



ID: 715095
Cookbook: browseurl.jbs
Time: 16:14:24
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://kawanakajima.co.jp/collinesredshare666.htm 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
World Map of Contacted IPs 10
Public IPs 10
Private 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 12
Static File Info 12
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
UDP Packets 14
DNS Queries 14
DNS Answers 15
HTTP Request Dependency Graph 16
HTTPS Proxied Packets 16
Statistics 150
Behavior 150
System Behavior 150
Analysis Process: chrome.exePID: 5176, Parent PID: 4544 150
General 150
File Activities 151
Registry Activities 151
Analysis Process: chrome.exePID: 5228, Parent PID: 5176 151
General 151
File Activities 151
Analysis Process: chrome.exePID: 4248, Parent PID: 4544 151
General 151
Registry Activities 152
Analysis Process: chrome.exePID: 6920, Parent PID: 5176 152
General 152
Disassembly 152

Copyright Joe Security LLC 2022

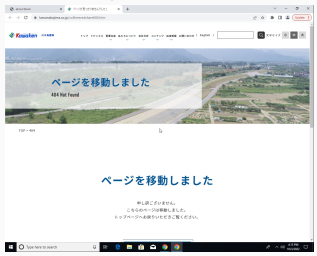
Windows Analysis Report

https://kawanakajima.co.jp/collinesredshare666.htm

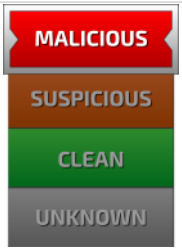
Overview

General Information

Sample URL:	http://https://kawanakajima.co.jp/collinesredshare666.htm
Analysis ID:	715095
Infos:	



Detection

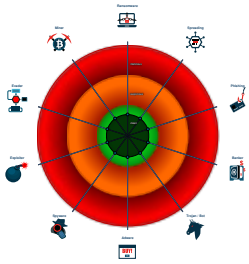


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5176 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5228 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1844 --field-trial-handle=1712,i,10524100664618611924,16229694031488129540,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6920 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=4300 --field-trial-handle=1712,i,10524100664618611924,16229694031488129540,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4248 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://kawanakajima.co.jp/collinesredshare666.htm MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

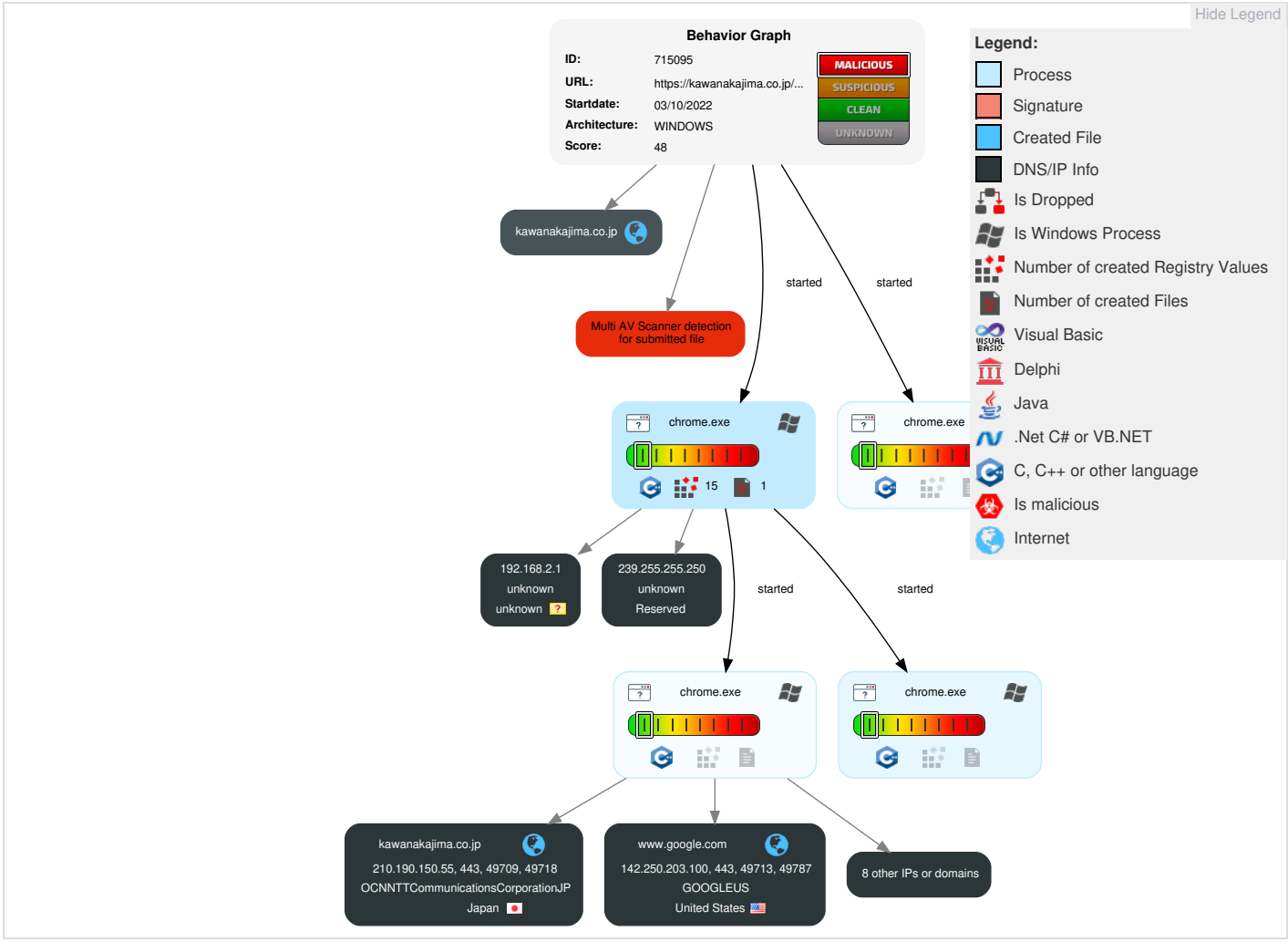


Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

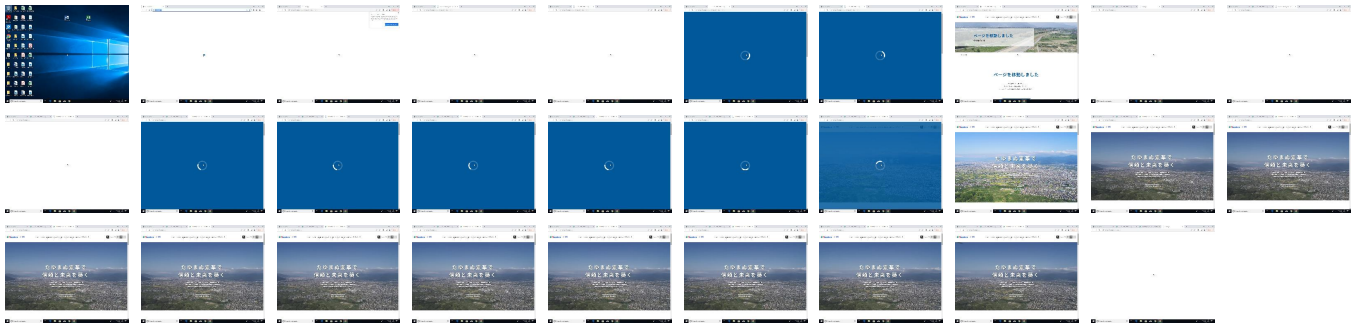
Behavior Graph

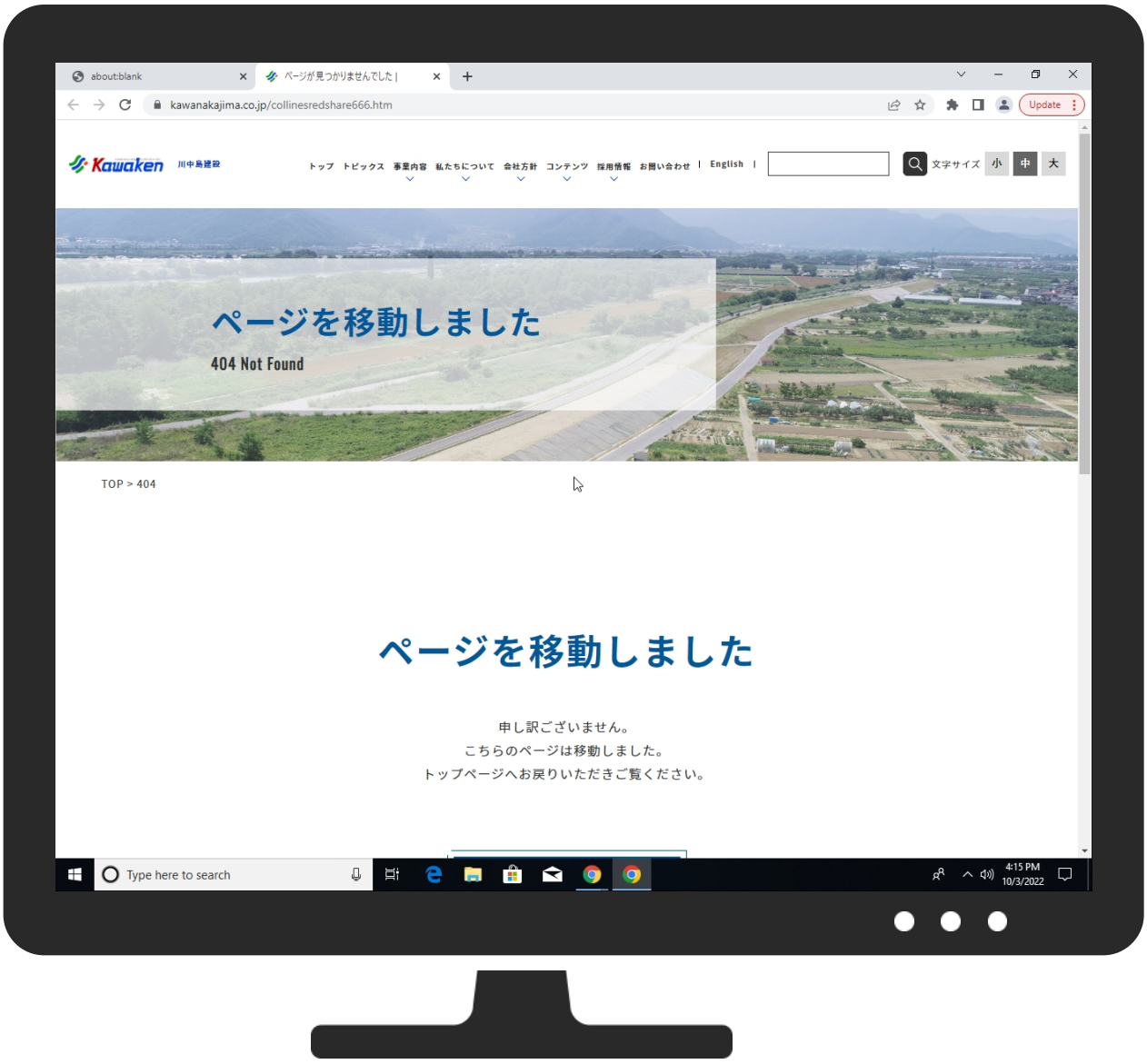


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://kawanakajima.co.jp/collinesredshare666.htm	6%	Virustotal		Browse
http://https://kawanakajima.co.jp/collinesredshare666.htm	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_01_w.svg	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_04.svg	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=842391531&_u=QACAAUAAAAAAAC~&z=82234443	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_blog.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/scrolldown.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_04.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_03.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_04_w.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/tel_freedial.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/js/base.js	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_mov.mp4	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_newsletter.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_facebook.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_ttl.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_03.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_img.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-includes/css/dist/block-library/style.min.css?ver=5.4.11	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_recruit.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_02.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-emoji-release.min.js?ver=5.4.11	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/about_company_img_01.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_recruit.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_search.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_circle_arrow_blue.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_01.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/logo.png	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_contents.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_circle_arrow.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/about_top_img_01.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/logo_footer.png	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_03_w.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_hyosho.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_tosys.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-embed.min.js?ver=5.4.11	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/low_main_img_topics_sp.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/js/scrolltopcontrol.js	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_twitter.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_rekishi.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_01.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_business.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_topics.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_ini.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_about.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_02.jpg	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=974897442&_u=YEBAAUAAAAAAAC~&z=640512449	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_img_sp.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_rakuseki.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_arrow_w.svg	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/plugins/wp-pagenavi/pagenavi-css.css?ver=2.70	0%	Avira URL Cloud	safe	
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_02_w.svg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

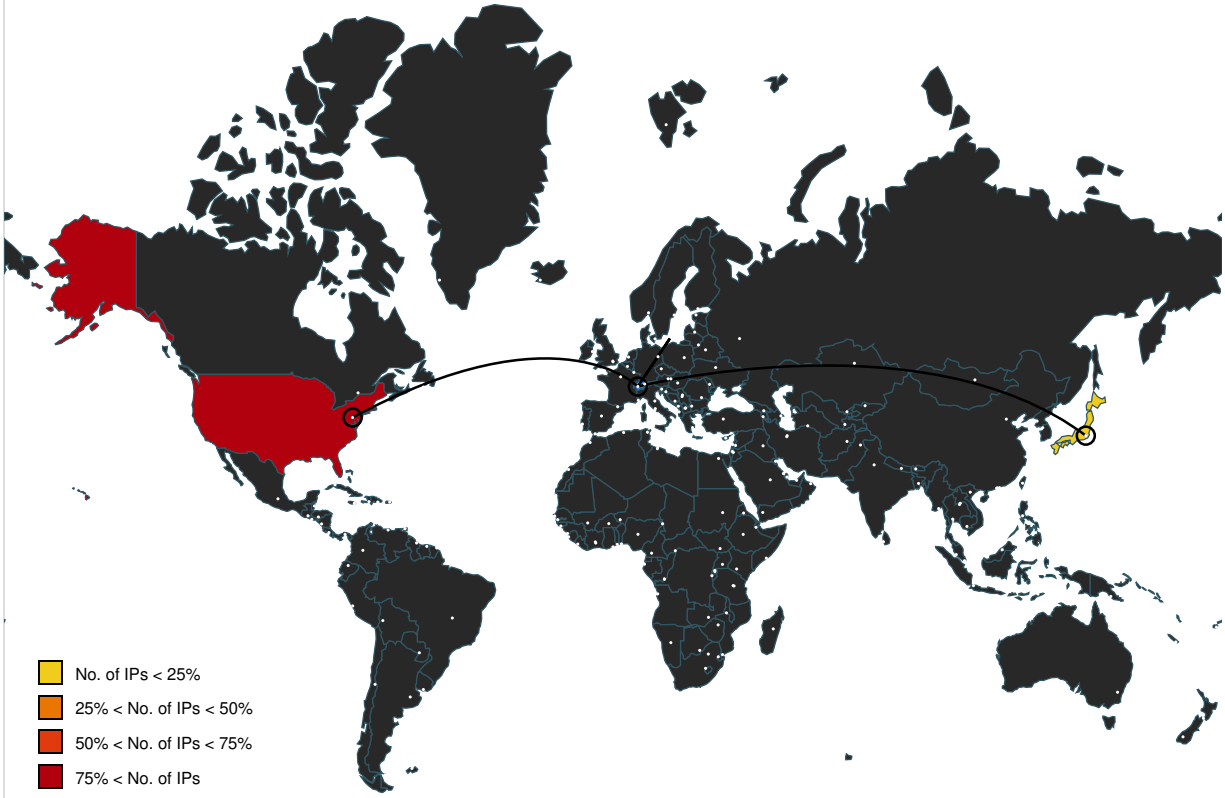
Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
www.google.co.uk	172.217.168.35	true	false		unknown
kawanakajima.co.jp	210.190.150.55	true	false		unknown
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
s.w.org	192.0.77.48	true	false		high
stats.g.doubleclick.net	74.125.143.154	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/scrolldown.svg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=842391531&_u=QACAAUAAAAAAAC~&z=82234443	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_04.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_01_w.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_blog.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_04.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/collinesredshare666.htm	true		unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_04_w.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/collinesredshare666.htm	true		unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_03.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/tel_freedial.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_mov.mp4	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/js/base.js	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/	false		unknown
http://https://kawanakajima.co.jp/news/	false		unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_newsletter.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_facebook.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_ttl.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_03.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_img.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-includes/css/dist/block-library/style.min.css?ver=5.4.11	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=974897442&_u=YEBAAUAAAAAAAC~&z=640512449	false		high
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_recruit.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_02.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-emoji-release.min.js?ver=5.4.11	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/about_company_img_01.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_recruit.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_search.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/	false		unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_circle_arrow_blue.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_01.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/logo.png	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_contents.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_circle_arrow.svg	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/about_top_img_01.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/logo_footer.png	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_03_w.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_hyosho.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_tosys.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/low_main_img_topics_sp.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-embed.min.js?ver=5.4.11	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_twitter.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/js/scrolltopcontrol.js	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_rekishi.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_01.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_business.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/news/	false		unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_topics.svg	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=842391531&gjid=820369651&_gid=1735943631.1664838942&_u=QACAAUAAAAAAAC~&z=292433703	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=842391531&_u=QACAAUAAAAAAAC~&z=82234443	false		high
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_ini.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/ttl_about.svg	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/business_img_02.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=974897442&_u=YEBAAUAAAAAAAC~&z=640512449	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/main_img_sp.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/top_rakuseki.jpg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_arrow_w.svg	false	• Avira URL Cloud: safe	unknown
http://https://kawanakajima.co.jp/wordpress/wp-content/plugins/wp-pagenavi/pagenavi-css.css?ver=2.70	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=974897442&gjid=761990059&_gid=1735943631.1664838942&_u=YEBAAUAAAAAAAC~&z=1809022200	false		high
http://https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/icon_business_02_w.svg	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
74.125.143.154	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
74.125.143.157	unknown	United States		15169	GOOGLEUS	false
210.190.150.55	kawanakajima.co.jp	Japan		4713	OCNNTTCommunicationsCorporationJP	false
172.217.168.35	www.google.co.uk	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715095
Start date and time:	2022-10-03 16:14:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://kawanakajima.co.jp/collinesredshare666.htm
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13

Copyright Joe Security LLC 2022

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:	mal48.win@29/0@16/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://kawanakajima.co.jp/ • Browse: https://kawanakajima.co.jp/news/

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 142.250.203.104, 172.217.168.10, 172.217.168.74, 172.217.168.78, 142.250.203.106, 216.58.215.234, 172.217.168.42
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, www.googletagmanager.com, ajax.googleapis.com, fonts.gstatic.com, update.googleapis.com, clientservices.googleapis.com, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

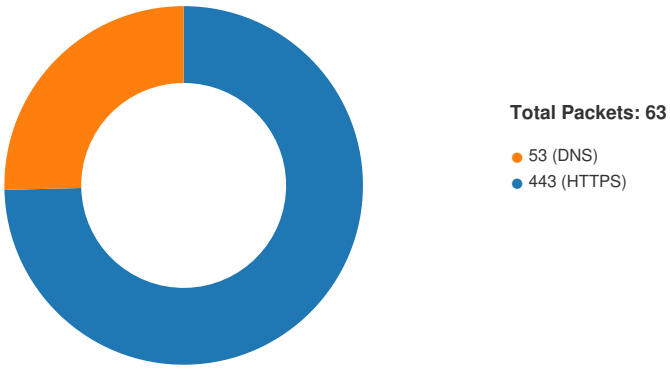
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:24.559900999 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:24.559962034 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:24.560040951 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:24.562769890 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:24.562799931 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:24.565815926 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:24.565875053 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:24.565965891 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:24.566329002 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:24.566368103 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:24.636204004 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:24.655086994 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:24.680260897 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:24.695913076 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.010665894 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.010696888 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:25.011599064 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:25.011640072 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:25.011779070 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:25.011876106 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.014024019 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:25.014152050 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.015016079 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:25.015126944 CEST	49706	443	192.168.2.6	142.250.203.109

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:25.971426010 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:25.971477985 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:25.971566916 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:25.972110987 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:25.972156048 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:25.972454071 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:25.972877979 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:25.972907066 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:25.973808050 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.973826885 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:25.974236012 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:25.974282980 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:25.974515915 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:25.977171898 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:25.977195024 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:26.011790037 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:26.011919022 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:26.011950970 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:26.012073040 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:26.012195110 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:26.015604019 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:26.028815985 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:26.028898001 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:26.028943062 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:26.029135942 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:26.029213905 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:26.043567896 CEST	49707	443	192.168.2.6	142.250.203.110
Oct 3, 2022 16:15:26.043606043 CEST	443	49707	142.250.203.110	192.168.2.6
Oct 3, 2022 16:15:26.069063902 CEST	49706	443	192.168.2.6	142.250.203.109
Oct 3, 2022 16:15:26.069114923 CEST	443	49706	142.250.203.109	192.168.2.6
Oct 3, 2022 16:15:26.885390043 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.886254072 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:26.886307001 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.888580084 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.888744116 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:26.892954111 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:26.892983913 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.893193007 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:26.893203020 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.893312931 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.934094906 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:26.934129953 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:26.975603104 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:27.315926075 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.315975904 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.316060066 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.316507101 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.316541910 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.387990952 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.388408899 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.388500929 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.389725924 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.389816046 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.392257929 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.392292023 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.392420053 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.496726990 CEST	49713	443	192.168.2.6	142.250.203.100
Oct 3, 2022 16:15:27.496788025 CEST	443	49713	142.250.203.100	192.168.2.6
Oct 3, 2022 16:15:27.596645117 CEST	49713	443	192.168.2.6	142.250.203.100

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:34.176827908 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.176944971 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.176984072 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.177023888 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.177098036 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.177133083 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.177150011 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.316236019 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.472106934 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.472141981 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.472228050 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.472270012 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.472327948 CEST	443	49709	210.190.150.55	192.168.2.6
Oct 3, 2022 16:15:34.472398996 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.472399950 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.472399950 CEST	49709	443	192.168.2.6	210.190.150.55
Oct 3, 2022 16:15:34.472448111 CEST	443	49709	210.190.150.55	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:15:23.694400072 CEST	56331	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:23.714263916 CEST	53	56331	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:24.467679024 CEST	50506	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:24.495517969 CEST	53	50506	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:25.030401945 CEST	59504	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:25.284606934 CEST	53	59504	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:27.245860100 CEST	62538	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:27.286262035 CEST	53	62538	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:27.293190002 CEST	54903	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:27.312752008 CEST	53	54903	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:41.737271070 CEST	55629	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:41.756509066 CEST	53	55629	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:43.206222057 CEST	61833	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:43.231681108 CEST	53	61833	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:43.834508896 CEST	60032	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:43.860522985 CEST	53	60032	8.8.8.8	192.168.2.6
Oct 3, 2022 16:15:49.864190102 CEST	57322	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:15:50.118765116 CEST	53	57322	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:28.175978899 CEST	54196	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:28.195405006 CEST	53	54196	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:29.770344973 CEST	57754	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:29.798125029 CEST	53	57754	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:32.299644947 CEST	52886	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:32.317226887 CEST	53	52886	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:50.140960932 CEST	57786	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:50.415467978 CEST	53	57786	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:56.166985035 CEST	54503	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:56.183734894 CEST	53	54503	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:57.113533974 CEST	54508	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:57.141154051 CEST	53	54508	8.8.8.8	192.168.2.6
Oct 3, 2022 16:16:57.305232048 CEST	53193	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:16:57.344384909 CEST	53	53193	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:23.694400072 CEST	192.168.2.6	8.8.8.8	0x537e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:24.467679024 CEST	192.168.2.6	8.8.8.8	0xe94f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:25.030401945 CEST	192.168.2.6	8.8.8.8	0xbbac	Standard query (0)	kawanakajima.co.jp	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:27.245860100 CEST	192.168.2.6	8.8.8.8	0xae14	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:27.293190002 CEST	192.168.2.6	8.8.8.8	0x7d61	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:41.737271070 CEST	192.168.2.6	8.8.8.8	0x30e4	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.206222057 CEST	192.168.2.6	8.8.8.8	0xae57	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.834508896 CEST	192.168.2.6	8.8.8.8	0x1fea	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:49.864190102 CEST	192.168.2.6	8.8.8.8	0xf258	Standard query (0)	kawanakajima.co.jp	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:28.175978899 CEST	192.168.2.6	8.8.8.8	0x9d77	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:29.770344973 CEST	192.168.2.6	8.8.8.8	0xe435	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:32.299644947 CEST	192.168.2.6	8.8.8.8	0xf41c	Standard query (0)	kawanakajima.co.jp	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:50.140960932 CEST	192.168.2.6	8.8.8.8	0xe014	Standard query (0)	kawanakajima.co.jp	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:56.166985035 CEST	192.168.2.6	8.8.8.8	0xd3fd	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.113533974 CEST	192.168.2.6	8.8.8.8	0x6f4	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.305232048 CEST	192.168.2.6	8.8.8.8	0xf202	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:23.714263916 CEST	8.8.8.8	192.168.2.6	0x537e	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:24.495517969 CEST	8.8.8.8	192.168.2.6	0xe94f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:15:24.495517969 CEST	8.8.8.8	192.168.2.6	0xe94f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:25.284606934 CEST	8.8.8.8	192.168.2.6	0xbbac	No error (0)	kawanakajima.co.jp		210.190.150.55	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:27.286262035 CEST	8.8.8.8	192.168.2.6	0xae14	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:27.312752008 CEST	8.8.8.8	192.168.2.6	0x7d61	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:41.756509066 CEST	8.8.8.8	192.168.2.6	0x30e4	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.231681108 CEST	8.8.8.8	192.168.2.6	0xae57	No error (0)	stats.g.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.231681108 CEST	8.8.8.8	192.168.2.6	0xae57	No error (0)	stats.g.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.231681108 CEST	8.8.8.8	192.168.2.6	0xae57	No error (0)	stats.g.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.231681108 CEST	8.8.8.8	192.168.2.6	0xae57	No error (0)	stats.g.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:15:43.860522985 CEST	8.8.8.8	192.168.2.6	0x1fea	No error (0)	www.google.co.uk		172.217.168.35	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:15:50.118765116 CEST	8.8.8.8	192.168.2.6	0xf258	No error (0)	kawanakajima.co.jp		210.190.150.55	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:28.195405006 CEST	8.8.8.8	192.168.2.6	0x9d77	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:29.798125029 CEST	8.8.8.8	192.168.2.6	0xe435	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:32.317226887 CEST	8.8.8.8	192.168.2.6	0xf41c	No error (0)	kawanakajima.co.jp		210.190.150.55	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:50.415467978 CEST	8.8.8.8	192.168.2.6	0xe014	No error (0)	kawanakajima.co.jp		210.190.150.55	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:56.183734894 CEST	8.8.8.8	192.168.2.6	0xd3fd	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.141154051 CEST	8.8.8.8	192.168.2.6	0x6f4	No error (0)	stats.g.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.141154051 CEST	8.8.8.8	192.168.2.6	0x6f4	No error (0)	stats.g.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.141154051 CEST	8.8.8.8	192.168.2.6	0x6f4	No error (0)	stats.g.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.141154051 CEST	8.8.8.8	192.168.2.6	0x6f4	No error (0)	stats.g.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:16:57.344384909 CEST	8.8.8.8	192.168.2.6	0xf202	No error (0)	www.google.co.uk		172.217.168.35	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- kawanakajima.co.jp
- https:
  - stats.g.doubleclick.net
  - www.google.com
  - www.google.co.uk

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49706	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:25 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: __Secure-ENID=6.SE=Md0Ynyf9ahpkx1CxTGF0vY434NJ6ymH-gDI2TI5Ly-NQYGPjnNfggtiFRMAwx4JRDOC_gavEPcD5cTBJzUgtbJobmBEuJ8xi2UuotxvOZgApoqSIg1b0RP47U08XG8Bz_SExSzKy0ETSsajbToDlYyFsxfl93p7AyRAd-OeIBA0; CONSENT=PENDING+070

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:25 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-10-03 14:15:26 UTC	2	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 14:15:26 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-58iEXsYCXbgG_nuhnz8A4Q' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 14:15:26 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-10-03 14:15:26 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49707	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:25 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:26 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-fDsri9P1W4gYLnGjJVVS6Q' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 14:15:25 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 26125 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:26 UTC	2	IN	Data Raw: 32 63 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 36 31 32 35 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="26125"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 14:15:26 UTC	2	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 14:15:26 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49734	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:42 UTC	273	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_arrow_w.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:43 UTC	277	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:42 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "1b6-5b252e7c40940" Accept-Ranges: bytes Content-Length: 438 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:43 UTC	277	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 32 2e 32 32 20 38 2e 35 39 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 30 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 38 2e 32 33 2e 31 33 61 2e 34 34 2e 34 34 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 12.22 8.59"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 10</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M8.23.13a.44.44,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.6	49960	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:56 UTC	11514	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_recruit.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Wed, 25 Nov 2020 04:14:36 GMT If-None-Match: "276ff-5b4e6aa49e300"

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11515	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:56 GMT Server: Apache Connection: close ETag: "276ff-5b4e6aa49e300"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.6	49961	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:56 UTC	11515	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo_footer.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "e43c-5b252e7d34b80"
2022-10-03 14:16:57 UTC	11515	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:56 GMT Server: Apache Connection: close ETag: "e43c-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.6	49965	74.125.143.157	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11515	OUT	POST /j/collect?t=dc&aip=1&_r=3&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=842391531&gjid=820369651&_gid=1735943631.1664838942&_u=QACAAUAAAAAAAC~&z=292433703 HTTP/1.1 Host: stats.g.doubleclick.net Connection: keep-alive Content-Length: 0 sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Content-Type: text/plain Accept: */* Origin: https://kawanakajima.co.jp X-Client-Data: CK61yQEIh7bJAQiltskBCMS2yQEIqZ3KAQiTocsBCIurzAEI7bvMAQiAvcwBCLLBzAEIxcHMAQjWwcwB Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:16:57 UTC	11516	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: https://kawanakajima.co.jp Strict-Transport-Security: max-age=10886400; includeSubDomains; preload Date: Mon, 03 Oct 2022 14:16:57 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Last-Modified: Sun, 17 May 1998 03:00:00 GMT Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Content-Type: text/plain Cross-Origin-Resource-Policy: cross-origin Server: Golfe2 Content-Length: 7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-10-03 14:16:57 UTC	11517	IN	Data Raw: 31 67 63 6f 2e 75 6b Data Ascii: 1gco.uk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.6	49968	142.250.203.100	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11517	OUT	GET /ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942 &jid=842391531&_u=QACAAUAAAAAAAC~&z=82234443 HTTP/1.1 Host: www.google.com Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 X-Client-Data: CK61yQEIh7bJAQiltskBCMS2yQEIqZ3KAQiTocsBCIurzAEI7bvMAQiAvcwBCLLBzAEIxcHMAQjWwcwB Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:16:57 UTC	11518	IN	HTTP/1.1 200 OK P3P: policyref="https://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA IVD OTP OUR OTR IND OTC" Timing-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Date: Mon, 03 Oct 2022 14:16:57 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Content-Type: image/gif X-Content-Type-Options: nosniff Server: cafe Content-Length: 42 X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-10-03 14:16:57 UTC	11519	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 ff ff ff 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 01 44 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.6	49969	172.217.168.35	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11518	OUT	GET /ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942 &jid=842391531&_u=QACAAUAAAAAAAC~&z=82234443 HTTP/1.1 Host: www.google.co.uk Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 X-Client-Data: CK61yQEIh7bJAQiltskBCMS2yQEIqZ3KAQiTocsBCIurzAEI7bvMAQiAvcwBCLLBzAEIxcHMAQjWwcwB Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11519	IN	HTTP/1.1 200 OK P3P: policyref="https://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA IVD OTP OUR OTR IND OTC" Timing-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Date: Mon, 03 Oct 2022 14:16:57 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Content-Type: image/gif X-Content-Type-Options: nosniff Server: cafe Content-Length: 42 X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-10-03 14:16:57 UTC	11520	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 ff ff ff 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 01 44 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.6	49964	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11520	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "31e7-5b252e7c40940"
2022-10-03 14:16:58 UTC	11520	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:58 GMT Server: Apache Connection: close ETag: "31e7-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.6	49966	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:57 UTC	11520	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_tosys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "2982-5b252e7c40940"
2022-10-03 14:16:58 UTC	11521	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:58 GMT Server: Apache Connection: close ETag: "2982-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.6	49975	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:58 UTC	11521	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "4356-5b252e7c40940"

