



ID: 483800
Sample Name: 3FLps29lWm
Cookbook: default.jbs
Time: 13:56:58
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 3FLps29lWm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 44
General 44
File Icon 44
Static PE Info 44
General 44
Entrypoint Preview 44
Rich Headers 45
Data Directories 45
Sections 45
Resources 46
Imports 46
Exports 46
Version Infos 47
Possible Origin 47
Network Behavior 47
Network Port Distribution 47
TCP Packets 47
UDP Packets 47
DNS Queries 47
DNS Answers 47
HTTP Request Dependency Graph 48
HTTPS Proxied Packets 49
Code Manipulations 81
User Modules 81
Hook Summary 81
Processes 81
Statistics 82
Behavior 82
System Behavior 82

Copyright Joe Security LLC 2021

Analysis Process: loaddll64.exe PID: 6348 Parent PID: 412 82
General 82
File Activities 82
Analysis Process: cmd.exe PID: 6384 Parent PID: 6348 82
General 82
File Activities 82
Analysis Process: regsvr32.exe PID: 6408 Parent PID: 6348 82
General 82
File Activities 83
File Read 83
Analysis Process: rundll32.exe PID: 6420 Parent PID: 6384 83
General 83
File Activities 83
File Read 83
Analysis Process: iexplore.exe PID: 6448 Parent PID: 6348 83
General 83
File Activities 84
Registry Activities 84
Analysis Process: rundll32.exe PID: 6516 Parent PID: 6348 84
General 84
File Activities 84
File Read 84
Analysis Process: iexplore.exe PID: 6580 Parent PID: 6448 84
General 84
File Activities 84
Registry Activities 84
Analysis Process: explorer.exe PID: 3388 Parent PID: 6408 84
General 84
File Activities 85
File Created 85
File Deleted 85
File Written 85
File Read 85
Registry Activities 85
Key Created 85
Key Value Created 85
Analysis Process: rundll32.exe PID: 6772 Parent PID: 6348 85
General 85
File Activities 85
File Read 85
Analysis Process: rundll32.exe PID: 6944 Parent PID: 6348 85
General 85
File Activities 86
File Read 86
Analysis Process: rundll32.exe PID: 7000 Parent PID: 6348 86
General 86
Analysis Process: rundll32.exe PID: 7076 Parent PID: 6348 86
General 86
Analysis Process: rundll32.exe PID: 5264 Parent PID: 6348 86
General 86
Analysis Process: rundll32.exe PID: 2740 Parent PID: 6348 87
General 87
Analysis Process: rstrui.exe PID: 3180 Parent PID: 3388 87
General 87
Analysis Process: rstrui.exe PID: 1708 Parent PID: 3388 87
General 87
Analysis Process: Taskmgr.exe PID: 4600 Parent PID: 3388 88
General 88
Analysis Process: Taskmgr.exe PID: 4860 Parent PID: 3388 88
General 88
Analysis Process: FXSCOVER.exe PID: 748 Parent PID: 3388 88
General 88
Analysis Process: FXSCOVER.exe PID: 5492 Parent PID: 3388 89
General 89
Analysis Process: mstsc.exe PID: 4872 Parent PID: 3388 89
General 89
Analysis Process: mstsc.exe PID: 2456 Parent PID: 3388 89
General 89
Disassembly 89
Code Analysis 90

Copyright Joe Security LLC 2021

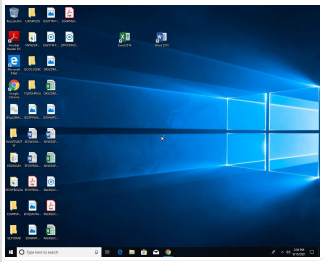
Windows Analysis Report 3FLps29lWm

Overview

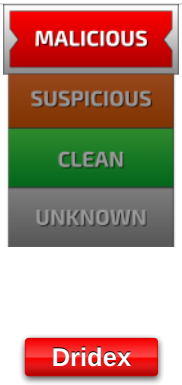
General Information

Sample Name:	3FLps29lWm (renamed file extension from none to dll)
Analysis ID:	483800
MD5:	0636cf8dafa624e..
SHA1:	b347c65c5add7e..
SHA256:	586999eb0a767ff..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

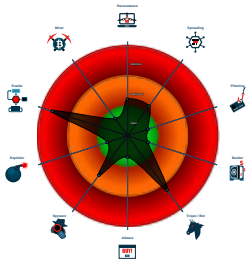


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Sigma detected: System File Execu…
- Changes memory attributes in foreig…
- Machine Learning detection for samp…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sigma detected: Regsvr32 Comman…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6348 cmdline: loaddll64.exe 'C:\Users\user\Desktop\3FLps29lWm.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 6384 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3FLps29lWm.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6420 cmdline: rundll32.exe 'C:\Users\user\Desktop\3FLps29lWm.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6408 cmdline: regsvr32.exe /s C:\Users\user\Desktop\3FLps29lWm.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rstrui.exe (PID: 3180 cmdline: C:\Windows\system32\rstrui.exe MD5: 3E8AFFA54035412F86663C8B44CAA2E5)
      - rstrui.exe (PID: 1708 cmdline: C:\Users\user\AppData\Local\UIPe\rstrui.exe MD5: 3E8AFFA54035412F86663C8B44CAA2E5)
      - Taskmgr.exe (PID: 4600 cmdline: C:\Windows\system32\Taskmgr.exe MD5: CB8FE4DA1AF43E62BAA6A4CBE0A93A74)
      - Taskmgr.exe (PID: 4860 cmdline: C:\Users\user\AppData\Local\zOAoLK\Taskmgr.exe MD5: CB8FE4DA1AF43E62BAA6A4CBE0A93A74)
      - FXSCOVER.exe (PID: 748 cmdline: C:\Windows\system32\FXSCOVER.exe MD5: BEAB16FEFCB7F62BBC135FB87DF7FDF2)
      - FXSCOVER.exe (PID: 5492 cmdline: C:\Users\user\AppData\Local\FQXVd7\FXSCOVER.exe MD5: BEAB16FEFCB7F62BBC135FB87DF7FDF2)
      - mstsc.exe (PID: 4872 cmdline: C:\Windows\system32\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
      - mstsc.exe (PID: 2456 cmdline: C:\Users\user\AppData\Local\yeShxe\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
    - iexplore.exe (PID: 6448 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 6580 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6448 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - rundll32.exe (PID: 6516 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginBufferedAnimation MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6772 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginBufferedPaint MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6944 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginPanningFeedback MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 7000 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintClear MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 7076 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintInit MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 5264 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintRenderAnimation MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 2740 cmdline: rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintSetAlpha MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Copyright Joe Security LLC 2021

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000002B.00000002.479085760.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000A.00000002.235930456.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000027.00000002.448796911.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000C.00000002.246415321.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.228897543.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:



Sigma detected: System File Execution Location Anomaly

Sigma detected: Regsvr32 Command Line Without DLL

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

E-Banking Fraud:



Yara detected Dridex unpacked file

System Summary:



Hooking and other Techniques for Hiding and Protection:



Modifies the prolog of user mode functions (user mode inline hooks)

HIPS / PFW / Operating System Protection Evasion:



Benign windows process drops PE files

Copyright Joe Security LLC 2021

Changes memory attributes in foreign processes to executable or writable

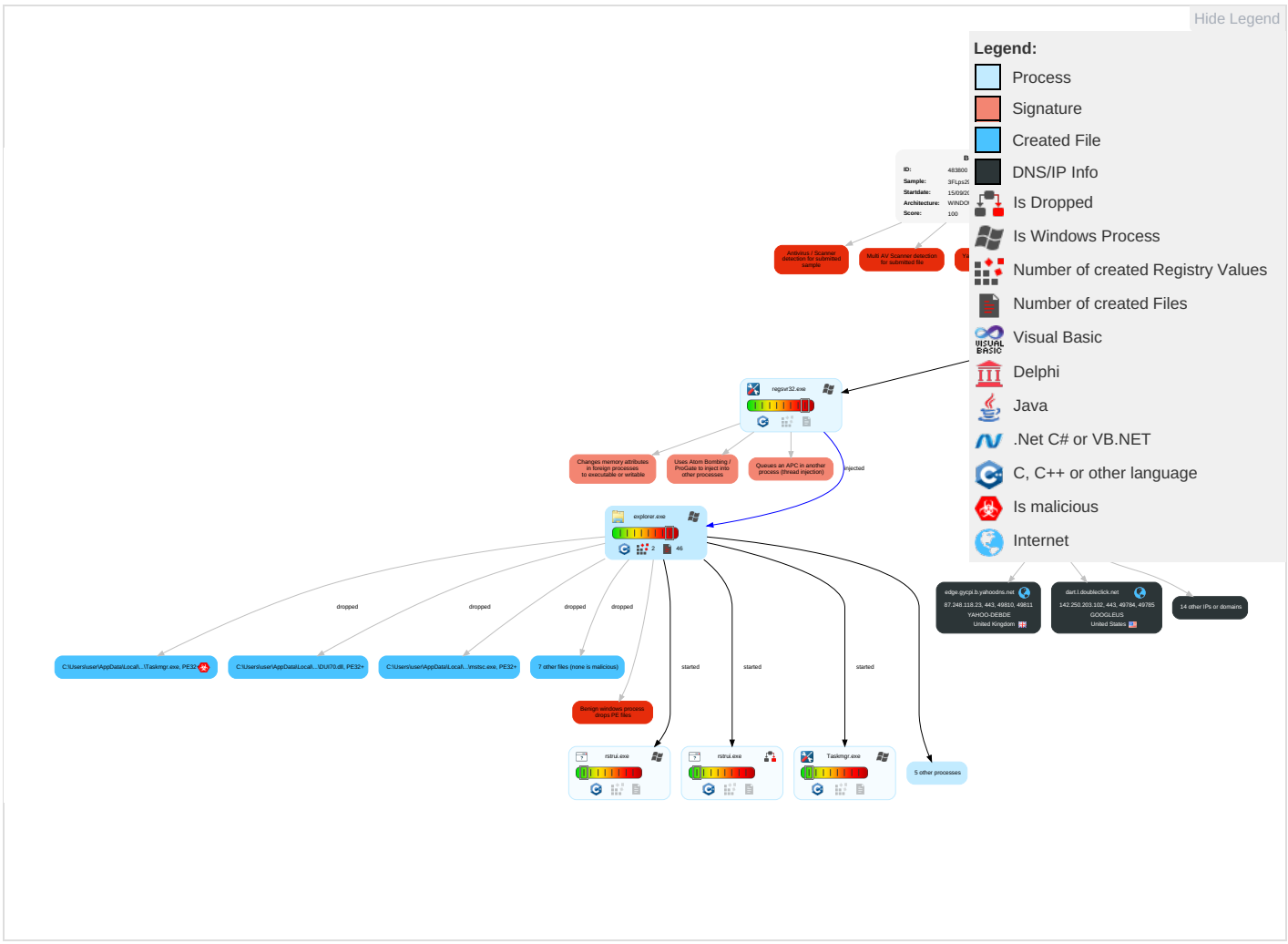
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Eff
Valid Accounts	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1	Credential API Hooking 1	System Time Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eav Ins Net Cor
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Obfuscated Files or Information 3	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 2 1	Exp Rec Cal
Domain Accounts	At (Linux)	Logon Script (Windows)	Access Token Manipulation 1	Software Packing 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Timestomp 1	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mai Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rootkit 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jan Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Ins Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols	
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols	

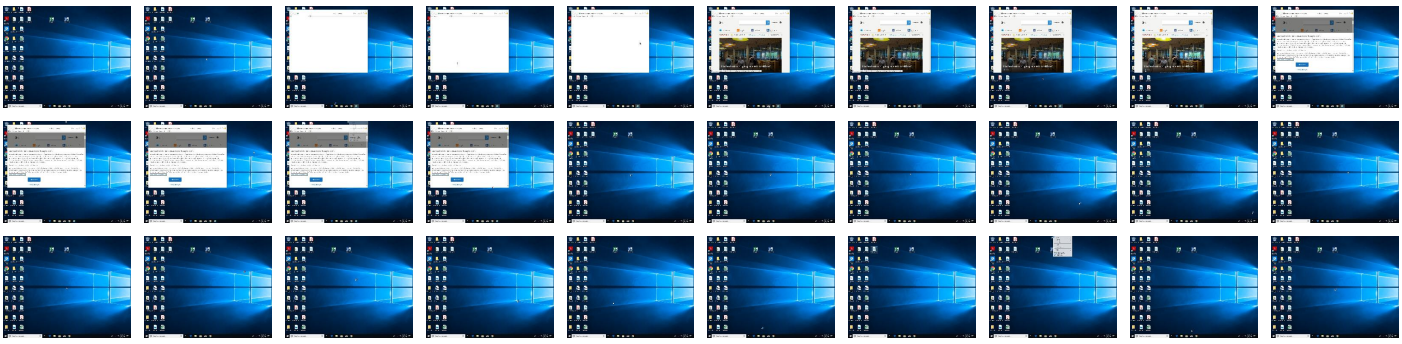
Behavior Graph



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
3FLps29lWm.dll	72%	Virustotal		Browse
3FLps29lWm.dll	63%	Metadefender		Browse
3FLps29lWm.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
3FLps29lWm.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
3FLps29lWm.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\UIPe\rstrui.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\UIPe\rstrui.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\c5BVxaoEy\dialer.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\c5BVxaoEy\dialer.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\lFQXVd7\FXSCOVER.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\yeShxe\mstsc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\yeShxe\mstsc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.2.Taskmgr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.rstrui.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.140000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.2.mstsc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.FXSCOVER.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5ac3b539d1cfda83dbe324033737805f.jpg	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_737%2Cy_504/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fe17134d780918219c201cb1db8da2d3f.jpeg	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_433%2Cy_315/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F560ad3dcc869b1dfc2bac1c99d35ac81.png	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.4888902266943189	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fb4d84d7a-e7a0-4e71-a4e1-288b18f4b1a1_166a74d60a77edc1b295914db4bc79ac.jpeg	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F7b4dbad0520957f16bd4e3f810f4c883.png	0%	Avira URL Cloud	safe	
http://https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp/datenschutz-ssp.html	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2F824258cd-2488-4e7c-b171-dad87f56f610_1000x600.jpeg	0%	Avira URL Cloud	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.160.23	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		high
hblg.media.net	2.18.160.23	true	false		high
lg3.media.net	2.18.160.23	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
btloader.com	172.67.70.134	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		high
ad-delivery.net	172.67.69.19	true	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		high
s.yimg.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5ac3b539d1cfda83dbe324033737805f.jpg	false	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_737%2Cy_504/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fe17134d780918219c201cb1db8da2d3f.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_433%2Cy_315/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F560ad3dcc869b1dfc2bac1c99d35ac81.png	false	• Avira URL Cloud: safe	unknown
http://https://ad-delivery.net/px.gif?ch=1&e=0.4888902266943189	false	• Avira URL Cloud: safe	unknown
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fb4d84d7a-e7a0-4e71-a4e1-288b18f4b1a1_166a74d60a77edc1b295914db4bc79ac.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/BXjlWewXmZ47HeV5NPvUYA--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1599143076228-3140.jpg	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F7b4dbad0520957f16bd4e3f810f4c883.png	false	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2F824258cd-2488-4e7c-b171-dad87f56f610_1000x600.jpeg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.67.70.134	btloader.com	United States		13335	CLOUDFLARENETUS	false
172.67.69.19	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483800
Start date:	15.09.2021
Start time:	13:56:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3FLps29lWm (renamed file extension from none to dll)
Cookbook file name:	default.jbs
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:	43
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@43/102@13/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.4% (good quality ratio 19.2%) • Quality average: 43.4% • Quality standard deviation: 37.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

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\DOMStore\BMWTD8BZ\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2186
Entropy (8bit):	4.879599447546181
Encrypted:	false
SSDEEP:	48:0wJLJLJLJLJOJOmJOJOJ9J9J9J9/J9J9/J9J9/kaJ9/kai:dhhhhh88m88vvvv/vv/vv/kav/kai
MD5:	66BD378DFBBF5FC467629E316E175663
SHA1:	1582CCDE052B189501ABB18940521E2DB30939C0
SHA-256:	B5EF265E02AFF344D90395864AE8E9AA7F5BCF6A80CF048946E89F893EEE4DFF
SHA-512:	7850A964E4CAF4E413E3514F14DA8B8686B5874A0E6470AAF75AD198084FA3452622AC69B2CA75B5A4EC6591AC4406529F2A013FF7F23B196463E6CF9C5E6200
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root></root><root><item name="HBCM_BIDS" value="{}" ltime="91075472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="91555472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="91555472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="91555472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="91555472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="101075472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="101075472" htime="30911093" /><item name="mntest" value="mntest" ltime="101075472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="101075472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="101075472" htime="30911093" /></root><root><item name="HBCM_BIDS" value="{}" ltime="101555472" htime="309

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\I1HSUQNA\www.msn[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	151
Entropy (8bit):	5.158058691162669
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAeotkH3sqSwKbZLKb:JFK1rUFkduqswEkIXH40AAeotRVub
MD5:	C91588ECEFC5B5E318C8D8CF27DA0F64
SHA1:	39FCE7B733BE0628FC2F32EE45123C5E8ECCAA90
SHA-256:	63E4B8C340E57B0305CE80025010ABCA330474E74AED6EE1CEF87CC6B62FBB84
SHA-512:	843155BE605C96C5ACCCAD5B7C0C50095A87CE19A186484F021764E7460E71C59F18897FC07D821CF2C2E54CEE6E422AE43760FFE313BC7EF0F5D43A39E44D8
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="141065472" htime="30911093" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3E34CBB0-1668-11EC-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7528207792093076
Encrypted:	false
SSDEEP:	384:rKvuLu12u1jfu1jwu1jadu1jaM5u1jHdMP0:s
MD5:	5B7CB363563A91B74ECFC7FE21A355BB
SHA1:	7CB201C61C685B1A2CA3B08D5F667E67D322F999
SHA-256:	19956D1E05E4596B0E53A4724B9FB14F825D57D2BD869A353B83FD9EFA6BD1EE
SHA-512:	CD7E2C3B4944677CCC0770BD1F47012E5B8215F14074D939BFE46E5EFB455357829C9BE440C557442716CB909088144ADE3EAEFA8DC50500ECA6D69A7A5E398
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3E34CBB2-1668-11EC-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	367052
Entropy (8bit):	3.6278849924304573
Encrypted:	false
SSDEEP:	3072:sZ/2Bfcdmu5kgTzGtgZ/2Bfc+mu5kgTzGtQZ/2Bfcdmu5kgTzGt5Z/2Bfc+mu5kT:FPOC6
MD5:	80DA4137352758A7E4E2F02C41EFED54
SHA1:	8E927E05D51218126A1AB20EBABEF6D3F22C9414
SHA-256:	C6E0E006537EB73DFFFF2044B5F06C29F71254207A8174DD20FFE8BBF96DA2FC
SHA-512:	73C491DCA52C0FE26ACF740525DCB7966D393A23DDA896669DCBB4EE548287352827B2B410816E7725EDF15D74B9CFA8943CE81B70FE7E46CFB6BD850AA8D5C
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\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):	5.069115427620107
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEL3xpI3xuNnWimI002EtM3MHdNMNxOEL3xpI3xuNnWimI00ObVbkEty:2d6NxOkxCxASZHKd6NxOkxCxASZ76b
MD5:	DEFAAAF495592511280C1FFBAA5D2699
SHA1:	E250850DDE7BD47598B7E5D2B2EC17059A84B3B7
SHA-256:	CF17C7948B2AE77E7FF422E96CFBEE5F86852FE85F45EFCCE84DBFAAD23078B3
SHA-512:	A24BDC4ECC708A578C7FEE99E3265265D7D0CE3CCEB21D1A03F7C43740B0603E124D953079F2E2CDB98BEAC6AECEAF0DC2D36A03F06AEAD5450AA4D232E0247
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x16106db3,0x01d7aa75</date><accdate>0x16106db3,0x01d7aa75</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x16106db3,0x01d7aa75</date><accdate>0x16106db3,0x01d7aa75</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\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):	5.082962273806184
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kTxpwxuNnWimI002EtM3MHdNMNxe2kTxpwxuNnWimI00Obkak6EtMb:2d6NxrMmASZHKd6NxrMmASZ7Aa7b
MD5:	70E3191019D51308C1563D8D510C8D2A
SHA1:	42C8E8FC4FAF8A19DA4AFC354E4DDCFB2CBA61B8
SHA-256:	D2C2D763BE0DD9ADDA8D79B00CC03A45FC24D07D3C35DF4320DF8940D99EDEA9
SHA-512:	724F55CAA6157F4803556B26AD901DCA853E07F1024D4F3BFFBD946339124372BC66C9115C7473A03629C51D320D9543EC6EAB5E00AC135B27DA7CEAC6A86CE
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</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>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</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):	5.086447876651904

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLL3xpI3xuNnWimI002EtM3MHdNMNxvLL3xpI3xuNnWimI00ObmZEtMb:2d6Nxv3xCxASZHKd6Nxv3xCxASZ7mb
MD5:	E748FBD1CEAC992B2ABE4C40A5FBA60A
SHA1:	F650AB8BE93086EED1F71B4BEF650D686950FA78
SHA-256:	30DDD728FF67A93D1E29D6A850A5D098ABFBDD3678AF4A1306C1DF8A9FA0147E
SHA-512:	6B23FBEA468341D868872727B9A83212F689EE8A544E50CFF6C780C51C4EB5C5CB9A641C2693AD4897CD7ECC3D57A50BDCDE3797195CB7E338B0D11DC2367F A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x16106db3,0x01d7aa75</date> <accdate>0x16106db3,0x01d7aa75</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>0x16106db3,0x01d7aa75</date><accda te>0x16106db3,0x01d7aa75</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	5.077313680496704
Encrypted:	false
SSDEEP:	12:TMHdNMNxiTxpwxuNnWimI002EtM3MHdNMNxiTxpwxuNnWimI00Obd5EtMb:2d6NxSmASZHKd6NxSmASZ7Jjb
MD5:	DF830B168C8105946A50E08E02673B69
SHA1:	1C0B099AFDA816AA3B1B76C705B052EBE445EB4A
SHA-256:	8A37080B0A1A9BF3FAB49B539213D20948D24CCDD0F9F844958069EC4D376C30
SHA-512:	20200D4C4D88E738F28E808059B890B4DF32807CB3D54FBFD10DCB0A18D8A54234D1D878041CA767BA192634E27958396D839AC2F5A7B000BEDE387EF9E8138
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1606e68c,0x01d7aa75</date><acc date>0x1606e68c,0x01d7aa75</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>0x1606e68c,0x01d7aa75</date><accdate>0x1606e 68c,0x01d7aa75</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):	5.10021592716898
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwL3xpI3xuNnWimI002EtM3MHdNMNxhGwL3xpI3xuNnWimI00Ob8K0z:2d6NxQYxCxASZHKd6NxQYxCxASZ7YKa/
MD5:	C9E385031B2CC71BAB887CF96FC4B2DB
SHA1:	C3983B3259412776121413A020CDF0EB7EF8B3AF
SHA-256:	B981284D826AE3290BD0D8E3BB08ADF20E371C5B19450773A3D5ADA08D2E5448
SHA-512:	673898247678820D1B549768ED4B6B310C7D9009B661EA23B148682CEDD54B942B0D32604EFF630D3D75AB9685AACF93B254FDA6F3F2F4988B6A4003BA342A95
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x16106db3,0x01d7aa75</date> <accdate>0x16106db3,0x01d7aa75</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>0x16106db3,0x01d7aa75</date><accdate>0 x16106db3,0x01d7aa75</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):	5.069738125199746
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nL3xpI3xuNnWimI002EtM3MHdNMNx0nL3xpI3xuNnWimI00ObxEtMb:2d6Nx0LxCxASZHKd6Nx0LxCxASZ7nb
MD5:	4A4E1121AD0509B020BDC73E5A77AEF1
SHA1:	3E9F297FAE1FC670F3DFECA7CD7D8BCA4521C9DB
SHA-256:	BB2F05D5AB3AB90BB2796190EA22816B1AE24F532856AE91C8B63B16ADC13088

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-512:	09F09CC9CFFB22B66668007ECD66BF173A04FAC3E7F2BB9BBDD4251F78BB12011E1BD4D55C6EBC306B3E5DE6AD813AE9150BB1C1B5CA716FC53908CA24DF2C38
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x16106db3,0x01d7aa75</date><accdate>0x16106db3,0x01d7aa75</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>0x16106db3,0x01d7aa75</date><accdate>0x16106db3,0x01d7aa75</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):	5.10242814127007
Encrypted:	false
SSDEEP:	12:TMHdNMNxxTxpwxuNnWimI002EtM3MHdNMNxxTxpwxuNnWimI00Ob6Kq5EtMb:2d6NxPmASZHKd6NxPmASZ7ob
MD5:	C7C1214FF676DFE25C7880C05D38AB0D
SHA1:	63EE487B9EB89C56465CF90D8ED1287416333DC5
SHA-256:	566ED94A038F17D0119DAFC7DCAEC3B64E4A9A77FFC39B4F8518C1CBA9A461F2
SHA-512:	68EC30C97EB2180710E5F68F38ACF32C0E437AAC51BDC2354D1831074B693F5DFF23F7F0D24CD5814F953EE5D05E84A914DA719009AF29FBF4D98AE329510E2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</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>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</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):	5.08129056484248
Encrypted:	false
SSDEEP:	12:TMHdNMNxcTxpwxuNnWimI002EtM3MHdNMNxcTxpwxuNnWimI00ObVEtMb:2d6NxUmASZHKd6NxUmASZ7Db
MD5:	04F02C66FCE99B2F51BAAF29D08B2BDF
SHA1:	1E3E91AD6D2776090C48C24B9685443EE7798983
SHA-256:	3353E3C348C2A42D888264E6C45D9D83BFB8B1C24C1CD6D9F0C48FECCE4397C5
SHA-512:	48E6EDB7452E9430F6F5CE1230423E03A78E578850CAA2B3C8053E168C5473E5084CA4DBA14C9C1136399B4344411158F6F243A2D39F39C385FF3642E07E1B6B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</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>0x1606e68c,0x01d7aa75</date><accdate>0x1606e68c,0x01d7aa75</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\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):	5.063287905117234
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnTxpwxuNnWimI002EtM3MHdNMNxfnTxpwxuNnWimI00Obe5EtMb:2d6Nx1mASZHKd6Nx1mASZ7ijb
MD5:	64771B2537EC2153FAAB9D30E2E5522F
SHA1:	0C37CF593256EF9BB8C364D24C82356C5B0C9AB4
SHA-256:	944DC31374764EE2B998C601C461DE827E1C33A643C876BFF5337036832B22B5
SHA-512:	1BEF769EB854F35C7F0B99DF9CD2EBB8E12CEAA2C02C9466B6809E6BE87CAA9AFFBC08E494C35AABE5172A010EC0874923F9A6D0853D692BA22EEE8B249C4CE2
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1606e68c,0x01d7aa75</date><a ccdate>0x1606e68c,0x01d7aa75</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>0x1606e68c,0x01d7aa75</date><a ccdate>0x1606e68c,0x01d7aa75</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.023129072160435
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGk4EX:u6tWu/6symC+PTCq5TcBUX4brE
MD5:	E0961C2817CD74E62E5D0CF795446B9D
SHA1:	FFB5BF8A2CE975E36F8057F27E26334CDB49731C
SHA-256:	DEB3B2285784A2FC589046029F568D65ACF2E9A1C2EEBB8D741BA6D0E3719BA8
SHA-512:	16F454D3F39D060103F9D593C53CAD003DD449047D57146C704ADA7A1F29BE192BF5392CE3D70015958184305 45CB4A2844697BDE33CA2AF45F56C49E2CD9A5
Malicious:	false
Reputation:	unknown
Preview:	E.h.t.t.p.s.:./.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .n_Ba....n_Ba....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
Preview:	wOFF.....A.....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOqRpw[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	16157
Entropy (8bit):	7.943312010785865
Encrypted:	false
SSDEEP:	384:N23tMYzfvY0Wzcxd/JfPynGRbjo/M4iBy62mGlyMG:N21DQpzwdJSw37Zd
MD5:	0813DF3E9B74E3A0A42DD1BE1D19F349
SHA1:	1FD727B125DB1102AFE25AA0E196F68EDD1576AD
SHA-256:	E38BC32CB72E0FCDB9D9B777111344679F3F34F969DE377591371A24A33ADA78
SHA-512:	C1763CE89175FE6FB77EAE5499FDBAA31CAA0153E7C79CDFCD234B8AA41969877E4FC9882FF684CE2771B2D605EFDC87DBAFEAFF9F0169AC3E6DAD94EE639 1F5
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.P+..$v).\R...dz..dz.`.#...(..... C....P...dz.`....dz....@. ..(.h..a@..-.&@..p...q7.,..p..X.-...P.@..W...d...oeurG.....S..n.....v..C... <r_.5T.....{'.^:e,2%.....B...7..t.~5K.Q...*O..`...Z.....kfe\..v...._Q]p....Z.wE`A.Z..Z.....!.h.g..b.....z..ua...oc^.....J.;.Q.....}....Q..E.:M.....S.^.$Rhvo.0}....!..w...-n.....Fr.(.d.. o.E*...M]..%1....-...P.....5,}.m-X.h.h..`.v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOqRpw[1].jpg	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOr330[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	13684
Entropy (8bit):	7.908063826482386
Encrypted:	false
SSDEEP:	384:NdXGvUtfq7nUVW/L7hw+Fxc46+orsf51IKjs:Nd2vKGUg/fS+3568fY
MD5:	D434391972BE55981A4B74BE9F11378B
SHA1:	92850CE6AC0CCD11A0EC47947CAE7DA63963949C
SHA-256:	186E4B7737CD9F450D80E4C883C44DBAC26C37DA99E364B359954F7833086097
SHA-512:	B28BEAEBC34C2A125A60E0448F42A5688A3037A93397F9E3AFE9DE2D58794AB5302CC89FFAB12C484C0D180B7BB3E186DE97B24A2B65C8F4DE01EA704486977 1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....=EJwW.ppveV.@...:....(.....P.P...,...x.."8q@.GJc...-...(.h..@...-..h.(.h.h.....Z.C....P..(.....>..F}..f....f.]'. ..c...@.. .Z.c.(..g....H...9..(..r....-.-.....B.@..b..(.....4.Z.J.Z.(.....J.Z.(..@.....Oz.....%fsW...*k...>n.7Nm.w.1$C@...%.....*.. .....-.8P..NR....P.@.....A@..h...4..@..(.....P...@..-.%..... (.h...>q.y.....[...WM.Y....23+.....,%.L..-.5.P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOrotA[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	23294
Entropy (8bit):	7.856757481287199
Encrypted:	false
SSDEEP:	384:IcyUFXHGzDaxY7zCoNundE+dJIGNnGx580R9etZ2t69TG0cxyuXlCY/PLi:I0dNrCuni+dJrnGxasELppG0Z8v/W
MD5:	C08ACB86DA254FA6E1CEC7C411E34DBF
SHA1:	C141670138D7BF6987A4E37F5BA0EBEF817B7DBF
SHA-256:	CFB7D84CB17F30BBA1D76F5FA0ADCD5B315DC7B5E57934691126BD6636CAFDD6
SHA-512:	CCA431D39AE209364E01B3F9F6FD21C29804D9CCFEE1E8D97AE892D7CA74A605653818390A2847004E912C810654627A644243B2D1042F79D031D647F1EDA547
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.t..m.5.!|.9n'oQG ..$...4..s...Ip..4.l'#..]..j.,.....B.Hf|....\.. .i....@.....J.R.. t..r...YW.i..l...E.....=.\..}(.XM.M..... ....ae.`Qt;.]...Af.Tt. p.dA.....\,D9nE....T9.4... .`U\,i.`P...x.12.1..5.7ZM\.#x..V..:.F....W.....~3.....v..o.-\.....=.....+.lr=....n.....y....zX."..(.....(.....Z.(.....(.....(...1.....4.*.(...P.I..(.....Q@..%...3@.~..P '".%.. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOrtsf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	21799
Entropy (8bit):	7.961437257211542
Encrypted:	false
SSDEEP:	384:NvkC32Xc9Axa7d2iYHWfPUg9Jn3hChYz8/6QPi3kOXv5A+yBTgsqN6HHnJ9pH1a:NvkCe47uHqXxChv9itv5AfshNwHnJ9pk
MD5:	A4A42035E692330B43A4FA876B5C657D
SHA1:	967ACD0FF1AD19E9CE48E72969B2D8F4094CC854
SHA-256:	A4118D303FE4ACCB655C772666C5F88C42E1238B6A1CE533535D9FD06102CA2C
SHA-512:	7F184DA8AD25C2E38AD357A4FCD63C0DE3F5B2F4A05D43E11F793773B93842D1F55D774EA2BB71A1CDE402E0A68A131B486AB34A134CD0F276B6DC98AFBFE 29
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAOrtsf[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..J.9.N.XM.<./pH...x..Ce)..#..`.=.e' .1....3B.&..(@....vqE.....$ .5i.c8... Yw.oQ.X...+..]..r...O.h.r.5._).Xn<T..#RR,.."ncZFW D.d..1.6.NCH...9.C'.H.#..`...%b...h,<Z.'...X.g.~.3M..Z\.>W..-K.j3yeI..+".%..`K.....*.....8*..`V4\.!Q.."^I...Z.$.D..i\.R.nqV..F.zi....j..T...^HK>.f.r..-..iX..J.i.1..Nw...h..\0....-..X.... ..T....T.y.c(]..P.8.R.-Z.].U-.-...j.N....|.5.....}.I..F. b.R.7ln..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
Reputation:	unknown
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:..J..;..G....Fl..1}.4..R.... .Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>.. T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.....[....8`.....;..@..B.....7.....<.....F.....6.....>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P .n...J.....Li..=.....F.....B.....:r....w..|.....`..[}.g...J.Ms..K.Ft....'..>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,....2.2..... ..3.`..9.(|.d.C .wH.(."D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.|Y....UU)gj...]..;x..(.."..$l.(.\.E.....4....y.....c...m. m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,I"...)...z.....>.OVObQ.....d?|.....F.QI$....qf.s....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S. ....&...T...?.X)${.....s.I."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v... .....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....|c(,.....I.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@....:..E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\a5ea21[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... .-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,..A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.tjS.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	23355
Entropy (8bit):	5.862969250051108
Encrypted:	false
SSDEEP:	384:x4LmOTY0iyRXOavY+UWECpK0UsfSvX2S5UG+jpqYC+w8g3rW9s1gtqY/N4GRMwSi:x4LmOc2pRM0UHfFivKWKXy
MD5:	59FFE3BAC035D18822C84504D7C94F28
SHA1:	977680FE72A8A78523CD0602D566A2BA42B809B7
SHA-256:	868B33AA4250ECED05BEB3286DD4D1DABEB053134B74DF096AC9DC907E252FCB
SHA-512:	AB753A18F00BBC8D07197A9F6BDD101EEA5C43E167B56DFD8806F8784B6BD31DF431A14184ACB21E89530F7B405EFDB1DD90C474D09434E065F4BC9B8ED3537
Malicious:	false
Reputation:	unknown
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_5771386aa5d069c904bbb6b8f93a1d20_40b77813-5d63-4d34-8df5-9050f14434a1-tuct83b6666_1631707366_1631707366_CIi3jgYQr4c_GJ3LgfXJzKTZJSABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_5771386aa5d069c904bbb6b8f93a1d20_40b77813-5d63-4d34-8df5-9050f14434a1-tuct83b6666_1631707366_1631707366_CIi3jgYQr4c_GJ3LgfXJzKTZJSABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"a4ddd93dd52947cd82240d0d2c0c03b6","RequestLevelBeaconUrls":[]}">..</script>....<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"gemini","e":true}" data-provider="gemini" data-ad-region="infopane" data-ad-index="2" data-viewability=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\de-ch[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\de-ch[1].htm	
Size (bytes):	429723
Entropy (8bit):	5.440982594619099
Encrypted:	false
SSDEEP:	3072:WfdJUcxx+xAkJ8dh5TPmJfP9DxdfO6VawmJpOM1EqMnOVfTBK0mnYabHo28c9Jxr:WfdTOx9swsMyETcdkJh
MD5:	0EAF55E223E3B7526741A3626124B6DD
SHA1:	9DE9DBB9573D78DE37EB2D07CCF075B6F1005971
SHA-256:	34A5D7C5E3F5D08D12928EBDC54A3086215F283183D98184E9A1A0B870251BD4
SHA-512:	30398F96ECF8E9C6D20B7480B9495839355F95933B00B0CD2F0E702FBC4B2B0664BC0BF6B21892473BC066672BDA5E537C9221DA89AD1FCE165455B31F5385C1
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20210910_239772 85;a:a4ddd93d-d529-47cd-8224-0d0d2c0c03b6;cn:6;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 6, sn: neurope-prod-hp, dt: 2021-09-02T18:53:22.1052839Z, bt: 2021-09-10T00:17:00.1970901Z};ddpi:1;dpio:,dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck:} ;xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-09-15 12:01:15Z;axd:;f:msnallexpusers,muidflt10cf,muidflt14cf,muidflt15cf,muidflt48cf,muidflt5 4cf,muidflt56cf,muidflt58cf,muidflt314cf,oneboxdhpcf,startedge1cf,complianceedge1cf,substancecrowdc,modvenduhrsc,pnehz3cf,article3cf,onetrustpoplive,1s-bing-new s,vebudumu04302020,bbh20200521msn,weather2cf,prg-1sw-quco3,prg-adspeek,1s-br30min,btrecrow1,1s-winauthservice,prg-wpo-hpolypc,prg-1sw-flyt-htpc,prg-1sw-halfwea,prg-1sw-ownformat,prg-brandupwhp,prg-cor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXll1pe/WNN0000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286 A9
Malicious:	false
Reputation:	unknown
Preview:	.....(...&... .....N...(..... ....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http___cdn.taboola.com_libtrc_static_thumbnails_560ad3dcc869b1dfc2bac1c99d35ac81[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, 207x311, frames 3
Category:	dropped
Size (bytes):	30700
Entropy (8bit):	7.98317065721395
Encrypted:	false
SSDEEP:	768:B8jiUbW95pmQWiB59NATcO7FaVapGfHmf2yJjK:B8ji9hLpQx11JjK
MD5:	2D3B14E350CB8481DABEC32ECFD0A4B0
SHA1:	5D1A1B48BF5D185CF41AAF1CB5D9733D5F4C3DA5
SHA-256:	6875CBE00B48173D9C98554DCDDB4B56389D794EABCC7C1A05C7F2A56BD325D6
SHA-512:	83B530444FDCC65B6EBE7DFBFC35A5F72C712B17549FBC66942F51216F5388E25265B4B0F1899A3AF728FC15136311D7BB87087C783E26F5DBA51475508C2744
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....&....&,%#%,5//5C?CWWu.....).....)$,$!$,$A3--3AK?<?K[QQ[rlr.....7.....6..... .....~:.<~.0.ed.>..}....y}.t..y..=i{.&...{s.9..c..w.....8qy..7..L.8K.[Nm.=.....(.....s.W.,..m.....w..C...._KK|._.... ..1.|.8..7eTc.gF.|.F.V....sz.C...../.....1..]...@.. Rm....Ey.&....3.Olm....hsm.[x.}dt.Zq..s}...'G....3o.G....E.0.....T...zN'.....m.....57..*..}<`.:.x....?1&H..Z.Js....TpH....L.[.....g..{S.;R@.{.R&....u...6..3.....d.Vm.l.%..V9....&...~.. .SoR....NP.....q..c.k1..V.s.Q..1..4.....ki:....ek.L..u.K.2.Tr1.).....3.UHW...M..3.s..'....Xg....`.:.j.%.,.yn3....&...j@tF.....e.Ido.....,*UD.89m6.!.).(Pe.r..S._.cs&.....d>'..o.J...L.: ..O.$.B.q9*...Eq..Si...V...i..TGi...p..9..m.A1..I...w/}J..J....-.M..CP.....5.cSiM.Sd....z.c..$d...H@...40$1*...H.PP.....O..s.c.}6....8...F...U4....)....I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_images_824258cd-2488-4e7c-b171-dad87f56f610_1000x600[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, 207x311, frames 3
Category:	dropped
Size (bytes):	16421
Entropy (8bit):	7.971960120905921
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_images_824258cd-2488-4e7c-b171-dad87f56f610_1000x600[1].jpg

SSDEEP:	384:ZvpoLBmJDIG2WNrEDZ96ASrYap4NuJYnRjiEuau+o:ZvikJR2mrm7LOp4NQYpiEuaro
MD5:	D2C20BF7706C810F628219875D8FD66E
SHA1:	9321BA0FB2923AD5198DBB22B69D37D59A182CCD
SHA-256:	1DB8BE2422C05B1D92BD856FB22DB5B3E89A1611662C2BAFADAC85418AEE4E7A
SHA-512:	5D2AB15C6C44D3AB0508DFE43398F2A6043EDE805C5E1B4AF5C18C0721F3B90F858E75DF87FD35360D9D040409005B35FA1296252DECE36F01E4FD6C68B19E8
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....+"..''+2*(*2<66<LHLdd.....+"..''+2*(*2<66<LHLdd.....7....''.....6..... .....A.XDX...&.....9.Aa_.....a...v+.h%.Tu.Ue..f.....|W$ui'...{}..{..!R.gV.18.{..3.....P..V.k.dz.(=....$.&..mI....s...8....s....)....].^..s].._.....!a.....$../.....^.<.....y.G.8m.._..4.j.. .i...T...j..Vj=N}}X.nK..._.u...w.....G+.%.u.92....\.H...P5..m.....z.5..g.p..u..%.U.)....*..X1..>PO..:.R...eIm.....Pysc6]..pc....D7}$...0;-X.T.l.z.Gc.J..2!s.&..v....FQ.....#.R..D..g/ .....?A.|=.....o...t].:..$*.0..mN.-..2-..''r.JD.\|..6....4..U...$.''.....R..l.F..hU.%.1q.0n..F...|8.....Bi....8@.jD.\DR.].l].fw.\4.V.f...[.....].Sd..z...h. (tL...%.v#.D.....5.....<..]-.W.)+... .}Qz{.$U.....Q.im9+v.. J.....:B...)...k..L...Y..a..)M5.R...vI.''.E.Y.[x.....KyT.[US.n.....4X.[...I....O7.oY.;K....Y1.&Z.oX.t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\medianet[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):	409467
Entropy (8bit):	5.484621894504284
Encrypted:	false
SSDEEP:	6144:z9CkYqP1vG2jnmuynGJ8nKM03VCuPbJErMrSl9Gmb:p1vFjKnGJ8KMGxT4M+cGmb
MD5:	4A11D6BB2186A35585656CBC86D485FD
SHA1:	F55ED91E75B527A5CC266249900FEA6E8A2ED3B2
SHA-256:	8651FE76AA50E3091D8745C4126C85205414745D2DB94149E3927E5B5C420702
SHA-512:	91CD0B945450781599B03F7716C8AAC451E16D9394CD2873D6C597F8D4A4F9F61E0D65D7C9F95DBD6E55C1B3063A8FE9C57D1157C55656998B6F3A5B02048BF
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript"> >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\nrrV75218[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	90611
Entropy (8bit):	5.421487324900678
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillux5Q3Yzudp9oXuvby3TdXPH6viqQDkjs2i:atiX0di3p8uhMfHgjg
MD5:	266B344BAA9D1D8D076BE1AB041F5FDC
SHA1:	21BCC171508AD8B2E05FB1BB944D820931B7A144
SHA-256:	6ABB63D55B62044D5439F604E3E0D5AF77F71E10535BB10949E71F743E692D8D
SHA-512:	218B417C1A887F3E6A6FE3F41BCE7234C096FC66E1A41850314252EAEF345EFE8289483BA4BA8CA6F5305AED8F88C09E0AA39ADB734ED26174A4DB09F62BE89 1
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProper ty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r) {if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine ("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isReso lved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n =g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otBannerSdk[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otBannerSdk[1].js	
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
Reputation:	unknown
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[])).next())})}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10055
Entropy (8bit):	5.443998211079296
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOYcpxrzZp50set1XDdVYnMLiKGWdrHpOlztlomlRIkr:4EamR7Ohxr9L0HBV+MLxGWdrVY+
MD5:	89A48656B1A403FD1B77C8C5682B2110
SHA1:	5314E9541F542965B237E654A40AF9BED66540EB
SHA-256:	C23483E07055D45989FE4A74C6C00E47210C1552D240360D19F2D86CA3128CCE
SHA-512:	1C7CC0B8348B6E4114C2833F7E099DD556C53DE6E7DFFBC7B50445EE0B4991AE7F1AE1D90DB24133BF45D39755DA154DF60FDDD28501D782692C379D9C3DAF9
Malicious:	false
Reputation:	unknown
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Reputation:	unknown
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\39ab3103-8560-4a55-bfc4-401f897cf6f2[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, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\39ab3103-8560-4a55-bfc4-401f897cf6f2[1].jpg	
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,,..".....Q.....!.1A."Qa q.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9. .n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o..._.....1..I...).(.l.4.....z[}.Z... .D2.y...o..}.=..+i.=U.....J$.(.IH0.-...uKSUm*P..T.5..H.6.....6k,8.E....".n.....pMk+..,q...n)GEUM..UUwO%O...)CJ&.P.2!!.....D.z...W...Q..r.t..6]... U.;m...^..:*.k.ZO9...#...q2 ....mTu..Ej....6.)Se.<.*.....U.@...K.g\D.../..S....~.3 ....hN.."..n...v.?E^,.R<-.Y^)...M.^a.O.R.D...;yo.~..x;u..H.....-.%.....].*.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.# .H.....\\|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AANcu7b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	35530
Entropy (8bit):	7.959645305810465
Encrypted:	false
SSDEEP:	768:ItvbJFJEtBLCleym4zx18nET0uH/BL9Wnc1o+4G9x3:ItvbJEGley1vL9fBL0ncK+4uF
MD5:	C3466D21DA49B7AADE86135CAF672867
SHA1:	31B0546925A77686B4CAA3B1B8DDB3094BC80774
SHA-256:	353E0A946A167793ACC429264BB2AB11546A2775FF7E454B9A26A145CF63435A
SHA-512:	EF48B1BCE8A44F35B7859C863BA73E18917ACD6C8AB513843093149EEA95AE21C07F2FDACD1DCEE0F1822483DD117DD38BB23D2AFEED92B6568BCE50AFA1E 4F9
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AANf6qa[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....bIDATx..?..a..?.3.w`.x.&..d..Q.L..LJ^.o...,....DR,.$.O.....r.ws..<.<.|..|..x..?....^..j..r...F..v<.....t.d2.^...x<b6....\.WT...L".`8.R..... .m.N'..`0H.T..vc...@.H$..+..~..j....N.....~.O.Z%..+..T*.r...#.....F2..X,.Z.h4..R)z..6.s:...l2...l....N>...dB6.%..i...)....q...^..n.K&..^..X,>'..dT)..v:.0D.Q.y>.#.u:.,...Z..r..../h..u....#'.v ....._&^....~..ol.#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOragN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	7.930203069199577
Encrypted:	false
SSDEEP:	192:QnTm4sn+thSKKRYqNAX1Lc+z3tjZdzQ72H5GAUaLIJYguwhr:0T+n+thOYqNeSIdjZdzwQgJjhr
MD5:	7217DEA32550ECA6EB4077F6FC7B22A2
SHA1:	E1006D9A77F02A26E3D7EEC75D42150414094911
SHA-256:	0749E2DE1F6A6CA5CB70FA36531E612AEA76381976FD9B280A370AFBD67DAFDC
SHA-512:	D2B1C7609BE3DB5CA8D3BB7DB8D8D5390FFE952F36E7E1A0C00BF02FD57B7C41510BCD8AC4D108612F37536FEFE9AACDC6D9ADD9F869462267B575B5B61D7C0
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...zg.8P"ko.....a.4k7.....?Z.$.;K....2f...?J.Q...Z%.....|...ZEjK9mj}.....s..&....06.l0q.\..OS..|..&kSD:nEd.E#...T....H."h.... P....U.U.?).g/..4....i0,..k)...7d.....}-.h..W.S+.R9.Ka&...[.g."7...@..x..o.Q...i5#.....i.i4.kP.f..E.r...G.d....._.....j..#.^5M.v$V...~.TE3.....!Xq@.w...e.([.RCc.%.....N=Mz.tB...`.% SA,.._b.....5.V....`.;?.>...&j...2.E...6.#.A.....&E.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOrf3O[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	43025
Entropy (8bit):	7.963921947978424
Encrypted:	false
SSDEEP:	768:l0d8zEw2R15YYrB8gyKn7EdAULnQ4AmNRk0rTNhZi858NOb1EQ+t+:l06enL18/Kn7MXLnQ4HWNf+
MD5:	F31C25CD109029BB9B81573238168754
SHA1:	E5720FBAE52D77E9322DFE546F6D2871241B4661
SHA-256:	47DB9857E31B2F2C07624CAADCF571E5511D76203DE517A6B006CABEB8322B56
SHA-512:	94BCC1E30747A3D99C830E30016E1628033690C53FC7FE78436B201AF8199428A094473CDCCC3C120C456CEED1BDE6C8EC21297A12477257A83C56299E8D6E1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....?.k.x8....W[...~".x..)b.$]j3....x..*.!..%...:....+'.....:>.0....^..?./.H>...b08Q....a..D.....Z,...W.V...Y....c.H...(.{pO...7...(..l ..i..%$.5m..C...{..A.....-v...@..._...^.q..7{.....+w:.f'b....EMA..a.....ECC....$...n...%F.....C...l\.....\p2.Qs.T.q.k..Z..P....x...B.m.cU.+.A!.D..P...=...../.....y....G~cH."..".....4S LL.+....M0.Y..A.M.3.M.H?...!V.5Lfm..'R#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOrhGb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	1951
Entropy (8bit):	7.753267922823104
Encrypted:	false
SSDEEP:	48:QfAuETAylFAlfRj8Um4qGLB8ITO7p6Xhg9yv:Qf7EpA9R4UmxGLyMNsyv
MD5:	431172B05E145BE51D798EF92AE95D6D
SHA1:	6EE53B78DF59C6B20A79BC848019F1E756C7D666
SHA-256:	50B388CB54F3CA5FBDBCEE0E69933FEE8C96D9D383E0BFA9B87144F18E9011FF
SHA-512:	119767CFE91D652B7AAEC3E2CDA380FE5E7B1149DDC1B60494170325A985D066FD29400504008108A54F532F045FFA5FF5EB30B4CC29D8BB5387A6716FECC0A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..sLF.....=~O.P2.}.....(Uy.@. .E0-..J.H\F .....Ni.....)..:...R.#A-.h.....C..3.Q...]f..._O..\..S.e\..Z....Qp%..,..V...*.O$.X.<%a. .oS....B..)..9..h_.,..%...p...{.a..s....Xd.[.....Z=.Sr.).....DL.....pk)D.).g.S.;....,-.....a....6....X.diuH...).W'n;.jODTRl.....Z..1.~{....+_.i..Y\....k.6aV)..A,..2.c.....o.[.M'..E.q..1..C.5`. .....M..[.....0...`.(...e..R{;l...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOrhGb[1].jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOrpxv[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2180
Entropy (8bit):	7.790586839304781
Encrypted:	false
SSDEEP:	48:QfAuETAzwj//SR86t+MbQCa8vRxXvTsAhubifq:Qf7E7yQCaknsMub4q
MD5:	79F8FDEE9B97ADB6CEE72CCB3D5222B9
SHA1:	5D8A268A6F15D9599550CC33C56920020B2F4245
SHA-256:	D29B2E0A369EC8A448A389CFC263069554A7E312F7CFA74F4A438504F14614BF
SHA-512:	78EF146F3C40A1B0E8586B9AF4318FCE6D2DF862D5204B9BAAFF348D0A4BEB21AF2582A9EBF45D76CE1F19DDEDE3A53B540ED118A8B30CC440B9B8C70C163D2A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..\P..L@..&).b....h..|.7....i\...C.=h.....1@. .....R..h.....p.S...].k..x...l..!.}..|.~....U.r.M9k...6...z..f.1{.>%...15...6.c.}.iNm..8$...ekc1...P.b..P..<.sN.7f).....QK..A.N1rvBn...D..3.luQ...^....n....j]..jS.....e^...>.%...S.".Z.lu7.....F....2...VZ.o.K....e..LH..J.1....LA..b.R.m4.L...p8.@0T,q@.h.....^.t.H\.....V..(.h.D..(.D...%[.}G....HJ..!i$..YE<.....ejr.[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAOrqro[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	15546
Entropy (8bit):	7.961712420653704
Encrypted:	false
SSDEEP:	384:0P9kIQI0tAy5NfCM8G4gRvT/Pe9pOADYftwaeIzyfNU/LzHppG:0P9GIEBfOgVSzOAcwapzyCjjppG
MD5:	82A0AB042F8820EFBCA69F387AB73415
SHA1:	D79491E34BBA5DE65EF3988ED1F4D04FA33B8A87
SHA-256:	15925D7C7CDC2DB2AEA17B2769FDA6B8C3B2A8132E104EBD70C7010318D6BA1F
SHA-512:	C2AED5B17ED21494AF5907B8487CBDF18185D6B998DCD7F24B9C948A9A8B28C10D44C82F35C3615B63EC63DE4518CC7D28323F1DD2F5E4640B2838F1E517FB2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..8.RPG....5....5.E.#... @?.....+....c.Z.CZ.4w.....ym...).....;.h.V...#q...S...v..|Z....9..Pv...*Q..g..3z.G;.m,"".\.#..v.....i..$.r<Q.o.bc.....5...8..p]X9.....RsBvzw...\....S..z..W...]...D@I..nh\..5|.]E.....0.Bs..R+.(..lb..g(.z..k...-:...cf....C]....R.c;.....A.pRL.>.1.....a..oa.0.(%G..}.9-P#5....>..2.?:.OD.C>.{bE.....uS.B.u.s4...\.w$.d.aS..RQ..o.3N...b..g.n..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1aXBV1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1aXBV1[1].png	
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...}..c.....j...2..Y.I....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7.....0.[...5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.';... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F..*.a..lj...t\.W.....&.l|?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..|]..c..\.'...l.....u8.....Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.....S.....S..)N..D;.....<.....7#..X2.ws.....H.vF'...,$l..R4.O/.~..j.'&..6.....!.D.m..].G.....W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA06
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#l.....x\|...\...&.T6..~.....Mr.d.....K..&..}.m.c....`.`....AAA...,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u.....Ic....,7..(..&...t.Ka.]..,.T..g..".'...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%".....[.=a.....X..j..<725.C..@.\. ..`.._....'...=....+.Sz.{.....JK.A...C|{.|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..}a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1kvzy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1100
Entropy (8bit):	7.749452105424938
Encrypted:	false
SSDEEP:	12:6v/7eZ3IqhrinW+y2UXaxTaJgfcoG7QKJ7OZfhL3cp1pW2krS7BiArfss7P7UIQb:jVT2aCTjG8MOZR372/7iU7UlylHdLN
MD5:	C6E13630360E0B6D880AFDF3CD2A2204
SHA1:	63DCA80F76834F5A3FBE79F661678375239F72A4
SHA-256:	49767874BCF0F0648266F3018B5CCE3CA539B85778E5395D1212ACB114287D65
SHA-512:	CB8F7629DA131226146B12119C06A846A2EC9E9D069711711AC50CD7F31E321144E39270E82EA693E2FE9BFD1634841BF450173807AB6607794E2AF0EBE832C8
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....IDATx..}H.u....m..rR>..9#--o.....[E1..kWB.#.],\F.8X.....\.&.....x.....y.b..p...z}~y..9....^..|.>....{l.?.;.....:.Uw.|...e.(.....r..Wc7Zq...F....N.O.}.n...^X..*$.q...&.%.....X....9d{.>...)..8..A...}.x#....K... z~$...4Y...<....)`..p....qr<arhwa.zY.Yq..$.<.....H...~...H\|..G...@\|./.8G.L..M...U..I...]..r(.s.."f..l...Q..b.x..MYd.D^.mg.G .H.....=Ot.v.D._..6.[o.7*L.....d./B)l....d.....u.....mqB.J.....4(R.....".dSj.....{.gB.<...gdT....u~.?`.X.&&&N...\|.R..0..O.yV~./..; .\.\X[P....[...1y+++M...J../.+...}>_mooo...~ohh....`l......R..."...`.....8...aeP...oL..f~n..m0..tY2.N.rrrT]].JKKk`"...Kw.i.....\|.....['<...bHM).....%;..=..D.s.....CN.....Y.,..l.<...s$...v.=5....N..E.YYYjzzZ..A...+]ohIII..L?<<|....}&q...].vM..?. ...+....m.....}6....|i.e+..Vf.....V.@...3.d.....cRv.f...E%G..Xvv.....ru...~..j.....\..f.....*.|m,//O..B....D...zUU....Z.kfccc*..."..V__...+**R.B..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\de-ch[1].json	
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\http___cdn.taboola.com_libtrc_static_thumbnails_e17134d780918219c201cb1db8da2d3f[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, 207x311, frames 3
Category:	dropped
Size (bytes):	16162
Entropy (8bit):	7.964456173223213
Encrypted:	false
SSDEEP:	384:/d1ktFHrTqw7+KKF326bGOKLNdPqzj19+giC4qZi8C:/d2LmNF3daOkNEzziC4gip
MD5:	E4216C30303B0FD3ECBE5C71E9ED5127
SHA1:	70D46FA259EA8E8AC4B3C3EF316BB9768F0CC762
SHA-256:	D1895A9D1AC7CEDA7D5CB215475785DB696CC94EDF152E0F2799140020AB9D51
SHA-512:	2233B76258AC908F64008D1B75E0AA39E510CE3CDA0259961BF082B01D4822E073D7AE5ABA12BBA3F167C4C5DE717922F247839247257AE8F9E9AF2F1A4157FC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....$.....$6"(""("60:/,/:0VD<<DVdTOTdylly.....7.....4.....L.@.@...$..6...C`...IbD...a.04.....LD....@.m.0.@..C@.m...=.....! .HBi.!....X....!.[..''...00 J...H.H%.M.....".i.!..m.&.B.;.HH.H.....@....6$.m$h.Q4..nX.....%6.....A.l.".B`.h..,....@HhhCcm....&.m5..RXHN.-...M [b.....4..C m.....`...9f6DT...n~.].n.8.....hhBA... ..S.O. :.U.e;..|.....C.q..@...6...@..6....U..n1..;...u..4.....B.....&.(...m1.RyYRB..K.....-.\`..l5h.m....4.I..L..0.....[..K..7..qo.L.j.H..>.....$m.....@@.D...1.US..b^f[a.t&.....5.G.....@.....3.wi.....w..4..Gs..''...d.7B:l'....h|>j.f;..J...os.....p.4,..g.]..H.`.dp.i.N8..e....U...Y...D...l.OZGV..+.h....i.(....h*.m8.X2(<....C..M.D.ok.Z\FTMj%C.x.....Lm.....T.@t.N..Q...Qe.5.....Y.oN.q...f...]<m.Am#.* ..q.....x.,].....w....26

