15 4e 9f 0c c7 ac 28 17 de 01 e0 bf 7b ba 7f 39 46 11 a0 5b bd 24 2e 8e c9 5c ac c8 82 9f ac 87 b2 69 1b ec 6f 82 b2 39 a5 db 39 3f ef 9f 44 de 96 69 56 78 e9 10 dc 1c cb 2e 94 a4 b9 4e 9f 42 36 09 54 eb 91 af ed 83 00 5f 83 97 1f a1 de ed 80 a7 de e5 f8 2f 8d e3 9b df 85 10 c0 9f a0 9e 5a 05 d4 81 2f 9d 19 4c b9 83 b5 ad e0 ec 19 58 85 14 37 48 12 c4 87 6f 1c 84 f4 1d 2c 65 99 23 6c 6c ca 11 8b b5 f6 bc e9 05 03 c3 9b 7d 32 8d e3 e9 85 76 7b 47 25 c8 2c 12 9a 36 4c 9d b4 dd 0e f2 02 d2 51 21 09 2e 07 87 08 5b f8 8c 5d 17 bb 1d 01 31 a3 89 17 33 be 82 c3 6e 8b f7 6d f5 67 b9 86 5b b8 92 20 9e 4e 80 9f d0 e8 5d 9e 93 88 47 af b1 b3 0e 0e bf c7 76 98 15 63 a6 85 e2 39 98 95 cf 12 fb 56 27 f6 f5 6b 4a 8c 50 df ec 77 fa 3f 6b 93 94 99 eb 6b 93 74 7f e4 4e fe 32 3c 0b 90 04 9e 9c a9 92 26 2a 8e 33 a4 56 c8 9d c9 91 f2 4a e6 25 88 68 8c e0 62 bb 1e fe f1 53 6b 7c b0 1b d5 15 07 d4 78 70 04 99 c2 34 c0 48 32 86 f4 f3 e8 70 bc f0 75 0e 5c e9 02 b3 b5 88 8c 35 e8 2d 46 10 25 70 d2 1e 67 fb 4e 44 91 49 86 2f b5 2b 7c 73 1c 7e 55 dc e0 83 1f f4 02 2d 67 c5 54 13 c0 a7 3e d6 1b 40 c6 35 0d 3c ce fe 7a fc f1 f9 cb 1d 6a d6 e3 2c 06 a5 fb 2e c2 a4 69 2a c3 76 c2 a9 5a 0d 85 38 93 4f a8 3e 6f 34 a2 ec 64 58 71 91 a4 3d 89 ca 23 c7 ae 8d 85 73 63 67 be 37 d9 29 9c 22 20 86 c4 58 13 c5 a2 05 e4 f6 19 5a 8a 61 33 ba 8d 76 c7 6a 85 21 d7 86 1c 14 1b 6b d4 b1 d4 b7 f1 e0 8f 4d 9d 39 d4 61 2b de 46 74 b7 33 89 8d 63 1d c7 ae 81 6a 78 83 28 55 bd ab 86 07 b1 06 6a 10 cb 34 73 0c 89 43 83 44 ce a7 3f 0e 6f c3 f0 07 e1 79 74 80 8e d5 7e 34 4a 28 fa 05 7c f3 df c3 03 a0 55 58 97 3e f8 43 65 b5 42 8b eb 9d b7 26 80 52 de 76 79 83 7a eb 9c 15 cf 99 34 e2 7b e7 bd d3 8b d2 03 89 42 6a 14 04 76 fc fd 2a f4 d3 fd ba 2f e2 f7 b8 6d 4c ed bb 14 ce 1f e5 56 2a e4 54 84 b4 98 21 89 a5 aa 1f f0 62 80 5b 9c 6f 82 f9 ea 82 ca ee be dc 77 3b fb 84 3f 06 85 ca 40 73 a2 6c ab 8d f6 13 c5 0e f0 4d 8e f6 c3 1a f1 31 db 52 44 8b d0 60 92 e1 87<br>Data Ascii: VQ8-_yZ,v[vTUbmn9*7N(efpfyJ8xt1X)KoG+05xgm)R]x,M5JMfYe(am?a\$B#b\&aQ[W&g]nT_5b(FI=RF.;r;G[\\c.3@K/;_nW<.C8*"]Y+e>9j*BKmHfJaUisN{9F[\$.\\io99?DiVx.NB6T_/_Z/LX7Ho,e#]]2v[G%,6LQ!.[13nmg[ N]G vc9VkJPw?kktN2<&*3VJ%hbSk]xp4H2pu5-F%pgNDI/+/s-U-gT>@5<zj,.i*vZ8O>o4dXq=#scg7)" XZa3vj!kM9a+Ft3cjx (Uj4sCD?oyt~4J([UX>CeB&Rvyz4{Bjv*mLV*Tlb[ow;?@slM1RD` |
| Jun 4, 2021<br>21:35:06.195847988 CEST | 2406               | OUT       | GET /wp-includes/js/jquery/ui/effect-scale.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecclvdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Jun 4, 2021<br>21:35:06.389192104 CEST | 2432               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "455-5c007b4699b9b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 586<br>Keep-Alive: timeout=5, max=95<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 75 52 4d 6f bd 30 0c bd f7 57 28 3a 04 52 a0 ca 36 b0 93 0b 21 87 61 c3 7a e8 61 5f d8 a1 e8 c1 b5 e8 5a 85 23 79 b2 dc 2e 4d fc df 47 7f 25 ce 8a 9d 44 8a 8f e4 e3 23 a3 cd ea 8a 6c c8 f3 d7 16 fc 9e fc bc 25 9f 8a 02 f2 d0 90 ef 79 56 01 49 64 92 c8 0f 3d a2 0c a1 4e a3 e8 f9 77 0f 6c 8d cc dd 0e bf fb c8 47 57 ef bd 79 2a c3 5c e5 b3 6b ad ce 82 71 96 64 56 13 17 4a f0 24 77 36 78 f3 d8 06 e7 9b 3e eb 1b 54 90 35 a0 09 62 31 8c 18 72 77 fb 83 54 26 07 db 80 7c d7 52 3a ff 14 4d d1 a9 f1 14 cf 6a 23 97 b4 a2 a6 a7 7e 0d c3 20 11 02 a3 ab 55 d1 da bc 27 c4 80 1f e8 ec 50 a5 c2 be 06 57 10 0d 85 b1 b0 5e 8f af cc 76 7a 3b 9a ec 9e 8e a5 a9 a0 32 1a 4b 2e cc eb c6 bc 01 7d 10 c0 53 60 e3 f4 bc 63 a7 66 2d 3f 78 08 ad b7 a4 95 63 42 33 bd 72 e0 a8 ce b4 44 e0 87 97 cc 13 a3 5a 16 4a d3 70 e1 14 26 fd 09 60 35 5b c5 e2 d0 61 13 51 aa 73 a1 06 c2 9d d3 c0 8c 00 b9 43 e3 78 a4 13 3f 2e 0a 55 67 be 81 5b 1b 18 c8 1a 3c aa 16 44 12 f3 e3 91 c5 4a fd 37 48 4b a3 01 55 51 e5 36 4e 93 38 e6 c2 2b 90 da 78 18 58 22 e0 11 97 49 45 8e bf 0e 57 6e ac d0 ea 50 42 bf fc d4 c8 d1 60 5c bc 1a 1d 4a fc 18 5e f4 5d 1b c0 7f 99 61 0b 6f 8e fd 9a 12 ce 0e e3 9d b0 8a 96 d8 e6 d0 2f 27 ab e8 4a 29 bf 2d 22 a4 95 26 38 20 7d 01 1f 4c fe 4f e0 c6 4d fa 28 3a ac 46 38 89 eb 6b 41 ad 12 34 f1 38 ea 0a 02 a8 20 66 ad 30 b9 5c af 99 9b e6 51 f9 f1 78 4f 77 46 eb 0a 93 69 2f 0d 78 5c b0 93 1e 1a 3c 5d 2c 84 aa 38 59 78 b7 43 11 fa 07 35 a5 4d e9 5e 47 dd 66 35 e2 49 84 f8 62 f8 78 39 6e dc a5 ba af 15 dc 49 43 3d 69 b8 b1 53 ba 1e 35 dc 14 17 65 f4 52 43 c4 2e 8a ea 85 86 9b a2 eb a9 66 1a 2f 7b c1 71 18 b7 67 2e 5d 9d e5 26 ec 55 3c b0 38 b9 09 17 e7 4b 78 8f 4e 2e d1 31 e7 c2 4c aa 33 c7 bb 8e df fc 05 1b 55 39 d0 55 04 00 00<br>Data Ascii: uRMo0W(:R6laza_Z#y.MG%#D#%yVId=NwlGWy*lkqdVJ\$w6x>T5b1rwT& R:Mj#~ U'PW*#vz;2K.)S'cf?xcB3r DZJp&'5[aQsCx?.Ug[<DJ7HKUQ6N8+xX"IEWnPB`\\j"jao/J)"&8 }LOM(:F8kA48 f0lQxOwF!x<l<).8YxC5M*Gf5lbx9nIC =IS5eRC.f/[qg.]&U<8KxN.1L3U9U                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.389955997 CEST | 2433               | OUT       | GET /wp-includes/js/jquery/ui/position.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Jun 4, 2021<br>21:35:06.576330900 CEST | 2560               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "1926-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2469<br>Keep-Alive: timeout=5, max=94<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 00 03 9d 58 7d 93 e2 b6 19 ff 3f 9f c2 eb 69 88 75 08 03 d7 74 3a 35 e8 98 b9 5c 32 b7 33 77 99 6b 4a 67 db 61 e9 8c b1 65 50 62 2c 6a 0b 76 29 f0 dd f3 3c 7a 31 36 b0 c9 a6 37 77 9c a4 e7 45 d2 ef 79 b5 fa 6f ee be f2 de 78 3f ff 7d cb cb bd f7 cf 7b ef 8b ac 84 12 b2 f0 86 e1 70 18 7e 8b c4 95 52 9b a8 df ff f9 bf c8 b3 15 61 22 d7 b0 8c 94 ef e4 66 5f 8a e5 4a 39 05 3f c8 6d 91 c6 5a 3e 2e 52 4f aa 15 2f bd 44 16 aa 14 8b ad 92 65 85 52 3f f1 9c c7 15 4f 3d e0 05 32 f0 78 9f ef a7 5e 2e 12 5e 54 3c bc da 32 94 e5 b2 6f a9 76 63 4b 8f 37 22 6c 1e ab bf b1 a7 ef 03 53 ff ab bb 6c 5b 24 38 0d 14 39 f8 6e e2 33 a6 f6 1b 2e 33 2f e5 99 28 78 a7 63 fe 0f e3 75 3a 31 c3 60 e6 1b b5 fe 9c 2a 12 a9 c0 5c 8f 9c 82 5a e3 3d 39 94 5c 6d cb c2 ab 97 c8 e1 3e dc 0a 86 3f c7 e3 e1 34 da c5 a5 27 e9 47 fa cc 3e c7 6a 15 ae e3 67 3a 35 c3 78 51 d1 4f 66 58 22 62 b4 60 fd 9c 67 ea 08 77 54 bc 3c 6a 4c fb 34 67 7d 25 37 6e 71 21 95 82 2b d2 8c f5 67 8f dd c7 de fc 31 ed 06 8f e1 ec 31 9d 77 c9 e4 eb 49 9f 56 ac ff 9f c7 a7 6e 9f ae 58 ff eb 3f f5 29 87 b3 64 45 e8 40 19 b9 93 7a 5f 02 45 05 e5 ee 0a b3 4d 5c 56 fc 87 5c c6 2a 50 b3 c1 9c bc 09 56 a1 e2 95 9d 4d 44 7f 38 18 44 43 42 5b 7c c3 16 f1 cc 26 dc f2 cd 4f f5 4e 1f 70 a7 1a 2a 2d 7f 5f a8 e0 3e 4c aa 4a 93 e8 70 40 8e c7 c1 e9 be 3e 26 3b 54 49 29 f3 7c 11 97 0f 22 55 ab a8 01 b0 c8 82 9d 14 a9 37 b8 63 4c 12 ab 55 6a a4 41 19 bb 0f fc 71 2a 76 5e a5 f6 39 67 df a4 a2 da e4 f1 3e 5a e4 32 f9 65 e4 f4 47 80 be cc b7 8a 8f 9e b4 fa bf 0c 36 cf a3 15 47 c8 cd 58 ee 78 99 e5 f2 29 5a 89 34 e5 c5 e8 9b 77 4d a5 96 13 6e 0a ac 46 43 0c ae 8d 5c 7d 60 b3 bf 3e 01 f4 c1 27 57 22 4f 4b 0e 47 07 20 47 f6 bc 70 ca 85 4c f7 3e 09 e3 cd 86 17 69 00 28 28 c6 43 99 65 15 57 fa ce 54 68 80 7c 77 14 9f fa 06 14 1f 59 19 0b 78 9b 9f 74 3a b0 24 60 93 30 c9 05 f8 8b 59 05 35 25 f5 83 92 80 50 c9 54 8f 9f e8 92 ab 7f 68 4d f7 45 26 a3 66 80 20 88 82 a9 50 54 0f a2 48 e5 d3 f1 88 e3 0f 32 d9 ae 41 e1 c4 f7 23 15 42 e4 e2 a4 7d b8 de b3 be ed ff 23 09 20 80 d9 dc dd e0 62 10 39 3e c2 a9 c7 9d 8e 0a 35 c2 e3 5a 1e 6f 68 b8 f5 0d 2d a4 07 63 87 86 1e de d0 c3 51 8f 31 db 2d 45 1f 35 65 72 76 c0 b0 ed 7f 01 89 06 d4 5a 5d fc 36 db 49 e3 fb 20 d4 4a 14 2f e0 7b 1f a8 e3 f1 49 c3 44 74 80 3a d0 02 b4 1e 5a f7 ee 0e 47 9d ce df 10 02 3c 66 21 53 3e 85 8c e5 2e 6b 6f 10 09 ea 64 23 4e cf 78 47 8a 1a cf 88 84 75 91 00 22 ec 80 f9 05 2e 02 09 05 ce 49 cd 09 3f e1 9a 08 cf 13 f0 13 33 99 02 9b 23 c0 18 d6 0d c4 80 ab 9a 08 63 15 b8 31 ec 00 81 e4 00 70 28 59 26 33 3b 73 7d b4 f3 13 c0 d4 4a 4c ac 86 29 d1 21 7e 97 1c 8f 77 09 1c de 45 38 c7 48 c9 f7 01 e0 5a d1 b8 5c ea 7b 56 64 94 00 7e fc 59 61 0c 1d 4e 34 21 3a 11 a4 34 a6 4b ba a5 6b aa e8 13 e0 ad 15 d1 07 d6 b0 5c cb 48 c0 f0 a4 27 84 ee 2f 98 ce 91 12 3c 10 ba 63 c0 9a c0 82 a8 80 0e 0e 96 e5 62 03 51 0c 49 46 a8 c0 f7 c0 97 17 0c ce 21 18 9a 2e 50 2c 10 ec 09 03 9f d4 26 9c 58 4f ad 11 ac 1d ab 46 cb 19 ef a0 2d 45<br>Data Ascii: X)?iut:5l23wkJgaePb.jv)<z167wEyox?){p-Ra"f_J9?mZ>.RO/DeR?O=2x^.^T<2ovcK7"SI §89n3.3/(xcu:1`^lZ=9\m>?4'G>jg:5xQOfX"b`gwT<jL4g)%7nq!+g11wIVnX?)dE@z_EMlV!^PVMd8DCB[!&ONp*-_.LJp@>.&T)! U7cLUjAq*v^9g>Z2eG6GXx)Z4wMnFC\}>'W"OKG GpL>{((CeWTh wYxt:\$'0Y5%_PTHME&f PTH2A#B)# b9>5Zoh-cQ1-E5ervZ}6l J {lDt:ZG<!lS>.kod#NxCu".l?3#c1p(Y&3;sJl)!~wE8HZl{Vd~YaN4!4KKHf/<bcQlFI.P,&XOF-E |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 1          | 192.168.2.4 | 49736       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.180651903 CEST | 1121               | OUT       | GET /wp-content/plugins/the-events-calendar/common/src/resources/css/common-skeleton.min.css?ver=4.12.10 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.368954897 CEST | 1126               | IN        | <p>HTTP/1.1 200 OK<br/> Date: Fri, 04 Jun 2021 19:35:04 GMT<br/> Server: Apache/2.4.18 (Ubuntu)<br/> Last-Modified: Fri, 02 Oct 2020 21:43:28 GMT<br/> ETag: "68db-5b0b705ecf241-gzip"<br/> Accept-Ranges: bytes<br/> Vary: Accept-Encoding<br/> Content-Encoding: gzip<br/> Content-Length: 5116<br/> Keep-Alive: timeout=5, max=100<br/> Connection: Keep-Alive<br/> Content-Type: text/css<br/> Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 5d 5b 8f db b8 92 fe 2b da 19 04 9d 9c 0d 15 91 ba db e8 01 66 83 05 f2 90 3c 1d a0 5f 06 41 20 4b 6a 5b a7 65 cb 23 cb ee 1b e6 bf ef 57 a4 64 cb 94 7c 69 db c9 c9 ce 69 cc b4 4c f3 52 2c 56 15 ab be a2 64 c5 ac ca 6c 94 b2 b8 98 4e 8b d9 33 bb 4f 47 77 59 c5 6e 8b 59 c5 16 d3 a2 a8 26 d9 6c 3c 88 66 55 16 e5 59 b4 48 93 21 9b 16 4f ac 58 3c e8 7d c6 65 f4 b8 88 a3 3c 1d ee 1e fc 97 d9 9e cd f8 c7 f3 a8 78 60 8b ec 89 ba 8d 8a 32 49 4b 86 1a ad 57 54 56 59 9c a7 ef b5 da 45 96 e8 75 49 5a 45 59 be d0 6a 6f b3 71 1c cd ab ac 98 75 1b 96 a5 4e e3 16 6c a7 a5 56 39 49 a3 a4 53 39 8d 32 9d e2 34 9d 2d b5 aa 59 b4 d2 6a 16 69 dc c3 cc 62 39 9d 46 e5 e3 73 92 2d e6 79 f4 38 18 e5 45 7c a7 49 62 b1 1a 0f 66 45 f5 76 50 82 c9 77 cf c5 2a 2d 6f f3 e2 7e 30 c9 92 24 9d e9 62 5b 26 59 a1 4d 12 47 b3 55 a4 cb 67 5e 16 e3 32 5d e8 d5 2b c8 b7 58 b3 93 cd f2 6c 96 b2 3e ae e4 44 92 af 3f 62 68 be 2c f2 c5 d7 77 eb 81 b3 62 96 0e 27 69 36 9e 54 03 eb af fe 99 9f b1 10 e8 38 ca 19 ec 64 3c 1b 8c 60 2b 34 9d d6 fd 0f b5 ce af 1a a3 55 3a c5 4c 55 ba 35 65 67 a6 74 23 ae 68 59 15 ba 64 97 a3 8e 3e e6 cf f3 62 91 91 aa 06 65 8a 09 b2 55 3a 3c 8e 51 1a 5b 15 f3 01 33 dd 74 da 9d 09 56 5f 55 c5 14 cd a2 db 3e 5a a2 4d 37 8e 6c 36 5f 56 1d 33 ca 61 48 1d 59 3c 54 51 99 46 fd 1b 6b 08 0b 1b 67 b3 8e 1e 24 f9 3f aa c7 79 7a 3d 5b 4e 47 69 f9 75 30 68 3c 41 36 9b 61 f0 62 9e cd d8 6e d6 76 8c 2d 96 d5 f6 d8 e7 da 10 7a 34 90 a7 e3 74 96 3c c7 45 5e 94 b0 b6 49 5a 66 d5 b0 d1 68 15 8d e0 57 a6 d1 03 bb cf 92 6a 32 e0 96 f5 66 78 3f c9 aa 14 d4 a3 38 85 ca cb 69 94 ff b5 43 18 b0 b1 ec 29 55 a6 b8 cf 0a 0e 2d 50 b5 eb f6 d7 ea 80 89 d2 6a 4f 3b 94 3f cd aa af cf f1 b2 5c 60 99 f3 22 9b 41 42 1b 9e 56 d9 22 c3 4a 7b d9 fa 03 c2 20 31 24 fd f4 d7 ad 0d f1 24 bd 8d 96 79 d5 4b 0b 2a 22 2f 7e 5b c4 cb 85 d2 70 1f cd 6e af 67 65 4b 03 6b 38 8f 92 84 8c 4b 37 a5 48 77 d3 a3 91 4e 3b 8a cb 62 f6 38 d5 6b 93 a4 c7 09 45 f3 79 9e ea 46 7e 7c 40 e8 f3 81 fa 46 1f 65 63 bd 86 9c dc 9f 4b c4 81 63 dc 67 7f 6c 89 d3 59 37 8c c4 59 97 64 d1 8d 62 49 27 ac e5 47 05 ba e4 56 e7 22 c9 f4 e0 93 74 48 e9 d2 4d 75 cd a4 d8 d5 3a 4b b7 59 9a 27 8b 8e 66 2e 10 6a 6f b1 93 f5 e8 cb f5 0a a1 57 d8 7a 85 a3 57 b8 7a 85 77 4c 8c cf f4 ef b7 65 34 d5 d7 91 4d 75 0b ca 66 ba 6e ee 46 ba 08 f3 68 d4 d1 ab 72 82 7a a5 ce 44 1f f0 88 ca bb 53 b0 48 31 fa 57 37 88 14 3a 5b f0 e3 dd f8 33 ef c0 08 5d 2e 7f 6a df cb e5 e8 51 0f 62 fa f7 68 aa d3 dd 01 97 e0 ee 75 36 11 0a 3a dd f0 ed 4e e7 0b 95 c5 4c 57 59 1f 02 90 88 ac 8b 0b f4 98 4b 7e 57 af 1b 15 89 3e b2 d2 15 5b d1 06 d0 eb 26 9d 0a d8 a5 5e 97 75 6c b0 d2 2d b7 d2 29 eb c6 b0 d4 c5 b7 8a 74 1a 0a 02 36 a0 61 e3 f3 87 4d 18 f8 eb 80 e1 2c f3 e7 3c 5b 20 19 a8 1e f3 b4 0f 97 61 eb 3c b3 29 45 17 78 82 79 41 28 ab 98 21 ea 24 e9 60 94 c5 4b fc 0d 5b 90 41 47 00 35 b2 d9 49 bd cf 73 f5 ee e0 66 a1 5b d4 e9 6b 3d 39 7d 6f 68 43 21 d3 94 45 ab 28 89 da a1 9d c0 c6 d7 67 1d 60 a9 ce 70 c3 99 61 22 22 94 8f 8c 20 32 4a c6</p> <p>Data Ascii: ][+f&lt;_A K][e#Wd]iILR,VdIN3OGWYnY&amp;l&lt;fUYH!OX&lt;}e&lt;x'2lKWTVYEuIZEYjoquNIV9IS924-Yjib9Fs-y8E l bfEvPw*-o-0\$b[&amp;YMGUg^2]+Xl&gt;D?bh,wb'i6T8d&lt;'+4U:LU5egt#hYd&gt;beU:&lt;Q[3tV_U&gt;ZM7l6_V3aHY&lt;TQFkg\$?yz=[NGiu0h&lt;A6abnv-z4t&lt;E^IZfhWj2fx?8iC)U-PjO;?\"ABV\"J{ 1\$SyK*\"/\"-[pngEkK8K7HwN;b8kEyF-]@FecKcglY7Ydb 'GV\"tHMu:KY\"f.joWzWzwLe4MufnFhrzDSH1W7:[3].jQbhu6:NLWYK-W&gt;[&amp;^ul-)t6aM,&lt;[ a&lt;]ExyA(!\$'K[AG5lsl[k=9]ohC!E(g'pa\"\" 2J</p> |
| Jun 4, 2021<br>21:35:04.390867949 CEST | 1133               | OUT       | <p>GET /wp-content/plugins/ultimate-faqs/css/ewd-ufaq-styles.css?ver=5.5.5 HTTP/1.1<br/> Accept: text/css, */*<br/> Referer: http://www.tonhc.org/coronavirus/<br/> Accept-Language: en-US<br/> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br/> Accept-Encoding: gzip, deflate<br/> Host: www.tonhc.org<br/> Connection: Keep-Alive<br/> Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.578720093 CEST | 1157               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Mon, 15 Jun 2020 15:21:49 GMT<br>ETag: "3391-5a820fc566d91-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2446<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 dd 1a 6b 6f e3 36 f2 73 0d e4 3f f0 b2 58 64 37 88 6c cb 8f 9c eb e0 80 e2 82 f6 d3 1d b0 68 17 28 ee d3 82 96 68 9b 58 59 d4 52 92 93 9c b1 ff fd f8 94 48 8a 7a d8 49 5b e0 12 6c 1b d3 c3 99 e1 70 de 9c 31 7a 8a 83 72 0b bf 05 7b 1c c7 28 05 a7 ab 11 00 31 ce b3 04 be ac 53 92 a2 87 ab d1 f7 ab d1 d5 68 2c a0 f8 bf 08 16 68 47 e8 4b 50 e0 22 41 41 41 76 bb 04 c9 8d 51 49 73 42 d7 20 23 38 2d 10 ed d8 bb 21 f1 8b 97 26 b0 88 56 ec 45 09 82 54 11 e1 7f ae 37 a4 d8 db f8 33 44 0f 30 c1 e9 57 09 76 80 74 87 d3 35 98 2d b2 67 30 95 a0 0e 60 80 0f 70 27 58 ff 61 03 a3 af 3b 4a ca 34 5e 83 92 26 1f ae c7 e3 89 f8 36 9f e0 34 47 b4 f8 c2 37 8c b3 74 77 fd 91 e1 fa 61 8f f0 6e 5f 30 ec 61 f6 cc 3f 3f e1 b8 d8 af c1 7c 2a 3f 4a e2 4c 36 d9 1a 04 f3 99 b5 98 a0 2d db 18 86 72 d5 39 27 2c 8b 3d a1 41 cc e4 c4 f9 f2 7e 2b cf b7 25 69 11 3c 29 36 ee a7 fa 84 15 ac 46 d1 0a e9 5e 0a 46 f9 1d a8 57 0b b8 cb 4f a6 80 c1 89 fd 3d b9 35 20 f8 fd 5b 17 6f dc fb ed a4 5d 67 e4 1e 25 b2 70 3a 7d ff 50 df 2b 68 5e ac 89 c0 b8 5a a6 43 45 41 0e ec 0e a6 86 24 9b 24 71 9a 22 0a 7c 1b 17 2b df 46 ae 9a 12 3c 83 71 8c d3 dd 3a 64 04 c0 6c 29 80 ab 55 75 8f cb a5 c6 51 63 c8 d9 41 a2 bd a9 85 4b ae 83 e0 6f f8 90 11 5a c0 b4 30 77 48 68 66 0c bb 7d c2 ef 48 d2 36 15 f2 dd f6 ef db ad 75 c3 a4 c8 82 2d 46 49 1c 24 70 83 12 b6 43 49 93 69 08 69 a1 53 a0 e7 82 09 23 2b 35 05 42 63 44 03 0a 63 5c e6 6b 97 bd 8a f5 90 f3 de c0 58 a9 59 5e 6e 0e b8 60 08 bb d1 59 f2 d9 23 c8 40 4d f9 84 d3 a6 14 25 14 80 eb 3d 39 2a 68 71 84 18 45 84 c2 02 93 d4 74 16 31 3e ba 9a c9 97 2a 3e 33 92 17 81 a4 f6 86 a8 82 fc e5 b0 21 89 ed c1 70 ca 7c 05 0a 36 09 89 be 3e 74 d1 62 a6 99 10 c8 94 88 ab 52 0d c9 7c d3 8e 01 45 48 d9 12 98 dc 2a 63 99 6b 1d d4 ee 47 2c 70 53 ab cc 89 2b 80 05 52 2d 28 8e a9 5c 0e 1d 75 66 66 c4 75 54 fd 9b a9 2f c5 41 34 a6 d0 bd 21 29 9b 2e c1 80 3c 83 5c de 6d b2 11 ae 29 c7 ff 45 95 eb 54 0a 31 d5 7c 37 09 0a 45 56 9e 4d 88 af 92 9e 12 c1 8f c2 a1 78 38 dd 87 77 9e c5 99 6f 71 ee 5b 5c f8 16 97 be c5 7b 3b a8 35 34 c2 70 0b ae 99 e8 5f 89 33 2a 73 e6 aa 4c 5b d7 3e da fa e6 08 93 52 b9 55 76 09 58 6a 19 45 09 d3 b7 a3 5f d3 cc 08 15 2e 6c eb 6b 12 f5 04 92 94 f0 28 da e2 3e c7 11 39 1c 98 fe 06 14 e5 19 49 63 cb fd 0a 9a b3 45 d3 e2 c5 d6 04 eb cd 72 53 82 99 52 e5 c5 0b bf f8 97 0c 99 86 ea ec e4 7a 01 29 82 66 9a a0 c3 89 61 9e f5 2d b4 88 4a c7 f2 e5 7b cb 90 58 a0 6a 61 b9 3a ed 96 c9 24 d0 dc 1b 82 7b 35 2f 2a 48 7a 48 4b ff 6b 45 d4 ca e2 cd 18 52 50 98 32 63 a4 48 79 f7 66 aa c6 d6 48 c2 97 de 85 61 68 ea 48 33 ce fa 99 90 8e da 13 be 34 3e 8d 7f bb dd 76 cb 51 e5 39 f8 b0 b3 14 47 b9 ae 55 df 35 88 4f 99 9d 06 8a 18 3e 6d aa fe d4 17 dd 1c bc 14 65 89 4a 09 84 83 16 b2 e4 77 cd 72 c5 8c 65 93 11 cc 3d 79 b2 dc 2b 3e 72 69 30 7a 9c 64 50 67 a8 6d d9 72 e5 4f 79 b8 48 77 b9 9d 8c 08 6b 65 e1 b5 99 f0 91 a7 34 38 12 9d f5 d5 37 10 d4 ba c5 4f bb 72 4f 5c ab f8 d2 27 0d fe 3b b9 f5 ff 5c 8d 6e c1 27 c8 a4 29 02 1b fb e4 ff 99 98 7c 4a<br>Data Ascii: ko6s?Xd7lh(hXYRHzi[lp1zr((1Sh,hGKP"AAAvQisB #8-!&VET73D0Wvt5-g0`p`Xa;J4^&64G7twan_0a?)*?JL6-r9',=A--+&lt;6F^FWO=5 [o]g%<p:)P+h^ZCEA\$\$q"]+F<q:dl)UuQcAKoZ0wHhf)H6u-FI\$PcliS#+5BcDclKXY^n`Y#@M %<=9*hqEt1>*>3lp 6>tbR EH*ckG,pS+R-(uffuT/A4!)<lm)ET1 7EVMx8woq[{:54p_3*sL>RUvXjE_..lk(>9lcErSRz)fa-J{Xja:\$ {5/*HzHKkERP2cHyfHahH34>vQ9GU5O>meJwre=y+>ri0zdPgmrOyHwke487OrO\';n'})J |
| Jun 4, 2021<br>21:35:04.703331947 CEST | 1173               | OUT       | GET /wp-content/themes/enfold/js/mediaelement/skin-1/mediaelementplayer.css?ver=1 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.901354074 CEST | 1203               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:47:41 GMT<br>ETag: "4747-55c779b5d4d40-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 3274<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 1c 6b 6f e3 b8 f1 73 fc 2b 58 04 07 6c 16 56 22 4b 7e c5 8b 02 dd a6 b9 2f bd 76 8b dd 45 81 a2 28 0e b4 45 d9 ec ca a2 21 c9 49 76 83 fc f7 0e 5f 12 29 51 0f 27 fb 68 8b bb 6c 70 16 45 0e 67 86 f3 e6 38 97 7b f2 ef dc db b0 b4 c0 34 25 19 7a 1c 9d 1d 58 4e 0b ca d2 15 ca 48 82 0b 7a 47 de 8c ce f6 34 f5 ee 69 54 ec 56 93 99 7f 78 80 91 35 de 7c da 66 ec 98 46 2b 94 b2 94 4f 8a 01 8c 17 e3 3d 4d 3e af 50 8e d3 dc cb 49 46 63 78 53 90 87 c2 c3 09 dd 02 d4 84 c4 05 0c dd 91 ac a0 1b 9c e8 e1 82 1d 60 54 ed e1 fb 3f a1 df d1 fd 81 65 05 4e 61 f6 e8 69 34 1a 5d ee 89 77 48 8e 5b 9a da 68 e2 75 ce 92 63 01 18 3c 89 49 40 10 d9 af 49 34 46 c6 03 5a b3 e8 33 5f 27 77 40 7c 0b d8 6f 47 e8 76 57 94 8f 7b 9c 01 f8 15 f2 e1 f3 01 47 11 4d b7 f2 c1 a4 f6 dc f7 f9 10 03 0a e2 84 dd af d0 8e 46 11 49 8d ed 4b 7e 7a f1 31 49 f2 4d 46 48 0d e7 98 3e 90 08 80 70 66 c8 1d 80 7e f9 21 93 18 89 5d 59 51 b0 bd fc dc ee ec 8b 47 d3 88 3c 08 ec 7d be 7d c7 ee f2 d5 9e 44 14 93 84 ec 49 5a 8c bb a6 df d1 88 b0 3e 76 35 e9 95 8f f8 18 51 f6 08 1c cf 22 80 9a e1 88 1e f3 15 0a 41 6c 10 3f c7 ab d7 e8 43 81 33 00 f3 cb db 7f dc be ff 80 5e 5f 29 38 15 97 db 4e b8 62 53 c9 39 4d b6 49 db 09 cb 7b 28 94 b0 01 56 51 d7 8e 6e a8 e5 71 55 c2 61 81 a2 fb 2d 07 27 79 e4 12 38 e3 45 44 f3 43 82 41 a7 d6 09 db 7c aa 50 c6 c7 82 b5 a2 cc 11 80 45 cf e4 84 a5 7d d6 0e d6 9b da 66 de 41 ed b8 39 66 39 03 ec 0f 8c a6 40 6d bb 62 6b d0 0e c8 a3 88 de 21 1b fc fa 08 fa d0 aa fd 92 a4 99 38 46 49 94 fc 5c 91 25 0c 97 41 8c 78 6d 3a ef 71 c3 86 7c f8 91 9f 6a d8 8c 46 a3 1a b1 09 c3 fc bc 9e 89 ce d2 c6 66 59 43 66 5a 22 33 15 6f 9e 40 6d 1c 1c d1 38 e4 07 2c f8 a2 d0 36 47 42 31 41 b1 b9 b6 df f2 0d 2a 5d 37 0c c0 cd bb bf 7e 7c ff ee 17 f4 c7 b7 ef f9 9b 8a be ca 23 55 cf 19 4b f2 56 6 6 b7 5b 6e c3 86 56 a2 ae 39 11 4a d4 6d 1b 60 f3 05 87 9b 30 12 7c a9 c6 2f 0f e9 f6 a2 36 d3 bb 27 eb 4f b4 f0 12 40 1b 67 de 96 73 07 4c d1 ab f3 29 9e 6e a6 e0 8d ce 83 75 10 05 d1 c5 1b 54 5b b8 67 5f 06 ac b2 17 0d d8 e5 0c 08 a6 79 e1 e5 c5 e7 84 94 4e fa 7e 47 0b e2 81 bc 6c c4 d8 7d 86 0f 86 25 17 a6 bb c6 f3 c7 fa 81 87 52 20 87 1c 17 e2 73 1e 4d 44 bc e2 f3 a1 c2 a6 34 6d 34 e5 14 79 5a 6e 5b 8f 53 9d 54 18 58 02 ad 8e 51 04 20 39 fd 02 f0 27 13 31 22 80 96 1a 3f a9 66 39 c3 14 93 c1 fc c0 73 72 10 27 2d 62 16 87 06 28 ff 53 63 84 20 5c 39 34 69 b0 2a bb d5 34 8c 0d e3 6e 10 e1 d7 29 f0 75 2c 15 91 0d cb b0 d4 02 c5 4a cd b2 05 18 8e 85 30 1e d7 82 5c 8b 7d 4e dd 29 f9 33 b7 94 61 26 8d 84 e1 88 4c fe 14 19 70 ee 80 33 ee 6d 39 af 34 e5 92 61 06 af 9e 84 c2 af 62 b6 39 e6 28 66 19 c2 9b 0d c9 73 ba a6 09 2d 3e 73 b5 17 a1 59 3f ff 14 08 e0 22 3b 16 9c 2d 2b 4e b9 82 2f 6c 4c cd 9c 18 86 e6 23 dd 13 f4 0a b8 2f f0 bd 42 d1 51 72 ef c2 b1 bf 53 90 e5 63 c1 c1 f0 63 64 09 3f c5 f3 38 8e 3b 84 b8 e4 eb c2 e4 ab f2 da e5 b1 2c e1 ac f8 2f b0 1b 0c 90<br>Data Ascii: kos+XIV"K~-/VE(ElIv_)Q'hlpEg8{4%zXNHZG4iTVx5jFF+O=M>PIFCxS T?eNai4jwH[huc<I@I4FZ3_'w@ oGv W{GMFIK~z1IMFH~pf~ YQG<}}DIz>v5Q"Al?C3^_)8NbS9MI{(VQnqUa-'y8EDCA PEj}A9f9@mbk!8FI\%Ax:qIjFYCFz"3o@m8,E&),o?cR@/4Hy9\Yj6GB1A*]7~ ~#UKVf[nV9Jm'0]/6'O@gsL)nuT[g_yN~G!}%R sMD4m4yZn[STXQ 9'1"?f9sr~b(Sc\ 94i*4nj)u,J0l)N)3a&Lp3m94ab9(fs->sY?";-+N/IL#/BQrScdd?8;./ |
| Jun 4, 2021<br>21:35:04.916371107 CEST | 1241               | OUT       | GET /wp-content/themes/enfold/css/custom.css?ver=2 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Jun 4, 2021<br>21:35:05.101507902 CEST | 1282               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:46:18 GMT<br>ETag: "2c3-55c77966ad280-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 325<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 cd 91 41 4b c4 30 10 85 ef fd 15 ef e8 2e 2e 7b 73 a5 20 28 2b e8 45 59 a8 7f 20 6d a6 6d 30 4d d6 64 ba dd 22 fe 77 27 dd 82 2e 88 e0 cd 9c 92 cc cc cb 7b 5f d6 4b 3c aa 03 a1 ee 1d 94 d6 c6 35 18 7d 1f 10 79 b4 84 96 02 21 5f 60 85 5d 91 e3 8e a1 ac 05 9b 8e 22 b8 35 11 b5 91 a6 d8 fa de 6a 54 de b1 32 a2 22 bb ae 23 c7 f0 41 0e a1 b7 74 09 cf 22 35 98 48 f0 7b 0a 0a 9d 69 5a 51 ab 18 65 df 34 23 f2 0b 2c d7 59 b6 5e e2 81 9c 34 58 6c fb c8 be c3 b6 28 a6 4a 96 8a d9 3d c5 57 f6 7b 14 c9 5d cc 6e fe bc 92 96 3c f2 ec 99 24 8f d6 70 34 a0 8a 12 c7 4b 22 42 47 da 28 bc f5 14 46 94 64 fd 20 b7 8a 13 12 0c 4a 22 49 9b 77 76 04 d5 35 89 f9 34 a2 67 4f 07 23 52 be 9e f1 19 a6 c9 f7 ed 49 71 1a 8a 55 20 12 40 4e e3 a2 33 6e 35 18 cd 6d 8e cd d5 f5 fe b8 c0 7b 06 88 b5 64 6a 92 38 cf 7a fa 8a a4 f8 31 b3 78 f2 65 a2 ff 9f 50 cc 96 52 c0 17 55 5a 62 ec 7c e0 a0 0c 9f e8 fc 0a 44 1d bf 80 6c 7e 02 72 16 f8 1b 8f 4f df 7a 91 85 c3 02 00 00<br>Data Ascii: AK0..{s (+EY mm0Md"w'._{ _K<5)y!_]"]5]T2"#A"5H{iZQe4#,Y^4XI(J=W[ n<\$p4K"BG(Fd J"lww54gO#RlqU @N3n5m[dj8z1xePRUZb]DI~rOz                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Jun 4, 2021<br>21:35:05.174473047 CEST | 1282               | OUT       | GET /wp-includes/js/wp-emoji-release.min.js?ver=5.5.5 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.361414909 CEST | 1291               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "3795-5c007b469ca7c-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 4662<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ad 5b 5f 77 db b8 b1 7f ef a7 b0 b9 3d 0a b9 a6 28 52 94 48 51 36 d7 27 76 e2 3d 7b 6e b7 db d3 a4 7b 1f 6c f7 1e 10 00 6d 6d 65 d1 97 22 63 a7 96 be 7b 07 3f 90 14 69 49 4e 9c e6 c1 43 fc 19 0c 06 33 03 cc 00 1e 0d 7e 3c 3c f8 78 3b 5b 1e a4 b3 b9 3c a0 2f 2b 8b ac 7f 23 17 32 67 85 14 07 3f 0e fe 34 18 1c 7c c8 ca 9c cb e9 c1 c3 7d 7f b6 e0 f3 52 c8 e5 e0 8f e5 a0 78 90 77 d9 1f 33 e7 6e b6 70 fe 58 fe e9 13 cb 0f aa a6 38 2d 17 bc 98 65 0b d3 7a 32 ca a5 3c 58 16 f9 8c 17 c6 b1 c2 49 e3 a7 84 2d e5 d4 b8 2d 8a fb e5 74 b0 a1 c3 1e b9 58 38 3c bb 1b 7c 1a 78 be e3 3a ee c0 b0 e5 63 31 35 9c fb c5 8d 61 2f 67 ff a6 61 e1 f0 31 1c 1a 36 9f b3 e5 f2 af ec 8e 5a 30 9c 5a b2 c5 27 99 17 d3 a7 34 cf ee ce 33 21 ff 96 cd 16 c5 b4 e1 45 58 4f 22 36 14 2b 44 2c 8e 8b cf f7 32 4b 0f c4 e9 3d cb 97 f2 97 45 61 0a db 0b ac a9 38 9e a5 a6 38 09 c6 63 3f b0 72 59 94 f9 e2 80 d1 e0 e3 a6 3c 1e 0f a3 e0 c8 34 45 3f d6 58 3f fd e4 b5 96 3d 0e fc a1 7b 64 7a ee d0 ef 09 cb 5a db 45 b6 e1 62 b6 b6 33 92 6a 9e e5 d3 96 70 0a 92 bd 43 f3 cb 45 f1 57 42 ed f5 9e 35 38 b9 bc 9f 33 2e cf 6f 67 73 61 de 98 e8 66 f3 c2 3e f4 2c 5b 55 68 16 b0 df 5a a5 5d 5a 4f 65 af 67 d4 2d c6 61 bd d4 72 b5 32 cb f8 89 b3 f9 3c 61 fc 5f d3 72 5d 2f ca dc 21 96 16 c5 c4 7a aa 16 9f 51 ad 2d 50 a5 d0 d2 4e 6d 1e 0b 5b c6 8f d4 64 b3 38 71 ea 29 4c 49 63 95 3c 69 69 cc 7a 4a b3 dc 4c 0f 66 8b 03 1e 1b 27 b3 bb 9b 03 83 b4 bd e0 ac 30 df 40 9d b1 f1 c6 a6 c1 b5 66 ed 37 c6 c1 1b fb 8d c8 d9 cd 0d 4b e6 32 36 52 36 5f 4a 34 92 10 14 b6 20 1c aa 1d 2c 73 ae aa 4c 55 2d bb 24 16 58 41 2b 4a ca 42 2e 89 65 69 59 a5 73 cb 96 bf 3d 2c fe 96 67 f7 64 25 9f cd d4 ea f5 dc c3 38 4e 9 d d9 42 c8 c7 df 52 d3 20 61 51 63 df 8b e3 98 6f 5a 0f 8c a3 f4 c8 88 55 97 c9 a9 a3 62 99 da 69 e1 6f d4 b4 e5 65 7a 5d ab ca 2c ec 85 05 36 ac e3 36 f6 e0 27 c3 5a 57 52 e4 6b 6b fd 4c 63 d8 19 36 b7 25 ad 21 b1 89 86 9d db 99 3d b3 97 f6 bc d9 4d 07 c2 24 59 6b 5c 60 c6 a5 c3 95 65 28 53 59 da 49 cc 9c b9 5c dc 14 b7 c7 4a d0 c7 49 bf 7f 6c f1 98 5d 26 d7 b6 4f 4b 32 25 b1 b3 20 d4 8f a4 62 eb 34 75 ee cb e5 ad c9 ad a9 47 52 90 ab 95 91 3d 90 85 7e f8 fd e7 f7 73 79 47 06 68 28 45 ad 56 b7 0e c9 b0 30 f5 50 a5 16 a7 c8 fe 92 3d c8 fc 9c 76 b1 69 59 ab 95 30 39 b1 55 ef 8f 74 4d 2b ba bc b6 ec fb 78 de e1 e7 5e f1 03 1b 90 f1 a1 47 dc 8b 8c 97 6a 22 87 e7 92 8e 9b 77 55 f5 82 f4 ad be a6 45 4b 9a 5f de 5f db 05 e9 53 cd fe 3b 9b 97 d2 5e c4 ee f1 2c be 73 e4 a3 e4 66 61 11 4d 32 30 73 19 cf b4 ca 2c 5a cd 82 cc cd 61 f7 f7 72 21 9a ad e3 2c e7 33 52 cf c2 5e 5a f6 a1 6b 59 76 16 cf 2e dd 6b 7b 46 66 9b 59 44 75 79 94 55 fc da 4b 25 d9 da 86 67 a4 1f 7b d6 eb 2d 35 f3 9c 0c d8 cc e3 85 7c 38 f8 e5 8e dd 48 cb a9 36 36 8d a9 4a 76 ee 2c 65 f1 b6 b6 40 d3 68 4c d8 b0 2b 1b b6 ec 94 f0 5b 46 4a ca b6 ac f4 b9 91 f2 ca 48 f9 73 23 3d cc 15 ea 66 0a 85 f8 6c 56 52 ca 25 bf 26 bd 6c 76 94 5a 56 b3 bb 72 75 92 c4 99 62 96 76 cf 92 f6 ef a1 6b 77 c5 96 93<br>Data Ascii: _w=(RHQ6'v={n[Imme"c{?iINC3-<<x;[</+#2g?4]}Rxxw3npX8-ez2<Xl--tX8< x:c15a/ga16Z0Z'43!EXO" 6+D,2K=Ea88c?rY<4E?X?={dzZEB3jpCEWBS583.ogsaf>,[UhZ]ZOeg-ar2<a_rj]/zQ-PNm[d8q)LLc<iizJLf0@f7K26R6_J4 ,sLU-\$XA+JB.eiYs=,gd%8NBR aQcoZUbioez],66'ZWRkkLc6%!=M\$Yk`e(SYIYJlI]&OK2% b4uGR=-syGh(EV0P=viY09Ut M+x^Gj"wUEK__S;^,sfaM20s,Zar!,3R^ZkYv.k{FFYDuyUK%g[-5]8H66Jv,e@hL+[FJHs#=#fIVR%&lvZVrubvkw |
| Jun 4, 2021<br>21:35:05.368179083 CEST | 1296               | OUT       | GET /wp-content/themes/enfold/js/avia.js?ver=3 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.562823057 CEST | 1373               | IN        | <p>HTTP/1.1 200 OK<br/> Date: Fri, 04 Jun 2021 19:35:05 GMT<br/> Server: Apache/2.4.18 (Ubuntu)<br/> Last-Modified: Thu, 26 Oct 2017 18:47:35 GMT<br/> ETag: "1c1be-55c779b01bfc0-gzip"<br/> Accept-Ranges: bytes<br/> Vary: Accept-Encoding<br/> Content-Encoding: gzip<br/> Content-Length: 31241<br/> Keep-Alive: timeout=5, max=95<br/> Connection: Keep-Alive<br/> Content-Type: application/javascript<br/> Data Raw: 1f 8b 08 00 00 00 00 00 03 cd bd eb 7a e3 46 92 20 fa 9b 7a 0a 08 ae 16 81 12 48 49 e5 76 f7 0e 69 96 be 72 d9 1e d7 8e 2f b5 5d d5 d3 3b 2b ab f5 41 24 24 c1 a6 00 0e 00 56 49 96 f8 2e fb 77 5f e0 3c c0 9e 17 3b 71 cb 2b 00 4a e5 b2 7d c6 33 5d 22 f2 12 79 8b 8c 8c 88 8c 88 8c 2e d6 c5 bc c9 cb 22 7a 12 ef dc 0d 76 02 f8 2f 5c d7 59 50 37 55 3e 6f c2 e9 ce 60 67 70 70 70 91 df 04 e7 e9 fc e7 e0 a2 ac de a7 d5 22 98 a7 f3 ab 2c c8 eb 7a 9d 4d 82 ab a6 59 4d 0e 0e ea 06 4a 94 ef b2 ea 62 59 be 1f cf cb eb 83 ff 5c 67 35 02 af 0f 8e 8e fe e5 af ff 72 f4 d9 5f 0e ae cb f3 7c 99 8d ea f4 22 ad f2 11 c2 1c 9d af 9b a6 2c a8 e9 27 d1 fb bc 58 94 ef e3 f1 39 fc 8d c2 55 7a 99 d5 57 e5 fb 30 09 74 47 b3 77 59 d1 c4 c1 dd ce 00 6b e4 17 01 a7 8c cb 2a bf cc 8b 74 f9 15 7d ad b2 aa ce eb 26 5b e8 92 41 fa 2e 4f cf ea bc c9 ce 56 55 b6 2c d3 45 56 45 f1 94 33 37 3b 83 0d fe 96 5e 2c ca f9 fa 1a 9b 19 57 59 ba b8 8d 74 e3 31 15 b8 a3 3a 5c 93 12 f0 bf 77 69 45 4d 9c 97 8b db f9 32 ad eb ac 0e 66 c1 0b 48 f9 a2 2a df d7 59 f5 65 d6 64 0c 65 78 d5 5c 2f 87 d0 de ce 60 f0 64 4c fd 5a 37 f9 32 6f 72 aa d3 4a ba bf 0f ee 36 d0 bb 41 7e 11 05 07 2f 8a 45 55 e6 8b fb f7 d9 f9 0f 6f ee f3 d7 57 65 91 c1 9f 74 01 ff 94 8b fb 2f 96 30 a9 5f 64 55 75 7b ff ea ab ef 68 ba ef 7f 80 e9 48 83 ef f2 22 3f c8 c7 0d 2c 4a 54 40 13 97 69 53 56 63 58 ed ea c5 25 cd e9 de 5e 30 2c 8b a6 5c cf af 60 31 ab 66 18 e4 45 a0 e6 62 ac 7e 7c b5 cc 68 6e 68 e4 83 3b fe d3 1a c7 38 af b9 71 18 50 d0 54 eb 6c ca 05 37 fc 27 5b d6 d9 07 00 b8 48 a1 bc 86 c0 7f f5 cc 1f 1c 00 32 02 72 02 2e e0 60 f0 9f 3a 78 f5 d5 5f 83 11 26 dd c2 c7 a2 2c 86 4d 90 dd 64 f3 75 93 05 0d a0 ae 5a d1 a0 ac e8 1b 46 b4 0e de e7 cb 65 70 0e 4b fe b3 86 0d 33 ee 2d ea 18 30 33 bb f9 e1 22 0a 31 63 74 5d e7 d9 e8 af 61 1c cc 66 c1 e8 28 66 2c ab b2 7a 05 68 9f bf cb ce 10 30 a2 99 d5 db 60 91 cd a1 11 ec e5 55 86 68 18 d4 f9 2f 59 f0 fe 2a 2b 78 00 f5 bc 2a 97 4b ec f6 fb 42 d7 23 c0 5c fe 0c cb 23 50 95 67 03 af b3 06 e0 2d b2 73 c0 c7 eb 14 16 90 86 56 ae 70 b4 2e 30 29 a5 bb d8 01 2d 85 49 7a 97 02 c6 d0 24 c1 66 9e ff 7c 1b d4 eb 73 ac 02 f8 c8 60 28 f5 4c 52 01 90 86 33 00 e2 31 78 1c 90 ab f4 fa 7c 5d 5d 66 55 d7 84 21 09 90 49 09 9a 72 15 58 14 c3 0c 86 b2 cf 20 fb ec 02 e6 a8 67 3c b8 fd 03 bd fd 11 66 be 6a fc 59 f1 29 44 07 9c 79 ba 9c af 97 30 26 c0 99 45 73 15 94 17 c1 1c 76 0e 6c 0b 07 d8 4b 28 f6 92 d3 ff 81 e5 fa a0 01 36 e0 f4 d4 59 5a cd af 60 88 e5 b2 c9 57 ba 40 91 bd 07 9a 80 94 e4 2d e7 44 77 21 21 63 38 09 86 84 84 5c 71 24 15 87 c9 22 6d d2 be bc 80 c8 e5 64 38 5f c2 3a c0 e7 aa 84 11 03 6e 4c 86 e7 25 4c eb 35 24 d5 f3 72 05 74 3d 44 ac 07 d2 9b 36 40 d9 af 26 c3 8c 37 fe 70 e3 ae 8e ea 3d 4c 19 4e 08 c0 6b ea 5f 31 06 ae be b0 3a 6a 8f a2 9d ab 3a 39 96 ac 33 6a 38 09 80 8c 8c ea ab b4 ca 46 e7 e5 4d 47 ef 01 2e 54 b8 9d 1c f6 0c 23 fd 29 bd 91 95 e8 e8 fd 0b c8 7d 43 99 d1 1d f7 60 f8 09 6f 4a 9e 16 c4 f7 00 11 3e 7d 47 73 51 35 17 e5 32 2f</p> <p>Data Ascii: zF zHlvir/];+A\$SVl.w_&lt;;q+J]3]y."zv\YP7U&gt;o`gppp",zMYMJbYlg5r_]"',X9UzW0tGwYk*tj&amp;[A.OVU,EVE37;^,WY t1:\wiEM2fH*YedexV`dLZ72orJ6A~/EUoWet/0_dUu{hH"?.,JT@iSVcX%*0.\`1fEb-]hnh;8qPTI7[H2r.`x_&amp;MduZFepK3-03"1ct]af(f,zh0`Uh/Y*+x*KB#Pg-sVp.0)-lz\$[s` (LR31x[]]]fU!IrX g&lt;fjY)Dy0&amp;EsvlK(6YZ`W@-Dw!!c8lq\$md8_~nL%L5\$rt =D6@&amp;7p=LNk_1:j:93j8FMG.T#)}C`oJ&gt;}GsQ52/</p> |
| Jun 4, 2021<br>21:35:05.758357048 CEST | 1531               | OUT       | <p>GET /wp-content/plugins/ultimate-faqs/css/fonts/ewd-toggle-icon.woff HTTP/1.1<br/> Accept: */*<br/> Referer: http://www.tonhc.org/coronavirus/<br/> Accept-Language: en-US<br/> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br/> Origin: http://www.tonhc.org<br/> Accept-Encoding: gzip, deflate<br/> Host: www.tonhc.org<br/> Connection: Keep-Alive<br/> Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.322705030 CEST | 2419               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "2023-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2774<br>Keep-Alive: timeout=5, max=92<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 9d 59 59 73 db 38 12 7e 9f 5f 41 61 a7 5c 64 4c 53 76 ed 3e 51 d1 a8 3c 89 33 95 da 5c 9b 78 6a 1e 6c 8f 0b 16 21 09 19 8a e0 00 a0 6c af ac ff be dd 38 28 5e 4a 9c ad 54 ca 24 71 74 a3 8f af bf 86 c6 2f 46 3f 05 2f 82 af ff a9 98 7c 0c 7e 7f 1b 9c 57 5a cc c5 ba cc 99 66 c1 59 72 76 96 fc 0b 27 ac b4 2e d3 f1 f8 eb df 38 af e2 09 4c 81 cf 38 f2 4a 94 8f 92 2f 57 da 6f f2 46 54 45 46 35 17 45 40 8b 2c 10 7a c5 64 30 17 85 96 fc 0e 36 97 0a 57 d1 66 39 a3 8a 65 01 cc 85 61 98 13 bc 7f 7b 19 e4 7c ce 0a c5 92 9e c8 44 c8 e5 d8 8d 3a c1 6e 9c 96 3c 69 aa 35 a6 8d 13 8c 61 e2 f8 a7 d1 a2 2a e6 a8 50 c8 a2 2d f1 2f 64 3a d5 8f 25 13 8b 20 63 0b 5e b0 a3 23 fb 37 a1 eb 6c 66 1f c3 2b 62 b7 26 31 49 c6 73 21 99 79 b8 e7 d9 92 69 f3 58 0a c5 cd 66 f8 b2 66 45 45 6e 62 16 a5 2c b4 c6 88 76 61 2d 5b 44 5b c9 74 25 8b 40 24 76 87 90 80 ca 4d 75 49 bc dd 30 a9 60 76 4a ac ed 49 0c 9a d0 2a d7 17 39 83 ed 75 4a 5e f2 a2 ac f4 2f 24 16 25 6e ab d2 2d 2d 4b 56 64 97 22 2d aa 3c 8f 71 bf 37 62 5e a9 74 74 06 8b 73 fa 98 fe f3 f4 34 5e f3 e2 1d 2b 96 7a 95 9e c5 5e e9 74 bb 7e 4c 49 ce 16 3a d0 a2 24 31 d5 ee ed 4e 68 2d d6 24 9e 8b 3c e7 56 9d 42 14 8c ec 62 25 2a 39 67 56 d2 7c 45 8b a5 7f ce 85 72 8f 0b 23 dc 3c 0a 50 cc 3e 49 a6 4a 50 d6 4d 51 8c ca f9 ca 3f e7 6c ae cd f3 0e a6 81 b9 95 7e 0b 41 f1 90 9e c6 78 2e 5e 2c e1 e9 76 2e 19 d5 2c ad ad 19 6d 37 54 06 3c 56 71 11 b3 a9 5e 71 95 30 6b a2 ab d3 9b a4 10 19 fb 40 d7 2c d1 e2 9d b8 67 f2 15 c4 5a 18 c5 7a 4a 34 7b d0 14 f6 02 ef 4f 19 ac 24 c6 9c e6 6d 62 76 e1 ea 3d 98 9b bf 03 f7 4f f5 d3 d3 08 e2 a2 b9 7b 52 4a 51 86 84 ab 57 10 d1 f0 7e 91 71 4d ef 72 46 60 77 9c b6 a1 79 c5 de 33 bd 12 59 5b 2b d8 8b cd 08 0c 93 d4 28 01 81 e2 e4 7d 60 f7 ef 21 72 a6 a3 d3 b8 25 89 66 d9 ab 9c 2a 85 61 72 d2 0c 93 13 ab 73 94 50 ad 65 48 da 11 44 c4 62 e1 95 b9 05 43 35 b7 8c b7 7f b1 c7 4c dc 17 69 33 23 f8 22 1c 38 21 d8 28 fb 58 e4 8f 24 8a d4 b4 98 72 50 6f c2 72 c5 b6 ee ed 6c 82 0e d0 53 91 40 10 c3 b6 af c0 e4 13 75 cf f5 7c 15 32 ff 21 da ce c1 f2 81 4e 3e 9d ff 76 71 fb fb a7 94 d7 a7 bc 5d 8b 0d 0b 49 29 d9 86 8b 4a 7d a2 4b 50 9e 45 93 3b 10 fc d7 a4 b9 ec f5 c7 3f 3e f4 17 16 60 c3 e1 45 6d 31 a0 c9 c5 06 8e b5 17 d5 5f d1 95 b0 5f 83 52 fa f3 2f 3e 5c 5e 7c 4e cd 5c cc f9 84 82 d2 37 10 28 a1 d9 83 25 28 09 96 bf b6 a9 1b 3a 6f 98 a9 36 dc c1 ec 9d 2d 2f cf 7f 1d d8 70 60 5d 47 93 2f af ce 3f 5d 34 56 7a 27 72 08 9b 74 03 c9 6b 62 13 54 eb 06 f7 d3 93 3d ab 09 58 3b aa 99 5c 3b 5d 4d 3e 83 b4 81 c3 78 0d 1c 30 a5 6a 6f 37 9b d7 97 7c cd 44 85 ba ee 76 bb 18 6c 09 3b 28 d5 0d 39 1e 39 34 c4 58 8a 37 82 67 3d 15 8f 8e 46 df 3b 18 24 d5 80 82 b0 fd 48 59 84 f8 d1 00 fd 7f 62 f3 d9 61 f9 83 11 79 28 18 d1 ac 06 02 ba 36 2d bc 4d 0b 6f d3 a0 6f 9e c9 01 5f 39 e0 6e 20 ac 99 68 03 8f 65 6f 35 5b 4f 0d 62 9b cf 5e f5 69 33 8a 60 93 bb bc 92 d2 b5 6c 38 d1 62 ce f2 5f 61 0c 2a ab a1 16 9d cf 69 38 07 42 20 bd 3a 4e 32 6a 08 f8 df 8d 49 2b d2<br>Data Ascii: YYs8~_Aa dLSv>Q<3wjl!l8(^JT\$qt/F?/]-WZfYrv'.8L8J/WoFTEF5E@,zd06Wj}f9ea([D:n<i5a*P-/d:% c^#7lf+b&1l slyiXffEEEnb,va-[D[t%@\$vMu!0`vJl*9u.J^/\$%n--KVd"-<q7b^tts4^+z^t-Li:\$1Nh-\$<VBb%*9gV Er##<P>IJP MQ?!-Ax.^, v.,m7T<V^q^q0k@,gZzJ4{O\$mbv=O{RJQW-qMrF\wy3Y[+{}!lr%*arsPeHD bC5Li3#"8!(X\$ rPorlS@u!2!N>vq l)J}KPE;?>` Em1__R/>V^ Nl-7(%(:o6-/p`jG/?j4Vz'rtkbT=X;\;j]M>x0jo7 Dvl;(994X7g=F;\$HYbay(6-Moo_9n heo5[Ob^i3`-l8b_a^i8B :N2]l+ |
| Jun 4, 2021<br>21:35:06.325464010 CEST | 2422               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=7.4.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.518445015 CEST | 2475               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Tue, 01 Dec 2020 23:42:41 GMT<br>ETag: "183ee-5b56faec69ca9-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 34241<br>Keep-Alive: timeout=5, max=91<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 c5 bd e9 7a e3 56 b2 20 f8 7f 9e 42 44 fb b2 80 e4 11 45 70 27 28 98 37 9d 96<br>5c 59 e5 5c 2a 95 76 96 8b d6 55 43 24 48 c1 49 01 34 16 2d 96 d8 9f 7b 66 7a d6 ef 9b 07 98 3f d3 7f e7 d7 bc 43 bf c9<br>78 5e 64 22 e2 2c 38 00 41 4a f6 bd d3 e3 aa 14 88 03 20 ce 16 27 4e 44 9c 58 6a 8b 2c 9c a5 41 14 1e c4 e6 8c 79 6c 61<br>3d a8 92 c8 0c 59 6a 3d 04 0b b3 e6 4d c3 73 fe 6b 46 bf 6e bc f8 c0 77 0d f9 aa e1 ba e9 fd da 8f 16 07 b1 ff 73 16 c4 7e<br>bd 2e 7e 8c f1 9b b4 5e f7 ad d8 4f b3 38 3c f0 01 68 ad 65 61 79 22 cb 12 51 86 50 03 37 f4 6f 0f 4e e2 38 8a 4d e3 95 17<br>86 51 7a b0 08 c2 f9 c1 75 34 cf 56 fe c1 9f 8c 46 d8 30 fe 64 58 e3 f4 2a 8e 6e 0f 82 e6 2c 9a 43 53 de bc fb fa bb 6f 4f 2e<br>de be fb 78 71 fa ee bb b7 5f 1b 2c d8 20 bc cc c5 b6 bb 0f fe dd 3a 8a d3 c4 79 d8 6c c6 d8 87 69 eb bc 39 f3 56 2b 33 6b<br>8a 47 4c f6 c6 84 4e 8b 96 45 26 bd b6 9f 4f d3 f3 c7 c7 d4 da b0 8c e5 1f c4 8c 0f d9 46 bc 8d 35 c9 87 9b 05 74 00 1b 90<br>3c 67 98 58 ea b6 c6 e9 f1 a2 b9 f2 c3 65 7a 35 4e 1b 0d 2b 32 17 50 ab 35 96 4d d9 98 0f b6 33 cd 1b c9 42 16 5b 0f 46<br>96 f8 07 49 1a 07 b3 d4 18 a7 66 9b 8f a2 ef aa 59 bc 08 c2 d4 8f a3 f5 07 5e d3 d7 fe c2 cb 56 a9 d6 47 98 9d b4 79 71<br>e1 27 6f 68 84 27 a9 f3 30 e7 2f 39 e9 66 63 a6 a6 dd b3 ac b1 df 14 85 cd 8b 4b ef d2 5f bd 8f 56 f7 8b 60 b5 aa d7 8d 2c<br>84 47 41 e8 cf 8d 9a ec df 2c 0a 93 68 05 fd 13 3f 9a b7 5e 1c 16 ef 4c e3 9f 09 d0 d1 5a 40 3a 08 92 83 55 e4 cd 7d 9c eb<br>d8 3f 48 af 3c e8 75 38 f3 e1 0f dc c0 d3 b5 b7 f4 9b 07 1f f1 27 de c5 11 00 58 dd 1f 20 8a cc fd 24 88 e1 ce 3f c2 ee 86<br>08 c4 43 a4 f1 ee 0f ae bc 1b 9f 1a 04 03 e0 03 38 f8 78 71 30 0f 16 0b 3f f6 c3 f4 e0 c6 8f 13 18 a7 e4 00 9a 9d 5e f9 07<br>b2 39 c9 81 07 8d f0 d6 eb 55 00 c0 f8 c7 69 00 18 73 df 3c 78 bd 38 b8 8f b2 83 79 74 10 fa f0 30 8d a8 e1 85 cf 4b 7d 60<br>07 38 4f a5 1e 1f 85 d1 ab 28 5c ac 60 ee 0e 82 30 49 7d 8f 60 5d de af bd 24 21 68 38 50 41 b8 6c 1a 16 db 35 01 6e ad<br>b5 61 0f 76 cf b1 7b ac ed b4 37 e7 f0 f7 29 2c e9 58 2c 35 7b f8 a7 8b 7f 6c 9b fe b6 e8 2f 3d b3 db f4 97 9e 0e f0 cf 10 ff<br>f4 f1 cf 08 ff 74 5a 7d 7e 19 58 58 79 cb b1 5b cc b6 1d db 66 76 db b1 db cc ee 38 76 87 d9 5d c7 ee b2 8e d3 61 f0 be<br>03 ff e0 3a 80 eb 80 75 9d 2e eb 39 3d d6 77 fa 6c e0 0c d8 d0 19 b2 91 33 82 c6 77 b6 1b 0f 58 3d a0 fa db bc 41 6d bb cf<br>2f 3d 7e e1 cf da 2d 7e 11 85 23 7e 19 f0 42 71 e1 df b5 db fc d2 e1 17 9b bf 29 ee 78 0d 6d 01 93 a0 d8 43 3e 32 43 3e<br>28 43 fe 41 47 5c 78 b5 2d 01 45 5c 78 0d 2d 71 e1 a0 5b 1c 74 8b 37 90 0f 60 bb c5 5b d6 e2 f5 b5 44 ab 45 7d 7c 72 86<br>3d 7e e9 f3 cb 80 5f 86 fc c2 1b 38 e2 1f 8c f8 3c 8e 78 3b 47 7c 26 47 1c ca 88 43 19 71 28 23 0e 65 c4 a1 8c 78 b5 2d de<br>95 3e 6f e0 80 df 0d 78 03 fb bc 81 7d f1 0a ef 66 9f f7 61 c0 ef 06 bc 9b 3d 5e d8 e3 df f5 f8 77 3d 5e 43 9f 0f 48 9f bf d9 e<br>7 03 d2 17 35 f0 57 06 fc 95 01 7f 36 10 6d e1 ad e6 77 36 6f 92 2d 0b f9 10 70 0c b1 39 68 9b 37 d0 ee 8b 42 f1 1d 2f 1c<br>88 57 f8 98 f1 da ed 9e 80 c9 87<br>Data Ascii: zV BDEp('7Yl*vUC\$HI4-{fz?Cx^d",8AJ 'NDXj,Ayla=Yj)=MskFnws-..~^O8<heay"QP7oN8MQzu4VF0dX^n,<br>CSoO.xq_.,yli9V+3kGLNE&kOF5t<gXez5N+2P5M3B[FIfY^VGyq'oh'0/9fc_K_V',GA,h?^LZ@:U]?H<u8'X \$?C8xq0?^9Uis<br><x8yt0K}>'8O('0l}')]\$!h8PAI5nav{7},X,5[!/=tZ]~XxY{fv8v}a:u.9=wI3wX=Am/=~~~#-Bq)xmC>2C>(CAG\x-E\x-q[t7 '[DE]}r=~_<br>8<x;Gj&GCq{#ex->ox}fa=~w=^CH5W6mw6o-p9h7B/W |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 10         | 192.168.2.4 | 49799       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|-----------|--------------------|-----------|------|
|-----------|--------------------|-----------|------|