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:59 UTC	11521	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:59 GMT Server: Apache Connection: close ETag: "4356-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.6	49976	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:58 UTC	11521	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_facebook.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "28a-5b252e7d34b80"
2022-10-03 14:16:59 UTC	11521	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:59 GMT Server: Apache Connection: close ETag: "28a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.6	49977	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:00 UTC	11522	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_twitter.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "3db-5b252e7d34b80"
2022-10-03 14:17:00 UTC	11522	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:00 GMT Server: Apache Connection: close ETag: "3db-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	63355	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:42 UTC	273	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_search.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	278	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:42 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "1fe-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 510 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:43 UTC	279	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 31 20 33 31 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 33 32 33 32 33 32 3b 73 74 72 6f 6b 65 3a 23 33 32 33 32 33 32 3b 73 74 72 6f 6b 65 2d 6d 69 74 65 72 6c 69 6d 69 74 3a 31 30 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 73 74 72 6f 6b 65 3a 23 66 66 66 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 63 61 70 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 77 69 64 74 68 3a 31 2e 35 70 78 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 31 31"><defs><style>.cls-1{fill:#323232;stroke:#323232;stroke-miterlimit:10;}.cls-2{fill:none;stroke:#fff;stroke-linecap:round;stroke-linejoin:round;stroke-width:1.5px;}</style></defs><title>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.6	49978	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:00 UTC	11522	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "16b4-5b252e7d34b80"
2022-10-03 14:17:00 UTC	11522	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:00 GMT Server: Apache Connection: close ETag: "16b4-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.6	49982	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:01 UTC	11522	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "2ff37-5b252e7c40940"
2022-10-03 14:17:01 UTC	11523	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:01 GMT Server: Apache Connection: close ETag: "2ff37-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.6	49983	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:01 UTC	11523	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_02.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "72497-5b252e7c40940"

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:01 UTC	11523	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:01 GMT Server: Apache Connection: close ETag: "72497-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.6	49985	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:02 UTC	11523	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_03.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "2773e-5b252e7c40940"
2022-10-03 14:17:03 UTC	11524	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:02 GMT Server: Apache Connection: close ETag: "2773e-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.6	49986	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:02 UTC	11524	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_04.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "d4da-5b252e7c40940"
2022-10-03 14:17:03 UTC	11524	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:02 GMT Server: Apache Connection: close ETag: "d4da-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.6	49987	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:03 UTC	11524	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "621a-5b252e7d34b80"
2022-10-03 14:17:04 UTC	11525	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:04 GMT Server: Apache Connection: close ETag: "621a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.6	49988	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:03 UTC	11524	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Wed, 28 Oct 2020 08:52:19 GMT If-None-Match: "6ed50-5b2b747ec96c0"
2022-10-03 14:17:04 UTC	11525	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:04 GMT Server: Apache Connection: close ETag: "6ed50-5b2b747ec96c0"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.6	49989	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:04 UTC	11525	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics_sp.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Wed, 28 Oct 2020 08:52:20 GMT If-None-Match: "22fb8-5b2b747fbd900"
2022-10-03 14:17:05 UTC	11526	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:05 GMT Server: Apache Connection: close ETag: "22fb8-5b2b747fbd900"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.6	49990	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:04 UTC	11525	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo_footer.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "e43c-5b252e7d34b80"
2022-10-03 14:17:05 UTC	11526	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:05 GMT Server: Apache Connection: close ETag: "e43c-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.6	49991	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:06 UTC	11526	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "31e7-5b252e7c40940"
2022-10-03 14:17:06 UTC	11527	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:06 GMT Server: Apache Connection: close ETag: "31e7-5b252e7c40940"

Copyright Joe Security LLC 2022

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	21044	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:42 UTC	274	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:43 UTC	279	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:42 GMT Server: Apache Last-Modified: Wed, 28 Oct 2020 08:52:19 GMT ETag: "6ed50-5b2b747ec96c0" Accept-Ranges: bytes Content-Length: 453968 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:43 UTC	279	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	443	IN	Data Raw: bd 79 d0 b7 d3 c1 c6 95 52 ca 56 55 b8 52 c5 c8 03 7e 9a 7b 63 4d 81 12 2e 27 b5 cb 62 ab 29 76 b5 96 63 22 48 e6 15 78 a2 25 03 1e e0 72 a0 06 04 95 5a 53 e0 3a 6b 55 ba 3d 07 03 5c 62 2c b2 37 18 fb 5b 7c 5d c4 e8 14 c1 dc b8 95 ed d5 57 62 27 8d c2 90 f1 8a f5 04 8d 74 57 b0 e8 9b 6c c8 b7 49 e3 76 c3 1d 6f 86 0a b7 16 38 98 43 43 2b 47 0b 15 50 07 70 95 65 20 16 26 a0 f2 15 ad 69 e9 a8 57 b4 dd a7 e4 2d c9 49 ce f8 b5 e5 f2 db 1c 3e 4a 59 59 20 65 bb 82 79 07 71 a3 e5 5e 6b 22 15 45 01 4d 02 81 b8 f5 3d 35 df 87 b6 97 f6 46 e4 07 b7 46 c7 58 0b 6c 7a 3d ec af c4 c8 0c 8b 24 9c 86 c0 29 5e 05 a8 49 a5 2a 74 dc b9 bd 4c c0 79 1c a5 d4 6b 78 b2 2c b7 16 a5 08 b8 b1 e8 ca 4e c7 67 35 04 75 df 54 a5 65 82 24 cd 60 92 c5 25 b8 4b d8 6e 6e 6e 9d 4c 51 c3 3c Data Ascii: yRVUR~{cM.'b)vc"Hx%rZS:kU=\b,7[|]Wb'tWIlvo8CC+GPpe &iW-I>JYY eyq^k"EM=5FFXlz=$)^I*tLykx, Ng5uTe$`%KnnnLQ<
2022-10-03 14:15:43 UTC	459	IN	Data Raw: 3b 06 6f 52 36 d6 cb a3 1d da 10 36 fe e2 f8 1a dc 5f 43 68 08 25 82 c5 dd 32 a1 3f a5 4b 35 55 b7 a5 74 71 c7 c0 1b 26 78 ac 6f 2e 3a e2 da 2b f8 ed f0 f2 5c f2 b9 42 59 26 91 6a c2 35 56 29 db 27 da 48 2c 68 34 d9 af ac f9 19 db 4d 42 17 f1 e3 ec af 31 32 c2 f6 a8 12 3e 57 56 b7 2e 92 db b4 6c 49 67 ee 31 7e 4e a0 06 3c 46 c7 60 a3 6a c9 37 6d 01 56 0c b8 f2 08 64 ba 92 e3 17 61 8f 77 40 24 82 2b 5e e4 4e c6 4a d6 55 76 01 8f 10 2a 79 7b 76 dd 74 56 2d 21 89 c5 33 97 59 1b 5c cd dd ac f9 d9 e4 b6 c6 43 0a 9b 7b 76 89 a5 ee 70 e2 cd 10 55 96 32 c5 ce fc 89 1b 7a 68 70 75 ab 55 dc 15 ab ab 93 4e 4c bd ba c0 26 c7 63 2d ad f0 28 e9 2c 78 9b 78 a2 5e 5c a3 d8 5c aa 37 1a 80 6a 01 24 8d eb f0 d7 99 6c 4f cb d7 e4 16 96 f5 22 4d 95 9a 5c a5 b2 5f e5 65 ff 00 Data Ascii: ;oR66_Ch%2?K5Utq&xo.:+\BY&j5V)'H,h4MB12>WV.Ilg1~N<F`j7mVdaw@$+^NJUv*y{vtV-!3Y\C{vpU2zhpu UNL&c-(,xx^\\7j$lO"M_e
2022-10-03 14:15:43 UTC	475	IN	Data Raw: 4e ec 67 f9 45 5b 91 1f c3 4b cb 80 ed 79 25 da 61 da 1b 4c 3d dd 9e 52 59 ae 1b 84 b7 b8 b0 0b f0 ee 53 7e 64 71 1e a0 d4 7e 1e ba 57 92 5b 4d 19 d9 6d e0 0f 69 6d 6b 79 93 9e e2 e5 d9 ec ed 1d f8 5a b3 45 33 bb 02 a5 98 40 64 8d c8 a1 f4 5a fc b4 d7 c8 ea a1 06 ba 16 8c 35 9f 85 da 67 2e fe 8f 3f 24 97 81 63 18 f4 82 cb e9 da 5b 86 01 68 a4 b3 ee 29 fa 78 8a b7 f3 0d 4b 25 f2 f1 d6 ba 0a e5 9a 4c be 2d 39 b5 ef 22 43 61 0a 89 ae 2e 72 57 af 14 52 05 6a 15 02 dc 48 28 4d 2b 51 f3 dc eb 8b df a8 8d 7c 94 bc f6 17 34 98 7b 8b ae fd 85 e4 16 40 3f 6a d5 09 2e 08 15 56 68 94 02 78 9a ee 6a 7a 0d f5 d5 87 25 5b da 0c 9c 81 bc 7f 25 0d e5 a7 6f 19 e3 69 8e 59 24 6f a8 16 ea d7 90 04 04 2a bc 88 e8 ec 1b a9 66 af 4f 86 9f 2d 1d 5e ae 4a 3a f9 91 99 e3 c9 78 8e Data Ascii: NgE[Ky%aL=RYS~dq~W[MmimkyZE3@dZ5g.?$c[h)xK%L-9"Ca.rWRjH(M+Q\|4{@?j.Vhxjz%[%oiY$o*fO-^J:x
2022-10-03 14:15:43 UTC	491	IN	Data Raw: 45 45 1a 3d c0 a8 e8 e4 0d 71 e5 a4 68 0b a8 2d f9 1c d7 97 34 16 96 16 36 57 b1 d8 5c 0e dd b5 dc 16 28 6a 0d 7d aa c2 39 89 07 d0 d3 fb 75 cf 8e b4 f2 f5 24 e8 9e a5 2f 3f 7f 0e 21 be 92 74 ca db 65 24 67 9a 59 ee 4a 40 a8 24 01 56 39 51 e1 1b 7c 7d a3 6d 75 52 9c 94 e9 01 45 af 1c ad 05 ae 06 fa 6c 30 9e d2 19 2e 6e af b3 04 4b 70 82 15 8d 98 2b 39 88 c0 8e fb 12 85 77 ad 48 a8 07 5c f6 fb 9b 52 18 d7 fd 02 d8 df 20 b6 be b7 b2 38 5f 24 7c 6c d7 2e d3 c9 8d b6 b6 65 b6 40 d2 19 1e 05 8d 02 a7 35 eb c9 a3 0b 5f 4a 75 9d f1 b5 b8 ae ad 6a 48 c9 dc 4d 34 d2 bb c8 b6 f2 49 c9 cd cb a7 16 72 fb 37 22 8b bd 7f 0d 6c 68 29 15 39 ad 91 79 cf 2c ea 12 a1 1a 20 bc 9d 57 6a 82 09 56 00 8f 5d 5e 7c 22 a9 24 8a 7d dd ec 30 c8 0f d4 b4 51 4b 28 64 79 39 04 5a ec 09 Data Ascii: EE=qh-46W\(j}9u$/?!te$gYJ@$V9Q\|}muREl0.nKp+9wH\R 8_$|l.e@5_JujHM4Ir7"lh)9y, WjV]^|"$}0QK(dy9Z
2022-10-03 14:15:43 UTC	539	IN	Data Raw: f0 ec 91 63 e5 b7 b2 8e 03 24 03 dc b2 76 ca 38 4e e9 5e 2c 03 03 bf ce ba e1 c9 7b 5a da 1d 38 ee aa a0 a0 cb 95 b0 ff 00 54 63 f2 72 f8 86 26 19 a5 86 47 bd 86 e6 56 55 78 d4 02 88 63 58 57 89 e2 79 7c cf c4 0d cf 27 54 2e 4c a9 bd 8b d5 b4 98 4c 8d 84 76 cb e2 b1 63 d8 ce f3 34 76 93 b3 21 97 9b 3f 06 2a a1 42 97 23 60 47 e1 a8 db b0 d3 0a c9 57 e0 91 99 bf 31 63 ec 65 5c 3a e3 e0 8b bf f4 f0 cc dc 52 60 40 2a d1 33 3a 92 79 21 35 a1 f9 e8 be 56 52 6b dd 46 85 7e d2 ee d3 27 6e 2e 64 ce d9 d9 83 18 37 31 4f 0d d8 e2 d4 a9 46 92 18 98 13 4d bd b5 d2 2b 24 f5 38 9d 67 76 2b 29 85 b4 8e d8 09 fc bf 15 89 46 80 5c 76 c3 5d b1 31 9a d3 88 9e d8 b1 af e9 a9 1a ad 2c 93 32 af d4 c3 ec bc 76 ca 7b eb bb c9 3c d2 76 7b 74 74 c5 da b5 95 e7 6e e1 81 23 94 7d a4 Data Ascii: c$v8N^,{Z8Tcr&GVUxcXWy|'T.LLvc4v!?*B#`GW1ce\:R`@*3:y!5VRkF~'n.d71OFM+$8gv+)F\v]1,2v{<v{ttn#}
2022-10-03 14:15:44 UTC	599	IN	Data Raw: 1e 67 79 63 75 67 92 b7 c6 43 1b c5 24 38 d7 fa 60 ed 6a 92 81 51 00 b5 82 3a 2d 54 1a 37 21 e9 aa da f6 f2 93 3b 71 ac 89 6c 54 ce 0f ee 09 18 79 ad 32 d8 b4 b7 b1 21 b2 81 2c 2e 60 9a e1 2b ba 81 6c b0 84 20 7a d0 d4 f5 f8 69 6d 8f 1d d6 b5 86 51 d5 d8 b0 c5 69 98 be 9e e0 64 f1 c8 f1 b0 55 49 2d ed 67 92 66 1c 78 d4 c8 d6 eb 4d 80 1b 57 f1 d7 27 e2 c6 d6 32 a3 2b 97 3f 6f bc 3f 25 7a d8 f7 c2 3b 64 d6 41 71 36 38 5b b9 72 c8 be d7 fa 71 42 48 04 1a f1 d3 2a 5d 7f 90 b6 a4 e8 c8 d7 7f 69 2f c3 d3 17 e4 f7 be 31 8b a8 69 6d 23 f1 d9 a6 f7 9f e7 59 2d e7 85 85 7f f0 8f cf 56 c5 c2 3e fd 42 b0 d5 23 b8 8f b6 11 63 ef ae b2 13 7d ca 39 29 2e f8 02 2f 70 5c 25 08 8b 4e da cb 73 7f 2b 2a d2 95 55 0a 2b d7 7d 57 2b a5 aa 92 d2 0c f0 a6 33 93 fb 79 08 ec 99 b2 Data Ascii: gycugC$8`jQ:-T7!;qlTy2!,.`+l zimQidUI-gfxMW'2+?o?%z;dAq68[rqBH*]i/1im#Y-V>B#c}9)./p\%Ns+*U+}W+3y
2022-10-03 14:15:44 UTC	615	IN	Data Raw: 97 fd d2 ce 65 62 38 8c d7 da 2b 6b c8 ef 6a 20 8a db 21 c5 1e a0 ab c3 36 42 09 b8 05 62 7a b0 55 da b5 d2 27 46 f7 27 6e d5 d6 90 8f 9d 47 85 79 98 ca 64 63 b4 f1 bb 4b 2c 64 e6 16 8a 0f de f0 33 4c 2d e2 e6 a2 22 5b 24 b5 a1 6a 55 f7 3d 7d 4e ba d7 ae 37 26 d3 7a a8 3e 8c f0 df 2b cf f8 37 8e 5b 63 71 7f 66 a2 bc 8a cc 22 cd 93 bb f2 3c 53 cb 24 43 f5 b3 76 72 29 1a 8a d4 85 45 03 7a ee 75 1b d2 96 7b a0 d2 f7 4b 64 4e cf 79 f7 9a 79 7f 8e b4 38 cf b4 71 43 61 91 5e 37 19 1c 7e 72 c2 75 96 26 1c 59 23 56 bb 46 26 83 ae c3 d3 7d 23 c1 44 f5 65 39 5a 34 48 f8 6a ff 00 ec 87 de 4b f9 f2 02 d7 c7 72 91 c9 2b 81 c2 de 5b 17 8c c2 ee d4 2d c2 f0 71 a0 f8 13 5d 7a 98 f3 63 4a 0e 6b 61 b3 ff 00 f9 9a 4d e7 fb 7e fb 81 86 b5 8f 23 7a d6 76 5f 59 6d 6c c2 e7 21 Data Ascii: eb8+kj !6BbzU'F'nGydcK,d3L-"[$jU=}N7&z>+7[cqf"<S$Cvr)Ezu{KdNyy8qCa^7~ru&Y#VF&}#De9Z4HjKr+[-q]zcJkaM~#zv_Yml!
2022-10-03 14:15:44 UTC	631	IN	Data Raw: 2c 38 fc 06 0b 0f 71 15 de 3b 1b 6f 69 79 6d 46 8e ee 16 71 2a 9a 50 1e 45 f9 57 f3 d7 52 c3 4f 02 3b b6 4b 9e 49 6e 5c b3 bb 3e f5 20 9a f2 27 d4 93 5a 9d 55 21 19 d6 8e 65 51 1c 92 f1 4a 1e 6c 6b b0 fc 74 45 83 0b fb c1 e4 37 0b 84 bd c5 e3 24 b8 b1 74 23 bd 76 ac e8 8e 88 09 31 82 8a 4b 16 3d 6a 40 03 e3 af 2b b7 db 87 c5 15 78 da ac 9f 10 78 87 94 b2 e6 2e f1 b7 1c 45 ba 4c d2 4e b2 15 11 13 31 a9 66 ee 10 78 f2 f5 5e a7 e5 ae 2c aa bc 65 9c 9e d5 47 a9 ab db 64 2d 59 3b 6b 1d b1 2d 50 c8 b0 a4 66 9f 11 c8 80 47 a7 ae b8 b9 50 e8 a7 6b 1b d2 4c 3f cf b3 4a 97 62 c9 da 35 b4 47 05 ee 89 82 e2 50 88 ea 18 9e eb 25 01 2c 0f 6c 10 3f cb 41 ae ce bd 2a f5 47 2f 63 25 6c f4 24 e0 f0 a6 17 59 62 bb 9a f2 07 b5 66 83 26 8d 67 20 85 83 7b 82 87 b9 1d b6 65 61 Data Ascii: ,8q;oiymFq*PEWRO;KIn\> 'ZU!eQJlktE7$t#v1K=j@+xx.ELN1fx^,eGd-Y;k-PfGPkL?Jb5GP%,I?A*G/c%l$Ybf&g {ea
2022-10-03 14:15:44 UTC	647	IN	Data Raw: a4 86 a7 e0 3e 1a f4 3a f8 9d f5 7b 1c f9 6f e0 bf 66 b2 d7 19 0b b7 b9 46 11 46 00 8d 61 40 16 38 d1 45 11 10 0e 80 0d a9 af 52 aa 14 1c ec 03 20 9a a6 95 09 4a 1a 1a 12 4e 88 b0 45 b8 c9 5b e0 6d a4 ca 64 e4 10 c7 11 1d b4 3d 5a 82 b4 1d 4e fa 9e 5c 8b 1d 65 86 b5 96 7c 1d f7 0b 01 e4 39 8f 2b 93 cd 2f e0 6c d6 32 e3 23 0c d0 45 0c 4e 56 d2 d6 0a 14 17 01 22 e2 c0 03 d5 43 1d 8f e8 d7 81 97 b0 af 3a 9a d8 56 ec ca fc d7 ee 1e 72 2c 74 d6 58 9b 6b 6b 9c 29 95 3d 8f 3c b6 72 9e 94 08 15 6b 4a f4 da 9b d3 e7 ae 4a d7 96 8d 9c 59 b3 37 f6 ad 8c 9a 2c de 37 0f 2a 66 2f 1d 92 6c 88 91 22 82 29 e4 32 2c 8e bc 43 7f 5e 30 a6 34 45 00 95 a5 07 4e b5 d3 70 b5 b4 47 1b 19 c4 e7 21 cb 4e 6c 3f 73 8a d6 ea 29 9b 23 15 d3 88 95 78 2a 18 e8 56 9d df 77 21 e8 4f 4a d0 Data Ascii: >:{ofFFa@8ER JNE[md=ZN\e|9+/l2#ENV"C:Vr,tXkk)=<rkJJY7,7*f/l")2,C^04ENpG!Nl?s)#x*Vw!OJ

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	663	IN	Data Raw: 9b 35 b1 ee 5d ac 96 b8 fd de 2b 38 21 8a 56 a4 48 6a c0 75 15 dc 81 a4 b7 7f 23 b2 49 a1 2b 4b b8 55 21 f8 fd fd e5 8d 9d c5 be 43 1a b8 93 64 85 ed 6d 2e 61 92 4b 99 62 81 42 33 c4 b1 4f 22 31 3b 54 3b a9 fc f5 b2 e4 d6 66 4e da e1 c9 8f 76 92 fe 49 0d e6 51 ad bd bd b6 32 e2 cb 07 6f 6f 24 84 5b d2 48 8c a6 53 c9 92 e2 dd a6 ed 02 0a 8d 96 95 ff 00 13 69 1f 62 f5 fe 09 e6 bd f1 fd d5 69 96 8f f5 8d c7 21 7d e3 f6 78 cc 0e 68 c1 2c 52 e5 a2 26 46 8e 69 62 68 0d c4 02 a9 24 32 22 35 01 12 1a 6a 7f f6 2e af 63 9f f3 ae f7 3b 61 91 c8 db 5a 3b ab c3 77 7c e8 05 e6 6e e2 47 17 12 90 3d ef 2c 86 42 ae c7 e2 45 75 0b 77 dd bc 0e fb f7 6b 42 df e3 b9 8f 2f c1 c1 f5 18 79 31 dd c6 71 25 ca c9 72 49 94 72 1e d2 26 24 2d 76 d8 37 f6 eb 57 f6 0e a2 d7 b3 7f 26 91 Data Ascii: 5]+8!VHju#I+KU!Cdm.aKbB3O"1;T;fNvIQ2oo$[HSibi!}xh,R&Fibh$2"5j.c;aZ;w\|nG=,BEuwkB/y1q%rIr&$-v7W&
2022-10-03 14:15:44 UTC	679	IN	Data Raw: 02 f7 2e 21 e6 14 90 41 a3 d1 87 c3 4f 11 b9 7c 79 6d 4d 1e a8 b9 e3 7c 97 c7 af a0 82 e6 d3 29 15 c4 57 49 ce dc c7 20 2c c8 4d 2b c6 bc 87 e6 06 96 0b fb 2a fc 96 04 9e cc 8f 68 99 c9 15 a8 6d b8 9f cb 5a 0a c4 8b 59 e1 35 a2 04 f8 b3 1a e8 0b 1a 88 69 e2 20 d1 d4 d0 74 e4 41 d6 88 31 1c 4a c0 f3 ad 52 9e d2 5e bf d9 a2 d9 85 77 8c 0f f1 10 4d 3f 80 d6 30 c3 e4 9d 7d c2 45 a7 5a 71 23 61 f3 db 4d 01 81 af dd 2e 19 8f 19 6a bf 05 e3 d6 bd 77 a6 b4 05 23 cb 92 ba 63 50 25 7d be 02 82 bf 86 b4 86 0f 49 7f 31 00 14 a9 27 e6 29 a2 83 c4 47 d6 ca 7f f4 45 07 c5 b7 af cb 58 dc 44 9b 97 2e 0b 44 46 d4 af 32 7e 54 db 44 dc 45 77 42 f5 8c 1a f5 af 23 4d 00 71 1c 17 25 94 0e ca 1a 7a 88 98 ff 00 71 3a 26 84 3b 14 b2 d2 9d a0 95 1f ca 84 7f 7e 80 38 a2 42 Data Ascii: .!AO|ymM|)WI ,M+*hmZY5i tA1JR^}swM?0}EZq#aM.jw#cP%}I1')GEXD.DF2~TDEwB#Mq%zq:&;~8B
2022-10-03 14:15:44 UTC	695	IN	Data Raw: 8a 49 78 cd 32 8e 53 a4 64 b3 15 63 ed 6a 81 c4 03 5a fa 6b 70 fa 11 78 99 3e d6 4c cc 42 de 18 fe 8e dd 25 1c ec 24 bc 9b 94 28 c8 07 fd 4c 4f ce 40 4f 52 43 11 b6 fb ec 34 ad 22 16 5f 25 cf c2 b1 f1 65 bc a1 7f d7 de 47 71 8a c3 f6 0b c3 89 b7 31 5e ac 57 2c c3 81 99 e3 ee 01 14 8a 0b fa ed d7 e5 3b 44 68 86 af 16 d2 f0 0a 6c e5 9f 67 24 97 d1 03 3d fb cc b3 77 91 12 16 81 26 ac 5b c4 ab 4e 5b 6c a0 7e 15 df 52 55 6c 19 71 c3 7c 76 27 78 b6 22 f3 33 91 7a dd 63 ee 31 98 f9 4c f3 45 25 cc b0 09 e4 99 b9 c8 04 71 86 1d ba 9a 00 d2 7a 74 d2 e6 bf 05 b1 34 be 0d 55 7c 59 97 24 32 3d c8 ee 31 9d a7 b6 58 0f 77 b4 55 58 19 3d ac 01 63 42 00 34 a0 03 ae b9 3d b6 68 a7 ac 85 e4 b9 7b 7b 7e 38 cb 5c 1e 42 3c 2c 48 ea 97 96 f2 f0 2e ca 28 d3 13 19 90 c6 41 27 6a Data Ascii: lx2SdcjZkpx>LB%$(LO@ORC4"_%eGq1^W,;DhIg$=w&[N[l~RUlq|v'x"3zc1LE%qzt4U|Y$2=1XwUX=cB4=h{{~8\B<,H.(A'j
2022-10-03 14:15:44 UTC	711	IN	Data Raw: 31 0e e2 d9 9a f3 68 e1 f7 48 21 66 0a 14 d0 91 c5 8f 5e 9a 9b b3 43 3c 8e a5 bb c6 71 9e 2d 73 67 2c b7 b7 79 21 2a dc 34 12 0b 24 41 db e2 c8 0a ca b2 05 65 22 9b 80 4f 5f 4d 25 b2 31 a9 93 91 a5 5b 62 ac e5 8e 48 ec 72 f7 77 b0 f7 3b a2 3b 93 11 96 ab b0 1b 46 1c 8a 0f 89 ae a3 6c ac a7 14 c1 33 e2 39 cd f5 38 d9 56 63 69 23 3b 5a 9a db a7 3f e6 35 e2 63 35 f5 aa fe 7a 35 cb f2 68 15 0e 45 66 77 b5 ca 25 9e 28 31 d8 33 73 04 fc 0b 22 37 c3 e0 77 d7 44 ab 08 d3 22 e4 71 b2 88 5e e6 cf b7 70 91 ab 76 2a ff 00 d2 e5 e8 39 16 1c 57 7f 51 b6 83 a9 93 60 b8 af 67 b6 ed c6 4c 31 b7 13 24 82 36 2c bc 6a 46 c6 83 a9 e8 69 a1 b1 b4 1e 49 2c 32 26 21 7b 64 8e 21 76 91 66 04 25 18 8a 54 91 4e 47 a7 ea 07 59 b0 32 05 c6 02 df 24 e8 93 5c db cb 61 33 05 bc 92 e4 bf Data Ascii: 1hH!f^C<q-sg,y!*4$Ae"O_M%1[bHrw;;Fl398Vci#;Z?5c5z5hEfw%(13s"7wD"q^pv*9WQ`gL1$6,jFiI,2&!{ d!vf%TNGY2$\a3
2022-10-03 14:15:44 UTC	727	IN	Data Raw: 16 ad 2c 0d 8e c4 dd 35 e0 b8 0c 38 27 29 02 86 40 fc 81 21 3d c3 d6 9a 95 eb 5c b6 50 9f fa 92 70 9e 84 2b 9c 57 d2 c1 02 62 fc ab 13 6b 36 5a 07 97 f6 2b de f0 81 9c 2f 3e e1 92 49 25 4e 45 08 ac 6f bf af a9 d3 55 a9 d5 6c 2c a3 26 8f 2b 90 f2 1c 76 4b 0f 6b 67 89 67 82 c9 ef e5 c8 c7 6b 1d b4 51 2c 09 bb 40 cb 11 75 7d c2 6c c2 a0 6c 06 bb 55 2b 56 9b 19 42 66 b5 e1 f9 69 6d b1 b6 b6 39 8c 1d be 25 ae a1 88 b4 a2 dd 19 e6 41 41 dc 96 70 cf ea a0 93 b3 1e a4 8a ed c9 9f 1a 76 9a b0 55 86 e1 9a f2 fb 2d 23 e5 12 de 2b 28 ed e6 ba 37 b8 d8 ad ed cc d6 cf 31 89 a3 8d e4 0e 91 d3 97 13 45 0f c7 f9 b7 d1 6a 2b 28 b3 d8 db fc 47 c9 de 52 96 78 df 15 c8 61 71 8b 2b 5a c3 71 70 80 42 52 11 4e 5c 95 77 06 9b 35 68 47 af a6 bc bc d8 ac b5 90 52 d6 9d 0b e7 d5 dd Data Ascii: ,58')@!=\Pp+Wbk6Z+/>I%NEoUl,&+vKkggkQ,@u}llU+VBfim9%AApvU-#+(71Ej+(GRxaq+ZqpBRN\w5hGR
2022-10-03 14:15:44 UTC	743	IN	Data Raw: 58 d7 fc d2 15 5f 9e 8d 6b 6b 6c 17 0b 72 bb 3b 7d 73 9b 81 3a dd 5b 30 e5 07 66 5e 5e d2 36 ab 0d 9a bf 01 4f c4 ea f4 ea 2d ec 4a d9 bc 22 2c 96 36 6e c5 a3 81 ac 27 6d 96 e6 10 22 7a 91 b8 6e 1b 38 3f e6 07 5d b5 aa ae c4 5d 9b 06 dc 5a 5d 2c 64 c8 91 5f c7 1d 01 7e 34 71 f8 a2 d2 bf 97 f0 d3 00 8d 19 88 02 8c 8c b0 03 b2 a1 e6 03 7c c6 d4 23 58 c8 8d 35 ac 2e e6 78 66 12 ce de a7 fa 6c 29 d0 73 00 d4 7c 8e b4 80 8e 25 bf b7 67 6b 9b 76 99 29 56 92 d3 76 50 7a 92 80 d4 ff 00 e5 fe 1a c0 82 4a 5e f7 a3 32 da 5c 25 ec 2a 78 ba ff 00 3a d3 d1 87 55 3f 26 d1 90 41 10 dd 40 93 73 b7 43 0c c0 fb d4 ee a0 1f f1 0e 8d f9 6f f8 6b 01 b3 81 d5 a4 32 17 48 a7 24 93 71 b8 53 ff 00 60 fc ce 9a 44 6c 75 6c a7 66 12 77 77 3e e0 ea 7f f8 fe fd 34 84 95 f5 17 16 e0 3d Data Ascii: X_kklr;}s:[0f^^6O-J",6n'm"zn8?]]Z],d_~4q|#X5.xfl)s|%gkv)VvPzJ^2\%*x:U?&A@sCok2H$qS`Dlulfww>4=
2022-10-03 14:15:44 UTC	759	IN	Data Raw: cf 66 31 78 ac 96 1e e3 2b 74 56 67 6e c5 9a dc 49 fd 25 a8 24 c9 24 ec c5 c5 3d 03 57 e1 aa 57 b3 6e 30 9e 85 ab 92 d5 51 25 5f 35 0d ae 5d 56 cd 2f be 92 fe e1 7e 9e e6 e6 1b a9 23 31 da b2 13 d0 b0 60 1a 94 d8 53 d3 e3 aa 62 c9 75 0c 86 4b 37 a4 94 fb 3c 3f 8e 59 5b 45 1d 99 9a ca 25 df 1f 96 73 dc e7 76 01 3c d8 4e 55 0f 4a 29 53 d7 a1 d7 73 b5 ac e5 93 89 62 7c 4a d3 13 8f c7 de f9 1d ce 2b fd 33 9b bd bd 31 5c 5d f1 8a 09 ae 8b 3f 25 06 7b 62 6a c4 7b 8a f3 a8 e8 5b 7d 26 7b 3b 3e 29 ca 2f 5c 6d 13 2e bc a7 39 8d 6c 8b be 46 4b 88 d0 a4 96 a1 23 55 47 69 5a 9c 52 55 34 aa 82 2b 56 af a1 1a 87 a6 b6 6a 4a aa 6a 49 82 0f 22 ce 5b de 5a 60 b0 71 46 5e e4 fe fd 65 72 6e 71 c8 d3 72 5e 4d df b8 ed 31 64 34 3e e9 08 1e 83 54 51 f2 74 d3 a9 c8 bc c1 fe dd Data Ascii: f1x+tVgnI%$$=WWn0Q%_5]V/~#1`SbuK7<?Y[E%sv<NUJ)Ssb|J+31\]?%{bj{[}&{;>)/\m.9lFK#UGiZRU4+VjJl"[Z`qF^ernqr^M1d4>TQt
2022-10-03 14:15:44 UTC	791	IN	Data Raw: 1d 6e a5 c8 33 f6 64 b5 95 52 89 40 7f 58 15 e2 7d 0e a6 f2 d9 4b 4c 0a c5 e6 78 f0 90 2a 5c bc 0d 2c e9 6f db 8e e9 16 ad 0c 60 92 19 40 ad 77 1b 57 5c f5 bd 99 5a e5 e2 48 87 19 7d 93 61 1e 56 ff 00 f7 5b 69 a1 32 db 48 8a 12 e1 52 80 9a 90 05 00 df e2 34 6d 67 e1 0e ad 3b 80 72 89 68 f7 d0 5d 4d 7b 17 fa 76 da 37 86 0c 7b 30 29 70 ce 42 ae fe c2 08 61 d0 1e be 87 a6 ab 8e 5e 8f 71 5b 01 e5 3c 9b 07 8b b7 bc 95 ee 0d a6 36 cc 91 1d f2 80 d6 e2 49 00 26 28 a2 56 42 e3 6d de ab bf 5f 8e ba 2b d6 b5 b6 d5 92 b5 dc e8 49 b0 f3 8b 7b eb 59 ed b0 d7 f7 6b 69 68 8f 1b 0b 84 12 4c b2 c8 8b 24 6d 1a f7 9c 2c 67 96 c1 5c 80 37 3f 0d 51 f5 f8 bf b8 b2 7f 21 ab 5f 2d b9 82 69 cd c6 6a d2 fa fa 10 e2 4f 1f 0b 23 71 60 d4 4e dc 81 01 03 8d 2b 5a fc be 3a 9d b0 56 36 Data Ascii: n3dR@X}KLx*\,o`@wW\ZH}aV[i2HR4mg;rh]M{v7{0)pBa^q[<6I&(VBm_+I{YkihL$m,g\7?Q!_-ijO#q`N+Z:V6
2022-10-03 14:15:44 UTC	875	IN	Data Raw: 8d c4 9d 18 6c e7 70 85 e2 64 ed 45 9d d9 4b 7b 0c 6c 33 08 45 86 3d 2d e5 a3 48 ec b1 96 ed 31 43 51 d6 95 3f 1f 86 bb 28 eb 32 b7 3b 1d d0 ec 78 2c 0c 57 58 29 be be 49 37 2e ab 28 89 e0 8f b6 fc 55 1f 80 a8 35 35 a1 34 db 7a ea ae f6 e2 1e 7a 97 2b e2 ed 2c e7 22 21 82 e6 ce fd c2 c9 22 c2 a1 5e 39 88 76 a8 6a 03 50 0a 85 3a e6 b6 9a 0b 76 1e 7b 9b 49 f0 7d db 7b 1b 19 6f a4 2b 10 7e d9 90 f1 a9 af 2f 6a b1 53 42 d4 af ba a0 ef a6 a3 aa af d4 d7 d6 a6 63 92 c8 e5 25 92 ff 00 31 9b c7 59 59 e1 ac 61 54 4c 72 c5 2d a5 cc 80 8f 71 8c c2 11 50 8d ba 90 c4 53 6d 4f d5 0b 4d 59 1e 4d 6e 58 65 1e 39 e4 37 f6 77 51 19 24 10 4b df c5 2c 1d e8 22 84 50 85 8c bc 6b bf 1a 9f d7 42 de a7 42 ea c9 68 19 6b 62 3d d7 90 35 ad f4 f9 0c 9c a2 e1 30 81 fe 9e d1 4c 83 bf Data Ascii: lpdEK{l3E=-H1CQ?(2;x,WX)I7.(U554zz+,"!"^9vjP:v{l}{o+~/jSBc%1YYaTLr-qPSmOMYMnXe97wQ$K,"Pk BBhkb=50L