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\nrrV75218[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	90611
Entropy (8bit):	5.421487324900678
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillux5Q3Yzudp9oXuvby3TdXPH6viqQDkjs2i:atiX0di3p8uhMfHgjg
MD5:	266B344BAA9D1D8D076BE1AB041F5FDC
SHA1:	21BCC171508AD8B2E05FB1BB944D820931B7A144
SHA-256:	6ABB63D55B62044D5439F604E3E0D5AF77F71E10535BB10949E71F743E692D8D
SHA-512:	218B417C1A887F3E6A6FE3F41BCE7234C096FC66E1A41850314252EAEF345EFE8289483BA4BA8CA6F5305AED8F88C09E0AA39ADB734ED26174A4DB09F62BE891
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}})();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12282
Entropy (8bit):	5.246783630735545
Encrypted:	false
SSDEEP:	192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYLp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAk
MD5:	A7049025D23AEC458F406F190D31D68C
SHA1:	450BC57E9C44FB45AD7DC826EB523E85B9E05944
SHA-256:	101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5
SHA-512:	EFBEFAF0D02828F7DBD070317BFDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A96
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\otFlat[1].json	
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCIgcm9sZT0iZGlhbG9nIiBhcml hLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpdiBjbGFzcz0ib3Qtc2RrLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZ D0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyVpZ2h0IG90LXNkay1jb2x1bW5zIj48YXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI+VGl0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0b GU8L3A+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRhaW5lciI+PGgzIGNsYXNzPSJvdC1kcGQtdGl0bGUiPldlIGNvbGxlY3QgZGF0YSBpbiBvcmRlciB0byBwcm92aWRlOjw vaDM+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRlbnQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AAOplZ0[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB14hq0P[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..h.h.....(.h.....(.h.....Z.(.....(.h.....TNY...W....q@..~..<..h.....dG.@.....F....L.@%}.....-K.F.9...c..O.7X9u,%.k.4..4..c. <p"...cp.-...U.J.n2..9.b.d.SphR.\V.5Q-./.LV.6...HM.V.d^E...F.q.*+7..a.m..VOA..qR.X.rx5&.(..Q..P.R..x..WM-.?.....V..GTi.(.(.....(.....J.(.....J.(.....Z.(.....Z.(.....Z.(..... (.h.....i..H.@...;..Y...q...0.<e+.B...[.v..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB1cEP3G[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1103
Entropy (8bit):	7.759165506388973
Encrypted:	false
SSDEEP:	24:sWl+1qOC+JJAmrPGUDiRNO20LMDLspJq9a+VXKJL3fxYSIP:sWYjJJ3rPFWToEspJq9DaxWSA
MD5:	18851868AB0A4685C26E2D4C2491B580
SHA1:	0B61A83E40981F65E8317F5C4A5C5087634B465F
SHA-256:	C7F0A19554EC6EA6E3C9BD09F3C662C78DC1BF501EBB47287DED74D82AFD1F72
SHA-512:	BDBAD03B8BCA28DC14D4FF34AB8EA6AD31D191FF7F88F985844D0F24525B363CF1D0D264AF78B202C82C3E26323A0F9A6C7ED1C2AE61380A613FF41854F2E67
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK..[h\E...3..l.....k....AZ->..}S./.J..5 (H..A.'E...Q.....A..$.}...(V..B.4..f...I...l"...;{...~...3#.?.<..%.} {.....=..1.)Mc_..=V..7...7..=...q=.%&S.S.i,..]).....)..N...Xn.U.i.67.h.i.1I>.....}.e.0A.4{Di."E...P.....w.....|.O.~>..=.n[G..../...+.....8.....2.....9.!.....].s6d.....r.....D:A...M...9E..`.,I. .Q..],k.e..r`.l..`..2...[.e<.....|m.j...,~...0g....<H..6.....|..zr.x.3...KKs..(.j..aW....\.X...O.....?v...."EH...i.Y..1..tf~....&..I.()p7.E..^.<..@.f'..|.[.....{.T_?....H.....v....awK.k..I{9..1A., ...%.!...nW[f.AQf.....d2k{7..&i.....o.....0...=.n.\X....Lv.....;g^.eC...[*).....#..M..i..mv.K.....Y"Y.^..JA..E).c...=m.7,.<9..0-..AE..b.....D*.;...Noh]JTd.. .....pD..7..O.. .+...B..mD!.....(..a.Ej..&F.+...M]..8..>b..FW,....7....d...z.....6O).8....j.....T...Xk.L..ha..{.....KT.yZ....P)w.P....lp.../.....=....kg.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	482
Entropy (8bit):	7.256101581196474
Encrypted:	false
SSDEEP:	12:6v/78/kFLsiHAnE3oWxYZOjNO/wpc433jHgbc:zLeO/wc433Cc
MD5:	307888C0F03ED874ED5C1D0988888311
SHA1:	D6FB271D70665455A0928A93D2ABD9D9C0F4E309
SHA-256:	D59C8ADBE1776B26EB3A85630198D841F1A1B813D02A6D458AF19E9AAD07B29F
SHA-512:	6856C3AA0849E585954C3C30B4C9C992493F4E28E41D247C061264F1D1363C9D48DB2B9FA1319EA77204F55ADBD383EFEE7CF1DA97D5CBEAC27EC3EF36DEF8E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....wIDAT8O.RKN.0.}v\....U....-.. .....8..{$...z..@.....+.....K...%)...I.....C4.../XD].Y..:.w.....B9..7..Y.. (.m.*3. .!..p..,.c.>.\<H.0.*...,w:.F..m...8c,.^.....E.....S...G.%.y.b....Ab.V.-.}.=..."m.O..!...q.....]N.)..w..\..v^.^...u...k..0.....R.....c!.N...DN`)x..:.."*Brg.0avY.>.h...C.S...Fqv._.].... ..E.h.\|Wg..l.....@.$.Z.]....i8.$).t..y.W..H..H.W.8..B...'.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	458
Entropy (8bit):	7.172312008412332
Encrypted:	false
SSDEEP:	12:6v/78/kFj13TC93wFdwrWZdLCUYzn9dct8CZsWE0oR0Y8/9ki:u138apdLXqxCS7D2Y+
MD5:	A4F438CAD14E0E2CA9EEC23174BBD16A
SHA1:	41FC65053363E0EEE16DD286C60BEDE6698D96B3
SHA-256:	9D9BCADE7A7F486C0C652C0632F9846FCFD3CC64FEF87E5C4412C677C854E389
SHA-512:	FD41BCD1A462A64E40EEE58D2ED85650CE9119B2BB174C3F8E9DA67D4A349B504E32C449C4E44E2B50E4BEB8B650E6956184A9E9CD09B0FA5EA2778292B01EA5
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J...._IDAT8O.RMJ.@...&.....B%PJ.-..... ...7..P..P....JhA..*$Mf..j.*n.*~.y...}...:...b...b.H<.)...f.U...f s`.rL....}.v.B..d.15..\T.*.Z_..'.}..rc....(...9V.&.....|.qd...8.j..... J...^..q.6..KV7Bg.2@).S.l#R.eE.. ..:_.....l.....FR.....r...y...eIC.....D.c.....0.0..Y..h....t....k.b..y^..1a.D..|...#.ldra.n .0.....:@.C.Z..P....@...*.....z.....p....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc.....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+..,]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q...._...h...L.....X.{i... {.. &.w.:.....$.W.....W...''..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u.....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\checksync[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):	21628
Entropy (8bit):	5.304876309171232
Encrypted:	false
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:I86qhbS2RpF3OsBQWwY4RXrqt
MD5:	15AB6EFED5037151C230824221C3D017
SHA1:	14032EF23019158703CBBE4EBCD42CCAEF841F27
SHA-256:	0840E026E01293ABCC101F7C4C431CCA529BABBB8F6D83D897DF2047F2E19C67
SHA-512:	29710DABF33F7392D6557685BBC70F4998702C93E9CB1E8836FC3E6306C3ABC44BFA6C53C411E61402A43B418E1447879CCADD69AB61507A9F8C49180DD197E
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","co okie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x", "ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got" ,"mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\checksync[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):	21628
Entropy (8bit):	5.304876309171232
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\checksync[2].htm	
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:I86qhbS2RpF3OsBQWwY4RXrqt
MD5:	15AB6EFED5037151C230824221C3D017
SHA1:	14032EF23019158703CBBE4EBCD42CCAEF841F27
SHA-256:	0840E026E01293ABCC101F7C4C431CCA529BABBB8F6D83D897DF2047F2E19C67
SHA-512:	29710DABF33F7392D6557685BBC70F4998702C93E9CB1E8836FC3E6306C3ABC44BFA6C53C411E61402A43B418E1447879CCADD69AB61507A9F8C49180DD197E
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21628
Entropy (8bit):	5.304876309171232
Encrypted:	false
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:I86qhbS2RpF3OsBQWwY4RXrqt
MD5:	15AB6EFED5037151C230824221C3D017
SHA1:	14032EF23019158703CBBE4EBCD42CCAEF841F27
SHA-256:	0840E026E01293ABCC101F7C4C431CCA529BABBB8F6D83D897DF2047F2E19C67
SHA-512:	29710DABF33F7392D6557685BBC70F4998702C93E9CB1E8836FC3E6306C3ABC44BFA6C53C411E61402A43B418E1447879CCADD69AB61507A9F8C49180DD197E
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21628
Entropy (8bit):	5.304876309171232
Encrypted:	false
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:I86qhbS2RpF3OsBQWwY4RXrqt
MD5:	15AB6EFED5037151C230824221C3D017
SHA1:	14032EF23019158703CBBE4EBCD42CCAEF841F27
SHA-256:	0840E026E01293ABCC101F7C4C431CCA529BABBB8F6D83D897DF2047F2E19C67
SHA-512:	29710DABF33F7392D6557685BBC70F4998702C93E9CB1E8836FC3E6306C3ABC44BFA6C53C411E61402A43B418E1447879CCADD69AB61507A9F8C49180DD197E
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\e151e5[1].gif	
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\http___cdn.taboola.com_libtrc_static_thumbnails_5ac3b539d1cfda83dbe324033737805f[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, 207x311, frames 3
Category:	dropped
Size (bytes):	16943
Entropy (8bit):	7.9720190729044536
Encrypted:	false
SSDEEP:	384:/89mGVEdtzcy+jjKmB8Ww+d+AueNauqH1xbO6lSIgVrE:/8HVitzNSPB8W0NevwrbxrkrE
MD5:	886165EBBB25E2FD2D9AB2C4F3146762
SHA1:	D4B4D36486317A7F57BD12B7574A32BD4EB7CD06
SHA-256:	AA7B58D964164238A5A1B7BB72B54025FD48DA2AB9917FE0AEA10818C9CFDAAD
SHA-512:	784632187B7E42EFEABDAC4AB66062181BA8254E537E7AE2D382919565FBA8AD33346FB48EE2FE59AB6FFFC45D113D43723DBD6F229938B12A3F801789D5D7C
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....3.....D.D.H..)-.Rf+.....Y^M...@..w.4R...!.7.L...c...^p.o._#....).C.....YY.'3.....'D./..$l..'S..c.KK.;O.$..:m.?S..W"....C.W.d..i....l.,.v|>..$.+.....u.N~F\..v.....4..95.5.&m:kk.Q.%.....4.`r.....t.(.[&...-.q..V..y..d.ZiKbDO*a..t.2.Z1J$.,.|....!.S.J.....q.'"L.*....".I.Ue..'M.\Ekv.4.... .AH.Q.;0[-.h.....&..!P.J...2J:.....Q.S..#o.;h.g..2l.1./...~t.....Q.v.....Z...U.I|.R4.<.e..G.Lb./.Gg.'...-.P.....:8.....}..D`..x.t..RKu..G.....I.....$..|..|....A.I..{D.....J.....o....lZ....gf#....Z i"%...S..^.+....<..i.`..#....uf.1.8c-.D.=(. ..M..XRd.C%o..Q;0.@...Qr..u5I...^...j+.<.S....".....3...X.....7...Q#.,. ..L....{.Hy6k".pU.;+`..RA.`l4.....8..jb.6.D....2..-.z..i$vH...g....t1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
Reputation:	unknown
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2481
Malicious:	false
Reputation:	unknown
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16853
Entropy (8bit):	5.393243893610489
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF822
Malicious:	false
Reputation:	unknown
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
Reputation:	unknown
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return I(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\1599143076228-3140[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	195266
Entropy (8bit):	7.982741634919224
Encrypted:	false
SSDEEP:	3072:aThiNH8X9KhY0Uo2M5ChK4y69Ki+45ds9Z+EqtqiFYt1fPdLd4EHMWqT8Yg1Xzw0:aztz0UV71+gq9Z+zqiFGtdLd4EHMDT85
MD5:	2343B47650F79F6C20CEA00191EE349F
SHA1:	AB869D68DF372214A5B5EB8D1B3BE909E6BEADA5
SHA-256:	67B8F7F0067BEE8B4F358D0A471691BEA73B9335139E86CFA6000784C065BB09
SHA-512:	B35210865F995A1B1210279E2514B5ACFFA4706DC3CFAA2C771B882461711CD9D4CE22997DBA7BCC0C1EB109136F039A909FD40729595B2219FE58F0F08C65E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....p.n.....K.....!..1A."Qa..q#2.....B.....$3Rb.%Cr.4S.&'Ds.....D.....!1..AQaq.."....2.....#BR.3br$.C.4S...%D.....?..._.i...e'k.....zzn1....>...os.~.'.....Zx.}..S..@4..{.)..N..1..%..EY...?...IJr(...fw..S..-;!.....mV..okn/.S..A.:...<.n'.u.....D7.....-u.7.[..kX..cr.,_.....t.)..8.z_..`b~.....l66...~....l2.....u...<.....Z..6...z.:)...:.m7..i..._..9...>q^.`...V.....L....T[.sk..M...5...AC....U)A]..[....g...m...~....m...@....30..._.u.?x..'|G...>7BG[.o...>_..f#.[X$\t.bw.P.0..X.Z.[...9U....3..l....._.....~."!i!B.q..}..<...T.....@}...9..0D.....V-.n.= ....iM.....}...3...4.(...g...^.YfN.4.#.{}o...l.&....6....p.].Fw.....r..<...m*.....1S..r....p..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\2d-0e97d4-185735b[1].css	
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
Malicious:	false
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	396806
Entropy (8bit):	5.3241178464742696
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/jgyYZw44KfhmnidDWPqIjHSjaXCr1BgxO0DkV4FcjtIuNK:CW/VonidDWPqIjHdC16tbcjut
MD5:	FA58CDF103D2BBB8B254AA62DE24EAAE
SHA1:	FB123CA180B3D653CBC2C9292024441A76954038
SHA-256:	D0A148461AC2EDEA975A772CCA5B536C06202117BBF55FB3AAE2477575AD5628
SHA-512:	7EB196F080B1E33E9B0575F13E64DA00718A42EEF8F9B225D94D4F7249B1802CE8F3CD5C2DC187DFCBA316B8C120C8B46D428764DF9176D4EF3C1D713FB3FEB
Malicious:	false
Reputation:	unknown
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	4.796538193381466
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAmHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AyQshjUjVjx4
MD5:	8FCB3F61085635194CE5A73516DE39F9
SHA1:	4EF7BB8362EE512BD497C48C168085738EE010C3
SHA-256:	CEC95B7811CBF927FD338529A08F6B1BBF12F5B78459D07D15DE92C60C12DD64
SHA-512:	DB60AF665E02724F527C6781396105C456E56D23691A64F57BDD452C0568EF43DE36F63D8B18702A5C5A6FA29C9C16CD6ADEBB74E28BA94AF7291EAC3095861
Malicious:	false
Reputation:	unknown
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5a9f9a2b-8e64-4961-b3e5-fd11cf345b01[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, baseline, precision 8, 300x300, frames 3
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5a9f9a2b-8e64-4961-b3e5-fd11cf345b01[1].jpg	
Size (bytes):	54757
Entropy (8bit):	7.955842263789909
Encrypted:	false
SSDEEP:	1536:GwQKsNsbvSZIugo5Ndq6StBsbhHozPbovNW2J1:GwQ9ybqZIboo6VH4Uvw2J1
MD5:	FC1D5C2BBD7332A2EBFF6AC249421119
SHA1:	B44419370D698680DFBA2AD2A73680B6C1128689
SHA-256:	9ACF5AB02B6E483F1B3C6B0A29E6446A2ED2740A2EA86C711BAD80D9133E8C92
SHA-512:	8EAA8E473BB020A485D4C7C881C61725B320F622C7835A46335EB392DB9FBD02A67405630387F472DB6254ADA0F2CBB0D79A280271FA78E4B52A1C725BE7B8B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,.,.."..G.....!..1A.."Q.a q.2....#....3BR....$b..C4r..'S5.....@.....!...1."AQ.aq..2.....#BR...3b...r$Cc.....?....d....8.....].b}.. ..xO..Ps.....R....O|.....0z.2.G.>X?Q.:r:.t' >...hP.#....N..8.g.|w..o.pj.D.....?O....8..y....o..5.....2..u'..:.....c...`....w.....Q..9=...<....{..`1.l...NU.|....j&o.....s.....c...3..A)K.N...2H=.;...'....O.`.....1..V.U ..bA.f363n.I.B\...(|..A.. .V..J.}Y.....=.[\W..f...W..cenR..=..=.wB...1...}.I...._..p...+.z1VRR.G.g....G....@..#.;.....n.t.!....j.A...z..8=[.....b.A ..98.~..S...<...*."JE.h...~C.....v.:....`x.3.....<c!..\')8..F.s..?...@ .5.....v.....vU.Vi.....I.....g... .I....!AN....|..?..Rts..m!..O..F.$.S..{t'.;...4.G.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AA3e6zI[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	357
Entropy (8bit):	6.88912414461523
Encrypted:	false
SSDEEP:	6:6v/lhPkR/lNisu8luvaWYLlqJJnJq2bTzmNs9SlAT5fqSB6rlgp:6v/78/lNlu8YKq3JJbGNs9SaT5xB6Y
MD5:	272AC060E600BD15C7FA44064B5C150F
SHA1:	27C267507F3A73AAD9E3CA593610633A7E8AF773
SHA-256:	578548F464A640FC0D8C483A1FDC9399436C27391B17572484416492A5485009
SHA-512:	B8CF6622A690DB0A81FE08AE052EC945FD3A1439C3F0A2B85DB113D33EAFD4F08F8B8C9E2C7B69ED623BE24B7AB4290D38FA2B945666DF762D6E672068ED2F B9
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....~.....IDAT8O....0...,@CKCKGI..l.....l@M..,..8<#..$)."..gK.'Y.7q@?p..k....."J...}.y.....(...(.m.a...(.,..".2...|..g.!P.h....*8.s.>1...@U.`..{`..TUueo...&o..a...4e..[..).i....R..`.....7.....Tv..q...!.7N..U`FP.='.(.qL..}.E.y..1>...H..a.BL.Y:x....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOpzgh[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	7.842604630697056
Encrypted:	false
SSDEEP:	48:QfAuETAKEqN1qjJMtlNDSqBEXENXSUt65ZQ1Oobqz3SxaEXUl:Qf7EgjJMtbmXENXxc5616z3waEEl
MD5:	00313D1599DB1FB50A343952BFF63434
SHA1:	626800ADAC1C4C401B3AF82D9E64315B15A73C31
SHA-256:	B4CFBDDD575224F174E7565F485D0F5635AE717F810E8EF2257721EAA89DDD0A
SHA-512:	F9E5D21AFB0AF54C999DA5FE5CA15407ECD06D2F716C919CFB880ACB088B048D317F4AE836189114A04FC56E1021C0DBF46435D4F3E3413D6597DF394525B8C
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.1.O.....:.q..n1..l...N...&-...$.....M.r9..&H.NGJh.V.....2?>-..g>..t.....61.}).:..Fn.1..G=...d:..]...7.B...XH...r}...!..+>..4.<.&...s..ic..# (b.EsX.RI..p.....ZL.$..-..Wl_1...\|...I.F.s..YTz(.4(..#y..F.f9$.T...."@OU?.W!...7J.S?j_]6S.f.I....Ib.....S..o'b...b|.....k....*Rq.].....iP9..Hw...=}.....LW-4e.d.#.+...)\..# .....r....pQ.E.s .R.....l...S..Z...Y.E..0.-..V8..A...x:3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOrFGY[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	16251
Entropy (8bit):	7.957137655582027
Encrypted:	false
SSDEEP:	192:QtIafn+S5AnU2Y+y1660TRs8eTsMo3ZjbPDmg0/N4Y8hQA4f5N8jldW/Vlc7BSqi:+Iaf+hQp0THRx3gg0/N4ef5GjlElc7cP
MD5:	6EBB3ACCCFB290E0337E267C575037CE
SHA1:	EFF867D1812AFE049DED89F12E357B8CB786DB5A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOrFGY[1].jpg	
SHA-256:	4D3737C9ED710A18C627DAE81380E11EF46BB8675EB30550A5F69EC64F400D54
SHA-512:	A20D8E0A2751A3CF875993BFD20740E7212483D536DD49E318BD0E1CCFCBFFE2AD0AF2D5E1A323B7FEBD96CAB9D4303C70C1AE3269A89FD157D9E7451A5751 23
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..b.....QUbP.....u.)..Ti(Z).....XeA....x..2.S..N...i4..e.[.-"m./....}...t..(..^.k...Gs..u.#...x..J....mh.X..w.d.l/...]WVF.s.\|p._.N...1...(y .o.Q..$\...o.....;R...k..M.=.8.}+8.Q.J`:f.....T..O.XW'...d)j.3..;T.....R.....i...sQ..n5....@u..~.....lU.n .R(c...I.N...7..[/.5...../c@...V1L..H(,Z@-...(.....q.....].)n...-..$lQbw|.|...E .".%.V,.I.....|_.{.s....qU..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOroVg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	46827
Entropy (8bit):	7.964431896614474
Encrypted:	false
SSDEEP:	768:IQ/5AUaXm+CpwGsixaAW0g1FQzliqYow8QN6RJLJhfLlIUDH7XmRQF4zdpQJ:IQRNaXmmGsTA7gUBJKN6VhfLlICH7Xmk
MD5:	61ADCE4F13DA1F6E8691BDFFA7122985
SHA1:	D5D5E66172A30CA81E594B1FCFF52C634CF2DD76
SHA-256:	E708972410675EDB89BEB11790B9B38E3B6CA0B74B8B06C3E7B1AC940F24004A
SHA-512:	D41A9720B70518F4C3E30F0EDB4AC3DBEC2EB5B33BFA49BD777AEFC85959B45C41CC5E8AFB2527E3D50B07AA6BC78DFD643A7097983D4D3F9CC9E6F490AB0 D66
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Jb.....(.....(.....(.(.h.(.....(.....(.....(.....(.....(.....Z.(.....).P...@.....(.h...e...[..7.....8.v...@M....!Y.d...y.s..VNn.J...j....%.. D.J..?....Z....t....##.u*.#.U..Z.f%...).....-....Zb...<...V..a.&.:o..2.3....X....$v..Km9.(i.d....E4r..D.6W.4g(W.Z.....{.0]..R.....=.J.Q...b.=}..#..b...~....MB...(.....(.....(.....J.(.....(.....(..... (.....(.....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOrsX0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	modified
Size (bytes):	12759
Entropy (8bit):	7.887160702338325
Encrypted:	false
SSDEEP:	384:N6N9/N5bhsmS+DpH8EfssEzXF+D9N/b0tm:Nsb5bV9DpcEfmbsXAtm
MD5:	AC06B29D0E39E772D06EE89B67F010F5
SHA1:	9632CA70966D3A98C3E0D72234D14FF47216B3C9
SHA-256:	665852486FF3938A0F874E410C4FE77894C66DC6A39E075E53D1F425404E8DD6
SHA-512:	376D9142962FFFAD59F8577A3D882068BA84A526B464D883F27906996339B847B5FA718984128263E463D9D79D614DD33AB62445DEE62EBBC25A9FA854FC8742
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...B....).).S.....(.....(.....(.....(.....(.(.h.).P.@.(.).(.....(.i.P.@.....(.....(.....(.....(.....(.....(.(.....P.@..-!.0..(.h.....(.... N..4...f+O.k7ic.].....b.,~"......=B...P...<....._qp.....B.....-...._..N....._i.u.Fh.^#.....Z.2..A..+..#O@.^[..?.Z..FE..es...Y...(.P.@....P.@....(.P.@.@....J.(...P0.....(.....(... ../I...F.3.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAzjSw3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	587
Entropy (8bit):	7.531438372526454
Encrypted:	false
SSDEEP:	12:6v/7r+k5j60/BRFEAYagzKQkIr76mpc0hneR2bHVkKPVXwZzv8gXAtz:GNO050agzTkVmpc0xguPViO
MD5:	2DF6E53A33E3D7D2E401F9FD0B723221
SHA1:	C2E3B5A6FF363BBD31CC6E39CEEC10B67BBBB9E9
SHA-256:	3484DE1DF304502392D694F16B843B7E1FF5C3F2FF88C6BCB30B195F34F8AEF3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAzjSw3[1].png	
SHA-512:	70A4CBD0A3BB14584F9D528CE87F69DE5CC10366BDEDB3B568E63411280C7D7B4900EC8101AC87774C9DACCBB9F1A8D989483A5CDFBD382FE814F1F181601E 1C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...Kh.Q...If..(*.....M.....PQ....QA..nD..''n.....4.`K...&.M.D..X...jH.4Nc..:0.{.....suv...G_.VI.3.w*k.cd.v...J.i..t.R.zd_.. .@..C.....$..J...5+...U/S.....k..:....1...!%..g.T...<plv...)Y....;..uq..(..b..X_...]=..K.[...\[.....r...`G.u.....{..n..._.....u..E.~..!f%.'..>..2ZZ...u.....>....8.w...t.Fi.W....l.~%h....h/.{.K#91 EGx.SGjUq...<.....0...c....P.h.....^G...%..S]..P...c.j..r..{.0x"#k.q..45.....r..E...k...)..y?|.-y..}.D`..`J?.u.}...sH....E.\2r.s~b!@a."........E...Hv.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BB10MkbM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	936
Entropy (8bit):	7.711185429072882
Encrypted:	false
SSDEEP:	24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/lxAZiuoSNYgO
MD5:	19B9391F3CA20AA5671834C668105A22
SHA1:	81C2522FC7C808683191D2469426DFC06100F574
SHA-256:	3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F
SHA-512:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66 C
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l.....LDA.....u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}....._.I$FS.\.c][4#... .....+...U@fZz.Y.....\|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V.....G...5....uc....XV.=.{..ai.pw.v)...(.9.z\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R.....c.....@S5.? 3...q..:..8.?....p.=6`..T...5.nn.....]..b.j.,..pf.....8...''.M..?.@K...L.='.1.O.2Kb.p..(..\.D.....n..._.....0.....w^bR....v\..)..l..f..l..M.m.6t.7....U.Y3?.h=..!.<..._.....pL..V"[..... {[P....e07...Wc....IH.T@...*..A@.....;....>Gt&...}...o...KP...7W1.sm~...&.....00.....>/....I.#.t.....2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<.. <&.M!mk:\|....%.<...,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.....c.&.>.3.....ek..+..~B.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	13764
Entropy (8bit):	7.273450351118404
Encrypted:	false
SSDEEP:	384:IfOm4cIa37nstlEM15mv7OAkrIh4McOD07+8n0GoJdxFhEh8:I2m4pa37stlTgqAjS0GoJd3yK
MD5:	DA6531188AED539AF6EAA0F89912AACF
SHA1:	602244816EA22CBE39BBD4DB386519908745D45C
SHA-256:	C719BE5FFC45680FE2A18CDB129E60A48A27A6666231636378918B4344F149F7
SHA-512:	DF03FA1CB6ED0D1FFAC5FB5F2BB6523D373AC4A67CEE1AAF07E0DA61E3F19E7AF43673B6BEFE7192648AC2531EF64F6B4F93F941BF014ED2791FA6F46720C7 DB
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....5.D..gJ.ks@..(...@.....l..pE..iT...t&..V.M..h....4.m.-.!....:.....*...a...CQ...c....Fj....F(...5 ..<.....J..E.0.''..].6...B.K... .....k.t.A'p..KJ..*A....(.....(.....(.....(.....(.....(.....(.....(.....(.....K1.....:...0.....I...M.9..n..d.Z.e.Q..HfE....I^...h.h.t...(.9:.2....z...@.....:...3..w.@.P4Ac1.a.@...A#.P1... ..4..@.@. (.h.h.(....0....Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F5 7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BBkwUr[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0..."..0....a....<....<....y..qS.....m..k..%.'|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[.. ..0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^l.P..5.0....?...&.A.K..|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/... .Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\http___cdn.taboola.com_libtrc_static_thumbnails_7b4dbad0520957f16bd4e3f810f4c883[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, 207x311, frames 3
Category:	dropped
Size (bytes):	13955
Entropy (8bit):	7.970358055601774
Encrypted:	false
SSDEEP:	192:IrAV0LA/KlTZ0vh+pZvjhDTD8pfokjGX0FVKGTdZn7VwvLom+zt:c9LASnJDTEQLX0rZn7VIqt
MD5:	E150F5DFC8FEBF67ABE61C2494132036
SHA1:	5B6AE976394DC035CC55518F7D469481FDC3EA21
SHA-256:	6D49939610DF358E30BF77C9FD4271742E0CCBD5464506298B09FA2999C7BBA6
SHA-512:	2FD52A8086ADE2BC115F91E5F873D76C4C2550C030875567A3084C49B5E9EC87EC281C6B93342B25060CE14485C08453FB9ABC1E29D4B20892795A69D1DD64B
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....C..... .....!%0)!#-$..*9*-13666 (;?:4>0563…C.....)..)W:1:WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW.....7.....)..5+bvE\I.....t.....*..^...O-...<...}C.^\..V.5L..J..3..A.....0.L.;...el.|.g'.v... ..C-..<.....1-d.....F... .....I.&.`9F..&....1.Bm.p..@.kd..{A. ..j`5....ir~..S.w.rgr.$.....<. .P(..F...me...5s.....^..Zv..h.$.....5].m...1.8.isK.!D.....p=+.u.;F..kSP..2.&.=.....#`....@.%j.Y..:,5?M.[..8V..eL}..U8.\,.4.L.b....V.sMy.*p,.....Rkv.....U.....6.j..../.Q}.Y`C&.....I.~z)..:!(.;b.T.j..r.UR+.L..O.=0.....WZk..*...N..`..Lq..b..Z.Ug.....W...R..R....M[-...^..k.... ....Q...R..kp.?....d+J.....1..I.\.P....9.9I..@+..!....L%8.....+!....^.....]]A..t;.d.....w...".G.....P.W..9..Z.+.F..F.G4B..4.Ph.Xs..H.Q.....?.z<..!.x9.h.~[..wh.b.6.T...y....1".O..H,J..w..-."6.I...-R..,[}y.....I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_b4d84d7a-e7a0-4e71-a4e1-288b18f4b1a1_166a74d60a77edc1b295914db4bc79ac[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, 207x311, frames 3
Category:	dropped
Size (bytes):	7639
Entropy (8bit):	7.935649066830113
Encrypted:	false
SSDEEP:	192:/8tw4Q4GuyHK7NTVt+VFOqP4gbnC/DIW2jqxmQ9:/8ePvHK7jt+ew4gGAtQ9
MD5:	AA0DC1037EF3AB4C187E7ACC5A5AD5CD
SHA1:	A4EE232A7C4033DA282B5E60CD7C864B3757FFC4
SHA-256:	290E922508503D37208A8566351E1BAC5A50073D21953F986D62D1AE3D6B49E6
SHA-512:	753CCABE6CCB3365F771EAFBB9C6076AA997434ECFD2C83B2C97ACCFB653620F66EC7A77D721B8F99D4C9FA6F45880F6F03AD43410072EBDD6093E9B169CD51
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF....."....."..$...$.6*&&*6>424>LDDL_Z_||....."....."..$...$.6*&&*6>424>LDDL_Z_||.....7...."..... .....4..... .....j7..M.a.@j4..T%...T.[.0S.z...[...b.3H'...8..5..c.D..(.%`.....tWc9.J..G....s.2..x..t.^.....U...2..!)*j5.D.$.(.1^d.4}U=..=.c...Gz(..O^..M9\|ucw.:.....w.*..# &...L..RH.I.\|.j...t2.}.. ..On....`sn.....N.q..U.X.....H.DBA.=~.[2.@"A..Ey..[T.[c.s.....=..E(w..F.V..s.Gv.....2.....@.?..Y..9!"&&j.-m.).....7.h..a...um{.K....t..v..#.v.KvNo..>wv=g#....7.<..o]....2g.{.f\|Ty..... .vE.?;w.}..j..G...o.....i.az.s..w..<.,...%.\|.o%.....Y)k\|...F.r.$.o....v..z..E..5.....1.l.-..F..F.{.[i..... .o...b...g#..Ue.g..Z....I...}.Z.p..zS?...~.)....i..7!.v,X...O..3..>...}/.../c..v.$..P..~'.m.n.F..... .'N..|.d..M.....n.....5s.`P...s.J=..KP.....pzZ..=i.....a...BP.H..{f.....H.w..f.3...b8.,.q.]d.r.....KI.LX..O.....-..j...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery-2.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery-2.1.1.min[1].js	
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"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=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\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 d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\medianet[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):	409365
Entropy (8bit):	5.484594748347012
Encrypted:	false
SSDEEP:	6144:z9CkYqP1vG2jnmuynGJ8nKM03VCuPbjErMrSN9Gm9:p1vFjKnGJ8KMGxTeM+fGm9
MD5:	C3DB41FE6B716BA10C39E5A58C1BA45D
SHA1:	47620AB535092B7AF20C5C262B5646BF758CA708
SHA-256:	79A48D772EB1B9C31FF61A58E7E743B816907FD1765F062F89A6876E698F256E
SHA-512:	D43E46190A4454D2B591A60A940480CA0D1BDF2C689619CB639B67A2FFE3F9A6B50EF564DC28B8C272FCADC934B06FEEA1915837AF31A0C62BC71182021B09E9
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)

C:\Users\user\AppData\Local\Temp\~DF3E5B0442C91F7FC3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.4182562834717611
Encrypted:	false
SSDEEP:	48:kBqoIm/Qm/um/ye/ce/ts/tQ/s/ce///H:kBqoIm/Qm/um/9/r/q/S/s/r///H
MD5:	AA7EF85CAA7A4BF74D053932FF8698A1
SHA1:	A766D0E95EF15E6FD0D59F243D1E88235BD7ACC5
SHA-256:	0FB4BC0AE7C6C4B6F6DA899A801EFD6F2EC05277B2FBE0BB2AAC03CAA59A90F1
SHA-512:	07C61AD1AA8205E73EEECBFC4B643FCCE1FDEA55707B1F79912650181C237D3AD98D0DBBD11CF7E30407F25F08BF1CB7504E2158641D692FA66429BFFB5AFFA6
Malicious:	false
Reputation:	unknown
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF98125A3D199168E4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	364814
Entropy (8bit):	3.286801947464921
Encrypted:	false
SSDEEP:	3072:9Z/2Bfcdmu5kgTzGtgZ/2Bfc+mu5kgTzGtgZ/2Bfcdmu5kgTzGt5Z/2Bfc+mu5kn:kPGC
MD5:	DF53265079679F6331F5D9D320468826
SHA1:	A03DE5E6431524DC4AF6CB79DB0B83D7C4198D0D
SHA-256:	B8D7511AFD2390403CB201C078E7DEC29EC5139CFE5A77DBC5834F0F8DCE507B
SHA-512:	31EA8DD1B5C5C323D6870F0777666F7E8A3FD6850C18B08B0FFF721E3BC05CDE8BE38994935F81470DE25963A28BEF88A0DCFA4AEFEF6CDFD4873CFEB8A6B714
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\~DF98125A3D199168E4.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\c5BVxaoEy\TAPI32.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." ....p.....@.....@.....@lx}..b..... ..V....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\c5BVxaoEy\dialer.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	5.557058773165724
Encrypted:	false
SSDEEP:	768:iBbgCd8gzNlMWrLpBARbyz5sAbYTkMZNuC9iifbd:sxWS6AbakMZNuC9Bbd
MD5:	0EC74656A7F7667DD94C76081B111827
SHA1:	416DA743A7A52CD4204DF396BD11D9DBAE98076A
SHA-256:	973389F8F3124B9EF0097909298F53AEFBCE38733FB07D204663B4DD17BEAC4C
SHA-512:	2A91A269C377BD0113C9CB3CBD4269ABC1FBBA4064033448FF2D073047FFF4448FDE4729072AC0CA01629C34DC33926CD417E0D02D3E00E4BFD1C42B730378E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m...m...m.....m.....m.....m...m..am.....m.....m.....m. .Rich.m.....PE..d...N.Uu....."....T...H.....`Y.....@.....`.....$.....(..... ....z..T..... ..p.....q..H.....text...pR.....T..... ..`.rdata.....p.....X.....@..@.data.....v.....@....pdata..(.....x.....@..@.rsrc..... |.....@..@.reloc.. .....@..B.....

C:\Users\user\AppData\Local\lFQXVd7\FXSCOVER.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	232960
Entropy (8bit):	5.805361894084464
Encrypted:	false
SSDEEP:	6144:v4J/ihC4Tb5//Jfl+QL+ooODUwq306Q/:v4khC4h/qiooT06Q/
MD5:	BEAB16FEFCB7F62BBC135FB87DF7FDF2
SHA1:	EAF18190494496329573CAA3F95CACA6EF0FB6F6
SHA-256:	E3C66F68737611DFD051F1D6EEB371FDE89B129925A85695B9F90CDE3E04BD96
SHA-512:	FF4E756B1D928C97523ADE2B30FAB56219659AA22E7F5D71CB3238A2C39E1C704C6A046C2DC14FA5207CE8E8C75CD7EF5416B36A1452D97D929A5686C75D2C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....).I.H...H...H...,...H...,...H...,...H...H...K...,...H...,...H...,...H..Rich.H.....PE..d.....3....."....@.....0...`..... .....h1...`.....T.....c..(....b..... .....d.....text...~..... ..`.rdata..... .....@..@.data.....@.....&.....@....pdata.....`.....6.....@..@.rsrc...h1.....2...N..... ..@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\lFQXVd7\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1675264
Entropy (8bit):	4.415808775460765
Encrypted:	false
SSDEEP:	12288:BVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Urx:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnbe
MD5:	3AC1AE9C23111206137C244F138C43D8
SHA1:	E4BA74996F975E33E6D3724AA5D1CBC4A1CE960B
SHA-256:	178787F0AE3AFDB19A8CE3ABD6D613DCEEE010CC20A11B68368A49F89C84B2BD
SHA-512:	1BB75E698F20F7F1367835A1560E7A2D3A83BDE86A22259B287564080C9550A81CAFBF64BB897C31C99A462F0A587F954D60D47C6C0CF5B906B5020DA614DAA8
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\IFQXVd7\MFC42u.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....p.....@.....@lx}..b..... ...l...c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\yeShxe\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1654784
Entropy (8bit):	4.38789233128203
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A177E1222CEC2B9624C8ABEAA8CB5D96
SHA1:	2C0F9640B911A80093F33605DB7A271600BFA566
SHA-256:	9CC37C2F755864EA368C0030B2D75D2453220F102449B881C218EA3579733398
SHA-512:	0C65EBF198A938EC1CAF6E7093987EA2A183233114565422AB2BCE23B2261B9280BB12D47B8E67842DFE447E044F4FC2ACC74AE0F07D4BC3C540A845838B01D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....@.....@.....@.....@lx}..b..... ..h....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\yeShxe\mstsc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3640832
Entropy (8bit):	5.884402821447862
Encrypted:	false
SSDEEP:	98304:q8yNOTNEpZxGb+ZPgN6tYDNBMe+8noqvEYw0n2WFfZT+xgsLOsMg:q8yNOTNEpZxk+ZIN6tYDNBMe+8noqvEB
MD5:	3FBB5CD8829E9533D0FF5819DB0444C0
SHA1:	A4A6E4E50421E57EA4745BA44568B107A9369447
SHA-256:	043870DBAB955C1851E1710D941495357383A08F3F30DD3E3A1945583A85E0CA
SHA-512:	349459CCF4DDFB0B05B066869C99088BA3012930D5BBC3ED1C9E4CF6400687B1EFE698C5B1734BF6FF299F6C65DD7A71A2709D3773E9E96F6FDE659F5D883F4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... w.dN$.dN$.dN$..M%.dN$..J%.dN$..K%.dN$..O%.dN$.dO$ TfN$..G%.eN$...$.dN$..L%.dN$Rich.dN$.....PE..d.....Y....."....."....$....%.....p.....@.....7.....K8...`.....].....p..H>!....`..... ..7. *..P...T.....`.....`.....\..`.....text...."....."....$..... ..`.rdata...\...@...^...(.....@..@.data...P(.....@....pdata..`..... ....@..@.didat..(....`..... .....@....rsrc...H>!..p...@!.."....."....@..@.reloc.. *....7.,...b7.....@..B..... .....

C:\Users\user\AppData\Local\zOAoLK\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1933312
Entropy (8bit):	4.879920181774836
Encrypted:	false
SSDEEP:	12288:fVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Zd:WfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	C2235DE4F2398B177D7D9F60942D1925
SHA1:	3A80FADD5E446EA6EF1E3ED69CC3E4FAF6CAB271
SHA-256:	20C654E9F7785C119448CD4922E1515ADF028E0BBCBBF0939B6A849AD3338543
SHA-512:	FFA9D1BA5245A5F8F9E3F8C3274C799C5472E44A8995EA2F747E95DDD65A99BBCDB4866797A70EAFE976AC6578A1F88BF68C6B17928CCB3425C2C5B4595F192E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\zOAoLK\DUI70.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....`.....p.....@.....@lx}..b..... ..dQ...c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.3982781345342215
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	3FLps29lWm.dll
File size:	1646592
MD5:	0636cf8dafa624e524ad748f38d22240
SHA1:	b347c65c5add7e2fb16fe30cedf46f57fd1eaa56
SHA256:	586999eb0a767ffedcc169d7aead09ebfc1528998def72fc9c5e4bfb245b1abc
SHA512:	ad546f7d8655c2c8501c30acf168d07851801c25ccc81db706123e5e50c230ba274c8edeefb1bf6ef6e15dac7cb6a25ab03c68183cf3b57b8b99f9ee5e1c90fc
SSDEEP:	12288:fVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:WfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E4E44CC [Thu Feb 20 08:35:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64f2c	0x65000	False	0.702390160891	data	7.86574512659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x880	0x1000	False	0.139892578125	data	1.23838501563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0x2324	0x3000	False	0.0498046875	data	4.65321444248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.qkm	0xc4000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvjb	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlmkv	0xc7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wucsxe	0xc8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fltwtj	0x10e000	0x1267	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sfplio	0x110000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rpg	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bewzc	0x157000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vksvaw	0x159000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wmhg	0x15a000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kswemc	0x15c000	0x36d	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kaxfk	0x15d000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pjf	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.retjqj	0x160000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mizn	0x161000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrub	0x162000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.susbqq	0x164000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.jeojcw	0x16b000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vwl	0x16c000	0xae7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mub	0x16d000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwxpmb	0x174000	0x573	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aea	0x175000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwpch	0x176000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nzgp	0x177000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qimx	0x178000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tkvgvo	0x179000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tgipu	0x17a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uwr	0x17b000	0x14ed	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.agscf	0x17d000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idba	0x184000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.txn	0x186000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.amfg	0x187000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fgnmv	0x188000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iqmp	0x189000	0xd57	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hkwa	0x18a000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.imjyew	0x18b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qlv	0x18c000	0x896	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vofo	0x18d000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.emh	0x18f000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.boy	0x190000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.twwn	0x191000	0xbde	0x1000	False	0.396728515625	data	4.69452673181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Copyright Joe Security LLC 2021

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 14:02:34.883313894 CEST	192.168.2.3	8.8.8.8	0x842a	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:37.606158972 CEST	192.168.2.3	8.8.8.8	0x6246	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:38.654280901 CEST	192.168.2.3	8.8.8.8	0x9f55	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.189481974 CEST	192.168.2.3	8.8.8.8	0x54ff	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.336389065 CEST	192.168.2.3	8.8.8.8	0x708e	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.597307920 CEST	192.168.2.3	8.8.8.8	0xf0f3	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.606154919 CEST	192.168.2.3	8.8.8.8	0x845	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:43.645606995 CEST	192.168.2.3	8.8.8.8	0xdf0d	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:44.168005943 CEST	192.168.2.3	8.8.8.8	0xce62	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:44.600941896 CEST	192.168.2.3	8.8.8.8	0xb35d	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:45.565083981 CEST	192.168.2.3	8.8.8.8	0xd0e	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:47.998759985 CEST	192.168.2.3	8.8.8.8	0xce47	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.096976042 CEST	192.168.2.3	8.8.8.8	0x9a6e	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 14:02:34.913018942 CEST	8.8.8.8	192.168.2.3	0x842a	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:37.648610115 CEST	8.8.8.8	192.168.2.3	0x6246	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:38.688934088 CEST	8.8.8.8	192.168.2.3	0x9f55	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:38.688934088 CEST	8.8.8.8	192.168.2.3	0x9f55	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 14:02:39.237052917 CEST	8.8.8.8	192.168.2.3	0x54ff	No error (0)	contextual.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.364670038 CEST	8.8.8.8	192.168.2.3	0x708e	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.364670038 CEST	8.8.8.8	192.168.2.3	0x708e	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.364670038 CEST	8.8.8.8	192.168.2.3	0x708e	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.638448000 CEST	8.8.8.8	192.168.2.3	0x845	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.638448000 CEST	8.8.8.8	192.168.2.3	0x845	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.638448000 CEST	8.8.8.8	192.168.2.3	0x845	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:39.641364098 CEST	8.8.8.8	192.168.2.3	0xf0f3	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:39.641364098 CEST	8.8.8.8	192.168.2.3	0xf0f3	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:43.676970005 CEST	8.8.8.8	192.168.2.3	0xdf0d	No error (0)	hblg.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:44.196976900 CEST	8.8.8.8	192.168.2.3	0xce62	No error (0)	lg3.media.net		2.18.160.23	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:44.632528067 CEST	8.8.8.8	192.168.2.3	0xb35d	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:45.594656944 CEST	8.8.8.8	192.168.2.3	0xd0e	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:45.594656944 CEST	8.8.8.8	192.168.2.3	0xd0e	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:48.028208017 CEST	8.8.8.8	192.168.2.3	0xce47	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:48.028208017 CEST	8.8.8.8	192.168.2.3	0xce47	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.028208017 CEST	8.8.8.8	192.168.2.3	0xce47	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.124707937 CEST	8.8.8.8	192.168.2.3	0x9a6e	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 14:02:48.124707937 CEST	8.8.8.8	192.168.2.3	0x9a6e	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.124707937 CEST	8.8.8.8	192.168.2.3	0x9a6e	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.124707937 CEST	8.8.8.8	192.168.2.3	0x9a6e	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:48.124707937 CEST	8.8.8.8	192.168.2.3	0x9a6e	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

Copyright Joe Security LLC 2021

- https:
  - geolocation.onetrust.com
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.net
  - s.yimg.com
  - img.img-taboola.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49762	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:38 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-09-15 12:02:38 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:02:38 GMT Content-Type: text/javascript Content-Length: 182 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 68f1b5103f5405f5-FRA
2021-09-15 12:02:38 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 48 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 38 31 35 32 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 34 33 30 30 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 30 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49776	172.67.70.134	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:39 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive
2021-09-15 12:02:39 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:02:39 GMT Content-Type: application/javascript Content-Length: 10055 Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=1800, must-revalidate Etag: "9e65f2af141ca0a7e5ebc06696b0cdb5" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 217 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=nt%2BKWo4MPBpBy%2FrBoHbeCBGwWg7Km0hG8oQ5cZRAfx7nRkVsOlmZXrJD%2FR7rm9L1%2FCcNwxQwh4fnefNLm1Kfa2kcm%2FpaCNf%2BhY4NMhnzBKyyu3zPA%2FejKyRpiS2LRw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 68f1b5149de04e8c-FRA

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:39 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 7b 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f 6e Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}cat ch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio
2021-09-15 12:02:39 UTC	2	IN	Data Raw: 69 6f 6e 20 74 28 74 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b Data Ascii: ion t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try {if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[
2021-09-15 12:02:39 UTC	3	IN	Data Raw: 74 2e 62 6f 64 79 7c 7c 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2d 34 2d 67 33 36 37 63 35 37 65 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 Data Ascii: t.body||window.document.documentElement).appendChild(e)}})var u,a,d,b,m;u="6208086025961472",a="bt loader.com",d="api.btloader.com",b="2.0-4-g367c57e",m="";var o={"msn.com":{"content_enabled":true,"mobile_cont ent_enabled":false,"website_id":"56717373886955
2021-09-15 12:02:39 UTC	5	IN	Data Raw: 65 2e 69 6e 64 65 78 4f 66 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 29 26 26 28 74 3d 21 30 2c 77 2e 77 65 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 77 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 77 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 Data Ascii: e.indexOf(n.toLowerCase()))&&(t=!0,w.websiteID=o[n].website_id,w.contentEnabled=o[n].content_enabl ed,w.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org= "+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u
2021-09-15 12:02:39 UTC	6	IN	Data Raw: 75 6c 6c 21 3d 63 26 26 63 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 6c 3d 6e 2c 73 3d 31 2d 6e 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 63 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 63 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 72 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 6c 2b 73 2a 6f 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 6c 2b 73 2a 28 6f 2b 74 29 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 75 3d 74 5b 65 5d 3b 69 66 28 6e 75 6c 6c 21 3d 75 26 26 75 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 64 3d 6e 2b 28 31 2d 6e 29 2a 6f 2c 62 3d 28 31 2d 6e 29 2a 28 31 2d 6f 29 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 75 2e 62 Data Ascii: ull!=c&&c.bundles){var l=n,s=1-n;Object.keys(c.bundles).sort().forEach(function(e){var t=c.bundles[e];r[e]={ min:Math.trunc(100*(l+s*o)),max:Math.trunc(100*(l+s*(o+t)))},o+=t})}var u=t[e];if(null!=u&&u.bundles){var d=n+(1-n)*o,b=(1-n)*(1-o);Object.keys(u.b
2021-09-15 12:02:39 UTC	7	IN	Data Raw: 64 69 67 65 73 74 22 3a 35 37 31 30 31 35 30 38 35 32 36 37 33 35 33 36 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 35 37 31 30 31 35 30 38 35 32 36 37 33 35 33 36 22 3a 31 7d 7d 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 70 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 65 74 75 72 6e 20 69 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 73 77 69 74 63 68 28 65 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 72 6e 20 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 61 6c 72 65 61 64 79 5f 69 6e 76 6f 6b 65 64 7c 7c 21 77 2e 77 65 62 73 69 74 65 49 44 3f Data Ascii: digest":5710150852673536,"bundles":{"5710150852673536":1}},window.__bt_intrnl={traceID:p.traceID} ;try{!function(){r(this,void 0,void 0,function(){var t,n,o;return i(this,function(e){switch(e.label){case 0:return window.__bt_alr eady_invoked||!w.websiteID?
2021-09-15 12:02:39 UTC	9	IN	Data Raw: 6e 74 22 29 7c 7c 77 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 77 2e 77 65 62 73 69 74 65 49 44 26 26 77 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 65 6d 6f 62 69 6c 65 7c 69 70 28 68 6f 6e 65 7c 6f 64 29 7c 69 72 69 73 7c 6b 69 6e 64 6c 65 7c 6c 67 65 20 7c 6d 61 65 6d 6f 7c 6d 69 64 70 7c 6d 6d 70 7c 6d 6f 62 69 6c 65 2e 2b 66 69 72 65 66 6f 78 7c 6e 65 74 66 72 6f 6e 74 7c 6f 70 65 72 61 20 6d 28 6f 62 7c 69 6e 29 69 7c 70 61 6c Data Ascii: nt"))||w.mobileContentEnabled),w.websiteID&&w.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|a vantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge |maemo|midp|mmp|mobile.+firefox|netfront|opera m(ob|in)i|pal
2021-09-15 12:02:39 UTC	10	IN	Data Raw: 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c 72 74 7c 73 65 29 7c 70 72 6f 78 7c 70 73 69 6f 7c 70 74 5c 2d 67 7c 71 61 5c 2d 61 7c 71 63 28 30 37 7c 31 32 7c 32 31 7c 33 32 7c 36 30 7c 5c 2d 5b 32 2d 37 5d 7c 69 5c 2d 29 7c 71 74 65 6b 7c 72 33 38 30 7c 72 36 30 30 7c 72 61 6b 73 7c 72 69 6d 39 7c 72 6f 28 76 65 7c 7a 6f 29 7c 73 Data Ascii: 0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg| pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc(07|12|21|32|60|\-[2-7]|i\-)|qtek|r380|r600|raks |rim9|ro(ve|zo)|s

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49814	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	265	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5ac3b539d1cfda83dbe324033737805f.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-09-15 12:02:48 UTC	300	IN	HTTP/1.1 200 OK Connection: close Content-Length: 16943 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 436451453480117415704695784570040513545,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "886165ebbb25e2fd2d9ab2c4f3146762" expiration: expiry-date="Sat, 21 Aug 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Wed, 21 Jul 2021 09:23:29 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 8 X-backend-name: US_DIR:3FP7YNX3LMizprTZsG7BSW--F_US_nlb106 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 2085910 X-Served-By: cache-wdc5520-WDC, cache-dca17754-DCA, cache-hhn4044-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1631707368.366499,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F5ac3b539d1cfda83dbe324033737805f.jpg X-vcl-time-ms: 1
2021-09-15 12:02:48 UTC	301	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 33 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 04 05 06 07 00 02 03 08 01 01 00 02 03 01 00 00 00 00 00 00 00 00 00 00 00 00 02 03 00 01 04 05 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 cd c0 dc 09 ff 00 44 12 44 bd 48 af d1 bb 29 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"3DDH)
2021-09-15 12:02:48 UTC	302	IN	Data Raw: c5 8a 36 4b 61 49 da 27 7e 79 94 ae 38 e7 06 bd 51 be 86 b9 26 0e d8 17 af 91 5d 79 9a c4 db e6 cd 47 9b 3a f3 ea 8d dd 4c 00 aa a3 8b 00 92 03 89 08 8b 16 5d 81 20 58 77 61 3b 89 18 c1 2b f0 2d 96 16 2b 57 3d 66 b0 ae 76 c0 94 9f 9a b2 90 27 6d 0a 75 28 72 08 44 15 bf c6 2b ca 1d 73 23 b7 ed 99 50 92 f3 20 96 56 64 9d 8c cc b9 bf 7c c9 7f 25 19 95 4b bb 66 14 9d e6 67 2f 6a ad f3 36 e6 df be 64 ae d9 98 55 a9 19 86 1f ff c4 00 2c 10 00 02 03 00 02 02 02 02 03 01 00 02 01 05 00 00 02 03 01 04 05 00 06 11 12 13 21 07 14 15 22 31 41 16 23 32 08 10 42 61 71 ff da 00 08 01 01 00 01 09 00 51 87 81 31 1f 94 fe 49 20 14 b4 8f d4 fd cd 76 82 0d be ce 4f f5 28 8e 29 be 93 e0 a2 a5 98 37 48 08 2d f9 d7 20 57 0c bb 9e c4 41 7a 8c 14 f3 e5 fe be 27 99 a7 32 46 10 55 Data Ascii: 6Kal'~y8Q&]yG:L] Xwa;+-+W=fv'mu(rD+s#P Vd|%Kfg/j6dU,!"1A#2BaqQ1l vO()7H- WAz'2FU
2021-09-15 12:02:48 UTC	303	IN	Data Raw: b8 a5 9c aa de 9f 6d dc bb f3 a8 2c f5 ca f8 cc 60 9e 8d ed ab bd 43 42 a6 75 31 aa 03 9d 7a 9d 7f 0a cc e8 b8 d6 6d 57 4c d0 47 e3 7e b0 bb 22 d0 c2 ca c8 b5 5e 1f 52 b8 3d 96 10 50 76 22 f2 f3 35 14 85 dc a2 1b 21 d6 7b 31 d0 b3 a7 ab 4a a6 e6 5d 91 25 58 cf b9 5d a5 44 95 72 ed 0c eb 8e a7 7a e3 f7 b1 bf bf c5 6c bf 24 b8 eb 1a 0b 2b 39 d7 d2 f5 83 d0 60 c5 cf d8 d0 b7 58 56 68 b0 a4 d8 75 58 2a ae 2b 3a 4a b2 ca 4a 60 dd 86 af cd a5 42 98 0c 5c 59 ad 6f 73 a4 f7 6e b5 54 f4 8d f4 3b 80 2a 8b d7 65 97 fb 0e 8e 85 68 4c c2 89 22 30 12 0b 34 45 49 f4 1c 1b dd 65 92 62 fa ba b5 b6 97 51 ab 4d 7e b0 16 9d 62 61 a7 99 54 9d 16 c2 12 33 91 59 1f 17 fe 48 9c a7 49 87 ae 9b 1a 75 6a 89 94 dd d0 a7 56 54 db 4f dd a9 57 b2 ea 45 d9 c2 af d4 66 6b fe 99 df be 79 Data Ascii: m,`CBu1zmWLG~"^R=Pv"5!{1J]%X]Drzl$+9`XVhuX*+:JJ`B\YosnT;*ehL"04EIebQM~baT3YHIujVTOWEfky
2021-09-15 12:02:48 UTC	305	IN	Data Raw: b4 52 91 34 ab 43 f4 15 a5 67 5c 5f a9 db ae 2f 27 13 2e ea 63 6f 57 31 54 ed df 2b 1d 42 b9 ee ea 69 76 3d 65 76 0e c2 5f cc d6 14 b8 ce 93 3f 65 95 60 9a d5 5b 5c 4c 4e 8d 61 d1 0a c6 eb 23 27 24 41 05 ab 6c 6f 8c 18 59 18 38 20 7f 1f 05 55 f1 ea 7b d9 34 e8 94 ba bd 6a 45 a1 8f 6e bb 69 1e e5 9c 5e c3 d7 ac 0b c0 b0 7b 26 24 10 59 ce 31 ac 6f a7 64 18 b1 f8 fd fd 1c 11 31 fe 4c 4c cf 36 af 4e 76 63 1c 36 fa 4d cb 48 ec 6d 9a cc d7 d7 fe 52 f5 4b c9 3e f9 62 eb c3 09 26 de 8d 93 72 c9 ee 1d 6b 74 60 c9 9a 7e 89 ca 53 0e d6 f1 25 3d 9e 58 5a 14 e1 e1 d9 70 2c e8 1d 15 d3 ad d4 66 a8 f5 fa 0b 15 df 22 c5 da 5c 55 9b 94 4a af 8b 34 45 cf a6 ca 6a e6 6d b5 2a f8 7e e1 a4 fd 19 6e bf be 22 29 56 d2 9a 7f 3f 88 8b be 4e 2d 53 cf b3 26 44 17 2a 54 16 be a3 95 Data Ascii: R4Cg_/'.coW1T+Biv=ev_?e`[\LNa#'$AloY8 U{4jEni^{&$Y1od1LL6Nvc6MHmRK>b&rkt`~S%=XZp,f"\UJ4 Ejm*~n")V?N-S&D*T
2021-09-15 12:02:48 UTC	306	IN	Data Raw: 1b 7b 16 87 4e c3 50 36 04 c5 52 62 31 af 9f 56 8a 55 0a 70 30 96 21 f2 4d 76 5a ad 61 48 e4 83 7d fd 24 6b d7 f8 d0 31 c6 8b 14 30 45 0a 7b 03 c4 4f 13 e6 f3 40 1c e6 88 0a 5b e0 7a ed 5a b6 77 fa b5 c3 e5 86 92 ab bd 06 ec 80 5d af c8 f8 b1 eb ac 42 0a fd 90 4f 5f ce 7e a3 db 79 88 b5 a4 aa d4 41 0b e0 e8 a4 f3 82 e5 82 ef fa b7 74 fb 43 74 99 56 6e 13 98 51 e3 a9 bb 45 fb cb ab 4a 35 18 f4 dd b6 91 04 b2 fd b3 6c 2f 2e 96 63 ac 5d ac e2 2d 5c a0 75 7b 15 62 3a ee 7f ce d5 6c 5f b2 d2 b3 ab 6a cb be 25 a8 17 9d 55 c3 62 4e 7c cc f0 74 9a 99 85 d9 4f ed 89 fd 04 91 09 b7 c9 f2 19 e0 7d 59 26 af 4a e4 e8 2d 29 f8 be 21 99 43 fc c7 8f 3f 1a 0d 12 50 1d 0d ee 4f 72 c4 26 59 b2 14 cf 25 e7 f3 1e 0a 72 b6 8e dd 22 0c f4 6b 44 0b 52 cb 55 15 e0 12 ab 3d 9b 59 Data Ascii: {NP6Rb1VUp0!MvZaH}$k10E{O@[zZw]BO_~yAtCtVnQEJ5l/.c]-\u{b:l_j%UbN|tO}Y&J-)!C?POr&Y%r"kDRU=Y