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 2          | 192.168.2.4 | 49737       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.370754957 CEST | 1131               | OUT       | GET /wp-content/plugins/the-events-calendar/common/src/resources/css/tooltip.min.css?ver=4.12.10 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.557161093 CEST | 1142               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 02 Oct 2020 21:43:28 GMT<br>ETag: "662-5b0b705ecf241-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 579<br>Keep-Alive: timeout=5, max=100<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 bd 54 db 6e a3 30 10 fd 15 d4 55 a5 44 8a 11 b9 b0 9b da 2f fb 2b 06 1b 18 d5 d8 c8 76 12 12 94 7f df 31 97 6e db 80 da 7d 59 10 c2 cc 98 99 e3 39 67 26 f6 16 32 49 bc 31 ca 43 d3 e5 27 eb 8c a5 8d 01 ed a5 65 02 5c a3 f8 95 82 56 a0 25 c9 94 c9 5f 59 cd 6d 09 9a 26 ac 31 0e 3c 18 4d ad 54 dc c3 59 32 2f 5b 4f b8 82 52 53 25 0b 7f 8f 3f 44 8f 62 c1 5d 05 b9 d1 8e 80 2e 4c 97 1b 85 c9 7e f0 97 70 b3 c2 68 4f 1c dc 24 dd fe 6c 5a d6 67 ac 24 94 95 a7 5b 59 b3 b3 b4 1e 72 ae c6 f8 35 08 a1 e4 63 06 73 d1 9b cf c6 80 e5 c1 68 43 e4 07 eb a9 e9 32 9e bf 96 d6 9c b4 20 23 c0 a2 28 58 66 5a e2 2a 8e f1 69 12 25 d1 be 69 fb c7 96 19 5f 1d 36 29 de 71 92 ae 87 6d 70 03 5d d2 cc 58 21 2d 41 0b 1b e3 ec f7 fb cf a7 ec 3f 2f c3 29 0f 49 82 c5 6d c9 05 84 af e8 36 49 ce 17 66 1a 9e 83 bf 86 6a 73 21 42 d8 6d 8a bf bd 95 9e 67 ce a8 93 c7 d2 5b ae 5d 61 6c 4d fb 15 12 22 57 24 4d 9e d7 83 67 d8 3d 46 8b e2 a3 63 67 70 90 81 0a c1 2b ac a5 d4 6c c8 bb 4b 13 4c 70 43 86 84 6c e9 cb 78 cd 16 3a 82 d9 52 cf 98 fb 62 cf d8 4f 4d 04 dd 44 f2 0e f3 1a a4 b9 50 58 e4 11 d3 e3 41 47 94 87 a6 5d c0 44 79 81 da 5d 40 b6 e0 1c f1 2d 78 03 ca c1 b5 20 0e 94 b4 97 da d3 a7 27 f6 fe 30 ff 00 3e 56 d8 55 72 56 bf 93 6b 46 c5 93 6b 4e cb 93 0f 15 3d 64 45 79 cd d4 6c 5c 10 05 ce 77 a3 c6 48 48 85 02 fc 62 7b a4 a0 0b 6f e2 fc 55 e1 9e 6b 23 29 4e 8c 7c 96 97 ae 8f 89 82 64 de 34 74 77 5c a4 af cb 8c f7 a6 0e fa 7f 66 6f 3f 0d 43 67 00 46 7e 7d c1 7d f7 cd 66 fd 00 a9 7f 2f 34 d1 26 34 52 64 8d 0f 86 43 2a 64 b9 fe cc 1f cf c3 04 9c 27 70 f2 cd 31 38 f9 66 29 9c 9c c8 e1 34 08 b6 ef 1b b7 5f e2 14 fc 5d 4b 01 3c 72 b9 95 52 47 5c 8b 68 f5 77 90 1c 8e 48 e4 ba fb ef 7a eb 07 c9 fd fe 07 45 16 35 00 62 06 00 00<br>Data Ascii: Tn0UD/+v1n}Y9g&2l1C'eIv%_Ym&1<MTY2/[ORS%?Db].L-phO\$IZg\$[Yr5cshC2 #({Xfz*%i_6)qmpjX!-A?/)Im6lfjslBmgjjaIM"W\$Mg=Fcgp+IKLpClx:RbOMDPXAGjDy]@-x '0>VURVkfNkD=EyIwHHb{oUk#}Njd4twfo?CgF-}}f4&4RdC'd'p18f)4_]K<rRG\hwHzE5b                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jun 4, 2021<br>21:35:04.702899933 CEST | 1172               | OUT       | GET /wp-content/themes/enfold/css/shortcodes.css?ver=2 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Jun 4, 2021<br>21:35:04.903542995 CEST | 1227               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:46:20 GMT<br>ETag: "2c3db-55c7796895700-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 32129<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed bd 6b 73 1b b7 92 30 fc 99 fc 15 78 93 4a 1d db 11 e9 e1 5d 97 da d4 23 c9 96 e3 ac ed 24 be 25 ce 3e 5b aa 21 39 12 c7 26 39 3c 1c d2 b2 cc d2 7f 7f 71 47 03 68 cc 0c 29 d9 8f b6 6a ed 73 62 ce 0c d0 68 34 6e dd 8d be 3c 7e 44 fe e3 5e fe a9 3f 7b fa ea e9 eb e7 a7 f5 ff d7 88 e0 7f c8 a3 c7 f5 7a 7d 71 98 cc 16 ab eb 3d d2 4c e6 ab e5 75 63 94 cd 57 f4 57 e3 6a 19 2f 16 c9 52 7c dd 8c d3 7c 31 8d af 0f e7 d9 3c 39 ba a9 37 e3 cf 69 dc c8 27 f1 38 bb da 0c b3 2f f2 e7 61 3a cf 93 15 89 48 6b f1 85 74 e8 ff 97 97 c3 f8 41 b4 47 e4 ff 9a ad 87 b4 72 fd f1 a3 8b f4 0b b9 4a 86 9f d2 15 b9 98 a6 a3 4f c9 32 9d 5f 92 e1 fa 92 a2 d4 14 1f ce 69 99 4d bd 21 1e 1a 14 93 7c 91 8c 56 e9 e7 e4 90 b4 a2 28 5a 7c 39 d2 1f 87 f1 e8 d3 45 3c 4a 1a 9f d3 3c 1d a6 d3 74 75 7d 48 26 e9 78 9c cc 8f ea b4 bd 61 36 be 26 4d d6 b1 38 9d 27 cb 73 d6 35 22 ba 30 5c a7 d3 71 b2 6c 24 d3 6c 3c 6b d0 da 53 8a c8 66 16 2f 2f d3 79 63 95 2d 0e a3 23 22 9f 86 d9 6a 95 cd e8 8b 9b 8a 00 a7 71 be da ec 5a f9 22 5d 9a da 02 11 dd 93 f8 73 23 9e a6 97 f3 c6 34 b9 58 6d 56 c9 97 95 78 3e 24 ec 85 6e 42 17 5b a6 97 13 bb 1c 7f e3 17 1c d1 81 4f 96 56 49 f1 8a b5 fd 23 c5 82 95 3d 4f e7 13 3a 5e ab f3 51 36 cd 96 e4 d1 86 ff 7b 28 df d2 92 81 82 b1 80 3b 4e 46 d9 32 5e a5 19 05 be 9e d3 de 52 8a 27 47 04 36 90 2d e2 11 1d c3 f3 cf f1 32 e5 25 37 f2 cd 21 9d 42 03 31 83 ee eb 92 7f fb e4 e7 b7 e4 e4 c5 ef a7 ff 79 8f 57 3d 9f 6d e7 6c 38 86 d3 6c f4 69 53 1f 4d 93 78 79 48 e8 2c 9d 1c d5 d9 80 34 26 09 9b 22 74 ad 35 fb bd 64 c6 97 51 f3 62 9a 7c 61 83 b9 9e cd c9 cf c4 05 b2 88 c7 63 ba 78 f8 64 ed b1 f5 79 af c7 e9 94 77 23 bf c7 83 a4 f6 09 86 27 23 6a 43 6c 06 9b 3a d8 14 38 9d d9 d8 dc 67 52 ff fa f4 f8 c9 f3 57 cf ee 31 a9 d9 0e c8 8e 97 34 9e d2 89 1f b3 69 bc a9 5f a5 e3 d5 e4 90 9e 35 3f 1d c9 f5 21 96 87 3a 0a 09 9f f6 47 fe 70 2c b2 3c 15 fb db 32 99 c6 ec c8 12 cb 87 af 97 59 46 0f a8 84 a0 2d de c9 61 87 40 ae 7a d4 d1 66 dc c3 4e 2c 63 7f e5 7b c8 5f 4c b3 78 75 c8 cf 1f 02 0f 2a a7 1c f6 ae b1 8a 69 e7 e5 f6 41 cf 39 49 51 f6 0b 40 e5 7d 9b 25 ab b8 1c d4 45 c6 f8 17 b9 81 cd b3 e5 2c 9e 8a ea a3 75 4e 7b d5 e0 e7 51 19 18 42 77 45 7e b0 11 75 b2 71 10 6e c9 61 b6 a4 44 dd a0 83 9e 7d 4e 96 b4 07 57 65 e3 d3 98 b4 48 08 b0 da 87 3b cd 2e dd 86 6f f0 ea ed d2 ea ed 66 3f 5c bd 53 5a bd d5 3c 08 57 ef 56 a8 5e d0 7a af 42 5f 5e b8 7a bf 42 75 41 3a 7f f0 d2 39 65 c0 f4 10 ba 0b 1b 6e 00 72 59 b0 99 78 d8 ea b1 f5 28 6a f1 8d 39 5f 5d 4f e9 4a cd b3 69 3a b6 3e 48 08 a1 4d 41 6c 19 14 3a 60 6f 5a 3d 3a eb d3 29 e5 b9 0e e3 e9 62 12 3f 90 df fe a3 d5 7b 88 ad 81 c2 2e 11 00 b8 7d 44 50 b8 ed e8 21 5b b1 81 b5 51 19 7c 37 00 be 2b c0 73 de ee 47 c6 ea 9e c7 d3 29 d9 6a 25 ee 11 c1 19 a2 75 e2 c2 af f9 6a 99 cd 8b 01 a8 2e 9e c7 b3 c5 c6 59 f1 0a f1 40 d3 25 0c 6d 51 d5 c3 09 db 1c 34 5f 1b 35 f7 8f 88 07 4d 0a 5b 1e f1 28 99 24 86 74 1b ff 8a 1e 26 7c 23 24 7c 23 64 45 e8 22 a0 4b 80 88 25 b4 9a d0 99 cc 3e 85 09 de 9c 65 b4 23 f3 c6 bf<br>Data Ascii: ks0xJj#\$%>[!9&9<qGh]jsbh4n<-D^?{z]q=LucWWj/R  1<97i'8/a:HktAGrJO2_iM! V[Z]9E<J<tu)H&xa6&M8's5"0lq<kSf!/yc-#"jqZ"]s#4XmVx>\$nB[OVl#=#O:~^Q6{(:NF2^R'G6-2%7f1B1yW=ml8lISMxyH,4&"t5dQb acxdyw#~#jCl:8gRW14i_5?!.Gp,<2YF-a@zfN,c[_Lxu*IA9lQ@])%E,uN{QBwE~uqnaDj}NWEH,:of?SZ<WV~zB^zBuA:9enrYx(j9_OJji:>HMAI:~oZ=)b?{.}DP!{Q 7+sG})%uj.Y@%mQ4_5M[(\$t& #\$)#dE"K%>e# |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.239675999 CEST | 1284               | OUT       | GET /wp-content/themes/enfold/js/avia-compat.js?ver=2 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Jun 4, 2021<br>21:35:05.426983118 CEST | 1354               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:47:35 GMT<br>ETag: "83a-55c779b01bfc0-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 960<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 03 9d 55 51 6f db 36 10 7e b6 7e c5 41 0f b5 15 5b 92 d3 60 c0 30 cf 03 9a a2 c0 f6 90 65 58 fb 52 04 41 40 8b 67 8b 31 4d 0a 24 65 5b 8d fd df 77 a4 24 b7 49 93 ac 9b 61 88 32 79 f7 dd c7 fb ee ce f9 19 44 03 57 0a 0b 95 c1 2d 2a 67 81 eb 0d 2c a5 28 d6 68 84 5a c1 52 1b 40 89 9b 70 56 0a ce 51 c1 4e b8 12 ee ed 04 14 22 b7 e0 34 2c 10 74 ed ac e0 b4 2e 3d 44 66 90 f1 06 02 66 c6 a4 d5 c0 38 99 5a da 30 4c 02 ee 9d 61 50 48 66 2d da 10 63 81 ce 21 2d 46 ef 2c ad b6 ae 2a 6d 5c cf 8e be 8c 9c 2b 66 98 43 58 0a 89 e0 4a e6 1e 11 90 9a 71 e4 40 bb ae a4 63 5d 79 2a fe b5 62 2b cc 40 d3 ab 21 d6 b0 ac 55 e1 84 56 04 69 4e 5e 0b 24 12 18 cc 0b a9 ad bf f9 42 d3 05 1c 5b 79 f8 0d 5b b7 87 56 50 7c 83 8a 13 d6 92 59 a2 1c 9d e5 51 5c 5b 3a 72 46 14 2e 8e a2 2d 33 c0 b6 82 dd 09 7b b7 d1 0b 4f 76 4e c6 d2 e2 2c 12 cb 11 e4 ef 14 37 5a f0 c3 0e 17 d7 1f 0f e2 af 52 2b a4 85 71 7a 68 7e b8 94 ac 58 5f a2 31 cd e1 8f 0f 57 01 e0 70 5d 51 de e0 4a 28 91 8b cc a1 75 23 45 21 56 cc 69 93 51 70 f3 6e 45 89 4e e0 cd 1b 18 6a e5 74 5d 94 d6 31 e3 86 20 14 c9 51 d4 5e bf ac 7f f9 d0 ea 99 44 0f d1 e0 3b a2 ce d4 c4 73 f0 92 53 16 44 fb 93 6d 10 c6 73 18 b6 17 ed 9c 87 b3 e8 18 21 dd d3 03 ff 27 00 8e 76 ed 15 0b 08 3f ea 79 6f ef 18 29 b9 0d 81 a3 51 af eb 28 a1 e8 79 6e 91 0a c1 30 65 49 d8 0d 95 b7 a6 0c ba 26 02 fa 78 81 a8 de 97 62 4f f7 bd 19 a6 a4 c3 5a b8 74 38 19 a6 1b fd 85 56 a0 17 eb d7 38 be 9d 7c 83 32 a7 8d 59 80 f0 25 3b f2 38 c2 67 b8 05 4b c2 c9 03 84 85 18 40 e9 5c f5 4b 9e 93 0e b6 c9 56 d4 34 f5 22 13 3a 5f 48 bd ca df 4e cf df e6 e7 d3 fc fc e7 dc ea b4 d1 75 ba 63 ca a5 4e a7 5c a7 2c 2d ac bd 48 2f 78 7a 8a 9d b7 a8 54 3f 6d b0 1b 71 3b 1e 9e 4e 5f d5 39 b3 ae 91 98 74 bc 1e 5e b6 7b 94 df b8 55 e6 eb e5 e3 d9 a3 4c 3c 4b e3 f8 1c 4b 4a bc ad 30 28 f5 43 3c ff 1f bf 0b ee 19 46 83 63 34 e8 e5 f7 e3 42 4a b6 87 8a 3a da 97 86 6f e5 6e d0 c1 7d bd a9 fc b0 f0 d3 c1 0f 81 c8 b3 76 4d 85 61 80 75 0c 56 d8 07 b7 97 cd fb 53 f8 39 95 5f 5f 6e 43 df 74 4f fd 9e 32 27 9c 4b 5d 2b 4e 73 e5 bd 14 b4 f3 37 e5 c3 c3 c4 3d 4c ec 61 9e 36 63 37 36 92 68 40 25 1d f8 9d 04 f0 e6 3b a1 b8 de 65 42 29 34 bf a3 58 95 0e 7e 83 29 59 07 f3 01 a5 e0 93 d8 20 0d e6 c7 bd 41 1f 5f b9 0d 89 38 9d d0 90 5c 92 a1 a5 1f 0f c7 ae d6 3f b7 27 a7 f4 cd ff 2d 21 a3 98 6d d3 de 3c 4e 26 21 06 b1 fb 44 2d 3d ef 69 fa 44 7f be 0e d1 e0 70 78 a5 0a 0a a3 a5 24 d7 59 80 09 8f d0 6e 81 f0 8c 78 ff 7a a2 96 49 54 2b 57 d2 e6 78 9c 40 7b b7 41 7f 78 d3 dc b6 25 95 b9 c0 23 9e 56 fb b8 05 1d 74 b7 1e cc e1 5b eb 67 65 1a 25 9d 4f 9b 1b 72 b9 62 ae cc 0a 14 72 04 a3 67 34 18 43 77 f5 b4 4f ae 27 90 c0 19 4c b3 0b e8 d0 7c 9f 7c 47 f4 e6 a4 ef ad e7 1b 7e 49 fa c7 1b 11 73 1a 46 e3 96 c1 38 ae f6 49 fc 0a 4c 7f 5f 56 3b fd 82 dd 93 51 8a 8a 2d 24 f2 93 86 7e a2 7a b7 a3 7f 52 59 fc 34 0d b4 8f be bd 8e 89 cf c8 3f eb 8e 47 23 3a 08 00 00<br>Data Ascii: UQo6~~A[`0eXRA@g1M\$e[w\$la2yDW-*g,(hZR@pVQN"4,t.=Dff8Z0LaPHf-cl-F,*ml+fCXJq@c]y*b+@!UUViN^ \$B[y[VP]YQ[;:rF.-3{OvN,ZZR+qzh~X_1Wp]QJ(u#E!ViQpnENjt]1 Q^D:sSDms!v?yo)Q(yn0el&xbOzt8V8j]2Y%;8gK@!KV 4":_HNucN\,-H/xzT?mq;N_9t\UL<KKJ0(C<Fc4BJ:on)vMauVS9__nCtO2*K]+Ns7=La6c76h@%;eB)4X-)Y A_8?-'!m<N&! D-=iDpx\$YnxzIT+Wx@{Ax%#Vt[ge%Orbrg4CwO'L  G~!sF8IL_V;Q-\$-zRY4?G#: |
| Jun 4, 2021<br>21:35:05.429833889 CEST | 1354               | OUT       | GET /wp-includes/js/mediaelement/mediaelement-and-player.min.js?ver=4.2.13-9993131 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.631339073 CEST | 1411               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 15 Nov 2019 22:36:20 GMT<br>ETag: "272c5-5976a3a1a7e8e-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 39664<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed bd 69 63 db 48 76 28 fa fd fd 0a 0a 2f 23 03 2d 88 22 65 bb 17 50 30 af da 96 d3 4e bc 3d 4b ee 99 5c 36 a3 40 24 28 a2 0d 02 1c 00 d4 32 22 f3 db df 39 a7 16 54 01 05 2e 5e 3a 9d dc 3b 8b 05 d6 be 9e ad ce 72 f4 dd de ff d3 fa ae f5 26 1c 47 c1 59 1c ce c2 a4 68 ff 9e 63 d2 b4 28 e6 de d1 d1 ed ed 6d 7b 86 b9 21 cb fd 3d 6f 8f d2 d9 11 94 c0 42 7f cd 82 f9 3c cc 5a c5 34 28 5a b3 68 16 8d f2 56 12 14 d1 4d d8 fa e5 e2 cd eb a7 5a c3 2d 3b 58 8c a3 b4 15 24 e3 d6 4d 34 0e 53 07 9b 58 ea 51 72 dd 0a 5a 37 41 16 85 c5 7d 2b 9d b4 8a 70 34 4d d2 38 bd 8e c2 bc 65 cf 17 59 d8 fa 97 e0 26 38 1f 65 d1 bc 70 5b 2f e3 20 9f ba ad 68 92 05 b3 d0 e1 23 79 9e ce ef b3 e8 7a 5a b4 8e 3b dd ce 21 fc f3 83 db fa 97 74 9a b4 5e dc c3 00 6d 3e 9d df db d3 e4 88 fa 7d 1d 8d c2 24 0f bd d6 9b 57 17 ac 8d a3 ff 67 6f b2 48 46 45 94 26 ad cc 0e dc dc 8d 9d 07 99 32 b6 0b 37 74 1e a2 89 bd 97 0f 8a 21 fb 0a e8 0b 86 de 4a 7c 4b 14 b5 7c bf b8 9f 87 30 91 2c fc fb 22 ca c2 fd 7d fe d1 c3 3a f0 33 71 b2 b0 58 64 49 2b 81 46 f7 3a 0e a6 2f 44 da 82 a7 61 ab a9 9f 84 b7 ad b3 2c 4b 33 db 7a 1e 24 49 5a b4 26 11 ac df 2c 1d 2f e2 b0 f5 c8 3a 28 0e ac 47 96 d3 2b a6 59 7a db 4a 61 73 c6 a1 6f bd 79 f7 e2 e3 eb b3 cb b7 ef 2e 2e 5f be fb f8 f6 85 e5 a6 2b 6c 2f f2 71 ec fe 43 78 37 4f b3 22 f7 1e 56 ab 1e ce 61 d0 19 b6 47 41 1c db 51 9b 67 b9 62 36 36 4c 9a 8f 6c 6c 53 d9 ee 70 10 0e 97 cb d0 59 b9 91 5b 56 c8 5c b6 64 2b 5e 1a 7b 12 99 ab 09 4c 00 07 b0 d8 66 99 dc d0 ef f4 c2 93 b8 1d 87 c9 75 31 ed 85 07 07 ce d8 8e a1 57 a7 27 86 b2 b2 1f ba de a0 1c a4 5b b8 89 f3 b0 72 1f 56 43 f7 58 c9 88 60 5c 30 03 5b 9d 0e 0e 04 8a fb 37 69 34 6e 75 f6 7c 3f ec 87 9e b5 48 c6 21 ac 6d 38 b6 f6 c4 c0 6e 61 a9 d3 db 3e fb 03 8b e5 a6 7e 64 77 9d 9e a9 ec 38 1d 2d f0 94 f7 0b 5f 7c 7 a 76 e1 27 03 eb f2 f2 9f 5f bf fb f9 f4 f5 e5 8b 77 cf 3f be 39 7b 7b 71 f9 fc f4 f9 2f 67 ff eb 89 35 74 96 cb 8d 65 fc d4 71 33 b1 90 7e b1 72 d8 4e 15 d3 28 77 4d 03 b9 8e d3 ab 20 ee b3 3f c6 69 e5 61 3c e9 e3 3f 5b 4d 1a b6 19 96 ba 0b eb fa 58 5b f0 c4 2d 4c eb da 2b fc cd ad 6e 5c f9 72 88 b0 ea c9 7f f1 ec 61 ea 4f ea 67 8d ee 27 dc 80 cc 2f e4 f8 1e 56 3d 09 30 02 db 79 60 b7 52 b9 c3 79 58 5c 44 b3 30 5d 14 ad 69 00 b0 12 ee f3 55 18 c2 79 e6 e3 70 56 b2 7e 6e aa 3f 8a c3 20 db b6 05 58 26 02 53 a9 ef fb 65 c7 02 ce 94 29 00 70 18 0c a2 92 c1 72 b9 97 3a fb fb f5 1a a9 d2 8a 5b ad 5e 64 f7 02 4e a4 94 b2 1a 05 c5 68 8a e7 42 cd 62 db 97 2c e2 d8 d5 0b e9 05 68 7f a9 c0 6a 25 a1 b2 cd 9a 4a 4d 30 a4 1c 4e bf fc f4 82 b2 fd d4 0f 56 58 3b 32 d5 56 97 b5 af fe f0 f2 b2 05 00 9e ab 95 cd 00 f3 d8 5d f8 83 a1 3b f2 f7 ba ee c4 3f ec 96 db 3e 87 51 8e f6 f7 c7 fb fb 36 e5 8e 39 14 eb 2f fc 31 40 e7 04 9a 03 58 ef 61 25 77 c1 f3 f6 f7 67 b6 a3 6c 1c fc 22 f4 32 62 a7 2c f4 63 7b ee f4 a0 b9 4e 4f 00 d2 c2 17 95 7b 45 0f d0 14 24 8f fd 05 8d aa 77 70 30 39 81 44 18 c2 78 30 19 b6 b3 05 ac 5c 8f 3a 2c 6b ad c6 3e 6d 02 9b 81<br>Data Ascii: icHv(/#-"eP0N=K!6@\$(2"9T.^.;r&GYhc(m[!=oB<Z4(ZhVMZ-;X\$M4SXQrZ7A}+p4M8eY&8ep[/ h#yzZ;!t^m >}\$WgoHFE&27t!J K 0,");3qXd!+F:/Da,K3z\$!Z&./:(G+YzJasoy._+!qCx7O"VaGAQgb66LI!SpY[V!d+^{Lf!1W'[rVCX `0[7i4nu] ?H!m8na>~dw8-_ zv'_w?9{[q/g5teq3~rN(wM ?ia<?[MX[-L+n!raOg/V=0y' RyX\ID0]iUypV~n? X&Se)pr:[^ dNhBb,hj%JM0NVX;2V];?>Q69/1@Xa%wgl"2b,c{NO{E\$wp09Dx0!;,k~m |
| Jun 4, 2021<br>21:35:05.645381927 CEST | 1453               | OUT       | GET /wp-content/plugins/jetpack/_inc/build/carousel/jetpack-carousel.min.js?ver=20190102 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.838049889 CEST | 1580               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "6e09-5c3db85dd1b89-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 8035<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 d5 3d 69 77 db 46 92 df f7 57 50 48 42 01 66 13 24 65 3b 8e 49 41 5c c7 4e 66 f4 5e 3c ce c4 9e 9d 9d 67 6b f9 5a 44 93 84 0d 02 1c a0 a9 23 12 ff fb 56 f5 85 c6 45 51 d9 4c e6 ed 1c 16 d0 47 75 a1 ba ba ba aa ba aa 39 78 d2 79 93 76 92 94 77 d6 69 18 2d 6e 3b 7c 15 e5 9d 45 14 b3 4e 18 65 6c ce e3 5b bf 73 ce 3b 50 38 4f d7 1b 28 0f 3b 8b 2c 5d 77 52 be 62 99 68 98 fb 9d 27 83 ff 18 3c e9 2c e3 f4 92 c6 9d cf 8c 6f e8 fc cb 6b 9a a5 db 9c c5 ef 79 16 25 cb 9c c0 38 f3 ed 9a 25 fc 43 ba 9d af b0 cb e7 bf 6e 59 76 eb 86 aa dc f3 33 46 c3 5b 77 b1 4d e6 3c 4a 13 97 79 77 57 34 eb 70 42 49 44 52 92 93 8c 24 24 26 73 12 92 0d d9 92 35 59 91 05 59 92 cf e4 8a 5c 93 59 30 1a 0d c9 4d c0 5c e7 32 0d 6f 1d cf 9f e7 b9 eb a4 57 2c 5b c4 e9 b5 e3 91 4b ac 5b f1 75 dc 50 77 1b 38 ce e4 3a 4a c2 f4 da 8f 92 84 65 7f 8f 42 be 3a 0d 5e 7c 3b ec 76 dd 59 f0 96 f2 95 0f df 93 84 6e ad d5 00 1a 3d 81 c1 3d ef f4 19 b6 76 d2 84 e3 27 e6 9c 66 dc 89 92 8e ec 71 7f af 7a 96 e8 d0 ed ea cf ef 44 09 f4 48 e6 2c 5d 94 49 e5 09 0c 86 1e b9 4a a3 b0 33 0c 82 e0 0d e5 cc 4f d2 6b a8 d0 8f 81 a1 9a 77 97 31 be cd 12 37 61 d7 1d ac f6 fc 25 e3 1f a2 35 73 bd 9d 37 41 8a 7e 09 6c 1a e7 d7 11 9f af 5c e6 5f af 22 18 ed 6e 4e 73 d6 79 fa dd 98 f9 9b 8c 5d 01 16 6f d8 82 6e 63 ee 7a 24 f5 f3 79 96 c6 f1 87 74 e3 da cf 5e 7f 34 1c 7a 93 4b 98 c0 2f 13 d1 ff d9 f0 51 fd 7b d5 fe 4f 5f 36 f5 8f fc cf 9b d9 5c 31 96 eb 24 ec 86 3b e5 6e 2f c6 e2 6f 23 f6 95 de 58 1f c1 73 19 c2 c9 8b 66 c4 4b 5d e7 71 9a 33 c7 db ed c8 7b 9b f0 f3 98 d1 0c 29 9d 6e b9 1b 7a 24 0c 72 49 79 7c b7 da 55 10 c9 e3 28 64 80 46 b9 74 11 f1 f7 58 e1 90 a3 61 0d f7 ed 26 84 99 15 f5 3f a7 79 84 70 f3 c6 86 00 e5 2d e3 54 d4 ed c8 c9 10 ff 7d 6d e3 0c 6b 82 76 a2 f5 f2 23 00 a4 7d ca 39 9d af 90 f5 fa 51 78 01 28 31 78 b5 51 17 0b 12 16 12 8a 09 cf df d0 0c 9a ba de 24 5a b8 47 5c bf 3a fe 92 c6 31 2c ed 7e 34 4f 13 00 12 b3 64 c9 81 d5 25 03 1f 05 d8 df f3 61 ac 0c 16 64 c6 16 8e 27 01 d3 e0 68 34 a9 d5 f9 f9 26 8e 00 ea d4 f1 3e 0e 2f 82 c0 8c 2e 1b 09 bc d3 2c 5a f6 51 18 55 9b 77 bb 23 e8 f1 97 ed fa 92 65 6e b3 64 f2 73 f8 37 66 b3 68 4d 97 6c a6 50 9f ad 59 1 8 d1 19 82 c4 f5 07 98 01 6d 6b a8 35 23 b3 61 d9 9a c6 51 f2 c5 29 ba 52 78 92 dd c3 f0 75 4c 51 fc c8 61 fb 62 d8 be 1a d6 51 83 20 1c 60 33 85 68 1f f8 3c 83 39 bc bb 8c d3 e5 2c 0a c7 fb bf 47 b5 82 d5 0e 1c 0a f3 7d 1e dc 71 96 f3 1f d3 0c c4 01 1d 9b d9 e4 5a 54 1c b9 47 ae 98 54 4f cf d5 fd 3d 4c 67 23 12 00 93 20 b4 f3 c5 bb 0d 4b 58 38 ae 09 9e 23 d7 08 aa e8 fe be 78 f6 53 d1 01 40 eb 47 00 85 0f ef b2 f7 2c 86 ad 46 b0 73 09 3d 4d dc 12 4b db a3 3b de b4 ba 98 0a 50 af f8 79 12 b2 1b 87 70 6f dc 08 09 07 07 aa 0a 41 3d 8b b0 ed 98 ef 14 52 05 1e a1 64 ce 75 70 17 71 b6 ce 67 72 84 34 1b 5b 7c 0e 15 9d a6 15 44 3a 3e c7 3d b3 7f 40 cb b6 45 48 6c fc 86 3b b2 32 3c d7 3c 41 b8 18 61 b1 95 04 0e 2e 4f ef 0e e7 d8 39 0d a3 ab b3 d3 01 fe eb d8 ec f8 79 d3 37 90 70 67 8c a9<br>Data Ascii: :=iWFWPHBf\$e; A Nf^<gkZD#VEQLGu9xyvwi-n; ENel[s;P8O(,; wRbh^<,oky%8%CnYv3F[wM<JywW4pBIDR\$ \$&s5Y\Y0M\2oW,[K[uPw8:JeB:*];vYn==v'fqzDH,]IJ3Okw17a%5s7A- _,"nNsy oncz\$yt^4zk/Q{O_6!1\$;n/o/#XsfK}q3 {}nz\$!ry U(dFtXa&?yp-T)mkv#}9Qx(1xQ\$ZG\;1,-4Od%ad'h4&> /,ZQUw#ends7fhMIPYmk5#aQ)RxuLQabQ `3h<9,G}qZT GTO=Lg# KX8#xS@G,Fs=MK;PypoA=Rdupqgr4[[D:>=@EH!;2<<Aa.O9y7pg |
| Jun 4, 2021<br>21:35:05.841454983 CEST | 1588               | OUT       | GET /wp-includes/js/mediaelement/mediaelement-migrate.min.js?ver=5.5.5 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jun 4, 2021<br>21:35:06.028692961 CEST | 2240               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "4a9-5c007b469ca7c-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 544<br>Keep-Alive: timeout=5, max=95<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 85 53 4b 6f 9c 30 10 fe 2b 04 55 2b ac 75 d0 f6 ba d4 ca a9 ab 5e aa a6 af 13 5a 45 2e 0c e0 d4 d8 c8 36 9b 20 c2 7f ef 18 96 7d a5 d9 70 80 99 f9 e6 f1 cd 83 9b a2 55 99 13 5a 45 9c f4 3b 2d f2 60 c5 18 ab e1 d1 c6 8d 6c 4b a1 ec 62 11 9d aa ac 1f e8 a9 1e 5b 21 77 60 a4 28 2b c7 d2 ed 9b 58 dc b4 b6 8a 7a d7 35 60 d7 e9 76 20 64 72 fd e2 6a f9 15 72 c1 3f 4b a8 41 b9 9f 95 a8 d9 9b c8 cb 4b 5f 82 fb 85 49 36 46 d7 1b 21 61 3d fa fe 76 42 da f8 02 1a e8 79 43 63 b2 0d 70 d7 1a 38 b4 75 66 9c fc 66 8d 5c c4 fb 22 c2 75 73 e4 5e 3d 62 96 24 3b 6e 02 60 a7 ac ef 25 ef c0 c4 8d d1 4e fb e6 63 a1 84 4b de f5 60 87 bd 90 de 55 c2 c6 ba f1 9a 8d 33 c9 ad bd 37 50 88 67 16 fa d2 b7 21 1d 1d 3e d4 3e 27 9b 64 a5 73 60 3c 1a 15 2f 13 0a 71 c6 a5 1c 2d 64 18 79 ba eb 3c 1f 6a f8 01 3c ef ae 73 9d bd 5e f1 cd b4 72 5c 28 30 33 8d 83 81 d0 83 6e b4 b4 a7 b8 d7 f7 f0 58 e8 00 4e 1a 42 31 6f 1a d9 8d 46 ca 4d d9 7a 52 d8 10 bd 4a 12 ef 62 0f 1d 69 02 e9 0d e0 9a 55 30 2d f9 86 31 be 58 40 80 67 eb b8 ca 40 17 01 bf 83 74 b5 5d c3 3b d9 ff b4 42 e6 c5 7c 41 c7 02 d4 51 41 2d e9 0b 6d 22 3f 6f c3 d2 b0 c1 e0 86 b7 16 42 1a 66 ad 31 98 0f 25 cc 55 62 ac 45 31 6f 0d f7 e1 28 3a c3 b3 bf de b6 d3 12 fb 44 a1 68 a5 b4 99 01 50 e1 96 4a b6 a2 8a 9d dd c6 4c 22 96 a0 4a 57 25 f2 93 4a e4 72 89 3f 36 96 d7 ff f7 4d e5 36 11 c5 38 d0 34 1c 5b 09 97 7a 4b 9c e9 fa db 8f 78 f9 06 cf 31 87 e7 6f 45 a4 c9 dd 85 17 f6 88 fb 21 f8 12 04 3b 5d bf 86 a7 11 0c 19 77 59 e5 47 8e 4b b6 5a 42 0c c6 e0 54 c2 f1 13 8c 01 42 95 01 06 51 20 03 3e 51 f4 84 65 f5 13 7d fc de 82 e9 08 49 fe 01 8b 8b 4a 07 a9 04 00 00<br>Data Ascii: SKo0+U+u^ZE.6 }pUZE;- Kb lw'(+Xz5^v drjr?KAK_I6F!a=vByCcp8uffl'us^=b\$;n%'nNcK`U37Pg!>>'ds</q-dy<j <s^r\(\03nXNB1oFMzRJbiU0-1X@g@tj:B AQA-m"?oBf1%UbE1o(:DhPJL`JW%Jr?6M684[zKx1oE!;jwYGKZBTBQ >Qe)IJ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.036482096 CEST | 2325               | OUT       | GET /wp-includes/js/dist/a11y.min.js?ver=28ae883082d3cc947b58ed059ff407a7 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jun 4, 2021<br>21:35:06.226697922 CEST | 2416               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "bfb-5c007b46a283e-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1167<br>Keep-Alive: timeout=5, max=94<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 e5 55 cd 6e db 46 10 be f7 29 28 02 25 b8 31 45 4b 81 1b 04 a4 d7 46 13 f4 d0 43 93 a2 c9 cd 70 83 15 77 24 6d 43 ed 12 cb a1 64 41 e6 bb f4 59 fa 64 9d e5 8f 24 ca 32 6a 9f 0b 08 e2 72 fe 76 e6 9b 6f 86 97 6f 46 de d7 a5 2a bd b9 ca c1 a3 a7 a8 d0 8c 17 a0 c1 0a 04 e9 bd b9 fc 01 49 1d 6f 0a de 3d 1f 1f 77 75 d4 9d 63 31 9d 6e f9 bc d2 19 2a a3 43 64 bb b5 b0 1e f0 5d 9d f6 42 4f 87 96 ed d4 3c 84 3b 7b cf 2c 60 65 b5 e7 ce 31 3c 14 c6 62 99 3a 17 c5 9d 88 ef 54 62 a3 3c 19 4d a3 4e 99 ec ea 3a ed 9c d0 39 65 22 cf 43 d5 fb 46 2a 3a 9c 35 a3 97 9c 8f 26 07 59 dd b9 ea 78 c5 31 d2 71 c6 81 fe e5 51 c6 11 44 94 9e 8e 8d 3b b2 c7 c7 cf b3 bf 20 c3 58 c2 5c 69 f8 dd 9a 02 2c 6e 1b b3 1d e8 6a 45 a8 cc 72 48 e8 8e 05 60 62 6b 56 53 3c 3b 40 c0 af 74 eb 2d fd 11 c7 6d 01 66 ee 7d d9 ae 66 26 0f 82 f6 19 a3 f9 82 56 e9 c5 57 b1 08 82 e7 6e 7c 6a 1b 11 ba 79 05 89 ff 9b 91 55 0e 7e cd a2 e7 9c fd 6f df a0 ec cc 7a b7 d1 a4 4d 17 07 e5 37 bd 99 06 10 04 21 72 57 00 8b de 07 d0 37 0a 53 d2 5e 39 ad 6f 9a ab 7c de d7 84 41 e0 7e f1 e1 a6 83 93 6b a9 e5 5d 72 99 05 a2 52 a8 ab 3c 67 2e 1c 01 46 94 78 26 75 1b f9 24 11 55 8e fe 29 e2 6d 15 48 55 bf 6d 12 2a 1b 5c 0e 20 23 9b 1b 1b 36 6c f2 14 65 c1 a8 d3 14 4f 45 fb 72 a9 d8 3d 97 e0 be 8e 67 4a cb 26 af 48 31 d6 d3 cc 3a 8c f4 19 52 9f 54 7b bb b7 38 44 8d bb dc eb e4 8c 72 4f 64 97 17 44 be f0 09 fd 08 dc 75 e6 a4 25 9d 61 07 51 61 0d 1a 57 64 bc 14 e5 e7 8d ee c1 6a 87 c1 39 b8 18 05 f7 fd 48 13 ba 25 bf 7a 77 c5 ea 70 37 4d 86 51 47 47 49 61 3f 22 fd 58 c7 6a fa 5e d7 21 85 7a fb ee 75 8e d2 ac fe 00 21 b7 8d 33 5d 3d 70 a6 a9 a4 89 28 c1 73 dd 22 fa a4 ae fb 54 76 87 41 49 85 16 7e 14 3e 85 ab a8 d9 c1 aa 00 f1 fd ac 95 24 ab 8e 6d 3a a4 c4 69 05 70 ea 9e e3 97 21 c9 94 1d f6 90 08 db 46 22 17 76 41 bc d2 58 c6 39 e8 05 2e 6f 26 41 b0 36 4a 7a 93 11 3f 28 ef 26 f7 b7 c7 2f 89 5f 98 5c 21 cd 13 70 69 b4 de 71 fb 97 1c dc 5b e8 4b b5 f6 59 0a b1 92 dc 77 ab 71 dc 64 3e f6 e3 cc e8 4c 20 71 29 82 38 cb 45 59 7e 12 2b 18 d8 58 58 50 96 14 3c 26 4c 7e 46 42 6b 56 d1 d4 10 cb b7 6e 86 e9 f2 52 b9 3a 12 4f cc 4a 93 93 2e 5d 51 7a 8a 04 e3 69 f1 90 16 42 4a 1a 87 c4 9b a4 4b 50 8b 25 26 9e 13 6f 94 c4 65 7b 34 6b b0 f3 dc 6c 12 6f a9 a4 04 9d 66 b9 2a 12 cf 12 c5 42 d2 47 de e0 8f a5 e3 0d cc be 2b 1c 3b b3 71 21 5c 18 a5 29 b9 f0 a7 c9 8f 2c 3d 2f 9d 19 2b c1 ba 24 36 74 1a 6f ac a0 1b b4 b1 2b 91 7b 23 b5 72 c4 11 1a 53 9f 3d a9 53 58 25 c6 b9 5a 53 ad f8 8c d6 42 0e 6b 72 27 34 5c b1 0e 8d d2 43 78 c0 e7 c2 09 34 2b 95 91 39 da 0a fc 96 28 7a df bc 88 38 13 cf 8c dc ee 27 3f 08 6c 2c 8a 02 b4 fc b8 54 b9 0c 9b f1 74 4e 15 cd d6 81 49 c5 9e 49 7b 1e d0 d7 a0 23 c1 87 ed af 32 3c 6e ac d2 68 cd b8 4f f3 45 2e c4 0f 9a 6f 87 05 8d c0 8b 3c 3a 6a b2 d4 6d 33 ce dd ae 3a 1a 96 93 64 4f 48 5b 90 1b 9e 52 f6 28 eb 08 9f a1 ec d0 c6 3d 3f 1a 8d 14 b3 db fc a1 a1 75 c9 42 ff 93 41 35 57 c4 7f d7 30 2a 09 ff 27 14 3f ad b3 cd 89 0a ed 0e 2d 21 8f 28<br>Data Ascii: UnF)(%1EKFCpw\$mCdAYd\$2jrvoof\$lo=wuc1n*Cd]BO<{,'e1<b:Tb<MN:9e"CF*:5&Yx1qQD; Xi,njErH`bk VS<:@t-mfj&VWNjyU-ozM7!rW7S^9o[A~k]rR<g.Fx&u\$U)mHUm^ \ #6leOEr=gJ&H1:RT{8DrODu%aQaWdj9H% zwP7MQGGla?"Xj^!zu!3]=p(s"TvAl->\$m:ip!F^vAX9.o&A6Jz?(&/_\lpiFq KYwqd>L.Q)8EY--+XXP<&L-FBkVnR:OJ.]QziB JKP%&oe{4klof*BG+;q! ),=/\$6to+{#rS=SX%ZSBkr4\Cx4+9(z8'?l,TtNII{#2<nhoE.o<jm3:DOH[R(=?uBA5W0*?~!{ |
| Jun 4, 2021<br>21:35:06.228796005 CEST | 2417               | OUT       | GET /wp-includes/js/dist/dom-ready.min.js?ver=ad4d8022261fd9f054a02278eda7c864 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.413465023 CEST | 2440               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "4c3-5c007b46a283e-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 596<br>Keep-Alive: timeout=5, max=93<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 75 54 c9 6e db 30 10 bd f7 2b 64 1e 04 31 60 99 05 3e 14 32 88 1c da de 1a b8<br>68 72 2b 82 40 96 c6 8e 0a 9a 14 a8 91 53 43 e6 bf 77 28 6b a9 9d 18 30 4c 7a 66 de 2c 6f 1e 7d 7d 35 8b 9e 5e cb 3a 5a<br>97 1a 22 3a b3 06 ed e7 0d 18 70 19 42 11 5d 5d 7f 42 72 cb b7 4a f5 e7 e1 d0 7a d1 df 65 61 b7 bf 20 2b f6 6a dd 98 1c<br>4b 6b 12 e0 ed 2e 73 11 aa d6 2f 06 63 64 12 c7 db 72 9d e0 6f f7 cc 1d 60 e3 4c 14 ee 12 fe 56 d6 61 bd 08 10 ab 82 49<br>b5 65 ea 84 4e 67 b7 a2 77 a6 ad f7 8b 1e 04 01 94 67 5a 27 76 c0 0a 2b a6 bb e1 f4 43 ab d9 cd 64 f3 3d d4 c8 ad 02 61<br>64 ae 90 be 8b ff 3a 16 28 a8 3d 23 6d b8 f2 c3 61 b9 fa 03 39 ca 02 d6 a5 81 9f ce 56 e0 70 df 85 b5 60 9a 2d 31 b3 d2<br>90 52 8d 0d 60 ea 3c f7 94 cf 9d 30 c0 1a 73 44 17 6c a6 70 5f 81 5d 47 8f fb ed ca ea 38 3e 9e 12 ed 23 ba d2 6c 9e b2<br>4d 1c 5f aa f8 3e 56 10 bb ba 81 94 3d d8 a2 d1 c0 3c 17 97 c0 ec e5 05 ea 3e 6c 80 cd 6e 8e ed e2 c9 f8 dd 6e 6e 63 8c<br>e3 04 54 18 80 8b 2f 31 0e 8b 82 05 79 e7 c1 cb 6c 57 8a a9 61 26 88 e3 f0 91 53 a5 09 14 56 ea 54 df 5c ee 80 e4 94 98<br>46 6b 1e d2 11 61 24 89 0b ad 3b c1 c8 92 35 1a d9 39 e3 c7 29 80 a6 be eb 1a aa 3b 5e 26 92 81 af ad 4b 3a 35 45 25<br>75 c1 69 d3 94 cf 8a 71 5c 1a 76 d4 12 3e 7b b9 2a 4d d1 f5 25 2c e7 83 cc 5c e0 c8 7c 20 ea b3 69 ef c7 88 29 ab ec 7b<br>f7 e9 07 ce 51 c8 a1 2f 14 2c 63 c4 be c0 50 ce 9e ad a4 0f ec 29 aa 9c 45 1b 86 94 af 59 bd 7c 33 03 59 c7 c7 10 00 21<br>47 a5 18 13 86 d8 ad d5 fc 6e ce 7d d2 d2 91 9e 28 dd 04 75 d6 10 05 e6 68 95 d3 1b 75 9d 70 73 bb ad 34 20 10 a5 aa<br>b0 39 71 6f 50 ba f0 c4 1f 91 36 48 94 97 06 69 1f 84 d9 5d 0a ba 1f 6d 59 51 7c df d1 e5 47 59 63 f8 4b 49 d8 b7 e5 c3 57<br>4b 19 c8 66 b3 82 de 87 00 9e 42 c2 7d 50 04 51 d1 f3 32 ee 3f 79 4f 22 bd 38 ee 3d 1f 78 5e fc 03 de b8 4b 8f c3 04 00<br>00<br>Data Ascii: uTn0+d1`>2hr+@SCw(k0Lzf,o)}5^Z":pB]]BrJzea +jKk.s/cdro`LValeNgwgZ`v+Cd=ad:(=#ma9Vp`-1R`<br><0sDlp_]G8>#IM_>V=<>InnnT/1ylWa&SVT\Fka\$;59);^&K:5E%uiq\>{*M%,\ i){Q/,cP)EY 3Y!Gn}{uhups4 9qoP6Hi<br>jmYQ GYcKIWKfB}PQ2?yO"8=x^K |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 3          | 192.168.2.4 | 49740       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.390271902 CEST | 1132               | OUT       | GET /wp-content/plugins/ultimate-faqs/css/rsssb-min.css?ver=5.5.5 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.575679064 CEST | 1144               | IN        | <p>HTTP/1.1 200 OK<br/> Date: Fri, 04 Jun 2021 19:35:04 GMT<br/> Server: Apache/2.4.18 (Ubuntu)<br/> Last-Modified: Mon, 15 Jun 2020 15:21:49 GMT<br/> ETag: "2b47-5a820fc566d91-gzip"<br/> Accept-Ranges: bytes<br/> Vary: Accept-Encoding<br/> Content-Encoding: gzip<br/> Content-Length: 1695<br/> Keep-Alive: timeout=5, max=100<br/> Connection: Keep-Alive<br/> Content-Type: text/css<br/> Data Raw: 1f 8b 08 00 00 00 00 00 03 ad 5a db 8e a3 38 10 fd 95 68 56 ad 99 95 42 84 b9 07 9e 76 a5 95 f6 69 ff c1 06 93 58 ed e0 08 9c a4 33 d1 ec b7 af 21 21 c1 60 73 89 57 ad ee 99 80 eb d4 71 b9 ca 1c 5c d9 94 65 55 21 0b 9d 38 67 45 75 43 ec cb aa c8 4f 52 ec 62 c4 ca 0c 97 96 b8 92 e4 ac e0 56 0e 0f 84 5e e3 6f 7f 63 7a c6 9c a4 70 f5 0f 3e e1 6f eb e7 e7 f5 1f 25 81 74 5d c1 a2 b2 2a 5c 92 3c d9 63 b2 db f3 d8 0d 8e 5f c9 01 96 3b 52 c4 76 72 84 59 56 e3 db c9 85 64 7c 1f 03 db fe f8 b5 91 68 c4 30 e7 b8 bc a5 14 c3 52 f0 e0 7b e5 fd 75 ef 22 c2 39 2b f1 2d 15 64 71 c1 e3 ef ab ef 49 46 aa 23 85 d7 98 43 44 71 0f 64 45 89 6e ba 94 41 1e 53 9c f3 76 06 35 c7 84 92 02 5b ed 05 57 4c 89 92 8a 5b 15 bf 52 1c 17 ac c0 8a 29 ae 9c e3 d7 d0 ed e3 02 3e 40 42 57 f0 86 60 fa b9 2b d9 a9 c8 ac 94 51 56 c6 bf d9 30 8a f2 7c ca 30 de b3 b3 88 92 c2 dc 0e 70 16 68 cd 73 98 62 c4 d8 a7 d2 b5 6b 07 60 bb 9d 61 ab f5 ee 78 5e 14 3a 5a 04 7e 3a 20 5a aa 7d 3b be 1d 64 93 96 7a cf 8e 1b 78 50 6b 2f d6 ef 13 8b 75 51 87 dc 0e 11 d2 c7 ec 65 3b 12 75 7f 1b b9 7a f6 17 c2 45 d2 2a 9d 3b 41 ea e5 60 da 54 ef 1b 43 38 b2 e2 3b c6 76 14 1f e9 a9 52 ba c7 5b 37 77 14 e5 a1 b0 d6 32 48 b1 13 00 3d 83 2b 3b f1 13 c2 4a f7 59 0e 52 57 3f fb a7 a9 d6 37 72 40 e0 84 5a 80 12 8b 6a e4 4a d7 11 42 08 eb d7 ac b5 d4 7a 0e 1c e8 66 fa 6a 39 12 b1 15 95 b8 52 3b 47 91 a0 ad 9f 77 c7 58 eb 3f 82 00 80 11 ff 2c fd c4 6a e7 38 f3 6c df 9b b4 d4 7a c6 9e 20 af af d5 1d e1 fb 13 52 7a f6 3c bd db d6 4c 5f e2 a8 fe d1 da 93 a2 e2 70 57 c2 83 d2 b3 0f c2 1c ea 9d 77 8c b5 fe 3d 3b f0 23 fd e6 96 61 4a 52 c2 34 75 66 ff 19 6e ff f2 e7 18 eb 0b 7d eb e7 48 3f 85 b3 7a 53 f7 b2 10 40 7d 9a 9c c7 b6 73 37 f3 61 a4 2f ec bd 30 c0 65 81 2f ea 29 e7 81 3d cb 54 bf af a4 be 63 2b 30 94 de d2 34 4d 1e cf f1 12 66 e4 54 c5 e2 f9 9b a8 1f f2 ad 34 40 54 a4 fa 5d e1 88 41 38 06 40 98 58 07 f6 d3 62 d5 97 75 bf 7e 60 42 83 d4 f6 22 3b ae 55 0a 29 4e ac 0b 46 9f 84 f7 07 c0 82 0b 0d 44 60 85 b3 3b e6 e5 ae 17 42 db 96 b4 44 ab 10 6a 6f ab 50 fc 02 c1 74 e5 88 ff 25 47 5 6 11 4e 58 11 97 98 42 4e ce 38 e1 f8 8b 5b 02 75 57 c4 29 ae 37 85 fb 95 0c a7 ac 84 cd d0 46 7e 34 17 79 29 e4 97 d0 41 87 f8 74 3c e2 32 15 4c 9e 5c 9b 7b 77 ec 7e ec 56 1b a7 5a 61 31 58 54 81 25 36 dc 64 c9 58 ad 8e 6b d6 69 d5 96 97 10 66 37 39 ea b5 c4 12 76 f5 a4 ef f1 b0 38 3b c6 db 6e 10 20 aa 18 3d 71 31 3b 71 e7 25 19 27 3d ad aa f3 ee d6 46 bc 0e eb c3 32 54 09 b2 a1 e9 ea 08 f9 7e 3d 6b 20 a3 d7 9d 98 59 4e 28 15 f9 ae 92 6d 2f ab 7a 89 6e 6d 69 a8 87 c6 30 ad 17 fd 2e 4d f7 30 63 97 58 6c 4c 62 2f ae 33 c5 ad 33 c5 17 7f ec 55 b9 43 f0 87 e3 ac 6d f1 b3 71 fc df 15 65 56 1d 20 ad 05 e6 53 8e ea c7 48 8b d4 2c 0b 3c 71 f6 54 b4 ab e6 53 5d a2 42 1b 5f e2 3d c9 32 5c a8 32 55 2c 52 33 74 2c 25 fa 3e 9b a0 9c 49 45 10 a1 84 5f 1f e8 3d bb 0d 15 54 b0 55 67 36 e4 eb 91 7b b5 ac 7f ac 7b cd 64 0c 46 0c 8d 73 52 0a 11 9f ee 09 cd e2 82 ef 2d 0a db 8f 3f c0 ef 22 76 af 8d c1 a9 f3 f4 f5 d1 3b 5f 0c b0 1d 81 3d 31 8b 71 f3 7f 9b<br/> Data Ascii: Z8hVBviX3!!`sWqleU!8gEuCORbV^oczp&gt;o%t]*&lt;c_ ;RvrYVd h0R[u"9+-dqIf#CDqdEnASv5[WL[R]&gt;@BW"+Q V0 0phsbk`ax^:Z-: Z];dzxPk/uQe;uzE*;A`TC8;vR[7w2H=+;JYRW?7r@[Z]jBzfj9R;GwX?,j8lz Rz&lt;L_pWw=;#aJR4ufn)H? zS@[s7a/0e/)=Tc+04MfT4@T]A8@Xbu~"B";U)NFD";BDjoPt%GVNXBN8[uW]7F~4y)At&lt;2L{w~VZa1XT%6dXkif79v8;n =q1;q%=-F2T~=-k YN(m/znmi0.M0cXILb/33UCmqeV SH,&lt;qTS]B_ =2l2U,R3t,%&gt;IE_ =TUg6{{dFsR-?"v;_ =1q</p> |