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	891	IN	Data Raw: b6 92 d8 dc 15 95 c0 4e 4a 02 82 53 a1 a8 35 a9 3d 36 d7 3f b5 a6 d4 9c 56 ec 64 ae e5 4b 37 e4 2d 0a 86 b8 c8 df 4b 20 95 43 c5 3b 11 09 53 5e 4d ec 64 3d 68 29 4a e9 b1 d7 e8 4a 96 56 71 06 7b 3f 86 cd e4 59 67 bd c6 5d 4e d0 c1 1a c8 cd 77 24 76 d0 96 ae eb 0c 8e 54 57 ad 07 22 7e 67 a6 ba 96 75 55 0c bd 71 2a ea 01 bf 96 0b 88 cc 59 ac 9d b5 8d e6 1d 42 5a e4 27 46 91 c0 8d 9a b1 9e 5e c9 40 00 6f d4 fa 03 a3 44 d6 cb 46 0b 56 bb a7 a9 77 fb 71 71 e5 19 6f aa c5 8f 30 c3 58 f8 fa 3a 1b a5 bb b9 92 38 67 7e 5b 15 44 8c c9 55 1f cd 40 00 27 e7 ae 3e e5 6b 56 be d7 2c 7a d9 b5 0f 62 d7 73 96 ca e6 f2 12 78 df 8a 60 ec e6 0a 25 89 ef 31 ad 2b 5a b7 16 2c 64 13 5c 85 24 d0 8d ce a6 92 c5 5e 56 62 2b da ee 2a a1 1b af 8e c1 91 f1 9c 5d 9e 43 2d 94 b1 37 d3 Data Ascii: NJS5=6?VdK7-K C;S^Md=h)JJVq{?Yg]Nw$vTW"~guUq*YBZ'F^@oDFVwqqo0X:8g~[DU@'>kV,zbs x`%1+Z,d\$^Vb+*]C-7
2022-10-03 14:15:44 UTC	907	IN	Data Raw: 91 a2 b2 68 64 1b d1 67 2c cd 2a 81 ca 80 81 5d b9 1f 5d 17 69 f1 a9 bd ff 00 1b 9f 49 fd b3 fb fb fb 2c 70 e3 33 b2 59 c9 8b b4 37 11 1c 85 fc 72 c7 73 df 42 bf d0 02 05 6e 74 62 6a e2 a0 fc 75 bd 8d 1e 87 5b bb 1a 58 fa 3b 1f 93 c0 79 b5 2f 70 d7 42 e9 52 48 e4 6b 69 23 95 ad d2 68 ea e2 93 71 2a ac 84 13 bb 6d b6 a9 4b ce e7 af 4c 95 ba 94 c9 16 d7 e3 17 67 fb 5b 5d 5d c5 69 66 c6 47 38 db 83 14 d0 b3 3f 26 94 88 19 55 d0 16 a9 35 f5 e9 aa 4a 63 2b a0 fc d9 9c fc 80 4d 67 92 4c ae 3d c5 25 ba 45 21 b8 b1 ab 07 11 a7 3f 6f c4 1e 43 e1 a5 e2 31 94 c7 f7 2a 65 f2 5c 9e 03 35 6b 1e 2a fa ca 78 db 18 d7 dc 27 b0 b8 85 66 11 45 74 b7 0e 10 ab bf 2d 85 58 30 fd 5b ef a7 aa 4d 12 bd 9d 37 d8 9d 69 9c a9 b2 c6 64 ac 2c ac 32 f9 8c cd fc d7 17 b1 d8 c3 24 2f f5 Data Ascii: hdg,*]]il,p3Y7rsBntbju[X;y/pBRHki#hq*mKLg[]]ifG8?&U5Jc+MgL=%E!?oC1*e\5k*x'fEt-X0[M7id,2$/
2022-10-03 14:15:44 UTC	923	IN	Data Raw: f2 c9 2d 27 38 bf db ae b3 42 61 78 86 19 81 22 01 24 d2 ff 00 4e d8 b8 ad 0d 19 88 24 d4 01 a4 57 b4 9c d6 ec da d6 4d b7 a1 6a be b1 cf 65 6f ef e2 b6 fb af 6c 96 ed e2 50 db 0b 49 31 d6 e0 dc 5b 97 94 8b 64 48 ae a5 11 c3 13 90 51 95 b7 af b8 57 72 ef b1 5d 74 67 75 7b 09 a5 a9 6c cc f9 3e 4d fc 7a f7 19 69 e5 3e 3f 9d ce db e2 17 17 8a b3 6c 6b a4 92 ab c3 25 ac a1 d2 43 24 91 1f 62 95 64 7a 13 4a 92 36 d4 6f d8 af 2d 9c 0d f9 b4 aa 2a 7e 19 8b 88 f9 67 8e 47 e6 9e 2b 0c 16 8c 61 0c 44 25 6c 0e 3d 23 12 ba 29 56 08 8a 24 43 b7 35 35 61 5a ed 5e ba e5 a5 94 a6 1c 59 31 d9 4b 89 3e d8 f0 df 21 fb 7d 9b f0 af 29 f2 7f b6 38 6c 15 ac fe 2b 1d e4 18 fb 7b 59 de da ee d2 58 e3 6e db 2c 4e d5 4e 43 75 23 f5 1a d2 bd 74 d9 97 ad a8 b6 e7 56 2a d6 d6 86 8a 1f Data Ascii: -'8Bax"NWMjeolPl1[dHQWr]tgu{l>Mzi>?lk%C$bdzJ6o-*~gG+aD%l=#)V$C55aZ^Y1K>!})8l+{YXn,NNCu#tV*
2022-10-03 14:15:44 UTC	939	IN	Data Raw: c4 b3 37 e5 ae 2c fd ba 63 fa b3 a7 1f 5d d8 b7 e3 f0 5e 47 e7 36 eb 75 29 87 03 e3 1c 96 41 3c c8 f1 c6 c9 f1 54 66 ac 87 e6 4d 3f cd e9 ae 4a e2 cd da d6 da 54 ad af 4c 5a 2d 59 69 86 eb c6 3c 35 59 7c 62 d1 2e 32 0e 0a cd 9d bb 1c e4 35 ff 00 e8 97 6a 0f c2 83 f1 d7 ab 83 a7 4c 6b 44 71 e4 ca ef b9 4c c8 65 6f b2 12 49 2d ed cb 5c c8 37 12 31 24 ed f9 50 7e 03 5d 89 24 4a 40 53 dc 39 14 56 2f 4d c3 74 15 f9 0f 5d 13 11 54 ce c5 6b b2 9f 88 34 27 e4 00 3a 30 00 94 76 aa aa 59 94 86 ad 57 d4 9f fe 3e 5a 06 14 b6 f3 4a 68 76 8c 9e bc 45 47 fd 9a d3 01 2a 7e 4d e6 18 2f 11 89 c5 dc cd 25 da 27 75 2d 50 17 77 1d 7f 05 02 9d 4d 07 cf 5e 67 6f f6 15 c5 a7 90 ec 62 df 71 72 de 73 9d fb 6d 98 cf de f8 e5 d6 0b c4 ed e7 b6 93 eb af 8c 70 34 eb dd 53 dc 09 23 77 Data Ascii: 7,c]^G6u)A<TfM?JTLZ-Yi<5Y|b.25jLkDqLeol-\71$P~]$J@S9V/Mt]Tk4':0vYW>ZJhvEG*~M/%'u-PwM^gob qrsmp4S#w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.6	49992	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:06 UTC	11526	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_tosys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "2982-5b252e7c40940"
2022-10-03 14:17:06 UTC	11527	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:06 GMT Server: Apache Connection: close ETag: "2982-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.6	49993	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:07 UTC	11527	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "4356-5b252e7c40940"
2022-10-03 14:17:07 UTC	11527	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:07 GMT Server: Apache Connection: close ETag: "4356-5b252e7c40940"

Copyright Joe Security LLC 2022

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.6	49994	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:07 UTC	11527	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_facebook.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "28a-5b252e7d34b80"
2022-10-03 14:17:07 UTC	11528	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:17:07 GMT Server: Apache Connection: close ETag: "28a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.6	49995	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:08 UTC	11528	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_twitter.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "3db-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.6	49996	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:17:08 UTC	11528	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "16b4-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49739	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:42 UTC	275	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics_sp.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	311	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:43 GMT Server: Apache Last-Modified: Wed, 28 Oct 2020 08:52:20 GMT ETag: "22fb8-5b2b747fbd900" Accept-Ranges: bytes Content-Length: 143288 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:43 UTC	361	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	839	IN	Data Raw: 9b 9f e0 09 6a 5b 8f d6 5e 3d c2 d8 63 63 6c 2d 9c 62 3c 75 cd a4 f2 f7 16 55 65 8d 8a 29 0b c5 87 6b f4 94 df 99 23 a1 e3 ad 92 ab ed 19 a6 fc 68 0c 78 2f 22 b4 68 66 86 e6 69 2e 1d 4b 45 23 ca 48 40 56 16 e1 2d c4 a9 05 59 79 16 61 08 60 39 05 0a c7 4b c9 2d 12 14 fa 19 af 66 c7 5e c3 32 7d 0a 59 ce dc 31 3f 54 2e a3 11 34 8c e5 9a 38 87 10 5a 30 8d c5 aa 37 d9 47 bc 95 ba a3 5f f9 86 1b 3b fd 1e e6 26 bd bf b7 bb c5 e3 ac d2 79 17 29 35 ac 29 14 a1 e6 9d 39 a2 bb 2a 29 25 14 2b 31 5a d3 71 41 5d 6a a4 b4 ae e1 74 70 01 ca 43 e3 d7 f0 5d 3c 18 32 d6 f6 96 8c f6 72 de c0 b1 b2 c6 b0 2b 39 82 d9 61 95 24 a2 0e 45 c5 00 0a 08 a1 1c 75 64 af cb 71 61 c8 5a 5c 6d 85 98 86 ea ca e2 5e fd fd b7 d4 5d 47 1d b2 ad ec d5 8b 9c 93 06 81 22 74 3c 48 a1 99 98 a8 d8 Data Ascii: j[^=ccl-b<uUe)k#hx/"hfi.KE#H@V-Yya`9K-f^2}Y1?T.48Z07G_;&y)5)9*)%+1ZqA]jtpC]<2r+9a$EudqaZ\m^]G"t<H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49744	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	278	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo_footer.png HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:43 UTC	312	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:43 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "e43c-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 58428 Connection: close Content-Type: image/png
2022-10-03 14:15:43 UTC	394	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 ca 00 00 01 18 08 06 00 00 00 dc 6a b6 f8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 e3 de 49 44 41 54 78 da ec bd 09 80 5d 45 95 ff 5f cb dd de d2 7b a7 bb 93 ce 4e f6 b0 27 01 c2 16 02 02 82 80 3b 23 fa 43 c7 51 61 c6 19 77 1d 9c f9 cd fc 32 38 32 e8 1f 19 71 43 65 54 74 46 9c 11 06 dc 10 95 c5 b0 04 08 84 90 10 c2 9e 7d ed f4 de 6f bd 4b 55 9d 7f d5 bd ef 75 1a 44 4d 27 dd 9d a4 39 1f a8 dc 7e db dd ab be f7 54 9d 3a 87 10 04 41 10 04 41 10 04 41

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49773	74.125.143.154	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	312	OUT	POST /j/collect?t=dc&aip=1&_r=3&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942&jid=974897442&gjid=761990059&_gid=1735943631.1664838942&_u=YEBAAUAAAAAAAC~&z=1809022200 HTTP/1.1 Host: stats.g.doubleclick.net Connection: keep-alive Content-Length: 0 sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Content-Type: text/plain Accept: */* Origin: https://kawanakajima.co.jp X-Client-Data: CK61yQEIh7bJAQiltskBCMS2yQEIqZ3KAQiTocsBCIurzAEI7bvMAQiAvcwBCLLBzAEIxcHMAQjWwcwB Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:43 UTC	313	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: https://kawanakajima.co.jp Strict-Transport-Security: max-age=10886400; includeSubDomains; preload Date: Mon, 03 Oct 2022 14:15:43 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Last-Modified: Sun, 17 May 1998 03:00:00 GMT Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Content-Type: text/plain Cross-Origin-Resource-Policy: cross-origin Server: Golfe2 Content-Length: 7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-10-03 14:15:43 UTC	313	IN	Data Raw: 31 67 63 6f 2e 75 6b Data Ascii: 1gco.uk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49763	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	393	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:44 UTC	851	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:44 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "31e7-5b252e7c40940" Accept-Ranges: bytes Content-Length: 12775 Connection: close Content-Type: image/jpeg

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	852	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	875	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:44 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "4356-5b252e7c40940" Accept-Ranges: bytes Content-Length: 17238 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:44 UTC	950	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:26 UTC	4	OUT	GET /collinesredshare666.htm HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:34 UTC	5	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 14:15:27 GMT Server: Apache X-Powered-By: PHP/7.4.5 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: private, no-store, no-cache, must-revalidate, max-age=0 X-Accel-Expires: 0 Link: <https://kawanakajima.co.jp/wp-json/>; rel="https://api.w.org/" Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-10-03 14:15:34 UTC	5	IN	Data Raw: 36 31 37 63 0d 0a Data Ascii: 617c
2022-10-03 14:15:34 UTC	5	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 73 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 7 3 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 21 2 8 49 45 20 37 29 20 7c 20 21 28 49 45 20 38 29 20 5d 3e 3c 21 2d Data Ascii: <!DOCTYPE html>...[if IE 7]><html class="ie ie7" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if IE 8]><html class="ie ie8" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if !(IE 7) | !(IE 8)]><!-
2022-10-03 14:15:34 UTC	13	IN	Data Raw: 21 74 2e 73 75 70 70 6f 72 74 73 2e 66 6c 61 67 2c 74 2e 44 4f 4d 52 65 61 64 79 3d 21 31 2c 74 2e 72 65 61 64 79 43 61 6c 6c 62 61 63 6b 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 44 4f 4d 52 65 61 64 79 3d 21 30 7d 2c 74 2e 73 75 70 70 6f 72 74 73 2e 65 76 65 72 79 74 68 69 6e 67 7c 28 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 72 65 61 64 79 43 61 6c 6c 62 61 63 6b 28 29 7d 2c 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 3f 28 61 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 44 4f 4d 43 6f 6e 74 65 6e 74 4c 6f 61 64 65 64 22 2c 6e 2c 21 31 29 2c 65 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 6c 6f 61 64 22 2c 6e 2c 21 31 29 29 3a 28 65 2e 61 74 74 61 63 68 45 76 65 6e 74 28 22 6f 6e 6c 6f 61 64 22 2c 6e 29 2c 61 2e Data Ascii: !t.supports.flag,t.DOMReady=!1,t.readyCallback=function(){t.DOMReady=!0},t.supports.everything||(n =function(){t.readyCallback()},a.addEventListener?(a.addEventListener("DOMContentLoaded",n,!1),e.addEventListe ner("load",n,!1)):(e.attachEvent("onload",n),a.
2022-10-03 14:15:34 UTC	20	IN	Data Raw: 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 22 20 63 6c 61 73 73 3d 22 68 6f 6d 65 22 20 3e 3c 73 70 61 6e 20 70 72 6f 70 65 72 74 79 3d 22 6e 61 6d 65 22 3e 54 4f 50 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 70 6f 73 69 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 31 22 3e 3c 2f 73 70 61 6e 3e 20 26 67 74 3b 20 3c 73 70 61 6e 20 70 72 6f 70 65 72 74 79 3d 22 69 74 65 6d 4c 69 73 74 45 6c 65 6d 65 6e 74 22 20 74 79 70 65 6f 66 3d 22 4c 69 73 74 49 74 65 6d 22 3e 3c 73 70 61 6e 20 70 72 6f 70 65 72 74 79 3d 22 6e 61 6d 65 22 20 63 6c 61 73 73 3d 22 34 30 34 20 63 75 72 72 65 6e 74 2d 69 74 65 6d 22 3e 34 30 34 3c 2f 73 70 61 6e 3e 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 Data Ascii: ef="https://kawanakajima.co.jp" class="home" >TOP<meta property=" position" content="1"> > <span property="name" cl ass="404 current-item">404<meta property
2022-10-03 14:15:34 UTC	28	IN	Data Raw: 6f 2e 6a 70 2f 77 6f 72 64 70 72 65 73 73 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 6b 61 77 61 6b 65 6e 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 5f 74 77 69 74 74 65 72 2e 73 76 67 22 20 61 6c 74 3d 22 54 77 69 74 74 65 72 22 3e 3c 2f 61 3e 0a 09 09 09 09 09 3c 2f 6c 69 3e 0a 09 09 09 09 09 3c 6c 69 3e 0a 09 09 09 09 09 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 74 61 67 72 61 6d 2e 63 6f 6d 2f 6b 61 77 61 6b 65 6e 31 33 34 31 2f 3f 68 6c 3d 6a 61 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 72 65 6c 3d 22 6e 6f 6f 70 65 6e 65 72 20 6e 6f 72 65 66 65 72 72 65 72 22 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 6f 72 64 70 72 Data Ascii: o.jp/wordpress/wp-content/themes/kawaken/images/icon_twitter.svg" alt="Twitter"> <a href="https: //www.instagram.com/kawaken1341/?hl=ja" target="_blank" rel="noopener noreferrer"><img src="https://kawanakaji ma.co.jp/wordpr
2022-10-03 14:15:34 UTC	30	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:15:34 UTC	30	IN	Data Raw: 61 33 0d 0a Data Ascii: a3
2022-10-03 14:15:34 UTC	30	IN	Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 6f 72 64 70 72 65 73 73 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6a 73 2f 77 70 2d 65 6d 62 65 64 2e 6d 69 6e 2e 6a 73 3f 76 65 72 3d 35 2e 34 2e 31 31 27 20 64 65 66 65 72 20 63 68 61 72 73 65 74 3d 27 55 54 46 2d 38 27 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <script type='text/javascript' src='https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-embed.min.js?ver= 5.4.11' defer charset='UTF-8'></script></body></html>
2022-10-03 14:15:34 UTC	30	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:34 UTC	30	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49788	172.217.168.35	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:43 UTC	572	OUT	GET /ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-63283810-1&cid=189789998.1664838942 &jid=974897442&_u=YEBAAUAAAAAAAC~&z=640512449 HTTP/1.1 Host: www.google.co.uk Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 X-Client-Data: CK61yQEIh7bJAQiltskBCMS2yQEIqZ3KAQiTocsBCIurzAEI7bvMAQiAvcwBCLLBzAEIxcHMAQjWwcwB Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:44 UTC	574	IN	HTTP/1.1 200 OK P3P: policyref="https://www.googleadservices.com/pagead/p3p.xml", CP="NOI DEV PSA PSD IVA IVD OTP OUR OTR IND OTC" Timing-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Date: Mon, 03 Oct 2022 14:15:44 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Content-Type: image/gif X-Content-Type-Options: nosniff Server: cafe Content-Length: 42 X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-10-03 14:15:44 UTC	574	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 ff ff ff 21 f9 04 01 00 00 00 00 2c 00 00 00 00 01 00 01 00 00 02 01 44 00 3b Data Ascii: GIF89a!,D;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49789	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	967	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_facebook.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:45 UTC	971	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:45 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "28a-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 650 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:45 UTC	971	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 31 38 37 37 65 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 35 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#1877ef;}.cls-2{fill:#ffff;}</style></defs><title> 1</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49790	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	968	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_twitter.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:15:45 UTC	978	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:45 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "3db-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 987 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:45 UTC	978	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 31 64 39 65 65 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 33 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 67 20 69 64 3d 22 44 61 72 6b 5f 42 6c 75 65 22 20 64 61 74 61 2d 6e 61 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#1d9eef;}.cls-2{fill:#ffff;}</style></defs><title> 3</title><g id="_2" data-name=" 2"><g id=""><g id="Dark_Blue" data-na

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49791	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:44 UTC	969	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:15:45 UTC	972	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:45 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "16b4-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 5812 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:45 UTC	972	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 32 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 69 6d Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 2</title><g id="_2" data-name=" 2"><g id=""><im

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49794	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:45 UTC	969	OUT	GET /wordpress/wp-includes/js/wp-embed.min.js?ver=5.4.11 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:15:45 UTC	979	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:45 GMT Server: Apache Last-Modified: Thu, 15 Apr 2021 06:44:35 GMT ETag: "592-5bffd3258ece7" Accept-Ranges: bytes Content-Length: 1426 Connection: close Content-Type: text/javascript
2022-10-03 14:15:45 UTC	979	IN	Data Raw: 2f 2a 21 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 61 75 74 6f 2d 67 65 6e 65 72 61 74 65 64 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 63 2c 64 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 65 3d 21 31 2c 6e 3d 21 31 3b 69 66 28 64 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 29 69 66 28 63 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 29 65 3d 21 30 3b 69 66 28 63 2e 77 70 3d 63 2e 77 70 7c 7c 7b 7d 2c 21 63 2e 77 70 2e 72 65 63 65 69 76 65 45 6d 62 65 64 4d 65 73 73 61 67 65 29 69 66 28 63 2e 77 70 2e 72 65 63 65 69 76 65 45 6d 62 65 64 4d 65 73 73 61 67 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 2e 64 61 74 61 3b 69 66 28 74 29 69 66 28 74 2e 73 65 63 72 65 74 7c 7c 74 2e 6d 65 73 73 61 67 65 7c 7c 74 2e 76 61 6c 75 65 Data Ascii: /*! This file is auto-generated */!function(c,d){"use strict";var e=!1,n=!1;if(d.querySelector)if(c.addEvent Listener)e=!0;if(c.wp=c.wp||{},!c.wp.receiveEmbedMessage)if(c.wp.receiveEmbedMessage=function(e){var t=e.data; if(t)if(t.secret||t.message||t.value

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49792	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:45 UTC	970	OUT	GET /wordpress/wp-includes/js/wp-emoji-release.min.js?ver=5.4.11 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:15:45 UTC	979	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:45 GMT Server: Apache Last-Modified: Thu, 15 Apr 2021 06:44:30 GMT ETag: "363c-5bffd3205b81f" Accept-Ranges: bytes Content-Length: 13884 Connection: close Content-Type: text/javascript
2022-10-03 14:15:45 UTC	981	IN	Data Raw: 2f 2a 21 20 54 68 69 73 20 66 69 6c 65 20 69 73 20 61 75 74 6f 2d 67 65 6e 65 72 61 74 65 64 20 2a 2f 0a 2f 2f 20 53 6f 75 72 63 65 3a 20 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6a 73 2f 74 77 65 6d 6f 6a 69 2e 6d 69 6e 2e 6a 73 0a 76 61 72 20 74 77 65 6d 6f 6a 69 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 66 3d 7b 62 61 73 65 3a 22 68 74 74 70 73 3a 2f 2f 74 77 65 6d 6f 6a 69 2e 6d 61 78 63 64 6e 2e 63 6f 6d 2f 76 2f 31 32 2e 31 2e 33 2f 22 2c 65 78 74 3a 22 2e 70 6e 67 22 2c 73 69 7a 65 3a 22 37 32 78 37 32 22 2c 63 6c 61 73 73 4e 61 6d 65 3a 22 65 6d 6f 6a 69 22 2c 63 6f 6e 76 65 72 74 3a 7b 66 72 6f 6d 43 6f 64 65 50 6f 69 6e 74 3a 66 75 6e 63 74 69 6f 6e 28 64 29 7b 64 3d 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 Data Ascii: /*! This file is auto-generated *// Source: wp-includes/js/twemoji.min.jsvar twemoji=function(){"use strict";var f={base:"https://twemoji.maxcdn.com/v/12.1.3/",ext:".png",size:"72x72",className:"emoji",convert:{fromCodePoint:function(d){d="string"==typ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49801	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:48 UTC	994	OUT	GET /wordpress/wp-content/themes/kawaken/images/favicon.ico HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:15:48 UTC	995	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:48 GMT Server: Apache Last-Modified: Tue, 10 Nov 2020 03:16:46 GMT ETag: "25be-5b3b81bd74380" Accept-Ranges: bytes Content-Length: 9662 Connection: close Content-Type: image/vnd.microsoft.icon
2022-10-03 14:15:48 UTC	995	IN	Data Raw: 00 00 01 00 01 00 30 30 00 00 01 00 20 00 a8 25 00 00 16 00 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 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 00 00 01 00 00 00 01 00 00 00 01

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49810	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:50 UTC	1005	OUT	GET /wordpress/wp-content/themes/kawaken/images/favicon.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:51 UTC	1005	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:51 GMT Server: Apache Last-Modified: Tue, 10 Nov 2020 03:16:46 GMT ETag: "25be-5b3b81bd74380" Accept-Ranges: bytes Content-Length: 9662 Connection: close Content-Type: image/vnd.microsoft.icon
2022-10-03 14:15:51 UTC	1005	IN	Data Raw: 00 00 01 00 01 00 30 30 00 00 01 00 20 00 a8 25 00 00 16 00 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 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 00 00 01 00 00 00 01 00 00 00 01