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	308	IN	Data Raw: 72 33 30 a6 10 51 00 1e 33 ff 00 80 7b 0e e1 2d 4b f6 f6 a8 82 f1 2c f8 e0 e1 61 e6 78 41 e5 d0 73 c8 8f b9 e0 2c 0f c7 98 78 c2 e2 44 42 62 04 fc 48 84 73 cf 22 7c 71 65 c1 9e 2c bc c7 06 78 3c 02 f1 c1 3e 0c fd 70 4b cc ff 00 be f3 25 1f 78 12 0e 7c 5d 9e 68 fb 1d a7 cc 4e 69 40 36 5c 55 cc 64 07 30 61 8f 77 97 24 79 b4 73 05 5a 04 15 ef 21 fd a0 cb ef c7 3f de 08 f0 0b c7 19 f1 1c 47 bc c2 d7 3f f0 4e 39 ef 1c 12 e0 cf fd 8e 01 f0 27 ef 83 3c 19 e0 cf 12 41 f2 47 c9 c1 2f a8 8e 41 c4 44 f1 c5 22 83 38 e7 59 d0 a6 31 64 fe 47 58 81 8d 02 89 ce 8f 42 a2 63 cb f4 de 16 40 25 aa 38 b0 c9 38 e6 cf ab ed fc 5e 58 e6 21 2b 31 80 3f 70 12 e0 44 73 cf 3c fd 72 58 3e e2 3c 89 e7 ff c4 00 2c 11 00 02 02 02 00 05 02 05 05 01 01 00 00 00 00 00 01 02 00 11 03 21 10 Data Ascii: r30Q3{-K,axAs,xDBbHs"|qe,x<>pK%x[]hNi@6\Ud0aw$ysZ!?G?N9'<AG/AD"8Y1dGXBc@%88^X!+1?pDs<rX><,!
2021-09-15 12:02:48 UTC	309	IN	Data Raw: c4 d8 08 ad a9 03 77 83 69 94 12 41 be f0 9e 8c 68 73 bc 2e dd c9 b8 18 f9 97 01 e8 e3 56 57 e7 b7 eb 6b 10 5d 88 b9 1d 07 b6 33 2b 27 b4 ee 44 c9 60 d1 27 69 50 2e c4 c6 1e eb 37 55 0a 13 b8 df 62 60 b3 31 d3 02 22 a8 03 71 66 18 14 81 5a 89 02 04 76 e0 7e 66 81 8f 13 dd 12 66 3a 0c 0f 80 63 b6 a2 4d 4e f0 9f 68 58 f7 60 81 7e 66 a5 d1 5b ef 70 56 93 bf 45 3a b7 b8 07 d8 88 30 20 e7 79 a6 7a 97 d1 45 96 d7 b9 13 52 80 f4 c1 af 60 41 b1 5d 7d 57 aa c7 e9 f4 ad 6b 73 54 a3 a1 16 21 4e 89 dc f8 83 29 bd f8 81 d4 92 bd ee 10 6a 3a ae 55 a3 07 a3 c5 8b 13 8c 60 0d cb 4a 41 8d 48 3b 93 38 02 27 a4 c0 99 0e 40 a7 51 37 64 fd 0c b7 30 8b d7 fe bd 34 2a de 91 50 30 d6 45 c3 a6 1a 02 65 00 3a 8e 2b eb c6 ae 1a ea 66 5b 3a 86 e4 c0 e8 dc 19 8d 02 93 bc 23 48 26 e2 Data Ascii: wiAhs.VWk]3+'D`iP.7Ub`1"qfZv~ff:cMNhX`~f[pVE:0 yzER`A]}WksT!N)j:U`JAH;8'@Q7d04*P0Ee:+f[:#H&
2021-09-15 12:02:48 UTC	310	IN	Data Raw: e7 e6 d0 15 05 62 91 5b 61 6f e6 35 8a 50 fc 2a 00 59 57 69 66 29 13 90 6b d3 66 28 28 9a 85 0e e4 9e 12 06 ac 7d 6d 4b 1f f9 72 98 08 69 c1 f3 b1 da 6c 10 99 a7 8a 14 d2 c3 a9 9b 4b 24 9f f1 2a 93 c6 b2 00 f1 81 77 e6 c8 8b 47 a1 d3 10 ff 00 2f 06 25 e3 9f 43 80 83 d0 8c d8 c4 f0 de 87 b6 56 a0 8d d6 3a 1f 61 80 91 e8 6c 7e 06 b2 41 06 d0 b1 71 61 31 44 91 f4 73 dd 5b ba 91 db db 0c 32 4d 62 45 5f 29 f1 17 8b 52 3d 73 c6 88 c6 36 b9 a0 ca 41 a2 0d 75 c0 41 ea 30 ed aa 2a 79 cd ac 2b cd d6 be a0 e1 af 6c b1 7c 1f c3 a6 79 89 b1 ef 89 23 47 62 59 db 78 86 22 3b 5a 06 66 3e ca 32 24 fc cc 8e 16 59 b5 49 a0 54 48 f8 54 1b c4 a4 8c d4 89 11 88 85 da 73 22 77 0c 7e 51 b9 1d 78 e3 00 d5 4a 49 9d e2 e1 1c 90 07 00 9e 3a 64 b3 69 12 4d 8c 92 bb 38 54 65 da a4 7b Data Ascii: b[ao5P*YWif)kf((}mKrilK$*wG/%CV:al~Aqa1Ds[2MbE_)R=s6AuA0*y+l\|y#GbYx";Zf>2$YITHTs"w~QxJI:diM8Te{
2021-09-15 12:02:48 UTC	312	IN	Data Raw: 82 82 be f6 32 45 dc 24 3b 15 fc d4 e6 c8 66 f4 15 87 c1 78 4b 34 68 bd 1c 70 05 d1 38 8f ab d6 bc 9a b9 9a 60 4b 30 90 3a 45 f6 d8 d8 ba 3b f1 60 89 4f 09 b7 4d 33 01 cb 0f d8 cb 92 c1 3c c5 27 8f c3 9b 7a bd a2 39 26 3b f3 21 d8 31 f5 7f 0c d4 42 b0 a4 aa 6d 42 ef 11 53 fd 51 81 60 71 d9 59 89 12 ab 02 0e e3 db 35 4f 2a 96 2e 64 a9 80 e9 5b 6e c0 c7 20 2d ab 81 9e 1b c4 ed b0 08 c3 8a 23 69 bf 11 82 e6 aa 58 3c 6f 15 96 47 8f cd 27 60 0a ee e9 e9 93 9d 5b 12 b1 9a 5f 22 df db b1 ed 93 88 e4 a7 75 01 96 bb 8e 99 38 9e c6 f6 91 09 01 7b 56 ea 35 8e cb 1b 10 93 40 4c 7a ed 35 71 fa b1 1f 30 c5 d6 c3 5c 6a 60 5f d5 5f fa e3 16 5b ea 39 f6 c4 9f 4c dd 26 88 86 50 7d 1a ba 11 85 8f a0 c6 43 d0 d1 e3 22 f7 36 00 c8 f7 5d 5a 9f 14 ff 00 44 cd 64 e3 b8 76 11 a9 Data Ascii: 2E$;fxK4hp8`K0:E;`OM3<'z9&;!1BmBSQ`qY5O*.d[n -#iX<oG`'[_"u8{V5@Lz5q0\j`__[9L&P}C"6]ZDdv
2021-09-15 12:02:48 UTC	313	IN	Data Raw: 73 84 bc 30 00 c5 bb db 12 cb f4 cf 0e b7 48 14 0a a3 5f f7 ca 88 96 6d 4e 95 47 f9 5e ae 83 f6 fa 8c 05 60 8b 78 a1 7b 8f ed c5 9a 56 43 29 51 40 18 c0 bb 04 91 c8 ac 99 53 9a 87 58 a5 d0 d1 a2 01 6e 46 7e 5c 94 e1 e3 1e 22 63 bb 48 8c 04 75 b4 5a b5 0e 46 09 22 0d 18 05 89 66 52 8c 5b 9a ae a0 d6 35 f6 ef c6 5f 1f 7e 72 d5 fc ac 3d 43 71 9e 34 ba 19 1f e1 da c1 56 25 89 41 54 b5 f4 28 31 8c 0e 4c ba 27 2a 58 be 9e 4e 57 ee bd 33 51 a7 20 9f 05 e4 88 a2 b9 02 98 5b 8e 78 3c 8c 89 75 90 24 6c 64 d3 6a a4 d3 38 49 89 8d de ad 81 20 60 98 69 21 93 48 81 61 66 73 12 80 eb bc ca a0 16 1d 88 cd 44 f1 c1 24 71 8d aa 23 de d2 c4 b2 3e e2 41 3c 59 19 73 fc 2b 5c ba c8 a3 2f cc b1 48 76 36 04 f8 54 3e 24 9a 8f 0d aa 4d 42 8f 92 24 3d 8c 8d c1 c9 24 7d 4e ba 08 14 Data Ascii: s0H_mNG^`x{VC)Q@SXnF~\"cHuZF"fR[5_~r=Cq4V%AT(1L'*XNW3Q [x<u$ldj8l `i!HafsD$q#>A<Ys+\/Hv6 T>$MB$=$}N
2021-09-15 12:02:48 UTC	314	IN	Data Raw: a8 34 42 d6 d0 1b 19 75 2e ca ba 4d 1b 2e e7 b7 3e 95 7e 6c 07 52 18 4f a9 0a 36 a9 79 39 3e 87 a5 0c 78 95 5c 06 35 c2 96 e4 0b c2 c9 6b 28 7d a4 15 d8 28 83 f5 bc 5e 7a 2f 60 31 41 3c 37 a6 dc 3e 08 1b 46 a1 4f 99 6f 80 48 ee 31 07 9b 6b 15 e0 15 ae a3 01 91 63 05 1b a8 7c 64 63 76 17 8e 7a 85 3e d8 5a 3b 24 a0 e7 71 19 4c 63 21 62 63 46 87 01 00 ed 92 ac aa 7c ca 38 64 3d 48 e7 b1 ca 00 59 24 d5 65 73 7c f7 c2 6b 9a c0 43 0e 87 b1 c4 46 88 f9 9b 4e aa 14 f1 c7 38 65 85 68 34 d0 a6 f9 14 76 b5 25 6d b1 e7 9a 39 92 58 b5 f2 c6 b0 cb 0b 42 c1 c3 c6 01 62 1f 8a c8 a3 d5 a6 d8 f5 29 c7 0c 14 29 64 1d 90 f0 c7 21 95 95 49 f0 c8 b6 3b a1 77 8d b9 1d 03 a8 c2 ed aa ff 00 75 3c cd dc 99 3e 33 36 44 1a 14 1e 33 d0 00 b0 41 23 9a f6 07 a6 46 74 fa 60 65 d4 3c 7b Data Ascii: 4Bu.M.>~lRO6y9>x\5k(}(^z/`1A<7>FOoH1kc|dcvz>Z;$qLc!bcF\|8d=HY$es|kCFN8eh4v%m9XBb))d!!;wu<>36D3A#Ft`e<{
2021-09-15 12:02:48 UTC	316	IN	Data Raw: d3 68 6a c1 46 06 5d 46 de a7 b8 54 c1 14 4e e5 96 28 ce d2 4a f5 34 3b 00 3a 9c 01 1f 70 5a 17 5b 4d 01 8e 0f e5 e3 87 4e 1c d8 48 e3 fd b4 3b 9b 39 d5 80 a1 93 1d 33 87 7d 40 5e 69 54 72 e4 63 4a e4 96 00 0a 14 6d 87 98 d0 c6 52 a8 2c ab 6f 66 51 dc 13 4a a4 60 68 f6 3c 52 42 f4 ec 24 b0 ca e0 a7 93 70 18 18 ac 76 85 aa 83 a8 e3 04 70 c6 04 88 84 db 48 57 04 51 92 ce 84 9e 5a 85 d0 ae a7 23 93 c7 81 bc 58 c2 d9 88 ab f1 bb f0 64 f7 c0 40 26 88 c6 dc 38 2f d6 be a3 01 15 e5 27 e5 fe f9 1b 46 78 aa 52 d8 0b 6d b2 07 6b c2 a7 bf ae 6b 26 75 88 b4 8e a8 3c 25 ef 7d f8 c9 4e 98 93 a5 40 5c dc 6a f6 e1 17 d1 77 e4 be 31 8b e2 31 a2 55 8b 79 88 06 cf 71 8f ba 6f 82 c5 a4 70 16 f6 84 f3 33 0f 4b cb d0 c6 50 4c 79 5f 15 c7 98 22 90 7f ae 6d 40 02 a4 43 81 4a 38 Data Ascii: hjF]FTN(J4;:pZ[MNH;93}@^iTrcJmR,ofQJ`h<RB$pvpHWQZ#Xd@&8/'FxRmkk&u<%}N@\jw11Uyq op3KPLy_"m@CJ8
2021-09-15 12:02:48 UTC	317	IN	Data Raw: bf 98 af a9 94 11 9d bf 1e 48 e0 e7 14 4f 07 d3 2b 90 41 c0 eb 3b 04 3b b8 db b5 77 6e 1e a0 91 47 38 de a0 fd c6 02 bc 59 cd ce 91 3c c4 f6 42 01 51 f7 f4 ce 77 d9 fb 60 16 49 39 c7 73 82 cf 5c 17 59 c5 7f 8d f4 f6 39 c6 ee 73 a3 0e 7d b1 f6 02 88 19 79 da 65 ea 45 f7 03 19 19 fb 11 e5 2d d3 29 b7 51 1f 4c 57 52 76 23 2f 00 aa 0a a5 f6 ca a8 f9 27 9a e3 28 5e 71 d8 65 25 7f 84 79 3d bf 88 58 16 46 72 48 1f f7 ca de d5 7d f9 c8 9e 27 dd a8 33 8e 7a d8 01 c1 1d 42 8c 3c ed fa 0f 4c 1e 20 47 ba 35 b8 0e b8 02 29 6d d5 9d ba e5 93 83 00 43 c5 0c fa 8f f0 80 3f c3 6f 22 31 50 3f e5 ca 62 dd 3b 52 f1 9c 06 dc c4 70 42 af 2c 6f b7 1d f0 aa f9 77 2f 70 ee 01 09 ff 00 48 cb 3b 01 bf dd 46 b3 aa 94 4e 3f 77 27 0a 00 81 40 3f dc f3 9c ff 00 05 8e 2f 0a fb 1f f0 fb Data Ascii: HO+A;;wnG8Y<BQw`I9s\Y9s}yeE-)QLWRv#/'(^qe%y=XFrH}'3zB<L G5)mC?o"1P?b;RpB,ow/pH;FN?w'@?/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49783	172.67.69.19	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:39 UTC	11	OUT	GET /px.gif?ch=1&e=0.4888902266943189 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad-delivery.net Connection: Keep-Alive
2021-09-15 12:02:39 UTC	12	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:02:39 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34 sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Wed, 15 Sep 2021 12:06:43 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 3148 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\Va.nel.cloudflare.com\/report\Vv3?s=UCTzhcN9WH%2BoQ2BQvKkljNTwyrKPcT ZLwTTw5uaSTzgU96aJqNm1DG2raHYgbfduW%2BhFaZxPXNv6uTZZNStWde3eSXLv8%2B%2BZW6S%2FgD 31K%2F0uQU0HivGYsI0pbHuz96kHfA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 68f1b5166e12bf28-FRA
2021-09-15 12:02:39 UTC	13	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 Data Ascii: GIF89a!
2021-09-15 12:02:39 UTC	13	IN	Data Raw: f9 04 01 00 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49785	142.250.203.102	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:39 UTC	12	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad.doubleclick.net Connection: Keep-Alive
2021-09-15 12:02:39 UTC	13	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Wed, 15 Sep 2021 05:48:26 GMT Expires: Thu, 16 Sep 2021 05:48:26 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Cache-Control: public, max-age=86400 Age: 22453 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:39 UTC	14	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	18	IN	Data Raw: 35 e9 bc 0a 99 73 ff 00 d1 35 e2 ed d1 b5 ac 76 d4 e4 d5 d0 28 92 5a 62 b1 f4 3a 6e c7 57 b8 bd cf af b7 ae 23 9d 26 68 20 cc a5 ae 18 fe b8 7b 69 50 9c 42 6b 30 30 06 e5 eb b7 2e 9c 1e 31 61 89 02 9d 48 c1 83 5b d2 df 87 7f 5f d6 f7 c3 0c 1c b6 08 3b 17 1c c3 d3 db ef 73 0c b0 a8 39 c2 89 e6 7a 50 57 5f 7a 57 3a 25 0a 84 6f a7 50 ea 05 ed 63 fb fd db 0f a4 7d 26 b6 36 ad 3f 90 d6 fd 9b 54 8f a4 f0 52 7d 47 2f 48 e3 20 d5 a9 2d a8 01 70 3d c7 7f 7d bd 3f 2c 09 3f eb 57 31 f7 f7 eb a4 37 95 ff 00 65 3a 55 fc 5c c0 76 6c 96 7b 5c 8d cd c0 db 7f 35 ad fe b7 38 82 0b 97 fe bc be d0 3e 17 45 d9 87 40 7a ee 6f bd b6 ef 6b 0d b6 1f 96 35 51 21 2a 22 e1 24 8e 6d 48 9f 51 cc 7a fb 68 1d cd 73 48 f2 9a 5c cb 3f aa 99 52 9f 28 cb e5 75 5b 85 47 9c 23 2c 51 8e 8b aa Data Ascii: 5s5v(Zb:nW#&h {iPBk00.1aH[_;s9zPW_zW:%oPc}&6?TR}G/H -p=}?,?W17e:U\vl{\58>E@zok5Q!*"$mHQz hsH\?R(u[G#,Q
2021-09-15 12:02:48 UTC	20	IN	Data Raw: 78 f2 31 24 d4 d4 dc 37 47 3e a9 d8 66 52 48 ef 55 2a 35 92 24 24 9e 4e bf 55 5b a9 bf 5e d6 c0 2e b9 93 02 74 27 a5 eb 5b b9 d5 bd 40 11 2c c3 2e 58 24 d0 9a 37 2e 1e 75 da 07 21 a8 ae e2 3e 7c b0 99 63 c9 62 1a 56 18 83 46 ac eb ff 00 91 da 43 66 5d 36 b0 09 75 62 2e 77 3b 35 52 42 11 95 74 25 9d da a6 8a a8 fd d3 58 5e 14 a5 b8 48 74 93 b5 b5 e4 f6 f7 79 9a 5a 28 18 42 f5 35 34 b4 59 54 2c 26 aa aa aa 44 42 fb 01 a6 9c 5a f2 cc d6 50 d2 32 96 50 41 e8 46 17 e7 33 14 52 80 58 52 80 9a b9 70 1e e0 0d bc a0 99 69 01 b3 50 e9 5d 74 71 53 7f d5 29 1d dc 45 c4 70 d6 c9 4d 95 e4 b0 bc 94 7c b4 f9 5a 50 f6 8a 42 82 ed 5d 54 4d ae 15 43 05 47 d3 bb fd 30 4c ac 3a 0f d5 e7 b5 6c fa f3 0d 4d e0 49 d3 56 26 7f 8c 12 c4 9a 03 cb c6 fc 86 95 88 da 6c a2 b3 32 a2 ab Data Ascii: x1$7G>fRHU*5$$NU[^.t'[@,.X$7.u!>|cbVFCf]6ub.w;5RBt%X^HtyZ(B54YT,&DBZP2PAF3RXRpiP]tqS)EpM |ZPB]TMCG0L:IMIV&l2
2021-09-15 12:02:48 UTC	21	IN	Data Raw: 8d da 91 61 38 8e 7c af 80 f2 28 61 cd b3 33 16 5b 1c 8e 32 aa 83 5a 99 77 09 e4 d5 01 16 25 a7 cb e8 e2 75 a8 e2 1a a2 e0 f3 f3 1a b8 dc c9 26 a2 18 0e 88 65 f6 8c e9 b3 4f f8 8a 93 9b 28 6b 35 19 bd 97 e1 68 b5 cf ec d9 52 b0 d2 e5 4b 98 03 21 d8 dc 38 0f cf d9 8a cf c4 59 d6 5b 04 ae f4 71 43 c5 69 5b 4e 66 ab 15 52 54 51 c1 4d 03 37 39 a5 a4 8d 48 1a 1c 82 ba f6 2c 08 17 17 c3 d9 53 66 14 90 89 65 39 98 1d 89 60 dc b5 f3 3a 42 59 88 c3 49 0d 88 22 66 a8 e0 28 fe 6e 69 d7 84 75 37 8b b4 e7 26 8e 8b 35 ad 8f 20 ca 6b 39 94 19 57 0d e4 b1 48 8e 91 41 f6 6b 1c 74 79 51 f9 d9 6a 67 fb cf 33 b1 32 5c 79 b7 38 98 76 6e 23 10 a4 95 82 12 48 25 a9 4b 5a d6 76 e8 22 25 f6 9e 1e 4e 1d 5f 25 2c aa 03 47 bb f4 f5 d1 de 02 73 3a 7e 37 68 a5 8f 2b e1 2c cb 2c ca e5 Data Ascii: a8|(a3[2Zw%u&eO(k5hRK!8Y[qCi[NfRTQM79H,Sfe9`:BYI"f(niu7&5 k9WHAktyQjg32\y8vn#H%KZv"%N_%, Gs:~7h+,,
2021-09-15 12:02:48 UTC	22	IN	Data Raw: e6 2a 9d 20 82 33 23 33 58 ed 7b 0b 81 e9 b9 df 1e 42 40 59 a7 74 33 0b d4 ec 36 7f 37 88 a7 4d 48 4d 00 72 2b bf 8b d2 83 dd a1 fb e1 97 85 cf 9d cc ad 52 0f 9b 7d 0c 83 62 76 1b 9e d6 b1 1e 87 f1 c3 5c 3e 52 41 60 08 61 a0 34 ad 0f ea e7 c6 b1 da 13 96 25 cc 65 10 18 91 c5 85 ba 6b e2 62 ee f0 37 c3 ec 61 d6 64 89 09 8f 4b 01 a2 ca c2 c0 d8 5a d7 3b 7a 9b 7a 77 16 5c 34 a7 67 4b bb 69 c5 88 27 ab 37 f1 1f 39 7c 79 da 33 91 26 6a 42 97 75 80 c4 86 a3 1e 65 9b d7 89 bd 1e 19 f0 15 36 51 0c 6a d1 68 60 74 c8 34 db 4d fd 6c 7a 03 b0 1f e9 87 32 b0 99 66 05 04 b5 0e 9e dc d6 3e 71 c6 cf 5c e5 94 ce 75 82 f4 59 7e 83 5a 5c 72 8b 5d c3 f9 11 7e 4b 84 02 24 b2 b2 da f7 07 7b 77 b8 b8 17 b6 2d d8 0c 1a e6 84 66 05 49 0a 49 2e 1c 16 d1 83 0f 3f d0 72 24 85 a9 29 Data Ascii: * 3#3X{B@Yt367MHMr+R}bv\>RA`a4%ekb7adKZ;zzw\4gKi'79|y3&jBue6Qjh`t4Mlz2f>q\uY~Z\r]~K${w-fII.?r$)
2021-09-15 12:02:48 UTC	23	IN	Data Raw: 90 c1 49 54 fa 92 92 9a 99 22 25 9e 35 3a 7e d9 8f 94 ea 37 ef 7c 37 44 81 84 22 51 ef 12 96 cc 5e 84 75 a1 a0 bd 19 f4 84 2a 9d f3 a6 09 a9 a4 bb 30 e6 de ec 20 92 8a 0a 11 14 95 d0 28 9e ba 28 da 38 2b 26 17 86 81 22 04 f3 a0 a6 d5 e4 9a 42 2e 2a d9 48 07 76 6b 0b 60 65 ce 5a 66 7f 6e 90 42 bf d8 6a 52 58 17 a3 b7 37 3c af 04 2a 52 14 12 54 dd da b9 7f ce 9e 71 0f 35 54 92 73 5a 6a a3 cb 59 15 52 7d 43 5a 3f 31 50 b0 3d 6c 6e 3b e2 14 e1 d5 31 65 c1 ef 3b 83 4e 5b fb e8 fe 13 be 5d 8b ea 1a b6 d5 be dc 47 5c 17 a0 97 36 cf 67 a6 09 a1 12 62 b1 54 be d1 c5 4c 00 33 57 cb b8 b4 64 ec f6 b5 da d7 de f7 61 9e 5c 84 65 0c 49 01 ee f4 a7 27 a3 8f 0b d8 79 68 99 3d 65 41 db 33 ec 29 f8 6d 8f 08 2a 9c cd 49 78 20 95 6e da 20 59 18 03 ad 57 ca 8e bb 02 23 98 9b Data Ascii: IT"%5:~7|7D"Q^u*0 ((8+&"B.*Hvk`eZfnBjRX7<*RTq5TsZjYR}CZ?1P=ln;1e;N[]G\6gbTL3Wda\eI'yh=eA3)m*Ix n YW#
2021-09-15 12:02:48 UTC	25	IN	Data Raw: b7 c3 3e 23 cf 6a 6a 1a 1a a7 cb 9d dd c4 fa 14 3e 64 94 80 fd a1 7a 8d 5c 9a 38 67 5b e9 31 96 76 1b f9 48 c6 b3 31 29 4a 54 84 b0 53 51 8d 43 b5 b4 b6 8d ad 08 35 8d e5 61 e6 2c ba 49 15 a9 0f f8 e9 d6 2f ef 03 64 5c 31 90 70 f1 ca 29 61 ca e4 cb de 54 fe 73 98 4c f2 cb 50 fa 2c 1e 16 d4 c4 d4 54 b3 f9 94 bc 9a 19 43 b7 de b5 d3 cc 99 36 71 5a 73 a9 00 02 c5 c8 d0 dc b3 bb de 1c a2 42 54 80 9a 38 fa 9c 1a b7 bf e6 2c be 47 4b 5f 5d c3 d2 66 d9 4d 0d 1e 49 c1 d4 d0 ac 35 9c 53 9e cf 1d 0e 55 14 34 fe 58 dc eb 96 39 2a 82 1d d6 8e 90 b4 53 3d 92 49 6d 85 12 e7 ce 28 23 bc a4 8a 0d 7c 4e bd 08 1e 30 c6 44 a9 60 00 54 94 d6 84 8b 0b 37 b7 7b 88 5f e7 5f 11 5c 29 90 88 b8 73 c3 5c ba be bb 37 9e 17 39 c7 19 67 7a 6a e4 ae 99 5b 92 a7 2b a5 56 d5 1d 07 9a f4 Data Ascii: >#jj>dz\8g[1vH1)JTSQC5a,I/d\1p)aTsLP,TC6qZsBT8,GK_]fMI5SU4X9*S=Im(#|N0D`T7{__\)s\79gzj[+V
2021-09-15 12:02:48 UTC	26	IN	Data Raw: c3 df 17 bc 3a b2 7c a7 47 97 4d c6 8b ea f5 eb df f7 eb 84 78 a5 3a c0 d9 fc 4b 1f bc 34 92 82 b5 39 15 5d 0f eb 5b 3b f9 41 bd 1e 5c 63 e5 01 18 f3 7a 8d f6 3d 77 3e 9d 8f e1 85 b3 14 41 d2 e4 7b fb c5 9b 01 20 cb 48 00 55 d9 8f 5a 58 7f 10 c4 c9 f2 d6 69 23 3a 2d e6 1b 80 3a 7b 9b ef be f6 f7 38 5c b5 e5 aa cf 97 bd e2 d3 86 40 29 7a 8a 57 4d a9 67 f7 48 6d e5 79 7e 8d 27 4e e4 8b ed b0 b7 e3 6f a6 db 8b 5a f8 4b 8c 9a 95 96 15 16 e2 c2 dc 77 f3 7d 21 de 16 5a 52 01 b1 29 73 5d 4f 46 b1 dc 0b 54 34 1c 51 53 46 b2 6a 23 ad 8f 4e dd 3d 7f 7f 9e 01 1b 69 b9 35 3e fe db 41 95 b1 d1 e9 66 d7 6b 70 7f b4 15 53 94 36 1d 80 f7 f7 bf ef fd f1 1a 40 72 6b dd b7 ec 74 fc 46 38 f2 6d 7d db ed 13 54 f2 2a a9 1f e9 f8 62 4d 7d fb d2 3d 7d 6a 79 fb f5 bc 73 95 d4 d8 Data Ascii: :|GMx:K49][;A\cz=w>A{ HUZXi#:-:{8\@)zWMgHmy~'NoZKw}!ZR)s]OFT4QSFj#N=i5>AfkpS6@rktF8m}T*b M}=}jys
2021-09-15 12:02:48 UTC	27	IN	Data Raw: 4a 94 32 3e 96 3e 36 0d ef 8c 15 d1 c2 b9 28 92 8f 2a 6c aa a6 8a 38 d0 55 d6 f3 64 26 5a e8 6c df 62 02 59 59 9a 46 d6 12 c0 8f 2d ad 71 81 a6 cc 49 26 aa 70 da 8d ac f7 b6 8d a4 31 12 94 51 29 5b 24 72 7d d9 c3 5e 25 65 39 7d 15 03 57 d5 c9 14 70 20 9e 48 f9 48 c6 9d 1d 2c 23 87 91 26 e7 96 49 23 97 71 dd ae 49 c0 bf 29 58 89 80 24 1c a1 a8 2e 5a 97 a7 93 71 da 09 33 a5 48 94 4c c2 42 c7 1b f4 b9 e3 af 2a c2 ae bb 33 ff 00 a8 e7 4c be 95 64 34 fa 89 ae a8 91 98 2d 43 8b f2 98 95 22 d1 46 37 10 9b 45 d9 94 ef 77 92 64 2e 44 b2 c0 7c c2 d9 1d 89 b5 46 95 b3 35 75 8a f4 dc 5f f7 5f 3d 1f e8 08 05 80 70 0e a0 d8 5b 5f d4 65 66 d5 34 4a 29 f2 5a 20 82 06 91 39 91 c0 8a a9 cf 36 42 c4 47 6b 2d 81 3a 56 ca 4f ae d8 d0 29 69 39 a7 d4 a1 8a 45 bb c3 e9 73 7e 62 Data Ascii: J2>>6(*l8Ud&ZlbYYF-qI&p1Q)[$r}^%e9}Wp HH,#&I#qI)X$.Zq3HLB*3Ld4-C"F7Ewd.D|F5u__=p[_ef4J)Z 96BGk-:VO)i9Es~b
2021-09-15 12:02:48 UTC	28	IN	Data Raw: 52 8b 12 1d cd 9c b1 66 66 e1 60 34 89 e5 4a 54 b0 04 ca a4 59 dc 28 80 05 4e e5 ae 3a ee f9 f4 d9 a0 a6 a6 f9 0c 96 08 69 90 b7 da 00 52 69 a7 60 6c d2 d6 54 d8 87 94 b5 d9 c1 90 d8 9b 2b 60 74 2d 53 65 82 a7 0e 68 35 bd 0d 40 3c 03 0f b3 95 f3 01 ff 00 b6 00 4e 97 3c 4e dd 2a 6f 12 99 45 06 65 5a f3 41 0c 95 03 e6 5d 3e 76 55 51 24 b3 06 3b d2 44 c0 31 58 06 fa 6f d6 e4 93 d3 12 21 29 cc 01 b8 b3 d0 07 7b b7 4a 6e 78 44 f2 b3 cc 4a a8 28 46 fe f6 a7 38 b3 dc 01 c1 d4 e2 3a 74 cc 22 4a 5a 74 32 0a f9 15 a3 86 a9 69 91 41 30 73 d6 cf 1c 8c 2c 74 40 47 dd eb 72 6e 3e 22 71 49 00 33 16 14 72 7e db d6 96 86 12 a4 92 9d 29 43 bb 37 96 db 78 45 8b c8 78 93 26 c8 68 60 7c 8a 37 a6 c9 68 a6 62 f1 d5 4d a6 4a b2 1c a3 c2 a8 d7 92 a6 59 48 d2 79 84 d8 b5 c0 04 ee Data Ascii: Rff`4JTY(N:iRi`lT+`t-Seh5@<N<N*oEeZA]>vUQ$;D1Xo!){JnxDJ(F8:t"JZt2iA0s,t@Grn>"qI3r~)C7xEx &h`|7hbMJYHy

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	30	IN	Data Raw: 6c b5 a2 d6 e1 4f 3b 8d 9a 20 e6 8c 99 2f 63 bd ef ed 6e 98 c8 5b 96 66 eb fa 80 4a 14 e6 95 73 c9 f8 78 c4 b6 53 44 cd 3a ed 61 6d 46 f6 bd 8d 88 23 d0 f4 f7 c6 d7 70 d4 f5 f2 fc c6 f2 41 44 d2 e1 f4 20 d1 9f 8e ae 34 e3 d2 1c 9c 3d 96 92 ea ba 7c a7 47 61 7b 96 f5 37 b5 fd 31 1f cc 2f f4 d1 aa 5f f5 c3 ce 1a 4a 09 b9 0c 45 81 be af c7 f9 f0 b1 9c 33 94 8e 5a 59 2e bb 6e 45 89 20 db 6e a7 d4 7e f6 12 7c cc aa 24 80 03 37 ff 00 66 e9 ae ff 00 c9 32 d0 a5 4c 0c 28 c5 ba f1 6f 7c 21 bd 97 50 88 82 9b 75 db 7b 9d 22 c6 f6 1f af 6e f8 4b 88 98 92 a0 5e 9f 8f 67 94 58 30 48 01 52 f3 55 9b 4e 6d 6d be ef 06 34 14 88 2c 64 5d af 75 b1 bd af 6f 6d bb de df db 0a 67 4d 75 10 90 f7 ad 1e bb 72 bd fd 22 dd 86 97 dc 74 8c c7 80 76 1c 3a f0 a6 b0 77 94 42 1a 58 d0 0b Data Ascii: IO; /cn[fJsxSD:amF#pAD 4=|Ga{71/_JE3ZY.nE n~|$7f2L(o|!Pu{"nK^gX0HRUNmm4,d]uomgMur"tv:wBX
2021-09-15 12:02:48 UTC	31	IN	Data Raw: b5 5e 95 6a 01 50 75 d6 bb 34 40 65 02 07 78 13 c8 bf da 03 33 cc da 8a 2a 5e 59 d3 04 54 c8 4d 85 f4 37 2f 64 5b de fc fa 83 e6 50 08 d4 a0 9e bb 12 30 80 cf 9c 90 c4 77 98 9e 00 1b 53 d2 c3 a4 05 8d 08 95 87 9b be 4a 37 4b 54 d7 f5 0b fc 9b 2c 6a 9e 6e 6d 9a b9 a1 96 b6 46 7e 44 83 4d 4c 19 6a 58 ea 66 6b e9 79 81 22 22 0e cc 0d c5 f0 f2 62 90 86 96 3b cc 3e a0 58 39 bb 06 e4 39 57 61 15 f9 68 98 b3 99 8e a4 bd 40 be b5 67 7e b1 39 4c b5 75 d3 8c c5 21 14 f4 51 5e 97 2b 88 82 a5 8e e8 b3 d4 1b 83 cd 11 96 72 7e e9 02 e0 06 ea ba 72 81 4b 0b e8 7d e9 05 e1 41 7e f5 6e 6c c0 6a dd 6e fa f8 c1 25 25 29 82 9a 47 11 a0 a7 a7 9a 28 a8 b5 b3 73 2b ab 4b 16 9a b9 54 9f ff 00 37 8c 6e c4 8b 32 82 2f b0 c0 3f 25 2e e5 4e 4e fb fd db 6a c3 41 3b 20 b5 2c 3f 54 e0 Data Ascii: ^jPu4@ex3*^YTM7/d[P0wSJ7KT,jnmF~DMLjXfky""b;>X99Wah@g~9Lu!Q^+r~rK}A~nljn%%)G(s+KT7n2/?%. NNjA; ,?T
2021-09-15 12:02:48 UTC	32	IN	Data Raw: 4b 21 ce 42 d9 94 01 20 54 69 4d 78 d7 48 c9 c9 e9 73 aa 89 25 ca b2 4a 2a da 8a 89 a6 0d 59 51 5f 4c 56 38 49 00 34 a1 22 55 be 8e 91 aa 00 34 81 aa e4 13 81 26 4d 94 95 66 56 52 00 7c a1 9c b3 52 ae 12 f7 75 39 ad 05 62 7c 24 b5 4f 48 f9 61 44 1a 92 cc 18 fa df 4d eb 47 83 88 f8 5a 1e 1e 93 5d 4d 52 7f 30 6a 64 7a ac e2 4f fb aa b7 56 7e 58 a5 a0 89 9d 56 93 51 d2 02 84 04 11 7d 8e f8 5f 8b c5 19 c9 02 59 08 94 1d 90 08 da 84 90 cf 42 5c 11 c2 82 1b ca c0 fc 95 66 2a be d5 e9 d7 c7 98 8c 9c a7 24 cd b3 ec ce 87 24 80 35 30 cd 33 05 85 ab 2a 66 34 ad e7 1a c1 aa a9 62 59 5d a2 4b 2a 86 d2 3d 77 c4 32 12 c0 15 31 7a b5 05 eb 5d 5d 89 1c f9 d2 49 eb 74 9d 91 e2 5a 9a 78 8b b0 31 37 99 e5 34 90 49 98 c7 1d 6d 16 4d 90 64 f2 c9 4d 57 55 af 4c d9 9c f4 cc 22 Data Ascii: K!B TiMxHs%J*YQ_LV8I4"U4&MfVR|Ru9b|$OHaDMGZ]MR0jdzOV~XVQ}_YB\f*$$503*f4bY]K*=w21z]]ItZx1 74ImMdMWUL"
2021-09-15 12:02:48 UTC	34	IN	Data Raw: 69 6a 1a f4 7a 44 e9 5a 9c 81 40 3d fb e5 15 4f 8f 2a 52 5f 98 f3 5c 15 6e 96 1d 0d 88 e9 ed eb bf a8 c6 64 25 c9 2a 6c bc 9c fb 77 df 94 6f 9d 44 55 83 f9 70 8a 43 e2 09 12 34 ba 6d e5 04 6d ef b1 ed bf 53 df f5 38 77 86 b5 bf d9 3f a1 e5 08 b1 af 51 fe a5 24 f2 f5 d0 81 7e 71 51 b8 8a 3d 32 be e5 89 77 d8 81 ff 00 b7 ef 6e bd 3d 86 1e c9 70 c5 2d 77 e0 05 3f 96 8a 27 68 87 50 20 53 39 07 6b 5f 57 1f 76 81 ae 58 eb d2 fb f5 51 6b fb 76 b7 e9 86 48 52 4a 92 03 b9 7b 8d 5a dd 74 84 38 84 82 a0 18 54 90 39 70 d1 8d 6f 4e b4 8e 40 11 b0 df 6f 63 b7 a6 c3 6f ef 89 e0 15 4a 48 23 d7 f9 76 e1 1f 0a ea d8 9d ad ec 3f 53 fe 31 ae 74 ef ef c3 ef 01 e2 0f 74 9c a1 bd 3f 9d 7d 88 c6 6a 29 1d ee 97 b1 b9 04 0b ed fd 8f 6f c7 1b a4 87 07 4f c8 85 25 65 cb 01 4a 7d b8 Data Ascii: ijzDZ@=O*R_\nd%*lwoDUpC4mmS8w?Q$~qQ=2wn=p-w?'hP S9k_WvXQkvHRJ{Zt8T9poN@ocoJH#v? S1tt?}j)oO%eJ}
2021-09-15 12:02:48 UTC	35	IN	Data Raw: 2d 56 28 19 8b 93 47 d8 07 35 3c af 60 a6 76 54 e9 28 ff 00 17 f9 13 a3 1a b0 17 e9 6d fe e1 99 d1 63 54 9a 4d d9 45 d0 5a c5 c8 17 d7 63 b9 51 6b fa 58 0c 5b 27 4f 95 f2 c2 a5 2c 28 a8 3a 72 97 d8 f2 14 e5 b4 45 21 0b 96 40 5a 54 08 a5 8d 1d 80 e5 58 43 71 8e 63 2e 5f 92 71 06 7d e5 5a c3 0c b9 75 14 c0 94 26 aa ad 84 2a 8a 47 dd b8 26 e1 7c db 1b 1c 27 c5 62 32 8a bb 97 1b d4 f1 fb 6d e1 0f 30 72 54 a9 9f 2d 39 73 11 98 56 8c d5 73 a7 9c 51 1f 1e b8 e6 ab 2a e0 d5 e0 cc 96 b6 1a 0c cf 34 a6 7a 39 26 70 8f 5b 1d 0c f4 e1 eb dc 33 11 64 56 e6 59 89 b9 bf 53 8a c7 6c e2 49 c3 94 85 30 1b 10 29 ae db 35 99 ba 18 bd f6 0f 67 11 89 95 34 80 a0 82 1c bb 96 7d 07 42 cd e0 d1 e3 0f f8 9b 78 b7 4d 9c 66 b1 f0 16 49 55 cf cb e8 6b 65 4a b9 80 eb 4b 48 1a 2a 89 65 Data Ascii: -V(G5<`vT(mcTMEZcQkX['O,(:rE!@ZTXCqc._q}Zu&*G&|'b2m0rT-9sVsQ*4z9&p[3dVYSlI0)5g4}BxMfIUke JKH*e
2021-09-15 12:02:48 UTC	36	IN	Data Raw: a1 d8 5b d6 f0 43 53 2d 25 30 87 24 a4 65 82 8a 8f 9b 25 58 44 d7 2d 45 53 20 0e f2 cc 2e 82 2d 81 01 ac 17 56 db ed 80 92 93 3c 92 b3 4b df 41 56 00 87 3d 76 20 bd 58 fc a1 09 ff 00 c9 89 22 9a e8 7a e9 ec c6 31 92 a2 58 a8 d6 98 b8 91 8b c3 4b 1b 21 8c c6 01 2b 35 7c ab bc 49 b9 31 a2 75 61 b8 c4 f2 e5 26 5a f3 30 6e 84 8d 29 cb d3 a4 62 5a 8a ee c0 8f b3 83 c3 d2 f7 11 90 02 c2 64 a7 a6 07 5a ab 1a ea c6 b2 c6 42 75 89 18 ec 56 21 7b d8 ea 6d c9 3d 4e 35 9f 2e 62 fb a0 33 d4 80 77 de b6 e1 d2 ec 23 54 cc 19 8e 60 e4 12 05 9d 85 3a 0d 1a b4 d6 23 b8 8f 34 89 ea 63 a5 cb aa 44 54 d5 14 14 71 3c c2 37 92 7a a9 42 b9 7a 78 02 7f e3 8d b6 56 91 01 6b 10 46 0a c0 48 4e 1d 0f 30 3b b9 2d 56 1a 3b 3e b5 3d 04 2f c6 4e 0a 9e 96 72 90 d6 14 6e 1b b7 07 e1 1c 32 Data Ascii: [CS-%0$e%XD-ES .-V<KAV=v X"z1XK!+5|I1ua&Z0n)bZdZBuV!{m=N5.b3w#T`:#4cDTq<7zBzxVkFHN0;-V;> =/Nrn2
2021-09-15 12:02:48 UTC	37	IN	Data Raw: 9b 62 4f ed b0 d2 9c ad 28 01 3a 38 7e 36 a7 ba 9a c4 a8 99 3a 70 ca 90 49 d0 87 a0 7b ab af 8f 46 36 ab 80 3e 19 b8 ef 3f 8a 96 ab 89 eb a1 c8 72 58 80 9c 64 30 7d 8d 45 56 db a2 c5 19 6d 09 db ed 2f b1 ec 46 15 e3 31 f8 20 e2 50 2e ec 19 24 b1 1a 3f 1d 5b 68 b2 60 3b 32 72 90 0a c3 29 4d 50 5f 90 a5 6a fe 55 8d 82 f8 71 e1 bc 74 89 4d 91 64 79 74 1c 33 1c 0a 05 4c 99 5d 1b 55 d4 56 29 55 1a 9e 5b 68 8d ed bb 5e c4 12 49 dc 9c 21 9f 8b 50 2a 75 77 4b da f4 d8 07 a7 1e 71 6a c2 f6 0a 92 07 cc 70 14 db 91 5a 07 3e 47 9c 5f 7f 08 fc 16 8a 9a 78 b3 29 32 7c ba a6 49 15 21 86 af 34 8e 6a 8a a4 65 dc cc a8 96 b4 bd c2 a9 d2 1b db 63 0c b9 d9 c5 0f 97 52 ee 3d 77 68 92 6e 1e 5e 1c e4 a0 cb 4b d3 c6 de f4 8d 82 70 9f 01 e5 39 7e 5f 1c 53 a4 59 9d 6c 91 ac 8f 2d Data Ascii: bO(:8~6:pI{F6>?rXd0}EVm/F1 P.$?[h`;2r)MP_jUqtMdyt3L]UV)U[h^!P*uwKqjpZ>G_x)2|I!4jecR=whn^Kp9~_SYl-
2021-09-15 12:02:48 UTC	39	IN	Data Raw: fe 9f 86 07 9f 2d 4b 09 52 55 95 52 d5 98 01 75 59 d9 ae c3 86 b1 82 85 2a 7a 42 58 a6 a1 4e cc 5f 6f 23 ce 2f cf 80 9c 53 fc d7 83 a9 68 a6 90 c9 35 1c d2 c5 1e a7 d6 fc 84 0a 89 e5 0b ab 77 2d 61 7e 82 f7 27 1d 8f e1 2c 68 c4 f6 72 24 e7 49 9a 80 01 75 31 48 0c ee 0e e3 76 67 b4 7c 97 fd 54 ec 55 76 77 c4 13 b1 29 46 49 73 98 90 03 66 5a 8a a9 4e 42 bf c4 38 73 5e 23 ca 32 65 be 65 5d 4d 4a 74 16 09 24 ab cc 36 da da 06 e0 df b3 75 24 7d 70 c7 b6 3b 7f b1 fb 19 39 fb 43 15 2a 5b 02 58 a9 20 96 b8 0e 5c 93 a5 3a 1b 47 3f c1 76 4f 69 f6 8f ff 00 b2 e1 a7 4c 04 84 85 26 59 28 73 67 56 83 72 f0 92 e2 ef 17 2a a7 22 8f 84 63 42 14 4c b5 15 95 28 ca 24 0e 96 8c d2 14 75 2a 51 8e a7 2c 2c 54 dd 0d c6 38 df c4 7f d5 bf 98 a3 86 ec 02 12 0d 3e 72 88 63 66 2e 1a Data Ascii: -KRURuY*zBXN_o#/Sh5w-a~',hr$lu1Hvg|TUvw)FIsfZNB8s^#2ee]MJt$6u$}p;9C*[X \:G?vOiL&Y(sgVr*" cBL($u*Q,,T8>rcf.
2021-09-15 12:02:48 UTC	40	IN	Data Raw: 0d 2d 4f 6f ca 39 e4 77 8e a6 7c d1 1f 93 47 47 48 d2 cc bb 59 e5 b3 05 8d 07 a0 04 5c 7a 9b 5a c3 1a 63 0b fc b4 33 8e f3 8d 80 dc 6f b7 26 77 ac 11 84 09 4a 94 b2 58 7f cb 4a 51 9f c9 f6 a8 bc 75 65 33 49 56 d5 d9 a5 51 bd e7 43 4e cc 0b 00 8c 49 08 a2 fd ba 79 76 07 f0 c4 2b 52 25 cb 12 53 dd 2e ea 72 c5 c6 dc ac 79 ea 1a 35 42 16 b9 ab 98 a2 4a 33 79 ea 74 b9 b7 88 89 ea da bc 81 a9 35 56 e5 35 94 15 85 49 5a ea 2a cd 54 c4 9b 5a 39 e8 dc b4 d2 4d eb 1a 0b 11 e5 04 31 c4 49 41 51 77 a5 28 69 4d dc 86 a5 dd c3 72 83 94 a4 b2 42 43 b6 c2 cd f8 22 be 31 8b 3c 39 5a 65 ca e2 be 59 63 a6 60 9f 28 69 d9 7e 72 ad 88 2b 12 ad d9 89 01 94 9d ba 9d 36 f2 9c 46 97 54 cc a1 24 86 16 34 fb 54 8f e6 34 3c 45 e9 cf dd 7f 31 97 1d 2d 3e 44 af 9b 66 75 b0 cf 99 4d 14 Data Ascii: -Oo9w|GGHY\zZc3o&wJXJQue3lVQCNlyv+R%S.ry5BJ3yt5V5IZ*TZ9M1IAQw(iMrBC"1<9ZeYc`(i~r+6FT$4T4 <E1->DfuM

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	41	IN	Data Raw: 95 f9 fd 46 77 58 ed cf a8 aa 9e a4 94 2b 1d d8 22 b1 b8 5a 7d fc 81 56 c2 fd ac 06 36 12 ca 1c 9a b8 6e 46 ff 00 63 f6 37 80 d5 34 cf 3f 2d 23 28 15 73 b5 be fd 06 b5 60 67 96 d1 d2 e4 10 c5 5b 98 ab 88 a1 89 9d a9 60 5e 65 64 c6 d7 1c e9 83 39 01 b7 b0 0b aa f7 18 18 a8 aa 68 96 06 5c c5 9e a0 01 b6 c2 a1 af 48 9e b2 52 4a 46 76 1d e4 80 ee 76 cb e5 c1 89 82 8e 11 cc 7c 43 e3 bc c6 d9 6a cd c2 7c 13 4d 28 8d ea 60 81 a2 ae aa 47 52 ba 50 4a 44 cd a9 49 b1 5b 2e f7 0a 48 c1 38 89 12 e5 4a 0a cc 14 b5 5d 88 66 e6 1c a8 9d 19 92 37 50 88 25 cc c4 4f 9a 46 45 4b 40 ad 88 d7 8b 7d b5 06 d1 63 aa b2 6a 2c 97 2d a7 ca a9 f3 98 78 7e 9e 70 25 cd 2b e6 ff 00 b9 ce 73 03 bb 79 02 1d 6a d3 6c 2c e5 c0 3d 53 6b e3 59 53 90 81 91 41 c7 10 43 31 d1 fc 3f 2d 0c d1 20 Data Ascii: FwX+"Z}V6nFc74?-#(s`g[`^ed9h\HRJFvv|Cj|M(`GRPJDl[.H8J]f7P%OFEK@}cj,-x~p%+syjl,=SkYSAC1?-
2021-09-15 12:02:48 UTC	42	IN	Data Raw: 1f e1 25 cb cb 40 38 8d a9 e6 49 bf d9 a2 7e 84 c9 70 06 d6 b1 df eb db d4 f5 eb d2 ff 00 5c 0e 94 cc 0d 9d f5 77 b1 f7 f9 86 45 32 c0 19 3d 1a 9f af 7b c1 bd 14 df d2 49 b0 db f4 db f5 fe fb e2 41 c2 d1 19 48 3b fb f7 e4 36 82 18 bc c0 5b d7 6b fd 31 b0 08 3f 50 0f d6 d1 a2 85 58 0d 3e e7 68 93 a5 89 d9 90 0b 58 f5 eb fa 7e bf a6 db db 1e 21 03 e9 0d bf da 35 ca 0f d4 3a f8 f9 bf a1 a8 bc 1e 65 14 6a 63 02 c4 9b 8e c4 6c 40 ff 00 7e ff 00 8e 30 01 25 b4 bb ed ee 8c dc 5e 21 5e 59 67 32 80 23 29 00 e8 6a da 68 fc 2a 6a d0 d9 c8 32 e6 75 56 55 e8 46 e4 7a b7 f8 03 f6 30 4a 09 4b 0d 28 1b c9 e2 bd 8c 9a 4c c2 45 b6 a1 61 a9 f5 f5 87 56 43 97 15 68 8e 95 23 76 df a8 1b 7a 8d ef 63 bf e5 86 98 74 da 96 f6 de 27 f6 62 bb 8e 5b 5c 71 e0 75 f7 7e 30 fd e1 9a 60 Data Ascii: %@8I~p\wE2={IAH;6[k1?PX>hX~!5:ejcl@~0%^!^Yg2#)jh*j2uVUFz0JK(LEaVCh#vzct'b[\qu~0`
2021-09-15 12:02:48 UTC	44	IN	Data Raw: 00 55 6a 32 c9 7d 46 8c fb 79 f1 d7 68 16 ce 59 ab 73 69 79 51 2a 40 a9 35 24 6c c0 8d 71 6a 0f 23 83 be d7 16 da d6 e9 d3 10 aa 60 4a d0 93 fe de 34 21 fd ef 05 25 2c 92 75 46 db 1a 9d ad f6 da 14 99 d4 e7 3c ce 86 5b 19 bd 1c 6c 91 46 14 79 47 29 98 3b 3b 76 53 a4 db d4 91 f5 c5 86 40 4c 8c 3f f7 09 00 10 45 39 87 eb cc 8f b9 84 b3 d4 31 13 8c b5 58 86 0f 6a 7b ad 4e b4 d2 39 d2 46 95 19 9c a8 19 4d 3d 3a 3c 10 85 be 99 4c 20 16 8e e6 ca 2c fb 6d d4 5e dd f1 b2 a6 94 27 e7 1b cd a5 78 da 97 fb 69 48 ca 25 a1 44 c9 4b 3c ad 34 da f7 e3 c7 d5 84 6a 16 8b 2b 7a b6 80 24 a9 ca 8a 9a 31 6f b5 af aa 21 0c 57 3d 63 8d 6c c0 ee 05 9c ec 37 c0 d2 0f cc 9a a3 f6 de 9e f8 78 41 4a 4e 54 74 3c ac 2d d4 9e b0 31 44 cc d0 54 4c d2 a9 49 65 92 86 9a 53 71 cd 26 60 6a Data Ascii: Uj2}FyhYsiyQ*@5$lqj#`J4!%,uF<[lFyG);;vS@L?E91Xj{N9FM=:<L ,m^'xiH%DK<4j+z$1o!W=cl7xAJNTt<-1DTLIeSq&`j
2021-09-15 12:02:48 UTC	45	IN	Data Raw: 4e 25 eb 6e 9c b8 ef 19 79 63 a9 9c 33 02 c5 0d c5 1c 6a 5a 38 6d 73 79 6a 88 17 17 b0 b0 be fb 12 31 1e 24 a9 1f 42 46 60 01 00 6b a1 ea c4 fb a0 c6 15 25 48 5e 95 b9 24 ea 1b a6 bd 6d 48 cf aa ab 48 e6 53 5f 54 6b 24 89 89 a7 a2 0a ac 80 93 7d 25 41 b3 90 08 17 61 6d be b8 1d 2b c4 2a 86 50 ad 2a 45 06 fa 73 d7 4d e3 d3 17 94 10 e1 eb ae db 73 a3 41 0e 4b 5d 2d 3d 5d 16 75 5b 34 d0 c1 4d 53 14 94 74 22 7b 49 55 52 8c 10 09 8a df 4c 31 c5 70 a8 a0 29 53 63 8c e7 f9 6e 95 d7 47 d3 9b f0 e2 1e da 9a ef 25 00 f7 ec 0d 5f 5a 0d 7c 9f 66 a4 7d e2 8e 21 ac cd 73 69 29 29 03 cf 2c 21 da 08 e3 46 e4 c6 95 45 5a a1 96 ca 42 c8 35 a8 d6 4f 40 6f 89 54 10 50 fa 1a e9 b5 35 ad 2a 76 89 40 5c c2 40 55 09 60 6d 4d ba 0f 62 3b 26 9b 2f e1 18 69 a4 e6 0c cf 3e aa 8d 6a Data Ascii: N%nyc3jZ8msyj1$BF`k%H^$mHHS_Tk$}%Aam+*P*EsMsAK]-=]u[4MSt"{IURL1p)ScnG%_Z|f}!si)),!FEZB5O @oTP5*v@\@U`mMb;&/i>j
2021-09-15 12:02:48 UTC	46	IN	Data Raw: eb fe fb 60 a9 61 8f 4f bc 05 37 6d 95 b3 69 ee ba f8 44 3c 51 8d 66 e7 6d 47 fb 8d 8e df 4f a9 c4 d0 1c d4 92 09 04 d8 d1 e9 6d bd b6 ae 20 ae 82 9c 3e 92 3a 0d cf 6f 4d ff 00 5d ad f4 db 1e 84 98 89 0a 4a b3 17 6b de 8e 35 e3 e2 fb de 08 85 32 d8 90 2e 1a dd b6 f5 db bf ec 5f 07 61 d6 0b e8 7f 8e 1e dd a1 34 ff 00 ad b6 27 9e 97 3a c1 16 53 45 e7 24 28 b6 dd 3a 0f 62 2f 70 7e 9d 36 be 0f ee 90 1f 5a ea 2a 05 79 b4 05 33 ba b6 3a 9a 75 f7 fa 68 62 65 74 91 f3 23 bd f5 12 a1 6c 0f 50 c0 5b fb 6d f5 c0 78 95 0a b6 a2 9a 56 f6 37 89 a4 25 cc d0 aa f7 1d 88 04 07 71 c6 b4 a3 71 ea fe e1 cc bf cb 19 0a 07 d9 a9 27 ad b6 36 bf fc 76 df 6c 23 9c ae ea 89 d6 ff 00 96 87 b8 4c 36 74 cb 2c cc e3 f7 c6 c6 db de 0a 45 3b 24 f6 03 ca 36 b6 d6 02 de a6 d7 bf 5f c7 0a Data Ascii: `aO7miD<QfmGOm >:oM]Jk52._a4':SE$(:b/p~6Z*y3:uhbet#lP[mxV7%qq'6vl#L6t,E;$6_
2021-09-15 12:02:48 UTC	48	IN	Data Raw: 33 d3 a8 1b c7 0c 88 16 c4 df 67 b6 c6 e0 df b3 69 6a 97 89 2a 56 25 09 2b 98 9c a4 91 de 03 85 09 f5 2f ac 27 9f da 18 ae cf 29 46 07 14 a9 12 d0 a6 2c 4e 55 a7 fe 25 34 02 bc 58 b0 e1 1d 47 c3 ba 5a 39 05 4e 4f 9a e6 34 33 13 78 e0 79 1a 6a 5d 4c 77 05 1f a2 ef d0 1b d8 6c 41 b1 c1 12 fb 2f 03 22 98 72 b2 a5 58 95 3a 5c 9e 80 3b d9 88 2f 43 19 1f 13 cd 9a 92 8c 66 06 4e 2d 06 8a 5b 8c c1 89 a9 bb f4 66 78 23 cb 69 38 b3 2f b4 71 cf 97 66 5a 36 92 36 9d e9 65 df a9 e5 b0 73 71 f5 22 c3 6e 98 6f 84 c1 63 a9 f2 71 12 90 01 05 94 40 7b 90 08 37 e4 0c 26 c4 e2 fb 1b 16 a3 f3 12 bc 22 98 94 84 20 ac 50 51 c8 ab 69 d6 09 a2 96 49 16 31 53 43 2d 3c 91 ef cc 31 16 8f 51 be a5 7a 98 8d da 30 45 c8 46 50 c3 ff 00 20 d3 61 83 26 c8 c6 bb 4c 21 4f ff 00 ee c0 63 ab Data Ascii: 3gij*V%+/')F,NU%4XGZ9NO43xyj]LwlA/"rX:\;/CfN-[fx#i8/qfZ66esq"nocq@{7&" PQil1SC-<1Qz0EFP a&L!Oc
2021-09-15 12:02:48 UTC	49	IN	Data Raw: 96 b4 0a 53 0a bc d6 a6 a2 03 99 ca d4 91 a8 9b 3a cd 6b 6a 9a 38 a9 d2 da ac 0b f9 04 ae 2d 68 d2 c1 0d 80 6d c0 c1 18 84 09 27 e4 8a bb 25 21 9d eb ce cd a5 49 b5 2a 42 f4 cd 33 0f 7f 5b 92 fb 83 a5 3a 3f ef 1e 5c c1 2a d3 f9 5d 17 32 9b 87 ee cb 53 52 11 96 bb 34 71 f7 02 b5 f5 2a 36 f6 b9 b5 ac f7 00 ed ac ac 3c 89 4b 54 c5 a4 aa 63 b9 05 8a 52 43 10 c2 ad f6 ae f1 24 f9 b3 14 84 48 4b fc b4 50 28 50 aa f7 6a f9 93 d6 24 b8 76 93 2b 8d e2 a8 8a 39 67 96 09 bf fc f2 ad c0 8a 28 d4 5d 20 31 5c 80 d0 82 15 98 1f 39 1a 8e e7 61 26 cf 5a e6 32 42 82 43 00 2b 5f b5 aa 1d 81 89 91 2e 5a 25 a4 86 cc 2e 4d df 7f b7 96 91 d5 98 57 54 e6 b9 bd 45 4c 43 95 47 4f 39 e4 88 c9 e4 cc ea 34 bb ca 76 fb 30 47 41 71 6f 53 89 04 b2 9c aa 48 75 16 72 40 71 f6 62 d7 7e 11 Data Ascii: S:kj8-hm'%!I*B3[:?*]2SR4q*6<KTcRC$HKP(Pj$v+9g() 1\9a&Z2BC+_.Z%.MWTELCGO94v0GAqoSHur@qb~
2021-09-15 12:02:48 UTC	50	IN	Data Raw: 6e 91 d4 3b 07 e1 91 28 05 cc a8 0c 5c ef 4d 4d ba 34 6e 07 c1 df 09 32 3c 96 9e 38 e9 a3 35 39 8b 68 59 f3 09 10 18 e0 66 ea 63 59 2f 2c f3 58 94 67 76 60 41 36 03 63 8a 5c dc 6e 69 8b 24 a8 f7 8b d4 90 fc 39 5b f1 17 61 82 44 a4 0c b9 4b 0b 81 42 dc 7c 6f 7f 28 b9 19 36 4d 5d 97 72 f2 cc bc d2 87 a6 86 14 8d 0c 07 9a ce 58 eb 77 00 84 45 d0 01 0d b8 bd af b6 06 56 21 d5 40 e3 cf 56 ea 2c 0c 42 a4 80 0b d1 80 af a7 bf bb 43 a7 85 28 e8 b2 e4 54 a9 34 d3 66 2a c5 e4 90 c6 d1 f3 8b 37 9a 3b d8 c6 40 52 45 80 0c 6c 0d c5 b7 2a 44 f2 2a 69 6a 39 eb d5 85 a8 e7 8d 94 63 42 57 94 00 1d aa 06 c7 9f f1 43 b4 34 e8 28 da 6b 9a 47 85 61 92 4f b4 80 a4 f2 e9 8e fa ad 6b 80 59 4d 8f a1 f3 0e f8 20 91 35 94 df 49 2d a7 e6 fc e1 3a 88 97 dc f1 7d 9d c6 97 24 f8 ec 19 Data Ascii: n;(\MM4n2<859hYfcY/,Xgv`A6c\ni$9[aDKB\|o(6M]rXwEV!@V,BC(T4f*7;@REl*D*ij9cBWC4(kGaOkYM 5I-:}$
2021-09-15 12:02:48 UTC	50	IN	Data Raw: bd 4d 3e 8a 7f 97 b3 1b 45 cb 60 59 83 75 2c 0d c1 27 7c 16 89 60 a5 c8 ad ea 2a 4f b3 e2 0d a3 4f 9d 4f 1f f6 7e 7e 3a c1 be 57 45 24 90 a5 35 25 4b d3 20 75 72 ba fe c6 7b b6 c1 c0 2a 0e a1 f7 bc fb 7b 1c 6f 87 40 0a 2d c0 86 16 6d 2f 73 e3 48 11 44 25 d4 45 1c ed 43 e3 fa e7 51 0c 1a 35 92 97 54 31 4d 1c 13 2a 23 4f 10 8e 92 34 2c e2 fa e3 e7 2c 8c 57 6b 1b 1b 5c fa 8c 1b 03 67 ce 39 1b eb 1e 0f 38 97 88 26 77 93 43 33 00 fb dc 9d 22 c2 db 5f 73 fe bb df 16 24 49 46 64 96 b8 a1 ad 29 6e 55 a1 d2 da c7 69 c5 63 b3 a5 40 1a 96 f3 3c 5b 41 b6 f4 bc 0b 50 57 56 54 54 46 51 9c 5b 72 2f b7 fa df b8 eb 6e d6 da e4 89 40 6d e1 fb f7 78 4c 26 e6 24 a8 58 12 ee 7d 01 f4 d2 1f 5c 2c b3 ea 8f 59 62 46 8b 12 4f a5 cf 5b 7a 8e 9f 4f 7c 6a 65 84 07 04 7b da a6 27 93 Data Ascii: M>E`Yu,'|`*OOO~~:WE$5%K ur{*{o@-m/sHD%ECQ5T1M*#O4,,Wk\g98&wC3"_s$IFd)nUic@<[AP WVTTFQ[r/n@mxL&$X}\,YbFO[zO|je{'
2021-09-15 12:02:48 UTC	52	IN	Data Raw: 94 02 e6 a5 08 54 e7 15 05 d4 14 6a 7e ac b4 dc 52 28 93 7e 0b 99 8a 52 f1 3d b3 db 3d a5 3e 72 8f 7a 5f cf 5a 30 77 73 dc 4a 85 03 d2 f5 b9 2c f1 d9 55 c4 5c 5f 9e c4 22 ae ce ea e7 83 ee 4b 49 cd 4a 54 00 ef a9 45 3c 51 f3 02 ff 00 4a dc 00 6d 6c 21 c7 7c 61 f1 0f 6a 21 72 a6 63 71 09 93 31 25 19 10 44 a1 95 61 89 05 01 25 88 34 3c c6 f1 2c 9e c2 ec 2e ce 20 e1 70 18 75 4c 70 f8 82 0a 94 f4 ef 39 24 85 06 73 ea f1 1b fc a5 51 19 f9 6c 75 05 d3 20 04 39 92 fb 73 03 12 5d 50 ef 76 2b d6 f7 38 ad 27 03 df cc a5 ae 69 b9 f9 93 16 b7 34 3d e7 2a cc dc 61 82 71 45 24 20 4d 29 48 d0 21 2e db 3e 57 e3 73 ca 30 ea a9 63 e5 18 2a 23 8d 19 f7 79 29 9c 23 87 16 28 fc 8b 15 e8 00 62 2e 76 e9 d7 13 a7 0e ee 16 96 22 89 d0 36 d4 6b 5b 6d 46 b1 2e 1a 76 20 4d 74 28 90 Data Ascii: Tj~R(~R==>rz_Z0wsJ,U_"KIJTE<QJml!|aj!rcq1%Da%4<,. puLp9$sQlu 9s]Pv+8'i4=*aqE$ M)H!.>Ws0c*#y)#(b.v"6k[mF.v Mt(

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	53	IN	Data Raw: 4a ce 1a 76 94 a7 98 eb 8c 03 b9 dc b5 ad be 1f 27 24 b4 85 d5 cb 13 5a 33 70 d4 eb c8 3e d0 8f 11 2c a5 5f e3 19 12 f5 0c ef c0 e6 7d 0f a7 18 90 1a 68 b2 37 58 98 a3 95 5a 5a 16 8c 00 d0 40 fe 59 08 0b b4 97 b9 53 a8 82 7d 2e 4d 87 99 31 13 26 15 65 a3 01 c5 f5 37 d6 fe 11 e1 2c 99 79 53 73 53 a3 9d 7c 7f 71 9a b3 fc 96 50 d4 91 14 86 9a 86 8d 1e a5 42 a8 92 6a 86 b0 09 29 ea f7 1e 60 2f 71 a8 0c 40 52 a5 2c 28 13 f5 3e 8e ee e6 c0 6e 1c d3 ed 1b a1 1f 2e 5c c5 7f b0 48 65 02 c7 5e 8e ef a1 b0 ac 41 e4 b4 32 35 43 55 5b 99 2d 5b 3a 97 7b 2b b9 0a c7 4c 6c 45 84 31 02 35 92 ca 8b 60 19 85 f7 2e 72 96 64 25 2e 1d d3 a8 34 a8 2e fd 39 79 40 52 01 33 8c c5 97 21 c3 aa f5 d0 ed ce fc 68 f1 f7 33 ac 4a aa fa 94 80 3f 2e 13 0c 4d 22 f9 a2 aa 29 18 56 45 88 03 Data Ascii: Jv'$Z3p>,_}h7XZZ@YS}.M1&e7,ySsS|qPBj)`/q@R,(>n.\He^A25CU[-[:{+LlE15`.rd%.4.9y@R3!h3J?.M")VE
2021-09-15 12:02:48 UTC	54	IN	Data Raw: ee 84 b9 0c 01 eb af 56 2f 48 12 52 16 a5 04 a8 92 1d 9e 95 27 5d 36 ae bb 9d 60 cf 2b a3 a7 0c b0 53 44 b6 a7 3a 56 63 f7 62 40 6e 5d 88 db cd f7 82 ef e9 f5 4f 8b c4 95 26 a4 95 58 ab 77 e5 6d 1b a6 d4 7b 84 90 50 bf 96 07 71 92 78 3b 0d b8 9f 3d e9 0d bc b7 21 7a a8 e0 92 19 e2 a7 40 55 aa 67 53 1f 3d b9 63 51 96 18 de c7 6e b6 06 fa 47 7b e1 7a 0a 96 0a ac da 00 cf cc 11 d5 fd 05 61 b2 83 30 01 f5 6d ce df 6b fe 49 da 66 0f 5f 1d 1d 1d 34 4d 9c d1 ac 82 86 a3 36 8c 98 33 39 5e ea 55 55 14 2b 3c 71 8d 99 db bd 80 d8 dc 64 de f6 3b 00 e3 a7 1f b7 42 70 f2 d4 54 e9 0c 72 9a dc 5c 52 a7 9e f6 f1 73 70 47 83 12 67 35 41 1e 05 a6 a4 2c 25 a9 ac 9c b1 9a 96 2b f9 42 10 4e a9 24 17 ba ee 41 04 db 02 62 67 a6 5a 48 cc 1f 29 71 f6 df db 68 d0 ef 03 83 9b 3a 62 Data Ascii: V/HR']6`+SD:Vcb@n]O&Xwm{Pqx;=!z@UgS=cQnG{za0mkIf_4M639^UU+<qd;BpTr\RspGg5A,%+B N$AbgZH)qh:b
2021-09-15 12:02:48 UTC	55	IN	Data Raw: a5 cc cd 99 ee cc 38 fb d7 6d 1e 19 e1 4b 25 4c d4 03 83 f3 e3 1c e0 80 86 4b 74 56 bb 2d 8e f6 1b 8e a7 f1 f7 f4 c0 e0 32 8a b5 f7 f8 fe 61 9c a2 e0 be c0 d2 ee 75 be 9e 90 43 4d 0d d9 77 bd b7 b7 af b0 df fe 7a e3 31 e9 a5 4d 41 43 be a4 69 a0 b5 9b 85 b5 27 a3 87 45 8b 2d 8f 5d 36 eb b7 4b df a7 fc 63 c2 f5 a0 dc 5f df 8c 40 0a 8d c0 02 0b a8 a3 56 20 00 09 1d b7 bd b7 fc 05 ff 00 e0 62 6c e8 e2 79 30 f5 8c 2e 95 d6 de b0 73 95 d3 9f 2f 96 dd 06 ff 00 8f fc fd 4f ae 3d 9c 12 00 06 bb b4 27 9e a3 de 53 b5 ec cd b6 a4 6f 6f 48 6a e5 70 81 4e b6 61 75 d2 4d c7 e7 f9 6f 6f c0 d8 e2 44 b8 58 04 53 29 3f 6a f8 f8 f8 42 79 c0 a9 20 8f ab 30 e8 de cb de d6 83 ec b4 e9 92 22 77 16 eb e9 bf 4e de bf 4f 5d f0 cf 0a 96 49 23 91 fb 40 98 84 07 4d 4d 48 f0 71 ef 9e Data Ascii: 8mK%LKtV-2auCMwz1MACi'E-]6Kc_@V bly0.s/O='SooHjpNauMooDXS)?jBy 0"wNO]I#@MMHq
2021-09-15 12:02:48 UTC	57	IN	Data Raw: 6a e4 59 1c 49 53 49 57 0d 43 02 75 d4 05 27 0e fb 2f b5 71 fd 9d 33 3c 89 b3 b2 8a 8c c4 e5 35 04 25 40 30 52 5c 77 92 a0 52 6c 60 0c 7e 07 0b 8f 94 25 62 25 4b 28 70 f4 73 65 24 a9 27 ea 4a 86 65 04 ad 2a 04 07 ca ce 23 c3 1f f1 84 ff 00 e9 f0 f1 6f e0 47 2b 8f c7 4f 84 e4 e3 8f 1c be 18 aa b3 b3 1f 15 70 8a e5 f5 9c 47 e2 8f 83 95 b5 05 8e 5f 5c f1 e5 d4 f3 66 1c 4f c1 26 3b 50 cd 98 18 aa 6b f2 77 8e 09 eb 65 ad a2 ac ad ad c9 ef dd 95 da 38 7e d6 96 4e 2d 08 c3 62 d3 44 a9 01 32 e5 4d 24 59 60 82 99 6b b3 11 96 59 0f 98 85 77 8a 45 e2 b1 5d 95 88 97 2a 54 c5 e2 70 27 32 a7 26 64 c5 cd 9f 28 04 e6 2a 44 c5 9c f3 d3 45 a9 52 96 a9 98 8c c5 28 c3 82 0c b9 31 e7 53 24 cd 32 9c fa a3 2d 8a 1a aa 7a a8 e3 97 5c c8 96 8d cc a8 0b b9 e4 bd a4 0a 23 d2 d7 2b Data Ascii: jYISIWCu'/q3<5%@0R\wRl`~%b%K(pse$'Je*#oG+OpG_\fO&;Pkwe8~N-bD2M$Y`kYwE]*Tp'2&d(*DER(1S$2-z\#+
2021-09-15 12:02:48 UTC	58	IN	Data Raw: 2c fc bc db c8 ec d9 85 1d f2 94 d3 fd ed ce 9d 78 5b ae 1d 4f 0c 64 d4 f3 ab 19 65 ad a7 0e 39 72 c6 55 cb 39 eb 1b 5f cf a0 de e0 8e 97 b8 27 03 0c 7c d5 25 e5 e7 4b 8f f6 02 9c 37 7a 3f ac 6f ff 00 49 42 0e 79 cb 92 a4 d1 43 2d 4f 22 1c f2 71 e3 12 d2 d7 51 d0 01 45 4d 4c b0 54 98 c0 e5 40 bc da 99 97 ff 00 56 00 16 5b db ef 5b d4 75 df 03 ae 4c fc 40 cf 35 61 59 68 2e fb b6 9b 8f e4 56 20 99 32 ce 5c 3c b3 f3 6a 5d 9c 5a ee cf a6 9b 1d 2f 81 51 49 2c c1 1e 48 23 a0 69 2d 77 90 af 3c ab 1f 31 68 dc f9 ae 2f d7 bf be 26 94 85 4b 09 42 00 cc a3 94 1a 92 e7 ab 0d 8d a2 5f 9b 25 01 f1 34 58 e5 a0 d0 9a d6 d6 e9 03 b9 97 11 51 e5 5a 32 ec 96 92 5a ba b0 c4 1a 89 17 54 52 13 75 20 c4 ba 94 f9 ae 45 ba 6c 4e d8 77 23 b3 27 29 19 b1 2f 56 23 6b 8e 6d 4d f9 69 Data Ascii: .x[Ode9rU9_'|%K7z?oIByC-O"qQEMLT@V[[uL@5aYh.V 2\<j]Z/QI,H#i-w<1h/&KB_%4XQZ2ZTRu ElNw#')/ V#kmMi
2021-09-15 12:02:48 UTC	59	IN	Data Raw: 61 73 f9 89 09 f8 79 97 53 94 da de a4 91 da e6 f8 c2 a6 29 98 90 5b 41 b6 9c 03 6d e7 61 1e fe dd 16 cc 3a 81 ee b1 0f 2e 59 a5 74 f9 bb f6 ea 7a 6d f8 1b 7e 9f 4f 19 e4 00 12 59 34 d7 89 3e 3a 83 11 af 0e 92 08 01 c0 6a 8a 0d de 83 4f 0f 1a ac b8 87 2f b3 4b 65 36 bf 70 76 ea 7a 7d 3f d3 06 c9 9c 54 03 dc 35 09 b8 3b 7a 78 3e 8e ae 74 92 14 e9 60 96 62 08 f7 ef 6a 42 73 36 8b 44 d2 00 37 07 d8 58 0d fd cf 5f af e9 6c 31 90 ae f5 68 08 a3 90 d7 1e 66 9e 2d 58 55 3a 4a 47 79 34 25 e9 e1 68 1f 55 16 62 3e f7 50 3d 77 ff 00 7f af d7 b1 39 93 bf ba fb f0 de 04 25 94 02 81 3e 94 b5 78 33 c1 af 0f 5b 9f 11 b7 44 00 92 08 be f7 b6 fe d8 1e 70 29 ab b8 7b 0d 1d 9b d7 58 d9 89 fa 6c f6 a7 bd 7c 21 fb c3 f4 de 40 ca 54 96 52 41 d4 2f d4 75 ef d7 e9 d8 da c3 11 73 Data Ascii: asyS)[Ama:.Ytzm~OY4>:jO/Ke6pvz}?T5;zx>t`bjBs6D7X_l1hf-XU:JGy4%hUb>P=w9%>x3[Dp){Xl|!@TRA/us
2021-09-15 12:02:48 UTC	60	IN	Data Raw: 75 74 24 ee 3d 6d 8d 0c 8a 12 b0 2a e9 07 8d fe dd 79 45 1f 17 d9 52 8f 7b ba 43 30 20 1e 4f 61 c7 5e 30 77 3f 8e 55 87 95 34 95 ff 00 74 22 04 32 c7 66 17 b0 00 2b 06 17 24 7b ed da d7 c0 cb c2 a7 2a 81 2e fc c3 56 9f 6d 5c 40 52 bb 3a 55 89 a5 06 56 35 e3 7d 3d 1c 44 a4 9f 10 d5 74 b0 00 5e 2b d8 1b 0a b2 4d fa 5c ad 9b 7d 87 71 6f ef 07 f6 89 3a 0f 3e 96 6f dc 6e 7b 2d 0e 08 0c 1c 54 83 67 7d 78 72 27 6a 16 0b e3 1f 8a ca 8e 16 e1 9c d7 38 aa cc a4 82 b6 35 3f 2a 9c cb 7d bc a0 c4 9a 46 af 31 01 d3 70 01 dc df ae 24 fe c0 83 44 d3 70 08 27 dd a1 f7 65 76 4e 06 76 20 09 c9 ee b8 bb 0d 5a 8e fd 45 6b 57 83 5f 0c 7e 2b cd 3e 47 93 0a dc da 65 98 c0 25 91 75 a9 0f 2b 00 c4 dc 13 7d 4d 7b 13 f8 6d 81 d5 84 65 1f a9 c1 2f 7b 8d af b1 14 e7 53 10 76 c7 c3 fd Data Ascii: ut$=m*yER{C0 Oa^0w?U4t"2f+${*.Vm\@R:UV5}=Dt^+M\}qo:>on{-Tg}xr'j85?*}F1p$Dp'evNv ZEkW_~+> Ge%u+}M{me/{Sv
2021-09-15 12:02:48 UTC	62	IN	Data Raw: c7 72 42 82 ab e5 b8 b0 20 8c 00 84 4d 92 a1 87 5a 0c a5 13 95 44 8b 95 0e 01 c8 21 ae 6c cc d6 86 3f 3a 4e 29 3f de 22 6a 0c b5 12 fd e7 c8 05 09 2c e1 81 04 50 96 3a 52 25 f2 da 0a dc ed 8c 89 70 66 d3 58 6a 2a 05 a3 a7 a1 8a fc c2 8a bb 68 75 0e ea d6 b6 93 bb 10 2d 8d 44 c0 0a c0 05 45 1d d2 37 2f d7 63 f8 d4 cd 86 79 ae 10 33 14 b1 50 7c b4 1f ec 5e 80 16 f0 be 82 39 e7 b5 30 53 d1 8a 5a 56 49 32 66 8d 6a cd 6a 30 ff 00 bd 8d 53 78 12 40 74 a2 dd 58 f5 04 82 96 d9 b7 97 0e 95 26 6b a0 12 01 ab d4 24 d8 83 62 e2 c5 e2 3c 6e 25 60 32 80 04 50 25 86 62 07 87 90 de 06 f2 9a 8c f3 32 cc a0 7c 99 26 cb a3 82 96 c6 a3 9a 69 92 28 8d ee b4 f3 4a 02 bc 9a 2d aa 2f 34 6c 09 da e7 05 e2 f2 4a 06 6c d0 14 66 56 5e 4b 83 41 56 d0 9f 2d 61 74 8f ee f1 2a 4a 00 38 Data Ascii: rB MZD!l?:N)?"j,P:R%pfXj*hu-DE7/cy3P|^90SZVI2fjj0Sx@tX&k$b<n%`2P%b2|&i(J-/4lJlfV^KAV-at*J8
2021-09-15 12:02:48 UTC	63	IN	Data Raw: 74 b5 75 da ec fe 02 36 13 e1 b6 49 25 0d 02 53 65 14 f4 b4 10 35 cc 93 4b 10 6c c2 a8 9d 89 a9 d8 84 65 07 4a 04 36 20 8b 8c 56 b1 38 85 2b 35 4a 75 0e 69 4d 8d 6e ff 00 7d e2 ff 00 d9 bd 9f f2 b2 93 96 a0 3a 9a 9f 71 e7 a5 22 d6 f0 c6 5d 96 40 b1 9a 98 1a a5 84 70 a1 2e e8 11 0e fa 99 a3 7e ee 6c 05 96 e6 dd ba 62 bd 3e 72 9c b3 d2 fa 39 db db bc 5c 25 e1 c0 40 24 02 c0 68 1e ba 0d 29 ef 48 7d 64 b1 50 52 c7 34 79 4d 0a ce 25 80 16 92 70 c3 44 c5 a3 bc 10 ad b7 7d 24 d9 80 21 55 4b 5f 63 80 5c 92 49 0d b6 a7 ab 53 d9 89 a5 4b 12 94 56 a0 4a 48 b7 4d 4d a8 dd 68 60 db 2a a2 62 89 35 5f 2e 8e 4b e8 3c f2 9f 30 63 6b 5f 94 b7 3e 52 07 b1 b7 63 b8 c2 9c 57 d5 77 d0 6f ef 71 bc 4f 2d 64 32 6e e6 84 9b 51 9f a7 f1 51 0e 3e 1e 58 80 a6 70 dc d5 69 39 49 27 30 Data Ascii: tu6I%Se5KleJ6 V8+5JuiMn}:q"]@p.~lb>r9\%@$h)H}dPR4yM%pD}$!UK_c\ISKVJHMMh`*b5_.K<0ck_>RcWw oqO-d2nQQ>Xpi9l'0