| Jun 4, 2021<br>21:35:04.703124046 CEST | 1172               | OUT       | <p>GET /wp-content/themes/enfold/js/aviapopup/magnific-popup.css?ver=1 HTTP/1.1<br/> Accept: text/css, */*<br/> Referer: http://www.tonhc.org/coronavirus/<br/> Accept-Language: en-US<br/> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br/> Accept-Encoding: gzip, deflate<br/> Host: www.tonhc.org<br/> Connection: Keep-Alive<br/> Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.900643110 CEST | 1198               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:47:36 GMT<br>ETag: "1dd8-55c779b110200-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1914<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 b5 59 db 6e e4 36 0c 7d cf 57 a8 08 16 4d 82 38 f1 5c 37 3b 41 81 5e 9e 0b 14 dd fe 80 6c 6b 3c 6a 6c cb 90 35 c9 24 45 ff bd d4 cd d6 cd 93 14 db 6e f6 21 a6 6e e4 21 79 48 29 f7 37 e8 57 5c 77 74 4f 4b f4 1b eb 8f 3d fa e5 eb 57 74 73 7f 71 d7 ee fb ac a8 d1 5f 17 08 09 d6 ef 50 fe 08 bf 35 64 2f cc af 2f b4 12 87 1d 5a e4 f9 27 f9 79 20 b4 3e 88 e9 fb 2d a3 5d 45 4e 52 b0 5e 4a 01 7b 26 7c df b0 97 1d 3a d0 aa 22 9d 94 f5 6c a0 82 b2 6e 87 f6 f4 4a 2a 29 2a 70 f9 54 73 76 ec aa 1d ba cc 0b f9 a3 56 f7 b8 a4 e2 15 ce be 7b 90 df 7b da 08 c2 77 08 37 fd 01 5f 99 d1 1f 1e f2 eb 47 f4 f7 85 56 fe 85 e3 fe 3f 51 7f 35 a3 2a 3b 8a 86 76 64 87 3a d6 11 f4 1d 6d 7b c6 05 ee 84 1c cb 5e 48 f1 44 45 26 cd d9 e3 92 64 cf 74 a0 05 6d 94 0d 06 80 51 d3 92 75 02 c3 4e 5c ab 4b 4e 22 c3 0d ad e1 ac 92 74 60 a6 7f 3e 2e 06 d6 1c 05 f9 80 15 8e bd 13 08 3d ae 2a da d5 f0 85 1e fa 93 a7 2c 3b 65 03 7d 53 83 05 e3 15 e1 52 a4 66 b4 ec ed cc f0 cc 48 6c e0 ae 20 7b c6 89 b2 53 0a c1 bc 1d fa fe 7b b9 47 45 87 be c1 80 0e ed 24 aa 59 d1 b0 f2 29 65 14 c4 91 a0 25 6e 2c 46 2d a0 d9 90 e9 30 25 ce c0 5e 34 7f f6 78 98 74 9d af 27 a8 a4 a6 4c 80 73 d2 60 41 9f c9 59 2d 67 b4 82 91 16 f3 9a 76 12 6e 7c 14 ec 31 f0 b0 74 51 18 70 9b 49 23 73 cc 81 35 00 2a 72 95 bc d5 5f f8 4f 7c 4a 0d 2b 1b 82 f0 28 8f 7c 60 32 69 a4 1e 13 5e 72 07 18 d2 4e 31 53 7a ce 6a 4e 86 41 4d 33 13 df 18 6b fd 49 8c da f0 b4 22 1b 4a 72 2e 28 ef 0d c9 18 4a c8 ad 68 52 08 d4 cb f4 68 6c 52 da 86 b2 61 03 b1 88 70 ce 5e cc ef 3d f8 8e 61 c0 e6 d6 ee 74 94 1a ab 9d ac aa c7 01 c2 75 20 0d 29 85 89 07 1b f0 c9 91 58 38 6a 21 8f 82 1c 50 bf ef 69 7d 3c 1f 6c c0 02 89 71 97 47 c6 a9 a3 19 26 71 1a 89 c0 65 a9 fe cd 93 83 4a f9 8d 76 bd 89 84 54 04 4e 1c a3 23 35 53 be 32 20 5a d2 4e 24 62 a8 82 eb 5c 34 5f 6e d0 ae a5 ba 28 80 1d 61 a5 71 a4 b3 9a 1a 4f de 1d 64 95 30 4b c6 45 2f 07 2a 1c dc 86 8c 13 5c bd 86 8b cf 20 3d 64 04 62 22 11 4c f1 fc e2 28 04 eb dc 98 72 24 2a b2 d4 c2 a9 98 29 5e d7 89 9e 48 0b b7 9a 09 8e bb a1 c7 9c e8 0a a1 79 d2 70 b2 8d 45 dc f7 04 c3 bc 92 4c 01 37 2a 39 72 8d 57 78 7c 4a 0f bd b2 8d f8 fd 80 2b a9 b7 5d 1a c9 00 05 6d f 2 6e a7 92 60 cf ca e3 00 3b da f2 e4 9f 35 59 e1 e7 a2 4b 3f eb b5 8e 16 4b e4 f6 5b 33 5b 20 4c 87 b2 09 bb a0 92 a9 28 ae 48 c9 38 d6 4b ac 51 e9 f0 76 7a 88 ed 66 be 89 d8 6e ae 83 32 99 a3 05 04 3c c0 a9 55 f4 c2 52 6e 03 11 95 0d e2 b5 51 1e e1 2d 6e 26 29 7d 03 e1 d2 a4 8b 12 ed 71 4b 1b 50 e2 27 4e 71 73 8b 7e c6 c3 13 e1 cf b4 69 20 d6 5a d6 31 08 9 1 92 38 b9 a4 e0 d4 89 71 eb 4a 94 5f 4c aa 8c 96 2d 1e d5 77 da 30 28 03 d7 d1 c6 b8 94 a5 cd ec a3 a0 5d f4 a7 c0 99 5 9 21 3a 88 00 14 b8 d7 e6 f4 4a fd 73 6a 56 8b eb a0 64 39 f4 4c f7 1c b7 89 61 77 cb 11 5a e3 f7 6c ab 01 74 fd aa 86 1c 47 65 66 ae 99 ea 96 3e a7 be 4f f4 7f 86 33 f3 30 e4 62 c6 75 bc bb 58 26 c2 59 06 8c 53 d1 46 e2 48 9f fa ef 22 73 6c 28 42 92 f7 f8 7b b3 31 09 e5 e5 ab 81 e5 4b ee a7 e4 c2 c6 b6 a5 0a 81 65 81 aa 0f 8d 1c cf 8d fd bc 2e f0 55<br>Data Ascii: Yn6jWM8l7;A^lk<jl5\$En!nlyH)7WwtOK=Wtsq_P5d//Zy >-JENR^J&{"InD"}*pTsvV{{w7_GV?Q5*;vd: m{^HDE&dtmQuNKN"t">,*;,e}SRfHI {S{(GE\$Y)e%n,F-0%^4xt'LS'AY-gvn 1tQpl#s5*r_O J+{()2i^rN1SzjNAM3kl"Jr.(JhRhIRap^=atu )X8j!Pj}<IqG&qeJvTN#5S2 ZN\$bI4_n(aqOd0KE/^)=db"L(r\$)^HypEL7*9rWx J+ mn};5YK?K[3[ L (H8KQvzfn2<URnQ-n&))qKP^Nqs-i Z18qJ_L-w0[ Y!:JsjVd9LawZltGef>O30buX&YSFh"sl(B{1Ke.U |
| Jun 4, 2021<br>21:35:04.908457994 CEST | 1240               | OUT       | GET /wp-content/uploads/dynamic_avia/enfold.css?ver=5e843620e3ec4 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.099627972 CEST | 1268               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Wed, 01 Apr 2020 06:35:12 GMT<br>ETag: "253ab-5a234e2eff5ab-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 18084<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 9d 59 8f 24 39 92 98 9f b7 7f 85 0b 85 41 cf 0c 3a 72 2a af 3a b2 a1 c6 2e 84 15 a4 07 49 0f 5a 3d 49 42 c2 23 c2 33 33 a6 23 c2 a3 e3 a8 a3 0b f5 df 45 77 d2 dd 69 27 8d 8c a8 9a c1 6a 66 a4 d9 0a d2 8c 4e 27 8d c6 c3 e8 5f 3e 3c cc 36 ed ef b3 43 b3 6e 16 c7 55 bb fd 32 af 17 bf 3e ef db d3 76 39 5b b4 eb 76 ff 50 bd 7a f7 f6 ba b9 7e ff f3 f0 f3 a9 ff cf cf 5f 1f 1e 4a b4 5e 8e 9b f5 55 f7 3f 8f f3 f6 53 b3 ac 22 55 27 d5 f4 ff a9 aa ea d8 ee aa 75 f3 74 ac aa 6d 3b db 37 bb a6 3e 56 87 c5 be 5d af 7f fe 3a 6f 97 9f 7f aa ba ff ad ae ea 0f ab 7a 76 6c db f5 71 b5 ab b e 3c b5 db e3 ec b0 fa bd 79 a8 ae df ed 3e fd 5c 7d bd 3a b4 8b 5f 9b e3 63 5f 8d 9f 2a f0 b3 5a ae 3e e0 a4 97 a6 5e 36 44 70 53 af b6 38 ad 3e ac 96 0d 4e 7c 6a db 23 55 af f7 c7 d5 62 4d 84 b7 35 79 fc c1 b7 27 4e ae 0e bb 9a 26 d6 bb dd ba 39 e2 e4 76 fe 57 57 08 4e 5d 3d ed eb 0d a9 c1 cb 35 49 b9 21 29 b7 24 e5 8e a4 dc 93 94 37 38 65 87 13 e6 6b f7 eb b7 93 6b 30 22 ba 27 49 35 49 98 cf 69 3b 3b 03 d9 7e de 90 e4 e5 72 df 1c 0e e4 f9 ab 67 9c b4 58 d1 ca 2c 5a da cd cb 66 4d 92 9e 48 07 35 a4 26 ab 0d 79 e4 6a 4b 2a f6 eb 7c 89 93 7e 23 86 42 12 ea 0d 69 e1 c3 a6 5e 93 8a 1e 8e fb d5 af e4 8d 5c 6a bb 25 95 3b 9c e6 34 89 3c e6 48 ac ed 43 4d fa 86 14 74 22 2d 41 5a be d9 32 83 69 49 9b 9e 3c 7f 49 1a b0 25 5a 27 92 b2 26 35 78 5a 35 eb e5 81 8e b1 a7 76 4f fa 76 5d cf a9 55 ac 9b e7 66 4b 2a 73 ac e7 d4 1b 2c ea 1d 37 f4 8f de db a1 c4 ce cf 90 c4 ce 77 91 44 d2 7e c7 17 92 42 b4 04 87 c5 ba bc 45 bd fd 50 13 73 5c 36 c7 7a b5 26 c9 cd 66 de 90 a7 3d ad 9e 4f 74 c4 8b 6d bf 7a 16 9a 8a 77 be bc 47 7f e9 a6 1c 62 c9 9b 66 4b cc 92 f1 d2 ed e9 b8 3b 91 8a ed 4f 73 d2 51 82 3f 3f 9c 36 9b 7a 4f bb 75 45 5d b4 93 fb 95 f4 c3 69 b9 6a c9 98 73 7d e3 12 5f 75 33 27 cc b9 da 9d d6 eb de d1 fa 39 d7 69 3a 7f b8 6b b7 87 d5 87 86 55 f0 b3 6a 73 70 15 6a b7 ab 7a 4d 35 bc c8 7c 5d 6f 7f ad 5e 75 d3 23 2c e2 6a e1 66 62 97 da ec 1f 3f ee eb dd c3 d3 6a 7f 38 ce 16 2f ab f5 92 ab e2 d5 93 ab 61 37 6f 57 57 c7 66 b3 5b d7 c7 c6 95 dd 3e bb aa b7 87 e3 a3 73 b7 ab cd 8a e9 5b 57 ab 4e 76 f9 d8 89 1d 5c 9d 66 21 61 76 38 7e 5e 37 b3 ae d8 aa fe 32 6f f7 ce 04 c2 ca e4 55 73 dd fd f7 e7 af b8 a8 6e 09 d2 74 eb 97 50 73 a1 2d eb e7 d5 b6 ee 3a b5 aa 1f 5e da 0f 4c a5 7a b7 3b 73 93 d8 87 55 f3 91 e4 3e b9 cc 6e cd 33 eb ea 3c 3b 7e de 35 b3 d5 02 2c a1 1e 5e bd bd 7e 7f 77 fb 3a ac 9d c6 a5 13 e9 a4 d9 b2 79 aa 4f eb e3 2c ac 6e f8 ae 9c 39 6f b5 68 b0 2c 15 5b d4 c7 da b5 f9 c9 d5 e7 48 a7 ae ab 8f bb 99 eb 98 cf eb 95 ab 75 27 00 53 84 21 19 cb 7c 19 96 82 e1 ed d0 fb d0 66 5c 75 56 30 b6 0a 6d c8 de a6 c2 02 42 32 8c d5 a6 7e 6e 7a 1b 24 fa cf fb fa 83 7b e5 7e 56 26 fa 2f fb c7 ce 10 dc 0c 44 f4 b6 cd c7 c3 ec f8 72 da 90 29 ad b7 d6 ae b9 37 f5 b1 ef 54 da cc 7f ad 3f f5 05 77 2b d9 03 5d d5 5c 1d 3f 36 8d b3 8a e6 d3 f1 ca d7 ee 71 4b 46 fa d5 b1 7d 7e 5e 33 86 17 d2 af 6a e7 74 3e 34 ff b6 3a ae 1b de 44 5f fd f5 f0 78 68 f7 c7 c7 ae 23 b1 93 be<br>Data Ascii: Y\$9A:r*:.IZ=IB#33#Ewi'jfn'_><6CnU2>v9[Vpz~_J^U?S"U"utm;7>V]:ozvlq<y>\):_c_*Z>^6DpS8>N]j#UbM5y'N&9vWWN]=5i!)\$78ekk0""l5li;:-rgX,ZfMH5&yjK*)~#Bi^j%;4<HCMt"-A22li<%Z'&5xZ5vOv]UfK*s,7wD-BEPs\6z&f=OtmzwGbfK;OsQ??6zOuE]ijs]_u3'9i:kUjispjzM5]]o^u#,jfb?j8/a7oWWf?>s[WNv\flav8~^72oUsntPs:-^Lz;sU>n3<;-5,^~w:yO,n9oh,[Hu'Se!fHuV0mB2~nz\${~V&Dr)7T?w+]}?6qKF)~^3j>4:D_xh# |
| Jun 4, 2021<br>21:35:05.324791908 CEST | 1290               | OUT       | GET /wp-content/plugins/jetpack/_inc/build/photoni/photoni.min.js?ver=20191001 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Jun 4, 2021<br>21:35:05.509699106 CEST | 1372               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "2f6-5c3db85dcfc49-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 421<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 85 51 c1 6e db 30 0c bd ef 2b 14 1d 0c a9 75 dc 9e e7 79 43 b1 f6 30 60 c5 0e 3d 16 3d a8 26 6d 13 90 a5 54 a2 13 b8 81 ff 7d b2 8d a6 dd 16 60 80 01 99 8f 7c 8f e4 e3 d5 85 b8 f5 c2 79 16 bd 07 6a 46 c1 1d 45 d1 90 45 01 14 b0 66 3b 16 e2 07 8b 04 d6 be df 25 1c 44 13 7c 2f 3c 77 18 96 c2 58 88 8b ab 4f 9b 66 70 35 93 77 4a 1f df 7e 05 a7 80 1a 35 6b 16 33 dd 22 a3 3e ee 4d 10 58 2d 60 8b 7c c3 1c e8 79 60 54 12 0c 9b ad 35 af e3 36 86 5a ea 32 51 31 cb 96 c2 04 6c aa 0a f5 12 18 80 bb 3d 3a fe 49 91 d1 61 50 d2 3b eb 0d c8 9c 75 89 36 e2 d2 02 d6 16 07 02 ee 72 b7 06 1d 52 db 71 09 59 06 5f af b3 cc a5 6f 7e d7 09 e3 1f c3 2c 3c 99 83 ce cf 24 57 1d 99 3b 9d d3 42 d6 7a 9a e6 ce e2 bf 03 4e eb fa 1f ed f2 41 ad 20 f8 7a e8 13 af 78 19 30 8c 0f 68 d3 01 7c b8 b1 56 49 ea db c7 c5 9f 74 14 63 eb 2d 50 1f 9f 64 6a 5f 5d 97 f4 05 0b 8b ae e5 ae a4 cb 4b cd 45 aa b0 0a 1f e9 49 4f a9 e0 d4 8a f5 91 8b 80 bd df e3 df ae 7f 50 4d a2 67 aa 62 ca a3 d4 53 29 07 07 d8 90 43 90 9b 8a c7 1d fa 46 1c c8 81 3f 64 d9 b9 dc db 4e c9 65 39 7b 40 ae 95 55 f5 be 6a 40 03 e3 03 1b c6 6f 27 ec 5f ff 6e 7f dd 7f f7 8e 67 2c 69 24 fd 1c f5 67 54 5a e7 27 d2 b3 87 f1 0c 33 9d 63 e7 23 6f 57 ff 51 4f 4a 97 bf 01 6e 78 59 3f f6 02 00 00<br>Data Ascii: Qn0+uyC0`==&mT)} yFEEf;%D <wXOfp5wJ-5k3">MX-` y`T56Z2Q1=!:laP;u6rRqY_o~,<\$W;BzNA zx0h Vltc-Pd _KKEIOPMgbS)CF?dNe9{Uj@o'_ng,i\$gTZ'3c#wQOJnxY?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Jun 4, 2021<br>21:35:05.511660099 CEST | 1372               | OUT       | GET /wp-includes/js/wp-embed.min.js?ver=5.5.5 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.824843884 CEST | 1577               | OUT       | GET /wp-includes/js/wp-embed.min.js?ver=5.5.5 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Jun 4, 2021<br>21:35:06.012485981 CEST | 2093               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "592-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 765<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 85 54 4b 4f 1b 31 10 be f7 57 64 dd 03 36 d9 38 09 48 95 da 8d 55 21 ca 01 09<br>ca 01 d4 4a a5 54 72 bc 93 c4 62 63 07 7b 36 94 26 e1 b7 77 bc 21 94 47 50 2f 5e ef cc 7c f3 fc c6 dd dd ac 75 31 b1 b1<br>35 b2 15 b4 e8 ab 6b f4 9d 31 38 08 1a a1 6c ed 76 df 65 a3 da 19 b4 de 71 93 97 62 c1 ea 08 ad 88 c1 1a 64 c5 5c 87 16<br>a8 ac 9f 3b 3a 0a 3b e2 a5 bc a9 21 dc 9d 43 05 06 7d 10 24 32 52 97 e5 d1 1c 1c 9e d8 88 c9 b3 20 48 af 68 54 b7 33 95<br>8e e5 72 b1 ca b3 74 93 01 0c d8 39 1c 4d 87 50 9e 42 8c 7a 0c e2 c1 74 9b 4e 3d 66 07 62 91 d2 41 05 b2 d4 a8 93 7f 4c<br>48 94 11 4c 00 5c 2e 51 4e d7 a0 74 9d eb aa 6e 3c 67 dd cb 5f ba f3 e7 a0 f3 a3 d7 f9 78 d5 95 08 11 1f 41 42 2c 46 3e f0<br>e4 38 e4 3a b7 79 54 2f 4a 3c a8 2a be 63 47 41 4f e1 32 c5 ed ac 81 8a ed b4 37 4e da 3b ec 6a 47 50 8f b6 41 87 95 37<br>d7 37 b5 c7 ff c1 bd ea 15 7e e0 64 05 6e 8c 93 c2 b7 db c2 5d fa 2b 19 f1 ae a2 92 6d 9c 55 fa 4e 31 e7 1d b0 22 25 bd<br>06 c4 a7 00 2a 37 a8 48 a8 1c 64 f4 75 30 a0 94 0a d2 78 47 83 c1 ef d6 95 fe 56 2c 92 15 f5 7a ea e7 70 80 34 e9 61 8d<br>c0 59 13 87 89 9c 4d c0 8e 27 c8 08 f9 d8 d0 06 d3 87 fd 01 b7 6a a6 43 84 63 97 7a d8 f4 38 ef f7 84 10 56 91 ba 80 8a<br>c8 43 a6 f7 f7 76 b0 d7 eb 91 94 ce 22 c8 b5 4b 65 57 a4 63 95 75 d7 cf bd 93 54 53 f3 a8 19 44 ca a3 0a a6 94 2c 67 9a<br>92 b1 db c5 5a 4e 02 8c a8 b2 31 e0 d3 12 82 49 98 b5 72 93 1e fd fa 88 14 4f 37 17 d1 b0 58 13 a7 e6 1b 9f a9 47 c2 48<br>f4 33 49 c3 d2 89 6d cf 5c ac 56 ab 1c c4 6b 9e 73 f6 50 00 cb df a2 6f 9e f5 45 5e 6e 41 7e 39 3b 3d 5c 4f e5 c4 eb 12 4a<br>96 63 63 bb 2d 4a 45 16 0f fa 62 b3 0e 2d e4 cd 50 32 27 16 2e ad db 86 c6 40 86 41 75 fa 99 52 4e cf ed 58 13 11 a5 9e<br>cd be 41 88 a9 30 e2 00 fc 3e a3 31 9c 9e 1f 1f b5 fa bd d4 4d 95 65 ff 6c 69 ff c3 01 bd 10 34 1e 8d 66 c2 bb 17 c1 96 e9<br>77 37 cc 3f f5 fb 3f 65 77 3d 96 57 54 67 eb 2d a1 4e 74 20 b5 80 aa ea 3c 30 8f 82 44 62 6b 1c d8 0d 5b 23 b1 b5 c9 9f<br>83 b2 97 f1 4a bc 18 e5 93 5d 61 42 a0 3a d5 38 91 41 13 81 a7 5c d0 a8 ce c9 d2 8d f9 fe 07 21 63 3d a4 f7 8a ef 25 22<br>26 de 07 d3 56 ec fd e7 cd a2 b5 31 09 df 74 9e a3 48 4f 49 58 2e b5 e0 e9 71 31 15 6d d8 57 5f 02 cf 88 d8 5b f6 04 4c<br>1d 2c de b1 14 8c 96 81 ca 4b d6 64 48 0b 6a e0 70 62 ab 92 53 4c 41 b4 59 f1 db 66 e7 f2 d2 9b 3a 51 4d 14 7f 01 f6 03<br>58 61 92 05 00 00<br>Data Ascii: TKO1Wd68HU!JTrbc{6#w!GP/^\u15k18\veqbd!::!C}\$2R HhT3rt9MPBztN=fbALHL\QNtn<g_xAB,F>8:yT<br>/J<*cGAO27N;jGPA77~dn]+mUN1"%*7Hdu0xGV,zp4aYM'jCcz8VCv'KeWcuTSD,gZN1lrO7XGH3lm\KsPoE^nA~9<br>;= OJcc-JEb-P2'.@AuRNXA0>1MelI4fw7??ew=WTg-Nt <0Dbk[#J]aB:8A!\c=%"&V1tHOIX.q1mW_[L,KdHjpbSLAYf.QMXa |
| Jun 4, 2021<br>21:35:06.021059036 CEST | 2166               | OUT       | GET /wp-includes/js/jquery/ui/effect.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.208996058 CEST | 2408               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "33a7-5c007b4699b9b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 5162<br>Keep-Alive: timeout=5, max=95<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 bd 5a 6d 93 db 36 92 fe 9e 5f a1 61 ca 53 a0 04 51 94 c6 e3 cd 52 c3 a8 12 c7 a9 78 6b 93 ec c6 d9 cb 07 59 e7 e2 48 d0 88 36 05 30 20 34 2f d1 28 bf fd 9e 06 f8 a6 97 99 a4 ae 72 67 57 8d 00 10 68 34 ba 1b dd 4f 03 18 74 cf 3e eb 74 3b 1f ff bd 11 fa a1 f3 9f b7 9d 37 cb a5 98 9b a2 33 0c 86 c3 e0 25 7d 5b 19 93 47 83 c1 c7 5f a9 cb 26 0d e6 6a 8d 66 fa f2 5a e5 0f 3a bd 59 99 6a fc b7 6a 23 17 89 49 95 ec 24 72 d1 51 66 25 74 67 ae a4 d1 e9 f5 c6 28 5d d0 a8 9f 44 26 92 42 2c 3a e8 8b cf e8 d3 f9 fe ed cf 9d 2c 9d 0b 59 88 e0 68 ca 40 e9 9b 41 f9 b5 9c b8 fc 9e e4 69 d0 66 6b 30 4f 8c b8 51 fa 61 20 dc 2a fa 73 a5 c5 00 23 06 9f 9d 2d 37 72 4e 9c 31 e3 6f bd aa e2 c5 b1 79 c8 85 5a 76 16 62 99 4a 71 7e ee 7e 83 64 bd 98 b8 22 9b 7a 6e 0e 6f c6 8d 1f 19 e6 d6 ea ef 58 4d b1 f0 b7 b7 89 ee 6c 78 c6 97 7c c1 0d cf f9 8a df f0 94 0b 7e cd 13 ae f8 9c af f9 03 97 5c f3 5b 7e cf 5f c7 de 26 ed 57 2c 7a fc 2e 2e c6 15 ad ce 07 66 30 4c 3a 8a 3a be 99 8a 80 38 9c 3d 3e 6e 77 63 2d cc 46 cb 8e dc 64 19 18 9f c8 c7 c7 33 11 80 cd 09 b5 44 b6 38 31 13 eb 60 99 29 a5 27 bf ff 6e a2 3c d1 85 f8 36 53 89 c1 c2 79 5a fc 90 fc 80 c2 c4 f5 d5 c1 5a 2d 26 cc f4 6c c1 7f 61 7f 22 73 15 4e 42 fa 96 dc 5f 99 89 fd 8d 8c bf ab 59 fc c4 b4 63 4f c5 39 f3 79 12 ab e0 83 be b9 4e e2 e9 ac e2 50 83 07 a3 fe a9 ee 84 7e 0d 5d a3 d7 35 d6 d5 a8 80 0b 47 41 c6 22 d0 22 10 f7 62 0e a2 5c c6 f2 fc 5c 04 96 67 26 7d 2e f0 b9 c 8 93 b9 78 7c f4 68 06 6f 9c 2e d1 5e 89 21 56 53 31 a3 7e 6a ba 42 29 98 27 f3 95 98 c5 b2 5d 6b b1 27 dd 2f 3f 1b ee c0 75 90 09 79 63 56 13 e6 85 dc fe 87 2d c4 49 f0 51 a5 92 f9 e7 e7 1b 30 65 84 5c b0 84 2f 03 a3 13 09 3e b4 90 90 a1 f2 a3 e5 54 cf 1a 79 7c 5f a9 ac e4 eb 55 97 c9 98 c9 de d0 7f 31 f4 af 86 13 d3 63 a2 6f fc ae ec be 8a 46 5d 89 16 11 5d e0 77 54 7f 61 a3 c1 45 5f fa f8 6e 1a b2 ef c8 52 49 48 82 2c 27 36 81 ba 93 42 7f a3 e6 9b 35 f8 20 fd 25 9b cc fc 57 2a ee 26 cf 7c 0b 6e 84 79 ad d6 f9 c6 88 c5 3b f3 90 09 30 4b d6 d6 02 4b 0e e6 1b 4d 4b b2 cd c5 30 30 88 57 9f 9f eb 52 3e 28 4d c3 19 fd a5 df 99 bf 54 1a 2b ab be 8e 65 bf 3f f6 bd 02 9b 5b de 34 1b 49 4f 45 ac a7 72 86 71 4c 4d 0b a8 61 2d 32 6b 04 c2 9f e1 8b 98 f9 63 91 15 a2 43 d4 44 27 85 b1 9c 24 e2 c6 8b 6a 48 29 5b d5 c8 e7 a3 13 3b d7 b5 e0 4d bc 75 bb 2a 32 71 11 a4 c5 bf b2 24 95 3f 5e 7f 44 0b d9 3c 13 b1 f1 83 aa c7 8e 53 97 6f 2b 93 14 b1 db 55 62 b2 dd 45 02 06 c0 74 2c c8 20 d1 0a 3b dc c2 64 3c b9 59 5f 0b ed 9d 55 5c c2 5d 9c 15 c1 f2 1e 36 2a c4 a2 98 d2 2e c5 30 89 61 a2 1c b3 37 87 74 64 65 49 16 f6 7d 7e 5e 54 76 46 7b 82 3e 3c 3e 62 6f 6e b4 f5 a2 dc d4 c5 d8 4e a4 96 4b 6c cd 8a 91 5a 5c 72 22 23 49 a2 6c 71 33 69 73 26 67 51 ab 1a 7c 28 0d 04 f4 e1 36 f3 4c 18 e8 8c 26 ae 6a bc 65 87 6f c9 0e 9d 84 cf 0c 36 e2 e1 e4 68 6b 4f 65 48 08 47 0a 35 56 54 a5 cf 2b 7f 5d d7 3d 09 19 1f 13 28 ab b1 fd b1 a6 1c e3 fb bb 52 d9 35 b5 5a e9 db dd 8e 7f 36 d8 0b 68 af 55 a6 74 e7 2b 99 ae ad 10 8b<br>Data Ascii: Zm6_aSQRxkYH60 4/(rgWh4Ot>t;73%)G_&jfZ:Yjj#l\$RQf%tg(jD&B.;Yh@Aifk0OQa *s#-7rN1oyZvbJq~ ~d"znoXmXk ~ [_ _&W.z..f0L::8=>nwc-Fd3D1')n<6SyZZ-&la"sNB_YcO9yNP~]5GA""b g&}.x ho.^!VS1~jB)]k/?uycV-IQ0eV >Ty _U1coFj]wTaE_nRIH,'6B5 %W*& ny;0KKMKl00WR6(MT+e?[4IOErqLMa-2kcCD\$JH);Mu*2q\$?^D<So+UbEt, ;d<Y_U \j6*.0a7tde ]~^Tvf[><>bonNKIZr"#llq3is&gQ[(6L&jeo6hkOeHG5VT+]=(R5Z6hUt+ |
| Jun 4, 2021<br>21:35:06.213124037 CEST | 2413               | OUT       | GET /wp-includes/js/dist/i18n.min.js?ver=772b1b30d38ec9ba77ae8ae1a39b232a HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.398035049 CEST | 2435               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "253c-5c007b46a283e-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 3678<br>Keep-Alive: timeout=5, max=94<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ad 5a eb 6f db 38 b6 ff 72 3f ed 5f 21 0b 5b 8f 58 d3 8a 9d 3e a6 23 87 31 16 33 53 60 ef 9d 9d 16 b7 5d 60 01 47 35 14 9b 4e d4 51 24 43 a2 f2 58 4b ff fb fd 1d 52 0f fa 91 76 31 b8 48 20 89 e4 e1 e1 e1 79 1f d2 67 2f 07 ce e7 db b8 70 36 71 22 1d bc a3 52 65 e3 1b 99 ca 3c 52 72 ed bc 3c fb 8b c2 b0 ff b0 15 cd bb aa 76 35 6f be fd 78 fa 2e 15 9b 32 5d a9 38 4b bd 94 ed ee a3 dc 51 62 57 cf da 4e 47 7a 39 db c5 1b 4f 2d f2 90 e5 52 95 79 ea d0 b7 2f 1f b7 59 ae 8a 19 4d 89 05 75 89 5d 1c e4 3c 09 06 53 de 0c 06 bb ba 9e 35 93 52 9a b4 8a 92 c4 8b db b9 3c e6 fd b7 64 68 24 62 30 e9 fb ea 66 aa f4 ef 44 ca a5 bf 12 0a cf b5 45 31 57 1c e4 49 3f a3 4f 56 55 1f ae bf ca 95 f2 d7 72 13 a7 f2 63 9e 6d 65 ae 9e 34 d8 4e a6 e5 1d b8 72 9d c8 00 6b dc 48 15 e4 35 ab 81 2f df e3 80 5b a6 66 f6 da 1d 08 f5 b4 95 d9 c6 f9 f4 74 77 9d 25 c3 a1 79 fb 2a fb a4 f2 38 bd f9 1c dd 0c 87 cf ad 78 0c cb c1 dd a4 94 81 fb 8f 6c 5d 26 d2 ad 19 7f 6e b2 bb 5c ca a2 01 6b a7 0d 26 86 5c b5 b7 7d 2d 9b e9 50 0d 87 5e 2a 24 36 c0 f8 bb a1 6a 05 95 ce 30 fa 9a 46 dd 4c 2f e5 8a 76 4f e9 70 48 ff 7e bf 52 3f 89 44 9a 8b 86 b8 55 2e a1 4a 5e 5a 26 09 23 74 60 18 54 e2 19 d2 73 ee a2 27 2a 13 e5 1e 72 dc ec 22 c5 ae cf 35 41 85 e6 4b cf e4 94 6d b2 dc d3 da e4 c4 a0 82 41 d2 c0 17 f3 6e bb d8 6c a7 4b 2a ac fd eb 38 5d 6b ba 78 cc 58 ab 66 39 f1 e8 94 52 1f ec 76 de 41 f4 58 fd 86 f6 3a 38 31 d8 29 32 d1 a5 b8 1b b9 e0 3e 57 b4 5c 76 20 92 06 b0 61 d1 36 cf 54 46 9b f4 6f a3 e2 c3 43 da 32 cb 18 03 4d 20 1c 5b e1 ba 5c 82 bb 85 78 fd e6 47 56 7b bb e9 4f 3f 06 7b 9a 2e cd 56 f2 d9 c0 22 cf 2d 0b e9 10 2f 21 dc c6 16 77 69 a6 96 86 bd c1 d9 e2 4b 11 9e 71 ea b9 ce b2 84 da aa 69 13 49 d4 fe dc b4 b7 79 7c 17 ab f8 5e 77 de 53 67 79 77 2d 73 b4 d6 b1 dc dc 98 0e 89 85 96 51 4e 88 af 57 ba bf 7c f1 78 6e 16 59 8a be af 0d ae a6 f9 85 da 4a 3e aa e0 ec cb e2 cb d5 e3 f9 9b 70 74 c6 ef 48 00 19 ba a8 63 77 5e 9f f1 6d 12 ad e4 6d 96 ac 69 39 dd ed cd 03 6f 31 1d ff 14 5e ad 5f b2 ab bf 56 57 9e b7 f8 c2 c2 11 bb 62 6c ee 5d 8d f0 98 54 3f 2c be fc 35 c4 d7 98 ba d6 d4 37 0f ae 7c fd 89 ef c5 f5 f8 26 fe 9a 15 ea 73 79 0f 1a d9 19 ff 43 3e 01 bd b7 88 c6 ff 5e 86 fa 79 b5 0e 5f b2 b3 98 46 96 d1 6a 25 8b 82 d6 f7 4f 81 40 d9 e4 a3 05 b4 d0 eb 5c 61 83 45 7c 93 d2 06 47 e3 f0 cc f2 9c 19 e9 5e a3 0a 91 b7 42 8b 83 71 60 61 aa 0a 56 77 60 e5 9e ce 64 7e b4 dd 26 4f 46 ad 17 29 3c 66 96 ae 22 e5 a9 aa 5a 84 cc 9a 16 99 69 24 71 c9 73 5e f2 88 17 7c c5 b7 7c c3 13 be 16 53 7e 23 52 3f 91 e9 8d ba e5 b7 d0 ad 19 59 57 2e 26 b3 fc e2 66 96 8f 46 0c a6 dc da 60 ef 14 c8 c9 df 8e 04 bd 67 32 81 66 11 d4 91 eb 20 28 f2 3b 5e a4 21 99 0f f6 15 da 7c 25 02 c1 3a e4 25 d6 29 2f 22 dd df 10 31 2b b1 26 4d a2 9d 09 21 99 ba cd b3 07 27 95 0f ce af 79 8e a9 99 f7 c3 a2 80 0e a6 6a 13 3a 3f 47 29 d4 c8 31 dc 76 b6 8d c5 38 ee 8b c2 75 40 41 e7 a3 1d ed 55 74 ff 0f dc ac b7 28 c3 ee 6b 3c 05 cf 66 52 c8 45 37 16 d6 7a 5f 52<br>Data Ascii: Zo8r?_ [X>#13S`] G5NQ\$CXKRv1H yg/p6q"Re<Rr<v5ox.2]8KQbWNGz9O-Ry/YMu<S5R<dh\$b0fDE1WI? OVUrcme4NrkH5/[ftw%y*8xl]&nk&}\-P^*\$6j0FL/vOpH~R?DU.J^Z&#t' Ts*r"5AKmAnlK*8]kxXf9RvAX:81)2>Wlv a6TFoC2M [xGV{O?{.V"-!wiKqily/^wSgyw-sQNW[YJ>ptHcw^mmi9o1^_VWbl]T?.57]&syC>^y_Fj%O@laE[G^Bq'aVw'd-&OF)<f" Zi\$qs^  S~#R?YW.&f`g2f (:^ !%:%)/"1+&M!yj:~G)1v8u@AUt(k<fRE7z_R |
| Jun 4, 2021<br>21:35:06.413151979 CEST | 2439               | OUT       | GET /wp-content/uploads/2017/09/TONHC-Website-Logo-2-300x106.png HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.577243090 CEST | 1146               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Tue, 01 Dec 2020 23:42:41 GMT<br>ETag: "d293-5b56faec79689-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 7907<br>Keep-Alive: timeout=5, max=100<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 3d 6b 8f eb ba 71 df fb 2b 94 73 70 91 dd 1b 6b 8f 24 cb b6 6c e7 1e 14 09 50<br>b4 1f da 02 0d 02 b4 48 6f 17 94 44 d9 ca 91 2d 45 8f 7d 5c e3 fc f7 f2 a1 07 49 91 12 65 69 db 04 6d 2e b2 67 57 1a ce<br>83 1c 72 66 c8 e1 e8 90 a7 69 79 33 cd d7 cc 04 e1 25 be 9a e5 19 5e a0 19 a4 49 9a 1f 3e 5b d6 2e f0 c1 51 fe da 0c 41<br>fe 0d e6 a6 6d 61 c0 ad 0f ec 11 40 87 00 6e 80 b7 fb fe b9 28 41 5e 9a 39 2c e2 5f 80 9f 40 13 86 71 89 20 0b 18 94 71<br>7a bd 85 71 91 25 e0 fd 70 4d af f0 fb 13 42 ea 27 69 f0 cd 04 55 18 a7 46 14 9f 02 90 11 b8 0b c8 4f 98 58 9a 1d 9e 36 f0<br>72 ac ff f6 d3 b2 4c 2f 07 1b 5e 7a 8d c9 cf db 6b 1c 96 e7 83 6d 59 3f 1c 31 b3 f4 cf b5 65 65 6f 4c 03 bf 42 58 ae cf cf 49<br>7c fd 76 ab 7b 24 8a a2 a3 0f 82 6f a7 3c ad ae 61 d3 4f 6b 67 bd 5b 07 47 3f cd 43 98 13 a6 eb df cd 1c 84 71 55 1c 1c 2f<br>7b 43 8f de cc e2 0c c2 f4 95 82 04 55 5e a0 d6 59 1a 5f 4b 98 1f 1b 99 e3 2b 22 08 29 0f c7 28 bd 96 26 ea 24 78 b0 31<br>8a 0c 84 61 7c 3d 1d 6c 27 7b 33 1c 17 3d 29 e1 5b 69 82 24 3e 5d 0f 01 24 78 c8 93 10 06 69 0e 70 1f 51 5a e9 0b cc a3<br>24 7d 35 5f 73 90 1d fc 1c 82 6f e6 2b 62 51 21 ee 01 a0 71 78 81 2b c5 db 28 0d aa 42 f5 f2 8c 69 a9 5e be c4 45 5c c2<br>90 e9 4e 05 07 4f 44 26 2a d2 ad 27 e4 60 a3 3c 3e 9d 4b b6 0d 79 d0 6b f2 14 17 66 51 be 23 e5 2b fe 52 81 1c 86 0a 9e<br>47 db dd f8 b1 b6 fa 94 ae a9 c9 c1 a8 28 89 70 22 e6 5f c5 97 2c cd 4b 70 45 d2 b4 5c a4 55 89 15 c6 90 e3 54 91 12 9b<br>df 04 55 16 75 bc cc c1 b5 c8 90 b8 d7 b2 d1 73 ac 83 45 9a c4 7d 25 2a 7a cc dc a4 da 5d 4f 57 32 3e 07 ac df fc fc f5 24<br>d3 b1 8f fa 90 80 a2 34 83 73 9c 84 37 0e 61 7f 20 0a 46 41 fa 2c f2 8d 1b 5e 12 18 95 72 4e 86 90 1d a2 38 17 b9 22 98<br>94 4c e1 b7 4a 9e 68 d3 5e 7f 4d c2 35 a1 9f d8 c9 d7 53 a0 42 f1 36 00 09 bc a2 a5 7e 70 b6 36 40 46 e9 a7 e1 bb 51 86<br>12 04 46 79 be 35 0b 9d 4b d6 4d a2 6e 76 a3 6e c6 e7 30 0c a5 38 23 64 cc 10 ce 1b b3 10 4b e1 b0 c9 61 6d 40 3d cd<br>90 a6 27 20 2b e0 a1 f9 85 2e bf 11 b8 c4 c9 fb c1 04 59 86 27 fd 7b 51 c2 cb ea 77 78 16 fd 33 08 fe 40 fe fc 07 04 b7 fa<br>03 3c a5 d0 f8 e3 3f ad fe 2d 45 0a 9c ae fe f5 ed fd 04 af e6 1f d0 c4 59 fd d1 af ae 65 b5 fa 3d 9a ba 68 0e 25 c9 ea 1f 61<br>f2 02 cb 38 00 c6 bf c0 0a ae 0a 04 84 ac 5f 1e 47 4a 86 71 b7 10 7e 5e 21 19 36 d7 b2 98 69 7a 50 75 0a b8 89 06 01 41<br>c3 1c cf 42 75 1f 82 1b ef 01 d0 bf 5e 40 fe 20 37 f1 8f 6a ae 6b 53 2d 1d 67 2a 16 d6 84 86 9e 6b b9 5b 97 97 a3 44 dd 9a<br>c7 90 51 6d 5e 7d 1d ce ca 8b f0 d4 18 b0 d3 48 80 4f 93 ea 72 2d da f5 29 4a a0 b8 0c 11 e3 8d 9f 53 e3 89 7f 7c ff fb 0b<br>f2 58 80 f1 d0 79 0f 3b 0f ad 87 8f b7 3e e6 ae e5 35 25 6d fb d4 9f ce a0 30 bb b1 6c b5 df 41 0e 89 b1 e6 27 3a 6d 42 b1<br>22 f0 d7 83 cd b8 30 d6 11 1b 75 93 d8 77 c6 ca ab cd 7f 2b 07 78 ab 51 6c f6 7b 99 1c 94 a0 0f 8a b8 20 73 86 31 45 92<br>ce d8 62 57 ea d1 00 d7 90 45 bd f3 ec 31 d4 48 37 82 87 8d f5 83 61 1a f6 16 01 77 64 8e 9d c4 56 af 3b 0e d7 f2 4c 97<br>b6 07 e7 fa c8 0d f7 1a 0d 8b 8c 45 c5 78 b1 cc 58 0c 4d bb 47 f3 4f c4 7e fe f8 53 d7 e0 e7 db 30<br>Data Ascii: =kq+spk\$IPHoD-E}leim.gWrfiy3%l>[.QAma@n(A^9._@q qzq%pMBiUFOX6rL/^zkmY?1eeoLBXl v{\$o<a<br>Okg[G?CqU/{CU^Y_K+)}(&\$x1a =l{3=)}[i\$>}\$xipQZ\$}5_so+bQ!qx+(Bi^ENOD&*"<>KykfQ#+RG(p"_KpEUTUusE}%*<br>z}OW2>\$4s7a FA,^rN8"LJh^M5SB6-p6@FQFy5KMnvn08#dKam@='+.Y'[Qwx3@<?-EYe=h%a8_GJq~!6izPuABu^@<br>7jks-g*k{DQm^}HOr-)JSjXy;>5%moIA:mB"0uw+xQl{ s1EbWE1H7awdV;LExXMG0~S0 |
| Jun 4, 2021<br>21:35:04.702666998 CEST | 1171               | OUT       | GET /wp-content/themes/enfold/css/layout.css?ver=2 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.901652098 CEST | 1204               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:46:19 GMT<br>ETag: "1b1e8-55c77967a14c0-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 21559<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed bd 69 93 1b c9 91 20 fa b9 f0 2b 62 9b d6 33 24 55 40 e1 28 d4 41 9a 68 6a 69 d4 b3 b2 1d cd 6a 87 6d a6 dd 7d 7a 06 4b 00 59 55 29 a2 00 2c 12 e0 d1 b0 fa ef 1b ee 71 b9 47 78 64 26 8a ec 55 bf 83 dd cd ae ca cc b8 3c 3c 3c fc f6 8b d7 ea a7 62 be 2a d5 e6 4e fd 61 b3 de 97 eb 7d ef bf ca 3f bd b3 17 ef ab 7d a9 de ef bf ac ca 5a ff f6 fb d5 e6 3e fc f6 97 e2 9e bc fb cb a6 de ab 1f 37 bb c7 62 6f 7e dd ed ef 36 ab 6a 13 be 78 5f 2d cb 79 b1 53 ff a4 fe 5a 2d ef 4b fc ec c7 cd 66 5f c2 a3 17 ef 37 8b 0f e5 5e 3f fa c3 e6 f1 11 60 a2 7f 7a ff 5e fd b0 ae 74 8f d5 66 0d 5f ff b9 5c 56 85 fa 6f 87 72 57 41 8f af 2f 7a bd 8b d7 ea 1f 0d 26 f9 4f 8f c1 ee 1f 3d 1b f9 8f 02 08 be 78 28 8b 65 b9 3b f6 b6 9b ba 02 48 bf 51 bb 72 a5 61 fe b1 7c db fb b9 5f ad 97 e5 e7 37 6a 3a 1c bd 55 17 af 5f 56 75 7d 28 eb 8b eb ab db 57 ba f1 a7 6a b9 7f 78 33 1a 0e bf 7f db 9b 17 8b 0f f7 bb cd 61 bd 7c a3 f6 bb 62 5d 6f 8b 9d de c7 b7 bd 27 3f c6 ec b1 a8 d6 6a b0 d0 58 af 7f 28 77 e7 6a 00 4f 66 7a bf 0f ea b0 7a 73 57 ed ea 7d 7f f1 50 ad 96 ea 9d 5a 55 aa 38 aa 87 b2 ba 7f d8 bf b9 b9 d9 7e 7e ab 1f ad cb be 7d a2 cc 23 dd 3b 20 41 bd af 16 1f be a8 8f c5 ae 42 74 d1 93 1b 3c ec 1f 57 33 3b f2 7e b3 65 bf db ef 5f c0 f8 47 b5 2d 96 cb 6a 7d df d7 5f d9 91 9e 54 73 fb b0 c2 85 ee c5 82 50 05 10 16 f3 7a b3 3a ec 4b 98 60 a7 89 a4 5d cd 55 9f cb 65 c7 f6 e6 d1 7c b3 df 6f 1e 67 eb e2 a3 7d 2b ad 6f 74 39 34 70 cb b5 19 14 1f ab a2 5f 97 c5 6e f1 a0 5b 6c 56 fb 6a ab 8e 0a da aa d1 70 f4 bd fa 4f d5 e3 56 1f ef 42 6f ae 7a 2c 76 f7 d5 ba bf 2a ef f4 8e f4 47 13 d6 77 87 29 db 47 87 35 3e 84 4f d5 c0 3c eb d7 8b dd 66 b5 2a 97 fd bb c3 6a 65 e1 a3 e7 61 77 7c 5e dd 2b f3 ac db 56 9b 47 2b 3d dd 52 84 ca e8 ea c4 99 db ae b2 98 7d 52 3f e6 47 3c 0c 74 27 5a 4e 87 f2 c7 43 d9 f9 b3 03 f2 cc 35 9d 82 4b 57 ee 0c e2 11 dc 95 fb c5 43 b9 6c 3c 85 ea 05 ee b1 ef 76 66 9b 11 e0 1d 0d 59 b9 bd fa fe ad 1b ed cd 10 50 ed 73 df bc 51 48 71 70 54 7d 23 6d d4 6f fc a9 e9 38 34 b4 9a ed 00 4a 6a 00 3f 1f 15 22 70 71 d8 6f de 2a 7c 0e 03 a6 80 0b 3d c0 a6 cc a0 11 d9 a4 23 76 82 27 c0 f4 81 fd e5 c0 1f 6f 76 87 ae f5 f9 4a 3a 4f e7 08 7d 08 a7 ba 33 2e 4d 87 09 26 e1 23 61 ac 2c aa 90 53 71 54 fe 12 99 e4 91 b1 69 c2 47 b5 58 69 6a f4 46 e9 8f 1e de 2a e1 9e e2 b3 35 04 ce 9f 0 2 c0 15 45 6e 2a 75 b7 da 14 fb 37 00 d1 e7 cd e7 dd b2 fa 78 fe 8c 76 11 e0 8f 74 4e 14 fe dd e7 64 70 26 37 c0 bb 55 f5 e6 61 f3 51 1f 28 bf 03 7a b0 a1 08 c1 e7 8f 39 80 bf fb 9a d7 79 74 77 c6 72 b7 d9 2e 37 9f d6 47 03 68 44 d7 b7 11 17 30 2b 56 9a f1 5b 17 fb 92 e0 c7 58 7f f5 42 40 a1 f0 31 a5 12 40 0f dc 26 af 37 eb d2 03 d1 9e 8c 5c 0f d1 d4 01 fb 0f 2b f8 d7 52 01 35 1e 5e 1b aa 96 eb 01 2e 48 dd c3 7d 31 d3 98 70 a4 e7 d1 50 00 58 6c ee b0 20 e9 59 68 c6 88 a3 f8 be fc bc ef 17 ab ea 5e 6f 8a 79 9b dd 12 b9 87 18 b9 96 55 bd 5d 15 5f de a8 6a 8d 87 63 be d2 0c b6 3b 07 8d 84 89 f5 4f a8 e3 14 f0 54 f5 fa 9f ca f9 87 6a df 47 0e e8 4e 33 fc 6f d4 19 fe ac 31<br>Data Ascii: i +b3\$U@(Ahijjm)zKYU),qGxd&U<<<b*Naj?)Z>7bo~6jx_-ySZ-Kf_7^?z^tf_\VorWA/z&O=x(e;HQra[_7j:U_Vu} (Wjx3ajb]o'?)X(wjOfzszWjPZU8---)##; ABt<W3;~e_G-j]_TsPz:K']Ue og]+ot94p_n[IVjpOVBoz,v*Gw)G5>O<f*jeaw ^+VG+=R}R?G<t'ZNC5KWCl<vYYPsQHqpT)#mo84Jj?"pqo*!="#v'ovJ:O)3.M&#a,SqTiGXijF*5En*u7xvtNdp&7UaQ(z9ytwr.7GhD0 +V[XB@1@&7\+R5^Hj)1pPXl Yh^oyU]_jc;OTjGN3o1 |
| Jun 4, 2021<br>21:35:05.213519096 CEST | 1283               | OUT       | GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.405353069 CEST | 1316               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 20 Sep 2019 20:41:37 GMT<br>ETag: "17a69-5930218bfd901-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 33776<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 dd bd 6b 7b 1b c7 b1 2e fa 7d fd 0a 62 a2 05 cf 08 4d 90 94 ed ec 64 a0 11 8e 2c d9 b1 13 5f 64 4b 8e ed 80 b0 9f b9 01 18 12 37 02 a0 48 99 40 7e fb a9 b7 aa bb a7 e7 02 c9 59 fb ec f3 9c e7 38 11 31 97 9e be 77 75 55 75 d5 5b 67 8f 3b 27 57 df df e6 9b 77 27 6f 2f fa 17 4f fa 9f 9c ec 4f fc 34 30 0f bf 58 dd 2e b3 78 57 ac 96 f4 fc ea 06 cf fa ab cd f4 6c 5e a4 f9 72 9b d3 c3 9f 56 9b ec d5 26 df 6e 4f 9e 9c 5f fc f5 f4 fc d3 d3 8b 3f 9f 3c 3e fb af ce e4 76 99 e2 43 3f 56 49 f0 e0 ad 92 ab 3c dd 79 51 b4 7b b7 ce 57 93 93 c5 2a bb 9d e7 dd ee 91 17 fd fc 7e bd da ec b6 c3 ea 6d 14 f7 b3 55 7a bb c8 97 bb 61 42 39 77 ce 83 b0 2c 28 78 28 26 7e a7 4c 12 ec 66 9b d5 dd c9 32 bf 3b f9 7c b3 59 6d 7c 4f 37 6b 93 df dc 16 54 e9 93 f8 e4 ae 58 66 94 e6 ae d8 cd e8 ce 7c e9 05 83 4d be bb dd 2c 4f a8 94 e0 10 f2 5f df a3 ce c8 27 c5 32 cf bc 8e a9 ae 7c 3f 94 9f 70 37 2b b6 aa da f2 b7 f1 e6 24 8d 46 63 95 39 95 57 79 94 f6 b7 e8 45 35 a1 ab 74 b5 4c e3 9d 9a d2 e5 fa 76 3b 53 33 ba a0 0c f3 fb ef 26 aa 88 1e 0e ea 2a 2a fa bb d5 eb dd a6 58 4e d5 35 dd cc e2 ed 77 77 cb 57 9b d5 3a df ec de a9 39 12 2d 22 4f c6 d0 53 cb a8 5a 09 dd 18 f4 c4 b2 3f 59 52 e6 c5 8e df 1c d4 2a 3a fb 75 74 b9 bd bc fd e2 f3 2f be b8 bc 7f 7e 3e ee ed 6b f7 8f ce a6 6a 4d c9 4e 17 db d3 33 75 13 9d 9d fa a 3 cb 2c 3e fd 7d 1c 9c 4d 0b b5 69 2f 2c a1 1a ff b8 a6 fa bd 88 b7 b9 1f 1c 06 28 39 5a f6 d7 9b d5 6e 85 de 8b 1e 64 46 85 0b 45 1d b0 dd 6d 6e d3 dd 6a 13 2e d5 36 9f e7 7c e9 79 6a 9e 2f a7 bb 59 78 ae 76 ab e7 9b 4d fc ae 1c 6e 5b 50 de 4f e3 f9 dc 47 df 53 7b a6 f9 ae 32 25 4c d3 6f e7 f3 4e 14 0f e3 a7 e7 43 a4 1c c5 3d fc f4 25 ff 71 28 cf c6 61 35 33 8c c6 eb 5d 9c 5e 57 b2 c4 90 26 d4 92 45 be 99 e6 9c b4 ef 34 c0 0f 54 5c 4e 1f 6a 6e fe f6 3b 9e e3 11 cf 8e 04 69 77 f9 bd dc 9a 1b 95 1c 54 1e a7 b3 d6 aa f7 1 86 cb a1 9c 69 9c e3 75 5b 32 ce ce 56 d8 a7 ea c5 6b bf 3a 21 13 95 da e4 b1 34 94 1e 61 1a 04 94 2f cf c7 96 fe ad 65 9c f7 e3 f5 7a fe 4e d7 67 33 e5 09 bd 45 06 93 62 b3 dd 1d cb 20 bf f1 cf 29 cd 3c 7e 6f 92 d3 0b 4a 93 df b4 74 b7 33 5a 2a 8d 7a 71 cf c7 50 26 e1 b9 ed eb 5a 3d d3 67 d1 79 b7 9b 3e 4d 86 23 1e dc 74 3c 0e 47 63 64 bf cc 8e b6 d2 0e d6 7e df 1c 57 99 0f e1 54 6d 89 16 85 b4 80 e9 47 6d d7 dc 6d 74 c7 17 07 45 c3 75 bf a3 32 22 5e 69 fa da 29 0f cd a1 75 42 fd 9e 29 5a fe b4 ea 6d 27 8e ce c7 fb 3d ad e4 59 74 41 eb de 3e 36 cd be 8a 3a 17 83 09 e8 58 b2 5a cd f3 78 59 52 cd 69 b7 eb 5f 45 d3 4a 66 33 9d 59 af 17 a8 06 99 9d ee f7 44 06 b6 5f 98 7a 4d 83 fd de 9f 12 19 09 a8 f4 28 2a 28 bf a9 4c d8 d9 e9 69 30 98 3d 2d 06 c8 88 08 ac ac 24 3f af 94 14 04 a8 57 76 52 d0 72 0c e2 68 3a ca c6 34 4a 39 7e bc df 7e e3 25 ff db 6f 44 35 a3 ac db 9d d2 4f 8a fa d2 e8 d0 0f aa f1 6a 1e 17 4b e9 78 da 7d a8 26 58 5e c5 96 57 3c 3d 08 82 a1 9f d0 ff a9 fd 44 2f e3 6e b7 7c 19 07 c3 18 c3 1a da e7 6e 5e fc 96 fa 00 f5 89 cc 60 f8 57 d4 eb 94 69 f8 76 55 64 27 e7 ba 36 9c<br>Data Ascii: k{.}bMd,_dK7H@~Y81wuUu[g;\'Ww'o/OO40X.xWl'rV&nO_?<>vC?Vl<yQ{W*-mUzaB9w,(x{&-Lf2; Ym O7kTX f M,O_'2 ?p7+\$Fc9WYEsILv;S3&**XN5wwwW:9-"OSZ?YR*:ut/~>kjMN3u,>)Mi/(9ZndFEmnj.6 yj/YxvMn[POGS{2%LoNC=%q(a53)^W&E4T\Njn;iwTiu[2Vk;!4a/ezNg3Eb}<-oJt3Z*zqP&Z=gy>M#<Gcd-WTmGmmtEu2"~i)uB)Zm'=YtA>6:XZxYRi_EJf3YD_zM*(Li0=-\$?WvRrh:4J9~~%oD5OjKx}&X^W<=D/n n^`WivUd'6 |