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49812	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:51 UTC	1039	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:52 UTC	1040	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:52 GMT Server: Apache Last-Modified: Wed, 28 Oct 2020 08:52:19 GMT ETag: "6ed50-5b2b747ec96c0" Accept-Ranges: bytes Content-Length: 453968 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:52 UTC	1040	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c ff c0 00 11 08 01 dc 07 80 03 01 11 00 02 11 01 03 11 01 ff c4 00 bf 00 00 01 05 01 01 01 01 01 00 00 00 00 00 00 00 00 05 02 03 04 06 07 01 00 08 09 0a 01 00 03 01 01 01 01 01 00 00 00 00 00 00 00 Data Ascii: JFIFddDuckyPAdobed
2022-10-03 14:15:52 UTC	1056	IN	Data Raw: 4e ae 23 a8 cf d3 ca 77 0a 16 9d 79 1a 1a fe 3a 6e 48 d0 47 66 65 24 6e 3e 00 e9 93 00 b8 d9 88 a9 a5 35 8c 2d 4f 4f 70 24 ef ad 06 16 5d 03 03 d5 ba 91 f0 d6 31 60 b4 4a aa 15 60 55 86 cb eb bf c7 52 b1 54 76 78 d7 93 2a 9e 4e 36 50 00 d6 31 1a e2 37 81 03 32 39 32 1d b6 a6 fa c9 81 a0 24 ee 51 fd dd 08 07 e3 aa c1 26 e0 48 b8 46 dc b1 de 80 01 fd fa cd 05 31 22 7f 70 0a 2a de 87 ae b4 18 90 1e 42 05 40 35 ea df f6 e9 4c 2e 09 e3 89 e8 c0 32 fc 07 51 a0 c2 b4 0c 83 09 50 0a d5 1b 7a 91 5e bf 88 d4 5d 99 43 c2 da d8 9f 6c 81 49 f8 8a 0f ed 03 47 9b 32 48 e0 8a 24 6a 85 52 cb d0 d6 a4 fe 15 d6 76 31 29 15 99 0f b1 76 f7 30 6f d5 f9 7a e9 24 64 84 21 12 11 c9 d5 51 58 8a bf 41 f0 e8 2a 75 82 85 95 5d c3 6d 5f e5 02 9b fc c1 d0 91 58 cc 8e 63 e4 ca a4 29 db Data Ascii: N#wy:nHGfe$n>5-OOp$]1`J`URTvx*N6P17292$Q&HF1"p*B@5L.2QPz^]ClIG2H$jRv1)v0oz$d!QXA*u]m_Xc)
2022-10-03 14:15:53 UTC	1072	IN	Data Raw: 48 ae a5 87 1d 87 b8 a9 27 55 f6 08 9c 13 8f 91 5b 15 85 a5 b9 bc 91 d0 d1 64 32 f3 2a 08 a1 3e e5 23 d7 d7 41 5d 07 ee 63 33 67 2c ae 16 1b 7f dc 2f c9 b7 21 94 f2 b4 0e 47 c1 a9 6a 0b 74 fe 6a e8 f3 a8 1a b2 f0 4e cb 79 54 59 cb 44 c6 df c2 b2 c7 10 0d 11 8a 1b 7b 76 04 02 b5 26 28 54 9e b5 a1 db 49 54 96 c3 5e f6 b6 e7 62 ce d8 c3 6e 96 62 c5 68 aa 02 c9 20 88 bf b7 af bf b5 5d ff 00 1d 19 42 4b 64 39 2f ec a7 9d 99 6d e4 5f 6d 69 1c a8 a3 af 23 bf 6c 81 d7 4f cd 03 52 0d d7 09 6e 41 69 6f 0a a0 e3 c0 49 13 26 c4 fa aa 25 45 3d 74 39 20 ea c2 36 0e 89 2f 29 08 65 46 26 92 ca 1d 4d 28 76 03 f4 fe 3a 9d ec 52 a8 32 b7 f6 92 5c 06 46 e3 6e ca 43 94 99 ea 18 7a 00 a2 bd 35 09 65 52 43 f1 de db 19 1d 38 5c 48 18 10 57 ea 5c 11 c4 54 50 77 10 ff 00 66 8e a6 Data Ascii: H'U[d2*>#A]c3g,/!GjtjNyTYD{v&(TIT^bnbh]BKd9/m_mi#IORnAioI&%E=t9 6/)eF&M(v:R2\FnCz5eRC8\HW\TPwf
2022-10-03 14:15:53 UTC	1088	IN	Data Raw: ec 70 ca a9 ca e4 2f 00 54 b1 fd 12 d1 48 dc 00 41 07 5c f6 4d 68 38 d2 5f ca 66 b9 8a 08 56 53 42 25 60 0d 41 03 6a 16 a0 15 f8 eb 70 30 32 2b d6 59 48 a3 49 12 b8 26 39 01 46 e4 3a b2 9a f0 26 9b d2 ba 77 45 02 ce a7 b2 59 04 bd 59 ae 1e 49 05 c2 aa a2 15 b9 44 e0 17 6a 18 a9 c8 d4 f5 df 5a 94 80 c9 22 04 b7 b1 b5 b6 c8 5d cc d6 ae a8 4c 76 91 72 57 91 63 1c 6a 64 91 ca f5 fe 51 f9 0d 16 b9 38 41 d8 08 b9 6f ab 6b 89 04 a6 27 eb 6f 03 55 94 b9 3d 3f cb aa fa 92 07 20 8c 59 fb ab 76 b7 b8 52 ca a2 31 1d 19 cb 72 60 7d c5 40 e9 4d b4 96 c1 57 a1 95 98 63 31 99 b7 b9 b7 b3 be b6 9b 8d d0 60 b3 a0 0c 18 92 2a d5 3b 8f 86 a7 8f 0b 4d a7 b0 cd 97 af 01 f3 ab ec 06 59 6f ec de 29 e5 31 3a 4d 6a dd 5d 0f 50 69 eb 51 e9 be a5 97 13 ae a8 b6 2c 9c 5c 9a 7a f9 b7 Data Ascii: p/THA\Mh8_fVSB%`Ajp02+YHI&9F:&wEYYIDjZ"]LvrWcjdQ8Aok'oU=? YvR1r`}@MWc1`*;MYo)1:Mj]PiQ,\z
2022-10-03 14:15:53 UTC	1104	IN	Data Raw: d7 d7 7a e9 7f 29 7c 81 40 62 2f b5 5f 6f 23 09 f5 79 bb 29 9f f4 95 82 ca 7a 83 d6 80 a8 54 3d 3e 1a 4b 77 52 f2 3a aa 61 28 fe de 7d b4 85 e3 a5 d4 ee 29 58 e3 30 46 bc b7 a7 ab 45 5f 96 91 f7 eb f2 3f 10 9c 9f 6d 7c 31 4a 4b 6d 72 d6 b1 54 b2 c8 f0 44 4f cb 71 77 b5 3f 0d 0f ce 4c 75 85 90 1b c1 7c 6a ee e1 89 cd 35 dc 8c b5 6e f5 9c aa c6 9d 47 71 66 3e ba 57 dc 48 de 96 c2 d7 7f 6e 5a c6 c6 3b df d8 22 fa 08 f8 b4 d7 97 f2 35 a2 8d c0 5a 7e a6 20 fc 4b 6f a8 5f b7 67 b0 cf 0c 03 ee bc 4b 11 18 96 e7 3f e3 b8 cb e3 2c a7 b3 35 d6 47 21 c5 10 d3 8c 69 f4 d7 50 2d 3f 10 75 cc bb 16 41 8a d5 6c 7c 09 f7 ba db 15 6b e7 19 6b 7c 2b 43 1e 32 7b 28 e7 8a d2 16 b8 78 60 92 32 56 45 59 2e 1d 9d 88 e3 fc c4 eb d7 ea dd da 92 d6 a7 15 b5 6e 0a 97 da 88 ad ee 7e Data Ascii: z)|@b/_o#y)zT=>KwR:a(})X0FE_?m|1JKmrTDOqw?Lu|j5nGqf>WHnZ;"5Z~ Ko_gK?,5G!iP-?uAI|kk|+C2{(x`2VEY.n~
2022-10-03 14:15:53 UTC	1152	IN	Data Raw: 4e ba b0 20 fe 35 df ea 5e 78 56 ee 11 dd ee e4 0c 9c a4 78 da 5f 69 ed 71 e5 53 e9 b9 23 53 b5 b4 81 89 37 72 5e 0b 81 25 b6 76 5b ec 7c 9c c0 8a 65 ea 1b 66 88 25 00 aa 9e bc 88 fc f4 d5 6a 36 30 31 b1 39 19 81 82 5b a5 b6 c7 94 4e c2 c5 0f d4 10 6b c6 86 92 2b 0a 29 d8 9a fc 35 4a e5 ad 7c 6a 06 c8 90 78 f5 bd 8d e5 a5 bb 5e da 4d 0b 51 6e 92 f5 1d 47 21 46 66 46 da 86 9d 36 1a ab ec 72 5b 0c 68 b8 e8 b1 36 b1 3c f8 e4 b5 61 76 1a b2 5e 73 79 28 2a aa f1 03 23 d6 94 a8 aa 86 f9 d2 9a e3 be 4b 5b 46 19 1c b4 cf dc c4 56 97 16 ec 91 d4 4b 1b 34 b1 f2 3f e3 55 75 0d b8 d8 f2 e3 f8 e8 55 f1 1a b7 82 e7 82 fb 93 7b 6c 6e e1 c8 63 ec f2 76 8a c2 58 03 77 91 61 f6 f1 2a 38 4e a1 b6 f5 eb f3 d7 42 ed 3a ad 8a fe 43 d8 b0 df 7d cf c1 cb 64 f6 76 38 1c 3d 97 ee Data Ascii: N 5^xVx_iqS#S7r^%v[|ef%j6019[Nk+)5J|jx^MQnG!FfF6r[h6<av^sy(*#K[FVK4?UuU{lncvXwa*8NB:C}dv8=
2022-10-03 14:15:53 UTC	1168	IN	Data Raw: bd 79 d0 b7 d3 c1 c6 95 52 ca 56 55 b8 52 c5 c8 03 7e 9a 7b 63 4d 81 12 2e 27 b5 cb 62 ab 29 76 b5 96 63 22 48 e6 15 78 a2 25 03 1e e0 72 a0 06 04 95 5a 53 e0 3a 6b 55 ba 3d 07 03 5c 62 2c b2 37 18 fb 5b 7c 5d c4 e8 14 c1 dc b8 95 ed d5 57 62 27 8d c2 90 f1 8a f5 04 8d 74 57 b0 e8 9b 6c c8 b7 49 e3 76 c3 1d 6f 86 0a b7 16 38 98 43 43 2b 47 0b 15 50 07 70 95 65 20 16 26 a0 f2 15 ad 69 e9 a8 57 b4 dd a7 e4 2d c9 49 ce f8 b5 e5 f2 db 1c 3e 4a 59 59 20 65 bb 82 79 07 71 a3 e5 5e 6b 22 15 45 01 4d 02 81 b8 f5 3d 35 df 87 b6 97 f6 46 e4 07 b7 46 c7 58 0b 6c 7a 3d ec af c4 c8 0c 8b 24 9c 86 c0 29 5e 05 a8 49 a5 2a 74 dc b9 bd 4c c0 79 1c a5 d4 6b 78 b2 2c b7 16 a5 08 b8 b1 e8 ca 4e c7 67 35 04 75 df 54 a5 65 82 24 cd 60 92 c5 25 b8 4b d8 6e 6e 6e 9d 4c 51 c3 3c Data Ascii: yRVUR~{cM.'b)vc"Hx%rZS:kU=\b,7[|]Wb'tWIlvo8CC+GPpe &iW-I>JYY eyq^k"EM=5FFXlz=$)^I*tLykx, Ng5uTe$`%KnnnLQ<

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:53 UTC	1184	IN	Data Raw: 3b 06 6f 52 36 d6 cb a3 1d da 10 36 fe e2 f8 1a dc 5f 43 68 08 25 82 c5 dd 32 a1 3f a5 4b 35 55 b7 a5 74 71 c7 c0 1b 26 78 ac 6f 2e 3a e2 da 2b f8 ed f0 f2 5c f2 b9 42 59 26 91 6a c2 35 56 29 db 27 da 48 2c 68 34 d9 af ac f9 19 db 4d 42 17 f1 e3 ec af 31 32 c2 f6 a8 12 3e 57 56 b7 2e 92 db b4 6c 49 67 ee 31 7e 4e a0 06 3c 46 c7 60 a3 6a c9 37 6d 01 56 0c b8 f2 08 64 ba 92 e3 17 61 8f 77 40 24 82 2b 5e e4 4e c6 4a d6 55 76 01 8f 10 2a 79 7b 76 dd 74 56 2d 21 89 c5 33 97 59 1b 5c cd dd ac f9 d9 e4 b6 c6 43 0a 9b 7b 76 89 a5 ee 70 e2 cd 10 55 96 32 c5 ce fc 89 1b 7a 68 70 75 ab 55 dc 15 ab ab 93 4e 4c bd ba c0 26 c7 63 2d ad f0 28 e9 2c 78 9b 78 a2 5e 5c a3 d8 5c aa 37 1a 80 6a 01 24 8d eb f0 d7 99 6c 4f cb d7 e4 16 96 f5 22 4d 95 9a 5c a5 b2 5f e5 65 ff 00 Data Ascii: ;oR66_Ch%2?K5Utq&xo.:+\BY&j5V)'H,h4MB12>WV.llg1~N<F`j7mVdaw@$+^NJUv*y{vtV-!3Y\C{vpU2zhpu UNL&c-(,xx^\\7j$lO"M_e
2022-10-03 14:15:53 UTC	1200	IN	Data Raw: 4e ec 67 f9 45 5b 91 1f c3 4b cb 80 ed 79 25 da 61 da 1b 4c 3d dd 9e 52 59 ae 1b 84 b7 b8 b0 0b f0 ee 53 7e 64 71 1e a0 d4 7e 1e ba 57 92 5b 4d 19 d9 6d e0 0f 69 6d 6b 79 93 9e e2 e5 d9 ec ed 1d f8 5a b3 45 33 bb 02 a5 98 40 64 8d c8 a1 f4 5a fc b4 d7 c8 ea a1 06 ba 16 8c 35 9f 85 da 67 2e fe 8f 3f 24 97 81 63 18 f4 82 cb e9 da 5b 86 01 68 a4 b3 ee 29 fa 78 8a b7 f3 0d 4b 25 f2 f1 d6 ba 0a e5 9a 4c be 2d 39 b5 ef 22 43 61 0a 89 ae 2e 72 57 af 14 52 05 6a 15 02 dc 48 28 4d 2b 51 f3 dc eb 8b df a8 8d 7c 94 bc f6 17 34 98 7b 8b ae fd 85 e4 16 40 3f 6a d5 09 2e 08 15 56 68 94 02 78 9a ee 6a 7a 0d f5 d5 87 25 5b da 0c 9c 81 bc 7f 25 0d e5 a7 6f 19 e3 69 8e 59 24 6f a8 16 ea d7 90 04 04 2a bc 88 e8 ec 1b a9 66 af 4f 86 9f 2d 1d 5e ae 4a 3a f9 91 99 e3 c9 78 8e Data Ascii: NgE[Ky%aL=RYS~dq~W[MmimkyZE3@dZ5g.?$c[h)xK%L-9"Ca.rWRjH(M+Q\|4{@?j.Vhxjz%[%oiY$o*fO-^J:x
2022-10-03 14:15:53 UTC	1216	IN	Data Raw: 45 45 1a 3d c0 a8 e8 e4 0d 71 e5 a4 68 0b a8 2d f9 1c d7 97 34 16 96 16 36 57 b1 d8 5c 0e dd b5 dc 16 28 6a 0d 7d aa c2 39 89 07 d0 d3 fb 75 cf 8e b4 f2 f5 24 e8 9e a5 2f 3f 7f 0e 21 be 92 74 ca db 65 24 67 9a 59 ee 4a 40 a8 24 01 56 39 51 e1 1b 7c 7d a3 6d 75 52 9c 94 e9 01 45 af 1c ad 05 ae 06 fa 6c 30 9e d2 19 2e 6e af b3 04 4b 70 82 15 8d 98 2b 39 88 c0 8e fb 12 85 77 ad 48 a8 07 5c f6 fb 9b 52 18 d7 fd 02 d8 df 20 b6 be b7 b2 38 5f 24 7c 6c d7 2e d3 c9 8d b6 b6 65 b6 40 d2 19 1e 05 8d 02 a7 35 eb c9 a3 0b 5f 4a 75 9d f1 b5 b8 ae ad 6a 48 c9 dc 4d 34 d2 bb c8 b6 f2 49 c9 cd cb a7 16 72 fb 37 22 8b bd 7f 0d 6c 68 29 15 39 ad 91 79 cf 2c ea 12 a1 1a 20 bc 9d 57 6a 82 09 56 00 8f 5d 5e 7c 22 a9 24 8a 7d dd ec 30 c8 0f d4 b4 51 4b 28 64 79 39 04 5a ec 09 Data Ascii: EE=qh-46W\(j}9u$/?!te$gYJ@$V9Q\|}muREl0.nKp+9wH\R 8_$|.e@5_JujHM4Ir7"lh)9y, WjV]^|"$}0QK(dy9Z
2022-10-03 14:15:53 UTC	1232	IN	Data Raw: f0 ec 91 63 e5 b7 b2 8e 03 24 03 dc b2 76 ca 38 4e e9 5e 2c 03 03 bf ce ba e1 c9 7b 5a da 1d 38 ee aa a0 a0 cb 95 b0 ff 00 54 63 f2 72 f8 86 26 19 a5 86 47 bd 86 e6 56 55 78 d4 02 88 63 58 57 89 e2 79 7c cf c4 0d cf 27 54 2e 4c a9 bd 8b d5 b4 98 4c 8d 84 76 cb e2 b1 63 d8 ce f3 34 76 93 b3 21 97 9b 3f 06 2a a1 42 97 23 60 47 e1 a8 db b0 d3 0a c9 57 e0 91 99 bf 31 63 ec 65 5c 3a e3 e0 8b bf f4 f0 cc dc 52 60 40 2a d1 33 3a 92 79 21 35 a1 f9 e8 be 56 52 6b dd 46 85 7e d2 ee d3 27 6e 2e 64 ce d9 d9 83 18 37 31 4f 0d d8 e2 d4 a9 46 92 18 98 13 4d bd b5 d2 2b 24 f5 38 9d 67 76 2b 29 85 b4 8e d8 09 fc bf 15 89 46 80 5c 76 c3 5d b1 31 9a d3 88 9e d8 b1 af e9 a9 1a ad 2c 93 32 af d4 c3 ec bc 76 ca 7b eb bb c9 3c d2 76 7b 74 74 c5 da b5 95 e7 6e e1 81 23 94 7d a4 Data Ascii: c$v8N^,{Z8Tcr&GVUxcXWy|'T.LLvc4v!?*B#`GW1ce\:R`@*3:y!5VRkF~'n.d71OFM+$8gv+)F\v]1,2v{<v{ttn#}
2022-10-03 14:15:53 UTC	1296	IN	Data Raw: 1e 67 79 63 75 67 92 b7 c6 43 1b c5 24 38 d7 fa 60 ed 6a 92 81 51 00 b5 82 3a 2d 54 1a 37 21 e9 aa da f6 f2 93 3b 71 ac 89 6c 54 ce 0f ee 09 18 79 ad 32 d8 b4 b7 b1 21 b2 81 2c 2e 60 9a e1 2b ba 81 6c b0 84 20 7a d0 d4 f5 f8 69 6d 8f 1d d6 b5 86 51 d5 d8 b0 c5 69 98 be 9e e0 64 f1 c8 f1 b0 55 49 2d ed 67 92 66 1c 78 d4 c8 d6 eb 4d 80 1b 57 f1 d7 27 e2 c6 d6 32 a3 2b 97 3f 6f bc 3f 25 7a d8 f7 c2 3b 64 d6 41 71 36 38 5b b9 72 c8 be d7 fa 71 42 48 04 1a f1 d3 2a 5d 7f 90 b6 a4 e8 c8 d7 7f 69 2f c3 d3 17 e4 f7 be 31 8b a8 69 6d 23 f1 d9 a6 f7 9f e7 59 2d e7 85 85 7f f0 8f cf 56 c5 c2 3e fd 42 b0 d5 23 b8 8f b6 11 63 ef ae b2 13 7d ca 39 29 2e f8 02 2f 70 5c 25 08 8b 4e da cb 73 7f 2b 2a d2 95 55 0a 2b d7 7d 57 2b a5 aa 92 d2 0c f0 a6 33 93 fb 79 08 ec 99 b2 Data Ascii: gycugC$8`jQ:-T7!;qlTy2!,.`+I zimQidUI-gfxMW'2+?o?%z;dAq68[rqBH*]i/1im#Y-V>B#c}9)./p\%Ns+*U+}W+3y
2022-10-03 14:15:53 UTC	1312	IN	Data Raw: 97 fd d2 ce 65 62 38 8c d7 da 2b 6b c8 ef 6a 20 8a db 21 c5 1e a0 ab c3 36 42 09 b8 05 62 7a b0 55 da b5 d2 27 46 f7 27 6e d5 d6 90 8f 9d 47 85 79 98 ca 64 63 b4 f1 bb 4b 2c 64 e6 16 8a 0f de f0 33 4c 2d e2 e6 a2 22 5b 24 b5 a1 6a 55 f7 3d 7d 4e ba d7 ae 37 26 d3 7a a8 3e 8c f0 df 2b cf f8 37 8e 5b 63 71 7f 66 a2 bc 8a cc 22 cd 93 bb f2 3c 53 cb 24 43 f5 b3 76 72 29 1a 8a d4 85 45 03 7a ee 75 1b d2 96 7b a0 d2 f7 4b 64 4e cf 79 f7 9a 79 7f 8e b4 38 cf b4 71 43 61 91 5e 37 19 1c 7e 72 c2 75 96 26 1c 59 23 56 bb 46 26 83 ae c3 d3 7d 23 c1 44 f5 65 39 5a 34 48 f8 6a ff 00 ec 87 de 4b f9 f2 02 d7 c7 72 91 c9 2b 81 c2 de 5b 17 8c c2 ee d4 2d c2 f0 71 a0 f8 13 5d 7a 98 f3 63 4a 0e 6b 61 b3 ff 00 f9 9a 4d e7 fb 7e fb 81 86 b5 8f 23 7a d6 76 5f 59 6d 6c c2 e7 21 Data Ascii: eb8+kj !6BbzU'F'nGydcK,d3L-"[$jU=}N7&z>+7[cqf"<S$Cvr)Ezu{KdNyy8qCa^7~ru&Y#VF&}#De9Z4HjKr+[-q]zcJkaM~#zv_Yml!
2022-10-03 14:15:53 UTC	1328	IN	Data Raw: 2c 38 fc 06 0b 0f 71 15 de 3b 1b 6f 69 79 6d 46 8e ee 16 71 2a 9a 50 1e 45 f9 57 f3 d7 52 c3 4f 02 3b b6 4b 9e 49 6e 5c b3 bb 3e f5 20 9a f2 27 d4 93 5a 9d 55 21 19 d6 8e 65 51 1c 92 f1 4a 1e 6c 6b b0 fc 74 45 83 0b fb c1 e4 37 0b 84 bd c5 e3 24 b8 b1 74 23 bd 76 ac e8 8e 88 09 31 82 8a 4b 16 3d 6a 40 03 e3 af 2b b7 db 87 c5 15 78 da ac 9f 10 78 87 94 b2 e6 2e f1 b7 1c 45 ba 4c d2 4e b2 15 11 13 31 a9 66 ee 10 78 f2 f5 5e a7 e5 ae 2c aa bc 65 9c 9e d5 47 a9 ab db 64 2d 59 3b 6b 1d b1 2d 50 c8 b0 a4 66 9f 11 c8 80 47 a7 ae b8 b9 50 e8 a7 6b 1b d2 4c 3f cf b3 4a 97 62 c9 da 35 b4 47 05 ee 89 82 e2 50 88 ea 18 9e eb 25 01 2c 0f 6c 10 3f cb 41 ae ce bd 2a f5 47 2f 63 25 6c f4 24 e0 f0 a6 17 59 62 bb 9a f2 07 b5 66 83 26 8d 67 20 85 83 7b 82 87 b9 1d b6 65 61 Data Ascii: ,8q;oiymFq*PEWRO;KIn\> 'ZU!eQJlktE7$t#v1K=j@+xx.ELN1fx^,eGd-Y;k-PfGPkL?Jb5GP%,l?A*G/c%l$Ybf&g {ea
2022-10-03 14:15:53 UTC	1344	IN	Data Raw: a4 86 a7 e0 3e 1a f4 3a f8 9d f5 7b 1c f9 6f e0 bf 66 b2 d7 19 0b b7 b9 46 11 46 00 8d 61 40 16 38 d1 45 11 10 0e 80 0d a9 af 52 aa 14 1c ec 03 20 9a a6 95 09 4a 1a 1a 12 4e 88 b0 45 b8 c9 5b e0 6d a4 ca 64 e4 10 c7 11 1d b4 3d 5a 82 b4 1d 4e fa 9e 5c 8b 1d 65 86 b5 96 7c 1d f7 0b 01 e4 39 8f 2b 93 cd 2f e0 6c d6 32 e3 23 0c d0 45 0c 4e 56 d2 d6 0a 14 17 01 22 e2 c0 03 d5 43 1d 8f e8 d7 81 97 b0 af 3a 9a d8 56 ec ca fc d7 ee 1e 72 2c 74 d6 58 9b 6b 6b 9c 29 95 3d 8f 3c b6 72 9e 94 08 15 6b 4a f4 da 9b d3 e7 ae 4a d7 96 8d 9c 59 b3 37 f6 ad 8c 9a 2c de 37 0f 2a 66 2f 1d 92 6c 88 91 22 82 29 e4 32 2c 8e bc 43 7f 5e 30 a6 34 45 00 95 a5 07 4e b5 d3 70 b5 b4 47 1b 19 c4 e7 21 cb 4e 6c 3f 73 8a d6 ea 29 9b 23 15 d3 88 95 78 2a 18 e8 56 9d df 77 21 e8 4f 4a d0 Data Ascii: >:{ofFFa@8ER JNE[md=ZN\e|9+/l2#ENV"C:Vr,tXkk)=<rkJJY7,7*f/l")2,C^04ENpG!Nl?s)#x*Vw!OJ
2022-10-03 14:15:53 UTC	1360	IN	Data Raw: 9b 35 b1 ee 5d ac 96 b8 fd de 2b 38 21 8a 56 a4 48 6a c0 75 15 dc 81 a4 b7 7f 23 b2 49 a1 2b 4b b8 55 21 f8 fd fd e5 8d 9d c5 be 43 1a b8 93 64 85 ed 6d 2e 61 92 4b 99 62 81 42 33 c4 b1 4f 22 31 3b 54 3b a9 fc f5 b2 e4 d6 66 4e da e1 c9 8f 76 92 fe 49 0d e6 51 ad bd bd b6 32 e2 cb 07 6f 6f 24 84 5b d2 48 8c a6 53 c9 92 e2 dd a6 ed 02 0a 8d 96 95 ff 00 13 69 1f 62 f5 fe 09 e6 bd f1 fd d5 69 96 8f f5 8d c7 21 7d e3 f6 78 cc 0e 68 c1 2c 52 e5 a2 26 46 8e 69 62 68 0d c4 02 a9 24 32 22 35 01 12 1a 6a 7f f6 2e af 63 9f f3 ae f7 3b 61 91 c8 db 5a 3b ab c3 77 7c e8 05 e6 6e e2 47 17 12 90 3d ef 2c 86 42 ae c7 e2 45 75 0b 77 dd bc 0e fb f7 6b 42 df e3 b9 8f 2f c1 c1 f5 18 79 31 dd c6 71 25 ca c9 72 49 94 72 1e d2 26 24 2d 76 d8 37 f6 eb 57 f6 0e a2 d7 b3 7f 26 91 Data Ascii: 5]+8!VHju#I+KU!Cdm.aKbB3O"1;T;fNvIQ2oo$[HSibi!}xh,R&Fibh$2"5j.c;aZ;w\|nG=,BEuwkB/y1q%rIr&$-v7W&
2022-10-03 14:15:53 UTC	1376	IN	Data Raw: 02 f7 2e 21 e6 14 90 41 a3 d1 87 c3 4f 11 b9 7c 79 6d 4d 1e a8 b9 e3 7c 97 c7 af a0 82 e6 d3 29 15 c4 57 49 ce dc c7 20 2c c8 4d 2b c6 bc 87 e6 06 96 0b fb 2a fc 96 04 9e cc 8f 68 99 c9 15 a8 6d b8 9f cb 5a 0a c4 8b 59 e1 35 a2 04 f8 b3 1a e8 0b 1a 88 69 e2 20 d1 d4 d0 74 e4 41 d6 88 31 1c 4a c0 f3 ad 52 9e d2 5e bf d9 a2 d9 85 7d 73 80 77 8c 0f f1 10 4d 3f 80 d6 30 c3 e4 9d 7d c2 45 a7 5a 71 23 61 f3 db 4d 01 81 af dd 2e 19 8f 19 6a bf 05 e3 d6 bd 77 a6 b4 05 23 cb 92 ba 63 50 25 7d be 02 82 bf 86 b4 86 0f 49 7f 31 00 14 a9 27 e6 29 a2 83 c4 47 d6 ca 7f f4 45 07 c5 b7 af cb 58 dc 44 9b 97 2e 0b 44 46 d4 af 32 7e 54 db 44 dc 45 77 42 f5 8c 1a f5 af 23 4d 00 71 1c 17 25 94 0e ca 1a 7a 88 98 ff 00 71 3a 26 84 3b 14 b2 d2 9d a0 95 1f ca 84 7f 7e 80 38 a2 42 Data Ascii: .!AO|ymM|)WI ,M+*hmZY5i tA1JR^}swM?0}EZq#aM.jw#cP%}I1')GEXD.DF2~TDEwB#Mq%zq:&;~8B