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	64	IN	Data Raw: 3d 02 29 44 92 34 7f 48 9f a5 88 2b 5a ff 00 91 ea 7d 6d eb d8 7b fe 03 18 f3 a7 bf 6f 10 cc 09 21 d4 6c f4 fd f5 b7 a5 e0 9a 96 76 89 15 7b 1f 4b dc 7d 4f 6e be bd b1 91 42 39 82 78 08 8d 60 2e 5b 01 56 a6 8e 35 d0 e8 ce ed e4 d0 49 97 66 3c b3 e5 3d ec 77 ed df eb eb f8 df 13 29 68 3a dd 85 1e e2 9a 06 15 f1 b7 08 50 b9 24 12 e1 83 bb dc 30 e5 5a eb e7 0c 6c a6 bb 5d 89 3b 0b 5a d6 b6 c7 d3 f0 ef fe 98 33 0c 52 97 75 17 a0 14 70 4f b3 76 e1 bc 03 30 3b a5 36 d5 83 5a c4 bb 38 d8 7a c1 85 3d 71 20 5e db f7 b6 df 4f df e6 3a 60 e1 31 22 c6 9c 8f b1 e7 d5 a1 71 92 33 38 2e 1c f9 f9 f4 f4 d3 35 2b d6 43 14 6b 73 b8 36 b9 24 db a8 e9 d2 ff 00 bd b6 c9 51 17 27 4d 77 b5 a3 39 48 d1 ef a3 fe 5b 46 fe 61 db c1 99 9d 3d 31 43 cc b1 0c 9a c1 df 7b da da ba df 70 Data Ascii: =)D4H+Z}m{o!lv{K}OnB9x`.[V5If<=w)h:P$0Zl];Z3RupOv0;6Z8z=q ^O:`1"q38.5+Cks6$Q'Mw9H[Fa=1C{p
2021-09-15 12:02:48 UTC	66	IN	Data Raw: 2c 67 08 fc 50 8a 0c c5 d1 f3 0d 00 88 1d 5d 64 29 75 76 6d 88 36 da c3 61 6f 51 70 46 21 97 da 8a 95 31 8c c2 a6 bd 0f 32 28 f5 d5 dc bc 53 7b 6f fa 75 85 9e 81 2a 74 91 31 44 77 4c a0 26 28 66 b1 21 0f b6 a0 b0 e9 16 07 38 f8 bf e0 6a 6e 1a a9 92 b3 36 86 9a 78 e9 e4 43 3c 4f f2 f3 19 59 0c 60 2c e7 49 1a 1d 83 1d 45 81 65 1b 35 86 22 ed 6e dd 48 ec fc 54 c1 3b 17 86 9b 91 5f 2b 2d 54 a5 07 66 67 6e ac ef ae 9c cd 1f d1 dc 50 ed 19 38 84 49 54 f9 5f 31 20 80 97 48 4b 87 cc 0b 00 d6 0d 40 f1 e5 af f8 b2 fc 54 27 8b bc 53 c1 7e 1d e5 59 dc 39 fd 2e 45 25 57 13 66 b9 c5 45 26 55 57 98 d2 4b 34 6f 4b 97 64 94 39 ca 52 0c c2 0c bd 23 96 49 e6 89 6a 95 5e 54 09 20 64 67 06 cd fd 06 c3 76 c6 32 4f 6a f6 c6 37 1b 88 9e a4 4e 50 95 2e 78 50 64 12 5b bc a0 03 01 Data Ascii: ,gP]d)uvm6aoQpF!12(S{ou*t1DwL&(f!8jn6xC<OY`,IEe5"nHT;_+-TfgnP8IT_1 HK@T'S~Y9.E%WfE&UWK4o Kd9R#Ij^T dgv2Oj7NP.xPd[
2021-09-15 12:02:48 UTC	67	IN	Data Raw: af 38 53 3f b5 f1 a1 44 cb 2e 39 35 7a da bc 2b a3 5a 20 94 4c 19 a5 ae 8b 35 a9 25 d4 c0 b0 41 33 73 1c fd c6 15 2c 48 21 6d b8 62 09 ea 7d 0c e1 12 6d 2e 5a 50 43 a7 41 51 72 4d 2f c1 df 9b b0 a1 78 c5 39 9d 3c ac 2a ac f4 63 52 05 d8 07 6a 8e 91 d5 2c 8d 55 51 ca 9a 29 29 43 d9 5d ab b9 aa 10 2b 0b 97 68 a3 69 36 22 e7 4a 1b 81 6d c5 ce 09 97 2a 62 41 51 58 b1 75 5e d5 14 b8 e9 c2 20 58 ab e5 26 9b be 9c fc c0 3e 31 21 51 97 52 09 12 19 26 a4 ad 85 63 32 2d 4d 32 54 c3 01 70 2f ca 59 26 8e 20 64 03 a7 e7 f4 85 6b 56 7b bf 12 f7 bf 9d e9 6a 59 cc 60 00 c5 93 95 cd 43 bb fa 1e 87 ef 10 8d 35 1c 72 18 a2 a0 9b 63 64 68 d3 9f 7b 5a db dc f7 ef b9 d8 db d8 9f f2 e5 72 58 73 0f c8 d5 83 0f c4 48 91 72 59 9b 53 ed a2 40 49 3c 31 17 6a 60 b5 07 74 5a a6 d4 c7 Data Ascii: 8S?D.95z+Z L5%A3s,H!mb}m.ZPCAQrM/x9<*cRj,UQ))C]+hi6"Jm*bAQXu^ X&>1!QR&c2-M2Tp/Y& dkV{jY` C5rcdh{ZrXsHrYS@I<1j`tZ
2021-09-15 12:02:48 UTC	68	IN	Data Raw: d2 a4 85 16 e8 0f 7b 9b 7b fb 76 c2 49 b5 98 58 3b 01 61 c3 7b 6b be b0 bd 64 3d 48 b6 fe 3e 02 ba 75 b4 77 66 19 39 8e 26 3c b6 6b 82 34 db dc 8e df a5 fe b8 8b 9f db 85 7e f6 fb 3c 13 2a a0 77 00 f3 72 7d d2 8f 68 4e f1 1e 57 a5 d8 e8 d3 a4 3d 87 ff 00 8a 0f bf d6 de b7 fa 63 0a 5e 56 ca 5c 9b b1 73 7e 1a 5b 58 3a 51 62 59 eb 52 dc 4e f4 2d ee b0 88 e2 aa 01 a6 da 4d b9 67 af d3 fd ff 00 7b e0 d9 13 c8 cb 9a d4 3f a7 b0 3c f4 e8 06 56 94 97 0d 52 3f 9e 15 6f 16 a4 57 3e 22 a3 d1 29 6f 77 07 a5 8f 5b 0b fe fb e2 cd 85 9a 96 74 ea 06 b7 2f e7 a7 94 26 c4 61 c9 24 83 72 7a 70 be d6 6e 0d ac 0a c1 01 d5 7b 1b df a1 e9 fa 7b 13 f9 7a 60 d2 aa 3f 80 37 f0 77 eb e0 f0 1a 70 ca ef 69 6f c5 47 8b f1 83 5c a6 03 f7 76 df a7 a8 04 28 fd fd 7a 60 6c 44 d2 40 de d7 Data Ascii: {{vIX;a{kd=H>uwf9&<k4~<*wr}hNW=c^\V\s~[X:QbYRN-Mg{?<VR?oW>")ow[t/&a$rzpn{{z`?7wpioG\v(z`lD@
2021-09-15 12:02:48 UTC	69	IN	Data Raw: 92 c9 55 0d 0d 32 ad 55 7c 8d 59 99 e6 32 c6 bf 31 55 50 ed a9 e7 60 c7 50 56 20 1b 81 6d ac 00 16 b3 1c 8a 4d 08 34 d5 bc fc 3c 05 21 74 ac 56 18 fd 49 4e 63 73 43 5b 9b 6b fc bc 76 47 c6 2d 53 2b 49 34 b6 92 fb 4d 1d d5 d4 ed b8 23 7e de bf 86 35 b5 cf 8b 46 93 d5 2a 79 00 16 09 a8 23 a8 6e 3e 71 39 1f 1e cb 4e ba 0c c6 78 ee b6 76 94 c7 70 4d 8f 9b 5e c3 be ab 5c 5a fb e3 0b cb 94 85 b9 49 07 30 0e 54 47 00 01 7a b0 eb 00 cc 9b 35 0a 74 cc 5b 8a 00 49 b1 04 79 3b f9 b5 98 e2 90 e6 d9 c7 09 f1 2f 19 64 f9 95 15 54 1c 35 96 cb 5f 3e 5c b5 5a b3 36 a7 8c 13 39 88 02 55 ca db ca 74 91 d4 5c 60 1c 5f 6c f6 4e 1b 19 d9 98 01 87 9a 14 7e a5 14 b0 75 16 ef 1d 2a 6b ed d4 ce c5 63 86 1b 13 89 2a 57 ff 00 0d 4e 81 de 39 d0 0b 90 35 22 9b 6f 7d 2b fd 6e 65 2f 16 Data Ascii: U2U|Y21UP`PV mM4<!tVINcsC[kvG-S+I4M#~5F*y#n>q9NxvpM^\ZI0TGz5t[Iy;/dT5_>\Z69Ut\`_IN~u*kc* WN95"o}+ne/
2021-09-15 12:02:48 UTC	71	IN	Data Raw: 67 f4 30 e7 a7 8a 1a 69 12 9a 6c 9a 7c ab e6 be 62 36 7b 41 21 4b e9 5e 8a fb 61 78 14 e1 7b 41 52 d5 f2 e6 21 d6 95 51 24 94 b1 b9 67 7b 3b b5 62 6c 0e 13 18 66 64 5a 5c 4c 24 27 30 d4 82 c4 d3 4b bd c8 e3 1b cc fe 34 1f c3 3b e1 47 e2 c3 3b f0 47 c7 ff 00 e1 f3 f1 15 f0 d3 e0 87 c5 63 40 f9 25 57 09 d0 f1 ee 4f c2 5c 33 e3 5d 07 26 9a a5 6a e8 df 2a 33 d6 53 e7 19 0e 61 13 34 4d 15 16 63 43 5f 43 5b 55 4f 98 e5 f5 0a 69 67 a2 55 82 f8 a3 05 da 58 61 80 ed 20 96 94 80 80 b4 e5 5a cb 00 cc 4d 6e e9 74 90 53 9d 45 25 d5 58 f0 5f 0b f6 fa 7b 4a 66 2f b3 e5 f7 d2 66 52 6a 54 24 cc 7c ec 95 64 20 28 11 95 40 b5 16 99 6a 62 a4 08 f2 6f f1 69 e1 f7 c4 df c3 6f 88 f9 47 87 bf 1d fe 04 e6 3c 0d c6 da 26 a8 c8 fc 4a c8 a9 e9 72 e3 e2 4e 44 b3 d4 c0 d9 e6 57 c5 59 Data Ascii: g0il|b6{A!K^ax{AR!Q$g{;blfdZ\L$'0K4;G;Gc@%WO\3]&j*3Sa4McC_C[UOigUXa ZMntSE%X_{Jf/fRjT$|d (@jboioG<&JrNDWY
2021-09-15 12:02:48 UTC	72	IN	Data Raw: 0d 57 20 dc a9 b5 ba 1e 98 59 37 1a a9 81 44 28 31 a5 c3 b1 a5 6c da db ca 2c 78 3e ce 32 10 84 65 49 20 38 27 c6 ae 36 a5 1a 0f a1 a1 4a 55 fb 38 2d 34 84 29 84 a8 d1 64 17 3b b7 4b 9d 88 b8 bf 5d fa e1 5a d4 56 4b 9b 38 07 9e ba f8 e9 0c 96 85 20 27 36 50 08 a3 53 4a 92 01 2d a3 35 37 da 0a f2 19 a4 35 2a 6f cb 56 b6 a8 db 48 40 c8 0e e9 6b 5e e0 91 7e 9e 98 85 6f 96 be 40 d0 10 5f 89 f2 78 f2 01 24 96 2f ef d1 bf 30 ed c8 6a e2 a5 30 49 1c 81 b7 51 38 1b 00 a7 75 07 d3 bd ff 00 5c 02 43 85 0e 3f 61 1b e5 72 54 cd c6 be ec 6e 6f 0f 8e 1f aa 8e a9 50 d0 ab 45 34 65 67 47 04 0b 6a 24 1b 6b da e7 d8 fe 78 4b 88 99 96 66 c0 d6 fb fa fb b4 0d f2 fb e5 c1 cb b8 a7 bd e1 ad 94 53 41 52 e2 b0 c9 f3 19 84 6c a2 46 a3 52 a8 a4 6d a2 ae 37 2b ce bf 42 c0 81 85 53 Data Ascii: W Y7D(1l,x>2eI 8'6JU8-4)d;K]ZVK8 '6PSJ-575*oVH@k^~o@_x$/0j0IQ8u\C?arTnoPE4egGj$kxKfSARlF Rm7+BS
2021-09-15 12:02:48 UTC	73	IN	Data Raw: 63 f9 fe 3d ff 00 76 c7 a3 45 fd 06 fa 72 7d 74 a6 8c da 79 13 d2 c9 a5 41 bd 89 d5 eb 6b 96 04 7e 16 e9 d7 f5 c7 a0 78 94 4a 9d 04 5c dc 5b a6 e4 7b 6f 70 07 eb b5 b7 ed 8c 36 ba fb f7 ed e2 29 a9 04 3e be fd f1 dc 47 53 d5 d9 89 07 fd 87 7f 5f c7 a7 e5 8f 38 df a4 42 91 97 2f 12 49 14 ae c3 f4 37 8e bf 9a 1e 52 3d 41 3b 76 fa 9d bf 1c 79 f4 06 be 9c e0 a2 1c 34 10 51 e6 86 3b 0d 4f 6e 9b 35 87 5f 6e bf 87 b7 4c 6c 2e 39 86 85 d3 a5 ba 98 d8 96 3b 5f a3 07 3a ff 00 05 14 99 93 4b 6f 33 1b 0b 0b b5 f6 b7 41 b8 f6 fc 6f 86 32 ad d3 dd 38 ef f9 85 f3 b0 df 2f be 8d eb c3 8d 8b 6d fa 8b 01 e1 67 c8 cf 59 18 7e 58 60 a0 4f 0c ea 25 47 24 74 8f ef 0d 47 62 0a ee 2c 7a 0c 0d 3e 6b e2 50 80 5e 51 29 0a d8 7f cb 5a dd 9f a4 25 c5 e7 48 74 df a7 b7 af 13 e9 0d bf Data Ascii: c=vEr}tyAk~xJ\[{op6)>GS_8B/I7R=A;vy4Q;On5_nLl.9;_:Ko3Ao28/mgY~X`O%G$tGb,z>kP^Q)Z%Ht
2021-09-15 12:02:48 UTC	74	IN	Data Raw: 45 c3 19 fd 8e 0b 08 89 f8 a9 a3 0b 32 5a 51 92 42 69 3f 10 19 f3 25 24 32 52 7f fd e2 fb ac 46 54 cc 21 a3 d6 8f c1 27 ff 00 4e 77 c2 b7 84 19 66 53 c5 bf 15 95 12 fc 4c 78 92 21 5a ba cc 97 37 92 7c b7 c2 5c 86 ad 96 19 a6 a2 ca 38 5a 19 01 cd 16 92 78 af 4b 98 e6 73 d4 c8 fa e6 57 45 49 4c 58 af 62 fe 22 13 56 b9 32 00 5c a2 9c 86 61 65 02 14 92 14 90 08 ca cc 4b b0 72 09 49 24 52 39 8f 6c fc 53 da d8 b0 24 60 db 0f 25 0a 06 58 94 a2 99 99 90 b2 b9 73 15 93 29 52 d2 a2 02 54 a6 fa 12 59 c6 68 f4 13 c2 99 1f 04 78 73 c3 f4 3c 27 e1 df 0d f0 e7 06 64 14 11 24 34 d9 4f 0c e5 94 59 4d 0c 50 28 d2 8b c8 a3 82 04 77 55 1a 5a 46 50 cf 6d 4c 49 b9 2a 93 31 53 96 73 4d 2b cc 49 24 97 29 e0 4f 9f 4d 6f 08 11 d9 d3 f1 49 cd 8b 99 32 6f 74 b2 66 12 53 2c aa e1 09 Data Ascii: E2ZQBi?%$2RFT!'NwfSLx!Z7|\8ZxKsWEILXb"V2\aeKrI$R9lS$`%Xs)RTYhxs<'d$4OYMP(wUZFPmLI*1SsM+I $)OMoI2otfS,

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	76	IN	Data Raw: a5 43 28 96 ac b1 e3 d3 37 e0 dc ff 00 c3 4a ea 9a 1c d6 9e 3c df 23 ad 84 8a ca 39 29 18 d2 08 8f f5 cb 4e 07 2a 2a 94 b9 52 42 29 1b 12 6c a3 17 6c 17 6d 49 ed 40 95 09 9f db cd 09 4a b3 85 65 33 48 4d c1 35 25 e8 2a 4f 8b c7 3a ed 4f 84 71 3d 84 16 14 0e 36 50 52 d2 94 19 74 94 80 a2 c3 e6 58 d2 b4 0c ec 22 3c 64 55 b4 f1 1c fb 85 33 cc c3 85 e9 a6 0b 1d 3a d2 57 d5 8c aa 7e 60 0a b4 93 18 24 d7 40 ec 4e 9f b6 4e 51 b2 ec 2f bb 24 e2 a4 ad 7f 22 76 14 4c 5d 7f cc a0 eb 20 eb 9d b3 33 ee ef 15 79 92 31 12 93 f3 30 b8 83 2d 44 7f d9 f9 85 6c c1 c5 3f d4 55 98 50 6a ed 02 d9 bd 77 1b d2 a3 53 e6 d2 cd 51 a7 c8 c4 54 2d 59 d0 4e cc b2 5d b5 06 be ae 8b ea 4f 60 78 18 44 00 e5 f6 00 b3 16 d6 fc ac fb b5 a1 6f cd c5 39 f9 a1 59 ec a5 1b 2b 8b fe 75 b4 0b cf Data Ascii: C(7J<#9)N**RB)llml@Je3HM5%*O:Oq=6PRtX"<dU3:W~`$@NNQ/$"vL] 3y10-Dl?UPjwSQT-YN]O`xDo9Y+u
2021-09-15 12:02:48 UTC	77	IN	Data Raw: 6f 50 7a 56 13 62 31 72 88 ee 9b 7d eb cf d2 96 de 13 5c 5b f1 0f 9b e7 b2 54 d5 c3 e2 0c f9 87 11 d6 51 83 f2 f5 d0 31 c8 72 f7 99 c0 4c bd 39 cc 1a a4 29 b0 2c 62 3e 5b ec 3a 62 d7 85 ec e4 ca 4a 4a be a1 e3 a5 f7 f7 a4 56 71 38 c9 69 59 20 82 e4 24 eb 43 7a 53 d7 c6 2b 57 8a be 23 71 8d 6a c4 73 3e 31 e2 8a fa e5 45 45 a0 c9 a5 5c bb 26 81 6c a5 c4 74 88 cf 4e 2d 6d 9b 40 63 72 6d be 91 62 c3 4a 97 2d 00 ab e9 4d 54 7c 74 fb e9 48 4d 88 33 2a ac 10 24 aa 84 5d f7 0d 4f 63 ac 54 bc d7 8b 78 8a a6 43 07 10 66 55 b0 65 8a 2a 23 a7 96 21 1f f3 0b c8 ee 52 39 e7 7a 4b 33 ad fe d2 de 5d f6 18 7f 84 97 82 6c f4 b7 00 c7 9f bb 3c 55 31 88 ed 45 4c ff 00 b4 4b 17 34 fc f1 f1 84 b6 69 c4 ec d2 08 a9 38 aa 9e 95 4b 3c 8f 05 5a c6 6a 43 23 bc 21 a5 0b 04 0a a6 cb Data Ascii: oPzVb1r}\[TQ1rL9),b>[:bJJVq8iY $CzS+W#qjs>1EE\&ltN-m@crmbJ-MT\|tHM3*$]OcTxCfUe*#!R9zK3]l< U1ELK4i8K<ZjC#!
2021-09-15 12:02:48 UTC	78	IN	Data Raw: b4 15 ad 82 9d 8d 1c 00 38 0a 6a cf 15 6f 36 e0 6e 1c e1 89 6a 60 a3 8a 2a 7a 68 98 1a 19 23 0b c9 a8 a7 b6 a8 f5 a0 37 1a 57 cb 70 46 c2 dd b6 56 bf 92 84 ff 00 8c 01 73 61 c7 ef 7e 5c a2 f1 86 ed 2c 4e 36 58 f9 a1 41 4c 2e 4b 93 c4 37 ad 1c 03 00 35 bc 63 96 c1 4b 53 42 9f 2d 2c 2c ae b5 28 87 97 10 54 eb b5 f7 75 ea 6e 7a 90 37 ec 3f ce 4a d2 52 4d 4d 68 da 36 a0 bf 2f 3b c4 8a c0 4e c8 a5 8c c3 bc 0b 82 45 09 af 43 bd c5 de cf a4 0f 8d 28 f8 6f 31 ab cf f3 c3 4d 4e 29 a8 e2 a9 97 9a 62 8c a3 cb 18 0c 01 da cc 0e e8 0e d6 b1 27 73 82 70 64 67 a0 15 6d 2b 76 f2 df ce 19 f6 84 b4 0e ca 49 2a 65 a4 5e af dd 0e 2a 3a 30 b5 45 e3 41 35 39 8b 57 43 9a 66 2a 42 ff 00 f7 23 98 51 a0 b8 5a 78 12 65 52 96 24 e8 ba 82 41 ed 7e b6 c3 b0 b2 2c 00 77 b5 3e fb 8a c7 Data Ascii: 8jo6nj`*zh#7WpFVsa~\,N6XAL.K75cKSB-,,(Tunz7?JRMMh6/;NEC(o1MN)b'spdgm+vI*e^*:0EA59WCf*B#Q ZxeR$A~,w>
2021-09-15 12:02:48 UTC	80	IN	Data Raw: 09 c6 d5 7c 0d f1 63 f0 db e2 6f 87 55 f1 e5 9c 4d e2 2f 84 5c 57 91 71 a3 ac 6a e3 33 a4 e0 cc e7 22 ff 00 a7 63 ad 50 51 a7 fe 5d fc eb 35 39 7c c5 84 91 0a ba b5 88 e8 a9 99 1f b0 7f 4c 15 ff 00 51 ec be d6 4e 21 2e 24 ce c3 a6 5a 95 52 81 96 71 59 04 d0 3e 50 e3 56 0e e4 08 f9 f3 fa 92 bc 5f 61 f6 9f 62 e1 f0 ca 59 94 51 da 33 e6 61 41 ee cf 32 c4 9e f1 ff 00 d9 00 36 52 1f 20 06 80 01 a7 4f 83 1f 87 af 14 3e 38 78 bc 67 3c 73 9a d5 c3 e1 2f 0e e6 02 9b 36 92 9e 4a ba 44 e2 8c c5 09 90 e5 f0 1b 84 7c be 32 39 75 96 67 59 18 34 4c 6c 18 06 1f 1a fc 4f 83 f8 43 08 bf 94 53 37 1c b7 2c 48 ff 00 1c b5 27 b8 9c b5 39 88 39 83 96 4a 59 81 2a cc 9b 2f f4 87 fa 7f 8f fe a1 e3 67 f6 df 68 a5 58 7f 87 64 af 2c a4 b1 0b 9d 8d 92 a0 e3 30 57 ff 00 b3 a1 7d c5 4b Data Ascii: |coUM/\Wqj3"cPQ]59|LQN!.$ZRqY>PV_abYQ3aA26R O>8xg<s/6JD|29ugY4LlOCS7,H'99JY*/ghXd,0W}K
2021-09-15 12:02:48 UTC	81	IN	Data Raw: b4 66 00 54 0a 37 97 28 bf 1e 1a 70 f5 13 40 20 31 33 d3 aa ac 6d 3c 4c 8b 0c f2 79 77 04 00 40 24 5e ca 7b fd 70 83 15 37 be a7 d4 2b 57 2c 01 f7 47 f3 11 7e f8 7f 0f 9f 23 a4 1e 2c 19 f8 8d c7 5e b1 70 38 63 85 aa 1e 97 99 4b 4b 1d 1d 2a 2a f3 a5 91 46 b9 46 90 ba 96 46 df a7 42 08 3b 62 a1 88 9c 4a 66 56 a1 4c f7 3b 36 e0 ee 1b 4a 47 55 ec c9 59 10 00 0d 46 00 00 e5 e9 eb ef 58 6b e4 f9 1d 4a 53 29 54 58 e3 6f b3 8d 63 52 35 d8 85 2e 48 f3 36 a1 66 63 7d ee 3b e1 3c d9 d9 6e a3 d4 9a 91 b7 ba c3 f9 68 29 d2 db dd e9 a1 f0 f6 61 a1 47 93 1a 78 e0 60 84 b4 96 8b 50 b9 3b 1b 99 49 da e3 55 c1 bf a5 b0 21 5b d7 35 ea c4 ef a4 4c c3 64 f3 20 5c 73 73 5e 40 ec 28 c4 85 69 a6 34 f2 42 a0 95 8c 83 24 ac 0d c2 ed ba 7d 46 e7 ae f7 b6 35 38 af 97 dd 15 03 60 f5 Data Ascii: fT7(p@ 13m<Lyw@$^{p7+W,G~#,^p8cKK**FFFB;bJfVL;6JGUYFXkJS)TXocR5.H6fc};<nh)aGx`P;IU![5Ld \ss^@(i4B$}F58`
2021-09-15 12:02:48 UTC	82	IN	Data Raw: 12 c4 5a fd 37 f4 fd fb 6d 8b 04 b2 12 3b a5 89 d3 ce 83 cf ee 5a 00 98 94 87 00 7f b7 1e 31 85 4f 78 db 51 3b 12 06 c4 ee 76 ff 00 1e d8 d8 92 5f 7f 0f 48 8d 2c 93 4a 3d 37 f5 fc c1 8e 5f 31 1b 86 65 d2 3f a7 a1 b9 03 7d f7 de df f1 81 94 92 cc d5 d1 e0 8f 7e de 1a 39 5d 67 44 2e d6 0a a3 b6 f7 02 fd 7d 2f 80 b1 08 4a 87 79 36 16 e4 07 be b7 83 d1 f4 24 8d 92 de 1b 5a 0e e8 ab 02 d9 35 93 f5 36 22 e4 6d b7 a7 6f 4f 6c 2b 28 ef aa 94 d0 72 f7 58 99 20 10 09 1e df 6b 41 be 55 5c a5 55 98 92 47 4d fa 1f 71 f9 75 be 20 ae 65 03 a3 0f 2a fb fd 46 14 90 2d 4b bf e0 71 d8 6b 58 37 a2 ab 0c fb 9d 8a a3 5c 1e 9d b6 fc b7 df de d8 cf bf 6d 11 94 24 d4 82 49 f6 ce 2e 6d a0 d7 58 2b a5 2b 3d 88 3d 5a c3 a7 51 be ff 00 98 ef db f3 f4 40 6e 79 98 26 a2 88 6b 50 4f 6e Data Ascii: Z7m;Z1OxQ;v_H,J=7_1e?}~9]gD.}/Jy6$Z56"moOl+(rX kAU\UGMqu e*F-KqkX7\m$I.mX++==ZQ@ny&kPOn
2021-09-15 12:02:48 UTC	82	IN	Data Raw: 31 62 15 6e 3d c0 db f1 ed fe 71 ef 77 88 d7 a7 b1 1c 25 82 ea a6 dd cf 4d bf cd ba fa 63 1c 37 78 f2 15 a7 83 7d e3 06 75 28 bc b5 d8 1d cf d7 d0 91 63 fa f6 c6 02 40 ab 44 91 12 03 2e b6 e8 2e 01 3d 7a 5f d7 fb 0c 60 55 44 9d 2d c2 fb 47 a3 94 2e 75 13 da f7 b8 fa 93 fa df f5 18 db 63 ef f7 18 24 0b f2 89 d8 d8 c8 89 cb 1e 7d f5 5a f7 22 fb 75 eb b5 ba fb e3 29 0a f9 89 17 4b 8d 9f df 94 01 3f eb 41 14 19 80 27 83 96 bf b0 f5 a3 c3 63 83 29 a4 a5 9a 9e ae 39 0a 48 85 1c 31 df 71 b8 16 b5 af ee 4d c6 d7 d8 60 a9 a3 22 09 14 23 ac 2f c4 cb 0b d5 d8 13 f7 37 af e4 88 da 5f 81 3e 22 51 57 50 41 c3 1c 49 45 47 9c d0 55 ab 17 4c d2 28 eb 68 a6 8d 90 47 ca e5 54 73 52 25 6b 59 a3 00 02 09 da e7 1a 60 71 ab 95 89 42 66 94 14 38 a2 90 96 67 d6 9d 2c 5b a4 73 ff Data Ascii: 1bn=qw%Mc7x}u(c@D..=z_`UD-G.uc$}Z"u)K?A'c)9H1qM`"#/7_>"QWPAIEGUL(hGTsR%kY`qBf8g,[s
2021-09-15 12:02:48 UTC	84	IN	Data Raw: 7d c0 1c 9b b5 f1 73 fb 43 1e 7b 56 64 d3 32 79 49 47 78 e6 48 49 2c 40 41 ee a4 9d c0 0e 6f 0d fb 23 b3 c4 9c 14 9c 00 9e 32 a0 0c c6 8e 5a 94 55 e9 4e 0c c4 5a 24 e8 61 af ce 91 d1 a5 d7 1e bd 2d 14 24 46 f1 a8 36 1a 97 63 b1 1b 10 0a 9e c7 70 70 bf 0f 37 10 b2 52 55 dc 24 86 09 48 60 e5 b4 76 03 f3 ac 1b 88 9d 82 c1 f7 52 9e f2 46 52 b2 a2 73 33 0b 93 ad f9 37 18 ec cc 32 15 5a 19 d6 38 0d 54 fa 49 22 30 59 8e 9f 2d e4 24 90 6d dc 8b 5c df 0c 15 21 59 68 0d 5e f6 24 d7 a4 6b 84 ed 80 99 e9 69 81 29 70 18 b6 ad f7 df c0 d2 16 f9 06 63 49 c3 5c 40 95 55 70 29 11 49 1a b9 2a 1a 1d e4 09 a5 5c 1d 9d 4c 97 6e 84 5b 6d af 89 bb 32 78 c3 62 92 56 18 95 0f 7d 35 d8 3c 5b 7b 6b 09 37 b6 bb 20 cb 94 a3 f3 12 8f 98 32 86 2c 03 bb 0a 6c 38 41 87 1b e5 94 11 4c 4d Data Ascii: }sC{Vd2ylGxHI,@Ao#2ZUNZ$a-$F6cpp7RU$H`vRFRs372Z8TI"0Y-$m\!Yh^$ki)pcl\@Up)I*\Ln[m2xbV}5<[{k7 2,l8ALM
2021-09-15 12:02:48 UTC	85	IN	Data Raw: 56 6b 6a 66 70 36 37 3f db 0f be 1d ed 03 83 c5 32 54 00 51 65 06 49 04 1b df 73 ae 9c 63 9e fc 65 d8 48 c6 f6 54 c1 36 4e 72 99 8a 09 20 a9 24 24 07 15 0c 4d ea 5f 9b b5 28 22 c3 9b f8 73 c4 8d 5b 4f 33 d1 25 1c bc 88 aa 4e c9 22 ea bc 94 13 21 de 48 ca b0 6d 45 74 80 fb 74 6c 75 21 3a 54 f9 23 fb 75 13 35 45 fb b5 2e c1 dc 3b 36 fe 3a d3 e7 25 e0 97 82 c4 af 0e b4 28 49 3f 43 b9 20 83 aa 8d 75 02 f6 de 90 cf cc 22 e0 af 10 23 35 d0 4b 45 91 f1 0c d4 c5 aa e3 3f 67 93 d5 c9 a5 54 8d 51 aa f2 aa dd b4 fd cb a9 d5 e6 36 df 04 85 64 42 02 94 e4 7d 76 7a 87 15 35 0d c8 5f a4 01 88 c3 ad 2b 74 17 1b 69 6e 82 df 8e 30 9f cc f8 7b 37 c9 2a 9e 08 e1 9c b4 2b a9 63 89 cc 88 90 df cb 22 bc 65 43 46 e5 5b a9 d4 3c b7 20 dc 0d d2 b4 9a 92 2a fc 2f e5 e1 6f 28 d4 4a Data Ascii: Vkjfp67?2TQeIsceHT6Nr $$M_("s[O3%N"!HmEttlu!:T#u5E.;6:%(I?C u"#5KE?gTQ6dB}vz5_+tin0{7*+c"eCF[< */o(J

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	86	IN	Data Raw: 82 82 8b 3b 90 fc c5 8e 9f 80 f0 9b 1a 0e 1c b1 48 51 55 98 07 04 eb 41 e3 52 d7 d2 8e e8 21 ca 68 a2 48 67 78 eb 2a 4a 92 f2 bb 42 b4 d0 ba 80 ce 85 64 20 0d 3e 8b bd f0 c6 59 51 14 ab d6 db 69 d6 13 ad 2a 5a b3 04 90 49 a3 b8 a5 69 fc 45 62 f1 af 8d f2 2a 59 a9 a8 e9 de 29 24 4a c6 92 51 1a aa 84 fb 17 40 ab b0 52 bb 6c 57 60 6e 06 0a 96 90 6a 6f ae 97 e5 05 e1 30 13 66 29 7f 30 92 18 10 2b 4a 8e 3c 7d d8 79 57 f0 ae 4e 4c d0 2d 85 82 a8 27 7e 9d 05 cd bd fa f6 b7 be 1c 4e 25 68 24 8c af 4f 2e 23 96 ba f2 8e e1 82 24 14 80 1c b1 a0 e4 a7 7e 35 26 36 51 e1 cd 70 86 38 2c 64 bf 95 6e 0d 92 da 45 81 b0 23 a7 52 4e fd ce 10 ce 91 de 2c 4d 4b 55 b4 be dc b9 41 b8 b5 8c a0 2a 84 02 db 54 71 3a 9d a9 cd de 2c 6d 27 11 ac 34 ea a6 45 b0 5d b5 11 df d0 df b7 f9 Data Ascii: ;HQUAR!hHgx*JBd >YQi*ZliEb*Y)$JQ@RlW`njo0f)0+J<}yWNL-'~N%h$O.#$~5&6Qp8,dnE#RN,MKUA*Tq:,m '4E]
2021-09-15 12:02:48 UTC	87	IN	Data Raw: 99 95 0f 8d 59 0a d1 f0 d4 89 2c 9c 33 e2 2e 5e cf 37 07 f1 54 a1 99 20 a6 86 ad 00 8e 83 3c a8 94 46 17 28 ae 9a 19 e6 f2 2d 13 55 16 60 aa 47 65 4c c3 e2 11 75 26 a7 31 0c 00 d8 b6 ad 6d 0d aa 41 8e ff 00 d9 bf 1a 76 2f 6c 76 7f f7 38 45 15 62 53 2d 95 29 40 09 80 14 e6 59 48 15 29 48 05 44 80 32 80 4a c0 15 3e 5f b8 8f 89 f3 7e 3d e2 bc f7 8c f8 86 76 a9 cc f3 ea a9 67 92 39 75 7f db e5 ee c0 d0 52 d9 89 d1 a6 1b b3 e8 72 ad 20 b8 25 45 f0 f1 72 c2 11 2f 7a 16 0d ef 9e e6 d1 4a c5 62 8e 2f 12 a5 1c cc 55 b1 60 35 3e eb 10 f9 9c b4 4a 32 e8 6b 51 9e 86 a7 38 ca 29 b3 75 53 67 97 29 6a fa 74 af 41 65 2d ab e5 1e 50 81 7a 1b 1e d8 10 94 a1 64 ac 94 a4 07 70 1e d5 6f 40 f7 6a d0 b4 15 4f 94 52 a1 40 0b 16 72 ec 58 f8 fb ac 6f 1e ab f8 5c 7c 29 7c 45 c3 92 Data Ascii: Y,3.^7T <F(-U`GeLu&1mAv/lv8EbS-)@YH)HD2J>_~=vg9uRr %Er/zJb/U`5>J2kQ8)uSg)jtAe-Pzdpo@jOR@ rXo|)|E
2021-09-15 12:02:48 UTC	89	IN	Data Raw: 5d a0 9e c2 c2 4f 97 f2 cc d6 09 5a 80 64 9a b7 0b 39 27 f7 14 93 8a 7c 67 a2 cb 62 96 79 aa d5 09 40 b1 c6 d2 14 93 a5 84 ec e4 d8 2a 10 58 46 17 54 b7 b2 95 22 e5 0e 2c 66 29 96 92 09 50 2e 2a 4d b4 01 9e bb c7 47 c2 60 66 2d 8a 47 d0 41 c4 15 f7 42 13 46 ad 01 a3 0a fe e3 4b ff 00 1c bf c5 27 21 f0 73 22 e2 2e 15 e0 8c c4 71 3f 8c 79 b6 4f 59 43 c2 f9 7e 5d 2b bd 07 09 d5 d6 2b d3 47 c4 d9 eb a4 c9 23 25 2c 0d 31 a5 a3 8a 6a 69 e4 ab 08 c2 41 1a 4a f1 59 7e 11 f8 43 17 da 78 9c 3e 37 12 95 49 c2 48 98 09 2a 48 0a 58 4d 4a 3b ce 02 88 21 8b 16 24 12 19 c1 e4 ff 00 d5 6f ea 4f 64 7c 3b d8 fd a3 d8 bd 9b 3a 5e 2b b7 67 8f 93 fd ba 14 54 89 39 fb bf 35 e5 b2 b2 4b 24 a9 45 4a 42 4e 50 90 b0 b5 24 2b 44 3f 02 3c 3d 51 c5 be 3e 66 7c 65 9e 49 26 6b 9c 65 74 Data Ascii:]OZd9'|gby@*XFT",f)P.*MG`f-GABFK'!s".q?yOYC~]++G#%,1jiAJY~Cx>7IH*HXMJ;!$oOd\|;:^+gT95K$EJ BNP$+D?<=Q>f|eI&ket
2021-09-15 12:02:48 UTC	90	IN	Data Raw: 8c 3c a4 b5 5e c3 e9 f2 fd de 0f f2 a8 68 68 b9 11 53 b4 95 55 52 5b 97 41 41 4c c7 ed 07 99 79 d3 0d 7a 23 2d d4 5d 49 df 02 89 ca 53 05 51 9f 5f 3d 87 da ef 07 4b 96 96 49 15 bb 30 e2 6f 4a d3 ef bb 43 97 87 32 99 64 cc 21 39 d3 53 a6 63 3c 3c c3 49 0c ad 2c f4 51 69 d4 64 0e 43 88 14 0f bc b7 e6 13 75 46 5c 0f 88 9a 13 95 29 3f ea e6 ba bd e8 7d 6b 07 22 58 52 72 10 42 8a bb ac d5 e3 5a 0a d2 9d 77 8b b3 e0 ff 00 08 53 e6 35 30 c6 28 e4 9e 97 2f 5e 70 8a 48 65 92 92 79 19 49 15 52 99 0b 03 2a 93 a8 1d 57 b8 bd ba e2 bf 89 c6 2d 39 d2 40 23 99 bd 6b b1 e0 0d 3c a2 e7 d8 7d 99 31 53 10 a9 89 ee a4 66 49 61 52 69 e5 67 fe 62 f5 f0 76 5f 97 7c b4 02 7d 6e 44 91 20 9a 14 20 87 4b 5a 02 48 de 12 46 ea 36 be fe d8 a8 e3 31 4a 2a 53 78 3d 6f 7f e2 3a bf 66 e1 Data Ascii: <^hhSUR[AALyz#-]ISQ_=KI0oJC2d!9Sc<<I,QidCuF\)?}k"XRrBZwS50(/^pHeyIR*W-9@#k<}1SfIaRigbv_|}nD KZHF61J*Sx=o:f
2021-09-15 12:02:48 UTC	91	IN	Data Raw: 85 b5 69 04 ea d6 fd 09 04 ec 37 fa 76 fc fa 63 22 49 ca 7b a4 dd c1 1b 06 3f 7f b4 09 33 10 33 8c a0 80 19 ff 00 5e 3a b6 d6 8e 98 b3 02 d1 6c c5 8b 1f 30 bd ca dc f5 ec 0e dd 3d 6d ed 80 57 26 ea 21 87 5d 07 87 2e 5b 43 29 33 73 30 65 00 34 d2 ba 0b d4 6d f9 8c ff 00 9e b2 00 0d db 4d b7 17 b0 3d 41 38 12 6a 50 1b 93 30 25 fd 7f 8f 08 28 ce 21 b2 8a 80 41 76 bd 9f a7 ac 0d e6 33 73 41 06 c2 db df f3 d8 7d 36 eb e9 89 25 48 25 96 3b a3 8b 9e 2d 40 74 f7 78 d5 53 16 a4 8b 30 3a 5f de bd 5e d4 02 15 8b ac 93 7b 9e eb 61 d6 e0 7f bf f6 c3 39 4a 08 19 49 73 a3 6d 53 ef f3 11 29 4a 50 21 ef c3 ca 30 d6 00 df d3 bd ed b1 00 76 c4 c5 63 8f be b1 16 43 4b 7b e9 eb 12 10 d2 98 cd c1 bf a0 f4 b5 b7 f7 db fb 7d 31 14 49 05 34 68 ba 6c 00 dc f5 b7 fe bf e7 bf bf 7c Data Ascii: i7vc"l{?33^:l0=mW&!].[C)3s0e4mM=A8jP0%(!Av3sA}6%H%;-@txS0:_^{a9JIsmS)JP!0vcCK{}1I4hl|
2021-09-15 12:02:48 UTC	92	IN	Data Raw: 59 23 68 96 28 ca ac 64 87 b3 29 22 ec 19 3d 3b 11 85 2b c3 4a 2a 25 25 49 a9 25 de ef a6 b1 70 c1 f6 c4 ef ed 91 2c cc 47 72 5a 51 5e 09 03 6b 37 26 f2 87 dc 5f 18 7c 73 05 3a e5 c7 3e a8 9a 9e 55 47 73 57 3b b4 4a 62 dc 5d 2e d0 80 7a 38 65 08 e3 af 72 25 95 28 cb 50 08 51 5b 55 93 5a 51 ef b7 8c 0c ac 6e 26 6a 9d 32 11 31 28 24 99 81 9b a9 ff 00 5f fe c7 4d 44 55 cf 13 b8 ff 00 39 f1 9b c4 ee 04 ca 78 6f 29 ae e2 6e 30 cd e0 7c 8f 87 f8 3b 85 f2 97 cc b8 8b 3e cf 2a 9c 34 31 51 65 54 11 73 a5 57 11 c9 23 55 31 5a 08 60 49 a6 ab 9e 18 51 e4 56 89 93 39 72 56 c9 a2 58 a9 6a 21 29 40 6b a8 9a d9 e8 1c a8 7d 21 4a 61 15 fe d0 c5 e1 e4 ac 62 31 13 25 e1 fb e0 31 53 a8 8c c9 04 a4 27 36 66 2b 4b e5 7c a0 b9 21 35 8f 57 3f c2 93 f8 29 d6 f0 1c dc 2d f1 33 f1 Data Ascii: Y#h(d)"=;+J*%%l%p,GrZQ^k7&_|s:>UGsW;Jb].z8er%(PQ[UZQn&j21($_MDU9xo)n0|;>*41QeTsW#U1Z`IQV 9rVXj!)@k}!Jab1%1S'6f+K|!5W?)-3
2021-09-15 12:02:48 UTC	94	IN	Data Raw: 5c 18 be da c8 05 f7 d3 a9 fa fb 75 c5 07 e3 c5 09 9d 9b 2a 65 5d 52 cd c3 77 9d 4f a7 1d 81 61 61 50 3e a2 ff 00 f4 c6 24 cb ed 8f 89 92 41 f9 93 15 20 49 73 f4 a6 5a 51 9c 2b 5a b2 b2 dc 1f 08 f4 61 9c 24 f9 4f c3 b7 1c f1 54 4e e2 a2 9f 87 64 68 25 55 20 87 a8 68 e0 b2 81 d5 99 5c df fb 63 e7 79 12 52 bc 79 76 ae ba 51 fe e4 3d 34 8f b3 7b 77 11 38 49 42 64 a0 a8 4d 28 64 02 90 a1 98 04 bd 48 77 a9 a3 30 f2 45 fc 33 64 66 aa b2 85 0c 25 9d a2 a6 2b a6 26 62 39 41 58 83 ff 00 e3 30 37 63 be d6 3b 9b 82 bb 52 79 96 0c a4 b9 32 81 19 52 c7 36 61 a5 be d4 ae 90 16 1b 0a a4 61 97 32 60 06 68 48 51 43 f7 8b ba 9b 51 a1 15 3b 34 6e 56 82 9f 86 b8 2f 85 62 e2 1e 25 85 ab 69 28 a2 13 65 fc 3f 0b fc a8 cd ab d5 44 83 f9 81 23 50 ca 95 d4 3c 8c 01 e6 20 78 c8 0a Data Ascii: \u*e]RwOaaP>$A IsZQ+Za$OTNdh%U h\cyRyvQ=4{w8IBdM(dHw0E3df%+&b9AX07c;Ry2R6aa2`h HQCQ;4nV/b%i(e?D#P< x
2021-09-15 12:02:48 UTC	95	IN	Data Raw: 37 59 59 8b 3d 85 bc ad ed d8 0e df a9 19 60 28 96 dc d6 d5 af 88 b5 7c 35 88 26 12 5c 03 c2 be 7f ce d0 45 4f 96 09 e4 46 45 21 1a c1 e5 d4 5c 0d 3b 5b 43 10 a2 fd c8 b6 f8 8f 2a c5 73 06 00 d2 bd 7f 23 9f 23 02 ac 30 23 97 9b 70 89 99 32 34 31 e9 43 70 35 31 75 1f 7c 95 3d 47 40 49 b0 20 7f c4 f2 4b 90 a2 47 74 d4 3d 48 dd ad a7 e3 58 11 55 5d 9d ce fe a6 e4 52 fd 79 af 73 2c 9e 78 cb a4 51 12 4b 83 10 23 51 2f 63 b1 b7 45 22 ff 00 43 6c 31 96 45 14 14 00 e7 56 bf f2 c5 f6 88 f3 24 10 0b be b6 de cc 5f 5f d8 b9 84 d7 16 c9 50 9c e4 92 2d 25 57 97 78 dd 98 ac ab 7b ea d8 02 07 bd 80 e9 db 0f 30 ac 42 48 22 85 cd 74 31 0e 21 04 10 52 58 54 90 e7 66 e5 a7 90 e2 d5 d7 88 a6 78 9a 46 6d 4c 11 41 e6 30 b3 74 37 20 7f 5e f7 f2 9e 9d 7e 8f 24 2f 28 14 7a f8 bd Data Ascii: 7YY=`(|5&\EOFE!\;[C*s##0#p241Cp51u|=G@I KGt=HXU]Rys,xQK#Q/cE"Cl1EV$__P-%Wx{0BH"t1!RXTfxF mLA0t7 ^~$/(z
2021-09-15 12:02:48 UTC	96	IN	Data Raw: 8a 92 94 02 80 36 ab 8e 9f 4b 1f 6f ef ed eb 80 ca 88 98 4e dc 6e 36 ab 71 00 e9 b6 b1 91 2c 00 5e ae d5 d0 75 0f f9 34 b6 a6 f9 64 3b 25 ce d7 00 df 71 61 d7 a6 fd 7a 1f c2 d8 c2 aa b7 01 c1 27 85 5b f0 39 52 f7 8d 82 01 24 04 8d d9 b9 74 6e b6 2e e5 a0 d2 8e 58 c1 ef 71 60 3b 6c 3d 3f c7 b7 e3 8c 3f 31 71 a8 f0 d2 9c c5 aa c1 e3 c6 58 b1 00 16 d3 4b 68 fe 6c 6e c1 e8 20 b2 82 70 af 18 53 b3 5a fe df ad ad 6f c8 e3 35 7e 7c 79 97 67 76 db 6d 6c 20 75 25 8b 1e 60 fd c6 d6 86 36 5f 52 0e 90 3a 5f bf d7 a7 5e db 74 fc b1 b7 be 7e 90 be 63 a9 c1 36 a0 e0 de eb bc 15 c4 e3 4d f5 0b 10 3a 11 dc 6f d3 f5 c7 a0 63 4a 46 2d 44 a3 a5 98 8e b7 be c3 7f d7 f6 2f df 18 af be ba 7b bf 48 f7 0d 63 16 34 2c fa ef b0 36 dc 5f af af e0 36 fc 7d 86 33 1a 95 14 90 c1 cf b0 Data Ascii: 6KoNn6q,^u4d;%qaz'[9R$tn.Xq`;l=??1qXKhln pSZo5~|ygvml u%`6_R:_^t~c6M:ocJF-D/{Hc4,6_6}3

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	98	IN	Data Raw: f0 8a f8 47 fe 1e 99 6a 66 3e 1b f0 c4 fc 6f e2 ed 64 31 27 10 f8 db e2 08 87 3b e3 7c dd 96 20 92 8c ad a5 85 68 78 6b 2b 76 69 4c 34 19 35 35 0e 94 91 d6 6e 69 67 76 af f6 9f 6f 63 31 0a cb 26 6a 64 c9 00 bc 94 02 12 14 72 8a 0e 21 23 32 89 cc a3 53 de 24 9e 7f 88 ed 39 fd a4 a9 8b 99 f3 06 70 a3 9a 62 81 58 25 73 16 94 e6 49 60 94 99 ab c8 84 86 42 48 4a 48 40 48 1b 17 e2 1a e8 d4 72 95 93 9c ec ca a9 7d 45 96 e0 d9 57 a2 2a e9 53 65 16 b8 df 14 dc 56 21 21 4a 2b ef 2c 96 26 a7 47 f0 7f b8 02 f0 7f 63 60 f2 ab e6 cc cc a6 76 52 9c b7 2a b9 f0 70 d0 19 51 08 11 a5 53 29 66 13 06 72 2e 3e cf 57 99 2c 6e 0d d6 f7 b7 5f 43 6c 2d 28 ce ac cd 47 24 9d a9 a0 15 e9 f9 8b 3c 83 fe 45 cb 49 09 ce 92 12 7f f2 00 94 ea fa 0f 6d 09 ea 3e 20 a3 cb 33 1e 25 86 ba 48 Data Ascii: Gjf>od1';| hxk+viL455nigvoc1&jdr!#2S$9pbX%sl`BHJH@Hr}EW*SeV!!J+,&Gc`vR*pQS)fr.>W,n_Cl-(G$<Elm> 3%H
2021-09-15 12:02:48 UTC	99	IN	Data Raw: 49 b9 d0 a0 ec 5e 23 b3 a5 62 27 19 ff 00 dd 30 96 03 80 06 55 2a 8e 40 62 ad 1a f4 8e 27 da ff 00 d6 ec 51 13 fb 3f b2 bb 11 7d c1 95 38 d9 93 9c cd ae 50 5a 8c 06 57 7c 81 de 2e 8f 1e 7f 0a 6f 0e 7c 5b e1 8c c3 23 a2 f1 e3 c4 0e 16 ac a9 a7 6a 6c b6 b6 86 8f 87 c5 56 57 1a 46 63 10 98 26 cb 0e a8 9c ef 29 b8 62 18 80 7a 59 8e 03 03 22 69 03 fb 9c a0 58 06 b8 60 9b 82 1d ce c4 75 68 e7 93 7f ab 1d bd 82 2a 99 3b b1 65 e2 96 49 cd 36 6a 9d 21 24 d4 0c bd ec cc 69 51 60 c2 3c cd 7c 63 ff 00 02 4f 8b 6f 85 ba ec fb c5 2e 1c e2 35 f8 a7 f0 b2 9e 9e aa b7 32 ce 72 3c 8b f9 2f 89 1c 31 48 81 a4 69 33 2e 13 a6 a8 aa a2 e2 3a 34 5f bf 3e 50 f4 d5 ea 45 a1 cb 2a 2e 0a da a6 4b 57 cb 97 f2 a4 3a 12 df 31 41 69 fa 40 1d e4 82 1d dc 17 46 77 39 bb b5 01 0a 63 d9 df Data Ascii: I^#b'0U*@b'Q?}8PZW|.o\[#jlVWFc&)bzY"iX`uh*;eI6j!$iQ`<|cOo.52r</1Hi3.:4_>PE*.KW:1Ai@Fw9c
2021-09-15 12:02:48 UTC	100	IN	Data Raw: cc 58 69 7f 26 8e fa 9e 1d 5a d4 93 93 19 76 ff 00 f0 0c a2 da dc 6c 36 da dd 77 17 df fb b0 c2 24 94 b1 a5 cb 13 c7 c1 e9 ee d0 b6 66 23 e6 29 4a 06 8c 48 3b d5 ad ef f0 86 e3 1e 02 ac 85 2a 25 10 e9 d4 24 d4 1a 22 d6 95 7c ce bf fb 0b ed bd 8e ff 00 96 1d 48 ee 94 f7 ac e0 ea 6d af 20 7d 68 6d 10 8c 41 2f 9d 4d c6 96 e2 6d e1 6e 55 8a 87 e2 0f 0f d6 d1 53 3c 8d 0a 93 a5 c9 8d 47 9f 48 50 41 0a 46 e2 dd f6 bd ed 87 f8 65 50 15 1c b5 05 3e df f8 0c 23 55 2d c1 08 a8 6a 87 15 b3 d4 e9 c2 28 37 88 59 c6 75 47 3c bc 9c b6 ba 6e 5d f4 08 60 28 14 16 23 56 ab 85 fa d8 dc 8d ba 9c 5a b0 78 79 73 d8 cc 50 48 b9 24 16 6e 9b 7a f9 22 c7 4f 9b 2e 5e 73 87 53 07 37 0f 4e af c4 3f 86 91 57 78 a7 88 fc 4a cc 63 e5 65 99 70 a3 dd c2 d4 54 44 f2 97 65 de ec a8 c3 96 7b Data Ascii: Xi&Zvl6w$f#)JH;*%$"|Hm }hmA/MmnUS<GHPAFeP>#U-j(7YuG<n]`(#VZxysPH$nz"O.^sS7N?WxJcepTDe{
2021-09-15 12:02:48 UTC	101	IN	Data Raw: 91 eb 87 01 5e 57 1a 06 e9 e2 f6 a4 45 36 e3 ff 00 57 3a 5c 93 c3 4f 6d 0c 3c ba a8 e8 4b b0 0d 7d c1 ea 3d ff 00 7f e7 12 42 c3 73 cc fa c1 8c 15 a3 48 fb c7 61 bd 87 f9 ff 00 4b e3 d1 02 c3 17 df f3 68 90 5b 4a 35 5d 6d b0 23 70 7f 2b 1f 5b 7d 71 ef 28 8d 13 00 2c 6a 45 ec 00 eb 6b 46 6d 14 1c dd 94 ff 00 55 b4 f5 b9 26 fd 7b 5a de fd 6f 8c 7a ff 00 34 3e fe f1 14 d9 a1 cb 0a ef d3 7f 12 46 d5 78 6c f0 b5 12 17 49 0a 6d ad 7c a7 d7 ea 49 e9 7b fb 8b 0c 15 87 19 b2 87 62 c7 8f a7 ba c5 6f 19 3f fc 84 10 e0 be ae 35 a7 be 1b 18 6e 49 99 43 97 45 00 90 94 b2 01 d4 5b 6f 5d 44 76 bf de f7 eb 82 ca 18 12 fe fc 61 5a a5 99 8b 04 5a 8f fc 8b bb 68 79 96 78 cc e1 ee 34 a6 8b 30 a7 62 64 09 2c e6 1e 62 14 92 07 62 76 02 14 75 55 1d 4d 98 03 ef 84 d8 c4 66 2a d8 Data Ascii: ^WE6W:\Om<K}=BsHaKh[J5]m#p+[}q(,jEkFmU&{Zoz4>FxlIm|I{bo?5nICE[o]DvaZZhyx40bd,bbvuUMf*
2021-09-15 12:02:48 UTC	103	IN	Data Raw: 5a 25 69 1a e6 1a 56 a8 31 9e a3 1b 62 25 af 12 30 29 c1 12 a5 61 c8 33 89 7e f8 37 dd ec 37 d5 83 91 0c 7b 1b 14 b4 e2 31 bd 9d 34 83 2f 10 ff 00 25 2a a0 41 05 c3 3b b3 5e ee ed 78 45 78 9b c4 d4 cb c1 69 c4 79 5c 70 e6 55 fe 1d e7 69 c4 a6 9a 9c c4 f0 d5 70 9e 67 1a d3 66 aa d3 0f b5 96 18 22 3f 34 8a 0d 84 91 f9 8e e3 0c 0c b7 25 d8 17 a8 cb 63 b7 4b 56 1c e0 b0 f3 70 73 8e 0a 69 74 4c 04 f7 89 c8 a2 fc 77 3b 5f 8d 20 23 8c 3c 5b 9f 39 f0 df 88 e8 f2 6a f3 2d 3d 36 5b 45 c5 59 24 b0 3a 2b 54 3e 56 d1 66 54 72 a1 2c b2 22 11 17 cb b2 10 a4 c5 cc 04 79 b1 aa b0 ca 5a a5 31 ee 82 4b 0b 75 1a 59 e0 b4 e0 e4 e1 fb 6b 09 31 32 da 54 b4 29 18 b0 c7 fc 99 c7 f8 de da 6c e1 80 be a9 bc cf c7 fc aa 5a 1c bb 32 8a a2 a2 5c de 96 38 0d 44 25 ca 09 19 a0 46 44 95 Data Ascii: Z%iV1b%0)a3~77{14/%*A;^xExiy\pUipgf"?4%cKVpsitLw;_ #<[9j-=6[EY$:+T>VfTr,"yZ1KuYk12T)lZ2\8D%FD
2021-09-15 12:02:48 UTC	104	IN	Data Raw: c8 84 00 e3 27 06 30 28 93 8b c4 a1 6b 93 89 57 cb f9 4b 96 a4 09 6b 0c 28 a0 a7 20 ab 33 a9 93 a3 8a c7 5b 93 81 91 89 54 f3 d9 dd b7 80 ed 15 61 a5 fc c5 c8 c3 cb 21 69 a5 7b 89 98 54 59 54 ef 65 26 84 06 76 c0 f1 4f f8 45 fc 48 70 37 11 e5 d9 bd 1f 1b 53 f1 4c 7c 3b 95 3f 15 45 95 e7 d9 50 a3 4c de 97 2c 90 0c c6 1a 2a ca 00 20 8e a9 20 fb 9f 38 1d 1e 67 42 a4 20 d9 c1 c2 61 4c 99 d8 44 48 01 6b 41 ca a4 95 3b 93 9c 00 4e 60 52 19 29 ee 8c d4 aa 8b c2 49 73 a6 99 6a c6 4d 48 4e 49 85 d2 e4 14 b7 75 98 95 17 7a 90 e2 80 a6 84 82 39 e4 9c 3f 4d 51 95 47 51 0c 7a 63 96 30 1c 48 00 7a 7a 85 62 93 c1 22 ad d0 72 a5 56 8c e8 24 79 76 2c 31 cc d7 34 e1 a7 cf c3 ae f2 e7 29 29 17 ca 29 4e 4f fa d0 c7 42 c1 4b 44 fc 34 89 e9 00 15 cb 04 d2 e7 7e a2 dd 77 81 cc Data Ascii: '0(kWKk(3[Ta!i{TYTe&vOEHp7SL|;?EPL,* 8gB aLDHkA;N`R)IsjMHNIuz9?MQGQzc0Hzzb"rV$yv,14))) NOBKD4~w
2021-09-15 12:02:48 UTC	105	IN	Data Raw: 26 e1 f5 d6 9f 86 0d 05 9c 3f 47 25 05 2d 54 54 4e 13 52 08 4b fd b4 b2 98 26 f2 ca 23 62 c4 53 99 6e 43 05 51 7b 91 b7 79 91 8f 98 14 18 b0 17 04 f8 37 1d a3 c7 b0 b0 ca 92 0a d1 98 b5 03 52 ad f9 f6 21 b7 c1 5e 1f d5 39 4c b6 87 37 a8 35 1f 34 73 5a 0a 6c d6 a1 8d 00 43 1f 9f 2c 6a 69 61 93 45 13 58 a3 e8 6d 40 1b e9 63 be 08 3d b0 a4 10 14 4d 48 05 ce be 23 8d b5 f0 85 ca f8 64 14 a9 58 74 04 a8 17 ab 36 51 56 b0 2e 76 af ac 1b e5 3e 1a 78 5c d9 ec 95 95 3f 0d 34 d5 d5 29 58 b4 59 97 2f 3d 6a 7a 48 73 96 25 56 a2 6b d2 2a 9a 6a 89 09 9f 99 18 71 1c 4c ba 94 1b a8 da 6e 2a 4a d0 17 99 00 9a dd 2e 2b e3 5f 37 f0 1d 12 71 d2 cf cb 91 25 49 5a 2c 72 a9 21 4a d2 ac 43 11 b9 6d e2 f1 f8 2b c3 59 97 13 52 2d 47 12 70 75 2f 08 65 fc 21 53 5b 06 55 c3 19 6d 67 Data Ascii: &?G%-TTNRK&#bSnCQ{y7R!^9L754sZlC,jiaEXm@c=MH#dXt6QV.v>x\?4)XY/=jzHs%Vk*jqLn*J.+_7q%lZ,r! JCm+YR-Gpu/e!S[Umg
2021-09-15 12:02:48 UTC	106	IN	Data Raw: 55 24 95 15 75 28 a0 a2 e7 9c 4b 34 48 dd b5 54 43 1d ed 6b 5c 2a 29 db 73 8d b1 33 12 99 59 92 d9 59 ea 4d cb 3d bd 3d 95 f8 63 37 e6 84 28 ca 4a 95 52 9f ed 84 d5 80 4e 8b 23 ba 0e 81 9c 56 d0 b3 a5 cf 68 b2 ec ff 00 2f 9e a7 33 ca 68 23 96 96 49 e5 97 2d a0 86 a2 5a b7 d7 cb 86 2a 09 f3 0e 65 45 44 91 7f e3 90 c2 a8 03 6f 73 7c 57 d5 da 41 2a 1c 0d 0d ba 8e 3e f5 78 79 3b 09 34 c8 5a d3 25 00 29 24 77 8c c4 a1 5c 82 08 21 b6 2f 4b 07 78 b2 59 6f 14 d3 d3 d3 53 42 e9 53 3b bc 71 d4 09 33 33 4e 6a a4 04 2f da 68 89 41 85 48 20 2c 6d 76 52 18 5e c6 d8 95 5d be 12 c9 77 26 a1 c8 b9 0f d0 7f 26 f1 48 57 61 4d 9d 39 53 46 49 69 05 60 14 19 b6 21 ac b5 ab bc fc 00 3e 70 51 0f 10 54 55 29 8e 18 84 6a c6 fe 58 82 a9 bd 94 12 c0 d8 90 09 b5 c7 51 d3 7c 6d 23 b6 Data Ascii: U$u(K4HTCk*)s3YYM==c7(JRN#Vh/3h#I-Z*eEDos\|WA*>xy;4Z%)$w\!/KxYoSBS;q33Nj/hAH ,mvR^]w&&HW aM9SFIi`!>pQTU)jXQ|m#
2021-09-15 12:02:48 UTC	108	IN	Data Raw: 14 a0 95 36 58 79 d9 5d 9f da 3f 11 62 e4 76 7f 65 cb 4c a9 8a 5a 51 3f 1a b1 9a 5e 15 00 81 37 16 a4 82 ea 0c 48 42 03 05 4c 52 42 ca 65 e7 5a 7f 4c 8f e1 8f fc 37 fc 0c fe 1b fe 0d 53 f0 af 03 65 8b 9a f8 8f c5 19 7e 59 3f 8a be 21 d7 45 1b f1 07 18 67 70 40 cc d0 b5 43 29 7a 5c 9a 8a a6 6a 93 43 96 c6 44 14 dc d9 39 4a bc c7 d5 f2 67 c4 bf 19 76 a7 c5 dd a5 fd fe 2e 70 38 54 a9 5f 22 50 55 25 ca 04 fc b4 21 c9 2c 05 d4 a2 54 a2 49 51 52 8a 89 ee dd 9f f0 e6 17 e1 ec 10 ec ee cc 96 a5 ad 4a cf 89 c5 a8 e6 99 89 9e af fb d8 99 cb 61 99 73 08 7f f8 24 04 a5 28 42 12 84 a7 68 79 66 69 04 92 ca 65 85 a6 71 e5 48 b5 0b 05 b7 f4 22 90 35 0d 85 c8 22 d7 f5 16 59 2b 17 22 64 d6 32 81 59 14 dd bd bf dd af 13 e3 3b 3e 6a 10 95 a6 6e 51 90 66 a3 d4 55 4f cd ee 2b Data Ascii: 6Xy]?bveLZQ?^7HBLRBeZL7Se~Y?!Egp@C)z\jCD9Jgv.p8T_"PU%!,TIQRJas$(BhyfieqH"5"Y+"d2Y;>jnQfUO+
2021-09-15 12:02:48 UTC	109	IN	Data Raw: b6 7e 9a 03 ef 78 68 65 55 bc b5 90 11 1f 94 ea 60 59 43 58 ef b0 b6 e2 db 0b 7d 2f 8f 7b a7 1f 77 81 66 a4 92 e9 b0 3c 6a 1f 99 e7 ee 86 94 75 f7 81 59 39 60 35 80 2c ff 00 74 7b 28 e8 c0 f6 ff 00 6b c4 b4 66 a8 ae 84 3b 75 e3 4d f8 44 6b 40 34 b5 7d 7a db c3 c8 80 4f 41 55 34 70 92 f5 4a e8 4e a3 d3 58 3d 06 fd 7a 77 f6 f7 c4 0a 96 52 fc 2d c4 70 e5 af da 20 98 94 14 81 ad 01 03 71 af 0b 7e eb 43 dc 9f 38 34 f2 d3 05 61 34 3a 0a 98 df a2 17 6d c9 27 55 f7 37 22 de d8 d2 9c bd f5 f7 e6 ba 66 19 40 a8 a2 c6 bc 45 34 e0 fb 90 d0 ea c8 e6 8a 63 01 79 c2 1d ac da 42 80 ce 46 98 f6 02 e3 df f3 df 19 c8 54 1d 9f 29 f5 f6 38 75 84 58 94 2d 22 67 95 cb 1f 77 d6 1c d9 24 72 22 c0 24 95 e5 56 76 88 a3 aa 84 91 af b2 a3 74 1a ba 06 07 bd 8f 5d 98 e1 a6 32 42 46 8c Data Ascii: ~xheU`YCX}/{wf<juY9`5,t{(kf;uMDk@4}zOAU4pJNX=zwR-p q~C84a4:m'U7"f@E4cyBFT)8uX-"gw$r"$Vvt]2BF