| Jun 4, 2021<br>21:35:05.414107084 CEST | 1351               | OUT       | GET /wp-content/themes/enfold/js/aviapopup/jquery.magnific-popup.min.js?ver=2 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.606916904 CEST | 1403               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:47:36 GMT<br>ETag: "51d3-55c779b110200-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 7594<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ad 3c 6b 73 db 38 92 df f7 57 c8 a8 8b 43 8e 20 4a 4e 6e 76 a8 a1 75 89 c7 d9 b8 26 4e 72 13 cf 65 27 3e 57 8a 12 21 09 63 8a d0 90 94 1f b1 f4 df af bb 01 90 20 25 25 a9 ad ab 54 6c e2 d5 00 1a fd 6e c0 fd 1f 8e 3a 17 f1 3c 93 33 39 ed bc 57 ab f5 aa d3 eb dc 0e 82 9f 82 9f e0 e3 d9 60 f8 bc 37 7c d6 7b f6 e3 df 7e e8 2c ca 72 15 f6 fb 89 5c 16 62 29 32 75 1b 4c d5 b2 bf 4a d7 73 99 15 fd a5 01 d2 5b 21 90 3e f4 3f 55 ab 87 5c ce 17 65 c7 9b fa 04 aa f3 cb 52 96 f9 43 e7 83 1e 3f ea fc d0 ff 9b 37 5b 67 d3 52 aa cc 13 fe e3 6d 9c 77 4a 9e 71 c9 15 cf 79 cc 0b 9e 46 ec 34 55 85 60 7c 1a b1 97 62 a6 72 61 ca 49 c4 5e cc 4a 91 9b e2 da 36 bf 58 ad 44 96 30 be 8a d8 45 9c df ac 57 ef e3 1c 3b cc 22 f6 0e 5a 18 5f 02 c8 45 9c cd a1 6e 1e b1 e5 6c c5 f8 22 62 01 eb ce f9 2d 95 7b b9 88 93 07 c6 4f 6d 69 a9 6e 65 36 67 fc 41 57 ac 72 71 2b b2 b2 37 d5 33 df 45 d5 16 fc c7 2d 9f 44 47 47 77 32 4b d4 5d f0 e7 7f af 45 fe c0 cf 23 e1 e9 1a 9f df d7 9d 05 cf fc c7 32 10 b7 01 14 e6 5d d1 5d 40 c5 96 df d4 3d 0c 2a 34 5e f2 28 51 d3 35 20 ae 0c a6 b0 c0 52 9c a5 88 c6 d2 63 89 bc 65 fe 28 17 e5 3a cf 3a 79 30 4d e3 a2 78 1b 2f 85 5e 2d eb 96 5c 1e 1f 7b 79 20 b3 4c e4 af 2f 2f de 44 d2 e7 6a 9c 1d 1f 67 41 4c d8 3a 5d c8 34 f1 72 3f f4 72 58 6b ee 73 68 cb 4d db a5 f2 32 df e7 f9 96 5f d 6 2b 83 75 99 b5 97 70 c4 73 00 1b 67 49 2a 72 d8 07 36 f1 32 28 60 99 71 9a 4e e2 e9 4d 01 b3 67 51 16 4c 17 71 fe a2 f 4 06 7e 50 aa 37 ea 0e 8e 2e 2e 84 e7 77 b3 a0 48 e5 54 78 c3 f6 b8 ab ec fa f8 78 a7 0a d7 95 3e 00 72 44 20 8b 17 79 1 e 3f 78 d2 1f cb f0 4a 5e fb 80 bf 33 67 95 fe a3 c1 4a 16 45 51 81 b0 a6 eb 3c bf 14 cb 55 0a 08 0c e8 00 5f 96 d9 66 e3 1d 68 01 6c e8 f9 b1 ac c9 29 c8 05 f4 81 e5 b2 27 a5 2c 53 f1 84 e9 55 97 44 88 80 a9 22 ca 70 23 7b e1 6d f9 67 97 5a 44 60 d9 86 58 0f 4e a8 28 e3 6c 2a 70 41 51 26 ee 3a 77 00 48 66 b2 f4 7c 7e a8 6f 54 c2 a6 3f b8 50 91 5a c4 41 6a 59 31 1f 96 fb 90 0a 5e 46 57 6c 59 30 ce de c1 ff 0b f5 05 7e 7e 14 93 1b 59 b2 eb 91 9c 79 b7 4a 26 9d c1 51 14 09 38 e4 38 2b 24 82 f7 35 42 8f 06 23 e0 35 6f 54 06 a9 c8 e6 e5 62 e4 c3 80 32 00 de 87 f3 64 97 55 77 26 b3 8e a8 c7 98 8f e1 76 74 17 ac 72 55 aa f2 61 25 a2 c7 a9 82 bd e4 eb 69 a9 f2 f0 8e e3 7e c3 d6 76 80 7c e2 5b 39 8f a1 07 1e ff ff 88 bc 80 46 98 5e 16 e7 67 3f 46 bd 21 2c 33 03 94 24 e2 fe dd cc 63 17 1f ce cf 3a 3f 06 0c cf 01 7b fc 7d 7f 8f bf db 1e 40 8d e7 67 91 81 b6 d9 98 41 d4 f4 22 4b 72 40 44 d4 8f f5 47 7f 2e 83 52 14 a5 97 19 e0 ef 3e 44 7d b9 5a a8 4c 6c e4 2a 4e e0 87 6a 75 2a d6 ab 95 ca cb a2 46 4b f4 c1 c3 06 40 c1 24 9e a4 0f 17 6a 22 53 11 39 d3 99 35 bc fb b0 d9 f4 3d 10 5b 79 dc b9 00 bc f8 9b 5f 25 f2 d9 e6 4e 4c a0 ed 25 d0 e1 cd 4b 91 e7 0f 1b db 09 20 f9 1b ef 23 49 9b a2 f3 1e 97 e5 6f ce cf f4 0c 7d bb aa 0a 97 eb 42 e4 2f e6 40 17 20 10 80 d6 2d cd d0 e2 90 ca 8a d3 78 ba 80 13 da 6b b9 02 61 10 ba ac 25 81 4a a5 33 28 98 a8 e4 c1 f7 47 24 ac 90 80 00 dd c5 bb c9 9f<br>Data Ascii: <ks8WC JJnvu&Nre">Wlc %%TIn:<39W 7[{-,rb)2uLJs[!>?UleRC?7[gRmwJqyF4U]'lbrai'J6XD0EW;'Z_Enl"b-{Omine6gAWrq+73E-DGGw2K[E#2]]@="*4"(Q5 Rce(:y0Mx/^-\{y L/DjgAL:]4r?XkshM2_+upsgl*r62(' qNMgQLq ~P7..wHTxx>rD y?xJ*3gJEQ<U_ fhl)',SUD"p#{mgZD`XN(l*pAQ&:wHlf~-oT?PZAJY1*FWIYO~~YyJ&Q88+\$5B#5oTb2dUw&vt rUa%i~v[j9F'g?F,1\$&c:~?j]@gA"Kr@DG.R>D)ZL]*Nju*FK@&\$"S95=[_y_%NL%K #lojB/@ -xna%J3(G\$ |
| Jun 4, 2021<br>21:35:05.611881971 CEST | 1410               | OUT       | GET /wp-content/plugins/jetpack/_inc/build/jquery.spin.min.js?ver=1.3 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecclvdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Jun 4, 2021<br>21:35:05.812607050 CEST | 1560               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "70e-5c3db85dd0be9-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 697<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 03 95 94 4b 6f e2 30 14 85 f7 fd 15 26 0b 64 53 e3 42 e9 74 aa 54 d1 2c e6 a5 4a 9d c5 68 46 9a 45 d5 45 26 be 01 a3 60 bb b6 29 45 90 ff 3e 8e 4d a0 0f 06 95 0d 49 4e ee fd ee f1 b1 c3 59 0f 7d 51 48 2a 87 66 8a 8b 72 89 dc 44 58 54 8a 0a 10 17 06 0a 57 2d 19 ba 71 c8 8b 85 9a 69 af 73 54 1a 35 43 ca 4d c0 84 42 cb 50 ef ec e4 ac d7 3b 41 3d f4 59 e9 a5 11 e3 89 43 b8 20 e8 7c 30 1c f6 fd cf 08 7d 83 4a 3c a1 ef 32 b7 b6 29 bb 15 05 48 eb 59 73 c9 3d c6 b3 d0 8f 9b df a8 8a f2 49 03 ec 94 73 59 38 a1 24 06 b2 12 25 4e d4 df a9 f7 93 64 99 5b 6a 50 25 82 27 ad 8c b3 04 b0 81 87 b9 37 8b 93 e9 c3 1c cc 32 21 74 ab 58 2d 64 42 c8 35 54 16 50 43 69 a9 3b 0e 87 52 48 e8 76 e3 95 e5 33 4e e2 2d be 6b 81 34 72 ee 29 44 52 e3 a7 b3 10 92 ab 05 fb e5 df 48 30 c4 d4 8c 5a 20 09 0b f4 d5 18 65 70 d2 bc 60 53 1b c2 d5 06 2c 48 97 f8 76 bc e9 9b fe 6c d0 f4 15 a5 ae f1 6e dd 54 92 15 b0 52 b2 66 7a b6 d5 2d 15 64 65 c0 cd 8d 0c db c5 20 2f 26 bb 36 b2 7a cc 7d a4 19 e0 e6 a5 cf 22 73 8c e7 2e c7 e4 da db 36 01 e6 47 75 bb bb 7b 66 9d d2 98 50 0e 15 38 40 5b 9d d0 ce b0 93 65 36 6c c0 a3 12 1c 0d fc 23 b6 19 30 78 72 20 39 5e 15 aa 52 26 15 eb b5 63 85 b5 38 09 cf 09 a9 e9 d6 38 0b 8b 77 f6 ce de af d7 96 10 16 ce 47 b7 bb e5 59 56 81 1c bb c9 0b 69 21 f8 2b c5 e4 5c cc 6d 5c 9d ce 36 e3 74 ce b9 90 e3 7e 05 65 93 ae ce 62 43 96 65 fa d3 20 d5 b9 b1 70 23 1d d6 74 38 20 b4 19 54 3a df aa e6 0e cc 9f 66 02 26 fd f3 1e 6e 1d 9c 6e e6 9e 6e a7 f5 75 df 46 c3 6d 38 9b c7 7a 1b 52 d6 ec b9 df 15 12 84 18 7a 5d ef 4b 20 5b 39 21 97 e9 aa f2 87 cb a6 57 34 0e 4d cf 69 18 ea af 71 68 3a aa a9 9d e5 55 f5 a6 f2 62 53 39 6a 2b 3f d4 b4 ca cd 18 da ca e1 a0 2d bd da 94 5e b4 a5 57 b5 37 45 9f 7f 54 6f fc b1 85 f6 16 4d 2e aa f4 72 40 ad 06 e0 e9 90 8d f6 ac 84 05 7f cf 8e c1 3b 96 b4 6f 1c d9 a3 ce c0 77 cc fe cf de 17 c2 7b d9 21 ac 37 e8 5d 6a 97 af 53 fb f8 6e f6 5d 12 32 89 27 f1 fe f9 0c 2f ec f7 18 1a 0e a0 c2 41 7b c1 0a ca b1 b0 18 e8 31 c6 62 c7 21 d8 51 d6 0e e0 c2 86 1c 63 2d 34 1c 40 1d 65 2c c2 6a 1c ff 8b c9 f5 3f 05 f1 03 34 0e 07 00 00<br>Data Ascii: Ko0&dSBtT,JhFEE&')E>MINY}QH*frDXTW-qisT5CMBP;A=YC [0]J<2)HYs=IsY8\$%Nd[jP%72!tX-dB5TPCi; RHv3N-k4r)DRHOMZ ep`S,HvlnTRfz-de /&6z)"s.6Gu{fP8@[e6l#0xr 9'R&c88wGYVi!+lm6t~ebCe p#t8`f:&nnnuFm8zRz]K [9!W4Miqh:UbS9j+?~^W7EToM.r@;ow[!7]Sn]2'A[1b!Qc-4@e.j?4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.814546108 CEST | 1561               | OUT       | GET /wp-includes/js/jquery/ui/core.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Jun 4, 2021<br>21:35:05.999996901 CEST | 2004               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "f59-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1811<br>Keep-Alive: timeout=5, max=95<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 95 57 6d 73 db 36 12 fe de 5f 41 e1 6e 54 a2 82 29 a9 ca b5 09 15 9e c6 b1 95 c6 73 89 ed 73 9c e9 07 55 bd 81 c5 95 84 94 02 54 10 74 ec 8a fa ef b7 00 48 89 b2 e5 99 bb c9 4c 4c 2c f6 0d fb f2 ec aa fb 43 eb bb e0 87 e0 eb bf 0b d0 8f c1 97 8b e0 4c 69 08 fa 51 bf 1f bd b2 17 4b 63 d6 71 b7 fb f5 4f 7b 5f 88 68 a6 56 48 b6 37 67 6a fd a8 c5 62 69 6a e1 f7 aa 90 29 37 42 c9 80 cb 34 50 66 09 3a 98 29 69 b4 b8 2b 8c d2 b9 95 ba 81 0c 78 0e 69 80 bc 78 8d 3c c1 a7 8b db 20 13 33 90 39 44 cf 4c 46 4a 2f ba d5 6d 65 b8 ba e7 6b 11 35 dd ea ce b8 81 85 d2 8f dd 42 9c cc f0 15 5d 64 ee 7e d7 9a 17 72 66 9d 0a 81 6e 48 7d 20 49 62 1e d7 a0 e6 41 0a 73 21 a1 dd f6 7f 23 be 4a 47 fe 33 9c 10 af 9e 4c 19 d0 18 42 ff 4c ba 0d 77 1a 39 dd dc 73 1d 00 33 4c 32 31 ac e9 81 0e 91 e4 ef 90 ce 74 02 91 54 29 5c f2 15 44 46 7d 54 df 40 9f 61 10 42 3a d4 60 0a 2d 09 d7 c0 d1 a5 44 8f 42 91 84 12 f9 d7 48 92 e6 12 a5 68 24 51 8e b5 c2 16 44 4b 0d f3 b2 6c 89 b2 24 2b be 26 ad 24 91 2f 68 a6 ed 76 d8 6a a1 36 1e 12 b1 5a 4c 8a 1c 50 22 f9 fe 6f a4 23 3a e4 fb 29 a1 93 de 14 99 54 28 28 a5 71 d8 fd 3d 14 72 5d 98 32 c7 04 cd 4c 69 e0 c1 58 af 4a 4c 9d 51 b2 54 77 5f 91 4c ff de 8d 0c e4 26 d4 74 84 ee a4 22 e7 77 19 a4 31 f1 de b7 db b5 8b c6 a9 06 ba dd c5 c4 9e 36 fe b9 01 8f e0 61 ad a3 b9 c8 0c e8 3c ba 17 b9 40 35 c8 d0 6e b7 38 fe a9 5e 9f 87 34 e2 69 fa 8e cf fe c0 2f cf bd 0f 7e ad 8d 2c 45 9a 82 cd 68 c2 a3 59 9e 87 66 29 72 46 9c 52 91 09 f3 48 e8 96 46 19 c8 85 59 6e 79 54 60 48 f0 bf b2 dc 6c 99 f5 c3 80 4c 43 4b 61 9b 7b 74 06 35 c7 c4 97 3f 61 7f c0 e3 19 46 37 de bc 3b 3d fb d7 e7 eb d3 b3 71 fc 9a 9d 5d 7d fa 74 1a f7 5f bf 66 e7 e3 8f e3 db 71 fc ea 27 76 7e f5 eb 65 fc aa c7 c6 97 e7 f1 e0 1f 8f e7 76 7c 13 f7 07 6c fc f9 ec f4 7a 1c ff 83 3b fb 70 f5 69 1c 0f 7e 62 1f c7 ef 6f e3 c1 cf ec fa f4 97 f1 7f 9c d8 e0 95 3f 7c b9 8e 07 03 76 3d be b9 b8 3a 8f bf 6f 7a ec e6 e2 97 0f c8 fb 86 79 cb 83 1f d9 ed e9 bb f8 0d b3 8c af b7 5b 8a ee cf 65 fd 82 4d 3e d3 2a cb ae 5d e0 e2 66 cd db 2a 34 89 0d 8a 8b 0e 59 ab 5c b8 16 a0 4c 26 84 df e5 2a 2b 0c d8 f0 19 26 12 18 75 43 8e dd 5a 7a 7d a5 0f 2e ed c6 07 64 da 65 e0 55 ee 33 f5 3c 3f ae 37 b0 00 2d 63 5d ea 61 4b 62 f1 e6 06 71 62 66 eb 17 9e 3a 85 35 20 7c 8d 55 57 0a d3 32 cf d4 37 42 3b 4f 28 27 8f 47 68 0f a8 02 f3 0d 7f 86 bd 5d 7b cd c5 03 a4 d6 9a b1 15 ea 4b 61 04 b1 f7 0c fb 20 52 df 24 e8 73 35 2b 56 f8 98 b2 4c ab 2f ba 65 85 14 08 02 17 69 1c 42 d2 63 cf 8a 2f 70 41 00 3e 5b 36 1f ee 88 22 2d cb b0 fa 4a 08 62 92 48 4f 48 27 e8 74 b0 2b f0 1f d3 b0 42 a7 bf d4 fa ff 47 d5 dd fd bd a6 df d2 4e dd 8b 95 0d 0c 5c 15 ea c8 ab 3e 35 46 63 f3 a7 b6 fe 7d b9 ec aa dd b6 df 84 c4 88 6c 1b 44 6c 1e 57 0d 39 c3 86 37 70 9d 43 91 aa d1 11 da de 11 b3 f3 bd 59 6a 9e d4 6a f1 c8 6a 75 20 88 86 1b d5 68 81 f2 08 9b 9c 0c a6 18 eb 39 86 dd 01 4a fc 5c a9 c3 d4 96 c8 2f 99 25 fa cf ed d3 80 11 c3 ef 04 ce 11 9b 73 94 c7 d3 dd 33 71 5f fe c7<br>Data Ascii: Wms6_AnT)ssUTtHLL,CLiQKcqO[_hVH7gjbjij)7B4Pf:]i+xix< 39DLFJ/mek5Bj]d-rfnH} lbAs!#JG3LBLw9s 3L21tT)\DF}T@aB: '-DBHh\$QDKI\$+&\$/hvj6ZLP"o#:)T((q=r]2LiXJLQTW_L&t"w16a<@5n8^4i/-,EhYf)rFRHFYnyT`HILCK a{t5?aF7;=q]}t_fq'v-ev\lz3pi-bo? v=:ozy[eM>]*f*4Yl&*+&uCZz}.deU3<??7-cjAkBqbf:5  UW27B;O(\Gh){Ka R\$S5+VL/eiBc/ pA>[6"-JbHOH't+BGN!>5Fc}DIW97pCYjju h9JV%6s3q_ |
| Jun 4, 2021<br>21:35:06.008611917 CEST | 2063               | OUT       | GET /wp-content/plugins/jetpack/_inc/build/facebook-embed.min.js HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Jun 4, 2021<br>21:35:06.193198919 CEST | 2405               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "2e1-5c3db85dcfc49-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 460<br>Keep-Alive: timeout=5, max=94<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 00 75 92 4d 6f bd 30 0c 86 ef fb 15 aa 06 18 72 a2 ca fb b8 25 30 86 66 b6 80 00 5d 2f dd 61 c0 b0 83 2d 51 89 5a 59 f4 24 3a 98 51 e4 bf 57 ce ba 74 0b b6 9b 48 be a2 f8 f0 55 35 63 9f 90 05 24 d6 a1 71 76 64 b4 73 89 59 e7 81 19 17 41 93 1f 15 db 10 cb 49 8d 5d 9f f3 86 d9 88 1d 43 da 41 3c 0a 93 62 b3 ea 55 35 63 5b 8f 6d e3 d9 7a 25 d9 7d 6f 5b e8 da 2c ce a5 0b 3b 04 4d 0e 83 80 f2 71 df 44 46 f5 29 f3 2b 01 92 64 90 66 c9 87 60 c0 ba 00 86 5f d4 34 f6 80 36 b7 2b 8a f5 4a 7d 5d af 3e df 7c f8 7d 50 7d 13 13 88 72 21 04 d4 06 f5 d0 41 20 a5 23 34 04 d7 1e a6 48 70 e3 f6 bc 2c 95 33 35 b7 ed 65 44 24 2e 4f da 2d d0 b3 30 ad c6 2f cd f6 b6 e9 40 f0 16 cd c8 cb 6f 6f be ab a6 ef 21 98 8f 3b e7 4d 1e 5b 52 cd ab 4a 63 08 79 25 ca 36 1a 5a c4 07 15 80 2a 3e 3f c1 2a 8f ba f1 30 e7 55 32 0f ea 3e bd fe 69 db ce d7 6f b9 7c 91 e4 be ce 14 85 a0 79 cd 8b 1c 6c f2 74 f3 b3 72 7e 6e aa ee 21 a6 bc a3 7a ff 4e bd e7 52 84 ff 82 26 1d 5d 4f 13 b6 02 ba 22 8a ae 1d 28 d3 a4 a8 b9 a4 52 0a f3 72 f5 c7 00 71 bc 03 9f 39 30 fe 79 35 6f 34 d7 6f d1 80 72 21 41 a4 15 58 8c 20 b2 2f 65 79 58 82 b2 ed 55 1a 83 de 04 f7 97 7f d9 12 97 53 e2 f1 08 b3 38 43 91 cf 10 0b 7e a4 38 94 f2 dc c2 83 fc 97 eb 2e d8 a9 2b dc e9 88 de 17 c5 69 fe c9 21 d5 18 73 bd cf d1 8d 4b 04 01 32 47 8f 89 2e 3d 36 e6 08 4c b9 ad 98 7e 72 b9 7c 02 9d cc c1 bf e1 02 00 00<br>Data Ascii: uMo0r%0fk)/a-QZY\$:QWtHU5c\$qvdsYAl CA<bU5c[mz%]o[;[,MqDF]+df_46+J]}> P]r!A #4Hp,35eD\$.O-0/@oo!;M[RJcy%6Z*>?*0U2>iojyltr-nlZNR&]Ok"(Rrq90y5o4or!AX /eyXUS8C-8.+i!sK2G.=6L-r                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.195882082 CEST | 2406               | OUT       | GET /wp-includes/js/jquery/ui/effect-transfer.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Jun 4, 2021<br>21:35:06.390338898 CEST | 2433               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "359-5c007b4699b9b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 502<br>Keep-Alive: timeout=5, max=93<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 6d 92 4d 6f d4 30 10 86 ef fd 15 ae 0f 6d 5c 65 1d 56 e2 14 9a ee a1 02 51 09 90 40 8b 38 20 0e 59 7b bc 71 95 78 82 ed 2c ac 56 f9 ef 9d 7c b5 cb c7 c9 33 e3 d7 af 1f cf 38 bb b9 bc 60 37 ec f1 73 07 fe c8 be 3e b0 b7 c6 80 8a 81 6d 7d e9 82 01 cf d6 72 bd 96 af 07 51 15 63 9b 67 d9 e3 cf 41 db 59 a9 b0 a1 f2 b0 73 8f ed d1 db 7d 15 17 a3 77 d8 39 5d 46 8b 8e 95 4e 33 8c 15 39 29 74 d1 db 5d 17 d1 87 e1 d4 17 a8 a1 0c a0 19 69 69 9b 34 ec e3 c3 96 d5 56 81 0b 20 ff b9 52 a2 df 67 f3 ee 7c f1 bc 5f b6 56 9e 63 65 71 a6 5f c1 89 9c 8c b4 d9 c5 a5 e9 9c 1a 98 12 10 27 be 24 bc 28 e2 b1 05 34 4c 83 b1 0e ae ae a6 55 96 8d de 4c 61 f2 9d 4f ee 3c e5 32 9b 2c f9 8f 14 44 0e c9 f4 60 d1 27 cf e6 4a 9c 3c c4 ce 3b a6 e4 a4 0d f3 2a 17 ac e2 85 24 8d e2 74 28 3d b3 85 4a 62 65 83 48 1d 45 20 23 8a d4 14 dc d8 df a0 09 b1 70 52 85 90 f0 16 83 1d a9 45 8a a4 e3 3b d4 47 8a 43 61 36 28 83 f2 58 d7 5b 6c 13 91 bf 4a f5 59 ed 03 98 38 16 91 8c d0 98 00 94 52 72 8a d8 e6 48 97 b5 ab 90 d6 24 a2 64 58 56 3a ad 60 18 68 ee a4 75 0e fc fb 31 a3 33 bf ac 8e d5 52 fd 36 24 89 e8 89 d9 be d8 fa 01 ec 56 db 03 53 75 19 42 71 dd d9 79 0e 61 b5 74 e0 fa ee 36 23 c5 1d 17 b2 6c 5b 70 7a 8b 89 46 d5 35 e0 a2 1c 1e 45 75 ad ef 87 f3 d4 8c d1 e7 53 d9 80 18 bb 30 52 bb 73 6a f7 17 b5 fd 2f b5 fd 83 3a 5d 7a 99 9b cd dc e7 9c 97 bb 80 75 17 81 f7 04 e0 6c 53 46 48 30 05 a9 3b 3f 7e 67 0a e9 cf 5a b7 4f 9f 47 48 e3 96 1e 1a 3c 00 79 d2 65 bd e8 7b f1 e6 09 85 a3 f0 8f 59 03 00 00<br>Data Ascii: mMo0mleVQ@8 Y{qx.Vj38`7s>m)rQcgAYsjw9jFN39)tjii4V Rg _Vceq_\$(4LUlaO<2,D`J<.*\$!(=JbeHE #pRE;GCa6(XlJY8RrH\$dXV: hu13R6\$V\$uSbQyat6#l[pzF5EuS0Rsji:]zulSFH0;~gZOGH<yey{Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Jun 4, 2021<br>21:35:06.391643047 CEST | 2434               | OUT       | GET /wp-includes/js/jquery/ui/widget.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Jun 4, 2021<br>21:35:06.578685045 CEST | 2563               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "1aab-5c007b4699b9b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2543<br>Keep-Alive: timeout=5, max=92<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 b5 19 db 8e db b8 f5 7d bf 42 16 0a 2f 19 33 9c 99 a2 4f f2 aa 46 90 0b 1a 60 bb 49 db b4 79 f0 ba 03 8d 45 db 4c 3d a4 97 a2 66 76 6a eb df 7b 0e 2f b2 24 2b d3 74 81 be 58 d2 21 cf e1 b9 5f e8 ab 17 93 ef 92 17 c9 97 bf d4 c2 3c 25 7f 7f 9f 7c 96 e5 56 d8 e4 86 df dc f0 3f e0 d2 ce da 43 76 f5 e5 17 dc 51 4b be d6 f7 00 c6 95 d7 fa f0 64 e4 76 67 23 fa 3b 5d ab b2 b0 52 ab a4 50 65 a2 ed 4e 98 64 ad 95 35 f2 ae b6 da 54 88 f5 57 b1 17 45 25 ca 04 f6 c2 32 ce 49 fe fc fe 53 b2 97 6b a1 2a c1 2f 8e e4 da 6c af c2 6a 38 ac d1 07 c9 bb 6c 5d 79 36 f8 a3 13 e1 0a 76 5e 7d 37 d9 d4 6a 8d 1c 11 4b 8f 69 fc 48 f3 dc 3e 1d 84 de 24 a5 d8 48 25 a6 53 ff e4 c5 7d b9 f0 af 64 99 7a da e9 8a 59 9a 59 e2 89 d3 86 b4 14 4b 7a 7c 28 4c 52 31 99 5f b3 22 7f 65 4c f1 c4 0f 46 5b 8d c4 79 85 4c cf 8d b0 b5 51 49 c9 d7 20 b6 7a 53 d8 22 27 55 de f9 64 5d 0e 37 da 10 a4 29 98 64 2a bf 9e ab 7a bf 9f e4 44 e6 76 a9 56 74 ae 66 33 6a cd d3 91 08 a0 70 0b aa 2e 88 64 a9 78 10 ca 56 29 a5 d3 a9 e0 46 dc eb 07 14 88 48 ca 41 f1 db ad 30 7f 02 6b ec 85 21 a9 5f 4c 69 b3 2e ec 7a 87 07 36 15 fc 36 94 95 41 6b f9 99 1b 60 41 78 09 15 ab 98 66 06 64 3c 36 ac ce 2d af 0e 7b 69 49 ca 53 ba bc 5e 45 11 6d 7f e1 66 c5 c4 e9 04 9c 4a d0 4f c9 bd 5f e1 41 e2 d7 83 59 a6 59 ba 5a 12 95 d7 b3 f4 65 3a b3 c0 aa fe 51 3f 0a f3 1a 5c 83 d0 55 de 55 8a a7 3f 99 94 dc 49 6c 99 a2 0d 2b 97 f5 2a c7 9f d3 09 98 aa dc eb d2 ae 98 8e 6f 5d 49 0e b9 21 13 bb 93 15 bf 5d 1b 51 58 11 f8 09 bc 2b f1 98 68 b7 71 5e 98 6d 7d 8f 0a e5 7b a1 b6 76 37 9d 5e a2 b9 9d 8d 93 c5 0a 55 12 0d 0a 3a 3e 08 53 c1 71 99 e0 e1 8d dd 3a 67 c8 da 6d c0 a8 a0 ec 76 bd 93 fb f2 b5 56 95 35 f5 1a c3 22 5b ae c0 04 c4 e4 c8 06 98 4d 1f 90 6f f4 12 6f 94 0e be 89 8b 4e 93 05 18 51 9c 1d 48 80 66 8e f1 2b a9 48 54 5d 22 cf 6e b9 14 2b 5e 1c 0e fb 27 82 62 b1 56 5a da b4 88 fa ac f4 67 30 c1 6d 4a 2e ab 77 f1 70 45 17 05 6c 39 ab dd fb 0e 68 2a f7 0a ac ea 83 30 e0 0b 9d af 57 48 ae f5 9f 33 3c 07 f2 83 5d b9 66 36 57 e3 ac 77 37 e7 e2 12 55 32 db 64 8e 39 05 7a d6 67 91 2e 34 6c d8 d1 03 de 62 4c 7d 34 90 0a 7e cd aa e9 d4 f0 0b f0 e9 64 1b 56 b0 e3 fa 6c c8 4c 33 55 dc 8b ea 50 ac 45 56 33 8f f2 13 40 32 1b 3e de 41 3c 3b 00 32 52 2d 48 b0 21 ba d7 d0 29 58 df 7f 51 97 32 17 67 de e7 91 77 22 79 7b ea 0c 42 6f 26 f9 f9 64 88 5b c1 bd 1f ba 30 87 e4 6b 45 32 76 1e cd e4 08 94 1f ea 6a 47 f4 39 41 f0 3b 83 4f 60 0a 80 ba 61 03 0d e6 5f cf 66 05 5f 17 fb 3d 69 cd c6 6e 40 05 90 39 35 98 d5 87 da bc fa 41 cf 2b c8 71 88 28 12 09 71 b9 ac 56 54 e6 f8 00 f3 31 7c f2 5d 51 7d 78 54 1f 8d 06 fb da 27 22 20 ed 3d 68 59 26 d7 93 3c 97 d3 29 41 af fc b8 2f a4 fa 70 f7 45 ac 41 3d 74 61 d1 f6 43 38 02 e9 62 24 c6 70 81 49 9a 8d 2c 01 d4 d1 92 b4 f5 da 66 a8 9a b3 0a 7a 34 9c e9 1a 8e f7 5d e1 74 d2 60 ca 8d 5a ea 4e ec c8 10 3c 79 0a 96 90 6a 7b 2e 58 5f d7 24 ba 7d cb d5 c2 05 81 73 ae 91 80 8c 99 14 c3 c8 44 51 52 09 66 2f d4 5a c0 61 b9 5c 40 95 12<br>Data Ascii: }B/3OF`lyEL=fvj/(\$+tX!_<%)V?CvuQKdvg#;jRPeNd5TWE%2lSk*/lj88jly6v^?j7KiH>\$H%\$)dzYYKz {LR1_ "eLF[yLQl zS""UdJ7]d^zDvVtf3j.dpX)FHAOk!_Li.z66Ak`Axfid<6-[iS*EmfjJO_YYZye:Q?UU?Il+*o]@!jQX+hq^m} {v7^U:>Sq:gmV5"[MooNQhF+HT]"n+^bVZg0mJ.wpEI9h*OWH3<jf6Ww7U2d9zg.4bLj4-dVIL3UPEV3@2>A<2R-Hl)XQ2gw^y{Bo&d[0kE2vjG9A;O^a_f_in@95A+q(qVT1j)Q]xT""-hY&<)<A/pEA=taC8b\$pl.ft4jT`ZN<yj{.X_\$sDQRf/Za\@ |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.698743105 CEST | 2583               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill-fetch.min.js?ver=3.0.0 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Jun 4, 2021<br>21:35:06.883961916 CEST | 2596               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "1ee4-5c007b46a37df-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2756<br>Keep-Alive: timeout=5, max=91<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ad 59 7b 73 db b8 11 ff 2a 34 db ea c8 86 a2 e5 e4 e6 9a 4a c7 d1 38 8e 73 49 eb c4 19 3f 7a 37 a3 e8 5c 5a 5c 59 4c 28 42 05 21 29 aa c5 7e f6 ee e2 41 82 12 95 c7 b4 7f d8 22 c0 c5 62 b1 d8 fd ed 83 47 d3 65 3e 11 29 cb 3d 11 80 ff e8 b2 fb 8f 30 11 6e 14 89 cd 02 d8 d4 81 cf 0b c6 45 d1 e9 b8 cb 3c 81 69 9a 43 e2 1e 99 97 73 96 2c 33 18 82 a7 a9 fc be 6b d8 d5 1c d4 aa 4e 47 fd 86 f1 3c 19 aa 47 6f e4 ea 75 ee 18 f7 ee 83 27 c2 5f 5f 9f de fc fa cb 2b 10 93 59 f4 58 fa a5 27 66 69 11 54 32 c6 28 e1 b2 00 a7 10 3c 45 29 07 ab 98 3b 10 f0 80 45 ee ed d5 c5 35 c4 7c 32 7b 1f f3 78 5e b8 69 ee 14 90 4d 83 3c 72 af 37 f3 7b 96 99 19 3c 4a 2a 80 c7 82 71 9a 52 2f 83 59 e4 be 4a 33 b8 82 38 01 6e 91 be c8 d8 7d 3d ac 04 f1 1f 05 df 3c 72 10 4b 9e 3b 39 ac 1d a2 0b 8e 7a e5 24 46 d1 3d e1 eb 77 47 27 65 e9 f9 41 8a dc 19 9f bf 8c 45 5c 09 56 44 ee 29 e7 f1 e6 c5 72 3a ad b7 1c 98 2d 9c 25 71 49 a7 9e 4b 87 cd 1f 6a ad 8b 4e c7 13 d1 b5 9c 45 1a 3f 38 1e fd 1e 77 ff dd eb fe f5 43 f7 0f 7f fc 53 e7 87 3f 3f 09 7f bf fb e7 f6 3f e3 e3 34 14 50 08 22 12 33 ce d6 52 d2 1b e4 72 ce 39 e3 9e fb 26 5f c5 59 9a 38 93 19 ea 6c 82 4a 71 50 8a 99 54 81 33 4d 21 4b 9c 3c 9e 83 eb 0f f4 41 45 28 d8 05 5b 03 3f 8b 0b f0 fc b2 92 75 5a 9f d8 11 d1 be c4 c3 4a da be a8 57 09 0f 2d 8e ae 50 44 8f 39 7c 16 7d 4b bd 6a 1a c2 62 96 4e 85 67 24 78 4c 58 0e fd 15 43 99 7b 11 5a 58 80 f2 2f 01 79 96 a5 91 31 27 ed 8c d4 ad 86 e6 a2 c7 91 c5 da c8 59 fa 81 25 4c 42 c2 90 b5 85 f3 78 81 b6 17 00 2a a3 10 71 3e 91 46 3c 84 70 ca f8 79 8c 97 db f4 18 b9 24 5e 2c 20 47 0e 81 f0 cb 80 66 fc be bc db 30 2d e4 2f f2 6e 65 d0 5c 2e 46 bd 71 20 46 27 e3 8a 09 ba cd a5 74 c8 f0 01 c4 e5 3a 7f cf d9 02 b8 d8 bc c3 6b 29 90 e9 d7 59 06 30 12 15 bf fa b4 13 6d 5c 22 bc 67 c9 e6 b6 80 c4 d7 6a c1 2d e6 69 01 21 07 da d7 db b1 98 d3 8c a3 79 6c 1c fa ef fa fe a0 5e 1f a1 f1 57 ec 17 1e f7 6d ef d0 4c 77 54 c7 43 96 67 2c 4e ec cb 11 1e c7 ad 8b 65 46 9a 24 02 a0 8d 6d 0a 40 0a 39 e9 97 a5 75 a2 0d 9d 48 e2 41 44 3b d6 ce 1c f0 68 81 aa 32 f6 41 27 8b 93 d3 c2 f2 3d 5c 19 f0 9a 53 56 e9 a6 c8 d2 09 f8 95 f1 cb a1 d7 f3 07 f5 36 b7 69 2e 9e ab 2b 46 55 6c 04 5c 40 fe 20 66 d6 6e 05 28 25 da 94 e8 b3 10 de cb bd eb 6d ef 2d d3 a4 1b ac 15 7b 22 6f 2f bc 4b f3 54 bc c0 d9 c8 be 6d 29 cb c0 53 14 b4 e6 0d 52 45 c2 1f 1a 2f 8c 6a 2f ac 89 6e d0 dd 22 d1 9f 75 3a 04 5c e1 82 33 c1 88 0c 0d f6 bd 79 be 24 af b6 d6 10 25 ae 49 3b 1d 83 65 df b6 ce 50 e3 5a d6 e9 ec e0 f4 b7 b1 50 e2 22 fa 68 1c f1 fb 18 91 50 78 cf 03 3c 6a a7 43 ec ff 91 c2 fa 20 37 f0 fd a1 a5 23 eb f2 a3 8c 6e 4e 3e fa c1 8e 16 0d b0 7b a3 d6 a5 63 5f ca e1 59 53 5f 38 ce 76 4b 86 66 9f 6a 47 0a c4 c6 9d 03 47 da f9 6b a6 46 03 e1 24 ce da 96 b8 ae 3a 83 02 f1 82 60 c3 73 27 2c 17 90 8b 2e 71 70 51 0e ef 90 69 98 55 c5 de aa c0 15 c8 fe 78 91 c5 69 3e a0 70 81 24 d1 ed cd ab ee 73 d7 96 81 94 d5 e9 34 c7 21 31 f8 2a ff 96 35 fe f7 99 8b de f7 4b 67 40 50 44 17<br>Data Ascii: Y{ s*4J8sl?z7lZ\YL(BI)~A"bGe>)=0nE<iCs,3kNG<Gou'__+YX"fiT2(<E);E5j2{x"iM<r7(<J*qR/YJ38n)=<rK;9z\$F=wG'eAEVD)r~-%qIKjNE?8wCS???4P"3Rr9&_Y8lJqPT3M!K<AE{([?uJZW-PD9j])KjbnNg\$xLXC{ZX/y1"Y%LBx*q>F<py\$^,Gf0-/ne\,Fq F:t:k)Y0m\ "gj-iiyl" WmLwTCg,NeF\$m@9uHAD;h2A'=\SV6i.+FUI\@ fn(%m-["o/KTm)SRE/j/n"u:\3y\$%l;ePZP"hpX<jC 7#nN>[c _YS_8vKfjGGkF\$:`s',qpQiUxi>p\$S4!l*5Kg@PD |
| Jun 4, 2021<br>21:35:06.896023035 CEST | 2599               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill-node-contains.min.js?ver=3.42.0 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jun 4, 2021<br>21:35:07.082915068 CEST | 2600               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:07 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 20 Sep 2019 20:41:38 GMT<br>ETag: "161-5930218c065a2-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 221<br>Keep-Alive: timeout=5, max=90<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 75 8f 31 6e c3 30 0c 45 af 22 6b 30 a4 c5 48 d6 18 42 a7 00 1d da 4e b9 80 21 31 b5 00 57 74 e9 6f 18 81 a1 bb c7 2a ea b6 43 ba 91 c4 e3 23 7f 75 9d 93 47 e4 64 ec ba 97 0a 06 76 8d 57 53 99 83 8a 49 75 f2 3e 7f 50 c2 64 2d 7a e1 45 25 5a d4 e5 36 d2 59 84 c5 e8 e3 0f a1 e2 a4 84 3e e7 28 14 b4 6d 03 17 0b fa 38 39 e7 60 85 30 4b aa 0e 79 e9 e3 40 06 0e 75 8d 66 ec 64 db 7c e3 40 b6 fd 26 8e 79 5b d3 cf 97 d7 97 f3 40 c5 ab b7 2f 8a a6 ae b5 e7 84 2e a6 a9 8c fe 10 cd 28 0c c6 f6 94 85 dc d6 40 03 81 1e 03 cd ae c8 be 83 ef 4b d6 ac cb fd fd ca 53 69 1e f0 0e a7 c0 fe 2b e8 ef ec 7f bd 43 36 b6 bd 03 02 23 c2 c9 61 01 00 00<br>Data Ascii: u1n0E"k0HBN!1Wto*C#uGdvWSlu>Pd-zE%Z6Y>(m89'0Ky@ufd @&y @./.(@KS!+C6#a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:07.088062048 CEST | 2601               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill-dom-rect.min.js?ver=3.42.0 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Jun 4, 2021<br>21:35:07.273055077 CEST | 2602               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:07 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "363-5c007b46a37df-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 330<br>Keep-Alive: timeout=5, max=89<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 85 d2 c1 6e c2 30 0c 06 e0 57 81 0b 6a 34 0b f5 5c 14 71 d9 15 98 f6 06 49 eb b4 99 48 82 52 87 31 95 bc fb 02 15 2d 1a 74 9c 9c c8 d6 97 df 52 e6 2a d8 92 b4 b3 19 b2 ee 76 9e 55 97 9b 47 0a de ce 8e 4e 57 b3 9c 73 8e eb bc d8 06 23 d1 a7 6e 1c 66 eb 0c 81 6e d3 f3 0c d3 24 9d cf ba dd 8a 6d 9a 5b 2c fa 13 31 16 71 f9 be db 7c 62 49 7c 7c 14 08 2c 68 d6 1d 85 9f 05 f0 e0 a0 04 c5 2f ef 83 48 85 18 98 54 2c 03 99 8a 66 ab 9d fc 4a c0 b2 42 a5 2d 7e 78 77 40 4f 1a db 8c 1a dd 42 77 2a ba 1a a9 18 f8 61 09 15 a1 bd 6f a4 f5 ea 4c c1 25 5f a6 38 42 e0 9e f7 8b b2 08 68 83 41 2f e4 1e 8b 79 1e e1 67 0a 15 cf 50 d1 a3 22 a1 8e 97 93 e8 b7 ae a8 99 82 cd 33 d8 f4 b0 79 91 b6 41 5d 37 34 25 cb 67 b2 ec 65 f9 22 f2 1e d5 a4 1b f8 f0 4d c2 5a bd 6d 04 35 4b a3 6d 96 83 61 45 78 a0 fc 7f 19 fd 68 f9 c1 12 a7 de f2 0f 16 b9 c3 94 e4 46 c9 ad c5 7d 2a c9 0a f7 20 49 47 e4 cc 14 56 8e 58 39 60 d7 58 09 2b ff 62 91 c5 78 fd 94 6c f5 0b 7f 25 96 e1 63 03 00 00<br>Data Ascii: n0Wj4qlHR1-tR*vUGNWs#nfn\$mq[1qlbl],h/HT,fJB--xw@OBw*aoL%_8BhA/ygP"3yA]74%ge"mZm5KmaExh Fj)* IGvX9' X+bxl%9c                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Jun 4, 2021<br>21:35:07.282490015 CEST | 2602               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill-url.min.js?ver=3.6.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Jun 4, 2021<br>21:35:07.475513935 CEST | 2603               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:07 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 02 Apr 2020 04:15:36 GMT<br>ETag: "b7ed-5a2470d845e22-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 13571<br>Keep-Alive: timeout=5, max=88<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 bd 7d db 76 db 38 96 e8 af 58 ac 2a 15 59 82 64 49 be 25 90 61 55 aa 92 74 a7 3b 1d 67 72 99 ee 1e 45 93 a1 28 c8 a2 23 93 2a 92 b2 e3 58 ea b5 ce fc cd 79 3c 0f e7 07 ce 17 cc fc d1 d9 1b 17 5e 41 59 4e 65 7a 25 8b 26 29 10 d8 00 36 f6 1d 1b 8d d9 2a f0 12 3f 0c f6 b8 9d 90 80 44 ce 5d fa c6 b7 43 12 3b 77 fe cc 6e 04 a3 70 2c ef 12 71 77 ed 46 7b 0b 66 e9 a2 16 63 c9 ed 92 87 b3 bd 88 ff b6 f2 23 de 6c aa 9b 01 7e 13 37 9b 0b 27 e2 c9 2a 0a f6 16 50 69 a3 eb e0 7b 57 bf 73 d5 3b ac d5 63 01 bf d9 7b 16 45 61 64 5b bf ba 41 10 26 7b 33 3f 98 ee 5d 85 d3 d5 82 ef fd 68 b5 c2 96 f5 a3 e5 0c 92 79 14 de ec 79 1d 2f 9c 72 66 fd e5 fc e9 fb 97 cf 3e be 3a 7f f7 f1 f9 f9 fb 57 4f 2d e2 6d b0 be 15 43 d8 d9 1d ff bc 0c a3 24 a6 77 9b cd 00 fb 30 ea 8e 3b 9e bb 58 d8 ab 8e fa 89 d8 ba 3b 36 77 ee 14 68 be 2d 0a f7 c6 23 3e 5e af b9 b3 71 c8 8a 64 9f 70 22 07 6d a3 8a 63 5b fa c7 cd 0c ba 80 20 b8 bb 0c 14 09 59 77 10 9e 46 9d 05 0f 2e 92 f9 20 6c b5 1c df 8e 70 b4 07 1a 96 8d 7d d7 a3 a3 0c 4a 6c dc b9 4b 74 83 2c 0f 3f 8c 6f d6 6a 43 b7 ca 1d 39 6a ef e0 51 8e f1 db 24 f2 83 0b f8 a2 65 ed f9 f1 1e 0e b7 bb 97 7e 98 b6 cd 37 1b 72 b7 19 93 7e b5 7d ec 62 c4 b8 6d 75 3a fb 7e 90 f0 28 70 17 f1 be 1f b7 c3 c9 25 f7 12 9c a9 3a 08 1b 11 dc 34 9b c1 6a b1 68 30 56 05 0e 11 e0 c7 64 2f e6 c9 9e d5 ca 43 ea c6 00 e5 32 0a 93 10 3b 56 02 b3 0e 10 7a 70 02 3d 38 d8 b5 07 37 7c b1 68 7f 0a c2 9b a0 1d df 5e 4d c2 85 e5 10 bf 52 4a dd 6d f6 22 ee 26 00 08 71 eb 4a 4c 39 a0 31 6f 03 d0 4b 1e 25 b7 50 34 64 d0 c3 55 10 7b e1 d2 9d 2c 78 0c af 62 f6 24 8a dc db 4e da b5 01 8e 0d 63 31 e0 41 b3 e9 76 66 76 4c 42 72 e7 85 c1 cc bf 58 45 f8 19 6d 74 c9 b5 bb 58 71 ea db 58 18 51 d4 3c e0 58 09 a0 31 6b 74 ab a3 54 ec 06 3d 3c 22 3b 75 82 1e 9e 90 fb 46 8d 9e e0 b0 1f ee 86 b8 f2 17 44 0d 9b ef f9 41 9c b8 81 87 88 9b 38 55 e4 78 11 78 61 14 01 58 80 1c 76 30 0c 00 2f 2c 6a 59 80 1f 7e 70 1d 7a ae 19 83 8f be 3d 06 ef b4 a8 82 bd b4 b6 dd 91 f5 b8 0a ac b5 8a 79 5e 0c 0d 40 a1 81 19 72 fd 49 7b 02 84 b3 0d c8 92 f0 cf 89 11 7b 93 30 ed a3 01 73 91 3e b6 6f fc 64 de 8e dd 19 6f fb f0 5e 0c 6a db 5b 84 31 74 50 e0 b0 61 d8 5c c4 61 55 3c 8c da 57 3c 99 87 53 81 dd 86 f6 25 bd 83 5f 17 d5 f6 05 36 e6 97 8c 57 29 73 c1 93 6a 4b 35 f3 85 a3 85 f4 7a 45 66 64 49 e6 64 c2 7c 78 4d a6 26 fa 9c cc fd 78 88 17 2a 56 24 b9 65 6e 74 b1 ba e2 41 12 2b 12 4d 2e d8 ed 59 6f 98 be 06 26 41 af 43 7f ba 07 eb 91 c9 1b 20 6a 17 e4 8a 79 f6 c4 21 37 40 df 01 61 ae 9b 4d fb 02 16 fe 05 b9 3d eb e7 3e ee a7 1f f7 1d 87 c8 55 7f b5 5e 4f 99 a4 08 cd 66 68 5f 39 0e b2 94 40 70 c8 a9 9d b0 d8 9e 28 58 1c e8 f2 d9 cd e0 06 98 c6 9c 5d 0f 2f ec c9 e8 66 4c 6e 1c 2a fe 2e ec 80 dc 90 b9 33 e0 0b c0 1d ac 63 c9 ec 19 bb 92 0c 70 e2 38 9d 00 10 84 a8 8a 07 0d 7b c5 96 f2 b7 19 fc 36 0d 03 9e d6 ec da 33 72 41 46 ab 8e 20 39 04 2a 07 c6 4d f5 63 da 90 66 87 0a 3c 76 43 82 2a b2 df 8b 5e f4 11 d9 8e 10 b4 77 4c 76 41 7d da 3f 20<br>Data Ascii: jv8X*Ydl%aUt;grE(##*Xy<^AYNez%&)*6*?D]C;wnp,qwF{fc#l-7*Pi{Ws;C[Ead[A&{3?}hyf/rf:WO-mC\$w0;X;6wh-#>^qdp"mc[ YwF. Ip]JlKt,?oJC9jQ\$e~7r~}bmu:~(p%:4jh0Vd/C2;Vzp=87[h^MRJ"&qJL91oK"%P4dU{,xb\$Nc1AvivLBrXEmtX qXQ<X1k1T=<";uFDA8UxxaXv0/.jY~pz=^@rlf{{0s<odo*}[1tPalaU<W<S%-6W)sjK5EfddlxM&x^V\$entA+m.Yo&AC jyl7@aM=>U^Ofh_9@p(X)/fLn*.3cp8{63rAF 9*Mcf<vcC*^wLvA)? |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:07.501946926 CEST | 2617               | OUT       | GET /wp-includes/js/dist/vendor/wp-polyfill-formdata.min.js?ver=3.0.12 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Jun 4, 2021<br>21:35:07.688786983 CEST | 2619               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:07 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 20 Sep 2019 20:41:38 GMT<br>ETag: "1bfd-5930218c07542-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2754<br>Keep-Alive: timeout=5, max=87<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 00 03 95 59 59 73 9b c8 16 7e d7 af 40 3c 28 50 6a 33 76 a6 66 1e 60 fa aa 9c d5 b9 37 ce 3e 49 3c 1a ca d5 40 23 11 23 90 01 59 51 64 fe fb 3d a7 17 68 2d 9e ca e4 c1 c0 e9 ee d3 67 f9 ce a6 04 4e ba 2a e2 26 2b 0b c7 dd de b1 ca ba 09 34 c1 ca 1d 26 69 11 3d 0d 2a de ac aa c2 32 76 2b 4a f4 07 f3 72 5e cc 9a f9 64 9b 94 05 f7 87 67 e4 8e e5 2b ee b3 69 34 1e 87 ad af c8 a7 6d db 22 b7 05 b5 35 17 9b d2 66 b3 e4 65 6a bd 8d be f1 b8 f1 12 9e 66 05 7f 57 95 4b 5e 35 19 af 27 c7 e8 1b bf 93 82 91 88 24 ee 96 0d e9 79 55 b1 8d b7 ac ca a6 44 96 a3 11 d0 d4 61 83 e8 80 4c 21 4d 3c 21 a0 db 92 82 da ab 42 32 4f ec a1 16 66 9d 15 49 b9 1e 8d e4 93 82 90 f3 ac 9e e0 1f ff d8 f6 59 5e 46 2c 1f 8d 8a 55 9e 0f a9 fc 9a c8 87 8f 87 7a 8b 2e c1 6c 4b 6a d8 b0 0d 0a ef e3 66 11 95 f9 fd bd a3 5f 69 e5 0a 43 55 74 cf 37 ec 88 1f 22 ed 08 fb 5b 1d 97 8b e5 75 2d 78 5c db 63 27 ba bf b7 6d 77 cc c6 e3 b6 75 dc 60 d0 89 b1 42 31 80 22 79 ea 6b bd ac e1 15 6b ca 2a 60 20 cc 11 7a 47 71 6c 4d b2 5d 37 e8 bd d9 59 64 cf 19 53 16 8e 46 0b 67 8f 4a 18 d9 c6 65 91 66 b3 55 c5 a2 1c 11 42 d6 55 d6 e8 77 09 a2 43 c0 dd 39 b9 83 66 75 dd b6 75 83 d5 8e 39 db 4e c7 3b 04 2f 28 1a 30 ba 2d f8 f7 c6 67 6d c0 a6 07 3a 85 f4 f0 02 64 de 6a 43 b3 9e e5 f7 3e 1e 8e c1 40 72 1e 8d f6 6e 00 24 4e f7 2f d5 cc a3 49 e4 c5 2c c7 40 f3 a5 94 f8 2a c3 64 13 0c b2 d4 79 38 54 6a de bc d3 a6 7c 9b ba 1b 7a 94 1e f0 bc e6 42 e8 1f 01 f3 c5 cb 39 dd 96 18 8d e4 09 05 fc 35 d5 66 fb c4 bb be 16 6e b9 be a6 e7 c1 0f fa c4 2b 83 a8 e2 ec 06 b4 8f 59 13 cf 51 f1 f6 07 1d 9e b5 1b fa 63 62 46 1f c4 9e 71 38 0a 40 64 83 30 a4 34 72 9b 79 55 ae ad 82 af ad 4f 20 d2 f3 aa 2a 2b 87 8d 6d 2b ab ad a2 6c 2c d0 9a 17 75 06 4e b7 dd de e8 3e 06 93 b0 c3 53 ba e9 03 e8 19 78 09 dd e3 cd 40 98 40 bc c5 14 b7 ca f7 05 bd 2b b3 c4 3a 95 5f 11 55 5b 72 11 c0 5e 4d d5 42 2a 8e f4 8e 7d 8e fa 09 c9 67 47 a5 b5 5f f2 42 7a 0e 85 66 39 98 26 d9 58 d5 aa 28 b2 62 06 52 33 14 e7 b4 7d d6 63 db 9b f7 b8 62 4a e4 e5 05 08 0e cc 4d d9 e1 a6 94 6e 57 3e 23 77 e8 20 ad 85 14 fe fe 5e ea d2 06 06 8b a9 ad 82 3f 3c ca 4a af 22 f8 4d 66 c0 a4 53 fe 45 97 44 61 35 51 1e d8 ca e0 8b 8c 80 7a d9 31 5e 53 26 b9 7d a3 d3 30 48 c1 40 22 28 ac 0c 1c e7 ca 05 6f b9 aa e7 90 9b d4 3e af e2 77 bc aa b9 e3 f6 fc 2e 3a 7e 90 6a c0 dc cf e4 de 73 b0 d2 c5 83 86 7c ee c8 13 2e 02 4d be 7a b1 ab 50 f3 4a 50 88 26 7b 18 50 90 64 d4 f7 5c 09 03 6f c0 49 23 ed bf 32 95 b4 46 76 fc 9f c4 35 80 02 ef 41 d5 12 ca 90 21 de 99 f4 97 31 a2 cd 0b 8a 27 93 a4 f7 85 6f 8a bc 63 50 46 ba 5a 08 46 07 ae fd 21 84 91 f1 89 c6 eb 64 84 9c 70 f1 20 6e fe 8d 4d a6 b6 c0 b7 1d 1e b3 4b f6 cf 76 79 25 81 42 62 70 1b 24 0d 34 0c a7 3a 7f 21 73 00 11 8a 30 74 38 40 a1 6e 58 11 f7 e9 ca 3d 1e 58 af 54 46 b4 2a 5e af f2 c6 b2 c7 bc cf 0c ac b0 4a 71 d8 96 7c b9 87 c6 d3 9a e1 95 98 05 08 17 3e 4a 29 97 55 5d 65 ac 59 97 ce 85 6c 22 e2 d1 e0 a0 e5 cc 25 c2 a4 fd 42 10 77 6a 90 74 d7 ee 9d fa f8 b5<br>Data Ascii: YYS~@<(Pj3vf 7>I<@##YQd=h-gN*+4&i=*2v+Jr^dg+4m"5fejWK^5\$yUDaLiM<I82OfIY^F,Uz.IKjf_iCUt7"[u-xlc'mwu' B1"ykK* zGqIM]7YdSFgJefUBUwC9fuu9N;/(0-gm:djC>@m\$N/I, @*dy8Tj]zB95fn+YQcBfQ8@d04ryUO *+m+I,uN>Sx@ @+:_U[r^MB*)gG_Bzf9&X(bR3)c bJMnW>#w ^?<J"MFSEda5Qz1^S& }0H@"(o>w.:~js .MzPJP&{PdIol#2Fv5 A!1'ocPFZFIdp nMKvy%Bbp\$4:ls0t8@nX=XTF^JqJ>J)U]eYI"%Bwj t |