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:53 UTC	1392	IN	Data Raw: 8a 49 78 cd 32 8e 53 a4 64 b3 15 63 ed 6a 81 c4 03 5a fa 6b 70 fa 11 78 99 3e d6 4c cc 42 de 18 fe 8e dd 25 1c ec 24 bc 9b 94 28 c8 07 fd 4c 4f ce 40 4f 52 43 11 b6 fb ec 34 ad 22 16 5f 25 cf c2 b1 f1 65 bc a1 7f d7 de 47 71 8a c3 f6 0b c3 89 b7 31 5e ac 57 2c c3 81 99 e3 ee 01 14 8a 0b fa ed d7 e5 3b 44 68 86 af 16 d2 f0 0a 6c e5 9f 67 24 97 d1 03 3d fb cc b3 77 91 12 16 81 26 ac 5b c4 ab 4e 5b 6c a0 7e 15 df 52 55 6c 19 71 c3 7c 76 27 78 b6 22 f3 33 91 7a dd 63 ee 31 98 f9 4c f3 45 25 cc b0 09 e4 99 b9 c8 04 71 86 1d ba 9a 00 d2 7a 74 d2 e6 bf 05 b1 34 be 0d 55 7c 59 97 24 32 3d c8 ee 31 9d a7 b6 58 0f 77 b4 55 58 19 3d ac 01 63 42 00 34 a0 03 ae b9 3d b6 68 a7 ac 85 e4 b9 7b 7b 7e 38 cb 5c 1e 42 3c 2c 48 ea 97 96 f2 f0 2e ca 28 d3 13 19 90 c6 41 27 6a Data Ascii: lx2SdcjZkpx>LB%$(LO@ORC4"_%eGq1^W,;DhIg$=w&[N[l~RUlq|v'x"3zc1LE%qzt4U|Y$2=1XwUX=cB4=h{{~8\B<,H.(A'j
2022-10-03 14:15:53 UTC	1408	IN	Data Raw: 31 0e e2 d9 9a f3 68 e1 f7 48 21 66 0a 14 d0 91 c5 8f 5e 9a 9b b3 43 3c 8e a5 bb c6 71 9e 2d 73 67 2c b7 b7 79 21 2a dc 34 12 0b 24 41 db e2 c8 0a ca b2 05 65 22 9b 80 4f 5f 4d 25 b2 31 a9 93 91 a5 5b 62 ac e5 8e 48 ec 72 f7 77 b0 f7 3b a2 3b 93 11 96 ab b0 1b 46 1c 8a 0f 89 ae a3 6c ac a7 14 c1 33 e2 39 cd f5 38 d9 56 63 69 23 3b 5a 9a db a7 3f e6 35 e2 63 35 f5 aa fe 7a 35 cb f2 68 15 0e 45 66 77 b5 ca 25 9e 28 31 d8 33 73 04 fc 0b 22 37 c3 e0 77 d7 44 ab 08 d3 22 e4 71 b2 88 5e e6 cf b7 70 91 ab 76 2a ff 00 d2 e5 e8 39 16 1c 57 7f 51 b6 83 a9 93 60 b8 af 67 b6 ed c6 4c 31 b7 13 24 82 36 2c bc 6a 46 c6 83 a9 e8 69 a1 b1 b4 1e 49 2c 32 26 21 7b 64 8e 21 76 91 66 04 25 18 8a 54 91 4e 47 a7 ea 07 59 b0 32 05 c6 02 df 24 e8 93 5c db cb 61 33 05 bc 92 e4 bf Data Ascii: 1hH!f^C<q-sg,y!*4$Ae"O_M%1[bHrw;;Fl398Vci#;Z?5c5z5hEfw%(13s"7wD"q^pv*9WQ`gL1$6,jFiI,2&!{d!vf%TNGY2$\a3
2022-10-03 14:15:53 UTC	1424	IN	Data Raw: 16 ad 2c 0d 8e c4 dd 35 e0 b8 0c 38 27 29 02 86 40 fc 81 21 3d c3 d6 9a 95 eb 5c b6 50 9f fa 92 70 9e 84 2b 9c 57 d2 c1 02 62 fc ab 13 6b 36 5a 07 97 f6 2b de f0 81 9c 2f 3e e1 92 49 25 4e 45 08 ac 6f bf af a9 d3 55 a9 d5 6c 2c a3 26 8f 2b 90 f2 1c 76 4b 0f 6b 67 89 67 82 c9 ef e5 c8 c7 6b 1d b4 51 2c 09 bb 40 cb 11 75 7d c2 6c c2 a0 6c 06 bb 55 2b 56 9b 19 42 66 b5 e1 f9 69 6d b1 b6 b6 39 8c 1d be 25 ae a1 88 b4 a2 dd 19 e6 41 41 dc 96 70 cf ea a0 93 b3 1e a4 8a ed c9 9f 1a 76 9a b0 55 86 e1 9a f2 fb 2d 23 e5 12 de 2b 28 ed e6 ba 37 b8 d8 ad ed cc d6 cf 31 89 a3 8d e4 0e 91 d3 97 13 45 0f c7 f9 b7 d1 6a 2b 28 b3 d8 db fc 47 c9 de 52 96 78 df 15 c8 61 71 8b 2b 5a c3 71 70 80 42 52 11 4e 5c 95 77 06 9b 35 68 47 af a6 bc bc d8 ac b5 90 52 d6 9d 0b e7 d5 dd Data Ascii: ,58')@!=\Pp+Wbk6Z+/>I%NEoUl,&+vKkggkQ,@u}llU+VBfim9%AApvU-#+(71Ej+(GRxaq+ZqpBRN\w5hGR
2022-10-03 14:15:53 UTC	1440	IN	Data Raw: 58 d7 fc d2 15 5f 9e 8d 6b 6b 6c 17 0b 72 bb 3b 7d 73 9b 81 3a dd 5b 30 e5 07 66 5e 5e d2 36 ab 0d 9a bf 01 4f c4 ea f4 ea 2d ec 4a d9 bc 22 2c 96 36 6e c5 a3 81 ac 27 6d 96 e6 10 22 7a 91 b8 6e 1b 38 3f e6 07 5d b5 aa ae c4 5d 9b 06 dc 5a 5d 2c 64 c8 91 5f c7 1d 01 7e 34 71 f8 a2 d2 bf 97 f0 d3 00 8d 19 88 02 8c 8c b0 03 b2 a1 e6 03 7c c6 d4 23 58 c8 8d 35 ac 2e e6 78 66 12 ce de a7 fa 6c 29 d0 73 00 d4 7c 8e b4 80 8e 25 bf b7 67 6b 9b 76 99 29 56 92 d3 76 50 7a 92 80 d4 ff 00 e5 fe 1a c0 82 4a 5e f7 a3 32 da 5c 25 ec 2a 78 ba ff 00 3a d3 d1 87 55 3f 26 d1 90 41 10 dd 40 93 73 b7 43 0c c0 fb d4 ee a0 1f f1 0e 8d f9 6f f8 6b 01 b3 81 d5 a4 32 17 48 a7 24 93 71 b8 53 ff 00 60 fc ce 9a 44 6c 75 6c a7 66 12 77 77 3e e0 ea 7f f8 fe fd 34 84 95 f5 17 16 e0 3d Data Ascii: X_kklr;}s:[0f^^6O-J",6n'm"zn8?]]Z],d_~4q|#X5.xfI)s|%gkv)VvPzJ^2\%*x:U?&A@sCok2H$qS`DlulfWw>4=
2022-10-03 14:15:53 UTC	1456	IN	Data Raw: cf 66 31 78 ac 96 1e e3 2b 74 56 67 6e c5 9a dc 49 fd 25 a8 24 c9 24 ec c5 c5 3d 03 57 e1 aa 57 b3 6e 30 9e 85 ab 92 d5 51 25 5f 35 0d ae 5d 56 cd 2f be 92 fe e1 7e 9e e6 e6 1b a9 23 31 da b2 13 d0 b0 60 1a 94 d8 53 d3 e3 aa 62 c9 75 0c 86 4b 37 a4 94 fb 3c 3f 8e 59 5b 45 1d 99 9a ca 25 df 1f 96 73 dc e7 76 01 3c d8 4e 55 0f 4a 29 53 d7 a1 d7 73 b5 ac e5 93 89 62 7c 4a d3 13 8f c7 de f9 1d ce 2b fd 33 9b bd bd 31 5c 5d f1 8a 09 ae 8b 3f 25 06 7b 62 6a c4 7b 8a f3 a8 e8 5b 7d 26 7b 3b 3e 29 ca 2f 5c 6d 13 2e bc a7 39 8d 6c 8b be 46 4b 88 d0 a4 96 a1 23 55 47 69 5a 9c 52 55 34 aa 82 2b 56 af a1 1a 87 a6 b6 6a 4a aa 6a 49 82 0f 22 ce 5b de 5a 60 b0 71 46 5e e4 fe fd 65 72 6e 71 c8 d3 72 5e 4d df b8 ed 31 64 34 3e e9 08 1e 83 54 51 f2 74 d3 a9 c8 bc c1 fe dd Data Ascii: f1x+tVgnI%$$=WWn0Q%_5]V/~#1`SbuK7<?Y[E%sv<NUJ)Ssb|J+31\]?%{bj{[}&{;>)/\m.9IFK#UGiZRU4+VjJl"[Z`qF^ernqr^M1d4>TQt
2022-10-03 14:15:53 UTC	1472	IN	Data Raw: 1d 6e a5 c8 33 f6 64 b5 95 52 89 40 7f 58 15 e2 7d 0e a6 f2 d9 4b 4c 0a c5 e6 78 f0 90 2a 5c bc 0d 2c e9 6f db 8e e9 16 ad 0c 60 92 19 40 ad 77 1b 57 5c f5 bd 99 5a e5 e2 48 87 19 7d 93 61 1e 56 ff 00 f7 5b 69 a1 32 db 48 8a 12 e1 52 80 9a 90 05 00 df e2 34 6d 67 e1 0e ad 3b 80 72 89 68 f7 d0 5d 4d 7b 17 fa 76 da 37 86 0c 7b 30 29 70 ce 42 ae fe c2 08 61 d0 1e be 87 a6 ab 8e 5e 8f 71 5b 01 e5 3c 9b 07 8b b7 bc 95 ee 0d a6 36 cc 91 1d f2 80 d6 e2 49 00 26 28 a2 56 42 e3 6d de ab bf 5f 8e ba 2b d6 b5 b6 d5 92 b5 dc e8 49 b0 f3 8b 7b eb 59 ed b0 d7 f7 6b 69 68 8f 1b 0b 84 12 4c b2 c8 8b 24 6d 1a f7 9c 2c 67 96 c1 5c 80 37 3f 0d 51 f5 f8 bf b8 b2 7f 21 ab 5f 2d b9 82 69 cd c6 6a d2 fa fa 10 e2 4f 1f 0b 23 71 60 d4 4e dc 81 01 03 8d 2b 5a fc be 3a 9d b0 56 36 Data Ascii: n3dR@X}KLx*\,o`@wW\ZH}aV[i2HR4mg;rh]M{v7{0)pBa^q[<6I&(VBm_+I{YkihL$m,g\7?Q!_-ijO#q`N+Z:V6
2022-10-03 14:15:53 UTC	1548	IN	Data Raw: 8d c4 9d 18 6c e7 70 85 e2 64 ed 45 9d d9 4b 7b 0c 6c 33 08 45 86 3d 2d e5 a3 48 ec b1 96 ed 31 43 51 d6 95 3f 1f 86 bb 28 eb 32 b7 3b 1d d0 ec 78 2c 0c 57 58 29 be be 49 37 2e ab 28 89 e0 8f b6 fc 55 1f 80 a8 35 35 a1 34 db 7a ea ae f6 e2 1e 7a 97 2b e2 ed 2c e7 22 21 82 e6 ce fd c2 c9 22 c2 a1 5e 39 88 76 a8 6a 03 50 0a 85 3a e6 b6 9a 0b 76 1e 7b 9b 49 f0 7d db 7b 1b 19 6f a4 2b 10 7e d9 90 f1 a9 af 2f 6a b1 53 42 d4 af ba a0 ef a6 a3 aa af d4 d7 d6 a6 63 92 c8 e5 25 92 ff 00 31 9b c7 59 59 e1 ac 61 54 4c 72 c5 2d a5 cc 80 8f 71 8c c2 11 50 8d ba 90 c4 53 6d 4f d5 0b 4d 59 1e 4d 6e 58 65 1e 39 e4 37 f6 77 51 19 24 10 4b df c5 2c 1d e8 22 84 50 85 8c bc 6b bf 1a 9f d7 42 de a7 42 ea c9 68 19 6b 62 3d d7 90 35 ad f4 f9 0c 9c a2 e1 30 81 fe 9e d1 4c 83 bf Data Ascii: lpdEK{l3E=-H1CQ?(2;x,WX)I7.(U554zz+,"!"^9vjP:v{l}{o+~/jSBc%1YYaTLr-qPSmOMYMnXe97wQ$K,"Pk BBhkb=50L
2022-10-03 14:15:53 UTC	1564	IN	Data Raw: b6 92 d8 dc 15 95 c0 4e 4a 02 82 53 a1 a8 35 a9 3d 36 d7 3f b5 a6 d4 9c 56 ec 64 ae e5 4b 37 e4 2d 0a 86 b8 c8 df 4b 20 95 43 c5 3b 11 09 53 5e 4d ec 64 3d 68 29 4a e9 b1 d7 e8 4a 96 56 71 06 7b 3f 86 cd e4 59 67 bd c6 5d 4e d0 c1 1a c8 cd 77 24 76 d0 96 ae eb 0c 8e 54 57 ad 07 22 7e 67 a6 ba 96 75 55 0c bd 71 2a ea 01 bf 96 0b 88 cc 59 ac 9d b5 8d e6 1d 42 5a e4 27 46 91 c0 8d 9a b1 9e 5e c9 40 00 6f d4 fa 03 a3 44 d6 cb 46 0b 56 bb a7 a9 77 fb 71 71 e5 19 6f aa c5 8f 30 c3 58 f8 fa 3a 1b a5 bb b9 92 38 67 7e 5b 15 44 8c c9 55 1f cd 40 00 27 e7 ae 3e e5 6b 56 be d7 2c 7a d9 b5 0f 62 d7 73 96 ca e6 f2 12 78 df 8a 60 ec e6 0a 25 89 ef 31 ad 2b 5a b7 16 2c 64 13 5c 85 24 d0 8d ce a6 92 c5 5e 56 62 2b da ee 2a a1 1b af 8e c1 91 f1 9c 5d 9e 43 2d 94 b1 37 d3 Data Ascii: NJS5=6?VdK7-K C;S^Md=h)JJVq{?Yg]Nw$vTW"~guUq*YBZ'F^@oDFVwqqo0X:8g~[DU@'>kV,zbs x`%1+Z,d\$^Vb+*]C-7
2022-10-03 14:15:53 UTC	1580	IN	Data Raw: 91 a2 b2 68 64 1b d1 67 2c cd 2a 81 ca 80 81 5d b9 1f 5d 17 69 f1 a9 bd ff 00 1b 9f 49 fd b3 fb fb fb 2c 70 e3 33 b2 59 c9 8b b4 37 11 1c 85 fc 72 c7 73 df 42 bf d0 02 05 6e 74 62 6a e2 a0 fc 75 bd 8d 1e 87 5b bb 1a 58 fa 3b 1f 93 c0 79 b5 2f 70 d7 42 e9 52 48 e4 6b 69 23 95 ad d2 68 ea e2 93 71 2a ac 84 13 bb 6d b6 a9 4b ce e7 af 4c 95 ba 94 c9 16 d7 e3 17 67 fb 5b 5d 5d c5 69 66 c6 47 38 db 83 14 d0 b3 3f 26 94 88 19 55 d0 16 a9 35 f5 e9 aa 4a 63 2b a0 fc d9 9c fc 80 4d 67 92 4c ae 3d c5 25 ba 45 21 b8 b1 ab 07 11 a7 3f 6f c4 1e 43 e1 a5 e2 31 94 c7 f7 2a 65 f2 5c 9e 03 35 6b 1e 2a fa ca 78 db 18 d7 dc 27 b0 b8 85 66 11 45 74 b7 0e 10 ab bf 2d 85 58 30 fd 5b ef a7 aa 4d 12 bd 9d 37 d8 9d 69 9c a9 b2 c6 64 ac 2c ac 32 f9 8c cd fc d7 17 b1 d8 c3 24 2f f5 Data Ascii: hdg,*]]iI,p3Y7rsBntbju[X;y/pBRHki#hq*mKLg[]]ifG8?&U5Jc+MgL=%E!?oC1*e\5k*x'fEt-X0[M7id,2$/

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:53 UTC	1596	IN	Data Raw: f2 c9 2d 27 38 bf db ae b3 42 61 78 86 19 81 22 01 24 d2 ff 00 4e d8 b8 ad 0d 19 88 24 d4 01 a4 57 b4 9c d6 ec da d6 4d b7 a1 6a be b1 cf 65 6f ef e2 b6 fb af 6c 96 ed e2 50 db 0b 49 31 d6 e0 dc 5b 97 94 8b 64 48 ae a5 11 c3 13 90 51 95 b7 af b8 57 72 ef b1 5d 74 67 75 7b 09 a5 a9 6c cc f9 3e 4d fc 7a f7 19 69 e5 3e 3f 9d ce db e2 17 17 8a b3 6c 6b a4 92 ab c3 25 ac a1 d2 43 24 91 1f 62 95 64 7a 13 4a 92 36 d4 6f d8 af 2d 9c 0d f9 b4 aa 2a 7e 19 8b 88 f9 67 8e 47 e6 9e 2b 0c 16 8c 61 0c 44 25 6c 0e 3d 23 12 ba 29 56 08 8a 24 43 b7 35 35 61 5a ed 5e ba e5 a5 94 a6 1c 59 31 d9 4b 89 3e d8 f0 df 21 fb 7d 9b f0 af 29 f2 7f b6 38 6c 15 ac fe 2b 1d e4 18 fb 7b 59 de da ee d2 58 e3 6e db 2c 4e d5 4e 43 75 23 f5 1a d2 bd 74 d9 97 ad a8 b6 e7 56 2a d6 d6 86 8a 1f Data Ascii: -'8Bax"NWMjeolPI1[dHQWr]tgu{l>Mzi>?lk%C$bdzJ6o-*~gG+aD%l=#)V$C55aZ^Y1K>!})8l+{YXn,NNCu#tV*
2022-10-03 14:15:53 UTC	1612	IN	Data Raw: c4 b3 37 e5 ae 2c fd ba 63 fa b3 a7 1f 5d d8 b7 e3 f0 5e 47 e7 36 eb 75 29 87 03 e3 1c 96 41 3c c8 f1 c6 c9 f1 54 66 ac 87 e6 4d 3f cd e9 ae 4a e2 cd da d6 da 54 ad af 4c 5a 2d 59 69 86 eb c6 3c 35 59 7c 62 d1 2e 32 0e 0a cd 9d bb 1c e4 35 ff 00 e8 97 6a 0f c2 83 f1 d7 ab 83 a7 4c 6b 44 71 e4 ca ef b9 4c c8 65 6f b2 12 49 2d ed cb 5c c8 37 12 31 24 ed f9 50 7e 03 5d 89 24 4a 40 53 dc 39 14 56 2f 4d c3 74 15 f9 0f 5d 13 11 54 ce c5 6b b2 9f 88 34 27 e4 00 3a 30 00 94 76 aa aa 59 94 86 ad 57 d4 9f fe 3e 5a 06 14 b6 f3 4a 68 76 8c 9e bc 45 47 fd 9a d3 01 2a 7e 4d e6 18 2f 11 89 c5 dc cd 25 da 27 75 2d 50 17 77 1d 7f 05 02 9d 4d 07 cf 5e 67 6f f6 15 c5 a7 90 ec 62 df 71 72 de 73 9d fb 6d 98 cf de f8 e5 d6 0b c4 ed e7 b6 93 eb af 8c 70 34 eb dd 53 dc 09 23 77 Data Ascii: 7,c]^G6u)A<TfM?JTLZ-Yi<5Y|b.25jLkDqLeol-\71$P~]$J@S9V/Mt]Tk4':0vYW>ZJhvEG*~M/%'u-PwM^gob qrsmp4S#w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49718	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:35 UTC	30	OUT	GET /wordpress/wp-content/themes/kawaken/css/layout.css HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:35 UTC	32	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:35 GMT Server: Apache Last-Modified: Thu, 24 Feb 2022 07:44:56 GMT ETag: "260f0-5d8bec22c19f1" Accept-Ranges: bytes Content-Length: 155888 Connection: close Content-Type: text/css
2022-10-03 14:15:36 UTC	33	IN	Data Raw: 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 2f 2a 2f 2f 2f

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:36 UTC	133	IN	Data Raw: 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 70 61 72 65 6e 74 20 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 63 68 69 6c 64 20 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 61 72 63 68 69 74 65 63 74 75 72 65 20 7b 0a 20 20 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 63 61 6c 63 28 31 31 30 70 78 20 2f 20 31 2e 37 29 3b 0a 20 20 7d 0a 7d 0a 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 77 72 61 70 20 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 70 61 72 65 6e 74 20 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 63 68 69 6c 64 20 2e 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 74 6c 5f 61 72 63 68 69 74 65 63 74 75 72 65 3a 3a 62 65 66 6f 72 65 20 7b 0a 20 20 77 69 64 74 68 3a 20 39 33 70 78 3b 0a 20 20 68 65 69 67 Data Ascii: _main_img_ttl_parent .low_main_img_ttl_child .low_main_img_ttl_architecture { padding-left: calc(110px / 1.7); }}.low_main_img_ttl_wrap .low_main_img_ttl_parent .low_main_img_ttl_child .low_main_img_ttl_architecture::before { width: 93px; heig
2022-10-03 14:15:36 UTC	149	IN	Data Raw: 79 3a 20 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 0a 20 20 64 69 73 70 6c 61 79 3a 20 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 0a 20 20 64 69 73 70 6c 61 79 3a 20 66 6c 65 78 3b 0a 20 20 2d 6d 73 2d 66 6c 65 78 2d 77 72 61 70 3a 20 77 72 61 70 3b 0a 20 20 20 20 20 20 66 6c 65 78 2d 77 72 61 70 3a 20 77 72 61 70 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 20 6a 75 73 74 69 66 79 3b 0a 20 20 20 20 20 20 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 20 6a 75 73 74 69 66 79 3b 0a 20 20 20 20 20 20 20 20 20 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 20 73 70 61 63 65 2d 62 65 74 77 65 65 6e 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 2d 33 72 65 6d 3b 0a 7d 0a 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 Data Ascii: y: -webkit-box; display: -ms-flexbox; display: flex; -ms-flex-wrap: wrap; flex-wrap: wrap; -webkit-box-pack: justify; -ms-flex-pack: justify; justify-content: space-between; margin-bottom: -3rem;}@media screen and (max-wi
2022-10-03 14:15:36 UTC	165	IN	Data Raw: 72 65 6d 3b 0a 20 20 7d 0a 7d 0a 2e 6c 69 73 74 5f 70 65 72 66 6f 72 6d 61 6e 63 65 20 3e 20 6c 69 20 2e 70 65 72 66 6f 72 6d 61 6e 63 65 5f 69 6d 67 5f 77 72 61 70 5f 70 61 72 65 6e 74 20 7b 0a 20 20 77 69 64 74 68 3a 20 37 30 25 3b 0a 7d 0a 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 36 37 70 78 29 20 7b 0a 20 20 2e 6c 69 73 74 5f 61 72 63 68 69 74 65 63 74 75 72 65 20 7b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 7d 0a 7d 0a 0a 2e 6c 69 73 74 5f 61 72 63 68 69 74 65 63 74 75 72 65 20 7b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 20 20 7a 2d 69 6e 64 65 78 3a 20 32 Data Ascii: rem; }}.list_performance > li .performance_img_wrap_parent { width: 70%;}@media screen and (max-width: 767px) { .list_performance > li .performance_img_wrap_parent { width: 100%; }}.list_architecture { position: relative; z-index: 2
2022-10-03 14:15:36 UTC	181	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 74 6f 70 3a 20 61 75 74 6f 3b 0a 20 20 20 20 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 7d 0a 7d 0a 2e 6c 69 73 74 5f 61 77 61 72 64 20 3e 20 6c 69 20 61 20 2e 6c 69 73 74 5f 61 77 61 72 64 5f 62 6f 78 5f 74 77 6f 20 2e 74 78 74 5f 77 72 61 70 20 2e 74 78 74 20 2e 74 74 6c 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 33 72 65 6d 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0a 20 20 63 6f 6c 6f 72 3a 20 23 30 31 35 38 39 61 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 72 65 6d 3b 0a 7d 0a 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 36 37 70 78 29 20 7b 0a 20 20 2e 6c 69 73 74 Data Ascii: transform: none; top: auto; left: auto; }}.list_award > li a .list_award_box_two .txt_wrap .txt .ttl { font-size: 1.3rem; font-weight: 700; color: #01589a; margin-bottom: 1rem;}@media screen and (max-width: 767px) { .list
2022-10-03 14:15:36 UTC	197	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 59 28 2d 35 30 25 29 3b 0a 7d 0a 2e 6c 69 73 74 5f 76 6f 69 63 65 20 3e 20 6c 69 3a 6e 74 68 2d 63 68 69 6c 64 28 65 76 65 6e 29 3a 3a 62 65 66 6f 72 65 20 7b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 22 3b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 65 64 65 64 65 64 3b 0a 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 68 65 69 67 68 74 3a 20 31 31 35 25 3b 0a 20 20 72 69 67 68 74 3a 20 63 61 6c 63 28 28 28 31 30 30 76 77 20 2d 20 31 31 38 30 70 78 29 20 2f 20 32 29 20 2a 20 2d 31 29 3b 0a 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 Data Ascii: transform: translateY(-50%);}.list_voice > li:nth-child(even)::before { position: absolute; content: ""; background: #ededed; width: 100%; height: 115%; right: calc(((100vw - 1180px) / 2) * -1); top: 50%; -webkit-transform: tra
2022-10-03 14:15:36 UTC	213	IN	Data Raw: 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 36 37 70 78 29 20 7b 0a 20 20 2e 74 6f 70 5f 74 74 6c 5f 77 72 61 70 5f 30 33 3a 3a 62 65 66 6f 72 65 20 7b 0a 20 20 20 20 77 69 64 74 68 3a 20 63 61 6c 63 28 33 36 30 70 78 20 2f 20 31 2e 37 29 3b 0a 20 20 20 20 68 65 69 67 68 74 3a 20 63 61 6c 63 28 31 37 34 70 78 20 2f 20 31 2e 37 29 3b 0a 20 20 7d 0a 7d 0a 0a 2e 74 6f 70 5f 74 74 6c 5f 77 72 61 70 5f 30 34 3a 3a 62 65 66 6f 72 65 20 7b 0a 20 20 77 69 64 74 68 3a 20 33 33 33 70 78 3b 0a 20 20 68 65 69 67 68 74 3a 20 31 36 38 70 78 3b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 2e 2e 2f 69 6d 61 67 65 73 2f 74 74 6c 5f 63 6f 6e 74 65 6e 74 73 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 63 65 6e 74 65 72 2f 63 6f 6e 74 61 69 6e 3b 0a 7d 0a Data Ascii: nd (max-width: 767px) { .top_ttl_wrap_03::before { width: calc(360px / 1.7); height: calc(174px / 1.7); }}.top_ttl_wrap_04::before { width: 333px; height: 168px; background: url(../images/ttl_contents.svg) no-repeat c enter/contain;}
2022-10-03 14:15:36 UTC	229	IN	Data Raw: 6e 67 2d 72 69 67 68 74 3a 20 32 38 70 78 3b 0a 20 20 7d 0a 7d 0a 61 2e 6c 69 6e 6b 5f 62 6c 61 6e 6b 3a 3a 62 65 66 6f 72 65 20 7b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 22 3b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 77 69 64 74 68 3a 20 32 33 70 78 3b 0a 20 20 68 65 69 67 68 74 3a 20 32 33 70 78 3b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 2e 2e 2f 69 6d 61 67 65 73 2f 6c 69 6e 6b 5f 61 72 72 6f 77 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 63 65 6e 74 65 72 2f 63 6f 6e 74 61 69 6e 3b 0a 20 20 62 6f 74 74 6f 6d 3a 20 31 31 70 78 3b 0a 20 20 72 69 67 68 74 3a 20 30 3b 0a 7d 0a 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 36 37 70 78 29 20 7b 0a 20 20 61 Data Ascii: ng-right: 28px; }}a.link_blank::before { content: ""; position: absolute; width: 23px; height: 23px; b ackground: url(../images/link_arrow.svg) no-repeat center/contain; bottom: 11px; right: 0;}@media screen and (max-widt h: 767px) { a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49814	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:52 UTC	1040	OUT	GET /wordpress/wp-content/themes/kawaken/images/low_main_img_topics_sp.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:52 UTC	1072	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:52 GMT Server: Apache Last-Modified: Wed, 28 Oct 2020 08:52:20 GMT ETag: "22fb8-5b2b747fbd900" Accept-Ranges: bytes Content-Length: 143288 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:53 UTC	1120	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c ff c0 00 11 08 01 72 02 ee 03 01 11 00 02 11 01 03 11 01 ff c4 00 b9 00 00 01 05 01 01 01 01 00 00 00 00 00 00 00 00 00 00 05 02 03 04 06 07 01 08 00 09 01 00 03 01 01 01 01 01 00 00 00 00 00 00 00 00 Data Ascii: JFIFddDuckyPAdobedr
2022-10-03 14:15:53 UTC	1136	IN	Data Raw: 24 8a ec 7e 63 4c 9b 7e 41 2c 9a 72 16 d7 3f 4e a2 f5 0c f3 52 5b 60 c8 b1 b3 21 00 d4 01 c8 72 27 7a 1a 7e 54 d0 9b 02 46 c6 51 10 46 b3 ab 48 49 64 04 48 a5 ea 95 ae c0 00 0f 4f 4d be 3a d2 d9 a6 46 4e 62 14 7e f1 67 66 af 16 97 94 6c 53 90 a8 24 0d c8 04 12 d4 d1 55 66 10 27 b5 12 b8 08 1a 59 02 f1 bc 45 e6 a4 fa 11 51 d4 7a 57 4d a9 9c 8d 5d 66 af ad ad dd 5d 89 e0 c5 e0 e0 9e c0 05 17 8b 10 db fc 7a 7f 76 9d 52 40 d3 05 7f 5b c8 cf 03 4c 90 91 c4 82 af ed 1e 9b d4 b5 35 9d 2a 98 bc 49 0b 94 b9 54 8e e2 7b ff 00 a5 91 fd aa f1 34 6c ab 5d bd c2 be a3 d3 f2 d1 51 3a 06 02 0d 9a b5 6b 88 60 59 92 d8 21 ab c6 23 56 8a 50 77 04 9f 6d 2b 4f 9e b4 58 20 bb ff 00 24 4f aa 31 47 1c 77 50 0a 33 a3 2a f0 34 15 d8 81 f0 a8 d5 b1 ab 35 b8 1b 09 5a df e2 65 86 36 Data Ascii: $~cL~A,r?NR[`lr'z~TFQFHIdHOM:FNb~gfIS$Uf'YEQzWM]f]zvR@[L5*IT{4l]Q:k`Y!#VPwm+OX $O1GwP3*4 5Ze6
2022-10-03 14:15:53 UTC	1248	IN	Data Raw: e7 8b 61 2d ae 52 e7 2b 61 82 b7 88 80 e2 7f a2 b6 57 d8 12 49 32 c7 32 9d 81 de ba aa ec 65 88 97 fd c6 55 c4 f6 8f ec 5e ed d5 51 6d 21 13 49 74 97 04 9b 2b 78 95 42 f0 eb c8 2c 6a 36 23 a1 03 7d 73 da d7 67 45 5e 3a 93 6d f1 b7 d7 2e 23 b5 c3 f6 1b f8 8c 4e 42 58 ac 54 71 26 a4 34 ee 39 54 d7 f4 d7 4b c5 f9 62 df b5 4a ec 89 f2 e1 e2 b6 95 c6 42 f3 15 67 2c 05 3b 96 dd c3 25 c5 25 00 06 5e 6b 1a 91 f3 07 a6 ab 5a cb 39 9f 71 c6 88 2f 67 8d c5 a4 31 48 72 a2 79 a7 71 14 10 c7 71 1c 08 59 7a 87 e2 a7 a1 eb 43 f8 6a 8b 1c 12 f7 9d f5 91 e1 82 c9 c2 cd 70 71 d0 84 42 d2 3c b0 da 2c b4 0a 6a a4 cb 73 73 27 4d f7 50 3a 7a 7a d5 55 11 6e cf c9 32 f3 1b 79 9b 8a 23 77 90 cc 5c c6 7d f6 93 45 37 24 8f 89 20 95 58 e4 50 0d 36 04 1a fc 34 ca ce bb 03 db 6d 6e 55 Data Ascii: a-R+aWI22eU^Qm!It+xB,j6#}sgE^:m.#NBXTq&49TKbJBg,:%%^kZ9q/g1HryqqYzCjpqB<,jss'MP:zzUn2y#w \}E7$ XP64mnU
2022-10-03 14:15:53 UTC	1264	IN	Data Raw: ed e4 b5 0c 97 11 49 3c a2 3a c2 d2 a5 1c f7 d5 94 95 71 e8 4f ce 8c 46 a6 de 4c 0e 45 86 98 53 01 f6 8b c8 b0 99 16 b8 c3 f9 23 d8 c4 d2 47 da 9a dd 4b a3 1e 12 11 ce 84 a9 db 6e bb 83 f9 6a 96 f9 0a 64 50 d0 dc 64 b3 e2 bc 6f c9 32 30 48 3c bb eb f2 af 61 17 08 a2 fe a0 ea 65 b7 2b c4 c3 1c 84 88 f8 80 84 90 47 41 fe d6 f2 b6 6a 53 5c 70 bf 80 d6 be a1 69 7e ce 8c 45 95 de 47 c4 3c a2 7f 1c 7b b2 5e de 0c a5 b4 4f 22 a8 5a 08 91 c3 82 2a 64 25 9c 23 13 b7 e6 bf f2 5c a1 64 ac ff 00 42 d6 fb 54 99 cd c7 db af 32 bd a2 cb 7d 81 b9 9a 19 85 c5 b6 4a 19 a6 86 53 34 67 97 73 6b 7e 52 16 14 00 37 4a 57 5d 15 f9 0c 2b 69 23 ee d6 20 0f 9c c4 79 15 b4 05 e7 b2 39 4b c8 e7 95 da f6 06 9e 55 88 14 64 48 a1 60 00 4e 2c 2a c3 88 27 a1 da 9a e8 c7 93 1d b5 4e 02 ab Data Ascii: I<:qOFLES#GKnjdPdo20H<ae+GAjS\pi~EG<{^O"Z*d%#\dBT2}JS4gsk~R7JW]+i# y9KUdH`N,*'N
2022-10-03 14:15:53 UTC	1280	IN	Data Raw: ad 9b 85 35 dc 35 c8 d6 e5 6a 7f b7 19 a4 37 02 39 e3 ba ec 33 19 92 2a 06 54 53 4e 42 bb 9e bb d3 5d 55 ec d5 94 59 24 27 83 f0 6b cc 85 c2 db c4 aa 2e 94 f1 68 65 aa 06 53 b0 0a 48 00 9a fc f7 fc 75 af 99 21 b7 35 cc 37 80 62 8b 4d 1d f6 21 4d f2 53 b8 20 99 d0 71 8c b5 49 52 29 53 c6 a4 ee 07 ed d7 16 5e c5 bc 30 a4 58 df ed bf 89 cc 0d df fc 9d 77 35 78 b9 48 a4 94 f4 1e e0 be e0 1a a4 12 05 0d 7f 0d b5 c7 7e ed 96 8e d0 25 92 2e 18 cc 35 e5 88 48 31 78 37 c4 62 62 01 bb ac bd da f2 3d 0c 7c 4b 33 9e 94 0b b7 ca 9a e0 cd 93 1d d4 d9 cb 11 a9 2f 36 d8 5f 26 53 33 fd 44 48 b2 b8 58 a1 51 ce 30 80 ec ff 00 b9 52 7f 0f d8 75 c1 7b 63 7b 26 2b a3 0f db e0 b3 52 37 09 2f e1 09 40 23 b6 8d 6a c2 4a 1e 26 ac f1 29 5f 95 45 3e 20 68 2c 69 ec 56 9d 77 60 ba 78 Data Ascii: 55j793*TSNB]UY$'k.heSHu!57bM!MS qIR)S^0Xw5xH~%.5H1x7bb=|K3/6_&S3DHXQ0Ru{c{&+R7/@#jJ&)_E>h,iVw`x
2022-10-03 14:15:53 UTC	1488	IN	Data Raw: 55 b7 2d 2a 46 cf 0d b5 bb 05 2e a5 a5 b9 e4 44 95 52 a0 1e 2a 09 a3 11 d7 4a fa f8 f6 48 59 aa 7f 81 41 f3 3b dc 82 dc 59 bd b7 96 62 70 56 12 45 db 86 f6 e1 4c 97 9f 53 33 30 78 5c c7 21 34 ed 0e a6 41 bd 3d 9c 77 17 c7 86 be 83 e8 f5 49 85 3c 37 1f e5 36 78 b1 80 c5 5b a7 92 41 14 cf 24 77 36 96 e2 23 03 3c 80 98 66 35 92 30 ac f5 29 23 7b 9f d6 9f bd 6e e5 70 38 b5 5b db 59 44 f1 d6 f7 dd 17 b9 6e 2d 16 e6 d2 c2 2c 5f 99 2e 75 9e 48 ae f0 73 c3 64 a8 d2 94 02 34 b7 9b e9 8b b0 01 4b 33 50 28 df aa f4 f3 7d 9a ee 76 3e ba 5a 71 72 67 3f ef 2c c5 83 a4 61 b7 3e c5 a7 ad 28 00 db 5e 63 67 d9 48 eb 25 db 91 ca e4 85 a5 59 b9 1a 8f 5d c6 d4 d0 93 36 ce 24 31 7b 5c bb 4e 3a 50 12 dc bf 0e ba c2 bb 24 49 48 0c ee a9 14 0c 55 88 5a f2 e2 07 a0 af 22 36 d0 25 Data Ascii: U-*F.DR*JHYA;YbpVELS30x\!4A=wI<76x[A$w6#<f50)#{np8[YDn-,_.uHsd4K3P(}v>Zqrg?,a>(^cgH%Y]6$ 1{\N:P$IHUZ"6%
2022-10-03 14:15:53 UTC	1504	IN	Data Raw: 48 da 9e 83 f0 ae b1 a0 1d 79 7d 15 ac 6d 23 d4 04 1b 81 4a ef d2 b5 db f6 e9 5d 82 aa 54 2e 33 df 5c e6 da 19 45 bc 81 49 36 ed ed 9c 8a 1a 1e 15 56 a1 a7 51 41 f0 3a 7c 78 2f 93 7d 11 ad 7a d7 6d 4a cd cc 99 7b 76 0d 0d db 4f 03 d0 c9 03 28 0e a4 0a 54 10 29 bf 52 29 eb d7 5d d8 f0 56 9b 1c d7 cb 6b 0d a5 e4 77 4b 47 86 16 91 7a 55 4f 31 f9 7a 7e 23 55 e2 22 72 2a 3b 99 22 24 06 91 10 b5 11 89 e4 bf 85 45 76 1f 02 2b a5 75 09 29 2f 24 e4 08 2a d4 35 0c bb 53 e0 41 53 50 7f 1d 26 a8 29 91 25 92 17 e4 1a 15 2b 5a 34 ab 46 fc 88 db f6 f5 f9 e9 95 8c c8 2d 69 42 4c 13 2d cc 74 a9 45 a8 09 ff 00 8a 36 a1 db e2 45 3e 07 54 50 c0 32 6d a4 5d c4 49 34 6a 7f 95 4a 32 fe 04 53 6f cb 46 05 6a 4f 95 ac e4 28 8e 19 26 24 71 12 6c ca 47 f8 49 d8 fe 15 d2 b3 41 27 8d Data Ascii: Hy}m#J]T.3\EI6VQA:|x/}zmJ{vO(T)R)]VkwKGzUO1z~#U"r*;"$Ev+u)/$*5SASP&)%+Z4F-iBL-tE6E>TP2m] l4jJ2SoFjO(&$qlGIA'
2022-10-03 14:15:53 UTC	1520	IN	Data Raw: bb 6a 8f 1c 44 e8 0b 4a 39 67 9c be 96 ce f6 6c 8d 95 dd 95 bc d5 92 6b 3e e9 9a 67 66 00 2c 60 91 c1 0b 1d 88 07 ad 7e 3a 17 aa 9d 19 b9 30 54 3e 57 e4 17 36 f9 5b 6b cb 0f a0 c4 f3 5b 7b 3b 6b a2 b1 01 02 a4 61 4a 02 0b 10 58 16 35 02 9b ef c5 47 06 78 aa a3 d4 6f 77 c0 53 0f e6 b8 6b 89 e5 b7 c7 20 bf ca b4 40 95 b7 69 54 4a b0 91 11 9a 40 c8 23 35 20 7b 83 0a 8f 43 a5 cb d7 7b b7 08 7e 70 89 4d 92 9f 21 6b 71 94 cc 62 e7 c7 d8 59 19 59 2c 0d c2 0b 99 12 2a 3b 17 b4 65 a8 d9 4b 06 2c 36 e3 d0 9a 6a 4e 8a ad 56 ae 58 37 05 62 7c b3 c7 fc b6 6e 78 c8 ee 24 c1 ce 24 86 26 95 26 84 dc 34 74 12 a3 f7 89 59 54 2b aa 2f 2f 55 24 96 af 2d 5f 27 5b 26 15 ae e1 bb f5 0e 45 04 36 b6 ac e2 ce 2c 0a c4 4c 56 d0 ac b6 b2 16 ab 97 e5 c9 c1 0b 43 57 d8 d4 d4 d7 96 fa Data Ascii: jDJ9glk>gf,`~:0T>W6[k[{;kaJX5GxowSk @iTJ@#5 {C{~pM!kqbYY,*;eK,6jNVX7b|nx$$&&4tYT+//U$-_' [&E6,LVCW