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	110	IN	Data Raw: 27 b6 d5 b6 db eb 10 2d f3 11 b1 f7 41 48 97 9a ac 0d 94 82 b6 f4 5f 41 df bf f9 bf e5 90 93 ae 6f 36 27 87 87 0d 45 a2 25 0d 40 ab e9 7f 1f 38 e1 4f 55 76 50 6f 72 7f cf a0 f4 ed d3 19 ca 76 3d 5f 95 7d 98 8e a0 92 cc 00 3b 86 a5 eb f9 3a f0 83 ac ba 71 a5 2e a7 62 00 ed b5 bf 7f eb 89 10 92 1f 8e 9c 7d f3 e9 10 4c 52 54 74 61 73 bf be 9c 00 82 ea 69 b9 db 0d ec 36 3b 7a db b6 24 81 9e b5 d0 82 dc af 77 f5 e9 b1 05 39 b7 b7 94 0f f3 fe f8 d1 49 7b 00 f7 e7 10 2c 02 b3 6b d0 9b 0f c4 1a e5 ca 0e 83 6b ec bd 0d ff 00 7f ef b7 6c 46 12 a3 4a 8b d4 86 fc fe 77 8c 7f c5 bc 48 a5 2c c7 87 85 1c eb 0e 0e 1d a3 59 64 0a 40 3b 85 20 fe 0d 61 b7 ae df 53 b6 0a 96 92 54 19 d8 5f 8d af e1 5e 70 ab 14 03 a8 9d 09 6f 2a f2 de 1d 99 7d 0b 7c b2 08 47 98 ed a8 5b cb b6 Data Ascii: '-AH_Ao6'E%@8OUvPorv=_};:q.b}LRTtasi6;z$w9I{,kklFJwH,Yd@; aST_^po*}|G[
2021-09-15 12:02:48 UTC	112	IN	Data Raw: ce 5b cb 1c 51 06 62 4d 82 db 0e 7b 3f b2 e6 63 a7 a2 4e 16 41 5a 8a 82 49 c8 4f 79 ea d7 77 3b 7d eb 17 6c 7c 4f 82 f8 73 b3 b1 18 de d7 c4 c8 93 85 4a 14 b9 6e a4 a6 6b 00 48 ab be 56 e3 ac 69 db e2 0b e3 f3 32 f1 57 2c ce 33 18 7e 73 85 fc 11 49 e4 a5 e0 fe 07 a0 8d b2 ce 21 f1 83 36 47 0d 0a 67 55 51 68 a8 c9 38 1b 2f 93 5d 45 72 44 b1 d5 67 08 1e 90 cd 15 33 18 ab ba bf 62 fc 2d 84 ec e2 17 8a 02 66 34 0c ca 41 ef 49 92 84 9a 66 60 5d 65 c5 01 29 14 49 0b 5a f2 a7 e4 af 8c ff 00 aa f8 ff 00 8a 95 36 46 1a 60 c2 76 36 19 fe 56 5c f2 f1 78 f9 a4 82 82 85 66 49 12 01 a5 89 98 e5 4f 2e 5a 3e 64 dd 52 e6 b9 a5 77 16 e6 19 96 77 9d 54 fc c6 6d 9a e6 49 1c d1 d2 40 94 f9 74 54 e8 14 c3 41 97 c0 84 2e 5f 43 44 a5 62 86 08 c3 f3 11 0c 93 49 2c 8e ed 8b 44 d4 Data Ascii: [QbM{?cNAZIOyw;}l|OsJnkHVi2W,3~sI!6GgUQh8/]ErDg3b-f4AIf`]e)IZ6F`v6V\xfIO.Z>dRwwTmI@tTA._CDbI,D
2021-09-15 12:02:48 UTC	113	IN	Data Raw: e0 3c 5f 64 2f 1b 87 13 64 20 99 a8 57 79 22 a7 28 00 97 0c 1c 3b 93 4a 5b 8c 39 ec 9e db 18 10 65 28 66 0a 5b d6 b7 d8 74 a8 d3 94 5a 37 ce 93 31 a6 5c d2 86 78 e4 86 55 56 01 0b 11 a4 8b ab 3b 30 17 2c bb de c7 73 b6 dd 57 84 14 00 92 32 e5 19 72 80 cc de 37 e7 c6 f1 60 f9 e9 c4 e7 9e 90 00 50 4b 01 63 53 5e 0f ea f1 95 41 50 b3 c8 82 a4 eb 52 41 2a 18 06 07 4d c0 1e dd cf be c3 df 60 75 a1 e7 68 f4 8b 1f 60 77 85 fa fd c4 14 cf 1d 31 85 85 30 55 62 40 21 88 f4 ea 08 da fe f7 bf d3 6c 6a 52 f4 17 e1 ab d3 9e 9d 78 98 21 ce a4 80 2a 5c d6 95 e6 18 57 67 1b c2 e3 3f a8 58 a6 86 1a 65 66 91 97 ed 1c 13 75 27 ad 8d b5 1d ec 36 be d8 2a 40 29 de dc 9b f9 f4 17 85 b8 99 a9 44 c3 72 09 35 a5 48 7a bf 27 7f 5a 44 44 12 4e d1 87 9a 6d 25 4b 09 91 b7 d1 1a 11 62 Data Ascii: <_d/d Wy"(;J[9e(f[tZ71\xUV;0,sW2r7`PKcS^APRA*M`uh`w10Ub@!ljRx!*\Wg?Xefu'6*@)Dr5Hz'ZDDNm%Kb
2021-09-15 12:02:48 UTC	114	IN	Data Raw: 26 58 f5 8f 1a ac 8e cd 3b 45 cb 4d 3a 11 35 26 82 db 0d c3 2e de d6 c3 8c 1a d2 94 90 48 0d 42 48 ab f5 e4 fb bd 68 ed 15 75 60 8f 68 4d 5c c9 b3 32 17 ff 00 72 40 da 83 4d 79 de 3c ac 78 a3 5d 1c 89 51 67 1a 74 91 61 db 6b 5b f3 3d 7d b0 a1 0e 16 34 21 fd 0c 7d 30 00 6a 06 ab 73 bb 3e cc 39 de 28 af 14 5a 4a 89 ac 77 bd b4 8b 7a 86 bf e3 6f df 76 52 49 e1 fe be 7e fd 60 1c 60 2c 1b dd c5 ed c2 03 79 5f fc 7f 5f f7 c1 e8 1a b9 db a5 37 85 33 01 0c fe 1f be 3c 36 8e f8 d4 ae 9e bd ba f4 fd ff 00 a6 24 88 c8 ab ea 2a 2b bd ff 00 83 51 e3 13 f4 9d 47 b6 e3 ea 4d b1 a2 92 2a 75 bf 80 83 e4 a8 29 09 0a af 5d 5c 80 f0 47 12 dd 08 bf 53 fd 8f f6 ff 00 37 c2 b3 73 ff 00 b1 36 10 d3 0d 97 21 0a d1 54 be c3 6f bc 66 68 8e d6 0c 01 bd ee 40 f4 e9 b5 ce 04 9b af fe Data Ascii: &X;EM:5&.HBHhu`hM\2r@My<x]Qgtak[=}4!}0js>9(ZJwzovRl~``,y__73<6$*+QGM*u)]\GS7s6!Tofh@
2021-09-15 12:02:48 UTC	114	IN	Data Raw: f9 62 d4 40 0d d7 bd b6 fe f8 86 27 ce 38 f9 7e 62 7a 0b c4 81 7e f5 d4 0b a8 f4 f7 fa f6 c6 c1 2e 09 d0 3f 5e 11 ef 98 38 fb eb 12 b1 10 74 db de ff 00 97 fa df f7 7c 0b 13 7c e4 71 f0 8c 9b 9f fd 8f e7 88 0d cf 33 eb 13 a6 72 18 5e c3 4f c4 65 53 a9 66 fb c6 f7 1e 5f 52 3a 0f df ae f8 15 60 fc c2 5d 87 da fd 20 84 ad 26 59 50 e3 5b 35 4d fa 50 6b b5 e2 76 98 32 5b 7f 7f df e6 3a 7e 98 f3 54 9d fe c3 4f 38 18 97 2f 12 45 d5 d7 ef 10 6e 3b 0e b6 e9 bf ef fc e7 df ef f8 8c 47 d4 7e 5b 03 73 d4 79 bb 8d fd 06 3d e9 1a a9 8a 4b d9 a0 bf 2d ab d9 77 f6 37 27 d0 7a 6f fd bd b1 22 00 62 75 76 7b eb b0 f5 f1 b1 85 53 94 42 b2 8a 24 1a eb af 8d 1f d9 83 7c be a1 23 17 0d ac f4 0a 0f 5b 9e bd 6c 37 18 25 12 16 6e 7c ab e1 11 66 2f a0 b6 87 56 f1 fe 78 41 a5 0c a9 Data Ascii: b@'8~bz~.?^8t|q3r^OeSf_R:`] &YP[5MPkv2[:~TO8/En;G~[sy=K-w7'zo"buv{SB$|#[l7%n|f/VxA
2021-09-15 12:02:48 UTC	116	IN	Data Raw: c4 1c 65 99 c1 24 f2 29 a6 e1 fc 86 96 3c be bb 3a cf 73 37 46 64 a6 a0 8d e4 13 08 9c 82 b2 4a 4f 2e 14 d7 2c ad 1c 51 b3 87 bf 0f f6 06 2f b7 31 23 2c a5 7c 93 ff 00 f9 0c 52 8b b6 63 b3 75 8a b7 c6 7f 1a 60 7e 10 c0 9c 5e 36 6a 15 36 68 22 4e 19 24 15 d6 80 30 72 a2 6a 19 9f 5d e3 ca 17 8e 9e 3f f1 c7 c5 57 1f 56 71 3f 1d 57 d4 65 3c 09 91 cc f5 19 77 0a d3 cd 22 50 65 59 57 3a 43 4d 05 5a c4 dc aa cc ff 00 30 40 8a 27 50 eb 4c 81 e3 83 41 67 66 ee 38 3e cf c3 76 26 15 12 24 21 2a c5 94 a2 59 9e c0 a8 a8 06 56 42 43 84 97 a1 71 98 d5 54 01 31 f1 ff 00 c4 ff 00 11 f6 d7 c6 b8 d3 8d ed 3c 5c c9 58 34 2c ab 0b 80 4b 89 5f 20 2c 29 02 7a 12 a5 21 53 19 29 ab 10 90 e9 0e ea 30 8c ce b3 ea 8e 23 cd 23 ae aa d1 05 15 3c 6b 49 94 e5 c8 bf f6 f9 46 57 08 d1 05 Data Ascii: e$)<:s7FdJO.,Q/1#,|Rcu`~^6j6h"N$0rj]?WVq?We<w"PeYW:CMZ0@'PLAgf8>v&$!*YVBCqT1<\X4,K_ ,)z!S)0##<kIFW
2021-09-15 12:02:48 UTC	117	IN	Data Raw: 5e f5 49 32 67 a3 16 99 b3 a6 ae 52 01 04 66 7b 3d 1d cd 6e f4 f2 8e f3 8e ec f5 4a 94 ac 44 a9 93 31 a9 4d 4a 70 e8 41 3b b3 bb bd 98 bd c3 bd 9a 9b 7c 70 7f 0e 5c c7 2b 4a af 17 3c 0b 85 33 de 1e aa 86 4a fc f7 84 a1 94 34 8d 34 8b aa 4a ec b1 93 5f 2d a1 8c 1b c4 3a 9d b6 26 f8 bd e1 b1 29 9c 84 a4 2d 2b 09 a0 50 ca 90 ae 2e c6 bd 48 35 e7 1c f3 19 34 ae 6a ca e5 cc c3 a9 4a 27 24 d4 ff 00 92 59 14 65 00 1a b7 35 2d 7a d8 f9 f3 f1 2f 86 38 8a 9a e9 53 91 e6 b4 ef 10 48 99 66 a1 ab 4a a8 e5 04 46 01 8c 42 58 98 ee 01 60 37 5d fa 8d ec 9d 8c a9 32 66 af e6 4c 42 50 a4 14 94 af 72 2f 53 4e 5b 88 09 72 0e 47 42 d2 a5 86 50 01 ba 57 df 08 b8 7e 03 2f 10 ff 00 f9 33 a2 8b 89 21 a8 a7 ac 58 64 64 8e ae 09 21 9c 52 ee 20 12 2c 96 60 c1 14 11 70 08 04 5a f8 aa Data Ascii: ^I2gR{=nJD1MJpA;|p\+J<3J44J_-:&)-+P.H54jJ'$Ye5-z/8SHfJFBX`7]2fLBPr/SN[rGBPW~/3!Xdd!R ,`pZ
2021-09-15 12:02:48 UTC	118	IN	Data Raw: 8b fe 37 e0 dd 0b 64 d3 41 4c 90 42 e9 19 21 63 bc 68 23 b9 51 62 a6 53 b1 f7 6d ef b9 f6 c4 88 9a a0 32 91 41 66 bb 71 f5 1a c2 ff 00 93 f3 a6 7c c6 3b b6 87 47 d5 9a ed ac 61 d3 50 54 be b9 8c d2 d3 bc 8e f7 74 bb 4a e8 0a e8 d7 a4 36 c4 5c f4 00 10 07 5d b1 24 82 92 15 97 73 52 77 df df ee 29 f9 10 73 2b 30 24 b7 74 b5 b8 38 1a 47 91 0e 3c cd 9a 63 28 0d 7f 38 b8 bf 5b 8e e2 e6 c0 f6 3d ef d3 be 05 55 3b cd 6f 37 a7 94 7d 19 41 7f 2a be a2 f6 d3 4a bb 35 0c 55 fc d5 75 d4 4c c7 cc 49 3d 3a 6f 7f ec 06 e6 fb f7 c1 f2 41 01 2f 72 d4 3a 57 ce fa 52 07 c4 9e e8 2d a1 d7 8f bf 5d 20 58 80 84 8e 86 e7 af 4b 76 b7 6f af e1 86 08 b7 58 4d 88 20 d4 06 d7 7a 57 c8 56 3b 94 82 a2 c6 f6 b0 c6 f0 22 55 99 e8 cd 12 94 8c 15 41 bd 88 e8 3b df 51 b7 ef d4 63 c6 a0 8d Data Ascii: 7dALB!ch#QbSm2Afq|;GaPTtJ6\]$sRw)s+0$t8G<c(8[=U;o7}A*J5UuLI=:oA/r:WR-] XKvoXM zWV;"UA;Qc
2021-09-15 12:02:48 UTC	119	IN	Data Raw: d2 90 83 15 83 ca b0 c4 b5 6c 1a fa ed ed a0 f5 78 e6 8c b0 e7 67 35 b4 8d 0e c7 ed 5e 37 65 61 7d 2a c8 0a 29 1b 10 e2 f6 ea 6d 87 52 65 94 54 24 b9 6e 7c ba b7 13 a4 26 9d d9 ca 52 9c 21 07 7f 9a 72 0a db 42 c0 ea c2 9b 40 07 12 56 52 e7 31 54 35 0e 6b 34 d5 4a 44 ee 6b 6a e1 cc 59 c2 12 c8 54 49 1c 52 2d ba dd 64 b2 93 b8 07 6c 36 96 9c e9 4a 94 3b c7 af 85 1f 97 de 25 c3 3e 1d 59 7f b6 95 4b aa 5c cc c8 3c 94 d5 dd b7 a7 18 07 91 c2 bc d5 52 c5 2b 05 a0 90 b2 c4 6a 22 79 66 d0 43 14 d1 23 a2 dc fd d2 10 93 bd 86 d8 99 38 73 99 25 b3 16 bd 80 3a 8b 9f 7d 23 69 d8 86 55 29 7f 6c c4 fb 0f 09 6e 2f 32 4b 24 67 2c 89 e9 52 9e 05 0e 63 9b 9a ed 52 3e d8 3b 0a a5 6d 5a 5d 06 ab 2d c5 c8 37 17 18 99 52 0a 5d 6c dc 39 0e 70 4e 1e 7a 48 42 54 4b 28 80 f7 f0 d3 Data Ascii: lxg5^7ea}*)mReT$n\|&R!rB@VR1T5k4JDkjYTIR-dl6J;%>YK\<R+j"yfC#8s%:}#iU)ln/2K$g,RcR>;mZ]-7R]l9pNzHBTK(
2021-09-15 12:02:48 UTC	121	IN	Data Raw: d0 b0 d1 df 5b d3 68 2d a6 c9 e0 99 44 8a 84 11 66 2a 07 de 1d 48 6f af e9 fa e2 e7 86 c3 84 85 31 72 c0 83 e3 6e 1e f5 a2 09 bd a5 35 1d c2 b0 c6 8e 58 d7 f8 d6 f4 d4 88 32 ca 92 08 c8 42 a2 eb 6d 48 4e 90 b6 da de 61 63 6e db df d6 d8 77 81 5a 85 14 a0 03 16 25 85 45 6b cc 59 b4 3a c5 6f 1d 31 53 4a 88 20 bf fe 2e e7 c0 3f 1b b5 84 75 f1 56 6f 0c 54 8d 0c 04 17 ea 42 b0 60 3c bb f4 36 bd ef fe 98 23 17 89 50 41 4a 56 92 14 2b dd 0f a5 bd 6b 62 38 c6 fd 87 d9 d3 17 34 4d 5a 6c a0 47 75 aa f7 ad b2 81 e1 14 0b e2 2f e1 e6 83 e2 bb c3 be 34 f0 3f 37 e2 2c d3 85 b2 8e 36 a3 92 87 36 ce 32 58 e9 db 31 82 9a 73 69 23 a4 35 51 4b 14 4e 14 9d 32 08 de c7 7d 37 c5 3b 1b 3d 2a 25 0a 50 0e 08 35 6a 1a 11 cd ad a1 07 48 ec d8 5e d4 97 f0 ee 16 5e 3f e4 a6 72 e5 e5 Data Ascii: [h-Df*Ho1rn5X2BmHNacnwZ%EkY:o1SJ .?uVoTB`<6#PAJV+kb84MZlGu/4?7,662X1si#5QKN2}7;=*%P5jH^^?r

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	122	IN	Data Raw: 75 48 8c 01 9d 4b 48 02 8d f6 37 72 41 3b 5b f5 df 1b 56 9a 6e 2f f8 85 b8 8c 30 1d e4 a7 9a 58 7b d3 6e 1b 82 e8 a4 cf 2a 44 51 b4 4c 65 44 d2 c5 74 00 7c c3 6b dc 6f 6f 7f ef d0 a0 1d 39 b9 53 9b 6b d7 68 03 e5 00 6a 00 e0 d7 1e 5c 78 3c 1d e4 b9 b1 0c 66 91 8a 4a fe 45 0a ac 47 4f 28 b0 d8 5b a1 3f 9f a6 0e 92 b2 13 2d 49 0c 42 46 f5 f4 85 f8 99 09 21 56 ef 12 f4 b1 e0 d7 d4 f9 56 1b 99 0e 79 53 34 51 c4 d2 85 25 91 41 ee 50 0e 87 f5 da e7 e9 87 18 3c 4a ca c2 8a 88 ad 9f 6f 1b bb 80 d1 5c 99 83 0e a7 ad 09 ca df 83 e6 d5 a3 43 df 85 f3 88 a4 09 ce 66 66 89 42 8b 8e c3 a5 8f 42 0d ba da c2 c3 b5 8e 2d 58 4c 53 b9 25 ec 59 f7 d6 96 3b 79 d6 2a fd a3 84 39 88 40 6f aa db 1d 9b db f0 b3 09 33 1a 69 63 fb 28 50 2f 5d 60 dd 81 f5 fc fd b6 f5 df 0d f3 21 60 Data Ascii: uHKH7rA;[Vn/0X{n*DQLeDt|koo9Skhj\x<fJEGO([?-IBF!VVyS4Q%AP<Jo\CffBB-XLS%Y;y*9@o3ic(P/]`!`
2021-09-15 12:02:48 UTC	123	IN	Data Raw: eb e1 55 76 69 c5 b9 d3 c2 f5 df f6 c6 0a bb c0 39 9e 79 04 91 1f fc e9 79 d7 4b 1d fb 29 36 ed 86 78 3c 0a 40 1d da 82 ca 70 3f 83 5a ed 0c 97 86 4a 55 60 ec ed a5 6b d3 cb 89 85 8d 7e 7f 1d 6b 08 91 b5 31 d4 6a 16 49 79 6c d5 04 dc 48 10 bb 6c 4d c9 21 c8 3e 83 7c 5a b0 d8 40 85 20 84 da a4 b7 4e 4f a0 db 5e 18 ca 94 fd 20 de bb 6e 46 be f7 a4 0b 57 25 24 cb 32 54 d4 9a 76 55 59 24 84 b2 32 c8 f7 b2 be e4 30 20 03 f9 5f df 0e 25 e1 d8 29 93 f5 a8 37 97 0a 3f ab f1 8d 92 bf 96 b4 b0 ef 31 bd aa e1 ab a0 6b f8 9d a2 e8 f8 a2 2c 88 a8 a6 11 49 e6 b5 99 08 66 23 6b f9 88 5d af d4 0b 1e fb 03 89 57 82 f9 bf ea cc dc 28 3c f8 93 c7 c0 85 9f 9c 93 44 86 0e ce fa 69 43 d7 89 86 96 51 e2 cf cc 8a 4c ae 6c d2 92 89 65 60 5c 4f 25 2a a9 54 f3 fd e5 37 42 2e 2e 58 Data Ascii: Uvi9yyK)6x<@p?ZJU`k~k1jIylHlM!>|Z@ NO^ nFW%$2TvUY$20 _%)7?1k,If#k]W(<DiCQLle`\O%*T7B..X
2021-09-15 12:02:48 UTC	124	IN	Data Raw: 76 7a 02 e7 0a 0a 7a 54 3d 38 86 a5 3c 5a 2a 7d b6 ea 96 73 3b 35 05 aa 3d f3 a6 ef 0e 44 8d 6e 86 3d 81 21 db 6d c1 7b 5c 75 e9 63 d2 d6 bf 4c 5c 25 c8 22 58 ca 13 9c b1 4b 1a 36 ce d4 e2 3c 9c 47 3d 5a a9 30 4c 24 b3 b3 68 d4 d7 af ae f0 6b 97 d2 46 ca a4 8b b8 0b a7 61 7b 1f a7 5b fd 7f 0e f8 b6 76 64 81 91 0a 21 9a 84 7f e5 47 2d 66 7d 3a 51 8c 57 71 33 ca 49 67 cb 5a 9a 5e dc fc 2b c6 90 57 47 47 24 45 59 16 c1 b4 82 2d da fd fe bd cd 81 b7 be 2c f2 65 2b 32 69 dd 71 d7 f2 de ac f4 84 38 89 e8 5b b9 a8 7b be e5 ff 00 5f cc 4b 54 46 39 24 3d 37 2c 69 6f 3d c5 ef be e2 fe bb f6 fa ef 86 b9 12 94 82 c6 81 b4 60 4e d6 d7 47 6e 0d 00 49 51 33 43 2d cb 9a 6c 0d ed 5a d8 70 ad a1 6d 99 65 a1 84 a4 54 0b 36 a2 4e a1 75 6e a3 d4 0b 76 eb db 0a 96 02 89 bd 09 Data Ascii: vzzT=8<Z*}s;5=Dn=!m{\ucL\%"XK6<G=Z0L$hkFa{[vd!G-f}:QWq3lgZ^+WGG$EY-,e+2iq8[{_KTF9$=7,io=`NGnIQ3C-lZpmeT6Nunv
2021-09-15 12:02:48 UTC	126	IN	Data Raw: d2 11 94 38 7b b9 02 8f a1 36 22 a7 73 6e 91 65 72 1e 24 13 c7 1c 4f 24 93 46 ab f6 a2 27 d0 d7 50 02 9d 87 9a c6 fd 3a 75 c1 08 57 73 2e a5 bc 98 7d a1 1c d9 2c 4a 4f ba 72 a3 70 be bc 1c 79 2e 6a 89 00 68 d5 ef f7 87 32 52 cc 01 eb 61 7b f4 3b ff 00 c6 0b 97 49 68 1a e5 16 e5 fa d4 79 c0 33 30 e5 60 da 8f cc ed f8 a7 11 bc 31 32 5c dd d0 07 8e cc a5 b6 d2 4b 10 c4 11 d7 b1 05 8f b5 ec 6f 89 65 2c a5 60 f7 87 4b 68 79 dd aa 35 6d 61 4a f0 fd e5 3e 50 32 87 7d 07 50 fc b6 7b d9 9b dc 2d c4 1a ec fc ea 88 e5 8e c0 8b 96 53 e6 b0 53 db 4b 00 43 6f d6 c0 77 c3 ec 34 f5 0b d2 d7 1e 77 ad 87 2a 83 58 47 8b c3 a5 c8 01 2a 02 fe 3f bb 79 34 3a 32 da ca 99 10 30 30 f2 a5 62 79 77 b1 d3 d6 e0 5e c2 fd fb db be 1e cb c4 28 a7 5b 70 ad 3e cf f6 ac 57 31 38 74 85 28 Data Ascii: 8{6"sner$O$F'P:uWs.},JOrpy.jh2Ra{;Ihy30`12\Koe,`Khy5maJ>P2}P{-SSKCow4w*XG*?y4:200byw^([p>W18t(
2021-09-15 12:02:48 UTC	127	IN	Data Raw: 51 a9 a4 92 57 2c 90 36 b3 a9 57 97 b1 40 3e ed 81 b7 70 00 c3 89 38 60 05 50 7c 37 f6 fa f5 a4 4b f2 92 4a 4b 82 1d 89 2d 7b d3 d7 43 d6 20 b3 2e 2f ac 86 36 79 19 15 a7 0b 1a a2 80 cc cb 19 36 6b df 55 88 3b 81 6f 7f 4c 39 93 87 96 00 74 81 7b d8 91 4f 0f ce a2 20 9e 94 85 02 0a 43 53 5d 99 de b7 f2 a3 68 60 3a ab 8b 33 97 74 9d e7 8d 69 e2 57 b4 7a 16 fa 4d 94 0f 31 bd c0 dc 7f 9c 4d f2 13 50 12 19 80 24 07 7b d5 fc 68 f1 18 59 62 c4 74 d3 93 46 36 59 c4 d5 10 56 49 aa 9d 6a cc e1 5e 3b a6 82 b6 6d 4d ba dc 30 75 04 10 76 b5 c5 8e 35 32 02 5f bb 47 6b 1a 8a ed e1 66 e9 19 49 62 5e 94 db c2 1c fc 33 c6 a9 56 82 26 ca 24 8a 75 60 23 31 6e 35 82 05 f9 52 01 1b 8d cd d1 46 a3 da e2 f6 d5 41 49 66 4d 3d 36 b7 ea 34 c4 80 94 bf 71 cb 10 28 e5 da a4 eb d3 4a Data Ascii: QW,6W@>p8`P|7KJK-{C ./6y6kU;oL9t{O CS]h`:3tiWzM1MP${hYbtF6YVIj^;mM0uv52_GkfIb^3V&$u`#1n5 RFAIfM=64q(J
2021-09-15 12:02:48 UTC	128	IN	Data Raw: 91 4e 7b 51 b8 f0 7e 3b 5d 88 c1 e1 c4 b2 95 b8 7b 35 2a fa 72 00 1d 1a 00 f3 4e 68 a7 75 08 39 77 3b d8 5d b6 b9 df af fa 0e 96 db 09 26 54 4c 63 50 ef c3 8c 5a bb 3f 2f f7 05 f8 5f 95 20 6f 81 dc cf 9d d4 56 6b d8 10 9d c0 f2 3d 88 b1 27 a8 da e7 b7 be 29 12 e7 1f fa 8c cd 40 55 55 7d 78 3d 9b 7d f5 b3 7f 8a 51 f2 fb 32 54 b4 d1 4a 4f 75 16 24 10 ef 6a 57 ca f0 fe f9 8d 63 94 d6 53 d6 ea 37 b7 ef f7 7c 5d 30 98 82 2c 2c 00 e8 07 e1 ff 00 31 ca 46 18 a4 12 ee 3c 3a 78 6a c7 56 da 3a a6 21 25 05 00 3a 96 e7 7d 96 dd bd 86 dd 81 eb d7 7b e1 97 d6 af 98 e7 bc c5 80 6e 15 7d ab b5 37 8d e5 80 7b aa 16 b7 eb 4f 7c 61 3d e3 5f 04 e5 5e 28 78 59 e2 07 87 b9 f5 2a 56 64 fc 5b c3 99 86 53 5b 03 80 e5 be 62 9e 54 85 d5 48 36 e5 4c 51 b5 28 04 12 3c c2 d8 8f 13 95 Data Ascii: N{Q~;]{5*rNhu9w;]&TLcPZ?/_ oVk=')@UU}x=}Q2TJOu$jWcS7|0,,1F<:xjV:!%:}{n}7{O|a=_^(xY*Vd[S[bTH6LQ(<
2021-09-15 12:02:48 UTC	130	IN	Data Raw: b1 e5 1e 93 27 bc 52 53 4b 59 f5 16 fd 55 b5 15 8a 33 e2 9f 89 b3 51 d6 43 0d 03 c4 b2 73 18 cf f6 8a 5c 9d 2c 3c ea fd f7 1e 61 f4 38 5d 39 94 01 2a d4 ea 3c a2 c5 80 c3 b8 50 52 6c 3f e3 c7 d3 6f 4d 63 ce 75 44 fb 16 b9 b9 1f a9 3f bd bf 1d b1 d1 62 e1 7b f4 f4 d7 4f 56 68 16 ad 9f 62 3a f5 db f7 7f df a8 b6 3d 03 62 3e 8f 1f 4f 7e eb 10 f2 31 91 4d 96 d6 d8 db 7b df a7 61 dc 7e b8 9e 56 9f fb 7e 3f 1f 68 58 bb 0e 7f 98 e3 0c 1c c2 40 3a 48 5d f7 37 bf eb de de 9f 8d f0 4c 46 1b ed a5 be dd 69 c9 a2 62 9e 01 19 b9 b1 3b 5f 56 e2 fb 03 6f 42 7d 8f 5c 78 d0 13 b4 6c 8f a9 5b 58 3d da 91 3d 0a ec 08 00 01 7d 87 ae 16 aa 63 a8 bb de 19 a7 e9 1e f5 8c c4 8d 9a c4 5f f0 ff 00 3e df ed 8d 4a f6 f3 83 e5 ff 00 db 48 fe 23 35 63 76 bf 96 d6 fc 88 1e 9d 7f 63 10 Data Ascii: 'RSKYU3QCs\,<a8]9*<PRl?oMcuD?b{OVhb:=b>O~1M{a~V~?hX@:H]7LFib;_VoB}\xl[X==}c_>JH#5cvc
2021-09-15 12:02:48 UTC	131	IN	Data Raw: 2b a6 80 d4 45 4f 5d 50 8f ff 00 da 68 aa e4 8a 34 13 0b 4d 1c 64 d9 81 24 61 c6 03 b3 24 62 67 ca 93 29 e6 66 58 b5 54 a2 4e 56 61 56 e1 53 6a e9 14 0f 88 7e 27 47 67 e0 b1 33 90 40 28 96 b3 9d 45 80 00 54 d5 80 0c 09 75 52 8f a3 c7 9a 8e 26 f1 ff 00 89 bc 40 e3 4e 31 f1 03 32 a5 58 e8 f8 9f 35 9e bb 29 ca 53 56 ae 1a c8 d0 88 f2 6c a4 4c 84 ad 5d 42 65 a2 9f e7 64 5b 27 f3 07 a9 a8 0a ba 82 af 49 9b 83 c3 e1 be 5e 1e 50 0f 2d 09 0a 53 be 65 26 84 81 4e eb fd 3b 86 51 00 92 07 09 c1 7c 57 da 13 57 33 19 88 72 99 ab 51 97 2c 9a cb 04 ba 52 a0 28 56 10 01 5b 12 12 a2 50 14 a0 90 a2 bf ce 38 d3 3a e2 68 fe 44 33 c3 0c ec 00 0c ce 5f 49 36 20 dc 8f 32 af 7b 6c 45 c0 be 32 80 12 46 c3 dd 5b 7b 72 da 07 ed 2f 88 31 58 b7 01 2c 15 40 de fe dc ef 0a ca ca 01 4d Data Ascii: +EO]Ph4Md$a$bg)fXTNVaVSj~'Gg3@(ETuR&@N12X5)SVlL]Bed['I^P-Se&N;Q|WW3rQ,R(V[P8:hD3_I6 2{lE 2F[{r/1X,@M
2021-09-15 12:02:48 UTC	132	IN	Data Raw: 10 c2 45 00 11 72 09 36 b9 e6 2b 29 8f dc 1b dc 8f 50 31 e5 4e 0e 33 b6 94 b9 61 4a 5c 39 fb e9 0c 65 a0 19 92 56 54 ca 96 41 00 73 0c 7d f1 e1 1f 96 ef f1 9e f0 be 9f c3 ef e2 8d f1 49 96 40 8c 90 67 79 af 0f f1 94 25 95 52 c7 3b c9 60 13 18 82 8b 08 de 5a 77 e6 30 be a9 b9 87 bd 85 a4 4d 07 01 23 e5 97 19 e6 a5 83 06 4b 4a 25 34 d7 31 cd 56 be c6 3a 96 16 67 ce 91 29 73 09 50 08 4c b4 a9 ce aa 52 c9 20 93 50 e0 50 58 97 7a 98 a7 9c 0f 53 35 35 3c 01 4a e9 6b 2b c6 48 2a ad 70 10 81 63 d4 01 bf 63 6c 2b 29 41 72 a1 61 76 d1 b6 df f8 da 1f e1 16 a9 40 31 64 d9 b9 8f 01 4e 1e 50 f9 ca 6a dd a2 8e 09 1c af da 2c 8b 20 7b db 63 75 be e6 d7 ed db 0b 56 93 99 45 36 a9 7e 1a f2 db 6e 24 43 fc 3c c2 a0 4d 08 63 ae c0 97 e1 c1 ef c6 0a a8 aa b5 d4 c9 25 fe e3 88 Data Ascii: Er6+)P1N3aJ\9eVTAs}I@gy%R;`Zw0M#KJ%41V:g)sPLR PPXzS55<Jk+H*pccl+)Arav@1dNPj, {cuVE6~n$C<Mc%

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	133	IN	Data Raw: cc 18 1f 28 eb b1 37 b5 bd 7a fb 7e 27 7e f8 f6 75 6c 7f fe 9f 1a 18 91 29 a1 71 c3 df be 51 cd 21 6d 57 be c3 b0 da d7 fc bf 7e f8 c4 69 bf dc 7f 3e bc e2 6a 8d 80 5b 03 f7 4d 8e df 81 fe f8 f6 52 a0 5a 3c 6a 47 e7 60 de a0 1e 50 55 42 c8 cc 2f a4 d8 00 07 40 00 fc bf 7d fa 61 79 4e 55 ac 7f eb e6 38 41 a8 fa 47 5f 53 06 34 46 fc bb 13 a6 dd 3f 2f f9 be 05 4f d4 ae 9f 7f 4b 46 fa 0e 5c 77 fe 43 70 7d 60 9e 9f 65 52 36 20 8d c7 ff 00 8a 7f 7f df 1b 44 0b fa 8f 4f 48 9d a3 0a 48 2c 2f d0 9d 85 ef 7f df e1 f9 63 d1 a1 0e 08 05 9e 18 19 6a 95 e5 90 6c 08 e8 36 fd f6 3e 9d bb 60 99 3a 72 3e b0 be 72 5b c7 5f 37 f7 f7 83 ca 36 48 53 50 36 03 7e 9d c9 ff 00 3f 9e 09 47 d4 3a fa 42 f2 a0 9a 9b 7b d6 09 68 67 79 24 5d 17 75 d2 1b a8 bf 72 4d 8f a7 fa ed 83 51 64 Data Ascii: (7z~'~ul)qQ!mW~i>j[MRZ<jG`PUB/@}ayNU8AG_S4F?/OKF\wCp}`eR6 DOHH,/cjl6>`:r>r[_76HSP6~?G:B{ hgy$]urMQd
2021-09-15 12:02:48 UTC	135	IN	Data Raw: 84 50 56 d2 ca c2 75 5d b8 87 8a 69 e2 9d c0 12 d5 37 23 2e cb 2a 96 34 2d 4f 15 79 8d 98 4f ab 1c 5b fa e5 f1 4a b0 fd 9b 87 f8 67 01 39 33 26 4d 57 cc c5 21 25 25 68 59 19 44 ae ef 78 64 04 e6 0e e4 a9 96 02 92 00 eb 9f d1 fe c2 98 9c 6e 2b e3 1e d3 49 44 a9 b2 d7 83 ec e2 a0 a0 15 21 2a 00 4c 40 50 01 42 72 a5 a1 68 50 cc 15 2c 21 68 2c a3 1e e2 b8 63 87 93 27 cb e3 a5 48 84 9c b4 61 cc 0a 03 18 9f 66 01 8e fe 56 01 41 ea d6 24 ee 4e 3e 70 44 b9 a9 4a 25 e4 64 84 27 33 8a e6 6a f8 92 5f 84 75 b9 bd a1 3a 7c c5 a9 7a cc 50 1b 64 07 bb e5 ad 83 5a f0 3f c4 bc 39 55 98 d3 b4 70 9d 35 06 69 34 4c e4 83 1c 1e 66 68 86 a3 62 af 73 6b a1 6b 8d 85 b7 32 a2 57 ca 0d bd 7f 8d 3f 98 79 d9 b8 a9 58 75 09 a4 67 ca c4 80 ce ef b7 8b 75 a9 84 e6 55 e1 0e 5f 95 1a bc Data Ascii: PVu]i7#.*4-OyO[Jg93&MW!%%hYDxdn+ID!*L@PBrhP,!h,c'HafVA$N>pDJ%d'3j_u:|zPdZ?9Up5i4Lfhbskk2W? yXuguU_
2021-09-15 12:02:48 UTC	136	IN	Data Raw: dc 1d 40 5c 7b 01 f9 e3 5f 56 d0 fa 7e 4c 79 a8 ef b7 0d ad 57 a1 a5 9a f1 33 4f 03 bb 02 cd a2 fd 02 d8 9d fa 0b f7 1d af ff 00 38 20 58 72 1e 91 38 b0 89 b5 a2 7b a9 d0 d7 5b 11 d4 a6 e6 fd 7b 8e e7 6d ba 62 54 ac 00 05 63 d0 57 97 a4 d5 10 b2 ca 88 fc b8 f4 06 4d 20 00 bd 00 be fb 77 00 f5 c6 e2 60 0e 1c 8f 7a 5e 30 d6 e1 f8 68 23 a5 8e 4e 4a 20 50 39 7b 29 20 03 7d f6 b8 b7 bf 7f cc e3 49 8a 2b 01 8d 52 a0 76 a7 85 79 46 8b 21 99 ea ff 00 98 cc a6 a7 9c 4c 43 3e 97 7f 2a 91 b9 02 fe 61 6b 9b f5 06 df 5d f1 b0 39 80 ff 00 c6 fe f4 15 8d 1d 98 d4 36 ae 3a d1 b6 de 9a 41 5e 5f 5c d4 4c da 18 ca f0 01 6b 9f bc e6 d7 04 0e d6 b5 bf c6 31 36 5e 64 8f 16 f4 d7 cb a4 6e 10 f5 77 e5 7b 3f f3 7e 70 de e1 9a e9 63 9a 19 b3 05 2d 11 bc 8c 17 6d 4d 20 b8 d8 7f 52 Data Ascii: @\{_V~LyW3O8 Xr8{[{mbTcWM w`z^0h#NJ P9{} }I+RvyF!LC>*ak]96:A^_\Lk16^dnw{?~pc-mM R
2021-09-15 12:02:48 UTC	137	IN	Data Raw: 05 41 05 81 20 92 0a f4 00 5c ef 88 1f c0 df a4 3e 97 45 86 a0 16 00 73 d2 9c 23 37 32 cc 34 38 14 a4 a4 13 22 cf 3c 66 53 2b 46 ca 00 70 97 e9 73 ff 00 e0 c1 b5 cd 87 6c 0c a0 54 b6 bd e8 5b df 8e 96 86 d2 00 ee a8 8a e5 3e e8 44 41 9a bd 6c d5 0e f5 52 26 ec 88 91 20 91 01 e9 e6 62 08 5b f6 53 6b 75 03 11 09 33 04 c4 aa b9 42 81 22 c2 84 70 af a4 12 dc 43 1d 69 6f 1a 7b 11 83 1c f3 54 c9 2c 6b 0b 24 2f 17 30 48 c7 ef 6a bf 94 13 b6 af 61 f4 1e b8 35 9e f0 3c c5 e4 24 82 4b 1d da ef 6f 60 8e 71 10 22 a7 a7 59 63 a9 96 68 63 56 51 1a c2 39 b1 9d ef e6 63 e7 17 27 a8 1b 5b f1 c6 b9 53 7c a3 c3 dd b4 fd 98 95 33 db ea 0f e3 e1 5b eb 4b e9 04 46 18 92 23 cc 8a 4a 98 6a 11 16 33 a0 86 56 db 49 36 21 f6 b5 fa 5f 6e 98 d8 50 00 28 05 86 91 1a a7 02 a5 10 58 72 Data Ascii: A \>Es#7248"<fS+FpslT[>DAlR& b[Sku3B"pCio{T,k$/0Hja5<$Ko`q"YchcVQ9c'[S|3[KF#Jj3Vl6!_nP(Xr
2021-09-15 12:02:48 UTC	138	IN	Data Raw: 90 d4 b7 90 2c 1e 2b af 0a f1 1f fd 47 97 52 c9 cf 59 a3 75 e6 69 24 b3 00 c4 fa ec 0d c1 07 d0 11 81 f1 09 4a 41 09 a1 62 d4 e7 5b fb a4 5a 97 87 03 30 20 38 50 22 83 95 83 7e f8 c3 37 28 a5 73 28 e5 45 ac 69 04 0b f5 be dd af a7 7f 7e dd 70 b7 0c 92 b9 a3 31 d7 5b eb 6a 31 e2 47 a4 45 33 28 49 cc 4a 88 14 04 9a 78 5a fa f3 86 c6 49 97 cd 2c 11 b9 5d 32 07 02 d6 25 48 56 b1 b0 b5 ac 6d bd ed 7c 58 f0 d8 67 62 34 6b ed a9 db de f1 59 c7 62 11 2d 45 a8 0a 4b 9d a9 cf c1 81 de 19 74 f1 18 e3 52 12 c4 8d c8 5d af 6e de 9f 8e e3 e9 8b 0c b5 94 82 05 c8 22 d5 6f be bc 5f ab d4 27 4e ce a2 1f 95 6e 2a 3a df 9c 4a 50 d2 34 f7 71 1d 8d f7 6e c6 fe c3 db b7 fb e1 ae 15 33 19 25 d4 02 9b f9 a9 e1 fa 7b 81 89 c5 09 41 b5 16 1c c7 bd 78 02 20 c6 87 23 8b 43 30 94 16 Data Ascii: ,+GRYui$JAb[Z0 8P"~7(s(Ei~p1[j1GE3(lJxZl,]2%HVm|Xgb4kYb-EKtR]n"o_'Nn*:JP4qn3%{Ax #C0
2021-09-15 12:02:48 UTC	140	IN	Data Raw: 22 7a 18 85 2b 85 75 67 0e cc a9 b9 2a 2c 6c 4d ac 7b ef 6b f4 c6 62 35 13 98 d4 e9 af 08 99 44 65 8d 5a 31 a0 07 3c c0 8b a7 cd dd 80 1b da df 91 3f 96 3d 34 31 e4 cc 09 3d ea bd 9e a3 dd 62 62 9a e1 6c 4e a0 ff 00 72 d6 26 c7 b9 b5 fd 7f 03 eb 8c fb e7 ed bd b4 40 b5 77 8b 13 57 f5 fe 3f 88 e6 9f 65 58 55 49 be 92 6e 4d c5 cf 71 bd 85 87 a6 36 93 f4 9f 7a 98 93 cf de ad bc 4a 50 45 c8 9f e6 23 91 79 85 8d f5 fd a2 93 60 6e 41 fe d6 c4 ee 4d 1e 36 04 8a 0a 37 4e 0d ef 99 86 46 51 9a 54 dd 22 24 72 c0 94 99 74 f4 1d 7a 5e d6 bf bd 80 d8 58 e1 6c e4 05 2e 9a 1b 8d 3a 6b 5a fa d2 23 52 4e 52 52 e9 d2 96 7b db cb 7d cb 59 8b 90 d7 b4 11 4a 0d 6e 91 36 d4 f2 f9 4e a7 3d 54 de e1 75 0b 83 7b 11 7f ae 34 f9 63 57 24 72 f7 b7 07 e8 62 19 8f 93 bd 53 43 51 a9 a1 Data Ascii: "z+ug*,lM{kb5DeZ1<?=41=bblNr&@wW?eXUInMq6zJPE#y`nAM67NFQT"$rtz^Xl.:kZ#RNRR{}YJn6N=Tu{4cW $rbSCQ
2021-09-15 12:02:48 UTC	141	IN	Data Raw: 53 9c 7d 46 82 ba 1b e8 2d 0d 13 30 22 81 dd b5 1c 79 c7 2a 5a 0a 94 32 49 2b 2d 73 2b 12 eb 21 d2 42 81 a9 79 68 bd d7 62 bd 41 6b 13 ed 97 a0 70 1d b4 71 f7 d3 f9 8d d5 34 b1 b8 61 a0 b5 88 d7 dd 5f 48 e5 53 41 58 f1 d3 be 52 f2 49 05 44 8b 31 8e 72 56 75 03 cd 32 05 40 4a a0 b1 08 87 ee f6 db 1e 88 04 c4 7f b1 04 d0 54 8f d8 b5 77 af 36 94 a6 c9 67 9e 44 6e 58 92 a0 3a b7 29 96 ef 1b 29 b8 e6 35 ca da c3 b8 e9 6d b1 ef 77 8d 8c c4 17 05 40 71 70 f6 7e 94 bf dc 56 0a ff 00 97 54 29 48 1a 54 04 fd ad 4c 92 72 92 18 81 dc 22 b9 61 e6 16 fb a0 5e c3 d4 e3 cc ad 3d 09 fb f0 30 22 e7 32 d4 94 1a 02 c3 a8 e5 5d 75 81 ec c7 30 8b 2c 9f 5c 6f 4e 04 f1 c9 1c 53 42 c2 39 de 45 e8 65 d1 67 d3 aa f6 f3 79 97 71 da db 04 ab 56 f3 1a d9 9d fd ef 1a 4c 98 57 29 8d dc Data Ascii: S}F-0"y*Z2I+-s+!ByhbAkpq4a_HSAXRID1rVu2@JTw6gDnX:))5mw@qp~VT)HTLr"a^=0"2]u0,\oNSB9EegyqV LW)
2021-09-15 12:02:48 UTC	142	IN	Data Raw: 42 fb bf 91 31 62 38 6d 35 06 31 e9 0c a5 55 4d ee 76 16 b0 fc 77 d8 5b a6 3d 84 35 dd de d4 d8 d3 63 77 f4 84 38 84 94 05 e7 51 29 df af df f3 4b 88 78 e4 34 2e 69 91 d9 c6 a0 2f 63 6b 93 6f c0 1e bd bd ed 73 8b 5e 01 21 49 04 39 e7 ee cd be 91 42 ed 5c 50 13 4a 5b 53 53 67 d9 ef c0 37 08 28 48 df 4a c5 61 e6 6b 8d b7 27 ad 8d ba 7e fa 61 e4 99 4b 52 81 21 ae c0 69 b5 2a 5f 70 dc 61 22 a6 20 2b 3e 6f f5 6a 9a 35 76 7e 30 43 43 47 54 ba 09 24 29 17 0b 70 2e 0f ae d7 db ae ff 00 9f 6c 3a 93 29 45 93 f4 d0 5a 9c db 4b dd ac 69 b9 84 b8 a9 d2 96 a5 90 49 a9 0f 7a 70 2d 52 7d bc 16 d2 c2 74 1d 20 07 f2 8d 56 e8 7b 7e 47 fd 7d 70 ea 40 21 00 10 ec 54 4f 1b 69 e9 e1 a5 10 62 54 12 a7 0c cc 69 ef c7 83 70 89 31 48 79 7c c9 3c ff 00 41 bb 6d b1 23 d0 10 2f e8 3d Data Ascii: B1b8m51UMvw[=5cw8Q)Kx4.i/ckos^!I9B\PJ[SSg7(HJak'~aKR!i*_pa" +>oj5v~0CCGT$)p.I:)EZKiIzp-R}t V{~G}p@!TOibTip1Hy|<Am#/=
2021-09-15 12:02:48 UTC	144	IN	Data Raw: fe bf a8 fa 63 01 7f f2 f1 a7 bf 75 8d 14 0a 88 35 0c 35 a0 3d 0e cf be b1 9b 45 48 f4 af 23 ea d6 06 ca 2f f7 54 ee 74 8e df 8e ff 00 87 4d d2 a0 68 1f 7a fb f7 ac 6a 41 77 3f cb d5 f8 da f1 d1 22 aa 49 ac b1 0a cc 4a b8 1a 8e a3 fd 27 71 61 db d3 d3 12 49 fa 7d ee 62 40 b5 0a b0 f3 d9 f5 e1 e3 a4 74 ad 51 46 bc 6f 23 04 3a 8d 94 0e bb 5b cc c0 5e c3 d7 fb 60 84 a4 9e 02 25 49 2a 4b bd ee 1f 8b bb 6c f5 a7 18 96 a7 e2 83 1a a5 3d e4 2f 23 0d 2c 50 08 82 5e ee 24 d2 c4 82 c3 6d af 8d 7f b5 0e ec a7 e4 fb 7b 1e 75 8f 53 f2 ff 00 66 fb f8 c1 ed 1e 75 0b 2c 71 ce 8a f1 a1 42 91 80 e1 14 bd 86 a0 41 17 0b 70 c3 7e c0 63 43 21 05 46 95 7d 0b 7f 11 1a a5 95 50 9a 1a 8a 80 6f d6 db ec 34 02 86 79 7e 77 04 00 a4 f1 09 26 16 92 2a 80 65 64 e5 ff 00 eb 6d 7e 63 a7 Data Ascii: cu55=EH#/TtMhzjAw?"lJ'qaI}b@tQFo#:[^`%l*Kl=/#,P^$m{uSfu,qBAp~cC!F}Po4y~w&*edm~c

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	145	IN	Data Raw: 2a 71 41 49 4a c1 0a be 8c 06 a5 89 36 3a ef 04 59 65 3c 15 ce 93 24 93 bc f5 60 9d 52 48 ca 60 b1 3d 4f de 56 27 a0 db 63 f5 c0 b3 08 14 20 01 4a b7 e0 6f 0d d0 b0 a4 85 38 07 9d ed 66 d2 9c 20 c6 84 1a 18 96 76 a7 6a a9 a2 25 2b 63 b6 b1 cb 3d 1b 59 25 81 22 c2 fd 40 e9 db 10 28 26 e0 f4 6d 78 6d f9 f2 dd 4b 05 24 66 d0 d3 9e 9b 9a ef 6d cd ce 65 3e 65 47 49 34 d1 be b8 e8 aa 15 f9 70 c6 a9 1c f4 e6 4e a2 39 ed ac fd 4d ad d3 a6 30 94 a9 4d 42 2f e5 b6 86 00 98 bc a0 d7 5e 81 b8 fe ef b3 56 3d b8 eb 2f cb c2 53 d2 2b ad 4c cc 12 59 64 dd 9d 4e df 7b a8 b5 94 92 09 f5 ee 30 4f f6 fc 0e 9a 7e 0d e9 58 19 53 ca 03 e6 3b d3 57 fc fe e2 33 35 e2 2a 7a f1 f2 b9 82 09 68 19 4b 04 8b e6 23 9a 29 97 ee cd ce 8d 87 31 6f d9 ac a4 12 3a e2 61 87 64 05 39 e4 07 be Data Ascii: *qAIJ6:Ye<$`RH`=OV'c Jo8f vj%+c=Y%"@(&mxmK$fme>eGI4pN9M0MB/^V=/S+LYdN{0O~XS;W35*zhK#)1o:ad9
2021-09-15 12:02:48 UTC	146	IN	Data Raw: ae a6 36 86 76 bc 8c ba 8b 10 74 db 7e 83 6d 87 bf e9 6c 0f 88 fa cf 79 cd bd 8a 52 96 f4 2e d2 4f 1f 2d 2b 5a 6a a2 aa b1 67 1e c9 f4 d2 2d 8f 05 d1 4d a4 31 b3 a3 69 f3 a8 ee 40 3a ac 06 d6 e8 6c 7b e0 9c 02 16 b9 89 19 69 99 9e d7 15 a6 b6 dd d8 ec ef 57 ed 49 87 26 7c ec 54 e3 2f a9 e9 cb 5d c4 59 ce 1b cb 22 9a 28 f5 a7 fe 35 04 0b 91 a8 9e d6 1d 77 e9 6f 4e 98 e8 1d 9b 25 21 2c 51 56 0d 66 73 5a 58 97 eb 78 e4 7d b9 8a cb 34 d4 9b d8 b3 6f 6d fc dc c3 0a 9f 87 60 36 70 a5 5c 6e 14 6e 15 87 73 7f c8 1e bf 86 2d 38 4c 26 72 09 a0 7d bc f4 e1 47 8a 84 ce d4 58 61 61 ab 9e 16 17 af d8 3d 23 bd a8 9a 29 95 49 d4 05 d4 58 f6 b5 8e c0 6f b7 f6 c3 41 21 28 37 0e 06 a2 da 71 fb 72 d2 34 18 9c e9 cc 2c 77 a5 74 d3 4e 7d 62 42 18 88 25 42 8d 80 eb b1 b7 a9 16 Data Ascii: 6vt~mlyR.O-+Zjg-M1i@:l{iWI&|T/]Y"(5woN%!,QVfsZXx}4om`6p\nns-8L&r}GXaa=#)IXoA!(7qr4,wtN}bB%B
2021-09-15 12:02:48 UTC	146	IN	Data Raw: ad 02 cd 5e 6b d4 1b f3 ae fb 47 4e 61 52 68 a9 da 49 64 d2 96 62 58 13 e5 b0 dc df a9 eb ef 7b 93 6b db 05 4c ee c8 51 ff 00 d4 9f 33 f6 68 df 0d 20 62 66 09 52 d1 fe 45 be 54 ff 00 ca ac c5 83 50 d6 35 59 c4 de 24 53 f8 bb f1 48 fc 19 46 66 aa c8 7c 36 a7 81 ab ca 17 48 93 36 ae 0d a5 8a f5 6e 5c 4b 75 26 e3 7b fd 78 5f f5 07 b6 a6 4e ed 1c 27 67 e6 ca 8c c1 6a 2f 70 83 40 d4 67 73 b8 e7 1f 51 7c 3b d8 8a f8 7f e0 79 dd a1 30 a5 38 9c 64 bc a1 20 31 46 64 d4 95 97 05 c0 02 c0 1b 0a 54 ec d3 82 29 61 8a 08 40 f3 22 a2 2d ed b3 05 02 f7 00 5f b5 ff 00 5f 6c 34 f8 76 4a 02 93 30 58 01 d0 91 7a 71 d7 4a 47 cd ff 00 11 cf 5c d9 ab 98 e6 a5 48 26 ee ea 23 31 62 36 bf ea 1c b4 44 95 21 d1 56 c0 11 6d ee 2d b6 ff 00 4b 7e 78 eb fd 92 ac aa 4a 32 66 cc 01 cc e0 Data Ascii: ^kGNaRhIdbX{kLQ3h bfRETP5Y$SHFf|6H6n\Ku&{x_N'gj/p@gsQ|;y08d 1FdT)a@"-__l4vJ0XzqJG\H&#1b6 D!Vm-K~xJ2f
2021-09-15 12:02:48 UTC	148	IN	Data Raw: 11 aa 6a 40 0a 0a b9 76 a5 38 8b 07 a5 5f a4 4d 4b 9a 49 03 c3 aa 47 8e 05 4f 2a 03 ad f5 11 ff 00 90 91 e8 0e c0 ed 6d db 19 20 13 61 c5 f9 37 e6 e3 94 09 35 61 63 33 f3 e4 2b 4e 24 69 04 d9 2f 10 c6 8f 0d 04 68 ff 00 36 ce ba e3 8a 28 e4 ab 63 21 f2 39 dd 87 29 89 dc ed a4 6f 8d 56 11 91 44 ac 20 a6 d4 a9 0d 42 e7 6b 78 eb 40 07 cc 00 2e 85 56 da b7 0d 5b 7a 70 b4 5f af 02 e8 64 ca 23 87 35 ac 80 25 6c c8 aa 92 3b a2 7c b6 92 6c cb bd ae 07 e0 0f b6 15 1c 40 49 a1 cd 50 1e de 1f bf d4 55 fb 40 2a 62 94 7f f2 a0 35 fb f9 f1 de 2d 92 f1 b4 14 f6 84 d5 dd d7 49 2f 34 da 96 5b 9d f9 63 a6 a1 fd 40 0b fe 18 82 7c f2 aa 58 9a 6a 79 68 38 55 fc 0b 42 11 83 52 94 49 a3 ea d6 f6 39 18 fe ad e2 39 aa 69 9a 62 24 e5 b6 da f5 c6 b1 e9 bf 45 e8 7f 0b 5e e7 af 6c 60 Data Ascii: j@v8_MKIGO*m a75ac3+N$i/h6(c!9)oVD Bkx@.V[zp_d#5%l;\|l@IPU@*b5-I/4[c@\|Xjyh8UBRI99ib$E^!`
2021-09-15 12:02:48 UTC	149	IN	Data Raw: 9c a8 22 9d 0a b1 12 b2 dc b6 a3 dc 8f ed d7 7b 62 21 25 37 21 9e b6 27 d3 f6 7c 22 74 4f 04 16 2c c7 fd 89 7b 0e 9d 62 2e 93 34 fb 46 9d aa 1e 6e 76 ed 02 4a 9a 2f 7d 83 ad ae d7 1b 58 74 f5 c6 93 50 10 d9 43 b9 6d 76 eb af 86 b1 b1 9e 47 fb 7a fd 89 83 5c af 3e 96 22 1a 1a 63 14 40 81 24 92 96 6f 2f 4d 31 0e c0 5f 6b 90 07 b6 02 9e 54 52 52 cc 5f 47 a3 1b bf af e9 a3 45 cf 39 48 07 bc 59 aa 43 80 5f 5f dd e0 d6 2c e6 96 9b 95 53 57 59 13 c2 fa 96 38 9d cc 29 af 76 e5 49 22 90 4b 3f 50 08 bd ae 47 a6 23 93 2c ac 80 45 4b 0e 06 c0 9a 78 39 b3 52 01 c4 cf f9 68 24 a8 27 ba 5f 90 15 2d af f1 09 ef 12 7c 61 82 82 82 b1 63 af 8e 97 28 a3 82 5a 8c c2 aa 32 23 a3 cb 69 e0 52 65 54 2c 4b b5 44 aa 1a 34 62 ea a4 b6 ab 13 d1 ff 00 67 60 42 67 39 48 61 ab dd fd d4 Data Ascii: "{b!%7!'|"tO,{b.4FnvJ/}XtPCmvGz\>"c@$o/M1_kTRR_GE9HYC__,SWY8)vI"K?PG#,EKx9Rh$'_-|ac(Z2#i ReT,KD4bg`Bg9Ha
2021-09-15 12:02:48 UTC	150	IN	Data Raw: 03 bd 4f 2a da 91 89 3e 49 36 6e 8b 04 9b 44 df 7c 1b d9 95 ac 08 ed bd bd 6c 31 aa 92 b5 a7 e5 a4 12 55 b3 e9 d6 8e ed ad fa c4 92 bb 51 38 05 e7 40 ef 04 29 97 aa 57 46 ca 39 f9 8d d9 aa 2f 17 f8 09 97 f0 37 8b 0b e2 2f 0e 65 91 d3 c3 c4 10 43 4d c4 02 9e 25 4e 73 c3 75 8e a6 a1 c5 8b c8 35 d9 4e 92 40 bf 9a d8 e2 bf 1e 76 0c c5 76 96 1b 18 94 2d a5 f7 56 6b dd cd 7e 63 cb 53 1d 93 e1 8f 8f e6 76 c7 c3 33 bb 03 17 35 e7 21 46 62 26 2b 64 02 c2 b4 00 8a 35 ef ca 2c c7 07 85 d3 08 43 e4 b5 88 e9 b0 36 37 be fd ba df 7d f0 db b0 32 a1 29 40 76 20 24 d2 a0 b2 47 87 18 e6 5d be 92 84 cc 1a b9 2e fa 3b b8 22 9a fb a4 3a 29 95 4c 43 71 b0 5b 7a da c2 e0 76 eb b6 ff 00 df 1d 8b 02 84 c9 4c 99 82 d9 45 4f df c2 f6 de 39 cc f2 4a f6 77 e4 f4 eb 6f 58 87 af 72 55 Data Ascii: O*>I6nD|l1UQ8@)WF9/7/eCM%Nsu5N@vv-Vk~cSv35!Fb&+d5,C67}2)@v $G].;":)LCq[zvLEO9JwoXrU
2021-09-15 12:02:48 UTC	151	IN	Data Raw: 5d 1f dd 30 6a ea a6 a7 52 2b 05 9e f7 1a 58 86 d2 c7 66 20 69 f2 91 d1 48 d8 7d 46 09 ca 90 73 31 20 a4 1d fd 38 5e 00 5c d2 81 97 30 a1 df 4d f4 3d 76 82 7e 11 cd 72 9a 5a c1 54 4c b2 48 db 4d 56 65 4e 6a 2d f6 45 eb e5 07 aa df 55 ba 61 2e 3d 2b 53 00 0f 79 d8 54 50 5c 6d af 9e d1 08 9a 1c 00 b0 4a b4 bf 3a b3 0b 36 ba 98 b3 f9 47 8d 99 1e 4f 4d 1c 75 55 49 ff 00 6d f7 a1 69 af ad 40 be ad 5a ad 61 b5 c6 9b ee 3b e0 19 78 19 ae 49 49 f1 7a 6a 74 d7 8f ec 79 d2 42 99 d4 86 2a d4 81 d3 af 91 8e bc b7 c6 ef fa 83 38 13 41 59 a6 8a 9a 6b 44 a6 4b 58 35 8f 98 83 66 55 be c0 5b ca 06 36 9f 84 52 2a 41 70 c6 95 b5 bd 36 e3 5b 8c 1c 22 00 19 40 76 24 b1 e9 eb 4a 5e b1 65 b2 6f 11 7e 72 87 e4 fe 66 92 a2 9c 05 99 8c 72 13 27 31 80 27 7d 44 58 74 b6 c2 e2 d8 14 Data Ascii:]0jR+Xf iH}Fs1 8^\0M=v~rZTLHMVeNj-EUa.=+SyTP\mJ:6GOMuUImi@Za;xIIzjtyB*8AYkDKX5fU[6R*Ap6["@v$J^eo~rfr'1'}DXt
2021-09-15 12:02:48 UTC	153	IN	Data Raw: 55 4a 82 8c 42 6d 6e ad 7d fa 9d fe 9d 31 ef 98 3f e2 58 f0 35 df 48 d4 95 ff 00 a9 61 ea 75 36 3c 3a d6 30 8d 34 f4 1e 78 f9 72 44 1a dc c8 d4 09 b5 5f cf bd f6 0a 4e c4 6f d2 c3 19 cc 95 54 82 06 84 b8 1d 7f 74 8c 09 8a 48 51 52 81 60 d4 d3 c3 5d 1f 7f 08 cf 87 3d 14 71 02 f5 53 4a cd 21 b4 2e e2 45 b7 a0 d5 a0 82 76 d3 b3 1b f7 c6 8a 42 66 29 92 97 be e4 7e 69 6f c5 61 6c ec 68 41 2e b1 ad ac 7f 15 6f 3a 42 fb 8a 3c 45 58 da 4a 54 10 c6 aa c6 56 f9 b9 15 52 09 10 15 35 12 59 b4 aa 44 9a 89 63 60 48 0b d7 0c 30 58 10 55 98 a5 ad d7 f5 c4 d3 58 ac f6 af 6b a9 29 50 0b 15 04 38 34 26 ba 71 7b 5e f6 8d 62 7c 47 f8 e3 27 17 49 51 c1 9c 37 9a 73 38 6a 86 a2 37 cf ab 69 49 4f e7 39 8d 31 2e b9 7a 91 61 25 0c 13 1d 72 4a a5 96 42 a2 2b 1f 30 c3 d9 32 52 95 83 Data Ascii: UJBmn}1?X5Hau6<:04xrD_NoTtHQR`]=qSJ!.EvBf)~ioalhA.o:B<EXJTVR5YDc`H0XUXk)P84&q{^b|G'IQ7s8 j7iIO91.za%rJB+02R
2021-09-15 12:02:48 UTC	154	IN	Data Raw: b1 7a d5 bc 78 6e 6a 8c c1 46 9f 6d 87 7d 89 eb fb f6 c7 41 97 98 22 52 6c 02 43 9d 8d 3a 50 96 8a f6 50 a5 92 74 e3 e5 e5 ed e2 3a ac dd 59 c6 e4 f5 1f bf 7b 7a f5 f6 be 37 20 8d 3d fb 10 74 a0 d4 d8 7a b1 fd 7f 31 03 59 19 f9 72 75 0b 6e 49 f4 db ad ef d3 a7 e1 be 30 a6 20 82 a0 1a 8d ae f6 86 58 65 3c c6 62 93 60 fa 87 05 c7 50 3c e1 6b 98 4a f5 3c 41 4b 00 1e 58 90 97 ea 4b a9 03 65 b6 d7 ee 47 b8 b6 2a 7d b3 38 93 f2 99 c3 03 ce fa d7 4f 1d b6 b7 e1 d2 65 60 15 30 d1 d4 a6 35 02 d5 07 8d 40 71 6f 08 71 e5 08 90 53 44 03 1d c5 c5 ec 57 a0 16 1f 80 ff 00 6c 69 d9 d2 be 5c 97 be 70 1a b6 e5 ad fc 63 9f 76 82 8a e7 4c 51 17 ab f8 ec 1a 9a 0f 38 cd ab 87 52 6a 40 cd aa ee 4f 41 7f 41 eb ed d7 6b 76 be 0d 54 a2 53 98 53 bc 2f 6a 17 3c a2 0c 3c c2 9d a8 c0 Data Ascii: zxnjFm}A"RlC:PPt:Y{z7 =tz1YrunI0 Xe<b`P<kJ<AKXKeG*}8Oe`05@qoqSDWli\pcvLQ8Rj@OAAkvTSS/j<<