| Jun 4, 2021<br>21:35:10.149117947 CEST | 3005               | OUT       | GET /wp-content/uploads/2017/09/Favicon-3-300x300.png HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:10.339991093 CEST | 3103               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:10 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Fri, 08 Sep 2017 21:32:24 GMT<br>ETag: "7859-558b4500dea00"<br>Accept-Ranges: bytes<br>Content-Length: 30809<br>Keep-Alive: timeout=5, max=86<br>Connection: Keep-Alive<br>Content-Type: image/png<br>Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 2c 00 00 01 2c 08 06 00 00 00 79 7d 8e 75 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 00 09 70 48 59 73 00 00 00 48 00 00 00 48 00 46 c9 6b 3e 00 00 77 4e 49 44 41 54 78 da ed bd 77 b8 24 67 79 e6 fd ab aa ce f9 e4 9c 27 07 4d 54 9a 19 e5 2c 81 00 59 04 e3 5d b3 2c 6b ef 82 61 bf 35 9f 71 c2 c6 18 af 13 b6 d7 5e 6c 60 bf 35 ac d7 18 63 72 10 08 e5 3c 1a c5 d1 04 4d 0e 27 e7 d4 39 56 fa fe 78 7b 06 01 92 50 f7 9c f3 76 9f 99 be af ab ae 73 46 73 8d ba ba aa de bb 9e e7 79 9f e7 be 15 6a a8 e1 e7 e1 00 ea 80 08 10 04 02 40 a8 f8 7b b0 f8 77 41 c0 03 b8 01 67 f1 a7 eb 35 07 40 e1 35 47 1e d0 8b 3f 73 40 12 88 16 7f 26 81 04 90 2a fe 1e 2b fe 9d 51 bb 15 35 bc 16 4a ed 12 5c 92 f7 dc 07 84 8b 44 14 04 5a 81 ee e2 d1 51 3c c2 80 b7 78 b8 8b e4 e4 01 dc 0e 0d cd e9 00 55 03 4d 01 45 05 4d 05 55 01 55 15 7f 06 b0 2d b0 2c b0 6c 30 2d f1 67 d3 06 cb 04 dd 00 c3 c4 7c 0d 81 e5 8a bf 67 8b 47 1c 98 28 1e a3 c5 63 ba 48 68 a9 e2 df 67 00 bb 76 4b 6b 84 55 c3 ca 87 5a 8c 7c 9c c5 e8 a8 17 58 55 fc d9 0f f4 01 9d 40 93 aa e2 72 68 a8 9a 86 aa a9 28 2e 27 6a 43 04 1a 22 10 0e 42 28 20 7e 86 03 3f f9 dd e7 05 b7 13 1c 0e 70 6a e0 74 82 43 2b fe d9 21 4e 40 37 c0 10 c4 84 ae 83 6e 8a 3f e7 75 c8 64 21 9e 84 44 0a e2 a9 d7 fc 9e 84 85 98 38 0a 3a 96 69 61 9b 26 96 61 62 59 16 05 60 0e 18 07 86 80 41 60 18 38 53 fc 99 28 46 71 3a 60 d5 1e 81 1a 61 d5 50 fd a9 5c 53 31 42 5a 0d 6c 06 b6 00 3d c5 88 29 a8 28 f8 03 3e 1c 4d f5 82 90 ea c3 d0 d2 00 5d 6d d0 dd 06 ed cd d0 d1 02 41 3f b8 5d e0 72 0a 02 72 3a 7f f2 bb aa 2e cd c9 5a 96 20 b5 82 5e 24 b4 e2 ef f9 02 24 d3 30 31 03 93 b3 30 3a 05 63 53 30 b3 00 8b 71 41 66 73 8b 90 ca 60 d8 36 e9 62 d4 15 07 46 80 43 c0 ab c0 e9 62 74 36 57 4b 2d 6b 84 55 43 75 44 50 01 a0 01 58 03 5c 06 6c 2f 46 4e 3d 9a 46 b3 df 8b 1a f4 43 5d 08 fa bb 60 fd 00 0c 74 41 6f 07 b4 35 43 73 3d d4 85 7f 12 11 55 3b 74 03 a2 71 98 5d 84 a9 59 18 9e 80 b3 63 70 fc 2c 0c 8e 41 34 21 88 2e 9d c5 32 4d 66 8b 04 36 04 bc 02 1c 06 4e 01 0b c5 94 b2 16 81 d5 08 ab 06 09 f0 15 09 6a 47 f1 d8 55 4c ed bc 9a 8a a7 ad 09 75 4d 2f 6c 58 25 8e 2d 6b a1 bb 1d fc 5e 70 bb 45 1a a7 69 17 c7 85 30 4d 91 5e e6 f3 90 ce c2 e8 24 1c 3a 09 c7 ce 88 e3 d4 30 4c cd 61 99 16 39 44 5d 6c 1c d8 07 ec 2f 1e a7 10 75 b0 1a 6a 84 55 c3 12 c1 53 24 a4 01 e0 86 22 41 f5 28 0a ad 21 3f ae b6 66 58 d7 07 db 36 c0 15 97 89 b4 ae b9 41 44 4e 9a 7a 69 5e 30 d3 2a 46 62 0b 22 9d 7c f1 30 1c 38 06 27 86 44 64 96 48 53 b0 6d a6 8b 11 d8 3 e e0 09 e0 6c 91 d0 72 b5 47 ae 46 58 35 94 96 ea 79 10 3b 77 bb 8a 24 b5 5b 55 e8 f3 b8 71 86 83 28 1b 06 60 cf 0e d8 ba 1e b6 6f 80 ce 56 50 14 71 d4 f0 f3 b0 6d 71 8c 4f c3 2b c7 e0 e0 71 d8 bb 1f 8e 9d 85 78 12 3b 97 47 b7 6c 86 80 67 8 b e4 b5 0f b1 23 99 ab a5 8e 35 c2 aa e1 8d 89 aa 13 51 87 ba 06 b8 19 e8 74 3a 88 0c 74 a3 ae ef 87 6b 76 c2 ae 6d a2 40 de 10 11 45 f1 1a 4a 47 be 20 0a f7 63 53 b0 ef 00<br>Data Ascii: PNGIHDR.,y}ugAMAAsRGB cHRMz&u0':pQ<bKGDpHYsHHFk>wNIDATxw\$gy/MT,Y[,ka5q^'i'5cr<M'9Vx{[PvsFs yj@{wAg5@5G?s@&*+Q5J\DZQ<xUMEMUU-,l0-g]gG(cHhgvKkUZ[XU@rh(,jC'B( ~?pjIC+!N@7n?ud!D8:ia&ab Y`A`8S(Fq:`aP\SI BZl=)(>M]mA?}rr.:Z ^\$S010:cS0qAfs`6bFCbt6WK-kUCuDPXl\ FN=FC]`tAo5Cs=U; tq]Ycp,A4!2Mf 6NjGULuM/X%-k^pEiOM^\$;0La9Dj]/ujUS\$*A(!?fX6ADNzi^0*Fb"]08'DdHSm>lrGFX5y;w\$[Uq( o'vPqmqO+qx;Glg#5Qt:t kvm@EJG cS |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 5          | 192.168.2.4 | 49739       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.391630888 CEST | 1133               | OUT       | GET /wp-content/themes/enfold/css/grid.css?ver=2 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.578500986 CEST | 1155               | IN        | <p>HTTP/1.1 200 OK</p> <p>Date: Fri, 04 Jun 2021 19:35:04 GMT</p> <p>Server: Apache/2.4.18 (Ubuntu)</p> <p>Last-Modified: Thu, 26 Oct 2017 18:46:19 GMT</p> <p>ETag: "2368-55c77967a14c0-gzip"</p> <p>Accept-Ranges: bytes</p> <p>Vary: Accept-Encoding</p> <p>Content-Encoding: gzip</p> <p>Content-Length: 2054</p> <p>Keep-Alive: timeout=5, max=100</p> <p>Connection: Keep-Alive</p> <p>Content-Type: text/css</p> <p>Data Raw: 1f 8b 08 00 00 00 00 00 03 e5 59 dd 6f 1b 37 0c 7f 8e ff 0a 2e 45 d0 8f d9 97 8b ed d8 8e bd 15 c3 3a a0 2f db 30 60 eb c3 80 01 86 ec 93 73 42 e5 93 77 92 f3 51 23 ff fb 28 e9 3e 74 a7 3b c7 71 d3 75 c0 fc d0 da 94 48 91 fc 91 14 a9 74 ce df c0 1f 64 c1 29 88 15 bc 13 89 a2 89 92 9d ef 9f fc e9 00 7e 5e fc 48 24 85 ab 51 08 ef 53 16 59 92 11 ae e0 d5 6f 22 55 29 61 ea b5 25 ff 22 16 0c 0f 6d 23 ff 4c 92 48 2e c9 86 66 f4 77 9c 92 94 25 d7 f0 e6 bc 83 1a d7 0e 7a ba ba 5a 4e ac d6 1c 76 b0 66 49 ef 96 45 2a 9e c2 d5 45 b8 b9 9b c1 83 59 0a 52 2a 37 22 91 ec 86 56 77 65 7b 82 85 b8 a3 d1 0b 25 36 7a 99 a4 d7 2c c1 35 20 5b 25 66 20 6e 68 ba e2 e2 76 0a 37 4c 32 f4 c0 0c 50 ed 8d 90 4c 31 91 4c 53 ca 89 42 c1 33 f8 d4 63 49 44 ef a6 30 98 a1 4e 28 b6 13 2c 11 05 c2 12 9a c2 0e 8d 2f 78 a0 60 42 6a a6 ca 45 18 9e e9 9f b5 e3 35 1b 89 22 f4 97 d1 16 2e b5 ca 48 5c 6a 2f 4e 61 21 54 3c eb e0 51 78 18 4b f0 a0 5e 71 e4 ae e9 3c 88 29 bb 8e d5 d4 9c 96 1d 6d bf a3 8c f3 37 89 c8 ad 80 95 48 a1 90 35 bf 4d c9 06 90 b2 62 e8 28 58 5c 4b 90 8a a4 0a 22 26 11 59 8b e7 6d 4c 13 40 7d d0 5a ca e9 5a 47 1f 60 40 24 56 09 e8 bd 85 5b ca d2 08 96 71 2a d6 14 16 db 6b 44 2e a8 9d b1 ab db d6 e6 36 c4 a0 70 f8 85 76 38 d2 16 22 8d d0 05 88 63 4f aa 7b 4e a7 20 05 67 d1 ac ba 94 3b 5c 3b 52 83 b4 4d 98 ea 82 f9 4f 9a f3 11 6d a2 a6 c0 e9 4a 69 56 b4 71 c3 c9 fd 14 58 c2 51 d1 12 a4 9e de 31 2d 20 69 d6 d3 51 52 33 22 57 06 41 ae 40 90 8a db 3d e1 91 1d 85 ce 50 62 3d 85 7e 2b fe 2f b4 ff e6 84 73 23 ac 16 55 a5 6c c4 4d b1 a5 8e 61 8d a5 cc d1 18 86 c0 a4 dc 52 64 54 71 06 b3 a4 4b 83 1c c2 6d dc 5b 98 d2 d7 22 cb bc 88 59 14 d1 c4 3a d3 64 12 54 75 69 cc a0 84 d2 08 77 9a 30 d3 91 c4 30 10 34 8a da 16 c4 f6 57 2a 15 2e bf 13 7c bb 4e e0 1d 27 52 a2 b2 b8 be 10 d1 bd 05 2b 20 7c 13 93 2e 94 14 59 21 45 ec 06 82 15 4b a5 32 5a 54 30 0b 1d 1f 5a 9c 1f 0e 91 ec bb f6 41 2b 6b 4a 98 64 9f ac 86 6e da 07 e4 c6 64 24 26 43 6f b5 e5 3c 8b 32 d8 39 42 1e da 18 e4 9a 14 1c 39 c3 78 70 a6 3d 54 56 2c 8c 5c 5d e2 e6 86 60 bf c6 94 60 ac cf 25 e2 fc f1 1e 5e d8 9f bb 52 ef bc 34 06 4e ad 58 93 bb 9e b7 c1 20 d1 50 f6 8f 2b d2 1a 55 a1 30 29 7f a2 92 5d 27 06 7a 62 b5 d2 37 d6 78 34 d9 dc 75 e1 fd 56 29 8a a8 0c 42 fd eb 03 1a 8f df fb 58 f9 50 c2 0f 6b 1a 31 02 22 e1 f7 20 97 29 c5 7a 83 97 0b bc 72 2a ba 91 f2 3a 23 97 36 5d 4d ae 34 59 c3 e7 5e 06 59 c9 cf 03 b4 77 57 04 33 5a 5f dd ea dc 11 5d a8 ae 3d 11 80 f1 04 cd 99 79 f2 9b c1 b0 9b eb da d8 63 d6 e6 86 9d 63 a5 dd ce 95 05 c9 cf 3f 3f 4f ab c9 67 85 80 16 a2 7d 2a 38 b7 77 33 1e 99 05 40 d3 0d 7f 5c 04 b4 03 e8 18 3c 1a 5b a4 4e 1a 01 78 26 d3 9e 21 0c ba 9e 88 4c c3 40 aa 94 aa 65 3c d7 09 7f 64 b0 74 0f 63 32 d7 eb 86 a4 34 59 da 7a e7 27 bb be db 2b c9 6d 2f fb 06 07 04 2b 4e ef e6 4b 53 71 6d 3c cd 97 94 f3 5d 71 ff 2d b8 58 7e f4 02 b7 85 b7 60 2b b9 9a 18 4b 38 6b cd 52 51 67 27 97 e6 06 03 d7 0a 87 56 ef 96 8a 7e c9 56 fa b0 4a 4b cd d5 9b 11 ed 3d 9f 08 7b a7 7b 48 9b c2 db f5 69 99 7a c5 d1 39 73 a3 5f f6</p> <p>Data Ascii: Yo7.E:/0`sBwQ#(&gt;t;quHtd)~^H\$QSYo"U)a%#m#LH.fw%zZNVfIE*EYR*7"Vwe[%6z,5 [%f nhv7L2PL1LSB3c ID0N(./x`BjE5".Hlj/Na!T&lt;QxK^q&lt;)m7H5Mb(XlK"&amp;YmL@})ZZG`@\$V[q*kD.6pv8"oO{N g;\;RMOmJiVqXQ1- iQ R3"Wa@=Pb=-+/s#UIMaRdTqKm["Y:dTuiw004W*.jN'R+ [.Y!EK2ZT0ZA+kJdnd\$&amp;Co&lt;29B9xp=TV.])`%^R4NX P+U0)]zb7 x4uV)BXPk1" )zr*:#6jM4Y^YwW3Z_] =ycc??Og)*8w3@ &lt;[Nx&amp;!L@e&lt;dtc24Yz'+m/+NKSqm&lt; q-X-`+K8kRQgV-VJK={{Hiz9 S_</p> |
| Jun 4, 2021<br>21:35:04.703531981 CEST | 1173               | OUT       | <p>GET /wp-content/themes/enfold/css/base.css?ver=2 HTTP/1.1</p> <p>Accept: text/css, */*</p> <p>Referer: http://www.tonhc.org/coronavirus/</p> <p>Accept-Language: en-US</p> <p>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko</p> <p>Accept-Encoding: gzip, deflate</p> <p>Host: www.tonhc.org</p> <p>Connection: Keep-Alive</p> <p>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:04.900279045 CEST | 1196               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:04 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:46:18 GMT<br>ETag: "34e5-55c77966ad280-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 3996<br>Keep-Alive: timeout=5, max=99<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 bd 1b 6b 73 e3 b6 f1 b3 f4 2b 50 bb e9 dd b9 92 ac a7 ed 93 26 9d b9 4b 93 34 33 49 9a 26 69 fb 21 bd f1 40 24 24 21 e6 2b 24 28 5b e1 dc 7f ef ee 02 20 c1 97 ed 78 d2 da 27 0b 04 16 8b c5 be b0 bb e0 5d 5e b0 1f f9 36 10 2c de b1 cf e2 48 89 48 0d 3f fd cd 3f c3 c1 f9 f7 22 13 8a fd 89 bd e7 99 f4 32 e8 a0 06 fb 41 9d 02 81 8f 3f 48 25 aa a7 1f 4f 49 bc 4f 79 72 38 c1 c3 d7 32 ba cb e8 3b 53 f8 fd 55 c8 f7 04 f5 3e 57 2a 8e b0 f5 45 9c 86 34 0f 69 85 ef 6f 64 e6 0d 19 fc 9c ff 3b 4e fd ef 52 91 65 ec 4b 11 89 94 2b e1 eb 16 52 71 71 39 1c 5e 5e b0 06 71 ec f5 57 51 96 c8 14 20 b7 27 f6 f9 84 7d 23 4e 22 cd de bc 60 e3 0c 56 18 1c 54 18 8c d8 36 f6 4f 23 e6 cb e3 88 65 09 8f 46 8c 27 49 20 d4 88 c5 db 9f 85 07 df 72 97 f2 50 8c d8 61 06 9f 39 7c 16 f0 59 c2 67 05 9f ab 11 4b 00 47 10 7b 77 bf e4 b1 02 b0 24 85 3f 1c fe 6d b7 29 fc f5 d2 38 3a 85 d0 f0 7d dc 2d c0 ca fd 88 79 12 41 bd d8 87 bf be 00 2a fc 1d ac 2c 00 4e 86 30 2c 23 00 bc db fa 23 f6 0b 50 05 ff 78 08 ab 64 21 0f 00 34 53 a9 bc 13 f4 1d 47 00 9c e5 5b fc 03 00 0a a8 3d 72 58 15 3a 72 c0 02 2b 80 5e 08 e8 f0 71 09 18 f5 01 65 0c ed 1c 3e 01 8c ef a4 08 fc 0c 77 bb 03 49 41 1f df 22 35 81 d8 8b 08 40 15 8a 0d b0 f0 44 c9 18 08 54 9a 59 6a 17 c7 30 45 1d 04 47 a0 14 9b f0 81 36 4f 95 f4 70 0a 08 cc a7 99 d1 91 67 b8 47 c5 65 90 e1 16 b7 c2 c7 75 f7 39 f2 09 be 4b e4 88 14 69 45 ac f4 bd 4f 63 dc 55 28 22 d8 4c c4 41 40 71 ae 92 1c 56 4e f3 2d 90 91 81 78 68 66 96 87 21 4f 91 30 89 82 82 f6 1d 50 90 fb 32 06 7e 00 1d 71 31 1c 0c a0 77 2f a3 35 9b 6e e0 21 01 71 c8 68 6f 9e b6 a0 8b 22 35 0f 3b b0 a6 71 26 7f 15 6b 36 9b 4e 3f b1 5d 6b 10 ca 01 b4 53 61 c7 51 e0 3e 79 30 e6 81 dc 03 ce 2d cf 44 20 23 b1 61 1f 87 83 26 0f ca bd d7 36 b6 19 f0 f4 a6 cd 36 19 6e c2 97 59 12 f0 d3 5a 6b 1c 2e 37 1c a0 4c 68 10 29 18 1f 84 dc 1f 80 da 99 08 89 1a 2d 6d 33 9e c1 ce d0 94 d7 2c 8a 0d b5 93 2c 11 9e 84 ad 90 fa 12 1c b5 b2 5e 98 f5 56 80 b2 00 ed 8d 6e be 83 9d 10 02 4f 3b a4 35 7b f5 6a e3 3e 96 08 49 af 08 54 b3 7e ec c5 41 c0 93 0c 08 b3 ad 4a 2e 63 30 4b cf 08 0b 26 a3 f7 b8 60 05 1b 87 f1 af e3 6d fc 80 b2 a2 51 03 0d 5d 1b 02 c2 9f f1 bd d8 de 49 f5 24 5c cf 38 f2 17 fd 50 cd 27 be cc db 68 77 33 01 1f 90 80 6b 94 47 e4 5f f5 40 5e 08 f9 11 83 6a ed 82 f8 7e fc b0 66 07 e9 fb 22 da c0 d4 9a 98 b5 36 ce 16 c9 c3 e5 6c 72 b5 12 21 3b fb 9b 08 8e 02 35 f2 5b 91 8b b3 91 d3 c1 4c 4f d9 31 62 ef 52 90 19 fa 94 28 1b 67 a0 d1 3b 2d a3 20 06 0b 38 5f 2e 97 f8 68 f9 a6 c4 83 36 86 31 f7 7f ce 33 65 6d 02 19 33 d4 bc 71 8e 84 97 72 e6 f2 42 1b 9d e2 de 5d 86 9e 79 12 e4 9e f4 f9 98 68 04 52 32 7e 14 85 b6 cc 1d 0f 65 70 5a 9f 7d 4d 10 ec 07 80 c0 0d 9b c7 2f 53 1e f9 c2 e9 c0 71 f6 cf 48 a2 ab 7d 82 0d 6c 33 40 5d df 8b 18 1c 05 af 96 ad af fb a5 1e c6 25 7e 04 6f 93 01 83 ef d9 f7 71 c8 23 e8 a2 1e b4 58 e4 2a 61 e3 b8 8a 83 ab 86 cc d2 e0 50 f5 2f 91 fa 3c e2 35 f1 10 a2 a3 1e e8 21 ab 9a d7 46 d9 c4 74 b0 43 7d b8 9c b9 cf d0 2c b3 60 2f e1 d5 72 11 4c 28 d7 ac ad f8<br>Data Ascii: ks+P&K43l&lt;@\$\$!+\$( [ x]'*6,HH??"2A?H%OIoyr82;SU>W*E4iod;NReK+Rqq9""qWQ 'j#N""VT6O#eF'I r Pa9 YgKG(w\$m)8:}-yA*,N0,##Pxdl4SG[=rX:r+^qe>wIA"5@DTYj0EG6OpgGeu9KiEOcU("LA@qVN-xhfiO0P2~q1w/5n!qho"5;q&k6N?)kSaQ>y0-D #a&6k6nYZk.7Lh)-m3,,^VnO;5[>IT-AJ.c0K&`mQJ]S\$8P'hw3kG_@^j-f'6lr;5[LO1bR(g;-8_h613em3qrBjYhR2-epZ}M/SqH}j3@]%-oq#X*aP/<5!FtC);./rL( |
| Jun 4, 2021<br>21:35:04.905145884 CEST | 1240               | OUT       | GET /wp-content/themes/enfold/css/print.css?ver=1 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifeccl1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.093117952 CEST | 1266               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:46:19 GMT<br>ETag: "11fd-55c77967a14c0-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1623<br>Keep-Alive: timeout=5, max=98<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 95 58 6d 6f db 36 10 fe ee 5f 71 4b 50 a0 0d 2c db 59 96 62 b0 b1 0f 4d d7 37 a0 dd 82 a6 d8 3e 0c 83 41 49 94 4c 84 12 0d 92 7e 4b 90 ff be bb a3 de 6c cb e9 1a 27 b0 78 3c 92 c7 e7 ee 9e 3b 65 7c 31 b8 80 5b ab 4a 0f 77 7e a7 55 99 0f 2e c6 83 c1 68 29 72 19 c5 56 8a 7b 78 84 54 b9 a5 16 bb 29 c4 da 24 f7 33 68 27 a3 58 66 c6 ca 29 08 bd 11 3b 37 83 a7 c1 60 39 04 31 04 e7 ad 29 f3 c7 01 40 62 b4 b1 b4 56 24 f7 f0 93 2a 96 c6 7a 51 fa d9 e0 69 20 68 de cb ad 8f 52 99 18 2b bc 32 e5 14 56 65 2a 2d 9a 22 49 65 24 4b 6f 77 51 62 4a 8f 4f 20 a6 22 f3 d2 42 d8 98 65 53 38 83 7f ce 40 78 6f 5f 2e ac cc 5e c1 d9 bf 70 c6 6b ad d4 c2 cb 74 be 34 ce bb fe b5 bc cc 2b af e5 2b 5a 32 18 8c 2f e0 ab 8c 7e 37 f0 16 55 04 5a 61 dd e0 b7 67 7e 10 ae 51 52 ab f2 de 1b 95 fa c5 14 2e 27 93 17 b4 25 9c 7b b3 e4 09 b3 96 36 d3 66 13 6d a7 b0 50 69 2a 4b b6 32 36 5b 99 36 4a 07 ab 9f db 1b a0 10 36 57 08 d9 04 c4 ca 1b d6 5f 95 ca bb 61 f8 e6 25 8d ce c1 76 23 53 4a d6 1a f6 4a dd be d8 6f 4c af 18 11 ef d5 cf cc ca f6 ca d5 ba 57 df a9 6d af 58 ae 65 d9 37 21 55 be f0 7d 13 a5 3a 71 81 13 fb e8 53 27 f8 8d d4 ad ad ec 9f 51 a6 e5 76 8e 01 bd 2a ca 43 6c eb 41 14 1b ef 4d 31 85 9f 27 cb ed ec d8 a1 b4 51 70 39 de ce 5b e9 93 c5 3c 5b 69 dd e7 7c 8c c5 3f b3 cc 49 0c 5e 0c b3 60 82 61 41 14 ef 22 f4 d4 f0 48 88 7e ea 11 92 97 8e c5 e4 a3 1e 29 7a e8 58 8a fe e9 11 12 76 c7 62 f6 cd b1 98 3c d3 63 5b ef 0e ec 15 86 64 29 d2 14 69 29 d2 32 f3 55 10 23 2e 77 32 21 b2 80 db 30 4b 49 28 d6 4a a0 45 2c 8f 34 fa 42 c2 a8 4a f3 21 f4 ce 3a 95 ca 58 d8 bd 63 d0 10 74 1d 27 57 2d 6a 1c fa a2 3a fc 03 22 04 ce 14 12 aa 50 b8 5b 2d 89 d5 1a 1f 75 c2 04 0f 9e a3 a3 e6 0b a1 b3 ae 8b 7f f9 b5 89 86 93 fa 98 2c d6 f9 3d f3 2c 41 db 31 05 3e 4a 81 6c f9 3d 86 42 cd f7 8a 42 ae 14 6b c2 2a a3 c1 7c c1 6b e1 3c 7c 23 48 0b 5f e8 4a 3a a7 30 ed 8e 9d 57 c9 fd ae 56 0e 46 19 a7 02 65 33 d1 22 2a 04 1b 21 18 b8 66 ff 94 02 f3 ea 18 6a 4e 12 c4 a1 3a 85 94 48 27 36 16 87 0d f4 93 0e 37 17 48 a3 df a5 64 f2 92 c4 34 16 1a 3e 79 59 38 14 e1 d5 31 d0 32 63 b0 06 e0 83 4b ac d1 9a 8c 88 b0 d6 dc 63 ee ab 82 ea 1a 91 34 16 bb 2a 26 83 d5 75 a4 a0 30 31 45 81 11 85 55 af 18 52 7c f1 68 de a1 8d 42 95 8a 2e 83 37 3c ad 40 35 af 8e 7a 8e 4c aa 50 11 5a 38 78 6c 8a 6d 89 61 30 a3 5b 57 b1 bb 10 a9 d9 40 00 67 5b 0d a7 a0 4a 4c 19 e4 7f c4 91 ff 6c 1e 8b 97 93 21 54 bf 5c d4 46 b9 55 69 c4 85 14 46 aa 44 2b aa 41 4b 61 75 60 55 9c d5 3d a1 de f9 f4 09 3f aa 5f 95 21 b4 e1 b1 72 34 79 b8 ae 84 d0 2d 79 2d c1 3e 75 dc 0f ef 89 30 ff a6 4c 02 a7 d1 37 6e 61 36 ae 21 01 84 0f ab 36 c9 d1 63 41 44 0c cb 99 17 05 39 dd 7c 1f 69 0e 30 62 96 05 66 72 62 52 09 6f b5 14 e5 6a f9 3f 42 ed 1b ba 13 6e a8 39 c2 f1 f8 e2 a3 b1 ea 81 ee a0 e1 eb 4a 4b cb c2 bb a5 4c 14 4a 3e 86 d8 60 d9 27 bc 29 dc 98 6d 3b f8 ac 9c af ef 31 f7 56 94 8e 22 ad 0a 12 95 10 77 a1 06 7a 11 1f e9 69 4e 0f a1 b9 58 8a 44 79 bc cd 25 39 24 2a cc 43 d4 ac 9f 82 4b 84 96 2f 2f d9 59 d1 46 c6 f7 ca 9f 9a 3e 21<br>Data Ascii: Xmo6_qKP,YbM7>AlL~Kl'x<;e1[Jw~U.h)rV{xT)\$3h'Xf);7'91)@bV\$*zQi hR+2Ve*-"le\$KowQbJO "BeS8 @xo_~_pkt4++Z2/~7UZag~QR.'%(6fmPi*K26[6J6W_a%v#SJJJoLWmXe7!U);qS'Qv*CIAM1'Qp9[<[ij]?i^`aA"H-)zXvb<c[d] i)2U#.w2!0KI(JE,4BJ!;Xct'W-j;"P[-u,=.A1>JL=BBk' k< H_J:0WVFe3"*!fjN:H'67Hd4>yY812cKc4*&u01EUR hB.7< @5zLPZ8xlma0[W@g[JL!IT!FUIFD+AKau'U=?_!r4y-y->u0L7na6!6cAD9!i0bfrbRoj?Bn9JKLJ>`)m;1"vziNXDy%9\$*CK/ /YF>!<br> |
| Jun 4, 2021<br>21:35:05.211513996 CEST | 1283               | OUT       | GET /wp-content/plugins/jetpack/css/jetpack.css?ver=8.6.2 HTTP/1.1<br>Accept: text/css, */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.400007963 CEST | 1302               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "124ea-5c3db85de540a-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 13264<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: text/css<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d 6b 93 db 38 92 e0 77 ff 0a 6e f9 1c 76 f5 88 2c 92 7a 96 2a ec 9b 99 de c7 4d c4 cc 4d c4 4d ec 45 dc cd f6 39 28 09 2a 71 4c 89 5a 92 72 55 b5 a2 fe fb 21 01 90 4c 3c 49 aa d4 3d 1b 1b db 6a db 12 09 24 80 44 22 91 2f 24 ee 7e f8 87 77 3f 78 ff 98 7b 87 bc f2 f6 f9 26 dd be 78 d5 2e 2d bd 6d 9a 11 6f 93 16 64 5d 65 2f 81 e7 fd a1 f2 e8 d3 75 7e 58 27 15 39 d0 3f 1b 6f 5b e4 7b 2f 3d 6c d2 ef e9 e6 94 64 50 fd 44 2b fd f8 97 bf b0 da 65 f0 ee 87 bb 77 7f dd 24 55 e2 af 93 22 3f 95 24 f3 c9 73 55 24 3f 9d d7 a7 a2 cc 8b e5 31 4f 0f 15 29 5e 83 bf 1d db 22 4f 45 72 f4 7e 38 67 e9 81 f8 3b 92 3e ee aa 65 7a d8 91 22 ad e4 72 f9 77 52 64 c9 cb 79 95 ac bf 3d d2 67 87 cd f2 7d 18 86 af b4 3f 52 b9 6d b2 21 c9 93 5c d0 df e7 3f fb d0 42 52 f8 8f 45 b2 49 c9 a1 fa b4 ca ab 2a df 8f 8a c7 55 f2 29 1c c1 27 98 d e e2 9f e1 ed ed 03 06 f2 44 56 df d2 aa 05 c0 01 8e 32 b2 ad 3c 01 8c 7d af f2 e3 08 90 f5 49 06 7d 3b aa f2 4f 32 f8 db 87 63 5e a6 55 9a 1f 96 db f4 99 6c 1e 38 98 65 f8 f0 b3 4f 31 4d 9e 97 71 34 99 4f 16 e3 d9 64 fe f0 94 6e aa dd 32 0a c3 0f 0f 02 4f d1 f4 f8 2c 23 e9 40 11 ee af 4e 14 c8 c1 2b 8f c9 61 24 bd 3d 16 e4 7b 4a bf e2 12 18 4d a7 22 fb 14 04 77 7c 62 cb bb ba de 5d ba 4f 1e e9 ef a4 28 f2 a7 32 38 1e 1e 6f 29 fd f8 05 39 92 a4 f2 d6 04 e6 54 fc 83 f0 e5 97 e9 cf 64 19 87 e1 f1 d9 8b e2 99 da d3 7d f9 78 de e6 87 8a ce d7 3e cd 5e 96 37 7f 3e 92 83 f7 97 e4 50 de 8c 4a fa b7 5f 52 12 d8 3e b0 22 65 f5 92 91 e5 21 2f f6 49 f6 b0 49 cb 23 a5 03 4a 24 8c 64 56 59 be fe f6 80 a9 27 ba 3f 3e 3f 1c 93 cd 26 3d 3c 2e a3 08 9a a7 78 12 90 a0 4f d1 84 fe ac 00 53 49 96 3e 1e 96 a2 eb fb a4 78 4c 0f cb 98 16 f6 62 e8 75 e8 c5 b4 20 1a d1 3a cf 28 15 bf df 6e b7 74 a2 8a 0d 29 7c 98 ef 25 05 e7 95 79 96 6e 3c fa 6a 95 84 21 7d fb ec 97 bb 64 93 3f 2d 43 8f f5 80 81 c3 f4 10 dd be fe 76 4f 36 69 e2 e5 87 ec c5 2b d7 05 a1 e3 4f 0e 1b ef 53 4d 68 fb f4 e0 6f e8 8c ad 89 7f a4 d4 91 f9 45 42 49 65 19 01 99 ea 95 72 5b f9 f1 5d 6c 28 0f 85 d9 b2 e8 dd 82 a3 3b e7 eb 11 a1 cf 88 ad 1f 29 fa f1 33 a3 c6 57 9d a3 c8 b4 f5 3f 48 f6 9d 54 e9 3a f1 fe 27 39 11 4c 60 ff 90 ee 8f 79 51 25 07 85 db a4 87 6d 7e 6e 16 67 b2 a2 f3 7b aa 48 bb 3e 11 f9 00 0d b4 60 1e ea d9 e3 f4 b6 cf 73 ca 5f 29 21 96 a7 15 c7 1a 2d 93 d2 8a 49 49 36 ae c6 bd e5 92 7e a5 ec 98 b6 2f f1 bc d9 62 7d 4f 16 0f 2d 2d 1a eb b2 a9 bd 08 c0 71 97 57 b9 32 fe 82 64 74 ae bf 93 07 46 ef f1 f4 83 60 46 d3 f0 83 5c 99 72 fb 03 af 53 7a 36 a8 6d 99 65 30 29 3d 42 31 e1 e7 27 13 0a 76 31 ee 78 e8 85 08 cd 7c 01 52 a6 70 20 e8 a9 18 d4 fd fd 7d c3 27 18 83 40 45 60 5e 04 2f f1 a2 f1 f1 f9 2e 0a e2 29 49 7b bd 88 84 22 a0 a2 bc c2 a7 44 bb 86 59 c5 3d 12 fc 63 ce 96 ba dc d9 86 1b 71 b6 82 5f c1 b6 b6 cd 28 a3 d8 a5 9b 0d 39 a8 84 c5 7f 0b 5e a2 0c 96 bd 62 d8 dc d2 e1 a8 6f 07 d0 a1 75 0f 71 ae dc 33 6b 1f b6 29 8a 50 9f a2 1c f8 ae 3a 1c d7 ce 7f 01 9f d0 57 24 dd 6c 97 61 bb 2e 39 5d 2e 80 71 ff 9c d3 27 d1 43 0e 53 55 bd 2c 83 b8 27 a9 ba bb 65 a7<br>Data Ascii: }k8wnv,z*MMME9(*qLZrU!L<I=\$D"/\$~w?x{&x-.mod]e/u-X'9?o{[/!=dPD+ew\$U"?\$sU\$?1O)^"OE~8g;>e z"*rwRdy=g}?Rm!/?BREI*U)'DV2<}};O2c^U!8eO1Mq4Odn2O,#@N+a\$={JM"w b]O(28o)9Td]x>^7>PJ_R>"e!/I!#J\$dVY"?>? &=<.xOS!>xLbu :{nt})%yn<j!}d?-CvO6i+OSMhoEBler[]!();3W?HT:'9L'yQ%~ng[H>'s_]I-I!6~/b}O--qW2dtF'FrSz6me0)=B1 'v1x Rp }'@E'^/.){'DY=cq_(9*bouq3k)P:W\$a.9].q'CSU,'e |
| Jun 4, 2021<br>21:35:05.587819099 CEST | 1387               | OUT       | GET /wp-content/plugins/jetpack/_inc/build/spin.min.js?ver=1.3 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.790404081 CEST | 1533               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 03 Jun 2021 12:14:54 GMT<br>ETag: "119e-5c3db85dd0be9-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2205<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 7d 57 6b 6f db 38 16 fd de 5f a1 b2 a8 87 b4 68 59 76 76 76 b1 72 38 9d b6 b3<br>8f 02 ed 74 31 ed 3e 80 20 1f 68 89 b2 d9 ca a2 40 52 89 5d c7 fd ed 7b 49 4a b2 9c 0c 06 08 1c 89 a2 ee 8b e7 9c 7b 35<br>9f 46 bf a8 a8 56 36 da a9 42 96 87 c8 6e a5 89 4a 59 89 a8 90 5a e4 b6 3a 24 d1 3b 1b c1 62 ae 76 0d ac 17 51 a9 d5 2e<br>52 76 2b b4 df 68 92 68 3a 7f 36 9f 97 9b 9a 1b 93 6c a4 dd b6 eb 04 76 cf 4d 23 eb e4 8b 79 71 b7 48 ae 9e cd a7 d3 67<br>d1 34 7a ab 9a 83 96 9b ad 8d 70 4e a2 65 ba 58 cc e0 e7 2a fa bb a8 e4 3e fa 87 33 e1 b6 bd 97 b9 a8 0d 38 6b eb 02 fc<br>80 b3 e8 c3 bb cf 51 15 96 9f 39 8f cf cb b6 ce ad 54 35 b6 54 90 23 52 eb 2f 10 2f 62 cc 1e 1a a1 ca 48 ec 1b a5 ad 79 05<br>89 b5 95 48 ba 5b 26 30 c9 50 ff ea 79 77 21 4a 59 8b c9 24 fc 4f f8 ae 78 15 2e b1 20 99 4d 3e 41 2a b5 d0 ee ed 13 76<br>35 a2 83 77 70 dd 1a 11 19 ab 25 b8 5f dd 71 08 97 0a 76 83 ee c5 fa ab b4 88 a2 0f ea 1b fc ee 0c fc 7c 44 b7 54 b2 e3<br>69 d5 bf 1e a9 10 be 7b 4d 52 c5 0a 95 b7 3b 51 db 24 d7 82 5b f1 b7 4a b8 3b 6c 1f 1e 50 21 ef 10 59 95 4a 63 19 c9 3a<br>12 44 dd c8 5b 26 e0 67 a5 85 6d 35 d8 3a 0d 66 35 b6 e4 e8 f6 3a c3 82 2d c0 2b d7 1b 6f da 24 95 a8 37 76 bb 12 d7 72<br>25 e2 98 d8 84 37 8d a8 8b b7 5b 59 15 78 d8 76 23 6e 49 6f d9 9e 9c 9d 9a 1a 86 6b a6 30 32 f6 50 09 44 8f ae 7a 19 b2<br>62 6f e7 b9 31 e8 44 a8 c6 43 0a 1b 61 bb f8 cd 9b c3 67 be f9 95 ef 04 46 5b c1 0b 44 6e d2 5b 5a 13 5a 27 66 2b 04 64<br>07 17 ce e4 27 77 47 ce d5 e1 58 50 45 35 6c f5 15 e2 50 56 d5 f0 5c da 03 82 f5 ef df 1f 22 4d a7 82 b8 1d b7 c9 17 25 6b<br>8c 66 88 d0 8a 25 e9 22 d6 f3 7a 0a cf 69 c9 3e 70 bb 4d 76 7c 8f 17 33 f8 13 64 ae a6 ee cd 59 45 a0 f6 b4 61 36 31 ed<br>da 9d 60 bd c1 29 b5 89 04 d4 ed 3f 96 18 bd ae e5 8e 7b a4 10 92 58 f5 5e dd 0b fd 96 1b 80 01 2d 58 33 99 80 b7 b8 89<br>e1 17 ce 07 f5 c5 92 37 fc f6 e1 01 1b 30 63 84 b6 bf 01 fc 30 fa 19 c5 45 8c be 8a 43 a9 a1 0c 26 42 31 8f d1 31 7d 79 ec<br>f2 c9 50 5c c6 e8 84 e2 2a 46 e3 45 e1 17 71 15 43 46 64 fc 68 11 96 15 79 09 99 3c 7d 07 16 1f db 3e 21 6a 12 38 26 17<br>50 0f 02 42 5d b4 6c a1 28 3f 83 a7 02 4c ca 50 71 5f 7c 57 1f 77 3a 2b 59 e2 3b 25 8b 28 7d ce 58 0d c0 23 7d c6 01 96<br>4c 26 f9 96 eb d7 16 a7 ae 5a ff 06 54 75 d5 8a 65 62 1c 79 31 38 d2 2c 5d e9 6b d1 a3 50 03 02 2f ed 2a 00 b5 be 8d cf<br>e6 47 b8 2e 03 5d 7a 64 77 4c e8 e2 bb 09 81 3f 3c 3c e2 85 3d bf df 3c e2 05 90 e0 29 2f 20 a2 40 48 36 26 c3 aa 7f 4d<br>39 a7 92 84 88 19 48 c8 8d ba 9d 4c b0 fb c7 24 fc 90 d3 53 bf c5 a5 df e3 1e 44 45 95 a5 11 f6 bd 28 2d 3d 0c b7 9f 55<br>73 5a 59 d6 df fe 8b 6b 70 bf 22 22 d9 c7 ec e2 15 91 1c ce 2b f0 56 9f ac f0 54 cd d9 b1 02 f5 32 d9 62 49 43 5a d9 5f e8<br>bd 2c e0 ff 8f 54 f3 42 b6 f0 28 a5 5a 59 50 99 2c a5 b9 d2 a0 6f b0 06 57 95 d2 19 7a 91 a6 29 a2 a1 09 40 02 f0 c0 34 42<br>14 f0 df 6a 2e ab cc 11 ab 87 57 b2 fc 91 96 8d c9 96 29 fd f6 ce 51 27 5b 8a bf d2 bc 02 31 77 9c cf 90 09 f2 89 a8 55 4d<br>86 78 6b 15 82 a8 4a db 5f 37 ca 48 ef 05 69 51 01 df ee 04 1a 49 64 eb 6a<br>Data Ascii: }Wko8_hYvvvr8t1> h@R}{IJ{5FV6BnJYZ:;\$;bvQ.Rv+hh:6lvM#yqHg4zpNeX*>38kQ9T5T#R//bHyH[&0PywIJ<br>Y\$Ox. M>A*v5wp%_qv DTi{MR;Q\$J;IPIYJc:D[&gm5:f5:-+o\$7vr%7[Yxv#nlok02PDzbo1DCagF[Dn[ZZ'+d'wGXPE5IPV\<br>"M%kf%"zi>pMv 3dYEa61")?{X^~X370c0EC&B11}yPl*FEqCFdhy<}>lj8&PBj]A(/LPq_!Wwv:+Y%;{X#}L&ZTueby18,]kP/*<br>G.]zdwL?<<=<=)/ @H6&M9HL\$SDE(=UsZYkp""+VT2blCZ_,TB(ZYP,oWz)@4Bj.W)Q[1wUMxk_j_7HiQldj |
| Jun 4, 2021<br>21:35:05.794202089 CEST | 1535               | OUT       | GET /wp-content/themes/enfold/config-templatebuilder/avia-template-builder/assets/fonts/entypo-fontello.eot?v=3<br>HTTP/1.1<br>Accept: */*<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Origin: http://www.tonhc.org<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:05.980673075 CEST | 1873               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:05 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 26 Oct 2017 18:45:51 GMT<br>ETag: "b9a8-55c7794ced5c0"<br>Accept-Ranges: bytes<br>Content-Length: 47528<br>Keep-Alive: timeout=5, max=95<br>Connection: Keep-Alive<br>Content-Type: application/vnd.ms-fontobject<br>Data Raw: a8 b9 00 00 e4 b8 00 00 01 00 02 00 00 00 00 00 02 00 05 03 00 00 00 00 00 01 00 90 01 00 00 00 00 4c 50<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 1b 72 b3 29 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 1e 00 65 00 6e 00 74 00 79 00 70 00 6f 00 2d 00 66 00 6f 00 6e 00 74 00 65 00 6c 00 6c 00 6f 00 00<br>00 0e 00 52 00 65 00 67 00 75 00 6c 00 61 00 72 00 00 00 16 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 31 00<br>2e 00 30 00 00 00 1e 00 65 00 6e 00 74 00 79 00 70 00 6f 00 2d 00 66 00 6f 00 6e 00 74 00 65 00 6c 00 6c 00 6f 00 00 00<br>00 00 00 01 00 00 00 0a 00 80 00 03 00 20 4f 53 2f 32 3e 51 4a 2f 00 00 01 28 00 00 00 56 63 6d 61 70 d1 3c 19 b7 00 00<br>06 34 00 00 01 4a 67 6c 79 66 c6 b0 e9 87 00 00 09 dc 00 00 9f 48 68 65 61 64 02 b0 dc d4 00 00 00 d0 00 00 00 36 68 6<br>8 65 61 08 9d 05 54 00 00 00 ac 00 00 00 24 68 6d 74 78 e1 66 00 00 00 00 01 80 00 00 04 b4 6c 6f 63 61 47 8a 70 58 00<br>00 07 80 00 00 02 5c 6d 61 78 70 02 45 00 db 00 00 01 08 00 00 00 20 6e 61 6d 65 1c f8 8b 3a 00 00 a9 24 00 00 03 21<br>70 6f 73 74 14 37 5c 5c 00 00 ac 48 00 00 0c 99 00 01 00 00 03 52 ff 6a 00 5a 04 ee 00 00 ff ce 04 ee 00 01 00 00 00 00<br>00 00 00 00 00 00 00 00 00 01 2d 00 01 00 00 00 01 00 00 29 b3 72 1b 5f 0f 3c f5 00 0b 03 e8 00 00 00 00 cf 63 cc 9a<br>00 00 00 00 cf 63 cc 9a ff dc ff 41 04 ee 03 7a 00 00 00 08 00 02 00 00 00 00 00 00 01 00 00 01 2d 00 cf 00 0e 00 00<br>00 00 00 02 00 00 0a 00 0a 00 00 00 ff 00 00 00 00 00 00 00 01 03 4d 01 90 00 05 00 08 02 7a 02 bc 00 00 00 8c 02 7a<br>02 bc 00 00 01 e0 00 31 01 02 00 00 02 00 05 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50<br>66 45 64 00 40 e8 00 e9 2b 03 52 ff 6a 00 5a 03 7a 00 bf 00 00 00 01 00 00 00 00 00 03 e8 00 00 02 46 00 00 02 e4 00<br>00 02 bc 00 00 03 15 00 00 03 86 00 00 03 84 00 00 03 5c 00 00 03 5c 00 00 03 70 00 00 03 70 00 00 03 ac 00 00 03 e8<br>00 00 03 e8 00 00 03 d4 00 00 03 e8 00 00 03 e8 00 00 02 58 00 00 02 bc 00 00 02 9b 00 00 01 d6 00 00 03 48 00 00 03<br>20 00 00 02 44 00 00 03 48 00 00 03 20 00 00 02 44 00 00 03 48 00 00 03 20 00 00 02 44 00 00 03 98 00 00 01 cc 00 00<br>03 98 00 00 03 52 00 00 03 84 00 00 03 20 00 00 03 ab 00 00 02 bc 00 00 02 bc 00 00 03 e8 00 00 03 c0 00 00 01 68 00<br>00 02 26 00 00 03 84 00 00 03 20 00 00 03 20 00 00 03 e8 00 00 03 e8 00 00 03 e8 00 00 03 84 00 00 03 e8 00 00 03 84<br>00 00 02 fa 00 00 03 e8 00 00 03 e8 00 00 03 0c 00 00 02 ba 00 00 03 d4 00 00 03 e8 00 00 03 e8 00 00 03 20 00 00 03<br>e8 00 00 03 20 00 00 03 c2 00 00 03 85 00 00 03 e8 00 00 03 e8 00 00 01 f4 00 00 03 e8 00 00 03 5c 00 00 03 c0 00 00<br>02 a9 00 00 02 f8 00 00 02 bc 00 00 03 e9 00 00 03 e8 00 00 02 bc 00 00 02 bc 00 00 03 20 00 00 03 84 00 00 02 bc 00 0<br>0 03 e9 00 00 03 d5 00 00 03 84 00 00 02 f8 00 00 03 20 00 00 03 48 00 00 03 e8 00 00 03 20 00 00 03 e8 00 00 03 84 00<br>00 03 5b 00 00 03 84 00 00 03 84 00 00 03 84 00 00 02 80 00 00 03 74 00 00 03 8e 00 00 03 80 00 00 03 98 00 00 02 30<br>00 00 02 bc 00 00 02 bc 00 00 03 e8 00 00 03 e8 00 00 03 c0 00 00 03 18 00 00 03 84 00 00 03 20 00 00 03 e8 00 00 03<br>e8 00 00 01 cc 00 00 03 98 00<br>Data Ascii: LPr)entypo-fontelloRegularVersion 1.0entypo-fontello OS/2>QJ/(Vcmap<4JglyfHhead6hheaT\$hm txflocaGpX<br>\maxpE name:\$!post7\HRjZ-)r_<ccAz-Mzz1PfEd@+RjZzF\ppXH DH DH DR h& \ H [t0 |