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:53 UTC	1536	IN	Data Raw: 9b 9f e0 09 6a 5b 8f d6 5e 3d c2 d8 63 63 6c 2d 9c 62 3c 75 cd a4 f2 f7 16 55 65 8d 8a 29 0b c5 87 6b f4 94 df 99 23 a1 e3 ad 92 ab ed 19 a6 fc 68 0c 78 2f 22 b4 68 66 86 e6 69 2e 1d 4b 45 23 ca 48 40 56 16 e1 2d c4 a9 05 59 79 16 61 08 60 39 05 0a c7 4b c9 2d 12 14 fa 19 af 66 c7 5e c3 32 7d 0a 59 ce dc 31 3f 54 2e a3 11 34 8c e5 9a 38 87 10 5a 30 8d c5 aa 37 d9 47 bc 95 ba a3 5f f9 86 1b 3b fd 1e e6 26 bd bf b7 bb c5 e3 ac d2 79 17 29 35 ac 29 14 a1 e6 9d 39 a2 bb 2a 29 25 14 2b 31 5a d3 71 41 5d 6a a4 b4 ae e1 74 70 01 ca 43 e3 d7 f0 5d 3c 18 32 d6 f6 96 8c f6 72 de c0 b1 b2 c6 b0 2b 39 82 d9 61 95 24 a2 0e 45 c5 00 0a 08 a1 1c 75 64 af cb 71 61 c8 5a 5c 6d 85 98 86 ea ca e2 5e fd fd b7 d4 5d 47 1d b2 ad ec d5 8b 9c 93 06 81 22 74 3c 48 a1 99 98 a8 d8 Data Ascii: j[^=ccl-b<uUe)k#hx/"hfi.KE#H@V-Yya`9K-f^2}Y1?T.48Z07G_;&y)5)9*)%+1ZqA]jtpC]<2r+9a$EudqaZ\m^]G"t<H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49818	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:55 UTC	1624	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo_footer.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:56 UTC	1624	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:56 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "e43c-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 58428 Connection: close Content-Type: image/png
2022-10-03 14:15:56 UTC	1624	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 ca 00 00 01 18 08 06 00 00 00 dc 6a b6 f8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 e3 de 49 44 41 54 78 da ec bd 09 80 5d 45 95 ff 5f cb dd de d2 7b a7 bb 93 ce 4e f6 b0 27 01 c2 16 02 02 82 80 3b 23 fa 43 c7 51 61 c6 19 77 1d 9c f9 cd fc 32 38 32 e8 1f 19 71 43 65 54 74 46 9c 11 06 dc 10 95 c5 b0 04 08 84 90 10 c2 9e 7d ed f4 de 6f bd 4b 55 9d 7f d5 bd ef 75 1a 44 4d 27 dd 9d a4 39 1f a8 dc 7e db dd ab be f7 54 9d 3a 87 10 04 41 10 04 41 10 04 41

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:56 UTC	1681	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:56 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "31e7-5b252e7c40940" Accept-Ranges: bytes Content-Length: 12775 Connection: close Content-Type: image/jpeg
2022-10-03 14:15:56 UTC	1682	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 02 00 00 64 00 64 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 50 00 00 ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04 04 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08 07 07 06 09 09 0a 0a 09 09 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 01 03 03 03 05 04 05 09 06 06 09 0d 0b 09 0b 0d 0f 0e 0e 0e 0e 0f 0f 0c 0c 0c 0c 0c 0f 0f 0c 0c 0c 0c 0c 0f 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:58 UTC	1721	IN	Data Raw: af 4b 41 f2 42 38 ac bd 65 e2 1f f1 0c ff 00 ee 6c 0f cd 0f 57 89 6f 82 7d 4c f9 af 74 3d d5 4b 44 7a f6 4f 26 71 45 cb 44 05 3a af 62 90 91 e3 e6 6c 0a 7d e8 7a bc 47 0d ce a6 70 8f a3 5e aa da f7 3f 70 99 9a 93 f6 91 6d 91 c3 bb ea 0f 23 cc d8 1f 9a 1e af 11 c1 73 a9 95 a7 a3 8e aa 9f 74 90 e6 c6 66 fe 32 ca 86 e2 ed 72 34 50 b8 d0 d5 a0 5f 5c d1 81 f9 a1 ea f1 1c 37 3a 99 f5 11 d0 e7 54 e7 1d c7 0b 65 72 55 ac f9 32 b8 0e 92 8e bf a4 9a 70 1e 7f 74 60 7e 68 7a bc 47 0d ce a6 52 8e 86 7a ad f0 d0 65 b2 19 0e a3 e1 a0 e1 e9 a7 a7 8a 47 92 e6 7c 0f cd 0f 57 88 e1 b9 d4 cd 7f fc 27 d5 69 24 cd 5b 29 7e 35 f0 a2 be 5d 3d ff 00 a2 28 fe e7 c0 fc d0 f5 78 8e 1b 9d 4c ec 36 0f 2f 8e ab 2f 93 17 08 b6 aa 7d b9 6b 59 21 0e dc 3c 28 cc 9b 7c d5 57 17 a0 8b 87 de Data Ascii: KAB8elWo}Lt=KDzO&qED:bl}zGp^?pm#stf2r4P_\7:TerU2pt`~hzGRzeG|W'i${)~5]=(xL6//}kY!<(|W

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49826	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:58 UTC	1722	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_facebook.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:59 UTC	1723	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:59 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "28a-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 650 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:59 UTC	1723	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 31 38 37 37 65 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 35 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#1877ef;}.cls-2{fill:#fff;}</style></defs><title> 1</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49827	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:59 UTC	1722	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_twitter.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:15:59 UTC	1724	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:59 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "3db-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 987 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:59 UTC	1724	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 31 64 39 65 65 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 33 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 67 20 69 64 3d 22 44 61 72 6b 5f 42 6c 75 65 22 20 64 61 74 61 2d 6e 61 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#1d9eef;}.cls-2{fill:#fff;}</style></defs><title> 3</title><g id="_2" data-name=" 2"><g id=""><g id="Dark_Blue" data-na

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49828	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:00 UTC	1725	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:00 UTC	1726	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:00 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "16b4-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 5812 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:00 UTC	1726	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 30 20 35 30 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 32 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 69 6d Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 50 50"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 2</title><g id="_2" data-name=" 2"><g id=""><im

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49830	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:00 UTC	1725	OUT	GET / HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:02 UTC	1732	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:00 GMT Server: Apache X-Powered-By: PHP/7.4.5 Link: <https://kawanakajima.co.jp/wp-json/>; rel="https://api.w.org/" Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-10-03 14:16:02 UTC	1732	IN	Data Raw: 62 65 66 33 0d 0a Data Ascii: bef3
2022-10-03 14:16:02 UTC	1732	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 73 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 73 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 21 28 49 45 20 37 29 20 7c 20 21 28 49 45 20 38 29 20 5d 3e 3c 21 2d Data Ascii: <!DOCTYPE html>...[if IE 7]><html class="ie ie7" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if IE 8]><html class="ie ie8" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if !(IE 7) | !(IE 8)]><!-
2022-10-03 14:16:03 UTC	1740	IN	Data Raw: 74 65 6d 22 2c 22 70 6f 73 69 74 69 6f 6e 22 3a 31 2c 22 69 74 65 6d 22 3a 7b 22 40 74 79 70 65 22 3a 22 57 65 62 50 61 67 65 22 2c 22 40 69 64 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 5c 2f 22 2c 22 6e 61 6d 65 22 3a 22 5c 75 33 30 64 62 5c 75 33 30 66 63 5c 75 33 30 65 30 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 5c 75 35 64 64 64 5c 75 34 65 32 64 5c 75 35 63 66 36 5c 75 35 65 66 61 5c 75 38 61 32 64 5c 75 33 30 36 66 5c 75 33 30 30 31 5c 75 37 34 62 30 5c 75 35 38 38 33 5c 75 33 30 36 62 5c 75 39 31 34 64 5c 75 36 31 36 65 5c 75 33 30 35 37 5c 75 33 30 35 66 5c 75 35 64 65 35 5c 75 34 65 38 62 5c 75 36 32 38 30 5c 75 38 38 35 33 5c 75 33 30 36 65 5c 75 39 35 38 62 5c 75 37 36 37 61 5c 75 33 Data Ascii: tem","position":1,"item":{"@type":"WebPage","@id":"https:\/\/kawanakajima.co.jp\/","name":"\u30db\u30fc\u30e0","description":"\u5ddd\u4e2d\u5cf6\u5efa\u8a2d\u306f\u3001\u74b0\u5883\u306b\u914d\u616e\u3057\u305f\u5de5\u4e8b\u6280\u8853\u306e\u958b\u767a\u3

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:03 UTC	1747	IN	Data Raw: e3 83 bb 3c 2f 73 70 61 6e 3e e7 a4 be e9 95 b7 e6 8c a8 e6 8b b6 3c 2f 61 3e 3c 2f 6c 69 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 0a 20 20 20 20 20 20 3c 2f 6c 69 3e 0a 20 20 20 20 20 20 3c 6c 69 20 63 6c 61 73 73 3d 22 73 75 62 5f 6e 61 76 5f 6c 69 22 3e 3c 61 20 68 72 65 66 3d 22 23 22 3e e4 bc 9a e7 a4 be e6 96 b9 e9 87 9d 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 63 68 65 63 6b 62 6f 78 22 20 69 64 3d 22 69 74 65 6d 34 22 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 6c 61 62 65 6c 20 66 6f 72 3d 22 69 74 65 6d 34 22 3e e4 bc 9a e7 a4 be e6 96 b9 e9 87 9d 3c 2f 6c 61 62 65 6c 3e 0a 20 20 20 20 20 20 20 20 20 3c 75 6c 20 63 6c 61 73 73 3d 22 73 75 62 5f 6e 61 76 22 3e 0a 20 20 20 20 20 20 20 20 20 20 Data Ascii: <li class="sub_nav_li"> <input type ="checkbox" id="item4"> <label for="item4"></label> <ul class="sub_nav">
2022-10-03 14:16:03 UTC	1755	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:05 UTC	1780	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:05 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "5e397-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 385943 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:06 UTC	1781	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 5d 07 80 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 ef d8 8e 10 50 45 00 00 05 04 14 40 01 50 54 51 05 00 51 04 50 05 10 14 00 04 50 00 10 00 00 00 45 10 54 01 50 01 44 01 50 00 Data Ascii: JFIF"#"" ""#>1++1>H<9<HWNNWmhm"#"" ""#>1++1>H<9<HWNNWmhm]"PE@PTQQPPETPDP
2022-10-03 14:16:06 UTC	1797	IN	Data Raw: ec dc d8 f4 a9 3d 5d 72 dc 95 ab df b1 ce c9 5b 46 4b 95 9b 66 ed fc dc eb 73 c6 c6 16 66 cb c3 82 48 a3 ea b4 39 8e c2 b7 4f 15 3b 78 5d 05 9f 36 d3 db d1 c3 9a e7 4d c8 cb 06 a7 53 95 e6 bd a5 8a 58 bd 77 93 75 d2 49 77 3f 6f 4e f7 3b db f1 f6 ba cf 17 fa 33 e6 bf 5e a9 0b 22 f1 6f 4a c0 ad d2 60 74 9e 71 e8 f3 ee 59 9f 4f cb 78 5e 8f 7f 77 37 8a f4 bc bf 38 74 ac f5 bf 43 c4 cd cb ad da cf e5 5d 77 04 bd 14 fc 82 e4 65 a6 8d be a7 2b 15 2b 4a 59 8e 8c 96 a8 7a 0e a7 9a c0 49 7f 1e f3 75 29 52 5d 7a 94 5d 5b 5e d7 32 fd 65 c9 be cd bc aa 73 ea d8 89 d1 49 56 09 db 1c 71 6e 4e 98 dc e5 59 a2 d3 ec eb b2 bb 56 2b 33 56 92 a3 9b 79 61 14 93 9a af a8 fa b1 f5 36 67 a6 5b a7 43 77 16 9d bc dc 46 74 1a 3c e7 5d ca d4 d4 ca 2b c4 b3 e9 4b 62 f4 28 e8 d5 78 d7 Data Ascii: =]r[FKfsfH9O;x]6MSXwulw?oN;3^"oJ`tqYOx^w78tC]we++JYzIu)R]z][^2esIVqnNYV+3Vya6g[CwFt<]+Kb(x
2022-10-03 14:16:06 UTC	1816	IN	Data Raw: 33 63 36 33 73 3b 86 6e 5a 64 89 b4 d8 cc cd a6 66 c2 71 3e 39 84 71 c6 a6 6a 66 b3 13 10 56 67 6d 84 d4 cd 4c c4 d1 a6 8d 34 69 a9 fa e6 66 66 66 67 ff 00 83 e2 69 34 3f d7 c4 20 63 eb 83 fe 8f 3f e8 f8 da 1e 66 48 31 59 5b d7 6e 7e 39 05 17 0c cd 3f 2c cf 20 61 38 e4 6d b1 e3 1c f9 69 3c 47 d3 2b 99 83 9c 4d 5f e3 47 3e c2 85 9a e7 98 cb 08 0a 71 38 e4 cc 9c 0c 73 ea 6d ac ee 09 9d 8f 1c 8e 27 6c 95 da 37 fb 62 79 c6 f5 37 26 06 33 6c 4d f1 3b ad f3 b8 33 d8 99 04 42 a6 63 e9 80 60 53 ee 6a bf 21 84 3a fc fb fa 88 72 27 94 e7 30 ae 60 53 35 79 a9 f9 c4 ff 00 69 ea 1f 53 22 12 07 d3 c3 dc fe 26 ad 30 66 ad ee 05 84 63 9f a8 35 0e 4f 7a 99 dd aa 77 a7 7c 4e ea ce ec da 6c 67 94 0a df 3a 8f 9f c7 d6 5e 7e e4 4d f3 35 3f 25 18 89 d8 79 a1 fe de cd b3 4b 31 Data Ascii: 3c63s;nZdfq>9qjfVgmL4ifffgi4? c?fH1Y[n~9?, a8mi<G+M_G>q8sm'l7by7&3lM;3Bc`Sj!:r'0`S5yiS"&0fc5Ozw|Nlg:^~M5?%yK1
2022-10-03 14:16:06 UTC	1832	IN	Data Raw: 47 22 3b 12 4f d3 73 36 81 ab 85 97 e3 31 79 9a 10 b1 69 a7 dc de 81 05 d5 1f c4 9c fd 06 20 d3 e4 22 cd 71 ea 6c 07 b1 62 17 d0 6f 0d ff 00 c6 ca d1 92 ac 42 b5 28 cc 2d 93 35 2c c4 aa 00 a3 9c cc cc 98 ea ed 12 b3 98 07 f2 d5 d7 91 9b 0d 69 c0 44 b8 c1 4b 86 c9 ec 73 92 d4 ae de 05 bb 40 2c dd cb 39 9d 9d a9 0f 2b ae f3 93 3e e2 e8 b7 75 27 98 f6 81 58 9d e6 22 7e 52 ba f0 03 0e cb 85 e7 b2 f3 b0 36 20 fd ba c1 50 2c 70 6a f7 8e da 2a 8e ea fd b1 38 1f 6e 82 28 02 66 66 16 c4 de 64 fc 76 94 fe 42 9a c4 34 d7 99 a8 59 ac c0 87 45 8b d4 d8 33 07 52 fb 60 6e 31 c9 65 c6 61 61 c4 73 f2 11 8b 20 33 99 b3 67 13 6f 79 29 52 9c 9e d0 fe cc 27 a8 d5 bf 33 46 1c 44 5b f1 09 d5 67 70 33 11 1b 6d 8e c2 bc f3 05 5f 9e 11 ad a8 36 82 db c8 63 2c ea bc 71 35 b0 9c b3 Data Ascii: G";Os61yi "qlboB(-5,iDKs@,9+>u'X"~R6 P,pj*8n(ffdvB4YE3R`n1eaas 3goy)R'3FD[gp3m_6c,q5
2022-10-03 14:16:06 UTC	1848	IN	Data Raw: 6a 61 64 44 f0 ee dc fe d8 b6 7c b9 62 44 f5 19 73 88 a9 14 22 c5 b1 48 8e 58 8f 00 c2 6e 27 5c fb 1a 04 5e 8e b1 f9 75 55 d4 2a c4 2a 33 89 89 55 61 d4 e4 31 5f 42 b1 9e 3b 53 b0 33 b4 6e 9d 1b 30 74 43 e5 e8 44 0b 9e 97 ca bd 8f a5 30 63 89 fa 92 04 35 98 07 94 c6 0b 03 93 9f a0 24 43 75 9d b2 93 a1 7e 9a c1 db 7e b5 b6 a4 85 a7 a0 a7 b2 93 ae a5 aa a0 ca 3a 02 69 46 96 33 56 2f 51 47 4d 7b d4 af 2d b9 92 96 0d 49 b7 5c 8a fa cb 35 55 64 bb cf 74 1d 4d af 59 10 f9 13 9b 2e 7b 94 56 7a 33 5d 21 f7 ea 5f 2a a6 9a 8d 7e fa 81 79 af 56 a7 5e a2 d3 e4 68 e2 bd a8 d6 a4 5a d7 a8 ea ce 30 81 8f cd 4c b5 50 b2 db 5a c3 fb 74 5b d3 53 fb 86 c2 f7 f0 db 01 d5 33 38 74 b1 49 ac 93 ab 4f 4a af 3a 2d ad ea 4c ed 3f c5 be f0 f4 1a 2b 24 43 6e e8 da 5b 53 d7 e4 b4 da Data Ascii: jadD|bDs"HXn'\^uU**3Ua1_B;S3n0tCD0c5$Cu~~:iF3V/QGM{-I\5UdtMY.{Vz3]!_*~yV^hZ0LPZt[S38tIOJ:-L?+$Cn[S
2022-10-03 14:16:06 UTC	1864	IN	Data Raw: fd ba 18 c1 79 27 af ac 77 2c 2b e5 9e 69 ae d5 44 61 dc ea e9 62 f3 b9 8b 85 b2 fe ad 99 c9 3f a6 d8 05 bc f5 56 ae ca 47 dc 96 e2 35 8a 42 cb 3a a4 d0 e5 6f 40 b8 5a f3 f3 8d 23 f9 89 db 60 dc 74 7d 20 b7 ba 19 ff 00 4c fc 71 68 d6 e6 10 b1 6e 27 4d 5f 52 ca c5 17 44 e2 3d 62 c4 31 e8 7d 35 50 ee ae 44 a6 8b 6d ce 2c 5c d0 14 ba 2a 3e ad 4d fd 22 2e 96 de f5 33 e5 05 24 89 42 f4 ba 2a 3b d1 52 69 85 15 25 ea 53 fe ab 83 85 ea b4 bc 87 43 58 63 ab b2 b2 1c 1a da c4 46 20 5c d3 60 df 93 d1 83 ba 2e 1a 27 41 d3 56 b3 ac e8 aa a8 29 4e 92 86 bd 9c 47 e1 89 27 9e 62 ea 16 02 4b 4e 09 10 2f 3f 43 39 c4 cc 09 9e 4f 0a 04 f7 33 f4 f9 cc 6e 0c 3c fa 54 e7 99 90 3e ad 9c c2 17 13 65 03 00 01 89 8e 27 1b 8c 30 9a b0 39 98 cf 03 18 18 81 58 45 16 4c f8 91 01 c7 10 Data Ascii: y'w,+iDab?VG5B:o@Z#`t} Lqhn'M_RD=b1}5PDm,\*>M".3$B*;Ri%SCXcF \`.'AV)NG'bKN/?C9O3n<T>e'09XEL
2022-10-03 14:16:06 UTC	1880	IN	Data Raw: d1 59 2c 0d 54 bb 9e 96 47 95 2d d6 fc 34 7a 62 bf 36 a7 fe a7 8c 1f 8b 4a b1 56 31 c5 cc 8f 0b 38 6f a8 8d af c4 4d a7 2d 0d a2 b2 51 7d 58 eb c1 24 48 c9 1c 32 26 1f 7d 0c 3e c4 0d a5 78 27 26 c7 7e e6 3d 8b 18 c6 34 49 09 ee 68 8d f5 6b 24 59 b3 89 d0 c1 b5 46 d3 ec 6d 3e 30 25 2a 36 6e f7 c5 91 44 13 38 52 27 f0 6b f2 6c dd 1b 31 67 b9 18 ff 00 d2 51 37 5d 06 56 7b 11 d4 d1 e4 57 5d 06 ab b2 ab 16 84 22 6c 97 b6 0d 9f 0f 89 10 fb 9c 5a 75 11 08 f6 a3 67 1a 6f 02 7a f4 22 c8 c9 b4 f4 5d 0d a4 a1 fc ad 0f e7 03 8b b7 aa d0 87 a5 fe 19 21 9e ac 62 c9 5e 74 e9 be 4d ee 87 a1 76 23 28 be 68 93 c8 d5 e9 46 63 7a a2 1f 26 24 31 f0 99 ae a4 6f c9 1f b1 85 bb 08 6c bf 82 3b 98 8c 1b 5a f6 27 c4 33 ae e7 43 dc 9c a8 d9 1b 34 6c e2 42 bd 8e 52 59 dd 49 74 22 3c Data Ascii: Y,TG-4zb6JV18oM-Q}X$H2&}>x'&~=4lhk$YFm>0%*6nD8R'kl1gQ7]V{W]"lZugoz"]!b^tMv#(hFcz&$1ol;Z'3C4lBRYIt"<
2022-10-03 14:16:06 UTC	1896	IN	Data Raw: 48 70 fd 58 42 e2 c9 c8 d3 f7 11 2c 63 b1 11 23 c8 5b 97 d3 7b 96 f6 6a 2b 20 fe 98 b7 7f 04 1a f6 3f 09 f8 ba 3d 0b 8a bf 92 a9 2a 45 d4 9e b2 e6 4b 0f 90 91 2b 57 67 1f 17 53 f0 dd 59 3f ce cc 4a d7 c1 97 c9 1b 2c 4b b9 0e 0a d4 86 ae f8 bb 13 af 6a 29 d6 94 6c e9 f9 a2 3a d3 47 23 90 af 25 5b 59 c5 92 b8 c9 69 d0 b5 0e 1c df 5d d2 8b 62 b1 b4 eb af 42 76 b9 ab 25 1f c5 cc e1 4f aa 2d cf 8a ac cf f9 b4 12 55 c8 ea 4b 56 b2 fc 1f c6 50 d1 17 f4 31 7e 5c f9 15 f1 18 5c 5a 09 8c 92 24 be 77 47 8a 3d 08 c9 64 8b 75 d2 c8 fc ea 63 04 b2 de 32 4a 35 e4 ca 25 f9 8c d6 04 fa 96 7e 84 11 14 7a 7c 13 19 4f b1 b3 48 b2 72 89 b5 b7 f0 4a a6 b2 9a 29 be 52 b2 39 79 7e 4d 8a 6f b9 0a 72 c3 88 b9 a6 fb 1b 54 d1 c8 83 d3 a9 9a d2 cd 9b 94 7b 11 7d af 53 fc 47 ec eb bb Data Ascii: HpXB,c#[{j+ ?=*EK+WgSY?J,Kj)I:G#%[Yi]bBv%O-UKVP1~\\Z$wG=duc2J5%~z|OHrJ)R9y~MorT{}SG

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1912	IN	Data Raw: 17 d9 5f 37 00 8d 45 f7 04 bc 2e b5 d2 5b 01 17 57 08 29 03 9b 5e bc 4d 60 9a 5d 67 e2 2d 40 2a 9f 26 6c 9c 8a 4a 6d b4 5d e1 3d 4b 06 54 73 0f ba 6c 19 0d c0 aa d2 15 28 cb b7 dd 32 ee 8b eb c4 30 74 2e dd 09 87 44 ae be 21 e4 b3 87 92 1d d8 c2 eb f5 02 42 02 e9 dd ca 00 c8 e2 a1 61 98 c5 e3 53 2d e0 88 56 f0 68 6b 83 a2 cc 65 97 de 38 58 98 56 b7 ef 09 cc 33 dc 79 59 7a 27 74 fb 10 ba 8b 6a ee 30 42 66 a5 49 c6 6d a8 15 a0 ee 66 f4 5d 53 b9 6a 05 93 2c d8 99 6e ad b4 22 2c 1a dd 7f 12 9b 7b 78 2d af f7 2c 8d 4d 72 7d c2 b7 96 69 2e e1 40 1c ac 04 f8 85 03 a8 70 32 88 43 c9 fe 20 3b 15 a4 79 fb c3 5a 69 54 33 61 11 5d 77 33 f7 99 57 64 c5 96 4c a1 ed a1 fa 8a ab 56 0a 04 38 34 bd 68 a2 d6 56 2b af 32 d7 a0 2a 95 bf 89 47 bd 03 85 a6 89 9a 0f c8 3f 92 12 Data Ascii: _7E.[W)^M`]g-@*&lJm]=KTsl(20t.D!BaS-Vhke8XV3yYz'tj0BfImf]Sj,n",{x-,Mr}i.@p2C ;yZiT3a]w3WdLV84hV+2* G?
2022-10-03 14:16:06 UTC	1928	IN	Data Raw: 20 d1 0d e0 2a 5b a5 bf 09 87 6a e5 cb f1 2b 45 de 3c f9 8d 75 4a 5c 17 e9 2d 84 59 34 d3 e2 2e 5b 15 57 7a 80 83 f9 56 be f2 c1 55 7d 4e 36 d7 78 88 aa d0 2a a3 9d 44 42 1b e8 7c 62 3a b2 4b de fd c5 d6 47 25 ea 30 d0 f1 e4 7e d2 d2 8a dd 35 ea 16 5f 6c 5f de a7 8a 48 df ee 60 a9 bc 01 8f cc 59 4a 2d 2e be ae 50 27 e7 96 64 6b 39 af ee 62 c0 3b bb b9 8e 0b a4 54 b1 7f 2a 93 77 39 72 80 d1 15 cd 23 9e 7e d1 07 04 55 56 7e 0b 8b 6f ae d0 4a df cc 31 1f 3f 78 2a 85 0d 14 16 56 f9 19 2b 52 9e a1 cd 2e 51 d6 6c 9b ad fb 9b 8a 2f 81 fa a9 71 b0 dd 99 24 ac be b2 1f dc bd 2e 23 83 7a a0 94 71 7a c0 7e 97 11 68 57 7b 22 5a 64 56 62 5b b0 b2 0a 1e 94 32 5a 97 86 e5 c5 c1 78 73 99 4a 32 4d 86 79 8f ce 74 0b 7d b3 1a 12 76 b8 6d 10 31 a5 5f 8d c2 ae 60 f8 5f 1b 96 Data Ascii: *[j+E<uJ\-Y4.[WzVU}N6x*DB|b:KG%0~5_I_H`YJ-.P'dk9b;T*w9r#~UV~oJ1?x*V+R.Ql/q$.#zqz~hW{"Zd Vb[2ZxsJ2Myt}vm1_`_
2022-10-03 14:16:06 UTC	1944	IN	Data Raw: 58 50 42 70 0c 29 e1 5a e6 ae 2b 03 87 c6 2e 6a 2e 68 c3 a8 17 ae bb 7f e4 78 59 86 bc dd 66 5d 9f aa 2f 68 6f 74 99 9a 9a 81 9a ca 58 b0 c6 f7 ac 41 43 c0 8b 28 bf 33 2e 98 d3 c4 93 5e 66 88 75 a2 a1 1c 82 59 b9 f1 b8 09 44 56 4c 95 28 a0 ff 00 c7 64 5b 64 d6 9e ce 13 dc a5 b7 6b 35 0b 76 f8 0e 67 18 5f 6d c1 fd 00 13 7f 64 6e 4b 46 b4 de a5 4e 2e 4c 71 ce 39 96 16 d9 2a fc e2 5e cf 43 49 33 87 cc a0 06 2e 80 07 a8 b8 0d 8e e3 d4 dc 89 82 9b fd e2 56 ff 00 44 4a 75 8e 17 1a cf f3 30 13 23 a3 bc 24 68 f4 2d 75 89 b7 d3 51 ef d1 34 0a e8 02 ab db 30 ec 99 13 77 cc e7 1b 1c 8f 19 c5 d0 5f b2 f5 2c 34 6e dc 7c 54 03 25 33 a1 f7 0e ec a9 4b f8 b1 8a 85 55 5f 93 27 53 ad d0 04 ba ea 18 44 cc d8 b3 cb 0c d5 c8 b6 cf bb 2d fd ee 2b 6c 4b b6 01 ca 3d cd fb 95 b2 Data Ascii: XPBp)Z+.j.hxYf]/hotXAC(3.^fuYDVL(d[dk5vg_mdnKFN.Lq9*^CI3.VDJu0#$h-uQ40w_,4n|T%3KU_'SD-+lK=
2022-10-03 14:16:07 UTC	1964	IN	Data Raw: a9 7a aa b6 34 d7 11 1b 7d 80 81 78 9e 61 d3 0a e8 6f d4 b0 06 99 ad a5 11 ee 20 ca a6 f4 e4 80 8c 0b 93 a8 d9 11 b7 c9 04 60 be 74 fe e5 00 29 be 0e a5 5f de 41 55 c1 9f 71 26 19 32 bf 77 d1 d6 74 1b e7 39 6f d3 fe e6 4d 6d 4c b7 32 d4 bd 87 50 05 87 4f e5 99 93 62 2a af 57 ff 00 61 ab be b1 bf cb 1d c3 91 d0 cd fa 62 81 cd d9 19 79 0a e0 5a 2d c6 65 29 45 4a 91 37 9e 22 b9 77 ad c6 fa b7 c4 dd 7d e2 a5 af 05 f7 02 5d d7 82 69 84 b0 21 59 79 a3 98 85 8e ba 42 d8 19 0d b0 50 af 81 c4 c2 35 18 6e b8 ea 28 c1 ae 1f 12 85 33 b7 5f 76 30 d5 83 46 93 26 0d c8 af 88 5d aa d1 da d8 3a ff 00 84 ea 15 2a 2e 6d 16 4a 7c f8 dc 45 0b 55 4b 35 b6 33 9a 99 80 31 dd c4 90 55 39 87 2f b4 8a 4f 1a e6 91 5d 32 ce ca e3 f7 80 32 6a 3a b1 19 2e 8f 15 04 9e 65 2d 57 d5 04 0c Data Ascii: z4}xao `t)_AUq&2wt9oMmL2POb*WabyZ-e)EJ7"w}]i!YyBP5n(3_v0F&]:*.mJ|EUK531U9/O]22j:.e-W
2022-10-03 14:16:07 UTC	1980	IN	Data Raw: 16 90 e0 e3 ee 8c e6 be 23 6c 02 6b a6 25 57 c4 1f 4a b7 d6 2b 18 83 db 19 5b 94 a2 f1 5e e5 b5 0d 8e 04 41 d8 06 b5 0a b1 74 f9 1d 41 f4 a8 c7 c6 38 d3 14 ff 00 de 20 ba c0 d4 f2 4a 9c 4c be 77 db ce 86 6d 9e 06 c2 74 73 bc 3f 10 6a 12 de 39 47 b8 04 ec 08 a2 16 46 78 f2 2a 8c 11 3d a3 c4 cf 14 1e 5e a2 97 60 04 ed b6 f9 80 5c 30 2b 77 ea 2a 5b 72 89 ba 8b 32 29 44 53 31 39 c1 4e d8 37 8a a1 76 12 35 00 55 17 97 a9 46 5c 6c 12 58 fb 0a a7 f1 1e c6 4e 15 73 94 1e e0 98 2e 89 9f 36 06 b0 fd aa f8 80 28 9f 3a 61 43 47 a2 d2 cb f8 b8 6b 78 95 01 b2 a2 84 23 89 a7 86 9d 59 c4 43 81 67 26 de e0 99 a4 69 2f 73 93 dc 39 d3 1a b1 c5 7b 97 f0 07 19 59 f8 8a 59 81 75 87 10 c9 f7 8e 6f 89 58 d7 b8 71 28 96 bf 32 a6 53 59 74 f5 11 eb 17 ee 47 68 1d 27 9f 70 38 85 61 Data Ascii: #lk%WJ+[^AtA8 JLwmts?j9GFx*=^`\0+w*[r2)DS19N7v5UF\lXNs.6(:aCGkx#YCg&i/s9{YYuoXq(2SYtGh'p8a
2022-10-03 14:16:07 UTC	1996	IN	Data Raw: f3 4f f1 1f 09 fc 67 f0 9f 1e 1f 87 ac 8f f3 3f 91 89 93 79 31 3d 7c 85 c7 f8 1a fe 53 f8 4f 80 f8 7e 26 25 fe 30 c7 27 c4 32 18 9f 3e f1 ba f8 31 e3 21 f1 bc 66 15 c9 cf c7 89 db f2 99 a1 f8 4c 98 7c 3f 13 e0 f9 9e bf 84 f8 7f 84 fe 7c 7c 38 e4 c8 7f 10 f9 99 3f 8c fe 0f c4 fe 33 f8 4f 99 fc 67 f2 9f e3 9f c6 64 ff 00 20 1f ca 7f 39 93 e0 3e 26 4c 72 7f 92 64 c9 93 8d 7f 09 fc 27 f9 df 93 fc 11 fe 4f f3 7e 53 13 f8 4f 97 e5 fa f8 03 9f 8f 5f 0f c4 cb f1 be 33 5d e4 c7 13 26 4c 99 3e 7c 66 bb f8 fc e3 93 e2 6b e6 7f 33 f1 32 7f 07 26 1f 1d ff 00 00 99 31 c9 90 cd 66 be 7c 67 58 07 c4 f8 97 0f 99 f0 64 c3 0c df c3 fc e6 4f 98 7f 09 f3 30 3f c0 fc ef f9 cf e1 3e 1f fe 59 f2 9f 33 27 f3 9f e6 3f 8a 7c 4f e5 1c 9f 33 25 c9 93 27 cc f8 9f c8 c9 f3 e3 3a fe 66 Data Ascii: Og?y1=|SO~&%0'2>1!fL|?||8?3Ogd 9>&Lrd'O~SO_3]&L>|fk32&1f|gXdO0?>Y3'?|O3%':f
2022-10-03 14:16:07 UTC	2012	IN	Data Raw: f4 43 88 0b 8e b6 dd 4a eb b5 67 12 d2 1b ff 00 21 22 60 a7 a6 34 47 76 84 0c 12 6c f2 20 ce e6 37 88 ae 0d 23 a7 45 31 23 81 4a 14 da ae ee 2d e4 a3 5a 47 8d 9b 4c 7b fb 05 82 a6 ce 5a 32 f8 d2 90 11 3c 93 58 a6 98 9d 7e 81 ab fd 60 c7 b2 de 3d 34 21 9d 16 8f f2 2b ac 79 59 83 eb 66 dc 60 11 84 0a 43 c5 5c 27 29 bc 1d 78 86 cc ed 49 00 f6 3b 4c 27 c4 57 45 f0 2e 38 be 77 86 0d 78 55 78 28 dc 75 4a eb 9e 30 90 ce 09 1b 27 26 f2 61 7a 6a a7 82 57 92 f9 c1 ad 11 24 14 e0 e1 ce 04 7b 93 24 eb 63 02 80 f1 a0 28 9e 70 bc 49 40 5f ad 1b ca 12 c7 6a e8 11 19 87 5b 54 20 df 84 c3 05 43 42 c3 8d 3f d1 8e a7 24 11 c5 ea c5 c1 1b 80 75 02 fd 74 cb 84 71 21 89 0e 73 cb b0 23 4b 63 af 58 ba dd 4f 41 59 36 22 e0 63 1d e1 bf 6e 2c a5 5e 76 0c b4 c9 27 25 4f 3d 39 29 6d Data Ascii: CJg!"`4Gvl 7#E1#J-ZGL{Z2<X~`=4!+yYf`C\')xI;L'WE.8wxUx(uJ0'&azjW${$c(pI@_j[T CB?$utq!s#Kc XOAY6"cn,^v'%O=9)m
2022-10-03 14:16:07 UTC	2028	IN	Data Raw: 1a 34 d3 ac 85 d5 49 24 a5 00 53 04 5d b5 1a 41 86 fb c0 0a 41 49 87 91 0d 66 c3 46 d0 be cb 8a e3 79 aa 78 4d 68 cb ec 00 0a 37 ed cb 74 ed 72 7e da d0 60 a5 37 20 57 b5 d5 db 9c 8b ec 87 b5 3d dc 0e 13 60 07 db 9c e5 64 01 07 d8 95 c2 eb 3f 0e 8e fb 1e 43 04 03 6f 04 e4 e0 30 b8 23 b6 94 2d 0e 9c d3 c0 5d 11 76 79 b8 0b 10 26 40 73 dc a6 1f ba 95 0a f9 26 6d db 88 10 78 a3 06 f2 63 2b a2 a0 ab ce 0c 9c 9f c5 a7 94 1d e4 07 b8 5f 28 4a 85 fb c6 26 9d 63 15 dd 68 31 00 d5 c8 00 73 60 eb 1b 88 41 ea ba e9 df 4e b3 a8 8b 16 43 9d c5 c0 e4 4d a9 8c 6f 95 3d 64 69 78 90 80 d3 a7 58 89 20 0d 80 73 3e 74 f8 e9 a2 52 7d e2 a5 70 56 06 b1 0c 1b bf 1d df 16 71 05 08 d6 94 09 6a 61 44 a0 46 ad e0 5f 33 14 16 89 4d 79 7f a1 8e a0 a8 ba 26 a9 5d 7a 19 be d9 53 83 c7 Data Ascii: 4I$S]AAIfFyxMh7tr~`7 W=`d?Co0#-]vy&@s&mxc+_(J&ch1s`ANCMo=dixX s>tR}pVqjaDF_3My&]zS
2022-10-03 14:16:07 UTC	2044	IN	Data Raw: 35 e3 81 d5 03 5e 4b 8b 78 56 82 d1 e7 01 cb 27 08 e3 9d 9d 0c a8 51 84 43 10 a5 5c 32 a8 a2 9c 1f 78 9e c6 55 ee 28 66 08 79 b9 57 4b 6a 75 ce 30 22 00 03 4f 4f 57 04 15 e8 c2 4e 51 49 cd a7 d0 14 ae 45 1b 03 35 02 8a 01 44 bc e1 bb 0a a5 a9 5e 59 de 71 9e 2d a2 cd c2 37 9a f8 70 4d d0 40 d8 c7 f0 37 5d 67 90 60 82 50 07 dd 33 43 44 c6 9a 75 07 dc 7b e6 ed 25 57 d5 01 10 b8 1b de 40 3c ae f3 9b 3a 83 7d 1c b8 93 ae 70 9b 9f 63 cf b5 e0 7a fb 00 9e 94 f5 85 46 1a 8a 82 04 a6 98 7c 21 88 95 be bc 4c c6 a0 a3 8d 41 d0 77 ef 2b bf 25 cd 0a 70 9b b7 59 10 3a 78 e6 de 10 87 aa c4 97 2e b2 4f f5 0c b7 06 68 19 80 1e 3b c2 1b a2 40 25 2f 61 c1 c6 31 01 0b aa f5 88 16 df e6 e9 d0 2c c9 0a b2 24 7c a1 89 0d de d8 b1 1d 62 f0 5e 3a 89 6b 8d a3 00 2d 4f 26 68 e0 c4 Data Ascii: 5^KxV'QC\2xU(fyWKju0"OOWNQIE5D^Yq-7pM@7]g`P3CDu{%W@<:}pczF|!LAw+%pY:x.Oh;@%/a1,$|b^:k-O&h