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	155	IN	Data Raw: 7f 67 05 e7 48 94 5c 02 12 58 30 3a 3d ff 00 90 78 35 8f 09 8d 0a 12 f3 cc ce 97 04 87 0a ab 7a e9 cf 76 8b 25 c1 df 16 3c 05 96 f3 23 cc f8 87 2f 89 82 f3 08 69 11 34 80 d7 d0 0a 31 21 80 eb db 0a d5 d8 18 99 9f 4a 03 36 83 7d 7d 98 69 f3 b0 6b 0c d5 d8 5e f5 1a d1 bc 77 8e be 21 f8 e8 e0 1a 79 8c 39 6d 4d 4e 64 cb 29 32 18 23 9a 58 23 5d 24 2e 99 8e 84 72 76 d9 19 b6 de f7 be 27 93 f0 b0 58 24 17 b3 ee fa f9 c4 c9 c5 e0 52 96 ca 41 e7 95 f8 9f 7c eb 15 c4 d5 bd c8 b9 f4 b7 ec ff 00 ce 3a d8 42 09 6d df 40 3c dc c7 31 f9 aa e3 e2 63 1d a7 6e ac 49 f4 df f7 fe 31 bb 21 14 6f bb 3d 79 7d da 31 f3 16 f4 27 95 ed 1d 1a 99 89 20 ec 3b 1f f8 db e9 f9 1c 45 31 21 47 b9 5f 1f bc 49 9f 3f 4f 7e 71 c8 00 37 ee 7a f5 fc 70 3a d0 be 9b 7f 1f 78 f4 64 26 c1 6f db 7f Data Ascii: gH\X0:=x5zv%<#/i41!J6}}ik^w!y9mMNd)2#X#]$.rv'X$RA|:Bm@<1cnI1!o=y}1' ;E1!G_I?O~q7zp:xd&o
2021-09-15 12:02:48 UTC	156	IN	Data Raw: 1c 66 28 91 79 71 46 6d 65 40 4d 95 48 fb c2 fe 60 cc 4b 92 77 3d 06 25 40 ce 7b 94 ea 7d 58 1b 7f 30 aa 62 c0 fa de 87 52 78 eb ec 5c 44 1a c4 4c e8 1d 7e c1 45 c0 1b b5 fa 5b d4 ed 7b 7e 36 c3 24 4b ca c7 5a 1a 56 ba bf 53 6f 11 58 4b 38 82 be 0e f7 a8 fa 9b 8f 5e 11 94 d5 11 c1 20 66 55 d5 7d 31 8b 5c 91 7b 5b 48 db cb 71 aa db 8e 9d b0 42 4d 7a 6d ad f6 db 9e fa b4 62 5b 0c c5 a8 c7 7d 36 1b de 8c 2d e2 27 98 4a ef 5f 3a 18 c6 a6 1b 7f f1 b8 f5 17 bd c7 5f a8 e9 82 f0 e5 39 d8 8a 92 00 e5 72 de fe f0 04 fc d3 14 e0 d0 3b fe da c7 9f 85 29 0b 33 2c 72 68 ff 00 f0 69 76 4e 97 32 0e 9e 52 6f d7 d4 5a de e3 06 89 64 a9 49 35 4c c0 10 1f 9f e9 9f c1 a0 25 e4 09 20 39 52 94 82 1b 82 81 3c 74 3c 8e 91 e8 1b f8 14 70 f5 3c 34 de 2d 78 8b 31 b5 47 10 71 a6 4f Data Ascii: f(yqFme@MH`Kw=%@{}X0bRx\DL~E[{~6$KZVSoXK8^ fU}1\{[HqBMzmb[}6-'J_:_9r;)3,rhivN2RoZdI5L% 9 R<t<p<4-x1GqO
2021-09-15 12:02:48 UTC	158	IN	Data Raw: 2e b8 be 9d 3c d3 24 7a ec ad 21 20 81 60 96 fc 6d 72 05 c0 db 62 4e 24 c6 21 21 09 c9 fe cc c5 c5 6c c6 9c 4c 5c 3b 06 72 86 59 44 b1 2a 09 63 67 24 31 35 af e1 f8 08 f0 af fc 5d 7f 87 17 c6 df 8b bf c4 0f c5 1f 16 7e 1e fe 17 f8 e3 c5 1f 0e b8 bf 84 78 22 59 78 9b 87 ab f8 62 8e 92 4c fb 2e 8f 33 83 30 86 38 33 9c ef 2f a9 9e 51 4c f4 85 9a 38 79 7f 74 2b b3 eb 08 cf 0b da 18 29 38 41 25 73 65 22 78 59 0c b0 b6 a8 4f 7f 32 50 bd 52 d6 7a 02 29 1d 5b 03 8b c0 4b c2 26 4e 3f b5 64 e0 d4 9c eb 62 89 8b 72 a4 4b 4e 5f f1 a1 40 28 a9 24 bb d4 02 ec c9 cf a3 1f 10 3c 2d f1 5f c0 ce 28 3c 23 e3 9f 85 dc 79 e0 ef 12 0a 93 41 05 1f 1e 70 cd 6e 51 45 98 d6 18 16 63 06 4f c4 a8 27 e1 bc de 4d 24 ff 00 db e5 d9 ad 44 f7 8e 45 78 94 c6 e1 66 21 13 52 66 a0 a5 60 10 Data Ascii: .<$z! `mrbN$!!lL\;rYD*cg$15]~x"YxbL.3083/QL8yt+)8A%se"xYO2PRz)[K&N?dbrKN_@($<-_(<#yApnQE cO'M$DExf!Rf`
2021-09-15 12:02:48 UTC	159	IN	Data Raw: f3 3c 4e f1 20 e5 ff 00 4d 97 60 7a 8e 98 2e 4e 02 76 2d 39 f0 c4 84 6a c4 b9 27 7d 3d 7a 46 e9 38 2c 3a ca 71 13 0b b5 33 35 2a 29 73 e9 d7 71 b0 fe 73 72 7b 92 37 3f be d8 b0 a1 0a 70 58 81 5a 9e 46 39 ca 66 ad 40 9d 39 e9 cf 8b b7 f1 1d b6 56 17 24 5b b6 c6 f7 ff 00 17 fd ed 8f 2d 0c e6 c6 e4 7e 20 a9 4a 1e 37 e2 0d 0f 87 3b c7 c5 5d 37 de f7 f6 c4 51 92 bc a6 97 f6 d1 d8 b6 27 71 7c 79 da be ed ec c4 88 56 b7 06 a7 7a 39 f1 8c a2 84 81 a5 6f 7e bd 7a 11 fa e2 09 cc a4 d3 50 2d ad 58 e9 c0 9e b1 ba 8a 58 10 6b a6 9a 9a 71 14 f7 58 ee 55 70 06 d6 d8 77 1f eb 81 d4 82 12 05 6a 3d d7 57 d7 7a c1 49 c4 29 32 d9 8b d1 88 db cf 95 36 8c a8 1d d1 94 8b dc 5c ff 00 8f 6f f3 81 94 8d c7 5f 7d 69 0d 30 b8 a7 07 30 60 d4 60 6f e1 cf d9 78 9a 5a 92 14 05 2a 49 16 Data Ascii: <N M`z.Nv-9j'}=zF8,:q35*)sqsr{7?pXZF9f@9V$[-~ J7;]7Q'q|yVz9o~zP-XXkqXUpwj=WzI)26\o_}i00``oxZ*I
2021-09-15 12:02:48 UTC	160	IN	Data Raw: be a7 9d 74 a6 b1 13 39 31 44 ae 0f 2a e1 5f 53 6c 11 01 be fb 5c 6a 02 c3 be fb 6d be 1a 27 e9 1c bc 9a 15 4d aa c5 2e 41 7e 35 d2 e3 d3 78 8c 86 a0 54 3c f5 ad e5 8b cc 94 d1 10 76 23 67 7d 81 ff 00 ca 00 ea 7a 62 4b b6 f4 b1 ae fa bb 6b d4 f0 0f 1d 89 a1 62 35 04 87 e4 29 eb ce 07 ea 24 8c 09 ab a5 90 46 c4 91 18 37 f3 d8 f4 16 07 f0 bd ba fa 60 c9 52 8e 64 1f 36 f1 e5 6a d6 03 2e e7 99 e5 af ed a2 01 a4 33 eb a9 b6 a5 d4 02 a8 1d 6c 36 ed 7e bd 0f 4b f5 b7 5c 1e ba a0 a4 5c e5 03 7f a8 3b 79 bd af 00 cd 24 19 8a 03 e9 04 93 b6 8f a8 17 fe 75 f4 f3 fc 18 72 ba 3c 9b e1 ba 8f 38 9a 97 44 f9 f7 1e f1 2e 66 d2 58 59 b9 55 86 8f 9a c0 7d ed 2b 49 16 90 7a 0d 86 f7 c7 18 fe a7 28 4d ed 49 52 af f2 30 e9 07 ff 00 e1 02 cf bd f4 6a 6d 1f 4b ff 00 47 e4 a6 47 Data Ascii: t91D*_Sl\jm'M.A~5xT<v#g}zbKkb5)$F7`Rd6j.3l6~K\\;y$ur<8D.fXYU}+Iz(MIR0jmKGG
2021-09-15 12:02:48 UTC	162	IN	Data Raw: 69 da 39 19 55 03 69 60 14 df 59 70 0a 34 8c 0e c1 d5 d0 28 b5 81 c2 89 72 90 b9 fd e5 31 14 bd 9f f8 d3 4e 2f 12 f6 f9 ff 00 e4 a1 44 9c b7 35 a1 a8 ff 00 5a 6f eb 48 55 fc 47 fc 33 f8 37 f1 35 e1 d6 7b e1 9f 8e 7e 1d 64 1e 21 f0 76 7b 4d 35 2d 5d 3e 69 43 04 f9 95 12 b2 97 8e ab 29 ac 31 b5 4d 05 64 32 da 78 1a 8d e3 73 2a a1 23 ae 19 23 19 3f 0a 7f c4 0a 90 14 0e 71 71 94 b8 23 91 a8 6d 83 56 21 ec ee d5 5e 1b 11 2d 78 55 cc 94 b4 1d 54 a0 9c cf 52 0b 85 05 68 08 34 04 1a c7 80 2f e2 63 fc 34 b8 e7 f8 73 78 91 40 32 8c cb 34 e3 cf 86 6f 10 73 8a ba 4f 0e 78 f7 30 53 36 75 c2 79 b2 d9 e9 7c 3d e3 a9 10 18 e5 ab 58 83 c5 c3 fc 45 2a c1 f3 cb 04 59 6d 53 4b 98 bc 33 d6 bc c0 e3 a5 62 82 92 9c 81 80 2a 48 2c 42 89 21 6c 93 60 f9 48 4a 49 29 75 32 42 10 1b Data Ascii: i9Ui`Yp4(r1N/D5ZoHUG375{~d!v{M5-]>iC)1Md2xs*##?qq#mV!^-xUTRh4/c4sx@24osOx0S6uy|=XE*YmSK3 b*H,B!l`HJI)u2B
2021-09-15 12:02:48 UTC	163	IN	Data Raw: 7d bc 7c b4 27 af e9 4a 41 7b 07 61 e8 5a 33 e1 45 64 24 b5 b7 23 a1 ea 2d df d3 db f5 c0 d3 02 89 01 ae 40 d3 7a d3 ed 7a f4 89 51 3a 68 70 11 b8 ab fe 2b ed 8c 72 75 55 b6 93 70 7d ad 6b 62 09 80 a1 c1 4b 6b c4 d3 d2 36 13 67 0f f4 48 6d f3 3f 9d 7d d2 38 03 63 ef e8 7f 7d b1 12 6a d9 c5 8d aa 23 64 e2 16 1d f5 b8 1b eb cb ce 33 a0 72 5a cd 60 00 16 de c7 a0 db a6 ff 00 bd ba 60 83 21 2b 01 49 64 83 6a f8 c4 a9 9d 98 85 11 4d 1c ea 3d 3d 3a c6 43 10 01 65 17 f5 e9 f4 bf a5 bf 2c 45 33 08 b0 c1 4b 70 45 a8 e2 b6 2d ea 29 a4 10 71 49 a2 40 25 47 5f 0d 34 ab ef 5a 56 38 19 1e da 80 07 a1 d8 5f bf a0 3f be d8 15 52 52 97 ce 09 0d e6 dd 0c 30 97 35 45 20 20 80 45 f4 2d 53 ec b6 91 d0 6b 88 d8 bc 6a c3 7b 16 03 65 b9 27 7e d6 06 e7 f0 36 38 85 12 81 72 90 54 Data Ascii: }|'JA{aZ3Ed$#-@zzQ:hp+ruUp}kbKk6gHm?}8c}j#d3rZ``!+IdjM==:Ce,E3KpE-)qI@%G_4ZV8_?RR05E E-Skj{e'~68rT
2021-09-15 12:02:48 UTC	164	IN	Data Raw: 61 a7 c9 65 e8 49 38 ad 4d ed e4 e2 33 48 96 9c a4 d0 14 ff 00 a9 b3 9b ee ef e1 a8 27 4b ec 99 f8 74 26 76 28 96 41 2a 62 f5 04 58 8e 1e ed 09 4f 10 6b e4 0b 59 51 21 48 d3 97 20 82 38 89 00 01 e5 8c aa f5 1e 4b 0e 97 d8 9b df 11 61 53 32 5a 87 cc 25 6a 53 90 4e 9b d1 b5 b7 36 d8 42 dc 6c f4 ce 99 9e 53 21 28 ee a9 36 77 1a f2 7f cb c5 4e 94 2b 3c d9 8c fa 8a b4 a4 22 90 4c b2 54 9b 85 d2 3a 95 03 63 ee 77 c3 c9 72 c2 80 2d eb cf 9d 9b db 83 5e c4 2c 39 66 d4 7b 1c 6a e7 9c 43 d5 22 f9 9a ad 49 96 56 d7 64 ff 00 db 61 1a 1e b6 28 01 32 1b 6d 7f 71 83 91 2c d4 51 b6 d0 7d fc 3f 85 b3 16 03 66 ab f1 b5 0b 39 1e 9a 6b 03 35 82 a2 be 71 47 1b ab c5 a8 34 d2 03 e4 25 76 58 55 bb 90 a6 e4 9d 87 4e c3 0c 85 87 21 e9 f9 16 85 2a 39 89 3c f7 a0 2e da ed d6 a2 c2 Data Ascii: aeI8M3H'Kt&v(A*bXOkYQ!H 8KaS2Z%jSN6BlS!(6wN+<"LT:cwr-^,9f{jC"IVda(2mq,Q}?f9k5qG4%vXUN!*9<.
2021-09-15 12:02:48 UTC	165	IN	Data Raw: c6 10 e5 fc 9a c4 73 fe 37 82 fb 3d 27 e5 2c 3d 00 a7 3d 2b cc fb a3 4b d0 af 2d 39 bb d8 db fb 0e 84 0f 41 df bf e7 81 d3 44 66 b2 8d 01 f0 2d 57 b5 6f 0a f1 0a ef ad 2b ff 00 91 57 1d 9b 43 7e 3e 91 2c c0 14 52 7a ea 1b 7e 3f ad af d7 d7 01 4c cc 55 be d4 f7 71 ef 58 05 98 9a 5f df be 71 da f7 28 de b6 c4 88 70 43 d5 af 4f 7c b8 c6 53 45 a7 ff 00 b7 89 23 d4 c0 d5 7a 89 11 d4 6c 6c e3 da d6 b6 d6 f6 bf af 4e 98 9f 3a b2 b6 66 2c c5 80 17 16 21 bf 9e b0 df 05 fe 35 24 b5 09 0a bd eb c4 e8 29 fa 8e 9e 17 8d 51 65 56 f2 91 2b 5d 6f 6e f6 b5 bf 5f c0 7d 70 b5 12 c1 99 98 87 27 9d f4 d7 4f 62 3d db 33 04 d3 9d 9c 0a 0a 39 03 f3 6f 10 34 83 49 29 4c e2 45 5b 86 d0 7c c0 80 40 ff 00 e2 4e c1 ec 7c a7 a0 3d 46 e7 07 94 a8 c9 52 50 90 01 15 a5 df 89 ad 09 df 8c Data Ascii: s7=',==+K-9ADf-Wo+WC~>,Rz~?LUqX_q(pCO|SE#zllN:f,!5$)QeV+]on_}p'Ob=39o4I)LE[|@N|=FRP
2021-09-15 12:02:48 UTC	167	IN	Data Raw: 24 6a ed b8 f4 26 2c 1d a1 f1 4f c3 98 6c 34 85 76 a7 68 49 93 39 53 08 12 d4 b1 44 90 48 34 20 d8 72 b4 51 d4 fb c3 f1 fe d8 ee b1 f2 11 98 a1 dd 01 23 ff 00 2f f6 de 97 b8 a7 28 cb 4e 9b ec 37 b1 3b 5c fa 7b fe c6 33 4b e5 4b f5 fc c6 06 28 a4 b2 96 a2 49 6d cf ee e0 52 dc ef f1 db 48 04 1d b7 b9 eb 6e 96 f5 f5 38 d1 68 4c cf a8 78 53 d7 db c4 9f 3a 65 49 24 01 d3 d6 9e 91 c6 39 15 ae 2f 14 9e 80 9f b4 24 91 b4 60 03 aa c0 f4 fe c7 6c 45 f2 92 55 95 20 93 d6 25 f9 c0 8a a4 59 dc 5c f1 e3 e9 06 b9 0f 02 71 97 13 4c 90 70 f7 0c e6 d9 93 4a 74 a6 88 26 e5 12 dd 00 93 96 47 9a e0 91 7b 8d c0 38 36 4f 65 e2 71 8a f9 38 54 4c cc 9b a8 82 13 5a 8a df 84 0d 3f b4 30 b2 13 99 53 00 22 ee a1 4e 97 f1 6e 75 8b ad e1 37 f0 eb f1 bf c4 aa aa 11 9a c7 4f c1 f9 5d 4c Data Ascii: $j&,Ol4vhI9SDH4 rQ#/(N7;\{3KK(ImRHn8hLxS:eI$9/$`lEU %Y\qLpJt&G{86Oeq8TLZ?0S"Nnu7O]L

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	168	IN	Data Raw: 71 70 2f b7 a6 d8 3b 31 39 00 d0 87 e2 1d b9 54 57 ae 95 84 f8 85 65 5a 98 05 0e 5a 74 e0 01 fb c0 7f 10 d5 d3 c9 4f 3c 71 0d d5 af 0c 80 24 6c 16 d6 d2 2e 41 16 fa 62 66 26 c3 c9 e9 af be 90 0c f3 2c 27 30 01 db d3 cc 7e 4d 45 61 09 c4 fc 41 47 97 52 73 6b 6b 0c 40 5b 55 3c 0c 39 d3 8d ee a5 d3 cd bd 8d d4 ed 7d ec 2d 83 a4 c9 02 a5 df f5 4f be e1 b7 84 93 a7 9c a6 b5 b0 15 66 7b 93 ad 1a b5 61 0a 3e 0b e0 ef 12 7e 22 bc 56 e0 ef 05 3c 1a e1 b9 b8 83 8f 3c 48 cd c6 5b 92 64 39 72 4e ed 05 1c 4d ff 00 dc 73 fc de a2 38 e4 34 39 66 5b 43 ae 4a 9a 89 b4 53 bd 43 d3 53 33 a4 95 30 ea 38 27 2c 89 b3 25 87 52 41 62 ce 00 6a 28 d4 1c a1 54 25 ed b9 a4 27 5c c9 73 f3 aa 6a be 58 92 72 a9 e8 56 a1 60 87 b9 39 83 9b 00 e6 cd 1e bb 7e 17 bc 05 e0 af 81 5f 87 3e 2a Data Ascii: qp/;19TWeZZtO<q$l.Abf&,'0~MEaAGRskk@[U<9}-Of{a>~"V<<H[d9rNMs849f[CJSCS308',%RAbj(T%'\sjX rV`9~_>*
2021-09-15 12:02:48 UTC	169	IN	Data Raw: 87 e5 6f c5 9f 5e 2e c6 2c 37 0c f8 b9 52 95 31 6a 94 94 d2 4d f6 2e 16 e4 6f dc 9b 6c 77 3e 9e e0 79 a8 4a 0c c2 d5 04 eb 6d db 6d 0b 5b 48 5d 37 02 a2 2a 08 e9 a9 d8 9a 52 de cc 58 6c 9b c5 97 9c ab 3c d2 18 4a 85 4b 7a da e0 00 1b b9 ef d0 9e d8 4f 39 59 42 96 2f 66 34 01 ac 7f 3e 90 07 f6 14 c8 41 a1 7d 2d 7e 02 b7 e0 d0 da ca 3c 4a 86 9e 38 dd ea 99 83 b2 9d 1a 8e ad ef b1 b3 6c 37 ea 70 9d 73 16 49 2c d5 e3 a5 78 74 a0 88 97 80 0a 64 29 2c 09 a1 17 a7 4d 79 6f 72 d0 e9 e1 ce 30 a5 ce 0c 72 f3 00 d1 61 a4 7b 58 6f 7d 8e dd c1 17 eb df 11 ae 6a c0 e6 75 7f 1e 8c 61 27 68 60 13 21 25 29 04 b9 70 4f 57 d3 ad 38 c3 f3 87 73 68 0c 76 47 f3 58 1b f9 40 23 b5 8d fb 74 3d ef b6 fd 71 61 ec 49 c9 05 21 65 8e 60 47 3b fa fb 6a 47 39 ed 6c 1c c5 a8 b8 70 fe 6c Data Ascii: o^.,7R1jM.olw>yJmm[H]7*RXl<JKzO9YB/f4>A}-~<J8l7psI,xtd),Myor0ra{Xo}jua'h`!%)pOW8shvGX@#t=qaI!e`G;j G9lpl
2021-09-15 12:02:48 UTC	170	IN	Data Raw: 86 bc ab a7 0d 88 b2 ee 2a 76 a2 96 0f 98 56 ac 4d 5c a9 0c 8e 58 47 ec 09 bf dd db ae c6 c3 dc 0c 70 a9 25 ea fb d3 43 72 e0 df 41 12 ff 00 76 40 03 e6 13 94 16 ab 8b 6a fa ec dc 7a 0f 8f 10 73 5c 86 a4 4a ae d2 c7 f6 d6 86 66 67 0a a5 ee 48 43 a8 7d 07 43 eb 6c 4c 9c 1c c3 77 29 e4 19 fa 35 a0 59 9d a6 b4 b0 4b 97 50 25 aa af 01 a5 5a bb 08 38 e0 ff 00 1d 73 c3 27 ca 88 a4 a8 82 51 75 48 75 b4 c0 92 41 5d 4d 65 40 7a 6c 54 2f 4b e3 63 80 43 29 44 55 9d 8e 8d d0 68 29 5e 06 36 9b da cb c8 4a fe 6a 86 52 e9 4d 4a b5 6d df 9f 1e 71 73 3c 26 f0 53 8b be 20 25 6a ac cd 6a 72 ce 0c 83 44 b5 d5 b5 31 93 24 9a 48 0f 4d 4d 6d de f7 d2 64 42 40 5e f8 71 d8 dd 94 31 0b 0c 92 12 6a 0d 2a 0b e8 41 a7 1e 9a b4 73 df 8b fe 2f 1d 87 86 75 ac 7f 75 34 3e 1e 40 2a 72 2a Data Ascii: *vVM\XGp%CrAv@jzs\JfgHC}ClLw)5YKP%Z8s'QuHuA]Me@zlT/KcC)DUh)^6JjRMJmqs<&S %jjrD 1$HMMmdB@^q1j*As/uu4>@*r*
2021-09-15 12:02:48 UTC	172	IN	Data Raw: 0b dc af 3f 96 a5 cc 72 47 0c 74 c9 3c 89 0a cb 18 86 5d 2c c4 a1 75 b9 dc 82 0f b8 df 0d 13 28 4b 48 08 0e 37 6a f8 5f df 8c b2 bf c8 4a 89 1e 6f f8 77 a7 17 82 59 85 34 d4 ec 66 4e 64 ea 2e 8d 4d 7e 6c 65 81 2b a8 8e a2 dd 49 bd b7 ef d2 54 e6 61 de 0d a9 2f 4d f7 b7 38 de 68 53 97 4b b9 51 d8 5f 8b 7a 8b 5d ae 21 5b 51 2d 2c 6e f5 10 c3 2a 1b 8d 51 39 5b 2f 64 95 ae 34 c9 6e a4 1b b0 fa 9c 33 95 90 20 02 a4 e6 29 a9 1e eb ee b0 96 79 28 cc 0a 4e cd 4a 78 f1 af 58 01 cf aa e3 8e 96 49 24 5a 4a 44 85 44 b0 27 3b 9b 23 b3 91 b0 7d 4d 66 b7 f4 83 b6 3c c5 34 3c c7 2d 21 56 21 7f 31 23 29 6a b1 b1 b5 74 88 3c d6 bb 2e 82 23 5b 47 24 8b c9 82 24 91 5c af 32 79 a4 40 cc 22 bf 53 7f bb b8 b8 16 1b 5f 1e 8c 24 84 ca d0 9d 47 53 6f 56 af 5b 42 da a2 ba 5d e5 7b Data Ascii: ?rGt<],u(KH7j_JowY4fNd.M~le+ITa/M8hSKQ_z]![Q-,n*Q9[/d4n3)y(NJxXl$ZJDD';#}Mf<4<-!V!1#)jt<.#[G$$\2y @"S_$GSoV[B]{
2021-09-15 12:02:48 UTC	173	IN	Data Raw: 8d af df d7 70 37 3f ef 82 64 4a 42 6b 40 49 b6 da e9 7e 9e 2c ee 42 e7 83 6a 02 49 70 6a 6e da fd ad 58 0d ab 56 8b 9e 4c b7 06 4b 00 3d 4f 43 61 73 6b f5 3b dc 1c 38 94 91 91 3d e1 d6 ed d7 f8 8d 41 7a e9 a7 bf 2e 90 2d 36 65 35 31 2b 2b 5e cd b0 df 65 f7 3e fb 7b f6 c6 e5 09 ca 6a fe fa fb e1 12 a2 61 4d 6f 6f 6f e8 62 2a bf 38 49 50 58 80 40 de c4 ee 46 d6 b6 ff 00 8f 7e 98 10 86 51 2e e0 50 7a 9e 56 d4 b7 18 21 13 dc b0 06 da b3 6e 75 f6 36 8c 3a 2c fa 36 90 c2 54 02 b6 5b f4 06 e3 51 ed 6f f8 f4 be 22 62 54 1d 34 26 a6 da f8 fe 74 2f 19 f9 ee ac bc 6e 19 bf 30 73 43 9d c2 34 c4 cc 08 22 f7 df 6e 96 03 fe 36 ef db 11 aa 50 0a 24 80 41 1e 7c fd f2 89 11 38 d7 f2 de 7e f9 c1 3d 1f 10 9a 7a 88 cc 3a 91 03 02 00 b3 7a 5a e6 df a7 e5 85 b3 24 d5 db 57 f2 Data Ascii: p7?dJBk@!~,BjIpjnXVLK=OCask;8=Az.-6e51++^e>{jaMooob*8IPX@F~Q.PzV!nu6:,6T[Qo"bT4&t/n0sC4" n6P$A\|8~=z:zZ$W
2021-09-15 12:02:48 UTC	174	IN	Data Raw: 0f 7c 7a 8d 47 7d 5f ed 1b 7f 70 d6 04 71 7f c5 fc 44 30 f2 4c d9 a2 9a 22 d2 73 01 02 df 7b af b7 af fa 0c 08 b7 00 f3 f0 af 01 1b 22 7a 95 50 0d 2e 09 7d 48 eb a7 bb 3f f8 5f 36 81 9a 20 6c d0 38 0b 20 07 ee 48 a6 e4 fb 9f c0 7b f4 c0 6b 48 39 aa c7 66 e5 ed ec f0 ff 00 09 33 3c b6 76 dd eb d2 b0 f7 ca 5f 2f ad 2c ce 8c 39 1a 0c 4e 03 83 7b 01 6b a0 26 c7 7e c3 b8 c2 3c 41 29 53 57 60 74 7d 3a 03 e6 61 90 64 23 2b bb dd b8 8a f9 f4 f2 83 7a 3c a2 4a 80 94 4d 14 55 68 e4 c9 19 94 cd ad 43 11 b0 3b 0d 8f a8 1b 7a 5b 7f 4b 9e 50 cc e1 a9 e4 d4 d5 ac 7e ef 10 cc 96 85 86 6a eb f7 3c fe fa b5 e3 f3 df 09 68 33 28 27 99 e8 e6 d2 64 5b 15 99 b9 71 3d b7 62 03 91 6e bb 9b 00 01 e9 89 c6 2d 65 60 12 e1 87 5d 35 d7 c7 41 02 ab 09 2f 2d 43 bd 1d bc 0f a3 c2 b2 bf Data Ascii: |zG}_pqD0L"s{"zP.}H?_6 l8 H{kH9f3<v_/,9N{k&~<A)SW`t}:ad#+z<JMUhC;z[KP~j<h3('d[q=bn-e`]5A/-C
2021-09-15 12:02:48 UTC	176	IN	Data Raw: fa 71 61 e7 db 94 bd 55 45 1d 54 f2 e6 12 99 26 69 79 f4 ef 56 85 29 d2 9a 47 28 b6 01 b9 6a da 6d a5 48 07 70 6f d4 1c 9c 22 4a c0 4a 28 f5 a0 04 87 fc 6d be 8d 19 5c f6 4a 4b be 60 72 d7 35 43 69 c7 df 10 0e 2b e3 a9 69 d2 78 61 cc 4d 14 71 22 4f 3c 89 a2 48 22 94 25 91 62 62 a4 b9 b0 d2 ca 6e 05 fa 0d 86 1f 61 b0 28 20 0c a1 c0 da a4 8e 02 a1 ba 6f b4 27 c4 76 81 92 54 0a ab 66 35 bd cd 36 b7 1e 2f 55 ff 00 fd 47 96 3d 33 e6 75 b1 4b 59 3d 4a 03 4b 57 09 e5 17 a8 69 11 1a 3e 51 d0 09 0b 66 f2 ae c4 93 b5 f0 cd 38 70 94 e5 48 ff 00 5d 99 c9 d5 f4 07 6f 38 4d fd e7 cc 9a ee 00 cd 62 38 fb 1a 5b 4b 41 b5 04 b9 7b 4a b2 d4 69 12 33 23 14 96 a8 07 1a 00 d3 ad 4d ec 40 f2 d8 91 60 00 1d b1 12 f0 ea 27 e9 e7 50 e3 c0 bb 7d e0 f4 62 58 0e f7 1e 06 bc de dd 2d Data Ascii: qaUET&iyV)G(jmHpo"JJ(m\JK`r5Ci+ixaMq"O<H"%bbna(o'vTf56/UG=3uKY=JKWi>Qf8pH]o8Mb8[KA{Ji3# M@``P}bX-
2021-09-15 12:02:48 UTC	177	IN	Data Raw: 39 a5 96 77 2a 2f ab 44 51 b3 1e a4 80 40 bd c6 23 9d 35 12 30 b8 ac 42 c9 12 e5 61 e6 a9 44 07 20 29 05 29 20 5c d4 d7 68 cc 8c 39 c5 63 bb 3b 06 1b 3e 23 1f 85 09 04 d1 a5 cd 4c e9 8e cf 79 48 58 4b 86 2a 29 04 87 78 f7 21 c3 4d 0d 2d 7e 49 94 14 d0 94 90 d2 d2 e9 50 00 58 e8 a0 84 d8 01 d8 ba da c3 70 6c 4e 3e 55 ed 49 6b 9c 9c 6c e6 cc 85 cf 5a 90 a2 59 c1 37 67 a5 49 bf 18 fb 87 0a 9f 93 86 ec ec 19 19 12 30 c8 4d 9f bc 12 0b 7a d8 d5 b7 87 0f 8b 35 03 33 e1 47 91 2d ac a8 80 86 b0 e8 a0 02 0f 71 61 bf 5b 91 df 7c 57 be 1f 97 fd be 39 4b 50 62 54 c0 6f 50 de e8 fc 21 8a e5 ff 00 8d 42 84 04 a8 b8 20 b5 0d 6f ce 9e 51 48 32 fa a3 49 34 b1 b1 bb ac e0 02 36 b6 9d ad ec 2d 6e de a7 1d 83 0e 49 97 51 62 e6 c6 fc ad c4 3d f6 8a 52 c1 4a d6 a3 4c ce 01 26 Data Ascii: 9w*/DQ@#50BaD)) \h9c;>#LyHXK*)x!M-~IPXplN>UIklZY7gI0Mz53G-qa[|W9KPbToP!B oQH2I46-nIQb=RJL&
2021-09-15 12:02:48 UTC	178	IN	Data Raw: 36 5b 30 22 db 9b ed ed e9 8d a4 4e 12 a6 02 a2 c9 51 61 42 6a 43 5b 67 62 e0 75 87 78 70 53 3a 5c c0 58 80 08 63 a0 20 b1 6a 6e 1a a3 4d e3 f3 7b f8 de f0 d1 bc 1e f8 bc f8 86 f0 f1 9a 76 a3 c8 bc 45 cc ea 72 a8 e4 40 9a 32 5c f5 97 32 a3 78 57 48 2d 0b 4b 35 4a a9 60 45 d1 82 9d 36 c5 a2 42 d3 31 2a 06 f9 42 87 fe a4 07 3d 54 e3 7a 11 1d 63 03 3b 3e 06 44 e4 31 05 d0 49 fa 9d 2f 42 f5 a2 72 bf 13 78 ac 26 46 d1 bb 02 b6 1b 0e 87 d2 c4 9f c7 a6 23 01 ad 12 aa 70 56 ad c6 b4 ae 94 fb c7 62 cc 15 6c 1a dd cd ec 7f c8 b7 f8 c6 45 c6 cf 1e 4c f6 22 ba f1 1f af 4e 71 cd 2a d8 b0 dc 1b d8 5a db d8 7b 8f c7 eb 6c 4e c9 ff 00 8d 7a 7e 3e f0 47 cf 3b ff 00 fe d1 9d f3 40 a8 05 8d 85 87 dd d8 10 3a 5e de de b8 80 a3 39 22 cc 4f 2e 5b 5a 36 38 85 24 80 48 04 d0 51 Data Ascii: 6[0"NQaBjC[gbuxpS:\Xc jnM{vEr@2\2xWH-K5J`E6B1*B=Tzc;>D1I/Brx&F#pVblEL"Nq*Z{lNz~>G;@:^9"O. [Z68$HQ

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	178	IN	Data Raw: 3d 3b fe 9f bb 63 c9 c2 80 28 6b cc 6a 6d 6f c7 8c 6d f3 c8 b9 a8 bd 07 4b c7 f3 d5 79 af 7b 7f f8 db 83 df f7 ed fa e4 a4 a5 85 38 31 7b 46 e1 46 6a 42 85 46 8c de 62 fe fa c4 8d 3d 52 8d 24 2d 88 b7 61 de c7 a1 df e9 6f 6c 6b 1e 00 9a 0a c1 2d 06 67 2a 48 8c 47 95 45 fa 58 9e 9d 06 db ed fe 71 9c a9 50 20 9b d0 08 da 5b 07 07 57 6f 33 ef c2 1b fc 3d 9e 2a f2 79 6c 50 9e b6 3b ef 62 4d 89 1e a6 e4 ef b7 d3 00 4f 90 c4 81 51 5a da df 8d 3c f4 86 32 67 84 00 1c 86 d2 fb 0a 52 f5 da be 96 13 21 e2 3a 88 a3 8f 92 c5 86 8b b1 be e7 48 16 e8 47 53 d3 b5 ef 85 58 89 1f e3 2a 50 b3 bd 2a 36 3d 74 7f 03 0e 64 4e ce a6 51 27 63 5b ec cf ca f1 65 38 52 ba 5c ce a2 96 a1 1c a4 8f 4e b0 cb 72 74 aa 8b 1e e4 8f 37 42 00 bd b7 eb 84 eb 50 40 d8 6a 78 6f bb d5 e0 d0 92 Data Ascii: =;c(kjmomKy{81{FFjBFb=R$-aolk-g*HGEXqP [Wo3=*ylP;bMOQZ<2gR!:HGSX*P*6=tdNQ'c[e8R\Nrt7BP@jxo
2021-09-15 12:02:48 UTC	180	IN	Data Raw: d7 a4 91 a7 a7 4d 8c d2 fb 39 e6 12 52 c4 8a 90 3a 08 1f 19 8c 54 a4 b0 25 c0 76 34 e6 ff 00 6e 30 05 51 c6 f5 39 6e 58 50 c9 3d 35 37 24 c7 2c aa 10 4e f2 c8 4b 31 92 59 41 33 b1 d5 76 74 d9 8d 85 ba e0 d9 7d 9c 09 b5 43 11 4b 6b 7b 51 bf 70 11 ed b3 f2 d8 a9 2e 03 00 ec da 02 05 be db eb 0a d9 b8 9a 3c d1 c4 b3 d7 cd 5b 06 a3 14 11 b7 2a 9e 91 ea 2e 02 bb 21 0a ec cb b6 b6 7f 2b 00 6c 06 0f fe d7 e5 a1 d2 92 ef 50 06 8c ef bf db 68 55 33 1c a5 a8 ad 4a 24 1a 55 5e 77 b7 d9 a2 36 a7 3e a8 f9 ea 3a 79 2b a1 2f 45 cc 96 59 74 33 52 a4 cd ff 00 86 08 a3 b9 8b ca 57 54 8c 16 dd 0d fb 9d 44 b5 d1 c3 3e ba 0f e2 07 5e 2c a0 86 60 f5 bd 89 b5 5c 51 b4 b6 9c 23 31 78 8a a9 da 59 56 b2 0a 39 e4 37 97 34 ac 96 f2 29 60 16 48 e9 a9 87 95 d5 fa ab e8 24 5c ed b6 30 Data Ascii: M9R:T%v4n0Q9nXP=57$,NK1YA3vt}CKk{Qp.<[*.!+lPhU3J$U^w6>:y+/EYt3RWTD>^,`\Q#1xYV974)`H$\0
2021-09-15 12:02:48 UTC	181	IN	Data Raw: f6 c7 95 54 65 62 7b c0 d3 83 51 ba 46 a4 38 08 15 cc a7 7e 5a 0d 0f 3d 6a 22 cb 7c 16 70 95 4f 10 fc 58 f8 0d 1c b0 2c b9 5d 3f 1d 47 9a 55 8b 79 e3 a4 ca a8 66 96 57 2a 2f e5 59 e6 84 13 7b 86 60 7b 0c 03 f1 06 21 08 ec 6c 7a 00 20 ab 0c 13 56 67 24 12 e4 9a 38 76 f2 01 9a 1b 7c 37 d9 eb c4 fc 59 d8 a9 cc 04 a9 58 81 35 65 4e c4 04 2d 20 02 cc 4e 65 82 ce 06 5c c5 dc 57 d7 2e 59 98 24 9c 5b 46 df 31 68 d8 c9 18 b9 b3 d9 5b 76 20 da c5 b4 a8 27 b8 db 1f 3a e3 64 65 c1 84 94 d5 4a 24 d1 a8 49 ad 01 0c 69 5a 8a 57 8f d8 82 7a 4e 20 4b cf 49 48 42 50 a7 0c 4e 5f f5 36 3a b0 ac 3c 33 9c ce 93 32 cb 22 a2 7b 85 6d 37 62 2e 09 d2 0d fa ee c6 fd 3f 3b e2 af 2f 08 b4 ce 05 05 99 49 25 af 7d 46 dc b8 74 62 92 bc 84 12 40 ca 6b 57 ca 41 72 77 1b 45 50 e2 4c be 2a Data Ascii: Teb{QF8~Z=j"|pOX,]?GUyfW*/Y{`{!lz Vg$8v\|7YX5eN- Ne\W.Y$[F1h[v ':deJ$liZWzN KIHBPN_6:<32" {m7b.?;/I%}Ftb@kWArwEPL*
2021-09-15 12:02:48 UTC	182	IN	Data Raw: 00 1d fc 2e 7f 1d ce 07 8f 85 7f 88 06 61 9c 41 1e 88 f8 ff 00 c3 7e 19 ce e3 90 2d 96 7a 8c 92 69 72 ea ab b0 00 3b 7f df 25 c9 de fd 3a e2 c0 9c b2 b2 57 bd 32 4b 01 ab 4b 50 55 cd 49 79 c3 99 a4 74 de c6 9e a5 76 52 50 53 44 4e cc 6e 18 cc 43 0e 9f e2 d5 fc 63 4e 73 c0 db d9 40 b1 b0 b0 b5 fd 0f 41 d7 f3 df db 18 49 26 e1 a1 90 2e 1e 30 e4 a6 98 a1 b2 fb 7e 87 1b 02 1c 3b 5c 5e 32 63 1d 69 e7 93 ec d4 38 e8 18 f4 3e 9b 7f 63 6d c6 d7 c1 16 88 02 89 ff 00 6f 37 f1 f7 58 20 cb b2 09 a7 65 26 59 74 68 3b bc 9e 41 65 25 89 bf 40 96 b6 f7 1d 8e 08 97 2d 33 48 48 67 6d 2b 51 4a 6d f7 68 d0 4f 29 42 e6 1a 84 bf 06 cb c5 e9 6d 4f 18 46 f1 87 8e 7c 09 c0 dc 60 bc 1b 9a 56 4a 5c e9 69 f3 58 94 54 d3 52 17 27 4c 72 10 4a 23 5c 15 70 08 d3 e5 d4 56 f7 c3 79 7f 0f Data Ascii: .aA~-zir;%:W2KKPUIytvRPSDNnCcNs@AI&.0~;\^2ci8>cmo7X e&Yth;Ae%@-3HHgm+QJmhO)BmO F|`VJ\iXTR'LrJ#\pVy
2021-09-15 12:02:48 UTC	183	IN	Data Raw: 9e 75 68 dd 5d d5 c9 13 ea d4 2c 57 49 20 e9 f2 d8 95 b1 be 1a 76 8e 19 3d a7 85 5e 0e 70 79 5f 29 68 09 d1 94 92 97 f3 d9 f9 40 b2 c9 95 30 4d 4d 14 95 25 40 b6 a9 2f 71 bd e9 ce 3c d1 7f 19 ef 85 bc d7 c1 7f 89 4c af e2 9b c2 cc 9e a3 31 f8 6f f8 92 ac 5c c7 88 f3 7c 9e 36 92 9b c3 af 15 00 10 d5 c7 9f 2a 3a fc 95 0f 14 3e b8 52 a6 55 54 a7 ab 8e 1d 41 63 a8 32 45 f1 3f c5 df 09 63 fe 19 ed bc 52 a6 ca 50 ec ec 4a 92 30 c8 f9 64 a7 e6 66 29 ce 56 fd dc e0 a0 24 19 65 1f e3 3f e4 4a 8a 52 bf a1 fe 03 f8 92 4e 3f 08 70 f3 cf ff 00 25 0c 50 0b f7 d0 7e a4 b9 76 52 7e b4 bf d4 92 b0 f9 92 94 aa 87 f0 8e 6f 4d 4b ce 86 11 1a 94 8e 19 68 39 44 32 fc c4 b7 d4 c6 c1 ee 5c dc fd e6 06 e7 7b 6f 8a 7c ec 3d 40 48 a9 67 4d 98 d8 b7 2b 11 e1 1d 5f 0d 8a 74 9f 95 f5 Data Ascii: uh],WI v=^py_)h@0MM%@/q<L1o|6*:>RUTAc2E?cRPJ0df)V$e?JRN?p%P~vR~oMKh9D2\{o|=@HgM+_t
2021-09-15 12:02:48 UTC	185	IN	Data Raw: 7e ce 5d 41 f4 cd ab 75 58 57 92 ac 3b 05 25 da c6 d7 c1 b2 7e 8e a7 d6 90 a6 79 67 27 85 79 06 03 ce 90 36 ef 57 4f 4a 29 a9 a3 8a 3c d2 a5 cb 48 f3 5b 45 0d 2e e0 3c ac 0d 84 a4 79 a3 b9 dc ee 7a 11 83 70 ff 00 59 e9 eb e7 00 26 60 ef 1a b8 1c 39 be af 02 b5 6f 4a 91 3c 74 d2 35 4c 74 ee 7e 7a ae 43 f6 93 b9 3b ae b0 06 a4 46 2c 57 4d 85 8e f7 16 c3 43 f4 78 7a fe 07 bb c0 2a 58 5a cd 6b 73 57 d7 ab 71 fc c7 00 94 d2 24 65 0b cb 10 24 e9 db 4f 95 49 d4 4d b5 05 de db ed 7b e2 38 d1 af 7b d6 f4 e1 ce 94 d4 52 23 66 6a 89 82 12 ff 00 64 cc cb 18 4f b8 a8 3a ea d3 6b b0 5f ea 23 ea 31 e8 d6 62 9d 29 48 35 73 e3 72 dd 2d f8 8e 50 d0 89 52 48 a3 75 66 8d 49 12 b0 36 2d d4 83 bf 41 7e dd 31 85 2b 22 4a ce 9e fc 7d 7a 46 d2 e5 66 65 1d 3d 4d 69 b7 e7 71 1b 02 Data Ascii: ~]AuXW;%~yg'y6WOJ)<H[E.<yzpY&`9oJ<t5Lt~zC;F,WMCxz*XZksWqeOIM{8{R#fjdO:k_#1b)H5sr-PRHufI6-A~1+"J}zFfe=Miq
2021-09-15 12:02:48 UTC	186	IN	Data Raw: 1d e6 d1 55 d1 47 29 68 e3 76 5b 82 af 7d 5b ec 6d df 73 f4 ed 86 38 4c 46 55 dc 8b 73 bf 9f 3f 36 8a 2f c4 d8 25 cb 59 60 4b 93 f7 f7 f6 87 a4 15 71 b4 31 05 65 27 a3 b6 c7 63 f8 fb 1b f6 e8 36 18 76 99 bf 34 b5 f4 15 15 3b 01 c7 ce da 47 32 9d 84 9a 99 84 d5 df 95 39 7f 07 5a c6 5a cb 0d d8 ea 05 6d 6b 5c 7a 6f eb df df b8 c6 ca 97 24 0a d1 62 a7 c8 f1 e7 10 aa 44 c2 43 a4 92 4d 3c b6 e8 6b 03 f5 f3 d2 be b8 ee 2c e1 81 37 1b 75 00 83 73 66 1d 2f ef 81 96 97 4a 48 66 ce 07 df af 20 7c 84 38 c2 c9 9a 96 50 76 0d 63 52 76 d1 f8 0e 11 e2 8b ff 00 a8 13 32 a6 cc fe 32 3c 2b ca e3 de ab 87 fc 23 ce 1e b9 f4 90 6a 12 b7 3d cb a6 a5 0e 6d 60 23 54 36 eb b7 d7 07 4f 04 1c 2a dd 9a 5c e4 80 d7 2a 38 76 7e 59 0f 8f 43 d8 7e 1f 96 0f 65 95 28 3e 69 b2 48 e8 99 ef Data Ascii: UG)hv[}[ms8LFUs?6/%Y`Kq1e'c6v4;G29ZZmk\zo$bDCM<k,7usf/JHf |8PvcRv22<+#j=m`#T6O**8v~YC~e(>iH
2021-09-15 12:02:48 UTC	187	IN	Data Raw: b9 ca 28 96 0d 36 bf 3e 0c ed ce 20 52 94 b3 6d 6d c6 c3 96 df 98 0c e2 6e 38 86 88 cb 47 42 fa a4 54 63 24 a0 79 41 00 58 21 1e b7 3d 3f 0c 33 c1 76 5a e7 37 cd 05 ff 00 f2 0f e2 76 f3 83 a5 61 73 21 d6 03 ee 76 bf 96 b6 db 58 af 39 bf 10 3e 6f 3c c5 ea 59 5c b1 d7 a8 9b 29 6d bf c7 6e 96 b6 2d 18 4c 39 40 ca 65 80 00 ca 3b a0 3b 30 15 23 61 53 5b f2 11 30 48 0d 41 4e 10 07 9e 55 01 4a c0 ca 1c c4 44 9a c7 9b 48 4e 86 c6 d7 26 db 5f df f0 3f 0f 87 79 ac 00 ab 5f 95 b6 1c 59 fc 22 54 a9 20 54 07 af 3d 2a 38 d5 a0 42 4c dd 2b 68 1a 38 a6 d6 52 36 2c 41 d2 04 81 6e 3c b7 b5 c7 b0 db fb 3d fe d0 a1 52 cb 37 74 54 50 f0 16 d6 ad e7 bc 0e 67 66 51 4d f4 60 fb 6d 5b fb 78 59 cd 54 6a 59 a0 94 28 30 bf 7e da 3c f7 f7 db 6f af 7c 39 95 23 3a 08 01 ac a7 2c 2a 01 Data Ascii: (6> Rmmn8GBTc$yAX!=?3vZ7vas!vX9>o<Y\)mn-L9@e;;0#aS[0HANUJDHN&_?y_Y"T T=*8BL+h8R6,An<=R7t TPgfQM`m[xYTjY(0~<o|9#:,*
2021-09-15 12:02:48 UTC	188	IN	Data Raw: d3 39 4b 28 7e eb 93 90 24 30 48 02 a0 00 90 00 48 64 84 80 94 80 13 16 b2 a5 e0 a4 a7 9e a6 a2 45 8e 08 21 33 d4 4a ec 00 58 a3 56 92 49 24 66 3e 54 8d 11 9b b0 ea 49 b5 c6 25 5e 4a 85 b5 3d fa fe 61 6a 12 a5 2f 24 b0 14 43 01 47 53 d8 35 ab c8 fe b4 45 f1 4f 59 e2 87 8e be 3c 65 b4 7c 2f c5 b9 6e 55 91 71 8f 0b cf c2 5e 1b f0 d4 74 8d 59 98 3e 5b 16 61 cc e2 2e 26 9a 75 90 34 2b 5a c2 2a 7a 98 a2 55 31 d2 85 02 52 1d 80 a4 f6 a0 ed 1c 77 68 65 c1 a9 22 48 a1 3f eb b1 24 3b 77 b9 5d f9 c7 6b f8 5b fe 95 d8 1f 0f 4b ed 1c 42 4a f1 38 a9 99 17 2d 60 16 ab 06 0c fb d6 ac 00 bc 79 5d fe 30 19 e5 25 17 8d b0 f8 5d 97 66 12 e7 d3 78 1f c3 f4 fc 39 c7 55 91 32 98 3f ea 5a 98 c5 4a e5 14 d1 c6 7c a6 8e 26 8c 56 c4 b7 0a ee 8c fe 6b 5d 14 ec 24 c9 38 95 a6 71 4a Data Ascii: 9K(~$0HHdE!3JXVI$f>TI%^J=aj/$CGS5EOY<e\|/nUq^tY>[a.&u4+Z*zU1Rwhe"H?$;w]k[KBJ8-`y]0%]fx9U2? ZJ|&Vk]$8qJ

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	190	IN	Data Raw: 00 23 55 d6 74 93 d7 ab 54 00 cc 9a 89 48 c9 23 cb b1 b5 ee 7a ef e9 7b 7b 1c 33 92 89 79 5d eb cc 03 ce bb bc 01 3c 14 ae e6 da 3f ba fb 78 8b 8e 69 a8 3e d7 94 c0 0b 68 b7 50 06 eb 63 7f a1 df e9 89 94 94 90 6a e5 8b 39 06 ba 68 f7 88 92 58 8e 6f ef db c3 43 82 f8 e2 6c bd d6 a4 bc 91 c9 bf 5b f5 1b 8d b7 00 7a fa e2 bf 3f 0e 48 9a ab d4 f1 0f 6a 10 09 d7 86 90 7c a9 e0 80 97 2f a9 7a ed 7f 17 1d 6b 78 6c 53 f8 df 5c 59 60 32 1b f4 b9 72 40 e9 d0 6a d8 f7 d8 0d c7 4c 09 37 08 14 06 c4 57 7d db f4 69 c6 1a 85 21 a8 53 f9 f1 e5 06 74 9e 25 3c f0 19 a5 a8 76 95 c0 d9 49 b6 fb 76 23 7d b0 2f c8 48 a0 05 ac ed fa 3e b6 89 10 50 f5 e7 4a b6 ff 00 a8 94 87 c4 e7 a7 8b 57 36 50 aa 6c a3 5e 8b f4 b7 53 73 fd bd bd 22 5e 18 a9 41 39 43 6b 41 bf 9b f8 51 a1 8c 99 Data Ascii: #UtTH#z{{3y]<?xi>hPcj9hXoCl[z?Hj|/zkxlS\Y`2r@jL7W}i!St%<vIv#}/H>PJW6Pl^Ss"^A9CkAQ
2021-09-15 12:02:48 UTC	191	IN	Data Raw: e4 8c b9 62 05 b9 b1 ee a3 7b 10 08 d8 da e0 e0 75 a5 28 56 64 80 f4 d0 6d c3 97 86 9a c4 92 fb 73 16 72 a5 09 b9 35 37 d1 eb b0 e7 1b fd f8 38 c9 b8 0f 84 4d 24 99 3f 0d e5 94 f5 b3 1f b3 cd 1e 95 2a 2b 2c 40 62 a6 79 79 92 58 37 4d f7 ea 3d 8f ec a2 17 88 fa 52 59 b4 0d 70 28 ef cb 97 08 a2 7c 51 8f c6 4d 5a c2 ca 92 06 62 32 a8 8d c6 87 6f 37 31 b2 17 cd e5 95 6f cf 90 a8 2c db 36 ec 2d ff 00 8e f6 05 57 a5 94 6d b5 bb 11 8b d9 01 25 21 20 24 14 54 00 00 36 db ef 1c d2 6a 4a d4 a5 15 2b 3e 61 57 25 4c ec 58 bf 0d 4b 53 84 61 8c d1 df 51 2f bf 71 aa f6 03 a6 fe c2 c0 f4 c7 85 2d 47 da 91 0b 7f c9 cb 6f 53 e7 ef 84 7f 45 99 39 63 67 fe af fd bf 4f cb f5 bf 7c 7a 3c 00 d8 0e 2d 5d 78 3b 6f f7 8f bf cc d9 49 b4 bb 8c b6 3a 8f e2 35 0b 74 f7 c7 a3 c0 27 64 Data Ascii: b{u(Vdmsr578M$?*+,@byyX7M=RYp(|QMZb2o71o,6-Wm%! $T6jJ+>aW%LXKSaQ/q-GoSE9cgO|z<-]x;oI:5t'd
2021-09-15 12:02:48 UTC	192	IN	Data Raw: 29 10 c1 1b 6b 96 43 a4 33 7f 49 1d c9 1f 4e a0 7f ae 3d 12 e5 0e fa c4 44 82 7a a9 e2 d7 e7 31 dc b4 a1 9b 4a 86 ea 4a df cc 2c 4e 9b e3 64 a8 a4 b8 dc 79 44 53 df 21 6d 8f 93 69 1d 49 fc c1 eb 68 b2 ce 1e cb a6 cd 33 8c d6 be 87 25 c9 32 ca 4e 5f cd 67 59 ee 73 57 0e 57 94 65 54 9c c7 8e 3f 98 cc 73 1a b8 29 62 32 3a a2 bc a2 ec bd d8 4a 96 67 cc 95 2e e0 bd 2a 2b 4a 96 ab 01 c3 c8 b4 26 07 e6 cc f9 4b 50 40 50 33 0c d5 02 51 2d 32 c2 96 b5 28 00 49 08 48 2b 20 02 58 16 04 98 fd 2e 3f 83 1f f0 d9 e1 df e1 e5 f0 bf 94 e5 d9 e3 53 67 5e 3e f8 bb 16 55 c7 5e 38 71 82 45 1b 3d 4f 10 56 d1 42 f4 5c 39 95 4c d1 73 e0 e1 de 1d a3 5a 7c b7 2d a4 2c 1c a5 2a d4 55 34 b5 a6 69 e5 b6 f6 76 19 58 79 6a 4a 85 5c 92 58 02 5e c6 80 50 27 2a 43 d5 82 5c 92 e6 38 b7 c5 Data Ascii:)kC3IN=Dz1JJ,NdyDS!miIh3%2N_gYsWWeT?s)b2:Jg.*+J&KP@P3Q-2(IH+ X.?Sg^>U^8qE=OVB\9LsZ|-,*U4 ivXyjJ\X^P'*C\8
2021-09-15 12:02:48 UTC	194	IN	Data Raw: 6f 89 b2 27 6f 58 ca 4a 4d 89 6a d4 12 d4 eb 4a 6e da c4 24 f5 81 af a4 dd 74 83 b9 20 dc 8b fe 9f f3 db 10 14 25 cd 35 3a 98 c1 51 72 c6 8f c2 07 6a e4 e6 0f 34 8d 1e e7 7e de 9b 7f ad f1 12 83 12 dc 3d 3c 7d f2 8c a1 44 9b da ba 6e 22 02 b9 74 31 1f 7c ad 98 37 ad c5 ee 2d b1 e9 bf f6 ef 8c 02 45 a0 a2 69 43 52 29 ad 1f 41 f7 80 da fa 8d 2e c1 42 8d 51 86 be e3 4b 5c de d6 eb b7 7f 7d bd 71 ba 26 32 9c 87 a3 0b 03 e3 02 cd 0a fa aa f6 0f e5 76 76 e2 79 44 7c 79 ac e4 24 4c d6 45 3f 7b 7b 9d c9 f5 fc 3d c6 0f 48 13 06 63 a5 76 b7 86 a7 ac 2b 50 6c f9 9d c8 3c b9 8e 75 7f e6 27 a2 cc f4 aa 31 65 b8 de c4 1d f7 b5 c9 1f 4e 83 f1 18 df 22 76 f3 31 0c ac 6a 90 72 9a 01 ab 57 c7 88 d5 a3 2c 66 11 d6 32 6a 6d 24 1d b4 85 17 f6 27 b8 b7 b1 ed 88 e6 0c b6 a5 3c Data Ascii: o'oXJMjJn$t %5:Qrj4~=<}Dn"t1\|7-EiCR)A.BQK\}q&2vvyD\|y$LE?{{=Hcv+Pl<u'1eN"v1jrW,f2jm$'<
2021-09-15 12:02:48 UTC	195	IN	Data Raw: 03 41 5f 28 bd 88 0d 7b dc ed de df 9e fd 30 26 31 60 4a 3f f2 f3 ab f1 e5 66 f0 ac 37 ec 35 65 28 7a b1 2f c6 bc bc 40 f0 6a c3 6e 96 51 12 a9 00 6c 17 a8 3b ec 41 3b 58 0b 7a 6f d6 f8 a7 4d 2a 54 d5 71 25 ed b8 3c fd 2c dc fa 1c 8c 93 19 d3 54 e5 0e e4 96 3e da 3b a9 a3 92 aa 79 0a da f2 1d 85 f6 2d 71 60 3d 40 dc ef 7f 7b 60 79 85 49 70 08 b7 8d cf e3 6a da b0 c5 0c 18 69 a7 3d 09 f7 73 0c 5c 8e 84 aa 98 1a 44 56 f2 eb 1d 2c 01 da d7 23 73 de dd bb e1 61 52 8b b9 77 f7 ce 25 5a c2 54 9d 06 cc 3a 79 bf de 1b 39 5c f2 4b 4c 94 6d e6 55 2c 97 52 05 ed b0 6b 91 63 b7 d6 f7 16 be 21 5a 49 a8 67 d8 eb ee 91 99 78 87 59 a3 6b 71 76 61 cf f3 0c 3e 17 76 a1 0d aa cc d7 62 ba ec 40 b8 db 6e df 53 f4 eb 6c 03 3d 04 28 12 fc 2f c7 83 5a 0d 48 0a 48 cd 52 d5 ab fe Data Ascii: A_({0&1`J?f75e(z/@jnQl;A;XzoM*Tq%<,T>;y-q`=@{`yIpji=s\DV,#saRw%ZT:y9\KLmU,Rkc!ZIgxYkqva> vb@nSl=(/ZHHR
2021-09-15 12:02:48 UTC	196	IN	Data Raw: f8 ba 8a 39 f3 4e 11 ab 88 96 bd 64 39 8d 2a c9 f2 91 30 fb 4d 35 71 c3 c9 db 98 f6 b3 37 ce 98 ef 85 fb 6b b1 f1 0a c2 f6 a6 0e 64 89 c9 4a 94 55 29 2a 5c 8c 89 b1 ce 40 20 b5 48 20 0d 9e e7 ab 60 be 2b c1 63 12 94 0c 4e 69 8b 21 45 06 84 58 50 d8 de 8c 5f 46 84 f5 12 51 57 53 2d 45 36 68 b5 b4 93 c4 26 59 a0 96 16 e7 ab 0d a5 0c ad b8 26 e0 0d 41 80 dd ad 7b 04 b9 12 a5 65 44 c4 15 03 50 af d1 fd c3 e9 6a 54 e6 5a 14 90 87 72 a5 12 00 e2 7e ef d2 f1 1d 54 8f 12 72 e3 20 c3 b9 04 ec 4f 50 45 fb fa 5c 5c 7f 88 67 25 49 39 5e 59 6d 52 a7 6d f5 7b 55 a9 e5 04 64 17 f9 f2 0b d8 85 1a 9b 6b e1 a6 90 3d ff 00 dc 67 97 e5 62 57 28 09 d2 aa 3c 80 5b bb 7a 7a e2 1f 7e fd f9 c4 92 50 95 3a 8a 99 aa 18 02 e3 5d 69 c0 da 3e 4b 96 3c 6c 16 a0 a2 49 6d 5a b5 0f 2f 73 Data Ascii: 9Nd9*0M5q7kdJU)*\@ H `+cNi!EXP_FQWS-E6h&Y&A{eDPjTZr~Tr OPE\\g%I9^YmRm{Udk=gbW(<[zz~P:]i> K<lImZ/s
2021-09-15 12:02:48 UTC	197	IN	Data Raw: f7 d7 b2 82 3a 6e 7d 36 3b 62 15 2c d5 20 b0 07 cb f9 d9 fc ab ec 4f 68 61 10 14 99 21 2a 02 c4 dc 78 72 a9 a5 3c 85 eb e7 a8 79 e3 50 e8 69 d2 17 97 4c be 66 8d ad b2 82 48 2b af b9 1b f6 c6 65 a6 62 89 16 04 81 9a ae 2a 0f ba f2 d5 eb 33 f1 01 65 f3 6a 41 4d e9 5e 77 fc ef 4d 9a 7f 0a 6a e8 29 f3 ff 00 1c e8 56 58 d6 6a aa 3e 14 ab d2 6d f7 66 79 14 b2 d8 ec a1 e2 60 7f 4c 2a f8 b6 5a a7 4b c3 25 88 f9 48 c8 f7 76 cd 5a f8 96 a0 7d 62 e1 fd 26 79 38 be d3 60 08 5c ec d9 89 e0 94 35 28 d4 03 77 ae e2 37 40 61 53 49 24 6f 13 48 e5 8d 8b 31 2a 37 bd c7 6b 5b b0 db b5 fb 62 81 24 81 9d 04 d5 c8 1d 08 7e 22 cf f8 d7 b9 a8 11 30 92 28 12 c7 4b e9 e1 f9 b4 60 51 c6 b1 c7 23 aa 86 22 fd 1e c0 0b ee 05 8d ec 3e 9e d8 3a 48 e1 e5 ad 3d 88 5e af a8 f5 b1 fe 7f 1f Data Ascii: :n}6;b, Oha!*xr<yPiLfH+eb*3ejAM^wMj)VXj>mfy`L*ZK%HvZ}b&y8`\5(w7@aSl$oH1*7k[b$~"0(K`Q#">:H=^
2021-09-15 12:02:48 UTC	199	IN	Data Raw: 37 33 b9 21 88 d0 55 ef e5 ad a0 d4 ca 2a 94 08 0c 52 c5 af c2 bf af 58 95 7c be 9b 2c a4 9f 31 af 92 0a 7a 6a 48 5e a1 e6 63 64 45 45 2c aa e7 a2 86 02 dd ef 7d f6 c6 50 99 b3 a6 22 5c 84 e6 ce a0 33 6d 5d 2a 1f ab 75 8d b1 0d 86 c2 2f 13 39 62 52 91 25 6a 48 71 74 82 c0 92 41 0f 63 f7 8d 0d 7c 49 78 bb 5b e2 cf 88 b9 ac 94 b5 6d 37 0c e4 35 cf 97 65 34 c1 8a c3 52 d1 9d 13 d5 b8 28 80 e8 74 65 88 75 2a 35 29 60 c0 0e cd d8 58 14 60 70 f2 ca 92 7e 6c c9 61 44 90 01 0e 93 41 7a 13 5e 5c cc 7c a1 f1 67 6d e2 3b 57 1f 92 64 d2 65 19 93 52 02 4b 83 90 b3 3d 76 62 c6 87 4a 3c 57 35 42 4b 6f 73 ab 6d f6 37 3f 90 fc 36 c3 72 b7 0c 52 09 af 7b 5e 71 52 20 a5 60 14 e5 4d 68 3d ff 00 16 1a c6 6b a1 30 22 8e b6 ea 7d 41 bf d7 a6 dd b1 18 b0 7d 87 be 30 59 96 42 12 Data Ascii: 73!U*RX|,1zjH^cdEE,}P"\3m]*u/9bR%jHqtAc|x[m75e4R(teu*5)`X`p~laDAz^|gm;WdeRK=vbJ<W5BKosm7? 6rR{^qR `Mh=k0"}A}0YB
2021-09-15 12:02:48 UTC	200	IN	Data Raw: c1 92 e6 ba 03 0b 06 a8 ad 39 18 51 66 74 99 8c d3 c9 53 9e 7f 34 8e 9e 80 39 a5 8e 46 d1 13 34 86 ec cc e9 a5 24 8d ba a2 30 bd 89 06 e7 1b 03 9a 8a 50 08 7a 00 59 60 ee f6 be d5 6a b6 b0 56 1a 6f 7e a3 71 ed cf 9f b3 8d 5f c5 30 ae 5c b9 66 53 03 c1 3c 87 4a 54 a9 28 52 a1 ca a8 31 b0 b2 a8 53 e6 00 f4 b1 b5 bb 0b 32 5c c9 80 a0 ce 9a 11 98 65 1a 81 57 17 6f 52 6d c2 08 9d 86 4a fb c4 8e 05 37 77 dc b0 7d eb 5a b4 67 c3 9b d5 70 ee 43 3e 5f c7 15 99 77 18 64 39 95 3b 1a ce 1e e2 38 e0 cc e8 66 59 39 9c e8 c4 73 07 31 6b 52 43 98 8a 9f a0 24 14 3d b1 d8 bd 8d da b2 46 17 15 84 42 8a 98 2a 79 42 7e 69 2c 68 69 62 ef bd 00 82 30 82 74 92 26 4a 5a 82 b7 24 d8 d5 87 90 2e 74 e0 62 a3 f1 0f c2 d7 c2 3f 8a a3 31 fe 45 c1 b9 f7 82 f9 a5 53 bc d1 67 9c 1b 55 51 Data Ascii: 9QftS49F4$0PzY`jVo~q_0\fS<JT(R1S2\eWoRmJ7w}ZgpC>_wd9;8fY9s1kRC$=FB*yB~i,hib0t&JZ$.tb?1ES gUQ