| Jun 4, 2021<br>21:35:06.169617891 CEST | 2403               | OUT       | GET /wp-includes/js/jquery/ui/effect-size.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecclvdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.359833002 CEST | 2430               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "cb3-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 1224<br>Keep-Alive: timeout=5, max=94<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 95 57 4d 6f e3 36 10 bd ef af 50 74 30 24 2f 23 27 40 4f 0a 04 03 5b b4 68 80 dd 43 b7 29 72 08 72 60 24 4a e2 c2 26 55 6a 14 db b5 fd df 3b fc 92 68 d7 9b cd 22 41 c4 19 0e 1f 67 86 33 8f cc 62 7e f5 21 9a 47 df fe 1c 98 da 45 7f df 47 bf d5 35 2b a1 8f fe e2 ff b2 e8 36 bb bd cd 7e d1 06 2d 40 97 2f 16 df fe d1 76 03 cf 4a b9 46 b5 9e f9 55 76 3b c5 9b 16 3c c8 ef 72 10 15 05 2e 45 44 45 15 49 68 99 8a 4a 29 40 f1 97 01 a4 ea f5 aa af 6c c5 68 cf aa 08 6d 71 1a 6d a2 2f f7 0f d1 8a 97 4c f4 2c fb df 96 99 54 cd c2 cd ba 8d dd 3c ed 78 16 ba b5 e8 d1 f3 6b 66 c2 58 a0 dd e2 c3 55 3d 88 52 fb 93 40 ba 8f bd 10 17 05 ec 3a 26 eb a8 62 35 17 6c 36 b3 df 8c ae ab a5 1d 26 4f b1 45 8e 49 9c 2d 2c 64 fc 4c 20 cd 21 b1 c1 a6 c7 64 04 df a4 7b c5 60 50 22 da 64 d6 b6 77 df 4c bb 54 8c 86 0a 11 f6 af 54 45 92 b4 44 14 9b 04 5a de a7 84 15 4f 71 27 7b 6e 9c 23 31 c8 0e ff be 48 00 b9 c6 c1 8a d5 80 1f 93 69 fc 6e 78 05 2d 7e 5b e6 14 f2 95 a9 7a 25 37 7a d8 d1 92 c3 0e 3d ed 11 f2 fb 96 cf 84 e3 7c 8d 27 a3 0f 1b c5 12 c5 17 a9 f0 40 1e 64 f7 e8 d6 59 c5 2f e3 87 d7 75 b4 aa b8 68 1e 8c 8b 4e b0 16 88 42 47 94 cf e8 f3 29 cc 57 ed c3 19 ca 67 1b 99 93 8c 05 a2 d4 c5 94 c5 9e c1 17 59 b1 44 10 95 ad 71 70 38 4a ee 30 52 52 15 2a 53 ac c7 ba 0a d4 57 45 51 93 35 ce f4 25 5d 69 3d a6 11 77 6c 50 23 31 83 5c 1c 0e 4f f1 9a 57 d5 8a e1 ce 58 54 c0 14 ee 39 14 22 2b fb 3e 99 8e 21 25 5d 51 2d 59 fe 13 27 73 f1 20 76 c5 de e6 3f bf 21 e6 40 f0 2b 07 dc f5 0f af 35 d2 a3 9d 3a de c5 7d 8b 08 05 86 31 9b 89 4c 0b 49 4a e4 08 22 32 3b 40 a5 45 13 99 f9 6a a3 00 55 64 81 e4 e7 1e dd 82 49 48 d2 a3 0e aa 69 30 1b b8 a5 cd f1 6c 36 f9 b0 4c 44 56 2b a9 13 0a f2 70 d8 11 81 5f 14 b4 ee 70 90 69 3e cd 5b 55 12 ac dd e5 32 f5 0b f4 ea 24 6e 79 c5 a6 b9 94 b4 c5 5e 2f cb 7f bb dc e2 b8 e8 16 d2 0d c8 d6 4f 98 28 51 6f be 47 02 d2 2e 02 79 71 09 c8 b3 05 47 7d 6c 5b 5d 1e 6b 8c cf 14 85 1e a3 53 ad c5 df a1 d8 ea 75 bb d9 2c e9 8a 0e 09 45 94 14 92 52 87 60 42 3c a9 ca 07 45 85 2d 0b ac cd 92 78 10 67 eb c2 7e 7b 85 de cb d8 e9 44 d8 f5 5b ef c4 f6 d4 09 fa 0e 27 e8 08 f2 5e 27 a8 75 62 eb 9c 48 b1 1f 90 11 b0 25 2e a4 e9 07 59 e2 a9 1f f5 ef 70 95 ff 74 be f8 59 be 02 4b fa aa e9 a1 d3 10 ae 5b a6 c9 52 31 0a ec 51 d1 ae 63 2a 11 da c6 74 79 d0 a9 58 92 15 c3 76 37 13 de 9b 06 a3 6b 02 77 1a 06 9f f0 ce 5a e9 9b a1 21 d2 87 88 be 74 45 22 c3 5e bb 3e eb bc 74 de 8c 51 66 9a 2f 46 7b d3 80 d7 a7 dd a8 ad ed 71 5c 86 86 13 85 c7 46 ed 45 64 08 65 03 ed 13 e0 e3 7c e3 c0 93 b2 28 fd 99 22 63 52 85 dc 69 59 df 8e 3d e9 a7 53 09 20 ff d3 f3 25 8e e2 ad e0 18 3e c5 bd 89 4d fd 75 5a e4 5c 54 49 3c 7f 32 5d fb 8c c7 c2 68 d9 4e 37 ad bd 3d 61 bc 39 65 01 13 21 32 14 3c 19 72 1c 9f 52 60 ed 35 2e d7 77 d5 6c 76 56 46 40 10 12 6c f5 7a c2 95 f3 b1 56 2d e1 b2 f9 d8 67 21 e3 f2 c9 2e 20 db 7a 34 46 ca d2 25 1e c2 9a 82 9e 40 4d 2b 86 90 a3 4d 00 e8 0d 8f e4 52 47 c2 db 9d 07 21 53 81 ab 01 78 ab f3 60 62 2a f8 3e 53<br>Data Ascii: WMo6Pt0\$#/#/@O[hC]rr`\$J&Uj;h"Ag3b~!GEG5+6~--@/vJFUv;<r.EDEIhJ)@lhmqm/L,T<xkfXU=R@:~b5l6&OEI-,dL !d{P"dwLTTEDZOq{#n#1Hinx--[z%7z=]'@dY"uhNBG)WgYDqp80RR*SWEQ5%]i=wIP#1!OWXT9"+>![%]Q-Y's v?/@+5 :}1LIJ"2;@EjUdlHi0l6LDV+p_pi>[U2\$ny^O(QoG.yqG)]l[kSu,ER`B<E-xg-[D]l"ubH%.YptYK[R1Qc*tyXv7kwZ!tE"^^>tQf/F{qVFEdel("cRiY=S %>MuZ\TI<2]hN7=a9e!2<rR`5.wlvVF@lzV-gl. z4F%@M+MRG!Sx`b">S |
| Jun 4, 2021<br>21:35:06.362693071 CEST | 2431               | OUT       | GET /wp-includes/js/jquery/ui/menu.min.js?ver=1.11.4 HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.551265001 CEST | 2530               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 15 Apr 2021 19:16:47 GMT<br>ETag: "2547-5c007b469ab3b-gzip"<br>Accept-Ranges: bytes<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 2805<br>Keep-Alive: timeout=5, max=93<br>Connection: Keep-Alive<br>Content-Type: application/javascript<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 b5 5a 59 73 db 38 12 7e 9f 5f 41 63 a7 34 64 0c 51 d2 66 9e 28 2b ae ac e3 4c 5c 35 99 78 13 67 e7 c1 76 5c b4 04 49 98 d0 a4 42 40 76 5c b2 fe fb 76 03 04 09 f0 90 9c 3d aa 52 16 89 b3 ef fe ba 99 c1 8b 83 9f bc 17 de 5f ff 5c b3 fc d1 fb 7c e6 bd 67 e9 da 1b 85 a3 51 f8 2b 4e 2c a5 5c 45 83 c1 5f df 70 7e cd c3 69 76 07 c3 38 73 92 ad 1e 73 be 58 4a b3 f9 6d b6 4e 67 b1 e4 59 ea c5 e9 cc cb e4 92 e5 de 34 4b 65 ce 6f d7 32 cb 05 ee fa c8 12 16 0b 36 f3 60 2d 4c c3 1a ef fd d9 85 97 f0 29 4b 05 0b 1b 57 86 59 be 18 14 b3 c5 c5 c5 7c bc e2 a1 4d d6 e0 0e 28 1f c0 82 c1 4f 07 f3 75 3a 45 42 7c 16 6c 88 79 21 93 89 7c 5c b1 6c ee cd d8 9c a7 ac d7 d3 bf 61 7c 37 3b d6 8f fe 25 d1 47 12 4a c2 c1 34 cb 99 7a 78 e0 b3 05 93 ea 71 95 09 ae 0e bb a6 2c 88 98 af 79 0f b6 7e 79 65 1c 6c 72 26 d7 39 48 21 d4 1b 7d 02 14 22 75 84 6e ee 59 2e 60 55 44 b4 88 09 85 8b e3 75 22 4f 13 06 2b 64 44 8e d6 c9 2b 1c 4d e2 c7 e8 e5 70 48 b3 15 9e 2a a2 0d 9f aa 1f b1 be c5 a3 22 38 b3 8f 43 fd 69 9c c7 b2 3f ea 33 b2 a5 5c b2 3b 11 91 57 de 0b 42 71 15 3c af 13 42 0d d1 d1 e6 ee 31 22 09 9b c3 7a 4f 66 2b 42 63 b8 51 2b 11 5f b7 34 cf 12 16 11 4d eb 6d b2 ce a3 74 9d 24 74 9e 4d e1 28 f5 28 40 7f 53 a9 9e b7 f4 66 9a b3 58 b2 a8 e4 3d d8 c8 25 17 61 0c 6f f7 0c 2d 69 a2 de 99 66 8e aa 97 bb 6c 2d d8 3b b0 90 84 cd 26 07 23 6a af 08 d7 29 07 f9 9f cd fc 20 8c 67 b3 93 24 16 02 a5 d7 47 8a 3c f8 d5 02 ad 9e fa 68 5f b0 91 04 a1 cc 16 8b 84 b9 5b 94 84 04 a1 07 07 ce 2d a0 ea 99 4f c2 42 82 b0 37 61 e9 42 2e e1 4e 29 73 7f a3 84 a0 36 14 c2 0f 71 84 ca f8 f6 0c 8c f6 7b 34 dc 06 d4 99 9e 71 11 df 02 3b bd 9e 73 8d c3 81 90 20 a9 be 59 49 8a bb 48 9c f3 b8 1a a5 44 e6 6b 46 8a e3 6f 40 a2 1b a2 e4 35 cb 1e 52 2f 2c b9 02 35 93 c8 36 72 16 ae 72 76 0f 97 be d1 e6 e4 07 5b 4a a6 e0 37 5f 77 ed ba 8f c1 03 27 b1 cf 42 19 e7 20 cd 60 7c d0 50 11 f0 14 a6 99 d4 e2 6a 30 a1 05 d7 eb f9 6a 9f 36 0e 38 99 b2 90 8b f3 3c 5b c5 0b 15 10 3e 81 75 ad 18 68 f5 e9 c9 6f 31 82 21 30 1c 2e 63 a1 2f 51 d6 67 8e 3e d6 12 fd be 82 b5 70 70 e4 2a 92 c3 96 48 59 27 09 7a bd 58 9f 3d 83 77 9c bd 1c 5e 17 96 58 38 57 10 4e 93 4c 30 21 5b ee 31 2c 98 93 21 68 2d 16 0c 14 a4 4f a7 97 07 c3 eb 42 2d fa cc 5e 6f 34 99 4c ac 81 70 15 e7 b0 b3 8d 89 5e 6f 0a 51 2f bf e0 77 2c 5b 4b 7d 91 84 97 3c 08 50 4f 4a 18 b0 15 e2 e1 3e 65 8d d5 5e d4 35 87 4d 6f 79 02 9b 40 a6 be d6 e2 74 9d 23 09 17 5a 99 41 28 f8 6d c2 d3 85 b0 95 a7 89 05 d2 72 76 97 dd b3 ba 81 9a 69 cd aa 62 de 07 d3 47 3a 15 99 c0 c7 3d 44 88 69 96 24 f1 4a b0 d7 09 84 17 52 cd 94 0c 90 da 1a 1d 42 2a 7e e0 48 c5 11 b7 45 f8 f4 d4 74 53 c7 d1 54 7c 0b 42 f6 cd 1f 06 63 59 2c 37 44 72 a0 51 c5 2c 5b 6a da 91 54 38 f5 ad 30 15 87 18 38 62 9e 0a 47 ed 60 32 74 8f 0d 15 97 5a cc c1 35 5b b8 fa 2b 7b 44 2f 8d c8 4d f1 44 4c 98 c8 d9 3c 67 62 e9 5b 6e ed 5c 42 37 ca 53 5b e8 56 f6 fa 21 7d 53 2c 3c c1 65 30 5b c4 19 97 86 d6 e8 ba 45 ca 80 7d 21 f3 ec b1 11 a7 8d a0 b5 29 bc<br>Data Ascii: ZYs8~-_Ac4dQf(+Ll5xgVlB@v/v=R_\lgQ+N,\E_p-iv8ssXJmNgY4Koe26~L)KWYJ(M(Our:EBJly! Naj7;%GJ 4zxq,y-yeIrl9Hl)'unY.`UDu"O+dD+MpH"*8Ci?3\;WBq<B1"zOf+BcQ+_4Mmt\$IM((@SfX=%ao-!f!-;&#j) g\$G<h_-[-OB7aB .N)s6q{4q;s YIHdKfO@5R/,56rrv[J7_w'B ` Pj0j68<[>uho1!0.c/Qg>pp*HYzX=w~X8WNL0[L,!h-OB-^o4Lp^oQ/w,[K] <POJ>e^*5Moy@t#ZA(mrvibG:=Di\$JRB*-HEtSTjBcY,7DrQ,[jT808bG'2tZ5[-{D/MDL<gb[n]B7S[V!]S,<e0[E]!)) |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 6          | 192.168.2.4 | 49755       | 31.13.92.14    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:06.311615944 CEST | 2418               | OUT       | GET /en_US/sdk.js HTTP/1.1<br>Accept: application/javascript, */*;q=0.8<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: connect.facebook.net<br>Connection: Keep-Alive                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Jun 4, 2021<br>21:35:06.357503891 CEST | 2423               | IN        | HTTP/1.1 200 OK<br>Vary: Accept-Encoding<br>ETag: "ba9f0ec2174cb64bbf6b24041a464d02"<br>timing-Allow-Origin: *<br>X-Frame-Options: DENY<br>Content-Encoding: gzip<br>x-fb-content-md5: 9d743430d831ff90a09728221bca338d<br>Access-Control-Allow-Origin: *<br>cross-origin-resource-policy: cross-origin<br>Strict-Transport-Security: max-age=31536000; preload; includeSubDomains<br>Content-Type: application/x-javascript; charset=utf-8<br>X-Content-Type-Options: nosniff<br>Access-Control-Expose-Headers: X-FB-Content-MD5<br>cross-origin-opener-policy: same-origin-allow-popups<br>Cache-Control: public,max-age=1200,stale-while-revalidate=3600<br>x-fb-rlafr: 0<br>Expires: Fri, 04 Jun 2021 19:49:22 GMT<br>Content-MD5: ZTsoPVONwwIGPdARhTPv4w==<br>X-FB-Debug: ppWjtkZHKO3hfBS15FXgrn7eps2UjtbtAJKj3S6nFOUQ++uK3UNlykSco4ImfkfE3zY8uX+VPj6sZ9GqoXMw==<br>Priority: u=3,i<br>X-FB-TRIP-ID: 1527350943<br>Date: Fri, 04 Jun 2021 19:35:06 GMT<br>Alt-Svc: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600<br>Connection: keep-alive<br>Content-Length: 1781<br>Data Raw: 1f<br>Data Ascii: |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 7          | 192.168.2.4 | 49761       | 192.0.76.3     | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:07.859143972 CEST | 2622               | OUT       | GET /g.gif?v=ext&j=1%3A8.6.2&blog=140258946&post=1055&tz=-7&srv=www.tonhc.org&host=www.tonhc.org&ref=&fcp=0&rand=0.17398007048479241 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/coronavirus/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: pixel.wp.com<br>Connection: Keep-Alive             |
| Jun 4, 2021<br>21:35:07.902842045 CEST | 2623               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 04 Jun 2021 19:35:07 GMT<br>Content-Type: image/gif<br>Content-Length: 50<br>Connection: keep-alive<br>Cache-Control: no-cache                                                                                                                                                                                                                                                                                                     |
| Jun 4, 2021<br>21:35:41.187129974 CEST | 4651               | OUT       | GET /g.gif?v=ext&j=1%3A8.6.2&blog=140258946&post=116&tz=-7&srv=www.tonhc.org&host=www.tonhc.org&ref=&fcp=0&rand=0.7313772066002118 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/about/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: pixel.wp.com<br>Connection: Keep-Alive                     |
| Jun 4, 2021<br>21:35:41.229811907 CEST | 4654               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 04 Jun 2021 19:35:41 GMT<br>Content-Type: image/gif<br>Content-Length: 50<br>Connection: keep-alive<br>Cache-Control: no-cache                                                                                                                                                                                                                                                                                                     |
| Jun 4, 2021<br>21:35:43.998455048 CEST | 4672               | OUT       | GET /g.gif?v=ext&j=1%3A8.6.2&blog=140258946&post=130&tz=-7&srv=www.tonhc.org&host=www.tonhc.org&ref=&fcp=0&rand=0.7339871367483555 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/mission/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: pixel.wp.com<br>Connection: Keep-Alive                   |
| Jun 4, 2021<br>21:35:44.040345907 CEST | 4673               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 04 Jun 2021 19:35:44 GMT<br>Content-Type: image/gif<br>Content-Length: 50<br>Connection: keep-alive<br>Cache-Control: no-cache                                                                                                                                                                                                                                                                                                     |
| Jun 4, 2021<br>21:35:48.547990084 CEST | 5643               | OUT       | GET /g.gif?v=ext&j=1%3A8.6.2&blog=140258946&post=89&tz=-7&srv=www.tonhc.org&host=www.tonhc.org&ref=&fcp=0&rand=0.7034506522366686 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/facilities/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: pixel.wp.com<br>Connection: Keep-Alive                 |
| Jun 4, 2021<br>21:35:48.591696024 CEST | 5644               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 04 Jun 2021 19:35:48 GMT<br>Content-Type: image/gif<br>Content-Length: 50<br>Connection: keep-alive<br>Cache-Control: no-cache                                                                                                                                                                                                                                                                                                     |
| Jun 4, 2021<br>21:35:51.220779896 CEST | 7034               | OUT       | GET /g.gif?v=ext&j=1%3A8.6.2&blog=140258946&post=203&tz=-7&srv=www.tonhc.org&host=www.tonhc.org&ref=&fcp=0&rand=0.7936902269709519 HTTP/1.1<br>Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5<br>Referer: http://www.tonhc.org/facilities/sells-hospital/<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: pixel.wp.com<br>Connection: Keep-Alive |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                          |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:51.262768030 CEST | 7034               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 04 Jun 2021 19:35:51 GMT<br>Content-Type: image/gif<br>Content-Length: 50<br>Connection: keep-alive<br>Cache-Control: no-cache |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 8          | 192.168.2.4 | 49785       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:38.787404060 CEST | 3969               | OUT       | GET /about/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Jun 4, 2021<br>21:35:39.276021957 CEST | 3970               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:38 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>Cache-Control: no-store, no-cache, must-revalidate<br>Pragma: no-cache<br>Link: <http://www.tonhc.org/wp-json/>; rel="https://api.w.org/"<br>Link: <http://www.tonhc.org/wp-json/wp/v2/pages/116>; rel="alternate"; type="application/json"<br>Link: <https://wp.me/P9uvL4-1S>; rel=shortlink<br>X-TEC-API-VERSION: v1<br>X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br>X-TEC-API-ORIGIN: http://www.tonhc.org<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 11653<br>Keep-Alive: timeout=5, max=100<br>Connection: Keep-Alive<br>Content-Type: text/html; charset=UTF-8<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d e9 72 1b 39 d2 e0 6f 2b 62 de 01 a6 63 4c 69 9a 45 56 91 d4 45 89 f2 a8 65 7b ec f9 7c 28 2c 79 fa 9b b5 1c 0c 90 04 c9 b2 8a 55 d5 75 e8 68 b7 7e 7d af b0 0f 30 bb 11 fb 0a fb 58 df 33 6c 1e a8 8b 97 28 8b 3e 66 76 3c d3 22 0a 47 22 91 99 48 24 80 04 b0 ff f0 e9 db a3 d3 bf 1f 3f 13 a3 68 ec 1c ac ed e3 8f 70 a4 3b 6c 97 94 6b bc 3f 29 89 9e 23 c3 b0 5d c2 84 4e 18 05 2a ea 8d 54 5f 04 2a f4 3d 37 b4 2f 94 90 17 86 1f 28 c7 93 7d 15 18 7d 3b 94 5d 07 32 40 6c 5f 0d 64 ec 44 86 63 0f 47 51 d7 bb 12 54 49 67 a4 30 67 27 f2 7c fe 76 bc a1 d7 71 d4 20 e2 cf b1 b4 dd 8e 2b 2f 74 3e 1d a9 dc b8 13 20 1c fe ee c5 61 e4 8d 0b f0 c2 c8 ee 9d 5f 17 a3 46 81 ed 9e db ee 50 03 f1 ba b6 a3 18 96 3f f2 5c c5 d1 29 ca 85 a2 4a 06 bd 91 dd f3 5c 5d a1 e7 46 ca 8d 3a 12 1a e3 76 7a 10 4c 50 d3 05 62 97 10 c0 66 cd 81 c8 b4 9b 48 04 40 c1 75 c7 ee 77 2c 6b 0b 69 e6 7a 48 cc 0b 5b 5d 8a 12 b2 03 ca c2 cf 58 45 52 f4 46 32 08 55 d4 2e bd 3f 7d 6e ec 94 44 ed 60 6d 6d 6d ff a1 61 08 6e 98 80 c4 08 1b 6b 18 49 11 57 8e 55 bb 84 d0 7c 2f 88 80 97 dc 8a 76 e9 d2 ee 47 a3 76 1f 2a ea 29 83 3e 2a c2 76 ed c8 96 8e 11 f6 a4 a3 da 56 45 8c e5 95 3d 8e c7 49 04 e0 c3 d5 9d f4 02 db 8f c2 da d1 c9 89 90 6e 5f 5c fa d4 46 31 f2 bc 73 aa 7c ed 01 e5 3b 1d d9 a1 08 ed 48 09 f8 f5 fc c8 1e db bf 41 bb 2f ed 68 24 a2 91 12 7f f7 64 18 89 93 67 6f 85 ef c4 43 db 15 17 56 b3 da 10 06 50 26 f2 c3 56 ad 76 8d 19 aa 3d 6f 5c bb f4 82 3e d0 25 0c 6b 9c 35 ac 85 ca ab 51 65 0f f6 23 3b 72 d4 c1 a9 07 2c f5 c4 db c7 8f cc c6 ee 9e d7 1f c9 b1 78 23 23 1b 38 f8 42 49 07 ea 3c 92 81 02 e8 87 5d 2f 8e f6 6b 5c 0a 8a e7 28 d5 57 21 b5 0d 0a e5 88 b5 24 e4 4b 19 0a 15 46 c0 5c 3b c4 2e 02 0d fa 6b ec 5c 8b ba 89 ac 05 3a 01 15 92 6e 03 02 20 06 5e 20 fc c0 bb b0 fb c8 b4 5f 63 10 ad 08 e4 97 20 f6 10 60 a8 02 e4 4f 48 39 a3 c0 ee 4a 47 8c d5 b8 ab 82 b0 4a ec 2f e0 1e 78 5d 2f 0a 73 68 db 6e 5f<br>Data Ascii: }r9o+bcLiEVEe{[(,yUuh~)0X3l(>fv<"G"H\$?hp;lk?)#]N*T_*=7/({});2@!_dCcGQTlg0g[!vq +/t> a_FP?)J]JF:vz LPbfH@uw,kizH[]XERF2U.?)nD' mmmankIWUJ/vGv*)>*vVE=ln _F1s!;HA/h\$dgocVP&Vv=ol>%k5Qe#;r,x##8BI< /K(W!\$ KFi;.k:n ^ _c `OH9JGJ/xj/shn_ |
| Jun 4, 2021<br>21:35:42.989518881 CEST | 4655               | OUT       | GET /mission/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:46.272372961 CEST | 5434               | OUT       | GET /favicon.ico HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Jun 4, 2021<br>21:35:46.661710978 CEST | 5434               | IN        | HTTP/1.1 302 Found<br>Date: Fri, 04 Jun 2021 19:35:46 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>Cache-Control: no-store, no-cache, must-revalidate<br>Pragma: no-cache<br>Link: <http://www.tonhc.org/wp-json/>; rel="https://api.w.org/"<br>X-TEC-API-VERSION: v1<br>X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br>X-TEC-API-ORIGIN: http://www.tonhc.org<br>X-Redirect-By: WordPress<br>Location: http://www.tonhc.org/wp-includes/images/w-logo-blue-white-bg.png<br>Content-Length: 0<br>Keep-Alive: timeout=5, max=97<br>Connection: Keep-Alive<br>Content-Type: text/html; charset=UTF-8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Jun 4, 2021<br>21:35:46.664797068 CEST | 5435               | OUT       | GET /wp-includes/images/w-logo-blue-white-bg.png HTTP/1.1<br>Accept: */*<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Jun 4, 2021<br>21:35:46.855386019 CEST | 5436               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:46 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Last-Modified: Thu, 11 Jun 2020 00:06:21 GMT<br>ETag: "1017-5a7c3bb05348e"<br>Accept-Ranges: bytes<br>Content-Length: 4119<br>Keep-Alive: timeout=5, max=96<br>Connection: Keep-Alive<br>Content-Type: image/png<br>Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 50 00 00 00 50 08 06 00 00 00 8e 11 f2 ad 00 00 0f de 49 44 41 54 78 da e5 5d 09 78 55 c5 15 0e 5b c1 c8 56 10 d1 2a 29 9b 4b 6b ad c5 da 56 ad 6b b5 1b 4a 5d 6a 4b 45 6c 3f f5 ab b5 74 b7 04 12 21 09 7b 14 2c a0 a2 11 45 83 d9 13 b2 90 90 1d 92 40 c0 b0 84 b0 46 90 25 04 08 81 10 12 42 16 12 b2 4e e7 bf 79 93 cc 9d 77 97 b9 f7 bd 87 49 7b be 6f be f0 de 9b 3b cb b9 73 e6 9c f3 9f 33 83 97 d7 57 48 d7 cf 8b 1b ff ad a5 c9 2f d3 b2 7a 42 70 d2 96 6f 2c 58 57 f2 f5 80 98 9a 81 b3 23 5a bd 66 86 11 be 7c 6d 76 44 f3 d0 39 d1 17 46 06 c6 1c a2 cf a5 8d 08 8c 79 ab 9f 6f f8 b3 f4 b7 31 5e ff 37 34 33 6c d8 d8 c5 09 af de f9 76 ca e7 23 03 63 1b 45 26 f1 65 d8 dc 68 55 31 aa 7b 8d 7f e4 05 ca e0 08 fa ef a9 b4 0c f9 5f 63 5a ff fb 57 65 bc 76 fb d2 f5 c5 03 66 85 77 f0 13 1f b3 28 81 fc 36 7c 0b 59 bc e9 20 49 3a 78 9a ec 2d af 26 17 1a ae 90 8e 0e e2 44 f8 0e bf a1 0e ea e2 19 3c 8b 36 f8 36 e9 aa 6c b9 f6 8d a8 54 fa ef 29 b4 f4 eb b5 7c bb fd ad f5 23 9f fc 24 67 1d 15 b7 56 4e 0c c9 93 9f e4 92 0f b7 1f 21 27 2f 36 10 77 11 da 42 9b 68 1b 7d b0 fe 06 f9 45 56 f6 f5 0d f3 a5 ff 1e da 6b 18 37 22 20 66 e8 7d ef a5 47 0e 7e 23 aa 8d 4d e4 fb 2b d3 c8 ea ed 47 c9 a5 a6 16 e2 69 42 1f e8 eb ee 15 a9 5d 8c ec 3f 2b bc 96 fe f5 a3 c5 bb 27 8b 6a 9f 47 42 b2 16 50 25 d0 cc 06 fe ab d0 5c b2 ad f4 bc f4 e4 eb af b4 92 c3 e7 2f 91 cd 25 15 8a 98 26 1c 38 45 12 0f 9e 22 e9 87 cf 90 bc e3 15 a4 b8 a2 86 34 34 b7 4a b7 87 be 31 06 8e 91 15 f4 ef b4 1e c7 bb d7 53 0a 1f a3 8a a1 92 0d f4 b1 d5 d9 64 cf 99 6a c3 c9 5d 6e 69 25 19 5f 96 93 39 19 7b c9 4f 3f da 48 a8 06 36 54 14 7c a1 dd 47 43 b2 95 67 b3 8f 9c 55 18 6f 44 45 74 2c 3f f9 30 bb eb f9 81 7e 11 9b e9 df 71 3d 82 79 cf 7e b6 39 e4 5a ff a8 2e a5 80 15 63 b4 c2 c2 76 97 90 5f ae c9 c1 fe 24 cd 30 b3 32 c0 b1 b7 46 ee 39 61 c8 4c 8c 8d 29 1d aa 6c 2e d3 bf d3 bf 32 c6 8d 9e 17 77 ed 0f df 49 df cf 26 f1 a7 f8 1d a4 56 67 8f fb b2 b2 96 cc 48 dc 49 06 cf 89 72 1b d3 f4 0a d5 c0 e4 2f b4 af 92 aa 7a cd b1 60 8c 18 2b f7 cc 1a 5a 06 5e 55 e6 3d 1a 92 35 61 42 70 62 0d 06 30 3c 20 86 ac 2f 3e ad 39 d8 63 17 ea c8 ef 22 f2 49 1f df 30 8f 33 4e 2c 7d 7d c3 c9 d4 f0 7c 5d 46 62 8f c5 d8 51 b7 cf cc b0 1d f4 ef a8 ab c2 bc 57 e2 0a 1e a1 ab 4f 51 14 df 79 3b 85 1c af aa d3 7c cb 33 37 ec c6 a6 7d d5 19 a7 e1 c1 28 63 d1 b2 00 f0 82 ef 58 96 e2 60 78 58 29 df 3b d1 a3 cc 0b cc dc fb 3c 35 53 da d1 e1 cf 3e da a4 39 a8 8d 47 cf 3a 19 b7 3d a1 dc bc 30 5e 19 9b 96 d9 f3 f8 ea 8d 6c 5f 3c 47 ff de e2 11 e6 cd 48 dc f1 18 f5 43 15 4f 82 2a 0e d2 dc d6 ae 1a 48 6b 7b 87 f2 a6 7b 1a e3 c4 f2 b7 a4 5d 4e 63 c7 e7 a7 42 f3 98 38 97 bb 7d 25 3e 1d 9a 77 eb 0d f3 e3 5a d0 c1 af 29 f3 da da d5 be 16 5c ac 87 3e c8 ea f1 cc 63 e5 c7 ab 32 c9 f9 fa 26 d5 1c 30 27 c6 44 5a 4a dc b6 27 7e 7b 59 f2 e0 89 c1 49 97 d0 f0 cf 3f de e4 f4 f6 b0 07 de f2 66 52 af 61 1e ca d8 c5 89 e4 8f eb b6 3b 99 3 c 98 1b 6c 52 47 bd ed 6e d1 ce f7 bd 97 51 8c 06 bf fb 9f 0d 4e 66 0a 36 e1 9b e8 de d2 5b 18 47 e7 42 76 9d ae 32 75 0 5 99 62 51 4c 1c 57 88 9a 20 b0 91 08 75 cf c8 89 6a b5 39 50 7a b1 be 57 31 0f e2 29 4a 8f 1e 41 aa 86 77 43 68 f6<br>Data Ascii: PNGIHDRPPIDATxJxU[V*]KkVkJj]KEI?tl{,E@F%Bnywl{o:s3WH/zBpo,XW#ZfjmvD9Fyo1^743lv#cE#ehU1[_cZWefw(6[Y !:x-&D<66IT)]# \$gVN!/'6wBh)EVk7" fJG~#M+GiB]?+jGBP%V%&8E"44J1Sd]jni%_9[O?H6T]AGCgUoDeT,? 0-q=y-9Z.cv_\$02F9aL).2wl&VgHlr/z'^U=5aBpb0< />9c"l03N,}}]]FbQWOQy;[37](cX`xx);<5S>9G:=0^l_<GHCO* Hk{[NcBh}%>wZ)>c2&0'DZJ'~{YI?fRa;<IRGnQNf6[GBv2ubQLW uj9PzW1)JAwCh |
| Jun 4, 2021<br>21:35:47.233211040 CEST | 5440               | OUT       | GET /facilities/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/xr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:47.657120943 CEST | 5441               | IN        | <p>HTTP/1.1 200 OK<br/> Date: Fri, 04 Jun 2021 19:35:47 GMT<br/> Server: Apache/2.4.18 (Ubuntu)<br/> Expires: Thu, 19 Nov 1981 08:52:00 GMT<br/> Cache-Control: no-store, no-cache, must-revalidate<br/> Pragma: no-cache<br/> Link: &lt;http://www.tonhc.org/wp-json/&gt;; rel="https://api.w.org/"<br/> Link: &lt;http://www.tonhc.org/wp-json/wp/v2/pages/89&gt;; rel="alternate"; type="application/json"<br/> Link: &lt;https://wp.me/P9uvL4-1r&gt;; rel=shortlink<br/> X-TEC-API-VERSION: v1<br/> X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br/> X-TEC-API-ORIGIN: http://www.tonhc.org<br/> Vary: Accept-Encoding<br/> Content-Encoding: gzip<br/> Content-Length: 12017<br/> Keep-Alive: timeout=5, max=95<br/> Connection: Keep-Alive<br/> Content-Type: text/html; charset=UTF-8<br/> Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d 69 72 1b 49 b2 e6 6f d1 ac ef 10 82 ac 05 b2 0b 09 20 01 70 03 09 aa 59 94 d8 52 3f 2d 34 91 ea 7a 3d a2 0c 16 40 06 80 24 13 19 59 b9 10 44 a9 68 f6 cc de 15 e6 cf fc eb 19 b3 b9 c2 1c 60 8e 32 07 78 67 18 77 8f c8 0d 1b 41 11 94 54 dd a5 ee 22 22 63 f5 f0 f0 f8 c2 63 db 7f fc fd dd d1 d9 df 4f 5e b0 41 38 74 0e d6 f6 f1 87 39 dc ed b7 0a c2 35 3e 9c 16 58 d7 e1 41 d0 2a 60 40 3b 08 7d 11 76 07 c2 62 be 08 3c e9 06 f6 95 60 fc ca f0 7c e1 48 6e 09 df b0 ec 80 77 1c 88 00 be 96 e8 f1 c8 09 0d c7 ee 0f c2 8e bc 66 54 48 7b 20 30 66 3b 94 9e fa 76 64 5f b6 1d d1 0b d5 e7 90 db 6e db e5 57 3a 9e f6 14 6e d4 f6 31 1f f5 dd 8d 82 50 0e 73 f9 05 a1 dd bd 1c e7 bd 06 be ed 5e da 6e 5f 67 22 3b b6 23 54 5e de 40 ba 42 79 27 24 e7 92 0a ee 77 07 76 57 ba ba 40 e9 86 c2 0d db 1c 2a e3 b6 bb e0 8c 49 d3 09 22 97 08 c0 6a cd c9 51 f1 6e 22 10 32 f2 c7 6d db 6a ef ec 22 cb 5c 89 bc bc b2 c5 88 15 b0 35 20 29 fc 0c 45 c8 59 77 c0 fd 40 84 ad c2 87 b3 63 63 a7 c0 2a 07 6b 6b 6b fb 8f 0d 83 a9 7a 31 08 0c b1 ae 86 11 27 71 f9 50 b4 0a 98 9b 27 fd 10 9a 52 55 a2 55 18 d9 56 38 68 59 50 50 57 18 f4 51 62 b6 6b 87 36 77 8c a0 cb 1d d1 32 4b 6c c8 af ed 61 34 8c 3d 80 1e 55 dc 69 d7 b7 bd 30 a8 1c 9d 9e 32 ee 5a 6c e4 51 15 d9 40 ca 4b 2a 7c ed 11 c5 3b 1b d8 01 0b ec 50 30 f8 95 5e 68 0f ed 5f a0 da 23 3b 1c b0 70 20 d8 df 25 0f 42 76 fa e2 1d f3 9c a8 6f bb ec ca 6c 94 eb cc 00 c6 84 5e d0 ac 54 c6 18 a1 dc 95 c3 ca 48 fa 16 f0 25 08 2a 2a 6a 50 09 84 ac 50 61 8f f6 43 3b 74 c4 c1 99 84 16 95 ec dd d3 27 d5 fa ee 9e b4 06 7c c8 de f2 d0 86 06 7c 29 b8 03 65 1e 71 5f 40 ee c7 bc 6b 3b 50 55 11 ec 57 54 52 c8 23 c3 2e 4b 04 54 41 48 99 e1 d8 92 d9 a7 99 33 fc 74 64 97 87 50 67 a8 dc a9 70 9c a0 c4 4e b9 cb fe 9d 43 93 f8 e4 86 52 df cb 80 13 1f 31 e8 d4 1e 42 8e f8 e5 f9 f2 ca b6 b0 55 7d 6c a5 80 f5 a4 cf b8 e3 30 0f 4a 05 92 98 2b 84 15 94 49 0e 72 f4 fb b2 23 c3 20 43<br/> Data Ascii: jïrlo pYR?-4z=@\$YDh"2xgwAT""ccO^A8t95&gt;XA*`@; ybc&lt; HnwfTH{ 0f;vd_nW:n1Ps^n_g";#T^@By'\$wvW @*!"jQn"2mj"5 )EYw@cc*kkz1'qP'RUUV8hYPPWQbk6w2Kla4=Ui02ZIQ@K*;P0^h_#;p %Bvol^TH%**jPPaC;t ) eq_@ k;PUWTR#.KTAH3tdPgpNCR1BUj)0J+Irr# C</p>                    |
| Jun 4, 2021<br>21:35:50.170500040 CEST | 6726               | OUT       | <p>GET /facilities/sells-hospital/ HTTP/1.1<br/> Accept: text/html, application/xhtml+xml, image/jxr, */*<br/> Accept-Language: en-US<br/> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br/> Accept-Encoding: gzip, deflate<br/> Host: www.tonhc.org<br/> Connection: Keep-Alive<br/> Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Jun 4, 2021<br>21:35:50.599148989 CEST | 6728               | IN        | <p>HTTP/1.1 200 OK<br/> Date: Fri, 04 Jun 2021 19:35:50 GMT<br/> Server: Apache/2.4.18 (Ubuntu)<br/> Expires: Thu, 19 Nov 1981 08:52:00 GMT<br/> Cache-Control: no-store, no-cache, must-revalidate<br/> Pragma: no-cache<br/> Link: &lt;http://www.tonhc.org/wp-json/&gt;; rel="https://api.w.org/"<br/> Link: &lt;http://www.tonhc.org/wp-json/wp/v2/pages/203&gt;; rel="alternate"; type="application/json"<br/> Link: &lt;https://wp.me/P9uvL4-3h&gt;; rel=shortlink<br/> X-TEC-API-VERSION: v1<br/> X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br/> X-TEC-API-ORIGIN: http://www.tonhc.org<br/> Vary: Accept-Encoding<br/> Content-Encoding: gzip<br/> Content-Length: 11569<br/> Keep-Alive: timeout=5, max=94<br/> Connection: Keep-Alive<br/> Content-Type: text/html; charset=UTF-8<br/> Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d 6b 72 1b 39 d2 e0 6f 2b 62 ee 00 97 a3 4d 71 9a 45 16 1f 7a 51 a2 7a d4 b2 3d f6 7c 96 ad 30 e5 e9 99 b5 1c 0c 90 04 c9 b2 8a 85 ea 7a 48 62 bb 15 b1 11 df 11 76 0f 30 bb 11 7b 85 3d c0 1e 65 0f f0 9d 61 33 13 a8 17 5f a2 2c ca fa 7c 3b 9e 69 11 85 47 22 91 09 24 12 89 04 70 f0 f8 d9 db e3 b3 bf 9f 3e 67 a3 70 ec 1c 6e 1c e0 0f 73 b8 3b 6c 19 c2 35 df b7 0d d6 73 78 10 b4 0c 4c e8 04 a1 2f c2 de 48 f4 99 2f 02 4f ba 81 7d 29 18 bf 34 3d 5f 38 92 f7 85 6f f6 ed 80 77 1d c8 00 b1 7d 31 e0 91 13 9a 8e 3d 1c 85 5d 79 cd a8 92 ce 48 60 ce 4e 28 3d f5 ed c8 a1 ec 38 62 10 aa cf 31 b7 dd 8e cb 2f 75 3e 1d 29 dc a8 e3 23 1c f5 dd 8b 82 50 8e 73 f0 82 d0 ee 5d 4c f2 51 23 df 76 2f 6c 77 a8 81 c8 ae ed 08 05 cb 1b 49 57 a8 e8 04 e5 5c 51 c1 fd de c8 ee 49 57 57 28 dd 50 b8 61 87 43 63 dc 4e 0f 82 31 6a ba 40 e4 12 02 d8 ac 05 10 15 ed a6 12 01 90 3f e9 d8 fd 4e cd aa 23 cd 5c 89 c4 bc b4 c5 15 33 90 1d 50 16 7e c6 22 e4 ac 37 e2 7e 20 c2 96 f1 fe ec 85 b9 6b b0 ca e1 c6 c6 c6 c1 63 d3 64 aa 61 0c 12 43 6c ac 69 c6 45 5c 3e 16 2d 03 a1 79 d2 0f 81 97 aa 15 2d e3 ca ee 87 a3 56 1f 2a ea 09 93 3e 4a cc 76 ed d0 e6 8e 19 f4 b8 23 5a d5 12 1b f3 6b 7b 1c 8d e3 08 c0 47 55 d7 ee f9 b6 17 06 95 e3 76 9b 71 b7 cf ae 3c 6a 23 1b 49 79 41 95 6f 3c a2 7c 67 23 3b 60 81 1d 0a 06 bf d2 0b ed b1 fd 1b b4 fb ca 0e 47 2c 1c 09 f6 77 c9 83 90 b5 9f bf 65 9e 13 0d 6d 97 5d 56 1b e5 3a 33 81 32 a1 17 34 2b 95 09 66 28 f7 e4 b8 72 25 fd 3e d0 25 08 2a 2a 6b 50 09 84 ac 50 65 8f 0e 42 3b 74 c4 61 5b 38 4e c0 5e ca c0 b3 43 ee 00 94 b3 b7 6f cc 97 c7 07 15 95 0c f9 32 24 f1 65 57 86 41 86 20 b6 db 17 d7 25 36 90 8e 23 af 88 b6 b9 fc 43 29 87 8e 80 32 8b 8a 10 b5 cc c0 b5 3d 4f 84 4d 53 51 cf b4 c7 7c 28 62 86 36 1d ee 0f 85 4a b8 b4 fb 22 e1 34 64 9f ad b1 0b 9c 7c f0 fa 1c 18 1e 30 94 9d 96 d1 e3 ae 74 6d 60 b4 c1 46 be 18 e0 78 0f 3d 60 c1 d5 d5 55 39 94 ee a8 57 96 fe b0 32 e0 3d<br/> Data Ascii: }kr9o+bMqEzQz=[0zHbv0{=ea3_};jG"\$p&gt;gpns;l5sxL/H/O)}4= _8ow}1=]yH^N(=8b1/u&gt;)#Ps}LQ#v/lwIW \QIWW(PaCcN1j)@?N#3P~"7~ kcdacIIE&gt;-v~&gt;Jv#Zk[GUvq&lt;j#lyAo&lt;[g#;`G,wem]V:324+f(r%&gt;%**kPPeB;ta[8N^Co2\$ eWA %6#C)2=OMSQ[(b6J"4d]0tm'Fx= 'U9W2=</p> |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:55.553311110 CEST | 7126               | OUT       | GET /facilities/san-simon/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4 |