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:07 UTC	2060	IN	Data Raw: 34 e2 01 02 a3 55 4d 25 33 77 6e 0d e7 1e e8 5c 08 28 9e 8e dc 22 9b 4b e9 14 6d c3 50 f5 68 53 d9 63 83 42 92 56 69 87 94 a2 a4 d7 01 18 77 a9 84 da eb 69 36 e2 30 93 89 31 b5 06 b8 a1 82 4f ac 33 ab ae 7d 63 84 11 64 01 50 50 b2 0f 69 1b c5 76 5b b3 58 68 25 0f 06 d9 74 9b 38 56 32 90 9d 00 8c a0 da 12 1f 0a 9d a6 52 c8 49 02 81 23 de 2e c1 2a 55 05 2c 65 09 89 8b be 85 d1 8a 55 40 03 82 05 ad ce a7 16 41 36 8f 20 63 75 24 3b 80 dd d4 ce 38 6a c9 c1 0c 2c e3 35 da dd 20 6c d5 72 79 dd 58 60 85 ce 37 e6 c9 74 0c 03 63 54 b5 1e 5d 98 eb b2 f0 a1 30 78 f7 43 74 75 c8 65 95 b 0 c1 93 af 77 1a 3d 46 80 44 d3 19 3b 8b 3e 08 d4 9a 3c e4 cf 26 00 3c 91 b3 66 05 5a 08 d2 88 d9 a8 63 64 1f 42 fc b0 5 1 ca f5 67 90 84 83 0c 0f 7a 43 8b 4a dc ac 8f 58 55 d1 72 31 25 Data Ascii: 4UM%3wn\("KmPhScBViwi601O3}cdPPiv[Xh%t8V2RI#.*U,eU@A6 cu$;8j,5 lryX`7tcT]0xCtuew=FD;><&< fZcdBQgzCJXUr1%
2022-10-03 14:16:07 UTC	2076	IN	Data Raw: e3 c6 7d be fa 18 ce db 85 2f b9 6e 9c ad 24 58 87 91 d2 5c 52 0c c2 12 a3 bd 31 29 ec 4f 4d 5d 62 da 16 16 72 86 72 39 ce a9 f0 17 c5 63 bf c4 4e c8 9d 32 49 19 f0 1c 74 e6 c2 33 a0 62 43 4a 02 14 e1 7b b9 5d 08 78 7c 58 e2 8f 5d ee 17 12 4e 75 b0 5c 7b 12 1b 83 a2 e1 15 96 94 4f 42 1c 02 82 93 78 ed 74 08 d4 7b b4 c3 d1 2d 04 43 cb 58 2d 3e 3b 50 1e 8c 17 2b c2 ec eb ef a7 21 b5 b7 30 3d 8a 60 d4 05 a2 a4 ae 35 84 62 98 b5 81 d2 31 b9 d8 96 f3 c8 86 37 4a ee 8c 6c 29 6e 53 21 c0 9b 8e 9d b5 90 a2 8e c0 40 78 05 c4 15 13 a0 a9 ea 8e 52 40 50 ba 1e 97 02 f8 a2 50 ad 34 06 1 e f0 d4 3e d1 38 2b 57 13 97 48 55 31 20 ae 80 8b c0 ac a9 0f 40 a9 fd 99 92 d0 e2 40 03 09 ac 07 a4 30 a8 6d f1 d2 f7 9 5 2e 9a 62 6f d1 83 19 a8 9b db 35 c4 c7 85 e1 00 19 9d d3 f6 27 Data Ascii: }/n$X\R1)OM]brr9cN2lt3bCJ{]x|X]Nu\{OBxt{-CX->;P+!0=`5b17Jl)nS!@xR@PP4>8+WHU1 @@0m.bo5'
2022-10-03 14:16:07 UTC	2092	IN	Data Raw: 29 47 ce 72 6c 5d 05 a6 88 d8 1c 64 c1 8a 14 c0 b8 08 d4 a0 73 70 e4 5f f0 0e 3c 76 e8 00 ef 7c 67 13 99 62 90 e2 e0 50 58 70 d6 62 b6 ef e9 0f 92 66 89 1e 00 fa 2c 2b 5d aa 91 42 f4 8b 30 b0 22 c6 ea f3 49 a7 06 db c4 74 38 69 38 24 a7 bd 1c 10 ac dc 24 df bc d8 26 c6 3c 65 f1 90 88 03 38 a0 61 3b 1d b0 bf 82 63 30 29 38 ee e6 be 63 20 4e 39 1c 2c 09 2f 13 65 9f 5e f0 db 42 b1 46 f1 b4 71 62 0c b0 01 37 b0 eb 1d 05 cc d2 73 6b 27 87 d8 b5 30 9b 4e 23 63 cc 37 0b e3 dd f2 dc 84 c9 54 cb 27 4f 46 72 e1 94 a6 ec 16 61 57 4b cf a2 7b eb 15 26 1d d6 77 8b f8 a9 34 86 06 f0 02 cf 94 59 3f 2a 61 64 74 f8 07 f6 26 6c 68 ab bd 3a 03 66 1e 62 bb db 3d 2e 71 d1 0e 8b ec f2 61 4a 4a d4 11 30 51 75 d4 2e b7 89 9b 71 40 c8 c0 3a 6c 72 62 51 7d b5 97 d5 66 3d c1 a3 b7 Data Ascii:)Grl]dsp_<v|gbPXpbf,+]B0"It8i8$$&<e8a;c0)8c N9,/e^BFqb7sk'0N#c7T'OFraWK{&w4Y?*adt&lh:fb=.qaJJ0Qu.q @:lrbQ}f=
2022-10-03 14:16:07 UTC	2108	IN	Data Raw: 37 ba e6 0c 77 1a d9 a9 75 50 c0 0b 1f 37 fb c1 ef 23 bd 51 5d 17 1b 03 79 db 79 4c 20 f2 3c d3 33 79 13 78 0a d1 d4 cb 05 28 87 87 e3 1c 04 aa 7b 66 2e 8a c4 26 14 57 6a 75 90 be 15 5d 81 f4 18 30 76 8c 76 c2 00 05 87 8e 30 d7 6d 5b 6e f0 2e 1a 9e 86 03 d1 8e ea 5e 47 9c a0 80 7b db 9c 4d 4f 0a 4c 52 e9 d9 a6 73 8e 93 2b ca e0 73 9a 51 7a 70 03 a7 3f d9 76 dc ac 3b 41 ef 80 80 62 2c 65 9e 5c 3e 0a 61 2f 14 5f af 78 97 72 63 c3 2e c6 5b bf 38 d4 7c f6 58 3f 6f ac 8d 29 c0 de f0 5c 03 72 71 82 da 38 17 bc 8c 29 a2 e8 60 4f f4 b1 27 58 1b 5b c5 fa 32 81 83 49 af 37 1a f0 12 17 f0 26 3d 3a ed db cf 97 bc 25 70 61 a8 83 45 f3 90 69 03 a7 04 dc 3e 5c 5c de 00 1b 6d 7d 46 1a b2 b7 e4 43 70 ce 0d 11 91 f3 85 ed ad 83 ac 70 d4 66 1b 36 12 62 0a 85 1e b9 c9 40 d0 Data Ascii: 7wuP7#Q]yyL <3yx({f.&Wju]0vv0m[n.^G{MOLRs+sQzp?v;Ab,e\>a/_xrc.[8|X?o)\rq8)`O'X[2l7&=:%pa Ei>\\m}FCppf6b@
2022-10-03 14:16:07 UTC	2124	IN	Data Raw: 09 b8 e0 6d 05 9d e1 21 45 6d 2b e8 b8 68 5c 6b 16 40 a9 bf d5 62 6c 49 22 02 7b 4e d0 ae d0 8d c7 30 14 35 61 a0 00 12 2c c5 6e d0 01 b8 30 91 f4 c6 b3 28 03 cf 98 cd c8 85 ae 66 f6 a8 49 e9 63 c7 98 eb de 69 2c 49 24 ca bd e5 f2 44 1e d7 06 dc 09 41 bb 42 77 0d 17 48 26 00 2c 6d 73 10 5b a3 31 8e 01 58 5c 90 5b f3 08 37 a8 99 e4 98 ba b6 31 28 df 63 31 de d5 53 09 17 aa 8f de 0e 61 5a f7 9a 88 ea 31 d2 c6 a9 dc bd 5c 5a e7 70 60 22 f5 c6 04 75 57 c0 31 bd ae 28 24 54 0b c7 10 31 e4 4d 37 47 79 90 72 d6 0c b3 67 7d a0 a1 bc db 63 29 79 97 1c 6c 09 8c 41 b8 78 37 02 8d 89 9a 77 13 35 82 a1 68 cc a0 59 22 a6 40 6a 66 3d 8c c8 a3 76 23 ee 0c a3 5a ae 0a 8f a4 32 ad 93 18 9d f1 d4 0b 56 04 0d 1 6 f8 89 71 0a ed 00 a1 0e d4 6a 1f 37 17 9e 2e 2d 93 66 20 e0 c5 Data Ascii: m!Em+h\k@bll"{N05a,n0(flci,l$DABwH&,ms[1X\[71(c1SaZ1\Zp`"uW1($T1M7Gyrg}c)ylAx7w5hY"@jf=v #Z2Vqj7.-f
2022-10-03 14:16:07 UTC	2140	IN	Data Raw: a0 52 54 91 ec 61 7b 21 86 c6 29 e0 cd c4 2c 6a ea 84 fa 7d e2 ad d7 98 db 98 dc 51 35 cc b9 59 94 d1 a1 00 6e f5 10 93 70 da 81 cc df d8 40 3b 54 4d cb 1a 6e d2 88 37 b1 f3 2e c4 2a 28 ee 3b 4a 6d d4 d7 b1 80 58 28 48 e4 18 94 ac 0f e2 70 2b 6b bb 30 90 3b 7d a6 c2 e6 d4 6a 67 f9 85 c1 05 40 d9 63 b8 04 93 f6 33 ea 25 1a c4 d4 08 ad e0 d3 a4 9e 20 ab 0b 30 a2 6c 6c 99 8c de c4 78 00 c6 7f 94 9a ad 7f cc 18 94 81 64 78 31 1a d9 9b 4d 72 26 24 72 40 33 16 46 61 5f e2 05 2c 84 55 9b 12 dc f5 06 1d e6 4c b9 c8 09 48 09 a2 0e d0 9c d9 3e 60 e8 07 6f 7b 9e 92 c8 5d 42 62 de af 9d e6 22 08 d3 46 36 21 65 e9 40 e2 7a 9f 99 49 b5 f1 71 80 52 c0 1f 30 e7 72 bf 2f 7d 88 22 3a 5a d4 5c b8 ce d4 de f0 63 6d 5f 36 87 8e c6 06 62 e4 b7 db b4 57 25 15 d9 48 ee 26 5a 28 Data Ascii: RTa{!),j}Q5Ynp@;TMn7.*(;JmX(Hp+k0;}jg@c3% 0llxdx1Mr&$r@3Fa_,ULH>`o{]Bb"F6!e@zlqR0r/}":Z\ cm_6bW%H&Z(
2022-10-03 14:16:07 UTC	2291	IN	Data Raw: 1c 6d b3 51 94 0c 54 5a c1 a3 7d e2 2a 8d d0 38 04 62 05 14 73 09 3e 95 b1 19 c3 36 d0 71 c3 65 44 01 54 12 09 9e a5 3d bc 45 35 b5 6a 20 c1 22 e1 bb 3c 40 af 58 a8 0f 06 e1 18 04 45 0b 96 17 37 03 89 57 34 99 7d 62 22 ea 5a 28 1e 22 3e a1 46 26 c7 b4 d5 57 d4 e0 e9 e3 69 ac fd e3 ee e2 35 71 2f bd 19 8a 81 08 b2 2c f1 14 01 64 cd 2f 48 02 e2 9b 94 7d 30 98 47 2d 1d 98 85 22 bc 93 53 6d 8f 12 f2 61 bb aa a8 c0 6e 39 24 cb 17 03 b1 06 1b f2 bc 08 c4 9d c2 84 36 07 63 0d b0 03 11 9a 94 52 cd ad 80 49 ef 05 b3 56 4c 35 35 1d 91 86 a3 00 39 03 bc 04 38 96 94 79 26 01 b6 9a e1 1 4 2c 9f 68 c3 e2 05 24 79 a9 5a 76 4e 6a 7a 42 92 41 31 81 da 1b 23 93 1d 45 ee 96 03 12 2c 42 4b 33 1a 1e d1 ad 98 81 b4 08 59 85 1c 5e 25 d0 5a 26 1f 55 28 24 08 ac a0 11 73 51 8e d5 Data Ascii: mQTZ}*8bs>6qeDT=E5j "<@XE7W4}b"Z(">F&Wi5q/,d/H}0G-"Sman9$6cRIVL5598y&,h$yZvNjzBA1#E,BK3Y ^%Z&U($sQ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49719	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:35 UTC	30	OUT	GET /wordpress/wp-includes/css/dist/block-library/style.min.css?ver=5.4.11 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:35 UTC	32	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:35 GMT Server: Apache Last-Modified: Fri, 24 Apr 2020 15:32:14 GMT ETag: "d159-5a40b11d01b80" Accept-Ranges: bytes Content-Length: 53593 Connection: close Content-Type: text/css
2022-10-03 14:15:36 UTC	65	IN	Data Raw: 2e 77 70 2d 62 6c 6f 63 6b 2d 61 75 64 69 6f 20 66 69 67 63 61 70 74 69 6f 6e 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2e 35 65 6d 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 65 6d 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 61 75 64 69 6f 20 61 75 64 69 6f 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 69 6e 2d 77 69 64 74 68 3a 33 30 30 70 78 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 7b 63 6f 6c 6f 72 3a 23 66 66 66 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 2e 61 6c 69 67 6e 63 65 6e 74 65 72 7b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 2e 61 6c 69 67 6e 2e 72 69 67 68 74 7b 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 62 75 74 74 6f 6e 5f 5f 6c 69 6e 6b 7b 62 61 Data Ascii: .wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em}.wp-block-audio audio{width:100%;min-width:300px}.wp-block-button{color:#fff}.wp-block-button.aligncenter{text-align:center}.wp-block-button.alignright{text-align:right}.wp-block-button__link{ba
2022-10-03 14:15:36 UTC	81	IN	Data Raw: 20 69 6d 67 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 67 61 6c 6c 65 72 79 20 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 69 74 65 6d 20 69 6d 67 7b 77 69 64 74 68 3a 61 75 74 6f 7d 7d 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 67 72 69 64 20 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 69 6d 61 67 65 20 66 69 67 63 61 70 74 69 6f 6e 2c 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 67 72 69 64 20 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 69 74 65 6d 20 66 69 67 63 61 70 74 69 6f 6e 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 67 61 6c 6c 65 72 79 20 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 69 6d 61 67 65 20 66 69 67 63 61 70 74 69 6f 6e 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 67 61 6c 6c 65 72 79 20 2e 62 6c 6f 63 6b 73 2d 67 61 6c 6c 65 72 79 2d 69 74 65 Data Ascii: img,.wp-block-gallery .blocks-gallery-item img{width:auto}}.blocks-gallery-grid .blocks-gallery-image figcaption,.blocks-gallery-grid .blocks-gallery-item figcaption,.wp-block-gallery .blocks-gallery-image figcaption,.wp-block-gallery .blocks-gallery-ite
2022-10-03 14:15:36 UTC	97	IN	Data Raw: 61 76 69 67 61 74 69 6f 6e 20 2e 77 70 2d 62 6c 6f 63 6b 2d 6e 61 76 69 67 61 74 69 6f 6e 2d 6c 69 6e 6b 2e 69 73 2d 65 64 69 74 69 6e 67 2e 68 61 73 2d 63 68 69 6c 64 3e 2e 62 6c 6f 63 6b 73 2d 65 64 69 74 6f 72 2d 69 6e 6e 65 72 2d 62 6c 6f 63 6b 73 7b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 2e 31 35 29 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 7a 2d 69 6e 64 65 78 3a 31 3b 74 6f 70 3a 31 30 30 25 3b 6c 65 66 74 3a 30 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 6e 61 76 69 67 61 74 69 6f 6e 20 2e 77 70 2d 62 6c 6f 63 6b 2d 6e 61 76 69 67 61 74 69 6f 6e 2d 6c 69 6e 6b 2e 68 61 73 2d 63 68 69 6c 64 3e 2e 77 70 2d 62 6c 6f 63 6b 2d 6e 61 76 69 67 61 74 69 6f 6e 5f 5f 63 6f Data Ascii: avigation .wp-block-navigation-link.is-editing.has-child>.block-editor-inner-blocks{display:flex;border:1px solid rgba(0,0,0,.15);position:absolute;z-index:1;top:100%;left:0}.wp-block-navigation .wp-block-navigation-link.has-child>.wp-block-navigation__co
2022-10-03 14:15:36 UTC	113	IN	Data Raw: 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 2c 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 2e 61 6c 69 67 6e 63 65 6e 74 65 72 7b 64 69 73 70 6c 61 79 3a 66 6c 65 78 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 7b 6d 61 72 67 69 6e 3a 30 20 31 36 70 78 3b 70 61 64 64 69 6e 67 3a 30 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 2d 72 65 76 65 72 73 65 64 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 6d 6e 3a 66 69 72 73 74 2d 63 68 69 6c 64 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 7d 2e 77 70 2d 62 6c 6f 63 6b 2d 74 65 78 74 2d 63 6f 6c 75 6d 6e 73 20 2e 77 70 2d 62 6c 6f 63 6b 2d 63 6f 6c 75 Data Ascii: olor:transparent}.wp-block-text-columns,.wp-block-text-columns.aligncenter{display:flex}.wp-block-text-columns .wp-block-column{margin:0 16px;padding:0}.wp-block-text-columns .wp-block-column:first-child{margin-left:0}.wp-block-text-columns .wp-block-colu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49837	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1781	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_img_sp.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:06 UTC	1960	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:06 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "16c87-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 93319 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:07 UTC	2156	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 02 8a 02 ee 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 f4 10 01 50 14 41 40 00 10 00 00 11 40 41 40 01 00 01 14 01 0 0 04 00 44 51 10 01 00 40 10 09 80 50 15 00 01 44 51 00 00 00 11 Data Ascii: JFIF"#"" "*#>1++1>H<9<HWNNWmhm"#*"" "*#>1++1>H<9<HWNNWmhm"PA@@A@DQ@PDQ
2022-10-03 14:16:07 UTC	2172	IN	Data Raw: 9d 32 95 e5 58 4b a8 36 85 71 55 96 54 31 16 fb 1a 0b df 88 3a 86 05 a5 dd 49 71 89 d4 9b 42 7e 9d 81 2e e9 e2 d7 49 ad 21 e9 86 32 0f 4a 67 da d9 3b 17 09 62 5c a5 58 f5 25 d4 b6 3a 4b c9 ce 7a 9b 57 6d 67 af 7b 7f 05 cc af bb 91 0d 69 10 7f ea 41 f8 3d dc c3 b0 10 58 44 47 2c 09 98 3f 3c 01 31 31 31 fc e5 c7 10 9c fb d4 91 90 50 f1 3b 62 0f 73 fe 9b d8 c3 5a c4 09 b9 87 88 ab b8 e7 8f 4a 5c e2 2d af f2 a3 3c ce 73 36 f8 9b 99 99 99 dc 20 89 9f a0 4c ce c1 9d 8f e7 b2 25 bf a4 67 89 1e 3e 0b ed ad ce 71 87 f8 fb 8d 6b 0a 3d fb 00 7b 9d c2 06 05 5d 3b db 42 ed d3 74 d5 6f 71 37 9a 8f 85 75 5d 6e 55 05 fb 3b 98 ec 88 bb 44 ef 58 aa e2 cb 0f 6a b0 d5 f4 d9 4c 8d 0e c3 b5 d4 5b a2 ca 9b 5a 81 36 91 65 9c da 95 94 2c bd f7 ad 5a 53 66 55 59 ed 2a 54 06 f0 4f Data Ascii: 2XK6qUT1:IqB~.I!2Jg;b\X%:KzWmg{iA=XDG,?<111P;bsZJ\-<s6 L%g>qk={];Btoq7u]nU;DXjL[Z6e,ZSfUY*TO
2022-10-03 14:16:07 UTC	2300	IN	Data Raw: 4e e9 a6 75 d7 11 6a f7 bd a2 a5 59 6b 43 a8 f4 c6 26 2b 8a ca fe d0 76 1c bd 13 8b 62 11 16 4a 0e 4d 93 82 2b 75 72 e4 4a 09 70 41 c5 db f7 80 1e 97 78 cc 5b a8 68 be 5d f9 8b c3 55 0c be d6 46 a9 8e 3f 6a 58 32 a2 80 bf 30 7b 07 57 ed 00 a9 ca 6d a8 86 61 c0 15 9e b0 cb fa 58 07 d9 9e 93 72 3e d0 aa f2 e0 fc 4b 43 52 73 1c 77 c9 16 19 5d 27 10 46 cb fc ca dd 8a ee c0 d1 ba f1 04 55 eb 63 ed 2a b1 e9 cb 28 a0 b6 7a ff 00 52 ca 7a e9 0a d1 eb 68 06 50 bb 6d fb 83 b4 49 4c 62 39 f4 2d 92 0d 75 33 3f 10 8a f7 dc 37 71 d0 fd ce 04 f6 db 1d 71 6b 7f cb 94 ac ad ec 59 6c 94 bf 0b e3 31 c5 8a 31 46 e2 70 be 20 55 e6 61 b0 1b f5 78 97 44 d6 02 5a de d3 08 1a 50 5e 9d aa 0c 69 be f4 fa 4b 21 4c af 93 e6 e2 72 5f 12 fc 42 8d d9 df 13 d5 be ed cc d7 5b 85 b0 79 aa Data Ascii: NujYkC&+vbJM+urJpAx[h]UF?jX20{WmaXr>KCRsw]'FUc*(zRzhPmILb9-u3?7qqkYI11Fp UaxDZP^iK!Lr_B[y
2022-10-03 14:16:07 UTC	2316	IN	Data Raw: 00 01 3f 10 ff 00 55 9f ee b3 6f fe ac ff 00 7d 9f ef b3 fd f6 7f ba cf f7 d9 fe eb 3f dd 67 fa ec 3f fd d6 7f be cf f7 59 fe fb 3f dd 67 fa ec ff 00 7d 9f eb b3 fd d6 7f be cf f7 5c ff 00 7d 9f ef b3 fd f6 7f be cf f7 d9 fe eb 3f df 67 fa 6c 3f fd f6 7f be cf f7 58 7f fb ac ff 00 75 9f ee b3 fd f6 7f ae cf f7 d9 fe eb 3f df 67 fb ec ff 00 75 9f ef b3 fd d6 7f be cf f7 59 fe eb 3f df 67 fb ac ff 00 75 9f ee b3 fd d6 7f be cf f7 59 fe eb 3f dd 67 fb ac ff 00 5d 9f ef b3 fd d6 7f ba cf f7 d9 fe eb 3f df 67 fb ac ff 00 75 9f ee b3 fd f6 7f be cf f7 59 fe eb 3f dd 63 ff 00 ea b3 fd d6 3f fe fb 39 ff 00 ea cf f6 59 fe eb 3f dd 67 fb 2c 7f fd 96 3f fe cb 3f d9 67 fb 2c ff 00 7d 9f ec b3 fd d6 7f a2 cf f4 59 fe eb 3f d9 67 fb 2c ff 00 45 91 c9 93 26 4c 99 32 7c Data Ascii: ?Uo}?g?Y?g}\}?gI?Xu?guY?guY?g]?guY?c?9Y?g,??g,}Y?g,E&L2|
2022-10-03 14:16:07 UTC	2332	IN	Data Raw: bc 81 07 16 82 b8 93 08 36 3b 99 c9 70 54 ce ea 80 12 68 e2 4d 64 f5 02 51 89 da 82 0c 27 38 24 65 85 50 f1 c1 96 d7 a2 8a a3 a6 9a 1c 2b cb 04 f5 ed a0 61 e1 7a b9 0e 9a 55 c7 4b 80 65 38 6f 26 54 62 a1 9e 00 b8 16 c3 1b d1 6c 56 cc bf 89 d1 46 eb 5b 93 07 dc 0d c6 1e 12 c3 23 6c ca ea e0 07 0c 19 05 49 aa 38 4c 37 8a 28 da 92 a8 a6 5d 8b 04 0e 48 07 07 1b c6 c7 80 55 41 70 31 84 c9 9f fe 89 c3 9b f6 c4 ad ea f0 3c 05 39 c7 a9 6e 91 bc 08 cd 27 a2 84 c0 f3 d2 9a 07 43 a2 bb e5 c6 23 d9 b5 ca 91 8e 6e 23 80 03 83 4d 46 ae 6e 24 e6 cb cc 8b 97 c4 d9 01 f2 d4 03 00 14 e1 93 5 e 65 79 c6 6b 49 a5 17 12 b3 ef 39 4a a5 1a dc 26 a8 e1 d3 3f 4e dd e5 76 22 a9 aa e0 53 8c 01 27 04 7f e0 73 9d ec 9a b6 2e 81 c2 45 99 c1 82 5d 15 31 8c 86 44 0b 4d 8d 84 4f 66 2b 18 Data Ascii: 6;pThMdQ'8$eP+azUKe8o&TblVF[#Il8L7(]HUAp1<9n'C#n#MFn$^eykl9J&?Nv"S's.E]1DMOf+
2022-10-03 14:16:07 UTC	2442	IN	Data Raw: 92 08 1c 85 24 0c a6 08 ec 43 86 69 22 95 d1 e3 fc 8b 16 bc 66 73 90 04 59 36 a7 c0 f0 28 20 ce 4c 8b 91 a4 b9 36 44 a6 16 92 5d 83 32 bc 49 b3 3f e8 55 59 44 91 c8 ed 45 46 31 57 e8 15 c3 03 80 51 d8 8c 54 68 42 46 5e 65 01 40 50 24 f5 fd 10 ce db 7d ac ad bc 0b b4 30 c6 89 a8 bf cf d7 c6 23 f9 cf a0 8a d0 36 b2 9b 58 c2 3a a1 2a f1 36 08 d5 83 be 24 69 33 28 93 d0 38 25 dc 02 58 e0 66 1f 06 73 20 0f 60 49 83 68 07 68 9c b9 31 49 7c 33 3c 9e 69 8a b9 3e 5f 4b 23 e1 ca 8d 4a 2b 95 89 ca 05 f2 79 28 30 d8 57 c5 0b 96 5b 06 12 56 f0 12 0b 02 85 e4 20 c6 98 5c 8e 5b 08 0f 72 b5 01 d8 91 f1 5a 05 93 13 0a 2a f2 a6 36 28 47 31 86 89 14 61 c2 d9 58 47 40 3a 16 12 06 6c 55 fc d2 e4 43 00 4c 8f 46 25 d9 50 c7 38 29 d3 ec 49 22 4c d2 41 34 d8 e1 71 b1 dd 09 68 33 Data Ascii: $Ci"fsY6(L6D]2I?UYDEF1WQThBF^e@P$)0#6X:*6$i3(8%Xfs `Ihh1I|3<i>_K#J+y(0W[V \[rZ*6(G1aXG@ :lUCLF%P8)I"LA4qh3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49838	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1813	OUT	GET /wordpress/wp-content/themes/kawaken/images/ttl_topics.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:06 UTC	1960	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:06 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "9bab-5b252e8011240" Accept-Ranges: bytes Content-Length: 39851 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:07 UTC	2188	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 34 30 2e 30 39 20 31 30 33 2e 37 31 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 64 32 64 32 64 32 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 38 2e 39 34 2c 36 31 2e 35 37 6c Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 240.09 103.71"><defs><style>.cls-1{fill:#d2d2d2;}</style></defs><title> 1</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M8.94,61.57l
2022-10-03 14:16:07 UTC	2204	IN	Data Raw: 6d 2e 32 36 2d 31 39 2e 38 2e 30 36 2d 2e 30 39 2e 39 32 2d 2e 31 39 63 2d 2e 31 31 2e 32 34 2d 2e 34 31 2e 33 35 2d 2e 38 39 2e 33 34 5a 6d 2e 31 37 2e 38 34 2e 30 36 2d 2e 30 39 2e 39 32 2d 2e 31 39 63 2d 2e 30 37 2e 31 38 2d 2e 33 36 2e 33 31 2d 2e 38 37 2e 34 32 5a 4d 33 30 2c 34 39 2e 31 36 6c 2e 31 37 2d 2e 33 36 2e 38 34 2d 2e 31 37 61 2e 34 38 2e 34 38 2c 30 2c 30 2c 31 2d 2e 33 32 2e 33 39 5a 6d 30 2c 32 2e 35 34 2c 30 2d 2e 31 37 48 33 30 5a 4d 33 30 2e 30 37 2c 35 30 6c 30 2d 2e 30 37 2e 30 38 2c 30 5a 6d 37 2d 32 2e 38 35 2d 2e 31 34 2e 31 61 2e 31 39 2e 31 39 2c 30 2c 30 2c 30 2c 30 2c 2e 31 37 6c 2d 2e 32 35 2e 33 37 61 32 33 2e 33 2c 32 33 2e 33 2c 30 2c 30 2c 30 2d 33 2e 33 36 2c 31 2e 30 38 63 2d 31 2e 38 33 2e 36 34 2d 32 2e 38 38 2c 31 Data Ascii: m.26-19.8.06-.09.92-.19c-.11.24-.41.35-.89.34Zm.17.84.06-.09.92-.19c-.07.18-.36.31-.87.42ZM30,49.16l.17-.36.84-.17a.48.48,0,0,1-.32.39Zm0,2.54,0-.17H30ZM30.07,50l0-.07.08,0Zm7-2.85-.14.1a.19.19,0,0,0,0,.17l-.25.37a23.3,23.3,0,0,0-3.36,1.08c-1.83.64-2.88,1
2022-10-03 14:16:07 UTC	2284	IN	Data Raw: 2e 31 76 30 63 2e 31 31 2c 30 2c 30 2d 2e 31 37 2e 31 31 2d 2e 31 39 68 2d 2e 31 33 6c 2e 30 35 2d 2e 30 38 76 30 63 2d 2e 31 34 2d 2e 34 38 2e 33 31 2d 2e 35 33 2e 31 38 2d 31 2c 2e 31 32 2e 30 39 2c 30 2d 2e 31 2e 31 2d 2e 30 36 73 30 2d 2e 31 38 2c 30 2d 2e 32 38 68 30 6c 2e 30 36 2d 2e 31 33 63 2e 31 36 2e 31 34 2d 2e 31 32 2d 2e 31 34 2c 30 2c 30 2c 2e 32 35 2d 2e 33 2e 32 36 2d 2e 38 2e 34 35 2d 31 2e 31 39 68 2d 2e 30 35 63 30 2d 2e 31 2c 30 2d 2e 32 35 2e 31 33 2d 2e 33 73 2d 2e 30 37 2d 2e 32 31 2d 2e 30 36 2d 2e 32 34 2e 31 33 2d 2e 31 34 2e 31 31 2d 2e 31 31 2d 2e 31 33 2d 2e 32 33 2c 30 2d 2e 33 34 2c 30 2d 2e 33 39 2e 31 34 2d 2e 33 34 68 30 63 2e 31 38 2d 2e 33 2c 30 2d 2e 33 34 2e 31 39 2d 2e 34 38 68 30 6c 2d 2e 34 32 2d 2e 35 31 4c 32 Data Ascii: .1v0c.11,0,0-.17.11-.19h-.13l.05-.08v0c-.14-.48.31-.53.18-1,.12.09,0-.1.1-.06s0-.18,0-.28h0l.06-.13c.16.14-.12-.14,0,0,.25-.3.26-.8.45-1.19h-.05c0-.1,0-.25.13-.3s-.07-.21-.06-.24.13-.14.11-.11-.13-.23,0-.34,0-.39.14-.34h0c.18-.13,0-.34.19-.48h0l-.42-.51L2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49841	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1814	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_ttl.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1964	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:06 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "160fb-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 90363 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:07 UTC	2220	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 38 36 2e 30 31 20 31 39 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 69 73 6f 6c 61 74 69 6f 6e 3a 69 73 6f 6c 61 74 65 3b 7d 2e 63 6c 73 2d 32 7b 6f 70 61 63 69 74 79 3a 30 2e 36 3b 6d 69 78 2d 62 6c 65 6e 64 2d 6d 6f 64 65 3a 6d 75 6c 74 69 70 6c 79 3b 7d 2e 63 6c 73 2d 33 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 686.01 194"><defs><style>.cls-1{isolation:isolate;}.cls-2{opacity:0.6;mix-blend-mode:multiply;}.cls-3{fill:#fff;}</style></defs><title>1</title><g
2022-10-03 14:16:07 UTC	2236	IN	Data Raw: 32 6b 5a 6b 58 4d 33 65 69 72 44 6c 65 47 58 67 75 73 6a 36 54 61 47 73 6f 34 6a 66 44 73 4d 66 73 7a 46 73 48 75 4d 2b 64 46 66 31 44 70 34 56 55 7a 6b 72 37 34 4d 43 64 79 7a 4b 62 49 2b 71 54 46 77 6a 5a 50 33 75 4e 43 75 65 5a 55 47 50 30 39 64 39 58 42 61 2f 59 4e 65 2b 6a 47 63 65 50 36 54 76 7a 37 48 78 57 4d 64 4a 57 78 66 62 74 6f 41 54 2f 69 31 63 4a 35 2f 52 64 4a 67 31 54 56 73 73 48 5a 5a 44 2f 6f 6f 2f 6d 46 7a 6b 4d 63 38 55 78 6d 76 5a 78 63 76 67 66 55 78 65 56 37 46 6a 66 63 50 49 34 7a 76 73 47 6f 66 74 62 78 37 51 2b 46 33 68 64 2f 5a 2b 5a 72 42 45 43 69 36 37 47 37 6a 38 67 2b 75 2b 7a 72 76 4c 2f 6d 52 37 75 2b 37 7a 49 53 50 33 72 63 72 71 4b 7a 69 4d 77 57 59 65 32 4f 38 7a 57 45 49 65 46 53 43 71 6a 31 46 2b 63 41 66 76 62 78 55 Data Ascii: 2kZkXM3eirDleGXgusj6TaGso4jfDsMfszFsHuM+dFf1Dp4VUzkr74MCdyzKbl+qTFwjZP3uNCueZU GP09d9XBa/YNe+jGceP6Tvz7HxWMdJWxfbtoAT/i1cJ5/RdJg1TVssHZZD/oo/mFzkMc8UxmvZxcvgfUxeV7FjfcPI 4zvsGoftbx7Q+F3hd/Z+ZrBECi67G7j8g+u+zrvL/mR7u+7zISP3rcrqKziMwWYe2O8zWEIeFSCqj1F+cAfvbxU
2022-10-03 14:16:07 UTC	2348	IN	Data Raw: 6a 38 4a 37 6c 61 2b 56 71 64 62 31 36 2f 6f 57 73 58 46 54 38 43 2b 6e 76 49 48 4a 2b 6b 5a 34 76 78 57 2b 6b 2b 4d 57 67 5a 53 39 56 64 59 6e 42 75 34 31 64 76 77 39 6d 73 54 78 4d 38 33 65 33 2f 74 73 62 36 49 65 4b 69 6a 52 75 49 4e 64 4e 39 6a 34 61 69 36 4f 43 64 55 42 37 6f 6d 2f 65 41 67 49 65 70 2f 72 77 69 68 2f 72 30 55 79 71 4a 75 63 6c 4e 78 53 6c 6c 75 42 36 49 50 42 6f 79 43 50 4d 4e 53 78 4c 57 43 54 49 6d 4f 30 6a 35 63 34 6c 6a 41 42 6b 49 50 74 6e 48 58 4d 6b 51 6c 56 7a 47 72 6f 32 48 6c 66 54 74 65 73 6f 78 43 64 58 59 7a 36 72 7a 4d 39 61 62 6b 54 78 7a 30 4d 77 61 48 6e 54 6a 59 61 4f 6d 58 56 74 72 44 78 4f 63 58 4c 71 68 39 34 77 47 6e 39 53 64 46 43 49 45 57 43 56 49 61 56 55 59 70 6c 6b 44 57 61 6d 63 63 32 6f 74 49 35 30 39 56 Data Ascii: j8J7la+Vqdb16/oWsXFT8C+nvIHJ+kZ4vxW+k+MWgZS9VdYnBu41dvw9msTxM83e3/tsb6IeKijRuINdN9j4ai6O CdUB7om/eAgIep/rwih/r0UyqJuclNxSlluB6IPBoyCPMNSxLWCTlmO0j5c4ljABkIPtnHXMkQlVzGro2HlfTtesox CdXYz6rzM9abkTxz0MwaHnTjYaOmXVtrDxOcXLqh94wGn9SdFCIEWCVIaVUYplkDWamcc2otI509V
2022-10-03 14:16:07 UTC	2364	IN	Data Raw: 54 7a 50 2f 4c 31 6e 7a 6a 75 70 5a 56 4d 48 6a 75 44 6c 61 35 39 6b 71 7a 39 42 6e 79 7a 69 58 71 6f 43 57 41 44 34 51 54 4e 6b 67 73 35 7a 6e 51 5a 59 68 61 6b 50 76 50 42 43 78 4b 70 4b 58 5a 68 50 74 58 66 68 49 33 78 68 5a 71 6d 50 42 63 39 73 31 6d 6b 63 61 33 71 33 75 37 38 75 45 67 72 63 4b 32 58 36 6e 5a 69 38 30 67 44 56 4b 75 6c 42 55 48 4c 6f 4b 76 45 56 75 65 4e 46 59 7a 70 4e 6a 65 57 73 30 33 66 59 31 57 73 37 37 6b 31 44 75 50 38 68 2b 71 48 64 63 45 4e 44 59 55 4d 33 77 50 53 4b 69 34 4d 65 73 66 67 4e 62 6c 62 4e 61 42 71 73 67 56 57 72 48 70 4f 4f 61 6c 67 30 2f 4c 61 6c 2f 48 38 67 48 68 34 2f 6f 6c 36 2f 62 37 4d 68 4d 57 71 49 4e 51 48 37 55 31 68 51 7a 4e 47 5a 73 71 76 4e 74 76 32 4d 47 38 68 49 5a 37 41 73 77 57 6e 42 55 6e 62 4b Data Ascii: TzP/L1nzjupZVMHjuDla59kqz9BnyziXqoCWAD4QTNkgs5znQZYhakPvPBCxKpKXZhPtXfhI3xhZqm PBc9s1mkca3q3u78uEgrcK2X6nZi80gDVKuIBUHLoKvEVueNFYzpNjeWs03fY1Ws77k1DuP8h+qHdcENDYUM3wPSKi 4MesfgNblbNaBqsgVWrHpOOalg0/Lal/H8gHh4/ol6/b7MhMWqINQH7U1hQzNGZsqvNtv2MG8hIZ7AswWnBUnbK
2022-10-03 14:16:07 UTC	2380	IN	Data Raw: 75 72 2b 33 79 44 55 30 41 71 38 6c 48 49 32 6d 6a 71 72 58 54 33 46 57 36 68 54 4c 53 4e 6a 73 6f 32 73 4f 4d 59 64 39 51 75 6b 30 51 72 57 4d 4b 43 2b 72 6b 61 2f 6b 2f 34 4c 49 6c 73 62 4e 36 79 78 71 6a 61 63 5a 48 77 4f 6c 45 78 35 4e 75 38 41 5a 53 4d 65 36 52 37 39 30 34 77 35 67 44 59 63 38 55 45 59 2b 45 54 4c 79 6b 73 77 34 2f 6b 4c 49 38 52 4d 6d 51 63 34 36 78 6c 39 35 74 6c 66 2b 72 32 44 34 48 61 46 37 6e 37 72 33 36 6c 71 72 2f 77 66 64 39 32 75 2f 35 70 50 75 37 33 63 55 4a 37 65 41 66 4e 59 31 2f 45 53 57 78 52 79 44 36 2b 6d 35 6a 6e 65 49 70 2f 38 69 65 50 70 50 30 67 46 62 4d 76 55 36 36 74 45 71 79 50 45 63 6b 4c 72 5a 79 71 5a 4f 2b 44 50 35 67 50 69 32 2f 4f 36 31 57 6a 34 49 78 73 33 6f 72 47 72 63 38 36 67 47 42 6a 73 45 71 48 6c Data Ascii: ur+3yDU0Aq8lHI2mjqrXT3FW6hTLSNjso2sOMYd9Quk0QrWMKC+rka/k/4LIlsbN6yxqjacZHwOlEx 5Nu8AZSMe6R7904w5gDYc8UEY+ETLyksw4/kLI8RMmQc46xl95tlf+r2D4HaF7n7r36lqr/wfd92u/5pPu73cUJ7eA fNY1/ESWxRyD6+m5jneIp/8iePpP0gFbMvU66tEqyPEckLrZyqZO+DP5gPi2/O61Wj4lxs3orGrc86gGBjsEqHl
2022-10-03 14:16:07 UTC	2453	IN	Data Raw: 30 2c 2e 30 36 2c 30 6c 30 2c 30 63 2e 30 38 2d 2e 30 36 2e 31 37 2c 30 2c 2e 32 32 2c 30 68 30 6c 30 2c 30 2c 30 2c 30 68 30 6c 2e 30 38 2d 2e 31 31 2e 30 37 2c 30 63 2d 2e 31 2d 2e 31 35 2e 34 35 2d 2e 32 37 2e 35 31 2d 2e 33 35 73 2e 30 38 2d 2e 31 39 2e 31 39 2d 2e 32 36 2e 31 35 2c 30 2c 2e 32 36 2c 30 2d 2e 30 39 2c 30 2d 2e 30 37 2d 2e 30 38 6c 2e 31 37 2c 30 63 30 2c 2e 30 37 2c 30 2c 2e 30 36 2e 30 37 2e 30 37 73 2e 33 31 2d 2e 31 38 2e 31 38 2d 2e 33 63 2e 31 36 2d 2e 30 39 2e 32 31 2d 2e 30 36 2e 32 36 2d 2e 31 31 48 36 35 39 63 2e 31 2c 30 2c 30 2c 30 2c 30 2c 30 2c 30 73 2e 35 33 2d 2e 32 38 2e 33 39 2d 2e 33 39 68 30 63 2d 2e 31 31 2d 2e 30 39 2d 2e 32 34 2d 2e 31 33 2d 2e 32 37 2d 2e 32 32 68 2e 30 38 6c 30 2d 2e 30 39 2e 31 2c 30 63 30 2d 2e 31 Data Ascii: 0,.06,0l0,0c.08-.06.17,0,.22,0h0l0,0,0,0h0l.08-.11.07,0c-.1-.15.45-.27.51-.35s.08-.19.19-.26.15,0,.26,0-.09,0-.07-.08l.17,0c0,.07,0,.06.07.07s.31-.18.18-.3c.16-.09.21-.06.26-.11H659c.1,0,0,0,0,0s.53-.28.39-.39h0c-.11-.09-.24-.13-.27-.22h.08l0-.09.1,0c0-.1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.6	49840	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1815	OUT	GET /wordpress/wp-content/themes/kawaken/images/scrolldown.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:06 UTC	1961	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:06 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "c3a-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 3130 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:06 UTC	1961	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 37 37 2e 30 33 20 33 34 2e 32 35 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 73 74 72 6f 6b 65 3a 23 66 66 66 3b 73 74 72 6f 6b 65 2d 6d 69 74 65 72 6c 69 6d 69 74 3a 31 30 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 33 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 177.03 34.25"><defs><style>.cls-1{fill:#fff;}.cls-2{fill:none;stroke:#fff;stroke-miterlimit:10;}</style></defs><title> 3</title><g id="_2" data-name=" 2"><g id="