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	201	IN	Data Raw: 32 dc 51 2a 3d e2 05 8a a9 42 db d7 76 36 06 a8 cc 32 ac f2 43 07 09 f0 6c d4 42 ba 4b 65 d0 e6 75 53 66 d9 90 a7 8d 95 66 cc aa 61 59 25 57 73 21 04 c4 8c 10 93 ac 49 1a 9c 1f 25 2a 4c a4 e6 29 51 2e cc e7 4e 2c 7f 17 21 da 34 74 96 60 41 0e ef 5d 4e d4 b7 1e 94 89 f7 e1 aa 7c a9 69 aa 78 96 b6 48 dc 86 7a 5e 1d cb 9a 3a 5a c9 2a fb 7c d4 f4 c5 5a 15 5b 73 1a 9d cc 80 ab af da 1b 69 c4 53 94 43 a4 d0 5d eb 61 fb e9 c7 58 2b 0f 28 fc c0 a2 01 01 e9 4d a9 a1 dc 7a c4 5d 3e 6b 58 ad 24 6e 90 8a 70 cf a9 1f 5d 42 02 49 01 4b 10 ae ce aa 42 96 bd 99 af 6c 2f 25 d4 6b b9 f6 dc 7c 0f 95 87 0e 89 61 2d 97 4d 1b 9f 89 23 ed c2 3b e2 a8 cb 23 67 6a 6a 69 12 a6 d6 f9 95 8d 5e 15 2d d4 98 ac 5e c2 db f9 bb 0d bd 35 24 0b 36 b6 f5 d1 cf 0b 9d e0 83 88 12 9f 2a 7e c7 Data Ascii: 2Q*=Bv62ClBKeuSffaY%Ws!I%*L)Q.N,!4t`A]N|ixHz^:Z*|Z[siSC]aX+(Mz]>kX$np]BIKBl/%k|a-M#;#gjji^-^5$6*~
2021-09-15 12:02:48 UTC	202	IN	Data Raw: 64 bc 0a e4 58 13 72 a5 b5 1b f7 bf 50 01 db f1 eb 38 b4 26 51 5a 89 75 77 49 76 7a 8f 2d fd 01 8c 9c ae ad 59 95 99 18 40 e9 e5 49 0e a3 7f 4d ef 6b 1e 9d 7d ef 8c 1b 31 7a d1 f9 d2 be 31 2a 26 94 86 67 1e 62 19 19 14 a5 ec 0a d9 6d 74 20 a8 61 6e 8b db 6e 84 8c 46 a4 e5 2c e0 f2 78 94 4c ce 72 a6 9c 4d 3d 09 de d0 f0 e1 29 24 6e 4a ca f7 d2 4e 9e e4 8b dc dc 0f 4b 5b d2 fd fd 16 cc ee a9 88 77 26 d5 d7 f3 04 67 52 41 af bf df 17 8b 7d c1 f4 06 5a 68 8b c8 84 06 42 d0 ea b1 e5 9d ae de c0 0b 9f 41 f7 ac 2c 71 2c 89 06 62 bb a0 06 de ae 09 ae ef b5 75 b4 22 ed 09 ca 22 86 fa 13 e3 6d 75 e3 1a 5f f8 f0 f1 95 7c 4f f1 5d b8 4b 25 96 36 e1 8f 0f 5a 5a 0b c1 21 68 2a b3 b9 50 45 53 22 00 48 22 04 3f d5 ac ab 11 e6 01 6d 87 12 95 f2 92 52 68 c6 a0 f2 bf 16 e3 Data Ascii: dXrP8&QZuwIvz-Y@IMk}1z1*&gbmt annF,xLrM=)$nJNK[w&gRA}ZhBA,q,bu""mu_|O]K%6ZZ!h*PES"H"?mRh
2021-09-15 12:02:48 UTC	204	IN	Data Raw: 20 8e 08 5a 96 95 03 49 22 b3 4a e2 c0 74 de cd 7d ba 8d b7 dc 1d fa 8c 13 22 42 b2 e7 52 69 b9 6a 35 b9 b7 2f 56 38 2b 0c 58 d6 da fe 34 84 ae 6d 58 f1 c9 33 b4 9a 95 8b 39 b9 bb 02 2e 42 dc 1e 84 f5 1e 98 75 85 94 55 95 8f 74 eb ce fc fa 0e 4f 02 4c 5b 02 08 67 b7 ba fb a4 00 66 b9 8c 8f 10 74 75 1a 41 3c b2 fb 3d 81 00 58 03 7b 5c 1b 6d db e9 86 42 40 49 77 36 f0 73 6f 2e b1 12 0b 86 26 a3 d3 f9 85 cd 7e 7e 67 b5 2c 92 32 f2 ce ae 7a d8 3d c6 fa 45 c8 24 03 ed ed 89 25 ca 4a 96 90 6c 6e ec d6 3c 23 78 e7 97 71 4d 7b ba 52 56 aa cf 96 e9 d2 8c fe 79 08 dc 06 21 b6 16 eb b9 b8 b6 dd b1 99 b2 12 33 65 a5 09 23 a7 83 f1 fe 07 a2 4e 29 69 25 79 22 86 68 d8 1b ed 61 b0 04 5e e2 e7 f6 3e 98 00 a1 40 39 04 08 f4 62 f1 06 63 49 96 2c ba 61 e7 03 08 16 26 f1 ae Data Ascii: ZI"Jt}"BRij5/V8+X4mX39.BuUtOL[gftuA<=X{\mB@Iw6so.&~~g,2z=E$%Jln<#xqM{RVy!3e#N)i%y"ha^>@ 9bcl,a&
2021-09-15 12:02:48 UTC	205	IN	Data Raw: fc 51 aa 35 5e 0c f8 9a bc 13 e2 0e 6a 1a 9e b7 c1 4f 19 73 08 a9 93 e6 a4 83 9f 4f 49 c1 7c 73 cc 34 39 8a 44 b1 cb 35 44 d9 b3 4b 0c 4b f6 08 22 64 b6 09 5f f7 32 e5 26 5a a5 67 93 2c 7d 69 b3 12 12 9c e4 3b 54 28 0a 67 ef 3a 8d a1 69 5e 01 78 b7 9a a1 2a 76 24 25 4a 92 a6 4f 7c 02 a5 99 34 49 98 e1 49 49 19 be 5a 7e 58 4a 02 48 98 ea 4e 30 f8 67 f8 83 c8 33 f8 e9 78 ab c3 2c fa 8f 2a 7a 91 4d 41 c4 d4 2a 99 e7 02 c9 04 62 31 55 99 c3 c4 79 74 af 45 53 45 49 1b f3 64 9e 35 00 32 c8 9e 66 b0 3e 4c fe cf 29 01 33 e5 a4 9f a9 07 32 54 14 1c 17 19 1a bc 14 59 88 bb 88 1c c8 ed 11 3d 68 5e 16 62 65 b8 32 d4 0a 15 2d 49 21 e8 52 b2 43 33 77 92 18 d9 ee 66 32 ba ae 0f e1 68 b3 3c bb 84 ab 46 6d 5b 04 2f 4f 99 f1 e1 26 3a cc ca 58 f4 7c c6 5f 90 53 85 65 a7 ca Data Ascii: Q5^jOsOI|s49D5DKK"d_2&Zg,}i;T(g:i^x*v$%JO|4IIIZ~XJHN0g3x,*zMA*b1UytESEId52f>L)32TY=h^be2-I!RC3wf2h<Fm[/O&:X|_Se
2021-09-15 12:02:48 UTC	206	IN	Data Raw: 24 69 cb a7 e7 57 8d 11 50 c3 7f 7b 5f db 58 58 8c 95 21 48 69 f9 f4 89 a4 b2 b0 78 45 ec ac 02 9d 57 1f 78 5a e7 6d f0 b2 6e 20 ab 30 e8 df 6f 66 fb 43 3c 32 4a 52 92 68 f5 e8 ff 00 a8 23 9a 8f 2f a5 73 2f 22 eb 3b 1b 54 3a 80 ab 71 7b 90 3e b6 b7 6b 5f 03 a0 95 20 b8 2e f4 04 d4 b3 70 f5 16 bc 15 31 49 cb 43 a1 7d 1b 6a b5 f8 d3 ce 07 f3 0a 37 a6 7e 72 ca b3 c1 28 20 89 4d ad 7f e9 55 17 f2 ef b5 c0 c3 09 20 84 ec fe 75 3e eb 09 67 ad 24 90 0b 97 3b ea 41 f7 e7 03 55 34 71 05 65 53 11 d5 22 b9 8d 9a c0 6d 7f 28 20 82 3a db 06 26 a9 07 40 00 7e 3b 42 f2 08 2c 45 7d fe 23 15 94 0b 04 54 0d 1e 9b 08 ec 6d f5 03 7d fd 2d 6c 4a 10 08 72 5b 5e 1c 3d ff 00 31 84 f7 8b 71 6e 5e c5 62 5e 9b 35 48 1e 04 69 4c 2a 18 9d 60 6c 64 1b aa b7 5d bd 6f b6 35 32 02 b5 a9 Data Ascii: $iWP{_XX!HixEWxZmn 0ofC<2JRh#/s/";T:q{>k_ .p1IC}j7~r(MU u>g$;AU4qeS"m(:&@~;B,E}#Tm}-lJ r[^=1qn^b^5HiL*`ld]o52
2021-09-15 12:02:48 UTC	208	IN	Data Raw: ac 5c 79 8f cc 7f ff d9 Data Ascii: \y

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49813	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	208	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fb4d84d7a-e7a0-4e71-a4e1-288b18f4b1a1_166a74d60a77edc1b295914db4bc79ac.jpeg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	210	IN	HTTP/1.1 200 OK Connection: close Content-Length: 7639 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 3322308306793002246510820078718104138 75,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "aa0dc1037ef3ab4c187e7acc5a5ad5cd" expiration: expiry-date="Fri, 27 Aug 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Tue, 27 Jul 2021 18:22:44 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 21 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb801 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 1834677 X-Served-By: cache-wdc5539-WDC, cache-dca17727-DCA, cache-hhn4062-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1631707368.289564,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fb4d84d7a-e7a0-4e71-a4e1-288b18f4b1a1_166a74d60a77edc1b295914db4bc79ac.jpeg X-vcl-time-ms: 1
2021-09-15 12:02:48 UTC	211	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 01 04 03 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 01 03 04 05 06 07 08 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 ef 6a 37 e3 f4 4d 02 61 a0 40 6a 34 c9 14 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"4j7Ma@j4
2021-09-15 12:02:48 UTC	212	IN	Data Raw: 02 02 02 01 03 03 03 03 04 02 03 01 00 00 00 01 02 00 03 04 11 05 06 12 21 10 13 31 07 22 41 14 20 51 15 23 32 61 71 81 17 24 25 42 ff da 00 08 01 01 00 01 09 00 dc dc dc dc dc dc dc 06 77 4d ce f3 0d 80 78 83 65 3b 88 57 ad 8e 95 b7 37 ea 4c 1f bf 73 73 7f b3 73 70 90 36 4c cd ce c7 c3 a9 ad ca c9 b7 ea 3f 4e 53 61 55 b7 96 fa a1 c7 8a d4 71 15 72 3d 6d d5 79 d7 33 5b cb d1 d6 5d 5b 8a c0 d7 cc 71 7f 58 b9 3a 75 5f 2b c6 70 5d 53 d3 dc fa 7f f3 f3 c8 20 e9 81 84 c1 fb f7 37 e9 b9 bf 52 75 3a 87 a9 70 78 4c 36 bf 21 f9 9e 77 37 9a c9 7c 8c c7 44 2c 3b 66 26 0a 3d 16 2f 6e 56 26 42 37 95 36 95 3a 60 e8 8f e6 b9 a6 16 23 83 d2 3f 55 32 29 b2 bc 1e 7c d7 6d 57 d3 5d f4 5b fb c4 dc dc dc dc ee 9d d0 b4 ea 7e ab c3 e0 b1 3d c7 3c a7 29 9d cb e6 be 66 63 8d 6f Data Ascii: !1"A Q#2aq$%BwMxe;W7Lsssp6L?NSaUqr=my3[][qX:u_+p]S 7Ru:pxL6!w7|D,;f&=/nV&B76:`#?U2)|mW][~=<)fco
2021-09-15 12:02:48 UTC	214	IN	Data Raw: cb 72 f7 c9 2b e0 e7 25 a1 b8 ee 48 f8 fb b2 33 7d c1 a9 ca 5a 99 1c f7 29 72 c4 f8 f3 1c fd ba 9d 2c 4a e4 65 38 98 be 14 44 95 5d 65 44 f6 9e ab e8 7e 8d 64 39 38 a5 6a 76 d9 50 6b 75 1b 2b e9 f5 f9 b5 c0 f4 c2 4c 66 51 70 53 32 17 4a 1a 74 65 a7 f5 79 d5 93 57 7d 37 28 58 1a c5 a4 b1 98 f8 b9 f6 11 65 e1 02 2e 83 35 57 f1 de e2 1f d5 87 c0 da da b9 55 67 60 b6 d6 bc 9e 47 8e ab 3a 82 8e 68 c7 e5 78 fb 9e 9b 93 9b e6 6e c5 c2 72 a4 6f dd 22 03 1f 5a 9d 27 ae fc b6 d6 06 8d 5b 25 3e 3d 39 6e 25 39 3c 65 55 ba be 8c e9 5a 6d 5b 28 e3 b0 ba 77 8c c0 cc 5c ac 6b 3d 3e bf e8 d1 d1 89 29 6f be d7 99 76 37 6d 4b 3a 67 30 53 cf 54 84 95 2f 4f 72 4e 33 22 ab 6b 01 d7 90 c2 76 b5 80 ca 1c 4d cf 73 04 e6 b0 31 79 a7 47 55 7a 17 9e af b8 7b 56 e3 e7 de 8e ad 9f c5 Data Ascii: r+%H3}Z)r,Je8D]eD~d98jvPku+LfQpS2JteyW}7(Xe.5WUg`G:hxnro"Z'[%>=9n%9<eUZm[(w\k=>)ov7mK:g0ST/OrN3"kvMs1yGUz{V
2021-09-15 12:02:48 UTC	215	IN	Data Raw: 13 62 7e 65 9f 12 a2 35 e8 01 88 bb 22 6b c6 c4 d7 98 80 7d be 5d fb 44 1b f9 8a 7f 98 a7 50 37 88 cd f0 36 27 91 0f 88 49 02 36 f5 b8 a6 2b 6c 4d ff 00 33 60 1f 04 00 57 cc 67 11 4f f3 1d b6 7c 4a bc 08 67 69 1e 0c 03 51 9b 49 00 fc c2 e5 4e a0 3f cc f1 3f 31 44 1e 0e e6 b7 f9 5d 4d 7f bd 68 46 f1 a8 44 3e 20 31 fe 23 fc cd fd 80 08 ab 2c 6d 8d 02 75 2b d6 a7 fc 8e df f6 74 a0 c2 77 a8 5b f1 00 f4 13 7a d4 59 fc 42 62 fc 7a 6f 51 88 33 c6 8c 22 7c 4d c3 e5 a0 30 b7 cf a7 c1 11 3e 3d 00 fe 23 1e d1 3b f6 66 f5 09 d0 8a 7c 81 18 78 80 ee 03 01 d8 3a 8e 62 79 59 a9 a3 18 80 60 30 42 06 a1 84 81 06 bc 4f 93 07 fb 80 7d d2 b6 9b 8a 06 cc bb 7d c7 70 6f 5b 84 ec c7 6d 28 12 a5 fb 59 c9 77 fb 3e 57 c2 fc d6 7e d2 37 4b 6c 58 ba 27 7b 02 56 3c 4f fb 8f f8 10 7c Data Ascii: b~e5"k}]DP76'I6+lM3`WgO|JgiQIN??1D]MhFD> 1#,mu+tw[zYBbzoQ3"|M0>=#;f|x:byY`0BO}}po[m(Yw>W~7KlX'{V<O|
2021-09-15 12:02:48 UTC	216	IN	Data Raw: c2 89 8e 04 5a 6c 64 a8 a0 ed 3d c7 7f 01 0f 02 ba 3f b5 c1 00 80 c3 e2 63 86 90 83 de 93 68 69 12 82 bd 64 74 51 00 2c 92 53 20 63 35 68 04 46 49 c5 20 d5 da aa 95 2a f0 38 a4 10 16 80 e3 c4 a0 69 1d 78 8c 9c 9c 13 68 78 b4 e0 e4 e0 f9 03 e7 bf 3d 79 0e 15 73 fc 0b 56 7d 2b c8 c8 c0 c8 45 56 5b a5 ff c4 00 3d 10 00 01 03 02 03 05 05 05 05 06 07 00 00 00 00 00 01 00 02 11 03 21 04 12 31 10 20 22 41 51 13 30 61 71 81 05 32 42 91 b1 40 43 62 a1 c1 14 23 24 52 92 a3 15 50 63 72 b2 c2 d1 ff da 00 08 01 01 00 0a 3f 00 ee 80 57 50 07 39 80 9b f3 1f 66 a7 41 83 52 e3 a2 7d 68 d7 20 30 9d 52 b3 9b 04 d7 6f 0b 15 56 0e 4c a5 c0 d0 ab 11 f8 e1 ff 00 55 47 13 4f f9 e8 cd 1a 89 a6 ac 49 c3 d5 e0 aa 3d 0e aa 08 fb 11 9f bb 60 d5 ee e8 9d 25 c4 b6 97 c2 c1 d0 05 00 ea Data Ascii: Zld=?chidtQ,S c5hFl *8ixhx=ysV}+EV[=!1 "AQ0aq2B@Cb#$RPcr?WP9fAR}h 0RoVLUGOl=`%
2021-09-15 12:02:48 UTC	218	IN	Data Raw: cc 67 a7 09 0b d9 35 4c 18 cf 4d cc 00 95 ec e8 90 24 bd c4 4f f4 af 67 b5 8d 07 3f 67 49 ce 81 d3 31 85 8c 92 e0 7b 17 86 9a 31 d0 36 24 2f 84 89 fc d5 83 da c6 7a 5c 95 f7 ae 3f 99 da 08 ab 8a a6 4f 93 1b 04 ff 00 71 59 cc 69 8f 31 b9 81 ae e9 6f 66 ec 2d 17 d2 b4 5c bf 3b 9d b9 c6 30 d8 97 b8 74 0f 2d 46 e2 55 98 c5 c7 4d ed 7b 7d 10 87 37 4e 87 98 5c 07 de 1b 32 54 fe 60 8d 48 e8 e8 90 9e 40 d1 ae 7d ad e4 83 5a 3d d6 37 41 b0 c9 5c 40 65 60 ea e7 2b 93 b3 92 b3 5c df fd 3f 40 b4 68 1f 2d ca 9f 39 47 d4 02 a9 1a 90 f7 0c f4 c1 00 31 a4 af 64 1f 3a 0e 42 ae 24 b1 ac 19 5b 95 8c 60 d1 ad 0b a3 5a 3f 11 46 e6 4e c2 68 d5 f7 9b 3a 1e a8 38 11 2a dc b6 c2 11 b0 40 44 e1 f0 ef e2 23 9b b7 20 d5 73 ea 09 e8 44 0f a2 d0 ef 70 f6 45 8d ea 73 98 5c 46 15 82 b5 Data Ascii: g5LM$Og?gI1{16$/z\?OqYi1of-\;0t-FUM{}7N\2T`H@}Z=7A\@e`+\?@h-9G1d:B$[`Z?FNh:8*@D# sDpEs\F

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49812	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	208	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_433%2Cy_315/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F560ad3dcc869b1dfc2bac1c99d35ac81.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-09-15 12:02:48 UTC	218	IN	HTTP/1.1 200 OK Connection: close Content-Length: 30700 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 550204376734049424187239129429686063570,356783493054973386712452738309102663104,29ecf9b93bbf306179626feeda1fab70 etag: "2d3b14e350cb8481dabec32ecfd0a4b0" expiration: expiry-date="Sat, 28 Aug 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Wed, 28 Jul 2021 10:56:14 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 27 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb803 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 2770538 X-Served-By: cache-wdc5575-WDC, cache-dca17747-DCA, cache-hhn4047-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1631707368.294766,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_433%2Cy_315/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F560ad3dcc869b1dfc2bac1c99d35ac81.png X-vcl-time-ms: 1
2021-09-15 12:02:48 UTC	220	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 04 04 04 04 05 04 05 06 06 05 07 08 07 08 07 0a 0a 09 09 0a 0a 10 0b 0c 0b 0c 0b 10 18 0f 11 0f 0f 11 0f 18 15 19 15 13 15 19 15 26 1e 1a 1a 1e 26 2c 25 23 25 2c 35 2f 2f 35 43 3f 43 57 57 75 01 08 08 08 08 08 08 09 0a 0a 09 0c 0d 0c 0d 0c 12 10 0f 0f 10 12 1b 13 15 13 15 13 1b 29 19 1e 19 19 1e 19 29 24 2c 24 21 24 2c 24 41 33 2d 2d 33 41 4b 3f 3c 3f 4b 5b 51 51 5b 72 6c 72 95 95 c9 ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 36 00 00 00 07 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 07 06 08 09 01 00 03 01 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 f7 f0 00 00 00 05 7e 3a e2 3c 7e e7 Data Ascii: JFIF&&,%#%,5//5C?CWWu))$,$!$,$A3--3AK?<?K[QQ[rlr76~:<~
2021-09-15 12:02:48 UTC	221	IN	Data Raw: 4c f5 fe 33 bc c1 f9 bf 5f 73 9b cb d2 68 a0 87 01 00 60 a6 c2 03 48 00 30 82 41 30 26 b6 38 29 0c 7c 32 3f 03 da 98 b4 64 7a 96 9c c3 d5 f9 bf 57 ed f3 99 77 41 9c e7 f4 ec ae 86 d8 c0 30 88 e8 8e 31 22 81 20 01 4c 0a 8c 40 23 83 e2 6d b5 23 36 f0 3d d9 23 30 8c 2d f3 a7 ce 1e df c7 7a 83 0e 4f 2c f4 77 f2 58 fb c0 a7 9a 79 a9 6d be 27 29 30 92 12 21 34 01 43 84 9b 87 9c c9 25 46 6b 33 c4 7e 73 ed d2 20 52 c7 7e e3 46 f4 3c 2d 6f d3 f8 fe 9a 4c 1e fd 7a f8 e8 74 95 99 ba e2 45 61 21 e3 2e b0 9c 63 79 3a 5c 4b ba 8b b5 9b b0 9a 71 e4 b3 25 d6 60 5f 37 7e 7f f5 35 89 60 d8 00 dd f5 e6 63 d8 f9 6f 59 bf 15 92 d0 0b 33 3a c9 40 85 49 5a a1 6b 15 d5 5d c5 73 55 1a 65 59 4a ae d3 0b 74 4e d1 e7 a2 22 d7 ce ff 00 35 f6 ca 54 cb 97 50 86 47 67 a6 ba bc 98 7e cf Data Ascii: L3_sh`H0A0&8)|2?dzWwA01" L@#m#6=#0-zO,wXym')0!4C%Fk3~s R~F<-oLztEa!.cy:\Kq%`_7~5`coY3:@IZk]sUeYJtN"5TPGg~
2021-09-15 12:02:48 UTC	222	IN	Data Raw: b5 d3 23 c7 d1 65 36 9b 6f 96 97 fb ab c7 c3 f1 8d 5c f2 48 32 a1 fd 6e 4d 93 f8 dd bf 3c 7e 61 69 75 af 58 02 a2 da bb 6e 9b 4d 30 28 8d 8a a8 19 06 1d fd 10 69 25 69 f2 9f 4d 59 46 d1 8e 94 c0 b5 6c 41 42 ad ac 53 11 b4 af ee d9 ad 65 b0 51 ae b9 e9 83 16 73 b2 cd 4f 66 bb ca ba e6 c0 ed 30 13 fd 1d 33 31 41 4c 56 bb 41 c5 a1 3b 9e ad 58 f4 8d 0d d2 d5 14 4a 7a 14 6a d8 88 db 6a 91 a9 18 db db 02 75 b1 05 ed a4 5e 2c ca 07 d9 61 65 e5 c2 f4 a2 65 0c c0 07 1a f3 7f 96 74 ef 71 13 9e 0d aa 11 94 de 9c f8 c3 f6 a8 94 81 9d 7a b6 8b da 5a bf 6f bb 4d f0 d4 10 47 ce 19 fd 9e 6c f3 c0 6d 8a cc 5d 82 0f 6c ef 1f 5a bf d3 33 9e 92 36 d6 d6 b9 cb ad 48 1e 82 da 77 a7 b6 17 d6 37 b1 04 d4 7c f0 d7 16 ac e4 cc 14 87 88 5b 88 32 e2 ef a9 61 ff 00 f0 49 19 0f 86 ba Data Ascii: #e6o\H2nM<~aiuXnM0(i%iMYFlABSeQsOf031ALVA;XJzjju^,aeetqzZoMGlm]lZ36Hw7|[2aI
2021-09-15 12:02:48 UTC	224	IN	Data Raw: dc 4b 08 4a c9 e3 ba 92 c6 ce 9b a8 df 8b eb 88 fa 24 59 2c f1 3d 64 93 42 f1 4d 97 01 d6 64 5d f6 19 40 de 39 ea b1 fa d9 51 4e 1e 32 eb 3e ca e1 e8 b2 7c 5b d9 6e 2e 39 ea 0e be 30 ed 34 df 12 20 2c bc 5b d6 d0 bb ef 40 87 f1 1f 4b 96 5b 63 18 7f 94 1d 25 c3 a0 da 4e de 21 e8 f7 b6 1a 5f 78 f0 f3 e8 2e 49 a9 79 f8 7d c0 f7 da f5 32 7b ce 1f 3c fe 74 e5 67 c9 1c 7d 2b 17 fe 21 a7 93 b9 1c e2 b3 6e 43 4f 2a 73 98 cc 7b 72 b7 f2 da 9c ef f0 fe 35 7f 30 61 4d a3 2a a1 9f 35 17 4d a3 2a 29 af 9c 5a c6 b1 8d 17 d7 ce 6d f4 da 72 a0 15 f3 7b bd 35 d2 90 36 5e 6d 7f b4 6b 31 8c 79 ab a4 b8 fa 6d ef 6f 33 75 30 27 d7 9d f6 f3 3f 57 90 b9 eb f5 ca f3 17 55 9f d0 f7 23 7f 2d 75 35 2e 99 7d cf f9 a5 d6 58 e9 1e c4 63 e4 ce ab 7d 08 a4 91 4f 24 f5 37 13 5d 3e e6 fe Data Ascii: KJ$Y,=dBMd]@9QN2>|[n.904 ,[@K[c%N!_x.Iy}2{<tg}+!nCO*s{r50aM*5M*)Zmr{56^mk1ymo3u0'?WU#-u5.}Xc}O$7]>

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	225	IN	Data Raw: 68 0e e1 99 97 69 c2 b3 11 e4 eb 73 3f 0d 5d be 9f 44 31 ba 73 e1 05 30 f3 13 2f cd 2a 4b 31 79 d2 dc 92 45 fa 42 92 e2 9c 72 8a 1b f8 46 02 0b cc ae 34 9d 43 24 52 b2 af 8e 3b e3 b9 c2 37 f1 f7 58 2a 96 79 cc 13 e4 04 1f c7 1a 49 39 41 ae 94 22 65 04 e0 65 fa 64 08 dc 4e 82 19 1d 3a 14 6e 2f 01 11 1d 1a c4 8e ed 90 98 8f d3 2e 54 de d8 00 30 9d 10 ea 9d 5c 60 96 ad e8 73 01 a6 c1 86 a4 07 44 02 c4 85 d9 24 56 f1 80 85 12 b6 e8 54 b3 6d 8e 85 28 dd 1a b3 fa 28 cc b4 a4 a7 5f bf 52 40 25 29 35 68 c4 75 8c 54 10 b8 b0 af bf 5a cd 6d 33 b6 18 b4 e8 10 b7 c3 a5 ca 57 f9 3f 99 28 01 c8 9d ba ae d7 8b 72 be 32 99 8d f7 87 06 b7 5c ff 00 10 1c 26 26 f3 ab cc 52 b8 59 3a 29 29 e6 7c e9 75 ce fc d9 2e 23 9d d5 ae 30 9b 46 96 e6 bf 90 e7 3e e5 d1 28 dd a1 5d 87 01 Data Ascii: his?]D1s0/*K1yEBrF4C$R;7X*yI9A"eedN:n/.T0\`sD$VTm((_R@%)5huTZm3W?(r2\&&RY:))|u.#0F>(]
2021-09-15 12:02:48 UTC	226	IN	Data Raw: 5a 4f ef d5 74 f7 ce 26 d1 9d 2b f1 fd 5b 7c 66 f9 6b 4b 68 7e 6c 7c b7 c2 82 d9 74 f1 9d 01 cd 97 02 60 ed 18 e3 8f 73 c7 49 11 0c 79 69 2b 2d 02 ab 40 79 75 64 d7 55 7a dc 0e 55 09 3b e8 b0 91 44 e7 91 6c 5d d6 9e a8 55 0a f4 63 f8 f6 8b c4 04 7a 1b 65 cd 05 0f 28 14 ab a9 6b 5c 29 40 ef a2 96 b7 ce f8 af a6 aa 5b 6f 8e e1 05 5d 13 b7 27 02 d7 e1 5d 52 35 dc 53 97 4e 3b a3 60 40 ac 40 30 3d 95 1d 22 17 93 25 fa af 34 5c 75 25 92 bb 84 5a d9 fc ab 75 91 05 2a 2b 17 6d 00 c3 4b af 30 3e 85 86 23 6f 5c 4a 54 fc e9 1c ac 6f f4 be 36 8f 69 b5 2b 69 f6 f9 7d 3a cf b7 ee 33 ac 45 bd 72 5d 5b 7e 2f ac 5d d0 2f a7 90 82 1b 8b ed 40 ea 10 7a e1 7b 6d 16 3a 1f 6f b3 f2 87 2b 03 91 8b 45 90 f9 5b f2 69 8e d8 e6 7a 6e 8d 80 c3 eb 04 1e 85 db 61 72 b4 b4 2b 97 2d b8 Data Ascii: ZOt&+[|fkKh~l|t`slyi+-@yudUzU;Dl]Ucze(k\)@[o']R5SN;`@@0="%4\u%Zu*+mK0>#o\JTo6i+i}:3Er][~/]/@z{m:o +E[iznar+-
2021-09-15 12:02:48 UTC	228	IN	Data Raw: ce f3 6b 69 3e b0 a4 ce 31 68 8a d6 b3 1e be 13 3f f9 f6 88 9f 5f af 5f 09 ff 00 8a d6 67 df d4 c4 7f cc 7b 7b 44 fa f7 8f 5e 3c 88 bf 29 e4 5a 7a ba d1 fe 86 74 d6 c2 2d c0 83 d6 07 9e 99 e0 0a e0 f3 c6 27 a3 38 ae e6 bd f7 59 68 8a cf b4 fa f0 31 b0 1f 94 57 52 67 cc a2 58 af 16 f4 83 c7 a5 ee d7 31 54 3a f6 03 d4 29 00 3c 93 aa f4 8f 6d 58 84 d0 a0 f3 6f bc 80 3f dd 0e 56 6a 98 f4 f9 11 0d e5 a7 2c 68 51 ac 5b 56 56 f8 e3 15 d3 0a 89 25 e7 84 c5 0b 81 63 3c e8 14 4d 6d 11 3f a3 04 b0 ba fc 2d 6f df eb d7 ef d4 fc bf bf af fc fa f8 fa fd 7a fe 9f 7f 5e 32 ae 77 e7 bc 8b 4f 54 08 4c f0 a6 56 d6 1a 2c 5 c f9 59 b0 57 90 bc af d3 f5 e3 57 9e 58 90 e4 e2 a9 f0 af 5e 0e 33 49 9f 8c fb c8 27 98 b1 90 2c 03 bf 65 e6 c7 5d b7 3b ba 55 bc de 5a e1 4a c7 d4 d4 1e Data Ascii: ki>1h?__g{{D^<)Zzt-'8Yh1WRgX1T:)<mXo?Vj,hQ[VV%c<Mm?-oz^2wOTLV,\YWWX^3I',e];UZJ
2021-09-15 12:02:48 UTC	229	IN	Data Raw: 5b d0 44 27 79 e7 24 aa 75 45 39 00 9d 27 c9 52 7d 22 09 71 86 90 75 08 dd 37 89 3a 99 a7 00 b8 36 43 f3 87 8f 35 52 e5 af 23 4d 36 b0 e3 bc dc 10 02 f5 82 5d 2f 13 99 4f a9 4d f9 d1 98 f1 45 ce 63 20 39 da 5d d0 12 15 53 4e bd 9e c5 8f 63 04 12 4c 38 05 c3 6a c0 20 d0 6b 9a 22 5d 24 0c 6d 31 b9 55 6e ab 07 bf 48 30 f2 d2 34 93 a7 19 db 19 57 17 2f ae c6 35 ce 0e d3 91 01 52 a3 45 ce 3a c9 d0 1a 35 67 c7 18 f7 2a c2 93 1f a6 99 24 46 e4 cf 63 5a 1c 60 ba 04 6e ad 5b 49 da 98 e7 b6 1c 3c 32 99 56 e6 d9 b2 e0 27 58 ee c0 f6 55 7b 07 3d ae 75 3a cc 73 5c fd 42 46 98 9f 3f ab 41 c1 b5 58 49 23 3b cc 42 78 03 ed 6b c4 81 b4 02 9c d3 bc 61 15 08 49 ee ea 84 5a 35 41 28 d3 23 2d c8 f1 84 e0 47 50 82 03 53 00 d6 01 9d 8a 15 03 68 10 f7 39 e3 41 00 74 83 05 35 fa Data Ascii: [D'y$uE9'R}"qu7:6C5R#M6]/OMEc 9]SNcL8j k"]$m1UnH04W/5RE:5g*$FcZ`n[I<2V'XU{=u:s\BF?AXI#;B xkaIZ5A(#-GPSh9At5
2021-09-15 12:02:48 UTC	230	IN	Data Raw: 04 b4 1f 25 eb fc 43 ec f0 ab 26 fc 10 e2 5c 6c 7b 36 96 2d fd 57 7e 2b e9 5e 3f f9 9b 2f 93 ff 00 15 f4 a7 1f fc d5 97 c9 ff 00 8a fa 47 8f bb ad a8 fd 52 8d ef 1f db 9b 6f f0 62 37 3e 90 3b fe 72 98 f7 53 0b 9d e9 01 fe 90 1f b2 67 e0 b9 bc 7f fa c7 fb a6 7e 08 bb 8e 9d f8 91 fd 93 11 1c 5c ef c4 ea fc 1a 11 a5 c5 8e 0f 13 ae bd 57 89 3b 7e 27 75 f0 79 0b d4 a ff 00 ac af 7f 6a e5 ea 77 df d6 37 bf b5 72 3c 3a e0 fb 57 d7 67 df 54 a3 c2 dd 3f ce 2e 0f fe 42 be 87 0e f6 aa 56 3e f7 95 f4 15 07 6e 1e 7d e5 7d 03 6d d2 9f ef 5f 41 5a 0d e9 fe f2 85 93 41 db 75 ea 22 70 30 85 a0 0e 88 42 cc 64 42 16 51 20 84 db 40 44 42 16 80 82 0b 53 6d 01 10 46 57 aa 02 23 aa f5 59 1e c8 94 6d 9b 00 c6 57 ab 09 90 d5 ea ad 99 01 7a bb 1 a 62 17 aa 81 d3 0b d5 80 10 40 42 Data Ascii: %C&\l{6-W~+^?/GRob7>;rSg~\W;~'uyjw7r<:WgT?.BV>n}}m_AZAu"p0BdBQ @DBSmFW#YmWzb@B
2021-09-15 12:02:48 UTC	232	IN	Data Raw: d5 0a 20 c8 57 54 5a 0e 3d 97 2e 25 62 2a 31 ec 70 dc 2a 6d a9 c5 6c 1d 6a f3 fc be c7 34 8f 57 b1 70 bb c1 5e 93 49 30 76 70 f0 29 8e 6b 9b a6 53 40 f6 49 4d 0d f6 54 03 0d 92 bb bb 13 95 e4 42 df 10 a4 3b 07 04 2d 53 2d 2d c8 42 1c 23 00 a2 ee 87 74 1f 3b 60 a0 f2 e1 8c 15 aa 44 f5 47 c5 79 82 8b 88 cf 42 89 2d c8 ea a0 b4 f8 82 a0 0c 46 15 3d 2d 6c 0c a3 10 9c 19 51 ae 69 0a ee df 53 5c 36 70 57 94 eb d9 5c 53 bd a0 3f da 52 39 1f 79 bd 41 57 bc ba 35 a8 f1 3b 6f e6 b7 7f 94 fd 0a 8a de ae b0 08 5a 1c e0 08 08 87 1c c6 53 9a e7 00 71 21 16 12 01 91 21 16 6a c8 28 89 d9 c9 c3 1b ac 11 3a 91 d2 73 28 e9 39 dd 43 63 50 0b b9 ed 2d 4d 10 40 90 8b 80 3e cc 82 8b 83 76 18 42 46 fb 22 ec c2 6e 70 51 9d 89 4d 69 0b bc b1 0a bd 3d 4d d6 37 1b ab fa 04 82 46 c5 Data Ascii: WTZ=.%b*1p*mlj4Wp^l0vp)kS@IMTB;-S--B#t;`DGyB-F=-lQiS\6pW\S?R9yAW5;oZSq!!j(:s(9CcP-M@>vB F"npQMi=M7F
2021-09-15 12:02:48 UTC	233	IN	Data Raw: 46 ac f9 f7 55 6e 9c 3b 94 04 37 cd ee ec f4 a7 fd d9 47 ff 00 92 3f ca 57 03 6b 5f c5 ad c3 a0 80 1f 83 fd 92 a0 88 28 6e 89 ca 65 c3 da dd 13 2d 94 d7 07 6c 9e dd 42 13 06 90 02 a8 72 87 d6 8e dc 2a fb b3 e3 d8 ea ad a2 ca 95 9c 25 b4 d8 e7 9f 73 44 a7 3e ad 7a 8e 79 97 55 ac f2 71 b9 73 8a e1 d6 6d e1 d6 74 2d b1 af da a8 47 57 9d fb 3d 22 a7 cc e1 15 4f e6 de d7 7f 05 c0 dc 07 16 b5 27 68 7f f9 0a 1d 90 b0 15 37 e8 2b 9c d7 37 01 6b 83 94 e3 25 30 f8 a9 08 19 ec 8f ad 5a 3b a8 90 42 a9 48 57 a3 5a 8b a4 36 a3 0b 09 1d 25 70 de 03 43 87 d7 e7 d4 af ce 7b 7d 81 a6 00 3e 28 38 ba a8 3d 95 29 d3 ad 4a a5 2a 82 59 51 a5 a7 e2 b8 77 a3 f4 ec 2e c5 c3 ee 39 81 80 e8 6e 98 dc 46 7b 49 40 a9 ca 92 32 0a 92 54 94 1c 83 a5 34 c2 95 ad 07 76 ea 09 cf 00 63 75 51 Data Ascii: FUn;7G?Wk_(ne-lBr*%sD>zyUqsmt-GW="O'h7+7k%0Z;BHWZ6%pC{}>(8=)J*YQw.9nF{I@2T4vcuQ
2021-09-15 12:02:48 UTC	235	IN	Data Raw: c6 08 32 8c 8e e9 f4 57 89 ca 50 cc 66 1a ef 45 08 1a c1 b1 4c 84 0e 37 21 3d 9f 22 89 c6 86 07 02 0f 82 71 c6 80 08 83 29 ef c6 b4 34 88 32 8b f1 a0 0b 34 c8 45 d8 d0 e0 20 47 35 a9 8c 0f cb 0d 4d 76 34 b8 88 01 35 f8 c2 1d 2d 02 13 6a 63 1c 1c 72 5c 23 53 17 94 1d 30 8d 4c 58 68 39 01 9d c2 2f c5 02 d8 a6 3c e5 07 e2 b3 46 41 1c e5 36 a6 2c 92 0b 23 e6 85 5c 59 07 f2 c5 b8 2d 4c 5e 59 14 c6 f7 08 d5 c4 b6 3b 02 eb 3e 2b 37 e9 8f 34 1f 8a 39 a5 80 21 53 16 5b 3a 61 1a 98 a0 1b f9 60 a2 fc 54 81 90 42 0f c5 49 19 40 0b aa 03 dd 7f a2 ea f9 5a 43 58 e4 19 57 7d 32 85 3a dc 29 94 da 75 47 71 69 54 f8 16 9d 48 f7 7e eb 4e a7 c2 3d 56 9b c8 88 1e a8 b0 fc 4c fa 91 03 e3 a7 f5 05 d8 1f cd a4 3f f9 20 fa 23 7a f4 be a5 9e 87 f5 14 7e a5 9e 80 ff 00 31 4b d5 6a Data Ascii: 2WPfEL7!="q)424E G5Mv45-jcr\#S0LXh9/<FA6,#\Y-L^Y;>+749!S[:a`TBI@ZCXW}2:)uGqiTH~N=VL? #z~1Kj
2021-09-15 12:02:48 UTC	236	IN	Data Raw: 42 9b bb a6 50 a1 48 ec d4 29 06 89 60 85 2f 37 53 53 78 08 9a 80 ec 20 a3 a8 db 4d 8a cb 51 a6 ee 0b 1a 72 e2 01 1f 08 54 5e da 75 01 cd d9 29 a1 af 6b 98 f3 2c 78 58 69 63 df 83 ab c0 cd 32 9d 4c 6c e9 46 93 78 c9 42 9b 49 b8 5a 6d 16 70 5a 6c 06 0b 56 41 31 00 a0 c1 b1 01 43 36 20 21 92 e0 c2 3c a4 29 13 04 85 9d 91 77 2d 46 91 ba d4 a6 78 dd 17 30 dc 3a e8 d4 66 eb 50 6e 11 a9 96 f0 56 a8 dc b6 c5 67 23 81 5a 8e 16 c8 83 dc 6c 5a b1 c6 6b f9 34 26 1b e5 f4 58 4a ee 23 25 8c 6d 3b ac 4d 37 57 a4 2a 36 d5 69 5c 73 21 32 af 59 a2 da ad df 67 8f 14 e6 55 26 43 c5 b8 20 d7 bb bc 01 41 ae 3d f5 94 9e f9 05 69 9f 8c ca 0c 9e f1 95 a4 0e c4 a2 c6 11 b5 c2 d3 61 1b 5d 1a 6c 37 8b ac 8d 20 10 04 a0 d6 9b c5 d1 6b 66 40 0a 1a 2e 00 5d 96 dc 45 d7 64 15 99 a3 8d Data Ascii: BPH)`/7SSx MQrT^u)k,xXic2LlFxBIZmpZlVA1C6 !<)w-Fx0:fPnVg#ZlZk4&XJ#%m;M7W*6i\s!2YgU&C A=ia]l7 kf@.]Ed

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	238	IN	Data Raw: 2a a2 3c 50 6c c0 e6 61 08 63 47 00 02 aa e3 5b 56 a7 00 21 bd 18 37 65 c4 0f 10 42 c5 89 a0 f1 e4 8d 32 d3 22 51 12 64 94 e6 c1 80 43 82 01 0a 8c a4 f9 60 f3 4c ae 1e 36 40 f4 03 d1 3f c0 c3 ed 54 78 05 00 71 52 1a e6 99 b8 2a b5 7a 95 86 46 b6 01 dc a7 b4 33 0e e6 f8 74 02 5a e0 e1 b8 32 aa 62 9f 5d 99 1a c8 e6 51 04 a7 53 19 08 41 88 d3 81 64 69 26 d3 7b 40 32 13 1d 03 b4 b3 4f 48 e8 25 03 3e ce 1a 65 f1 79 17 44 35 39 b2 65 34 80 40 55 6f 45 fe 5d 38 7f 79 de 48 38 93 16 44 4a 8e 99 28 a9 85 9d dc d0 ac 56 bf 82 15 9a 78 14 1e c2 83 d8 8b e6 d2 8b c0 17 20 20 f6 f3 4e 73 40 dd 60 6a 10 ea b2 64 39 b6 46 42 02 56 93 83 81 55 2f 42 a7 92 07 a2 91 02 64 c2 19 49 9e 3d 24 28 44 22 16 55 1d 30 b2 95 95 41 e6 8b 0a ca 56 99 59 1e 36 30 89 ae 47 be 56 a5 71 Data Ascii: *<PlacG[V!7eB2"QdC`L6@?TxqR*zF3tZ2b]QSAdi&{@2OH%>eyD59e4@UoE]8yH8DJ(Vx  Ns@`jd 9FBVU/BdI=$(D"U0AVY60GVq
2021-09-15 12:02:48 UTC	239	IN	Data Raw: ff 00 83 b9 b3 e2 13 c2 5a 55 98 dc b8 32 de 3f 73 23 0d fb fa ab 8b de 44 bc 39 12 d7 ec d0 45 09 55 c2 c4 8a 70 c8 06 37 f3 52 49 69 77 0c b7 30 db a3 32 1b 69 25 01 1d 1c 31 f5 a3 81 bd 58 cb 24 3c 2e c1 ae 51 6e 44 df 0a ae 31 15 b3 88 c0 de 41 ea 43 d8 82 b4 f0 48 78 73 30 ba b4 8d 74 7d 97 a8 c6 e0 e7 0e c8 0f aa ad 6d ed b8 9b 73 a0 24 2d da 40 b2 c0 62 98 24 8c 32 19 94 ee 33 e9 ab 39 25 8f 1e a8 a1 48 de 3c 8d 2c 09 50 32 1f 63 de 99 2c ac b8 69 92 4b 97 0b 21 e6 ca 98 8d 57 04 12 75 6d 53 cc 9a 11 9e 49 82 1d 52 69 19 0a d1 b3 02 b9 1b 53 10 ca 4e cb 9a 48 a5 e5 c9 28 69 18 e3 0a ba 86 4a e4 e4 f4 ab 22 d2 ab 4c a2 4c 8b 97 08 37 e4 96 04 2e 09 dc 77 c5 70 ee 17 15 d0 36 76 e9 04 12 47 24 f7 89 87 06 49 30 40 5d 44 a9 ab bb 6b 9d 0d 6c b1 a4 c2 Data Ascii: ZU2?s#D9EUp7Rliw02i%1X$<.QnD1ACHxs0t}ms$-@b$239%H<,P2c,iK!WumSIRiSNH(iJ"LL7.wp6vG$l0@]Dk l
2021-09-15 12:02:48 UTC	240	IN	Data Raw: 00 c0 dd c9 15 c3 80 66 1c a9 23 2e 46 0f f1 e5 40 5a e1 c6 ea ea 19 a3 8a 7e 7f a2 17 31 13 1b 12 b9 d8 b5 4a d1 1b 8e 70 b6 4b ad 69 3b cd 9d 65 34 ec 1b 7a 9e e0 c7 1c ab cd 32 f3 8c 61 88 db 51 35 2e cd a4 91 be c7 be d5 7a ea 30 9a b9 65 87 f9 0a e2 5b e4 b3 7c 33 b6 77 27 73 57 47 2a 74 ca 88 e4 21 72 3b ae d9 ab c8 50 ca b9 b8 64 1a 63 cf a9 9c ac 98 0e 71 db 35 fb 33 3d cf 0d 31 cb fe d1 92 dd 91 61 49 57 10 c0 46 9c 3c 47 a3 90 0e 83 56 ac 78 65 c3 94 36 17 09 19 87 59 c0 e4 96 23 29 b7 4a bb 4b c7 b1 32 c1 79 04 73 4f 67 24 d1 1c 38 b8 8e 21 ae 2e 99 1f 30 a8 a2 96 e6 09 ad c2 4c 0b 87 2c cf 1a 18 49 5c 73 4b 20 65 43 82 29 4d f2 dc a5 fc 5c 46 69 66 b7 58 a2 8e 33 cf b6 11 f5 33 c1 2e 5b 4e fa ea 66 b3 e3 5c 35 ae 2c e5 9a 21 0c 92 28 20 98 e4 Data Ascii: f#.F@Z~1JpKi;e4z2aQ5.z0e[|3w'sWG*t!r;Pdcq53=1aIWF<GVxe6Y#)JK2ysOg$8!.0L,I\sK eC)M\FifX33.[Nf\5,!(
2021-09-15 12:02:48 UTC	242	IN	Data Raw: b6 d1 1c 45 3b 82 09 c0 74 a8 6e 67 dd 2e ed c5 ba 6a 89 fb 32 f9 43 56 77 8d a7 f7 9d 70 a0 92 07 ee 1b 5e ec 3c 1a b4 ba b1 23 32 3f 25 07 20 fd f0 63 27 66 fa 6c 6a dd b8 78 c3 35 f4 36 ca 10 c5 dc 3a 67 a8 3f 74 d7 0e 86 c8 67 95 7d 1d ba 32 b3 7d c6 01 4e a1 5c 32 12 53 16 d2 bc 09 22 ce fe ec a4 e0 37 9a b2 82 e0 61 ac e0 b8 85 48 93 1f 34 6a 49 f4 9f 00 ed 56 0b 7c e7 d7 60 62 55 d6 9d 15 c1 2d a4 95 ab 17 e2 00 91 34 28 81 1a 1d 5d c1 2d 86 46 1b 1a b0 9e 06 55 f8 80 63 d3 25 b4 9f 79 58 6a dc 0e c4 57 0e 9f 87 03 f6 97 c2 3f 58 1d c3 46 1c 1d 40 d7 0f 82 c1 75 8b 79 f0 64 8c 9d c8 d9 5b 50 43 ef b8 ab 1b 59 58 e6 38 24 04 c7 74 e3 c3 e4 80 70 70 2a cd 78 90 d5 9b 50 08 7e 51 f0 4b 61 bd c5 5a 4b 36 a5 e6 84 57 d7 69 37 92 32 72 be 0d 59 4b 62 53 Data Ascii: E;tng.j2CVwp^<#2?% c'fljx56:g?tg}2}N\2S"7aH4jIV|`bU-4(}-FUc%yXjW?XF@uyd[PCYX8$tpp*xP~QKa ZK6Wi72rYKbS
2021-09-15 12:02:48 UTC	243	IN	Data Raw: 66 d1 df dc 55 bd bf 1b b4 cb 3c 21 95 4b 69 3d 71 dc 1a b6 b7 e3 36 c7 54 d0 6a 55 2f d8 e4 77 06 ad a2 e2 36 bf de ad b5 80 0f 90 7c e6 ad 03 c5 b5 ed 91 70 01 1d f6 fd 08 ab 79 2c 25 22 3b db 26 60 00 c6 d9 00 d4 17 3c 16 ed 87 3e d8 91 ae 26 3d d5 1b 7c d4 17 7c 0e f5 b5 22 7c d2 5b 3b 7f 21 f5 0a 8a ef 86 cf 9f 85 92 30 65 92 16 6e c4 2e 58 54 73 26 7f 73 bd 88 f3 0a 0e c1 ca e7 48 1e 4d 42 9c 46 d3 d7 07 10 4f 5c 64 27 cb ad d7 21 7f 1a 5b 4e 2d 61 8c dd a8 22 de 7c 76 32 0f 4e 4f 8a 36 77 b1 9e 5c f1 c8 85 21 bb 1d f9 64 ec d5 32 2d cf a6 eb 87 4b 0b 21 97 b6 a8 c7 7f 63 57 13 58 df 80 65 e1 af 11 12 c6 64 1f 32 83 b5 5e df 70 db 9f 96 2e 49 13 5a 13 fe 3c 74 3d 85 5f 5c c3 6c 0b da df 24 2c b2 c5 a7 75 05 1b 0e c4 7b 0a be 8e fb 87 31 f8 7e 21 1c Data Ascii: fU<!Ki=q6TjU/w6|py,%";&`<>&=||"|[;!0en.XTs&sHMBFO\d'![N-a"|v2NO6w\!d2-K!cWXed2^p.IZ<t=_|$,u{1~!
2021-09-15 12:02:48 UTC	244	IN	Data Raw: f6 f1 c3 14 53 90 40 49 51 06 ea d4 b1 71 8b 31 ab 91 23 17 b7 95 47 46 8d 1f 2a 01 f6 a2 9c 56 d4 69 b8 b4 9d da 5c 81 b3 68 d6 49 00 d4 52 ae 71 7d 62 e3 5b 7f f2 df 6e a2 a1 ba e1 12 7f 7a b5 20 33 c0 c7 ab 0e e0 8a b7 be e0 53 10 15 f4 86 7b 46 3d c1 1b 8a b5 9b 87 ca a4 d8 f1 31 a4 b4 3f ca 5c 7d da b4 b7 98 a0 36 dc 50 15 8c 4d 17 5c 33 f7 35 75 6d 3e ce 8c ab ad 48 07 66 0c 9a a8 0b cb 64 0b 72 ab fc bb eb fc 3a fd 2a e7 e3 60 3b 49 06 19 76 f2 76 d3 57 03 88 c1 86 17 36 b2 2b c5 80 7a 48 4e 92 0f 72 31 4c 2f e2 c1 37 36 d3 23 41 9f e6 ce 1c 7b 8c 52 0b c8 11 75 dd c1 32 98 08 ee 18 1c 3e dd f6 a8 d2 e6 3c 13 77 14 c1 a0 f7 ca 1f 5e 07 82 2a d2 29 a3 03 5d dc 32 eb 89 81 1b e6 23 ea c7 b1 ab 18 9d 00 d7 77 0b 97 47 51 d7 30 9f d0 9a b1 b7 5c 03 2d Data Ascii: S@IQq1#GF*Vi\hIRq}b[nz 3S{F=1?\}6PM\35um>Hfdr:*`;IvvW6+zHNr1L/76#A{Ru2><w^*)]2#wGQ0\-
2021-09-15 12:02:48 UTC	246	IN	Data Raw: 12 96 23 34 0d cc 63 4c b0 cc cd 3e 3c a6 25 2d b1 a8 52 50 9a 6e 6d 88 d6 18 63 05 08 6c ec 6a de 27 55 d3 73 6c 23 1a 5c 60 82 8e bd c1 15 6d 09 40 45 d5 9a c6 02 38 ee ac 95 12 18 f1 f1 16 aa 80 29 07 72 ac 95 10 68 ff 00 bc da 80 3a 1d c8 2b 51 ea 8d 71 77 6c 08 d8 1e a1 94 54 4c 62 c2 de da ab 0c 81 dc 30 15 6e ea b8 4b cb 7d 60 1c 77 0c 2a 13 6b 3e d7 56 ae fa 4f b9 00 d4 72 d8 5e 01 ce b3 39 59 46 7b 88 ce f9 af 89 e1 b7 db 9b 40 8c 6e 20 67 f3 17 cc 28 df d8 5c 92 12 28 55 a5 9a 06 63 b8 65 1b 80 2a 7e 23 62 d9 31 cb 0c 7a da 05 f7 ab db db 34 05 e0 ba 58 8a c9 1e 37 00 23 e1 9b f0 ae 21 2a da 6f 6d 77 14 64 dc a9 07 03 ec 7e 72 05 5e 8b cb 2d 26 0b a8 70 d2 b8 1b e6 58 f6 29 57 0b c5 ad 9f fb 5b 66 46 03 b6 25 07 05 73 4a 97 aa 02 dc 4f 0c a1 a0 Data Ascii: #4cL><%-RPnmclj'Usl#\`m@E8)rh:+QqwlTLb0nK}`w*k>VOr^9YF{@n g(\(Uce*~#b1z4X7#!*omwd~r^-&pX)W[fF%sJO
2021-09-15 12:02:48 UTC	247	IN	Data Raw: e7 f6 7c e5 ef 96 db 7c 53 76 1b 13 44 63 a8 df d3 47 24 6f 93 f3 6d db 2b 5a bf 67 bf 68 99 42 30 75 43 69 7b b6 87 5f 05 c8 14 05 e7 0f 97 f7 6b 85 26 1f 8a b7 7d e3 97 d3 8c e4 51 6b 5b b1 a6 32 dd 56 4f fc 9f d6 a2 92 0d 7d 5a 30 c0 6a e8 e3 3e 45 2c 9c 36 76 dc 69 0d cb f7 19 ae 6f 0b ba 3e b5 51 90 33 d1 85 2c bc 32 e7 79 02 36 40 07 a3 0a 8a 6e 19 70 7e d7 4c 80 81 ee 2a 09 f8 5d c1 fb 65 12 0d bd c0 ec 6a 29 2c ee 30 66 b7 07 0f bf 4c 27 50 6b 98 97 1a 79 b6 45 0a 4d be e3 d0 77 06 ae 25 f8 8c 73 ec 0c 45 24 c9 df a1 d8 1a bc 61 70 07 3e d2 48 f9 6a 09 c1 ce b3 e9 ef d4 1a ba 30 dc 10 25 82 61 c9 8b 3d c8 73 b7 d0 8a 99 2d 2e b0 66 8e ed b9 71 0c 9c 65 59 75 6f 4b 05 85 c9 cb c5 77 28 0a 49 ff 00 db 31 ea 15 05 b5 84 e4 e9 b5 ba 93 50 66 3d 95 d3 Data Ascii: ||SvDcG$om+ZghB0uCi{_k&}Qk[2VO}Z0j>E,6vio>Q3,2y6@np~L*]ej),0fL'PkyEMw%sE$ap>Hj0%a=s-.fqe YuoKw(l1Pf=
2021-09-15 12:02:48 UTC	248	IN	Data Raw: d0 7e a6 bf 3a c6 4d 31 23 b6 4e df 4a 27 3f 43 db b6 45 0c e3 6d 87 f9 d1 c0 e9 d7 6a 77 80 7d 8d fc 00 ff 00 6f 6c e4 6a fc 57 aa d7 07 7e 19 c5 2e 79 e6 14 bb 8d 5e ce 67 1a 98 15 3d 14 f6 15 c3 0b 8e 85 27 88 b0 c7 8d 02 ae 67 00 9c 38 99 88 38 ef 5c 55 dc f5 45 8d e4 d3 9e d9 72 2b 8d cf f5 8d 13 f5 63 5c 46 4f 76 ba 54 cf d4 05 35 17 6c 73 6e 9d ff 00 4c 57 0a 5f f1 2c 8f fa b5 70 a8 87 85 b4 56 ff 00 5e aa 8a 31 81 fd 9d ac 29 fa 2d 5e 7f cb 21 8f fd 35 c4 25 f6 e7 48 d5 7b 2f b9 47 6a 93 88 5f c8 8a cf 0e b6 48 21 6f 00 21 05 ab 84 c4 40 03 52 da 44 1b f1 38 ae 15 2f 8e 65 a4 4f fa 83 49 c3 ef 61 9a 00 9c 96 d1 1c bc c9 02 15 31 f4 e8 49 da b8 6a 6a 40 dd 41 eb b8 ef 9a 47 6f 11 42 c6 a5 e9 b6 47 fe 0d 69 73 f7 9c e0 7f 98 a8 d8 7d dc 32 d7 6d f6 Data Ascii: ~:M1#NJ'?CEmjw}oljW~.y^g='g88\UEr+c\FOvT5lsnLW_,pV^1)-^!5%H{/Gj_H!o!@RD8/eOIa1ljj@AGoBGis}2m