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                                               |
|------------|-------------|-------------|----------------|------------------|-------------------------------------------------------|
| 9          | 192.168.2.4 | 49790       | 64.25.66.82    | 80               | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp                              | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jun 4, 2021<br>21:35:55.821789980 CEST | 7127               | OUT       | GET /facilities/san-simon/ HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: www.tonhc.org<br>Connection: Keep-Alive<br>Cookie: PHPSESSID=a5ulen80ifecc1vdmhk7ti8kb4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Jun 4, 2021<br>21:35:56.282046080 CEST | 7129               | IN        | HTTP/1.1 200 OK<br>Date: Fri, 04 Jun 2021 19:35:55 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>Cache-Control: no-store, no-cache, must-revalidate<br>Pragma: no-cache<br>Link: <http://www.tonhc.org/wp-json/>; rel="https://api.w.org/"<br>Link: <http://www.tonhc.org/wp-json/wp/v2/pages/346>; rel="alternate"; type="application/json"<br>Link: <https://wp.me/P9uvL4-5A>; rel=shortlink<br>X-TEC-API-VERSION: v1<br>X-TEC-API-ROOT: http://www.tonhc.org/wp-json/tribe/events/v1/<br>X-TEC-API-ORIGIN: http://www.tonhc.org<br>Vary: Accept-Encoding<br>Content-Encoding: gzip<br>Content-Length: 11332<br>Keep-Alive: timeout=5, max=100<br>Connection: Keep-Alive<br>Content-Type: text/html; charset=UTF-8<br>Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 7d 6b 72 1b 39 d2 e0 6f 2b 62 ee 00 97 a3 4d 71 9a c5 37 f5 a0 44 79 d4 b2 35 f6 7c 96 ad 30 e5 e9 6f d6 72 30 40 12 24 cb 2a 16 aa eb 21 89 6d 2b 62 23 be 23 ec 1e 60 76 23 f6 0a 7b a0 3d c0 77 86 cd 4c a0 5e 7c 89 b2 28 db bd 3b 9e 69 11 85 47 22 91 c8 4c 24 80 04 b0 ff f8 f9 db a3 b3 7f 9c be 60 a3 60 6c 1f 6c ec e3 0f b3 b9 33 6c 19 c2 31 df b7 0d d6 b3 b9 ef b7 0c 4c e8 f8 81 27 82 de 48 f4 99 27 7c 57 3a be 75 29 18 bf 34 5d 4f d8 92 f7 85 67 f6 2d 9f 77 6d c8 00 b1 7d 31 e0 a1 1d 98 b6 35 1c 05 5d 79 cd a8 92 ce 48 60 ce 4e 20 5d f5 6d cb a1 ec d8 62 10 a8 cf 31 b7 9c 8e c3 2f 75 3e 1d 29 9c b0 e3 21 1c f5 dd 0b fd 40 8e 33 f0 fc c0 ea 5d 4c b2 51 23 cf 72 2e 2c 67 a8 81 c8 ae 65 0b 05 cb 1d 49 47 a8 e8 18 e5 4c 51 c1 bd de c8 ea 49 47 57 28 9d 40 38 41 87 43 63 9c 4e 0f 82 11 6a ba 40 e8 10 02 d8 ac 05 10 15 ed a6 12 01 90 37 e9 58 fd 4e ad be 85 34 73 24 12 f3 d2 12 57 cc c0 ee 80 b2 f0 33 16 01 67 bd 11 f7 7c 11 b4 8c f7 67 c7 e6 8e c1 4a 07 1b 1b 1b fb 8f 4d 93 a9 86 31 48 0c b0 b1 a6 19 15 71 f8 58 b4 0c 84 e6 4a 2f 80 be 54 ad 68 19 57 56 3f 18 b5 fa 50 51 4f 98 f4 51 60 96 63 05 16 b7 4d bf c7 6d d1 aa 14 d8 98 5f 5b e3 70 1c 45 00 3e aa ba 76 cf b3 dc c0 2f 1d b5 db 8c 3b 7d 76 e5 52 1b d9 48 ca 0b aa 7c e3 11 e5 3b 1b 59 3e f3 ad 40 30 f8 95 6e 60 8d ad df a1 dd 57 56 30 62 c1 48 b0 7f 48 ee 07 ac fd e2 2d 73 ed 70 68 39 ec b2 52 2f d6 98 09 94 09 5c bf 59 2a 4d 30 43 b1 27 c7 a5 2b e9 f5 81 2e be 5f 52 59 fd 92 2f 64 89 2a 7b b4 1f 58 81 2d 0e da dc 61 6d 6b 0c 1d 06 35 bf 7d 63 be 3c da 2f a9 14 c8 92 a2 86 27 bb 32 f0 53 b4 b0 9c be b8 2e b0 81 b4 6d 79 45 64 cd e4 1f 4a 39 b4 05 94 59 54 84 08 65 fa 8e e5 ba 22 68 9a 8a 70 a6 35 e6 43 11 f5 65 d3 e6 de 50 a8 84 4b ab 2f e2 4e 86 ec b3 35 76 a1 13 1f bc 3e 1b 24 03 a4 d8 6e 19 3d ee 48 c7 82 3e 36 d8 c8 13 03 14 f5 c0 05 ea 5f 5d 5d 15 03 e9 8c 7a 45 e9 0d 4b 03 de b3 6c 60 10 01 a4<br>Data Ascii: }kr9o+bMq7Dy5j0or0@\$!m+b##`v#{=wL`)(;iG`L\$`!l3l1L`H`[W:u]4jOg-wm]15jyH`N`mb1/u>)!@3jLQ#r..geiGL QIGW/@8ACcNj@7XN4s\$W3gJgJM1HqXJ/ThWV?PQOQ`cMm_[pE>v];jVRHj;Y>@0n`WV0bHH-sph9R\Y*M0C'+_RY/d* {X-amk5}c</2S.myEdJ9Yte`hp5CePK/N5v>\$n=H>6_]zEKI' |