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	250	IN	Data Raw: 24 2c 20 31 d2 03 86 fa f7 a0 14 0e a7 ae f4 1c e9 21 81 03 14 b9 89 04 60 a7 a7 03 3a b7 14 f1 09 4a 93 1f 58 c9 1d 3a 77 14 a7 1a c8 20 6f 91 be 4d 5b 84 6c ee 5b 71 f8 54 8c e2 40 23 10 e0 ab 01 e7 3e 6a e4 46 c3 20 03 a8 05 23 04 0a 91 ec 21 b8 69 42 05 00 87 3b 31 cf 5a e6 09 10 8c a6 e3 71 a8 a9 e8 73 45 52 32 36 6d b2 31 d7 15 3c 48 ad f6 4f ac 84 04 1c e0 96 da a0 32 5e 70 72 ba 90 85 59 4a e3 60 b8 1b e6 a0 8a 6e 72 15 04 16 4d 0a 37 07 a1 ac 47 02 c7 aa 31 18 c3 b2 fb f5 15 04 91 ac a5 c2 b1 08 70 4e 71 9a 30 bb 59 c4 57 d6 b2 03 a6 40 7d 25 4d 49 a5 71 93 a4 90 33 e4 d6 d9 c6 6b 95 1f 2a 20 5f dc b5 19 6c de 73 c9 25 b7 43 11 3a d5 7f 94 93 43 65 34 68 86 65 c2 37 60 4d 7a c6 c7 41 c6 7e 94 ee 0a 85 24 f5 c0 ef 4d 94 0c 36 cf 8c d0 03 48 3b 79 Data Ascii: $, 1!`:JX:w oM[l[qT@#>jF #!iB;1ZqsER26m1<HO2^prYJ`nrM7G1pNq0YW@}%MIq3k* _ls%C:Ce4he7`MzA ~$M6H;y

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49816	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	209	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2F824258cd-2488-4e7c-b171-dad87f56f610_1000x600.jpeg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-09-15 12:02:48 UTC	250	IN	HTTP/1.1 200 OK Connection: close Content-Length: 16421 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 60277020389957980598597953116226675236 0,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "d2c20bf7706c810f628219875d8fd66e" last-modified: Thu, 09 Sep 2021 10:09:46 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-request-id: 8f8b2bee81a4ace00bdbca0cc35fc00b x-envoy-upstream-service-time: 22 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb802 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 523236 X-Served-By: cache-wdc5545-WDC, cache-dca17757-DCA, cache-hhn4038-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1631707368.304877,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2Fimages%2F824258cd-2488-4e7c-b171-dad87f56f610_1000x600.jpeg X-vcl-time-ms: 1
2021-09-15 12:02:48 UTC	251	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 05 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 01 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 36 00 00 02 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 05 06 04 07 00 02 03 08 01 09 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 03 04 01 02 05 00 06 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 41 0a 58 44 58 bb 12 cb 26 82 8c 92 Data Ascii: JFIF+""+2*(*2<66<LHLdd+""+2*(*2<66<LHLdd7"6AXDX&
2021-09-15 12:02:48 UTC	253	IN	Data Raw: a1 20 83 d1 0c 5a 0b 60 ef 69 ab 36 26 dd 05 55 a6 60 17 6b 81 cb 1c 39 05 55 f7 30 1e 6b 99 bf c8 a4 38 c4 f5 ad 43 ac 3b 80 25 7d 0e f3 0e 1e ef 91 21 03 57 cb 0e 1e e4 64 f7 55 55 ff 00 14 3f 2d ef d9 21 05 c8 6a 5d a7 e5 df 4f 9f 2d e9 19 d6 b8 1d 46 21 3c d6 04 76 ec de 6f 32 55 61 69 b5 46 b4 db 6d 7a 56 9f 34 fb 9d 5d 2a 7b 33 ce 2f e5 fe aa 40 61 40 d4 f3 bb 19 17 d3 b8 91 00 1d fb bc ad 1f 49 1e 5f e8 3c 56 5c eb 43 a7 56 7e 8e 52 77 61 f2 c6 a0 32 2f a7 af 0e b3 b1 eb b2 16 fa dd 7e 78 e8 2d 74 a7 4b 42 be df 3a 75 7e 74 f9 56 99 65 40 8b ff 00 76 7c e7 ea 1c 4f cc 5e 77 07 ea fc cf c9 5e bd df a8 ff 00 3f 3f f2 97 b9 06 66 79 bf 6e 5a db cc 63 9c 13 33 16 51 2f 6c cb b7 88 d9 8c 0a c5 8f 98 bd a1 cc cc 98 e0 0f 32 c2 ac 2a 3c cd df 33 1f e6 61 Data Ascii: Z`i6&U`k9U0k8C;%}!WdUU?-!j]O-F!<vo2UaiFmzV4]*{3/@a@I_<V\CV~Rwa2/~x-tKB:u~tVe@v|O^w^??fy nZc3Q/l2*<3a

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	254	IN	Data Raw: e4 9f bf eb 0e 76 53 ef da 75 ca 1e c3 67 f1 46 06 55 24 c4 cd 8a 06 b1 2c 35 93 9d 56 08 29 63 b5 84 5c 4a 0f d9 f4 ec 6d 68 8b bb a2 c4 12 fe 98 f4 9a d3 f7 7d f9 36 af ae 95 fa be 0c f6 e5 d2 ee ed 14 7f 05 30 fd f2 2f 94 fc f6 a1 ec 50 5b 00 c7 20 9b df f7 79 56 0c 47 3d c7 3d ff 00 83 c4 70 3c 02 11 c1 3c 5f 5f 1c 71 ea 7e c4 cb fe dc d1 1e 22 60 79 43 ef b5 e6 fd 4f 22 3d 84 91 5b 72 b4 b2 e7 76 2a a9 cc 39 64 7e ff 00 9b 3c 0d 69 dd fb 7c d3 03 ab 39 b1 b3 a3 3b f0 7e 38 eb 09 f2 db 5a 94 66 64 3e 44 ba 95 ae 51 c7 ca a1 56 95 8c e3 3c 51 c1 3c 9d c7 44 ea 5d 83 af 67 a6 26 54 18 38 50 54 f5 dc d9 b5 6e 6f 40 93 dd 71 24 91 aa bb fc ca bf 3e 6a 66 50 b0 c4 d7 35 23 d8 cd 65 31 58 af 63 d9 15 89 13 03 fd cb 79 5e 5a bc 95 22 f7 61 2f 6e be 1d 92 a5 Data Ascii: vSugFU$,5V)c\Jmh}60/P[yVG==p<<__q~"`yCO"=[rv*9d~<i\|9;~8Zfd>DQV<Q<D]g&T8PTno@q$>jfP5#e1X cy^Z"a/n
2021-09-15 12:02:48 UTC	255	IN	Data Raw: 6d d3 b7 d2 90 61 6d 18 24 68 24 32 66 d6 99 ce ec 4a 58 b1 3d a2 23 56 9e 5c eb c8 6c 36 36 ef 5d d4 2f 76 2f f3 4e 01 48 c0 77 1c d7 ad f1 c8 48 03 f7 f9 e0 4e 2a 1f 1e de 60 8f c9 62 15 fd 7d c0 f1 10 1f 43 8b fc fd f1 94 48 0a 90 91 88 8f 80 10 f8 4e 12 58 fd f3 f2 c5 e7 5c 8a 19 30 f3 a6 08 e5 d8 01 0d d7 29 36 62 81 55 4b 68 23 9e 76 6a d2 dc eb 4d 5e 24 ea d9 da 55 fa f5 a4 9a bc 16 8c 31 18 8a f5 c4 34 75 e7 7b 16 0c d2 7f 48 c4 f9 df 51 14 24 b2 03 d9 15 24 8a 94 40 45 18 d9 e8 34 2c 8e 75 fd 51 b3 8d 4a d8 62 ff 00 1a 82 79 ac 82 48 83 78 99 d6 04 6f ab 1d 8e 6a f2 3c 46 a0 dc 9e 54 f6 5b 91 ea 5e 8d ff 00 65 b8 35 ed 3c 0d 2c b1 26 d5 95 60 1e 08 b6 e9 12 04 bc 8e fd 29 1c 08 6c 1f 0e cd c0 58 85 f2 08 f3 e0 0e 7e 46 d6 17 fb 4c 89 0b f4 2a 7f Data Ascii: mam$h$2fJX=#V\l66]/v/NHwHN*`b}CHNX\0)6bUKh#vjM^$U14u{HQ$$@E4,uQJbyHxoj<FT[^e5<,&`)lX~FL*
2021-09-15 12:02:48 UTC	257	IN	Data Raw: 0f 14 f9 fe fe 4f f1 e7 d4 0e 4f 20 55 3c d2 97 cf 2d 54 37 27 2a 5a 85 a8 b4 63 f9 22 4c d6 30 e5 6c 7a 88 bc cb 56 64 5e 68 c1 f3 d1 51 e3 0f 41 21 b9 52 cc ab 97 3f f4 d9 7f 4e ed a5 56 3a f2 7a 96 d6 a1 0d 98 c2 49 cc e8 63 97 46 8a c8 ff 00 8b b3 ee 59 c4 b9 ab 7d b4 e4 8d ef d8 2e 7a e7 58 cc ce cc af 7b 52 9e dd 1c e4 ae ed a7 57 7f a3 7e 3d 8d e5 81 7a ef 65 e9 99 98 f4 6c da ca 8a c2 5a 9f 66 b4 0e b9 73 38 23 d9 28 c8 b3 42 8e 0b 81 cf 2c 38 a7 fb f1 1b cf df 3e cf 2e 3b 01 e0 0b a3 c0 f3 c9 fd 96 1b 15 c0 ca 22 94 32 96 e5 30 b5 69 9a f2 9c 59 4b ab d3 94 d7 98 c9 45 18 8b 10 ad 39 a7 88 88 26 26 18 25 90 4e 1a 5a 8c 03 6b d5 8e c5 71 e8 d9 73 1f eb 39 f1 29 ca ce a9 8f 8f 93 90 a3 2a 8a e8 f6 28 62 74 a2 04 d6 a5 bf 30 ec 96 cc d2 7b 1e 68 db Data Ascii: OO U<-T7'*Zc"L0lzVd^hQA!R?NV:zIcFY}.zX{RW~=zelZfs8#(B,8>.;"20iYKE9&&%NZkqs9)*(bt0{h
2021-09-15 12:02:48 UTC	258	IN	Data Raw: 2f e9 16 30 30 ec 81 f2 e7 6b 6a fa ab 2a 33 ca ce c5 89 67 70 3e b9 13 4b f4 08 fc 87 b7 fe 4c e2 55 7f c5 22 57 e8 99 13 cd cd 17 08 9e 39 a7 3f b4 9c 6f b0 4f 37 98 8e d1 96 e3 90 c2 1e 08 5c 8b 71 07 1e 4f 2c 10 8c 3e a5 4f d3 cf 24 43 88 e4 f3 ff 00 ef fc f5 34 60 c9 a1 3d f9 cd 68 ad 76 8e d1 9d 1d a3 69 95 63 90 98 c6 97 53 13 fc 12 61 4f 07 4d a9 27 dd 52 7a 96 a3 79 5b 51 b7 5d 61 33 54 ec 50 d6 61 18 78 bb 8d 9b 4d 33 71 57 c9 e3 8f a3 e3 9d a3 7c f5 fa 49 f1 72 c3 90 25 f6 3d 5e 8c 59 5d 5b 12 98 1b 16 81 66 f1 cb 05 9d c9 e3 f8 03 9b df bf 6a b3 f3 31 c4 b9 d4 dc 1b 03 e8 f2 d1 fd e7 eb 61 3c 1a d3 2a af d0 fb e0 3e 79 fd f8 a3 d9 bc 79 ef 9d 93 fa de 9b 53 ab 27 55 d9 a9 d7 bb 6f 5e da b9 0c 1f 93 3f 19 6e 67 7c b0 77 58 34 7a 8d d2 05 3f c8 Data Ascii: /00kj*3gp>KLU"W9?oO7\qO,>O$C4`=hvicSaOM'Rzy[Q]a3TPaxM3qW\Ir%=^Y][fj1a<*>yyS'Uo^?ng|wX4z?
2021-09-15 12:02:48 UTC	259	IN	Data Raw: 0b 46 3d 4d b2 d4 cb 19 a8 be ca ad d8 87 c0 18 35 da 8e be 53 f8 9a c7 d7 68 0d 35 ea 12 a0 f6 e9 eb b8 00 4e 55 6c 19 01 bc 9b ed 16 8a 74 f5 35 ad d2 0f e6 68 55 af b1 ad 7f 13 99 70 0f a5 b5 30 31 81 ff 00 c3 29 a9 ab dc 87 91 bb 88 f5 e3 6b 01 cf b9 bb c0 ec cc 01 18 f8 0e e3 24 d4 9c ea 2c f5 c7 f1 3d 9d a9 a3 47 af d3 6a 75 1a 7f 8f 5d 4f bc d5 9d a1 88 eb 27 07 8c cb 2d b2 e7 36 58 41 62 06 70 31 d0 c0 9a e6 3a cb 85 35 1c 54 87 19 1e 27 c4 ca 2a 5a 95 51 3a 02 6a 2c 35 d2 07 9f 7e 92 b2 4b e7 31 41 b3 70 ef 0a 4f f1 2b a6 d6 20 31 51 95 0d 8f 2c c2 a5 4e 0c 33 68 51 c4 6c 00 4c b5 83 da ec 3a 2c 4f be 8a 16 b1 9f 21 80 22 ac d4 6a d6 db ac a1 79 15 81 93 f7 f1 12 8f 39 a5 3f bd ea 84 43 67 ce af fe 9b 4f e2 3b 6e 68 61 9e d1 bf 65 46 b5 3c b7 7f Data Ascii: F=M5Sh5NUlt5hUp01)k$,=Gju]O'-6XAbp1:5T'*ZQ:j,5~K1ApO+ 1Q,N3hQlL:,O!"jy9?CgO;nhaeF<
2021-09-15 12:02:48 UTC	261	IN	Data Raw: 44 ef ae 81 a9 c0 97 52 ec f5 00 ba 11 06 d4 51 ec 3e a5 8b 19 ba 7d 86 4c 49 94 ff 00 c8 f0 23 45 16 26 f0 a0 af cd c6 20 d1 07 eb a4 c5 67 79 e8 7f 41 e0 4d 1e 05 c8 fb b2 50 41 ef e4 cd 66 a1 5d 95 57 9d b7 cc 1c 9b 8a 23 1e 4d c5 e7 89 d1 22 62 c4 d9 58 28 8a 8a 8a 14 74 04 b9 71 32 13 fd c9 50 f2 65 6d 1c 47 3c c4 30 4c 80 6e 11 38 20 88 39 a9 8b 1a 63 40 14 76 2c fd 0f d7 ff c4 00 44 10 00 02 01 02 04 03 04 07 06 03 05 07 05 00 00 00 01 02 03 00 11 04 12 21 31 41 51 71 10 13 22 61 05 23 32 42 81 91 a1 14 20 52 62 b1 c1 43 72 82 30 33 34 53 b2 24 63 73 92 c2 d1 f1 06 15 83 84 b3 ff da 00 08 01 01 00 0a 3f 00 2d 61 7b 16 b9 35 b5 58 36 70 7e 0b 7a 97 22 6f 66 36 1d 69 b3 18 23 7d 09 e2 35 35 8a 89 64 c5 5d dc 0f 17 76 06 ca a6 fb f3 6a 46 c4 01 77 95 Data Ascii: DRQ>}LI#E& gyAMPAf]W#M"bX(tq2PemG<0Ln8 9c@v,D!1AQq"a#2B RbCr034S$cs?-a{5X6p~z"of6i#}55d] vjFw
2021-09-15 12:02:48 UTC	262	IN	Data Raw: 32 e1 c6 72 07 17 20 85 1f 33 4c 51 54 c2 18 e9 7f c4 47 5d af 4c 35 bc b2 a7 88 9f 2f 21 a5 85 3c b8 b9 2e 88 15 6e 73 91 ab 1f ca a3 99 a3 8a f4 83 31 25 cd c9 ce 77 b0 04 5c f9 fc a8 cb e0 0a cd 10 bb 9b 6e 12 dc cf 1a 18 38 d5 48 53 7b b8 53 bf 42 dc 4d 1b 9a d4 8b 7f 62 72 b4 65 0a 83 6c e0 9d bc aa ce d7 0e a7 62 d7 b5 c7 50 6a ec 87 28 eb 51 c8 b1 8b b2 b5 f5 b5 41 9f 15 22 22 6a db b9 b0 e3 50 4c d8 79 84 4c e9 29 5b b5 24 52 05 44 31 a9 2d 60 16 81 bc 53 e8 37 1e 0a 2a 19 95 57 cc 9e 9b 01 c4 d1 fb 1e 1b 08 ef 1e 61 6c d2 c8 d9 55 d8 6b a8 03 7a c8 f6 f6 fc ed a9 e3 4e 31 f8 b5 12 33 cc b7 5c 32 7e 29 35 df 90 a6 b1 f0 cf 89 7b f7 ae 4e b9 05 b6 bf e1 1a 9e 35 16 1b 08 ca 32 2b a7 89 f5 d1 9b af 2a c6 62 e6 51 66 58 13 40 7c f2 03 6a 97 99 19 db Data Ascii: 2r 3LQTG]L5/!<.ns1%w\n8HS{SBMbrelbPj(QA""jPLyL)[$RD1-`S7*WalUkzN13\2~)5{N52+*bQfX@|j
2021-09-15 12:02:48 UTC	263	IN	Data Raw: d5 19 92 48 8a ad e4 02 b0 5d 3e d1 4e 1f 07 88 c9 28 12 b3 44 4d 81 1b d1 b8 0f bf 5a 19 b3 46 b7 f8 da b2 c9 0c bd e2 30 e0 d7 5b 1a 2e 98 ac 2c 18 a4 7c d9 81 0e b6 23 a8 3d 80 00 34 ec d0 8a 15 66 70 4b b9 d9 51 77 6a 92 47 ca 33 c8 d4 2e 45 5e f4 32 df b7 4e db 3e 2b 18 ba 79 25 7f 08 1e 99 8e 63 5a 14 5b 1e 76 4a 65 cf 73 b7 10 2d 44 05 52 48 c8 38 54 3d c4 82 e8 64 9d 55 88 f3 01 0d 62 11 23 c5 12 01 95 5f 51 d1 01 26 89 ce 56 e3 80 02 f6 d4 d5 b3 30 36 f3 26 ad 77 51 d7 c4 2b 3c 23 08 d8 8c 27 e4 19 c6 65 14 c2 fa 56 dd b7 ab 4b 2c 2a b1 37 30 a6 ec 2a 48 f0 b2 10 a9 89 57 ba ab 1d b3 2d 10 51 ac 45 64 69 5f 2c 6a 11 9c 9f 33 94 1b 0a 0c 18 0c a4 73 34 43 2e 87 ee 79 55 e1 c3 4a 90 2f 2b 44 73 c8 d5 66 94 0b 79 02 2c 05 6a 63 95 bc ac 00 1f bd 4d Data Ascii: H]>N(DMZF0[.,|#=4fpKQwjG3.E^2N>+y%cZ[vJes-DRH8T=dUb#_Q&V06&wQ+<#'eVK,*70*HW-QEdi_,j3s4C. yUJ/+Dsfy,jcM
2021-09-15 12:02:48 UTC	265	IN	Data Raw: 87 17 18 0e 50 c4 34 e4 37 b5 ea 48 64 32 a3 46 65 11 86 7e 24 ea 49 b7 33 59 d1 18 38 1c b9 10 38 8e 75 68 a7 8d c1 00 6e 4d ce 5f e9 6a f5 b2 82 f6 36 07 3a 9c da 8e 15 80 c0 c1 26 36 c8 26 2c cf 70 35 39 14 6d 51 e2 55 1d 54 4b 18 60 a4 36 97 b3 51 0d 1b 06 00 f1 47 d6 b4 e3 5e 13 da 7b 2c 3b 6f 73 57 64 42 c0 1d 3c 5b 28 a0 61 c2 61 98 a9 6d df 29 d5 bf a9 c8 14 6f 88 67 c4 4a 76 63 98 ff 00 a9 8e 95 63 f6 6c 3a 85 cd cc 29 b0 a0 18 44 a4 69 6d 49 b1 f9 11 57 06 5b a5 85 b4 dd 40 a7 12 94 72 c9 f6 45 91 63 03 4d 48 d4 83 5e 81 f4 ac 6c 01 31 e1 55 44 e9 7e 68 e0 57 79 8c 56 06 5c 4b 19 0b f9 08 f3 1b 21 a2 98 58 8b 44 a9 23 47 24 b1 e6 1a a2 71 39 b6 b0 e7 4e 88 24 f5 6b 6b d9 00 b0 27 ca c3 5a 38 79 d3 d6 24 a3 44 36 16 bb 65 1f 32 28 88 99 cb c7 32 Data Ascii: P47Hd2Fe~$I3Y88uhnM_j6:&6&,p59mQUTK`6QG^{,;osWdB<[(aam)ogJvccl:)DimIW[@rEcMH^l1UD~hWyV\K !XD#G$q9N$kk'Z8y$D6e2(2

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	267	IN	Data Raw: ff 00 07 85 c6 4a e3 ac 26 20 7e 72 50 00 02 cc c4 d8 00 35 24 9a c2 bc 0f 85 9f 14 b2 67 ca 3b 8c 3b f7 72 48 6f b2 2b 68 4d 61 58 32 ca c2 d2 a9 ba c0 d9 24 23 5d 90 e8 dc 8d 13 e8 cc 16 17 be 94 a4 2f 24 b2 0c ba 77 61 77 cc c6 cb 51 e0 f1 d3 7a 56 78 92 39 a3 99 52 1c 24 58 65 9b 3c a7 8b e7 70 97 1a 13 45 d9 98 3e 2f 14 da 34 d2 f1 3e 42 8b 02 6c 05 5a 49 0e 77 f2 bf 0e dd 46 2a 37 f8 15 a1 72 6d 46 d7 e1 59 56 68 c8 bf 22 35 06 bd 74 13 10 7c c1 d4 30 f2 3f 70 bc b2 35 91 47 13 59 e1 84 86 95 c5 d4 cf 27 05 1c 40 e5 e5 57 66 6c cd 6d 07 90 03 80 1b 01 c0 76 5e 57 f0 20 e6 c6 83 68 33 37 13 af ee 6b a8 35 a4 7e 8a 58 c1 ff 00 8d 2a 9f fa 2b 17 8f 9e 74 76 fb 34 22 51 19 8a 11 99 ce 21 a1 f1 08 b8 10 08 2d 4b 89 4f 47 cb 86 76 9b 1b 3a a2 c7 14 85 71 Data Ascii: J& ~rP5$g;;rHo+hMaX2$#]/$wawQzVx9R$Xe<pE>/4>BlZIwF*7rmFYVh"5t|0?p5GY'@Wflmv^W h37k5~X*+t v4"Q!-KOGv:q

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49815	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	209	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F7b4dbad0520957f16bd4e3f810f4c883.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-09-15 12:02:48 UTC	268	IN	HTTP/1.1 200 OK Connection: close Content-Length: 13955 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 588984576483381141123321612983958044313,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "e150f5dfc8febf67abe61c2494132036" last-modified: Sun, 11 Jul 2021 19:47:35 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-request-id: a91cbb646184bb40ad14786d0674b8e5 x-envoy-upstream-service-time: 12 X-backend-name: US_DIR:3FP7YNX3LMizprTZsG7BSW--F_US_nlb105 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 3024004 X-Served-By: cache-wdc5559-WDC, cache-dca17721-DCA, cache-hhn4053-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 2 X-Timer: S1631707368.311951,VS0,VE0 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F7b4dbad0520957f16bd4e3f810f4c883.png X-vcl-time-ms: 0
2021-09-15 12:02:48 UTC	269	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 15 0e 0c 0b 0b 0c 19 12 13 0f 15 1e 1b 20 1f 1e 1b 1d 1d 21 25 30 29 21 23 2d 24 1d 1d 2a 39 2a 2d 31 33 36 36 36 20 28 3b 3f 3a 34 3e 30 35 36 33 ff db 00 43 01 0f 10 10 15 12 15 29 17 17 29 57 3a 31 3a 57 57 57

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	273	IN	Data Raw: 53 c3 b2 76 27 d1 92 84 32 1e 5a 04 d7 45 18 fd b5 29 23 90 a0 75 31 58 65 54 e3 68 fd f3 31 c5 00 36 52 88 49 cf 2a 95 1d 14 18 c9 ee 4f 47 07 d4 32 70 0a 7b cb 0b c3 12 30 00 39 03 2f bf 65 29 4e 55 8f e6 f6 8c 83 24 8a 55 d7 88 73 5b e7 2d e0 b0 f7 a6 8e ac 91 d5 9b 09 e3 3b b9 c5 fb e0 ce 39 19 d5 9d 30 7a a3 a6 ac eb 96 7e 8f b7 be b9 b7 13 75 06 96 c5 75 2b dc 45 8f a3 90 b8 d2 76 82 cc 74 ac 0c 6f 3c 8b bf 94 d9 b0 ef c6 c9 3b 24 e4 16 7e d7 e7 b7 55 28 63 c0 31 8f f0 1e 20 7d e3 a7 69 3c 65 87 e1 78 c9 5b ef 92 37 19 b1 9f 94 11 03 a4 a5 1c 54 a5 70 2f 2a 7c e2 d6 8c 2a a2 94 e3 3a a6 9a 4f ab 8a 64 43 80 62 8c 51 8a 30 20 c9 e3 26 84 44 65 a6 02 0e 32 cb 81 c9 39 25 ae 58 a8 ca d3 45 16 8a 38 97 36 13 c6 b1 37 27 63 6d 65 b8 ca 98 63 e0 1e 45 69 Data Ascii: Sv'2ZE)#u1XeTh16Rl*OG2p{09/e)NU$Us[-;90z~uu+Evto<;$~U(c1 }i<ex[7Tp/*|*:OdCbQ0 &De29%XE86 7'cmecEi
2021-09-15 12:02:48 UTC	274	IN	Data Raw: 2a 59 b6 ca f5 bc 6c d2 de 8e 72 0b bb 59 42 66 44 8d 05 8d 8d df d2 8e a6 b4 07 59 ac 90 00 50 00 2d ef 80 15 3b d4 82 23 51 f6 01 bd 0c ea 69 45 fb 4d 0c 4b a2 e9 39 23 65 b5 b3 c5 40 bc 70 33 55 d2 dd 44 92 99 65 d3 eb 3a 6a f4 32 4a f6 94 69 07 60 73 6e 3d 04 1d eb df 6e de ce 3a 90 ad 7a a9 25 a9 48 12 76 9d ac 90 c7 fd 20 a7 3b d3 86 5d 8c b9 aa a4 29 d5 e0 9f 89 bd 4e 74 db ee 9a ac 8f 79 8c 76 59 91 ef e8 75 5b 1a 8e 2c eb 37 bd 19 af 82 66 15 a9 cd d3 d5 e1 e5 8d 45 d5 55 89 d9 85 60 0a f0 a0 47 c8 fe 78 38 b1 8e 3e c1 47 3e 82 f6 af bc 96 59 ae 96 86 96 6b 34 b5 35 8a 5a 35 e3 f0 03 2a ed 6d 5b 90 b4 d2 c7 2a a3 a9 6c 86 a4 71 c1 f3 73 e4 af 77 69 60 c3 5c 5a 9a 86 be 3e c1 92 cd 2d f9 c3 bb 57 8d a5 91 50 05 85 26 d9 2c 43 22 20 7b cf 8b db 67 Data Ascii: *YlrYBfDYP-;#QiEMK9#e@p3UDe:j2Ji`sn=n:z%Hv ;])NtyvYu[,7fEU`Gx8>G>Yk45Z5*m[*lqswi`\Z>-WP&,C" {g
2021-09-15 12:02:48 UTC	276	IN	Data Raw: 8d 09 6e 73 70 b2 49 ab 9a b4 59 56 b2 54 af 1d 74 c0 bc 0e 72 63 c0 3c e5 83 de e4 0c a7 17 6f 1c e0 03 8c 90 72 d8 29 cc 7f d9 15 39 87 fb 1e b4 c7 ec 8b 56 60 79 ec 15 a5 00 7d 32 d7 99 98 7d 0b 4e 76 9d 3e 8e be ab b1 b1 d5 9d 47 67 b2 2d 16 cc 28 fe 9a 2d 26 c8 1f fe b2 69 36 04 7b ac ba 4d 80 ff 00 f3 8d 2d ff 00 e6 b8 d2 ec 3d f1 5c e9 b6 0a 84 fc bf 49 e9 6c d2 e9 1d 74 6d 12 d0 b1 cf f6 d6 9c e3 fe 39 35 f6 26 d8 d2 e5 12 94 e4 fe c7 a7 37 6f 1d 93 d4 b0 7b b8 8c 6b ac 96 e7 c7 5f 5f 60 7f c6 29 ce 7f e3 4d 7c fc f3 d9 ff c4 00 29 11 00 02 02 01 05 00 02 02 02 02 03 01 00 00 00 00 00 01 02 11 10 03 12 20 21 31 30 41 04 51 22 71 13 32 14 23 61 81 ff da 00 08 01 03 01 01 3f 00 c4 b8 af 04 86 53 6b b1 a9 24 2d d5 b4 8a af 78 f8 50 fb 1f 5c df bc aa Data Ascii: nspIYVTtrc<or)9V`y}2}Nv>Gg-(-&i6{M-=\lltm95&7o{k__`)M|) !10AQ"q2#a?Sk$-xP\
2021-09-15 12:02:48 UTC	277	IN	Data Raw: fb 77 63 c9 b6 c8 96 4e e3 b9 9b fa 8f c1 e9 6f 94 77 6c 26 5f bf 8c dd 47 45 e0 de c2 db 82 a9 f2 6c cd b4 f5 f9 16 2f b1 89 fa 3f 0c af 7a f0 6e 8b 5a 6c b8 37 66 c3 db e5 ad 8e 50 9e 8d d2 b3 97 7a b7 44 78 dc ab 1b 62 5a d9 65 97 f2 2b 44 27 68 cb 2f dd f0 67 02 76 31 8c b2 cb 2f 4b 2c ee 2c b2 fc 60 f6 1b bf 07 c6 88 5b b2 43 7f b0 45 d7 8d a1 31 ec 2d 89 0f e6 2f 91 c9 46 e9 59 76 31 8f e6 af 27 c6 97 5c 8b 76 7a 8c 63 fd 8d f0 7a 6c 6e f4 7c e8 fe 6a f0 7e 0f 6e 0d 91 ce 9c 21 bb 37 f0 45 14 8a 28 af 05 e6 c7 ee b4 44 99 63 91 dd a5 8b 4d d9 52 2d fa 97 aa f9 2d 50 d8 87 b1 18 21 c6 3e 8c 92 a2 8a 12 1b f6 22 d2 1b b5 c1 2a f0 5a b6 5f 8b e0 62 1a 57 6c ef a6 7c 46 f8 18 b6 54 2d 12 45 16 f4 bd 56 8f 4f 4f 29 72 84 89 95 a2 56 4f 67 42 d6 d9 7a 56 Data Ascii: wcNowl&_GEl/?znZl7fPzDxbZe+D'h/gv1/K,,`[CE1-/FYv1'\vzczln|j~n!7E(DcMR--P!>"*Z_bWl|FT-EVO O)rVOgBzV
2021-09-15 12:02:48 UTC	278	IN	Data Raw: a2 e1 24 30 43 62 82 b2 33 34 a3 c2 f1 ff da 00 08 01 01 00 0a 3f 00 77 c5 3b e2 9e 5b b3 d1 6e cb 44 9c 8b 9e 65 d1 cc 06 8f e6 5e a8 c6 b0 53 be 28 ab 01 25 12 1c f3 00 39 3a 6d 91 25 39 e2 99 9b 3a e8 07 17 01 8a 62 c8 4b 3c 2f 0c b6 3e 1d 72 d7 8a 7b 4b 5e 5d 32 60 b8 f0 e8 0a a8 e7 d4 6b 5d 8c b8 f8 4c 5f d5 54 a5 b3 b5 a5 d5 1c d7 5f af 55 57 b3 61 86 62 79 c4 ee 70 aa c6 71 8c aa 95 28 9f 6a 9b 9c 7e 23 81 55 1c ca 8d 17 2e b8 33 92 7e 19 82 1c ef 67 f7 cd 3a 08 9f 69 3b e2 9d f1 4f f8 94 ef 8e ec 96 1d a3 6e 9d b6 a8 27 f3 c6 1f e8 0c 5d 61 1d ec 68 ec dc ef 11 81 6f d8 54 c3 49 f0 39 b6 07 a8 46 a5 46 34 bb 09 81 30 9b 46 b3 88 68 c6 e2 49 fd dd 51 71 a9 48 34 02 c9 83 13 3e a1 0c 6e 13 0c 10 3a a8 2e c2 d1 a8 b1 8b 7c 15 cd 72 c0 e2 74 50 c7 9f Data Ascii: $0Cb34?w;[nDe^S(%9:m%9:bK</>r{K^]2`k]L_T_UWabypq(j~#U.3~g:i;On']ahoTI9FF40FhIQqH4>n:.|rtP
2021-09-15 12:02:48 UTC	280	IN	Data Raw: a3 c7 88 b3 80 33 31 19 a7 31 b5 9a 19 47 68 93 80 10 df 13 5c 4d c7 8a 4d e0 df 92 6b da 2c 1e db 8c f8 ac 4f 69 6b 58 06 40 02 50 2f 3e ef d5 12 d1 c3 21 cd 17 89 b1 94 20 66 01 42 37 47 12 56 16 09 4e a8 d0 74 19 a2 c0 6f 04 41 59 e5 8b 82 0f 6f 26 c1 0a 41 cb 71 c6 35 1b 8f 25 23 81 d0 a6 da 24 77 1f 51 db 36 d0 cd a9 ac 69 bb f0 90 1c d1 cf 0d c2 75 7a 5b 59 9c 44 c3 5b 02 e1 d6 cf 2c ef 28 3e 99 b9 b4 0e 40 0f de 49 b8 be ef 8d d8 6d 04 3a 21 7e 28 36 d4 4f 34 e6 f1 0d 26 10 0e 17 96 98 2b 14 e6 1c d8 2b 0b 45 a7 9a 90 06 b6 52 84 6b 3a a9 a6 d1 26 a3 a1 a0 47 33 9f 92 a2 01 68 b8 68 70 f4 4d 23 dd 01 d6 f8 28 07 86 aa 4e ed 15 a7 45 03 8a 01 82 d0 3c ae ac 7b 92 d3 70 46 60 e8 42 a4 c3 50 87 63 a8 f2 1a e2 5d 17 19 cd f4 29 cc 7d 37 41 76 2c c7 1b Data Ascii: 311Gh\MMk,OikX@P/>! fB7GVNtoAYo&Aq5%#$wQ6iuz[YD[,(>@Im:!~(6O4&++ERk:&G3hhpM#(NE<{pF`BPc])}7Av,
2021-09-15 12:02:48 UTC	281	IN	Data Raw: f8 9f ee b0 b8 9c c6 5c c2 bb 5d 99 d4 f1 44 da 65 43 b2 89 57 40 3b 0d ce a5 58 4c 22 5a 39 a9 1a 80 6e 15 5a 63 8b a9 10 a4 0c ce 12 80 27 42 b1 34 7b c3 2d fe d3 b7 16 3a 2c e0 60 84 e3 b4 b9 ed 7e d1 4c 92 64 8b 5a 44 df e0 a9 53 a8 e9 06 9b bc 57 cc df 5d 53 6a 3d 84 e2 0d 06 23 cd 62 ad c0 09 41 f8 66 c0 67 06 ea 97 66 04 df 2e 5e 85 01 33 0f 69 f4 f9 27 3b c0 1f 19 f5 53 7c 40 b6 c0 1e 41 46 2b f9 a9 74 64 0d 82 e9 b8 0d 9d 8e 86 b4 80 61 52 75 32 40 6b 43 00 f8 a6 76 71 26 24 2a 8c d9 0b a2 94 d6 70 73 dd 37 8e 41 01 23 2c 29 be 4b 03 09 97 10 2e 84 c6 43 70 03 8c a8 20 c9 54 9c d8 c8 66 a3 aa 2c 6d 66 62 a4 0c c6 20 64 89 09 e2 ad 3a 5f 86 c0 24 5f 37 79 82 75 58 69 63 97 17 da 7e b6 8b 22 76 49 c4 d2 d1 0e 9d 1b d1 53 05 ee 3d 9c 1d 09 c8 8e 72 Data Ascii: \]DeCW@;XL"Z9nZc'B4{-:,`~LdZDSW]Sj=#bAfgf.^3i';S|@AF+tdaRu2@kCvq&$*ps7A#,)K.Cp Tf,mfb d: _$_7yuXic~"vIS=r
2021-09-15 12:02:48 UTC	282	IN	Data Raw: b2 ce d5 54 71 0c b8 1f cd 84 79 a9 2e 32 56 4a 1a c6 97 1e 81 19 ac f2 f0 0f 33 6f 4f f2 b5 dd 75 72 61 7f ea ec 6f ae f1 39 13 61 f2 2a ea 51 1b c9 dc 25 c5 9b 33 2d a7 b4 ef fe bb ac a2 a6 d0 45 16 9f e2 30 7d 25 78 69 88 1c fb fe a1 7a 85 ea 15 fa 85 ea 17 a8 56 c4 35 08 bf 15 37 52 a6 71 01 03 08 81 9a ff 00 e4 6f d5 7f 5b 7e aa ff 00 c6 df aa fe b6 fd 57 f5 b7 ea bf ad bf 55 a7 e7 6f d5 00 fa d8 f6 87 c3 86 6e 36 fe 90 10 f8 85 ea 14 36 96 3a a4 62 17 31 84 7f d8 ab 75 0b d4 2f 50 b5 fc c1 7a 85 ea 17 a8 5f ff d9 Data Ascii: Tqy.2VJ3oOurao9a*Q%3-E0}%xizV57Rqo[~WUon66:b1u/Pz_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49817	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	234	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_737%2Cy_504/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fe17134d780918219c201cb1db8da2d3f.jpeg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: img.img-taboola.com Connection: Keep-Alive
2021-09-15 12:02:48 UTC	283	IN	HTTP/1.1 200 OK Connection: close Content-Length: 16162 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 313369804364444699870713811989861120403,318552739597058339386846178970656559273,29ecf9b93bbf306179626feeda1fab70 etag: "e4216c30303b0fd3ecbe5c71e9ed5127" last-modified: Tue, 14 Sep 2021 09:02:30 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-request-id: 45f7ba688adb1cfd869c9f1f27353381 x-envoy-upstream-service-time: 9 X-backend-name: US_DIR:3FP7YNX3LMizprTZsG7BSW--F_US_nlb101 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Wed, 15 Sep 2021 12:02:48 GMT Age: 13489 X-Served-By: cache-wdc5526-WDC, cache-dca17741-DCA, cache-hhn4059-HHN X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1631707368.322501,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_737%2Cy_504/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fe17134d780918219c201cb1db8da2d3f.jpeg X-vcl-time-ms: 1
2021-09-15 12:02:48 UTC	284	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 0a 0a 0a 0a 0b 0a 0c 0d 0d 0c 10 11 0f 11 10 18 16 14 14 16 18 24 1a 1c 1a 1c 1a 24 36 22 28 22 22 28 22 36 30 3a 2f 2c 2f 3a 30 56 44 3c 3c 44 56 64 54 4f 54 64 79 6c 6c 79 98 91 98 c7 c7 ff ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 34 00 00 00 07 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 ff da 00 0c 03 01 00 00 02 10 03 10 00 00 00 f4 a6 4c 84 40 06 40 00 81 b4 24 12 04 36 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_|$$6"("""("60:/,/:0VD<<DVdTOTdylly74L@@$6
2021-09-15 12:02:48 UTC	285	IN	Data Raw: cb 2d ea d4 4d 9c 98 be a1 e7 f4 4e 23 0e 69 99 dd c5 6b a0 77 78 a3 c8 f5 f5 f2 f9 f1 a7 37 e9 d2 97 68 df e9 c9 ae 39 b7 5c dd 75 e5 e4 78 fd 1e 35 ec f8 f6 30 f6 7b 73 75 4c a3 98 de b8 c3 67 b1 86 b6 b3 42 e6 bb bf 8d d1 6f 59 f3 a5 bf 39 ed 74 da e5 d8 7a 3c 9a 1e 0f 4b b2 e2 73 b8 df 9a f4 74 d1 6a b5 7b 71 6a af 87 6d e7 7a 59 35 db 63 e3 e3 8b f5 f8 57 85 b7 f4 1c 1b 8c 55 5e 5d 15 a3 6f 12 0e d7 52 ca 5d 67 b7 79 9d 1a 27 9f 3c 9d b1 7b 6d 9d db 9f a5 75 f9 68 f3 7d 0e 97 93 e7 0e b9 bf 65 d4 dc 6d ef 0b 9d 38 fa 57 95 eb e4 5f 57 35 e9 c2 bd f0 35 d0 6c 35 e7 9d 86 db 1f 37 ae c2 57 36 da b2 dd 32 cd 66 34 cf b7 79 9a de 87 36 7a e1 fa 4a bd 32 e8 9d 5e 6a 7c df 4b ac 73 56 0d e9 cd 7a dd 0e d9 ea 74 c1 ed b8 ba 9f 95 eb 69 2f 2e 0f ad 25 67 17 Data Ascii: -MN#ikwx7h9\ux50{suLgBoY9tz<Kstj{qjmzY5cWU^]oR]gy'<{muh}em8W_W55l57W62f4y6zJ2^j|KsVzti/.%g
2021-09-15 12:02:48 UTC	286	IN	Data Raw: 61 3f 42 c7 99 e7 cc 2e 4e 0f 22 71 fe 33 bd c7 24 1c 5e 95 c8 d7 9d e9 6f 93 9e a2 32 a3 c3 62 1b f5 f5 db 49 a7 95 c9 1a 3a 94 e0 79 cd 98 a4 aa 5e c4 2e d7 2b 4d 5d 92 90 8f ce cd dd ae aa 19 4f 98 9a 4b 4f 6b 67 a8 30 29 8e dd fd 9b ed 2f 53 45 5a bb 5b 1e a1 91 ff 00 ef 5f 59 ea 3b 8e 26 89 6b a6 f2 de c1 e4 ad 34 a5 5e 85 30 9b 2b 3d 38 c7 3c b3 cc 73 3c 86 77 3c ff 00 c6 31 62 71 9f c7 0c 85 ce 34 8e a3 e0 2d 86 c4 94 13 f3 9b 0d 78 b8 82 54 88 cf 6e 66 fb 74 1b 9d 5b 37 11 2c d7 5a 71 6b 52 d5 aa 96 6e 45 62 b4 f2 9b 16 2d d2 82 74 9a 68 fd 8b 5e 76 5e fd 9b b3 45 5e a4 1a c1 2b 56 a1 e7 24 29 35 a8 74 41 52 08 e6 5d f5 9a f4 be db 53 4b 4b 04 f2 db b7 4d a1 1a 7b 55 a6 48 f7 56 7b 8c 71 8e 33 62 bf c9 e9 67 1c c4 38 ef c3 92 90 57 b8 85 06 3c ca Data Ascii: a?B.N"q3$^o2bI:y^.+M]OKOkg0)/SEZ[_Y;&k4^0+=8<s<w<1bq4-xTnft[7,ZqkRnEb-th^v^E^+V$)5tAR]SK KM{UHV{q3bg8W<
2021-09-15 12:02:48 UTC	288	IN	Data Raw: 86 55 d8 b5 39 bd e0 19 63 d9 56 49 aa d8 a9 75 66 f7 68 da 15 3a 5a cc 6c 5e 7b 1b 56 0b 4d 23 8e 3a 10 22 08 cc bf 93 d2 c1 ba 46 3a 86 c9 7c c4 fe e0 79 e7 0c 17 c7 16 47 23 99 1f c1 ca 44 fb 6f d3 2c be 3f 9c ad 71 62 96 5e e5 19 49 23 99 2d 92 11 50 9b 56 48 cd 6b f9 ce b9 a8 a8 d1 d7 89 8e 6c 98 c4 84 1c 66 92 ee c6 bd 38 97 71 04 da ad 85 ba 93 66 bb 45 1d 64 8e ce db 37 b7 12 4d 82 ac 71 ac ca 46 57 b7 25 49 0c 95 e5 7d ac db 44 58 ac ad 64 92 d5 9b a6 f0 8f 62 18 01 1d 69 98 92 4f 49 27 35 ef 42 f2 1f 6f 62 3d 3b 60 12 ff 00 7f 3d 5a 30 1e c9 b6 9b 6b e9 ca ff 00 aa 6d bc 9e ab f4 9a 8f d1 76 8d d8 6e aa cd 5d 68 90 5c ae 4f 5b cb e3 1f 47 24 df 3e f5 34 fb 68 cb 30 7b fe 6e c7 2c 4e 5d bf 3a 40 5a 55 cd 71 61 55 00 66 68 ac 23 c5 3c 56 e2 5f 4e Data Ascii: U9cVIufh:Zl^{VM#:"F:|yG#Do,?qb^!#-PVHklf8qfEd7MqFW%I}DXdbiOI'5Bob=;`=Z0kmvn]h\O[G$>4h0{n ,N]:@ZUqaUfh#<V_N
2021-09-15 12:02:48 UTC	289	IN	Data Raw: aa f3 f4 c2 e4 cb c1 93 1e 27 79 e9 3b b0 c5 75 10 57 da 59 b2 f0 3f 9c 53 58 47 24 18 e7 2a 4f c2 bb a7 9a b7 3a 33 d1 1b 0d dc 12 f2 ac d7 a5 f5 18 83 a9 9b 9d 8e ef cd e2 75 bd 25 c7 90 f9 19 9e 5f 6c 29 c8 64 51 12 8c f4 85 97 4b 4f 12 58 78 dd e2 ec ba df 51 a4 d1 49 2a a6 96 d2 48 3e 4d 57 f2 1d ca 72 88 c4 a5 89 b2 9f c8 6b 11 e1 99 72 5f 4d 7a 9a 63 d9 40 f4 87 a8 5d 41 11 1f 48 6f bf 2d 5e 2f 47 6e 03 8e c1 3f a4 6f 18 c0 64 af e9 bd e5 76 53 04 37 a6 de d9 81 62 7f 4f c9 a3 da 02 c5 a9 8f 4f dc 7e 97 8f fd ab 39 3d 61 fe d8 88 83 d1 ae d4 db a4 ea f5 ec 1d 97 a8 05 76 8b c2 ee b7 69 69 cb 3e c2 5f 4c ca df a8 ef 3f da f1 b1 e1 d8 47 e9 7d 79 e0 6d 8e af 52 9a a9 cc 88 c3 71 58 c2 12 4d 4e f6 47 bb 29 68 e9 cf a9 d8 c9 df dc 7d 06 cb a3 b3 2f a7 Data Ascii: 'y;uWY?SXG$*O:3u%_l)dQKOXxQI*H>MWrkr_Mzc@]AHo-^/Gn?odvS7bOO~9=avii>_L?G}ymRqXMNG)h}/

Timestamp	kBytes transferred	Direction	Data
2021-09-15 12:02:48 UTC	291	IN	Data Raw: b0 6c 6b 49 44 11 a2 6c 39 84 2a 6d b9 27 43 01 3d d2 e2 50 63 8e 90 88 8d b4 47 73 cc ae 3b 0a ec de cc f8 a8 5f 44 49 cb 67 6d b3 10 d9 ae c1 f2 29 c1 69 1c 0a 07 42 9c 0b 0e 21 91 45 e6 08 e2 98 c0 04 9c d6 67 92 a8 65 e7 6d 2b 30 2e 3e 3b 7b 29 96 b8 73 58 55 51 66 a1 92 ed ce 92 d0 82 39 20 8a 1f 21 a4 b4 ca b3 c4 82 b3 05 ae 4c 1d eb e8 15 dd e0 9e e0 c1 1a fc 86 88 6b 7c 11 b1 3e 3b 7b 19 ef b8 72 40 4a 7b 31 06 f1 09 a6 42 ed 27 15 57 26 84 fb 04 d6 bb 82 72 6d d4 5e 15 47 c4 37 52 98 49 04 9d 4f e1 b0 12 0c 83 09 cf 71 19 05 38 48 31 28 d7 26 c0 00 8a 95 fb bd 58 06 d0 42 dd 1c b1 1e 8b 77 50 fb a9 fd 8a b1 ef 1b 02 bf 72 79 c9 fe 8b b4 f6 77 76 77 31 ae 73 5c 5c dc 56 9b 5e 35 5d 99 d1 57 c9 35 f0 bf 79 0d f7 65 59 94 c9 e4 88 92 4a 01 55 c9 30 Data Ascii: lkIDl9*m'C=PcGs;_Dlgm)iB!Egem+0.>;{}sXUQf9 !Lk|>;{r@J{1B'W&rm^G7RIOq8H1(&XBwPrywvw1s\\V^ 5]W5yeYJU0
2021-09-15 12:02:48 UTC	292	IN	Data Raw: 40 62 72 a2 c1 06 33 43 50 53 82 93 e1 24 34 63 b1 d1 f0 83 a3 e2 ff da 00 08 01 02 01 01 3f 00 fe e7 3f df f1 fd d6 3f 55 9f b4 c4 28 24 90 00 ab 98 8b 36 82 97 78 0d b5 1c 66 15 57 31 b9 22 63 41 4d 8a c3 ae 59 b9 12 37 8a 5c 6e 10 be 4e d3 5f a6 94 97 ac dd 30 97 01 34 a5 58 4a b0 23 c0 cf ea 72 00 24 98 02 b1 58 cb 6e 99 14 90 a6 0b 1a b8 ca 6d 9b 6b 2c 41 d1 1b 48 5a 76 bb 74 da 5c 82 36 07 8c ed 02 85 ab 76 d8 87 5e fc 49 53 2c 0c 1a b9 60 47 dd a7 dd 90 a1 a0 4a d2 5a cc e6 42 e5 24 9e ee 82 2a c1 fd 19 ed 2a 17 08 ce 73 68 35 9e 26 88 20 fe 1c fd bc 67 69 95 11 4c 07 30 4c 1a 04 59 96 2a 0e b0 27 da 35 df c4 30 44 42 a3 2c 77 86 a2 3c e8 60 52 d9 66 21 cb 21 53 00 c1 1c 69 54 de 07 ba 07 13 af c6 96 d6 14 bf 60 d7 00 26 40 50 75 9a fd 1a d8 ba a6 Data Ascii: @br3CPS$4c???U($6xfW1"cAMY7\nN_04XJ#r$Xnmk,AHZvt\6v^IS,`GJZB$**sh5& giL0LY*'50DB,w<`Rf!! SiT`&@Pu
2021-09-15 12:02:48 UTC	293	IN	Data Raw: 43 2a ac 57 37 02 46 f1 42 69 d4 95 20 18 34 a8 ab d4 f2 0b 79 52 e8 a2 80 88 ac a8 66 44 93 57 61 3b a0 69 14 ae 40 da 5a 8b 34 c8 30 7c 3a ac 7b 5d 6d f6 45 5d e9 bb 18 4b af 63 15 66 e8 b8 86 09 b7 0c a7 8c ea 45 61 31 f8 1c 69 cb 62 f8 2f ee 37 75 ab a5 ee bf 47 f4 be 0f 1a 01 c8 6d 05 71 cc 03 0c 2b a6 fa 42 e7 63 87 c3 db 94 37 6c 8b b7 e3 91 d0 28 ac 16 15 b0 f8 3c 35 88 82 89 de 1c 8b 6a 6b 11 d2 98 0c 34 83 73 b4 7f 75 35 fa d6 0f 14 d8 c5 7b 9d 98 b6 8a 72 c4 c9 2d d6 fb 8e a8 a1 58 8f 68 1a 9a 1a 98 a2 20 d6 1f da eb 6f b5 fd 25 b4 53 1f 6a f7 e5 bd 64 7c 57 42 29 92 06 75 26 24 41 1b 83 58 0c 4d 9e 9a c1 b6 0f 16 7f e2 2d 6a ad c5 87 3f fc d5 8e 8c b2 6f da bd 74 97 7b 4a a8 b3 b7 dd 88 0c 6b a5 fa 5d af 3b 58 b0 f1 64 18 62 3f 3f fb 54 1b 48 Data Ascii: C*W7FBi 4yRfDWa;i@Z40|:[]mE]KcfEa1ib/7uGmq+Bc7l(<5jk4su5{r-Xh o%Sjd|WB)u&$AXM-j?ot{Jk];Xdb??TH
2021-09-15 12:02:48 UTC	295	IN	Data Raw: c7 d6 b8 55 c9 37 21 f2 fc 48 a6 58 03 97 ef d0 90 36 5f 32 d5 6d b4 de df d6 94 98 6d a7 c2 97 45 5f 2a c4 93 22 00 df 49 90 6b 39 e6 d3 e1 74 52 31 fd af 5b a2 ad e5 e6 7e 79 ad 2a d6 ef 13 c3 ab 13 6b 32 86 1b 8a 47 d2 90 0f 3f 53 51 de d8 7c 4d 2a 80 36 14 bb d3 55 d8 1a 06 8f 26 c9 43 37 bc e7 ce e8 a5 66 d3 4f e3 14 35 3c 3e 33 4b b7 55 f3 b7 b4 3c 43 45 77 e3 76 fa 52 b6 51 ec 37 cc 29 1f 4d 8f cc 28 19 26 93 d8 5a c4 ff 00 3e 71 41 5f 82 5c ff 00 4c 1a b6 86 75 46 db 8a 01 4a a7 97 d0 50 a4 dd bd 3a 85 5f b2 51 b3 2e c6 93 37 23 f3 57 7a 77 3f 35 09 ff 00 d3 34 3a af 83 a4 16 f4 01 be 86 95 2e 72 7f f4 80 a0 87 9b 7a a8 a0 3c 69 7a af a3 34 43 03 e1 13 59 48 dd 47 ca 69 52 75 ca 3e 5a 55 81 ec 7f 0d 01 04 d0 3a 0a c4 30 c8 64 1f 38 91 52 86 74 b7 Data Ascii: U7!HX6_2mmE_*'"Ik9tR1[~y*k2G?SQ|M*6U&C7fO5<>3KU<CEwvRQ7)M(&Z>qA_\LuFJP:_Q.7#Wzw?54:.rz<iz 4CYHGiRu>ZU:0d8Rt
2021-09-15 12:02:48 UTC	296	IN	Data Raw: 81 01 76 35 74 53 e3 9d ac 52 23 38 12 c8 7e 98 91 4d bf 69 03 69 f2 39 34 ba b9 27 2e a2 24 1d df 71 a0 49 51 e4 33 93 22 9d f2 3c 8a 8a 77 f4 da bc 74 e0 93 9d ac 2f 43 b1 8a 44 93 63 29 e1 95 81 0c 09 1d 6b eb 93 e5 11 f1 13 12 56 c1 20 b2 35 78 36 48 25 7e fb 3c 41 8a 34 62 4d 9b 63 25 45 57 5f 13 9d c8 d9 11 74 bb 1b 71 5b 1c 8b 1e df 8e 41 db 3c c6 34 95 77 1a 00 8a 2d e5 5c 1c 84 aa 84 47 8e 42 d1 83 47 9d cc 96 48 1d 7c 86 29 11 69 b6 68 d1 26 56 0d 14 83 d8 72 45 11 8a 27 4a 48 48 60 fd a7 80 62 7a 10 72 66 96 1d 40 59 65 76 1d db 1d e8 d4 1b 21 77 67 ca b5 20 30 5a 16 aa c4 81 d1 6b 27 66 28 8d 29 f2 e7 90 56 e8 1f 00 06 08 22 78 28 40 37 b3 b4 8c 48 ee 15 04 e3 c8 80 ed 7d fb 63 60 c0 f4 2c ec 00 6c 83 42 22 94 b0 75 72 58 97 8f 85 69 02 90 4f Data Ascii: v5tSR#8~Mii94'.$qIQ3"<wt/CDc)kV 5x6H%~<A4bMc%EW_tq[A<4w-\GBGH|)ih&VrE'JHH`bzrf@Yev!wg 0Z k'f()V"x(@7H}c`,lB"urXiO
2021-09-15 12:02:48 UTC	297	IN	Data Raw: 1a 3c 5d 62 cf a9 42 e7 73 02 63 1b 8f 01 56 42 f5 b7 16 50 18 11 b8 02 41 53 60 83 e1 8a 4e a7 4c d0 d0 ee 85 47 0a 0f e1 59 44 83 24 9e 7b a4 e7 af 98 1c 61 94 47 24 ad cd 29 b9 2c 5b 50 e7 82 71 f5 3a 99 ec 12 f4 b1 a2 df 01 55 7f 53 9a 94 d4 40 c0 23 06 0d dc 04 dc 66 c1 b5 37 86 0d 16 9a 53 28 d3 c0 81 59 e4 6e a4 b6 1d 62 47 20 64 3a 95 57 2a 55 3b 31 e1 e5 f5 69 de 16 15 8d 1c 60 bc 77 87 2b ce 01 ba 43 b1 8f d9 62 2d 49 fb c5 60 6e d5 82 e9 77 0e a5 86 ed c7 e0 30 92 7a 93 c9 c2 79 f0 cd b1 03 48 4f 25 fd ff 00 0f 5f b1 a7 1b 5a 87 07 af 07 3e c2 fe 9f 37 9f 99 7c fc f2 5e 29 49 04 1a 2b b8 58 23 00 90 21 05 7c 19 3c c6 11 14 a0 72 bf 61 fa 8f cf 91 89 12 c5 34 f1 44 8b d0 03 21 2c c3 dc dc 00 3c 00 cd ab b7 93 ef 26 b0 18 11 f9 ae 8e 54 55 71 e0 Data Ascii: <]bBscVBPAS`NLGYD${aG$),[Pq:US@#f7S(YnbG d:W*U;1i`w+Cb-I`nw0zyHO%_Z>7|^)I+X#!|<ra4D!,<&TUq
2021-09-15 12:02:48 UTC	299	IN	Data Raw: 6f 77 b3 f4 84 ae 3f 9c e4 f4 cc 8a 83 e5 45 85 0f 3c 23 e3 23 37 38 3f 12 70 d5 c9 d5 42 fd af 77 ab 90 3d 51 c8 c2 41 dc 52 de 1c f8 ae 24 7d be a2 49 36 06 dc 41 91 8b 79 66 b6 57 e6 96 08 16 4b fc 59 72 7e 84 ef 91 42 8e 3e 04 e0 75 0d c8 24 8f d3 2e 52 0f 31 cf cf fd 60 46 7a 58 a9 0e b7 db 69 48 af c3 35 a0 f4 ef 4b 08 aa 1e 35 82 bf 7e 41 d7 fc 38 b5 b6 c6 c2 5c 74 fd ec 0c 3c 54 dd 11 e4 6a 8e 7a 4d 07 01 8c 32 c0 17 70 f7 4a 4b 67 a5 4a d1 04 d6 9d 88 fc 17 3d 20 0a 9b 74 0b 11 a3 f7 26 7a 44 80 7e d6 cf 1f 82 8c 75 43 44 ef 20 df 3c f2 b9 4a 21 42 07 c4 5e 6a e3 0c ec 18 42 f1 2a f5 35 62 5a c0 ec 6b bd 26 91 24 af f9 1f 93 88 4b 9a 0b fe ca 60 bc 79 6e 27 14 71 60 8d 2f 62 6b ae 37 e4 31 3b b2 c9 54 6d b9 ae be ae eb 67 04 63 46 68 77 49 89 ac Data Ascii: ow?E<##78?pBw=QAR$}I6AyfWKYr~B>u$.R1`FzXiH5K5~A8\t<TjzM2pJKgJ= t&zD~uCD <J!B^jB*5bZk&$K` yn'q`/bk71;TmgcFhwI

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwSetEvent	INLINE	explorer.exe
RtlAllocateMemoryBlockLookaside	INLINE	explorer.exe
RtlAllocateMemoryZone	INLINE	explorer.exe
NtSetEvent	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6348 Parent PID: 412

General

Start time:	14:02:30
Start date:	15/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\3FLps29lWm.dll'
Imagebase:	0x7ff62f690000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6384 Parent PID: 6348

General

Start time:	14:02:31
Start date:	15/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3FLps29lWm.dll',#1
Imagebase:	0x7ff77d8b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6408 Parent PID: 6348

General

Start time:	14:02:31

Start date:	15/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\3FLps29lWm.dll
Imagebase:	0x7ff7b21f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.338160858.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6420 Parent PID: 6384

General

Start time:	14:02:31
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\3FLps29lWm.dll',#1
Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.225554693.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6448 Parent PID: 6348

General

Start time:	14:02:32
Start date:	15/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff6f37a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 6516 Parent PID: 6348

General

Start time:	14:02:32
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginBufferedAnimation
Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.228897543.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6580 Parent PID: 6448

General

Start time:	14:02:33
Start date:	15/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6448 CREDAT:17410 /prefetch:2
Imagebase:	0x150000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: explorer.exe PID: 3388 Parent PID: 6408

General

Start time:	14:02:34
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Copyright Joe Security LLC 2021

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 6772 Parent PID: 6348

General

Start time:	14:02:36
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginBufferedPaint
Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.235930456.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6944 Parent PID: 6348

General

Start time:	14:02:40
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BeginPanningFeedback
Imagebase:	0x7ff673410000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000002.246415321.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 7000 Parent PID: 6348

General

Start time:	14:02:44
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintClear
Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000D.00000002.259705303.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7076 Parent PID: 6348

General

Start time:	14:02:48
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintInit
Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000E.00000002.263971738.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5264 Parent PID: 6348

General

Start time:	14:02:52
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintRenderAnimation

Imagebase:	0x7ff673410000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000010.00000002.270992989.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2740 Parent PID: 6348

General

Start time:	14:02:56
Start date:	15/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\3FLps29lWm.dll,BufferedPaintSetAlpha
Imagebase:	0x1a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rstrui.exe PID: 3180 Parent PID: 3388

General

Start time:	14:03:26
Start date:	15/09/2021
Path:	C:\Windows\System32\rstrui.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rstrui.exe
Imagebase:	0x7ff6e8c30000
File size:	266752 bytes
MD5 hash:	3E8AFFA54035412F86663C8B44CAA2E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rstrui.exe PID: 1708 Parent PID: 3388

General

Start time:	14:03:27
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\UIPe\rstrui.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\UIPe\rstrui.exe
Imagebase:	0x7ff701090000
File size:	266752 bytes
MD5 hash:	3E8AFFA54035412F86663C8B44CAA2E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001B.00000002.365201686.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: Taskmgr.exe PID: 4600 Parent PID: 3388

General

Start time:	14:03:40
Start date:	15/09/2021
Path:	C:\Windows\System32\Taskmgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Taskmgr.exe
Imagebase:	0x7ff6b99d0000
File size:	1326952 bytes
MD5 hash:	CB8FE4DA1AF43E62BAA6A4CBE0A93A74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Taskmgr.exe PID: 4860 Parent PID: 3388

General

Start time:	14:03:45
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\zOAoLK\Taskmgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\zOAoLK\Taskmgr.exe
Imagebase:	0x7ff678770000
File size:	1326952 bytes
MD5 hash:	CB8FE4DA1AF43E62BAA6A4CBE0A93A74
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000021.00000002.404405311.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: FXSCOVER.exe PID: 748 Parent PID: 3388

General

Start time:	14:03:58
Start date:	15/09/2021
Path:	C:\Windows\System32\FXSCOVER.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\FXSCOVER.exe
Imagebase:	0x7ff7ab810000
File size:	232960 bytes
MD5 hash:	BEAB16FEFCB7F62BBC135FB87DF7FDF2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Analysis Process: FXSCOVER.exe PID: 5492 Parent PID: 3388

General

Start time:	14:04:05
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\lFQXVd7\FXSCOVER.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\lFQXVd7\FXSCOVER.exe
Imagebase:	0x7ff753ee0000
File size:	232960 bytes
MD5 hash:	BEAB16FEFCB7F62BBC135FB87DF7FDF2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000027.00000002.448796911.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, ReversingLabs

Analysis Process: mstsc.exe PID: 4872 Parent PID: 3388

General

Start time:	14:04:19
Start date:	15/09/2021
Path:	C:\Windows\System32\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mstsc.exe
Imagebase:	0x7ff6d3bf0000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mstsc.exe PID: 2456 Parent PID: 3388

General

Start time:	14:04:20
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\yeShxe\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\yeShxe\mstsc.exe
Imagebase:	0x7ff601010000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000002B.00000002.479085760.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

Code Analysis