HTTPS Packets

| Timestamp                              | Source IP  | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                                                                        | Issuer                                                                                                                                                                                                                                                                                                      | Not Before                                                                              | Not After                                                                               | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|----------------------------------------|------------|-------------|-------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Jun 4, 2021<br>21:35:04.699965000 CEST | 192.0.77.2 | 443         | 192.168.2.4 | 49745     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |

| Timestamp                           | Source IP  | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                                                                           | Issuer                                                                                                                                                                                                                                                                                                            | Not Before                                                                                 | Not After                                                                              | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------|------------|-------------|-------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                                     |            |             |             |           | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                      | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                                                                                                             | Fri Nov 02 01:00:00 CET 2018                                                               | Wed Jan 01 00:59:59 CET 2031                                                           |                                                                                                                                            |                                  |
|                                     |            |             |             |           | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                             | CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                                                                                                                          | Tue Mar 12 01:00:00 CET 2019                                                               | Mon Jan 01 00:59:59 CET 2029                                                           |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:04.701514959 CEST | 192.0.77.2 | 443         | 192.168.2.4 | 49744     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018<br>Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed 01 00:59:59 CET 2031<br>Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| Jun 4, 2021 21:35:04.738396883 CEST | 192.0.77.2 | 443         | 192.168.2.4 | 49746     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018<br>Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed 01 00:59:59 CET 2031<br>Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| Jun 4, 2021 21:35:04.741415024 CEST | 192.0.77.2 | 443         | 192.168.2.4 | 49743     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018<br>Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed 01 00:59:59 CET 2031<br>Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |

| Timestamp                           | Source IP    | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                                                                           | Issuer                                                                                                                                                                                                                                                                                                            | Not Before                                                                              | Not After                                                                               | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------|--------------|-------------|-------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                                     |              |             |             |           | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                             | CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                                                                                                                          | Tue Mar 12 01:00:00 CET 2019                                                            | Mon Jan 01 00:59:59 CET 2029                                                            |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:05.458935022 CEST | 192.0.76.3   | 443         | 192.168.2.4 | 49747     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| Jun 4, 2021 21:35:05.459863901 CEST | 192.0.76.3   | 443         | 192.168.2.4 | 49748     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| Jun 4, 2021 21:35:06.456482887 CEST | 31.13.92.14  | 443         | 192.168.2.4 | 49756     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                          | Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013                             | Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028                             | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| Jun 4, 2021 21:35:07.915507078 CEST | 157.240.9.35 | 443         | 192.168.2.4 | 49758     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                          | Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013                             | Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028                             | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |

| Timestamp                           | Source IP      | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                  | Issuer                                                                                                                                                                   | Not Before                                                     | Not After                                                      | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------|----------------|-------------|-------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:07.926059961 CEST | 157.240.9.35   | 443         | 192.168.2.4 | 49759     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US         | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:08.416997910 CEST | 212.188.75.209 | 443         | 192.168.2.4 | 49762     | CN=*.fhl6-1.fna.fbcdn.net, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Sun May 16 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Sun Aug 15 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:08.417622089 CEST | 212.188.75.209 | 443         | 192.168.2.4 | 49763     | CN=*.fhl6-1.fna.fbcdn.net, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Sun May 16 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Sun Aug 15 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:10.658534050 CEST | 157.240.20.19  | 443         | 192.168.2.4 | 49764     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US         | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:10.674757004 CEST | 157.240.20.19  | 443         | 192.168.2.4 | 49765     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US         | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US<br>CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |                |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                     | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                         | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |

| Timestamp                                 | Source IP     | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                         | Issuer                                                                                     | Not Before                                                     | Not After                                                      | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------------|---------------|-------------|-------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Jun 4, 2021<br>21:35:10.697419882<br>CEST | 31.13.92.14   | 443         | 192.168.2.4 | 49771     | CN=*.facebook.com,<br>O="Facebook, Inc.",<br>L=Menlo Park,<br>ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US                                                                                      | CN=DigiCert High Assurance EV Root CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US     | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.697630882<br>CEST | 185.60.216.19 | 443         | 192.168.2.4 | 49768     | CN=*.facebook.com,<br>O="Facebook, Inc.",<br>L=Menlo Park,<br>ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US                                                                                      | CN=DigiCert High Assurance EV Root CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US     | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.697786093<br>CEST | 185.60.216.19 | 443         | 192.168.2.4 | 49767     | CN=*.facebook.com,<br>O="Facebook, Inc.",<br>L=Menlo Park,<br>ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US                                                                                      | CN=DigiCert High Assurance EV Root CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US     | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.707530022<br>CEST | 185.60.216.19 | 443         | 192.168.2.4 | 49770     | CN=*.facebook.com,<br>O="Facebook, Inc.",<br>L=Menlo Park,<br>ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US                                                                                      | CN=DigiCert High Assurance EV Root CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US     | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.708020926<br>CEST | 31.13.92.14   | 443         | 192.168.2.4 | 49772     | CN=*.facebook.com,<br>O="Facebook, Inc.",<br>L=Menlo Park,<br>ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US | Wed May 26 02:00:00 CEST 2021<br>Tue Oct 22 14:00:00 CEST 2013 | Wed Aug 25 01:59:59 CEST 2021<br>Sun Oct 22 14:00:00 CEST 2028 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US                                                                                      | CN=DigiCert High Assurance EV Root CA,<br>OU=www.digicert.com,<br>O=DigiCert Inc, C=US     | Tue Oct 22 14:00:00 CEST 2013                                  | Sun Oct 22 14:00:00 CEST 2028                                  |                                                                                                                                            |                                  |

| Timestamp                                 | Source IP     | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                                                                           | Issuer                                                                                                                                                                                                                                                                                                            | Not Before                    | Not After                     | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------------|---------------|-------------|-------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Jun 4, 2021<br>21:35:10.709494114<br>CEST | 185.60.216.19 | 443         | 192.168.2.4 | 49769     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                              | Wed May 26 02:00:00 CEST 2021 | Wed Aug 25 01:59:59 CEST 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                              | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                                  | Tue Oct 22 14:00:00 CEST 2013 | Sun Oct 22 14:00:00 CEST 2028 |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.709969044<br>CEST | 185.60.216.19 | 443         | 192.168.2.4 | 49766     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                              | Wed May 26 02:00:00 CEST 2021 | Wed Aug 25 01:59:59 CEST 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                              | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                                  | Tue Oct 22 14:00:00 CEST 2013 | Sun Oct 22 14:00:00 CEST 2028 |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.861078978<br>CEST | 31.13.92.14   | 443         | 192.168.2.4 | 49774     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                              | Wed May 26 02:00:00 CEST 2021 | Wed Aug 25 01:59:59 CEST 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                              | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                                  | Tue Oct 22 14:00:00 CEST 2013 | Sun Oct 22 14:00:00 CEST 2028 |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:10.861713886<br>CEST | 31.13.92.14   | 443         | 192.168.2.4 | 49773     | CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US<br>CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                  | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                              | Wed May 26 02:00:00 CEST 2021 | Wed Aug 25 01:59:59 CEST 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                              | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US                                                                                                                                                                                                                                  | Tue Oct 22 14:00:00 CEST 2013 | Sun Oct 22 14:00:00 CEST 2028 |                                                                                                                                            |                                  |
| Jun 4, 2021<br>21:35:40.440865040<br>CEST | 192.0.77.2    | 443         | 192.168.2.4 | 49788     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 | Tue Jul 05 02:00:00 CEST 2022 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                           |               |             |             |           | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                      | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                                                                                                             | Fri Nov 02 01:00:00 CET 2018  | Wed Jan 01 00:59:59 CET 2031  |                                                                                                                                            |                                  |

| Timestamp                           | Source IP  | Source Port | Dest IP     | Dest Port | Subject                                                                                                                                                                                                                           | Issuer                                                                                                                                                                                                                                                                                                            | Not Before                                                                              | Not After                                                                               | JA3 SSL Client Fingerprint                                                                                                                 | JA3 SSL Client Digest            |
|-------------------------------------|------------|-------------|-------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                                     |            |             |             |           | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                             | CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                                                                                                                          | Tue Mar 12 01:00:00 CET 2019                                                            | Mon Jan 01 00:59:59 CET 2029                                                            |                                                                                                                                            |                                  |
| Jun 4, 2021 21:35:40.441744089 CEST | 192.0.77.2 | 443         | 192.168.2.4 | 49787     | CN=*.wp.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB<br>CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US<br>CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB | Thu Apr 02 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 | Tue Jul 05 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
|                                     |            |             |             |           | CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                      | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                                                                                                             | Fri Nov 02 01:00:00 CET 2018                                                            | Wed Jan 01 00:59:59 CET 2031                                                            |                                                                                                                                            |                                  |
|                                     |            |             |             |           | CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US                                                                                                                             | CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB                                                                                                                                                                                                                          | Tue Mar 12 01:00:00 CET 2019                                                            | Mon Jan 01 00:59:59 CET 2029                                                            |                                                                                                                                            |                                  |

Code Manipulations

Statistics

Behavior

● iexplore.exe  
● iexplore.exe

 Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6628 Parent PID: 800

General

|                               |                                                              |
|-------------------------------|--------------------------------------------------------------|
| Start time:                   | 21:35:01                                                     |
| Start date:                   | 04/06/2021                                                   |
| Path:                         | C:\Program Files\internet explorer\iexplore.exe              |
| Wow64 process (32bit):        | false                                                        |
| Commandline:                  | 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding |
| Imagebase:                    | 0x7ff6422d0000                                               |
| File size:                    | 823560 bytes                                                 |
| MD5 hash:                     | 6465CB92B25A7BC1DF8E01D8AC5E7596                             |
| Has elevated privileges:      | true                                                         |
| Has administrator privileges: | true                                                         |
| Programmed in:                | C, C++ or other language                                     |
| Reputation:                   | low                                                          |

#### File Activities

|           |  |  |  |        |            |         |            |       |                |        |
|-----------|--|--|--|--------|------------|---------|------------|-------|----------------|--------|
| File Path |  |  |  | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--|--|--|--------|------------|---------|------------|-------|----------------|--------|

|           |  |  |        |        |       |       |            |       |                |        |
|-----------|--|--|--------|--------|-------|-------|------------|-------|----------------|--------|
| File Path |  |  | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|-----------|--|--|--------|--------|-------|-------|------------|-------|----------------|--------|

|           |  |  |  |  |        |        |            |       |                |        |
|-----------|--|--|--|--|--------|--------|------------|-------|----------------|--------|
| File Path |  |  |  |  | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--|--|--|--|--------|--------|------------|-------|----------------|--------|

#### Registry Activities

| Key Path |  |      | Name | Type     | Data     | Completion | Count | Source Address | Symbol |
|----------|--|------|------|----------|----------|------------|-------|----------------|--------|
|          |  |      |      |          |          |            |       |                |        |
| Key Path |  | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |

### Analysis Process: iexplore.exe PID: 6680 Parent PID: 6628

#### General

|                               |                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------|
| Start time:                   | 21:35:01                                                                                     |
| Start date:                   | 04/06/2021                                                                                   |
| Path:                         | C:\Program Files (x86)\Internet Explorer\iexplore.exe                                        |
| Wow64 process (32bit):        | true                                                                                         |
| Commandline:                  | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6628 CREDAT:17410 /prefetch:2 |
| Imagebase:                    | 0x320000                                                                                     |
| File size:                    | 822536 bytes                                                                                 |
| MD5 hash:                     | 071277CC2E3DF41EEEEA8013E2AB58D5A                                                            |
| Has elevated privileges:      | true                                                                                         |
| Has administrator privileges: | true                                                                                         |
| Programmed in:                | C, C++ or other language                                                                     |
| Reputation:                   | low                                                                                          |

#### File Activities

|           |  |  |  |        |            |         |            |       |                |        |
|-----------|--|--|--|--------|------------|---------|------------|-------|----------------|--------|
| File Path |  |  |  | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--|--|--|--------|------------|---------|------------|-------|----------------|--------|

|           |  |  |        |        |       |       |            |       |                |        |
|-----------|--|--|--------|--------|-------|-------|------------|-------|----------------|--------|
| File Path |  |  | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|-----------|--|--|--------|--------|-------|-------|------------|-------|----------------|--------|

|           |  |  |  |  |        |        |            |       |                |        |
|-----------|--|--|--|--|--------|--------|------------|-------|----------------|--------|
| File Path |  |  |  |  | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--|--|--|--|--------|--------|------------|-------|----------------|--------|

#### Registry Activities

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|----------|------|------|------|------------|-------|----------------|--------|
|----------|------|------|------|------------|-------|----------------|--------|