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.6	49842	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:06 UTC	1816	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_company_img_01.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:06 UTC	1964	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:06 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:08 GMT ETag: "1344f-5b252e7b4c700" Accept-Ranges: bytes Content-Length: 78927 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:07 UTC	2252	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 03 84 04 4c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 06 03 04 05 07 08 ff da 00 08 01 01 00 00 00 00 f4 c8 83 90 e4 04 80 6c 24 c0 90 e4 39 01 20 90 12 64 87 20 24 06 bf 24 0e 7e dc 9a c7 8f 43 7a 1c 8e c4 50 07 1b c0 ab f0 87 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmL"l$9 d $$~CzP

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:07 UTC	2268	IN	Data Raw: 85 43 f4 00 6d 2a 57 01 6b bb 8a c5 ab fd 32 a1 f6 ee 33 40 9d b9 34 6a 49 ee 35 0c cf 75 ee 9d be c0 2c 1b 0d 14 54 a6 67 8f bd 7b 75 fc aa 31 9c 36 fd d1 a9 f3 2b 5d 2f ea 1e e0 c0 4b 8d 80 51 0c ed 75 43 87 ba 72 37 90 54 d6 65 2b 2f b8 5c fe aa a6 67 54 55 99 0f c5 fb 22 ee d1 55 79 5c d8 da de f1 59 1a 1d 61 b9 a3 f5 51 46 09 cc fe eb 75 2a 47 17 3c df 7e cb 70 58 1e 1c 29 a1 e9 e4 1f 78 f1 b9 72 f5 97 b0 ba a8 63 2a 72 87 8d 1a 6e 13 63 63 45 80 55 33 c5 4b 1f 48 ff 00 f6 8e 6a 0a 69 27 95 b5 35 5f ec 8f e1 0a bb b3 2c 2f f9 26 9b b1 87 c0 26 ab fe 0c 77 9f c3 de ec a0 a3 ab 91 db 88 ce 20 a7 7b fd e3 a0 44 07 8b 15 94 fc f8 29 9a 5a 04 63 e6 b2 e4 62 fb 3d 87 7a 4c e6 79 3b 8c e7 cd 4f 52 f7 bb a2 11 16 e6 36 29 a1 ad 68 68 dd ea 39 eb ff 00 d2 d2 Data Ascii: Cm*Wk23@4jl5u,Tg{u16+]/KQuCr7Te+/\gTU"Uy\YaQFu*G<~pX)xrc*rnccEU3KHji'5_,/&&w {D)Zcb=zLy; OR6)hh9
2022-10-03 14:16:07 UTC	2396	IN	Data Raw: 95 df c1 61 d1 35 a1 ad 00 70 fd ba 9d e3 61 f3 5f 68 ea 84 b5 1d 00 3d 98 ff 00 74 73 03 62 57 d9 7a 2e 96 b1 d3 1d d1 8d 3c d1 db 8b d4 19 6b 1f c9 ba 04 4d 9a 4a 63 75 6b 7e 6a 77 5d e0 2c 0e 8c 43 4a cc d7 cd 2b b3 9f 20 8e 55 51 50 e2 e1 04 3a ca ed e7 e0 1c d4 14 f1 d3 b0 86 9d 4f 79 df 16 d7 1c ad 2e e4 0a a7 6e 58 1b f9 b5 d9 7b 93 b0 75 ab 9d 96 99 d6 f7 b4 4d 68 63 03 47 0d 3a a4 d9 4d 88 4d 33 fa 2a 32 3f 34 a7 87 92 a7 a3 6d 3d 37 40 1c 7c 4f 32 84 10 53 d3 c8 03 74 b6 aa bf 19 a6 a2 89 ad 88 87 c9 97 b2 de 01 51 d4 54 e2 18 a4 0e 94 dc 66 f9 0d 13 98 c7 f7 85 d4 b2 c3 0c 65 f2 3c 31 a1 62 7f 68 a4 94 ba 3a 63 92 3d d9 ad ab 93 dc fd e4 11 e2 51 a9 75 88 05 53 30 97 5c a8 80 ba 71 ff 00 15 0d bd d6 85 4f 23 cb 05 d5 d5 45 5c 34 cd cf 23 b7 fe Data Ascii: a5pa_h=tsbWz.<kMJcuk~jw],CJ+ UQP:Oy.nX{uMhcG:MM3*2?4m=7@|O2StQTfe<1bh:c=QuS0\qO#E\4#
2022-10-03 14:16:07 UTC	2412	IN	Data Raw: 59 bc ee ac 32 ab 35 be a5 3b 72 0f 32 d1 1e 83 76 d3 19 f2 68 7a 2d 7c b1 b0 f8 c4 77 69 5a 25 21 e5 da 1c 2b b3 2e 05 e4 28 27 66 3b b1 b5 5f 0d 0c 4d d4 a8 ef 37 cf 1b 95 62 df a1 28 40 c4 74 b6 bd c5 7d fa 3e 13 3e f6 c3 99 ba 2a f2 27 f1 0c 3b 68 08 f2 e0 d9 c0 45 da f5 f2 79 a2 08 b1 01 c6 89 78 f6 be a6 3a ba bf 81 8c 4b 86 dd 8c a9 de e1 18 6f a3 f9 9f f0 ff 00 61 e8 3f 29 a9 a9 a9 d6 4e 77 0c 44 56 dd 63 96 32 ad cb 41 97 d1 1c 45 ab 22 ac c2 84 d2 a2 83 fa 28 61 23 b5 3b 12 95 32 8b 16 a5 e4 62 b3 41 a6 a3 39 54 1c cd db be f6 af 94 6d 0d 2d cb 27 6a 1e e9 97 c6 f6 fb 45 56 85 47 a5 d4 61 a9 df 7e c1 03 7c 25 23 56 d4 67 31 1f 39 f0 c2 3a ac 57 e0 c4 b9 a7 6c 5f 6a 82 75 89 d9 ab d2 c7 57 57 f0 31 d7 6a ec be e7 9b 83 ab 0e a3 d6 ff 00 87 fb 0f Data Ascii: Y25;r2vhz-|wiZ%!+.('f;_M7b(@t}>>*';hEyx:Koa?)NwDVc2AE"(a#;2bA9Tm-'jEVGa~|%#Vg19:Wl_juWW1j
2022-10-03 14:16:07 UTC	2428	IN	Data Raw: 1b 7e a1 10 a7 3b b2 d7 72 f5 e2 14 2e 2d 18 19 9b df b4 26 1e f2 bf 03 d5 71 12 96 5e 62 48 ac 8f 32 a5 0d 86 c7 7d 0b 36 d9 82 33 29 84 b6 82 5e 80 d5 dc 45 ef 32 a1 88 1a 6f f0 4c 7d 27 41 3d ca ed 03 43 a1 ae 48 27 23 2a 07 46 27 a9 4f 26 95 bc 4b 61 1d b4 20 5d 1d d5 4b 1b 17 e6 5f 8b 2b f0 2e 31 db 45 81 2e 52 da 07 bd 12 8f 29 8e 83 a3 03 a8 de c8 56 f8 84 9e 30 62 dd e5 07 97 41 75 2a 12 1b 1b c6 50 38 e8 44 ec 05 10 f1 72 de 63 00 2d 5a 3d ad 4c 2d 08 b5 4d c7 10 e1 03 b3 95 8a 64 bc 54 af 62 71 33 d5 4c 9f 82 29 5e 58 60 09 17 44 0c 6a 45 bf 3a 6f 0a 89 2d 58 d9 77 b7 06 a3 9f 25 27 b6 77 06 07 96 9b 98 50 62 bd ee a1 1c 02 e2 6d 7e cf b5 c5 e2 14 16 be 4c c3 51 ea f7 30 3a b8 f5 92 95 0d 45 82 0f 8b 39 a6 08 9c ec 20 58 3e c0 37 87 8d 15 35 29 Data Ascii: ~;r.-&q^bH2}63)^E2oL}'A=CH'#*F'O&Ka]K_+.1E.R)V0bAu*P8Drc-Z=L-MdTbq3L)^X`DjE:o-Xw%'wPbm~ LQ0:E9 X>75)

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.6	49844	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:07 UTC	2441	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_top_img_01.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:08 UTC	2462	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:07 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:08 GMT ETag: "f2fc-5b252e7b4c700" Accept-Ranges: bytes Content-Length: 62204 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:08 UTC	2464	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 03 84 04 b0 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 02 01 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 fa ea c1 02 80 b0 45 69 ca f3 f5 04 09 e7 f0 2c ca be cd 80 3c cb 77 2d e3 d3 d8 ee 62 b5 68 e5 dd dc ca 70 7c ea 7a 3e ef 33 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm"Ei,<w-bhp|z>3

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2480	IN	Data Raw: ba 35 a3 5a 3c c3 59 ac c2 4b ea 44 78 ff 00 a3 c4 18 67 b0 f8 27 ee 17 b4 c4 7b be c1 f2 fd 67 95 6e 07 d4 ca dd 70 17 53 12 dc a4 54 e0 71 19 87 67 63 49 a0 91 21 94 ce c7 72 45 67 f5 32 44 4a 6f 64 43 82 b6 56 34 dc 71 68 50 6c f2 91 e5 40 54 e0 59 21 24 3d b2 b1 63 48 97 d2 4b 66 53 99 8b 96 99 27 fb 1a 94 52 7f 27 99 62 bc ed 21 54 e0 d6 6a 1c 8b b2 f9 dc b9 84 f7 22 3e d5 e9 bf b8 c4 18 61 f0 54 f7 11 e0 c4 7b be c1 f2 fd 76 54 e0 7c f5 32 b1 df aa 02 e3 ae 1c 94 f8 36 2a 8f 82 87 28 5c 67 22 59 40 8d ac 36 ae 36 ac 55 4e 47 91 26 2c 33 21 4e c4 0a c5 84 99 11 a2 c5 8b 22 d1 2c 98 d5 89 f6 13 43 91 2a a7 98 4a b5 90 b1 6e ff 00 27 99 a3 ea bf d2 cc 4c f5 d2 ba 7c 32 87 d5 16 8a 95 6d b0 9f 99 15 fb 0e 36 48 43 91 72 fd 58 4f 79 0f 6a fb a5 e8 e2 0c Data Ascii: 5Z<YKDxg'{gnpSTqgcI!rEg2DJodCV4qhPl@TY!$=cHKfS'R'b!Tj">aT{vT|26*(\g"Y@66UNG&,3!N",C*Jn'L |2m6HCrXOyj
2022-10-03 14:16:08 UTC	2498	IN	Data Raw: 8e 9a 97 cb e3 3e df e4 f9 1f 27 e5 3b 9f 27 63 b8 b8 27 ed 23 d4 b2 59 cf 82 3c 66 91 11 23 c3 6a ed a7 d0 79 33 b1 58 a2 4b a2 47 71 66 fa 9e 52 e5 ff 00 39 4b 26 c7 93 19 22 5c 13 e5 0f 66 5c b9 a8 4e c4 a5 b1 27 b0 d8 fa 25 c7 d9 77 c9 f0 70 ce c8 7b f4 77 3b 1c a2 db 74 fc e7 c9 46 7a 6a 45 fc 32 9c af bf ca 20 21 0d 97 c9 ac e1 bb 7d 33 8e 99 d8 59 ac 9a 3c 5a 9f d2 d9 f9 7a 3b 7f 93 e4 ee 76 3b e4 f9 47 cb 3b 13 e0 8f a7 31 71 92 17 04 4f 83 03 2d 35 50 f7 b1 7e b6 f3 aa 52 25 d0 c7 c8 b3 7d 4f 29 72 ff 00 91 8c 63 65 f3 68 91 27 b1 27 bf 4b 65 f7 1b df a2 f9 3f 4b b1 db aa e5 f3 91 17 93 cf b5 fd 45 d8 c0 d4 d7 4a 2c 80 8b ec 36 5c 4f 29 0c a6 fe a9 7f 02 e8 ae bb 8b 34 21 9e 29 0f e8 c8 97 0b a3 b7 f9 1f e6 3b 9d 8f 93 b0 f9 3b 3c a6 2f 4e 5d 84 Data Ascii: >';'c'#Y<f#jy3XKGqfR9K&"\f\N'%wp{w;tFzjE2 !}3Y<Zz;v;G;1qO-5P~R%}O)rceh"Ke?KEJ,6\O)4!);;</N]
2022-10-03 14:16:08 UTC	2514	IN	Data Raw: 40 eb 26 fd 92 ef 17 bd f1 d3 af bd b8 e5 a9 74 b7 7f c5 bb 2d ee df 9b a7 b6 5e fb 2d be 3f 92 9e 49 90 8d 97 8e e8 f2 23 a2 75 74 60 9f 8c e4 8b 3e f1 2f 7f 90 06 3c 63 cf ef 0f d8 31 a0 7a e8 fe c9 cb c9 9f e1 16 0e b0 84 3b af 97 d8 2e 8d 1d 78 de f7 0e 3d bf b8 8f 2f 87 f7 7f c6 22 de ae d3 a0 2c bb 3c 06 74 b6 22 2f 8e 03 13 db 32 de 1f 18 f5 bf 9b 5b 73 fc 16 61 f8 72 35 5f 63 87 f8 01 e7 11 cd eb fb bc ff 00 5c 06 d9 e2 f2 6f 9c 33 11 e7 2c c4 df e5 41 be 16 67 90 8f dc c8 78 18 b0 de ef be 81 ee d2 bb 2b ea de d7 12 d1 18 10 12 61 c3 68 65 d9 3c 36 bf 40 99 f3 97 94 be 0f a8 4a e6 6d 9d 67 0f 0d 8d af de ee d2 3d ba df c5 f3 3c fc 67 4f 67 d4 34 e1 e3 6e ed 98 1b df 53 fa 7c 43 af db ec 5b bd ad a5 fb 29 28 63 7a 03 d8 ac c3 14 3a df 47 ac 9b 0f Data Ascii: @&t-^-?!#ut`>/<c1z;.x=/",<t"/2[sar5_c\o3,Agx+ahe<6@Jmg=<gOg4nS|C[)(cz:G

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.6	49853	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:07 UTC	2461	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_recruit.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:08 UTC	2497	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:08 GMT Server: Apache Last-Modified: Wed, 25 Nov 2020 04:14:36 GMT ETag: "276ff-5b4e6aa49e300" Accept-Ranges: bytes Content-Length: 161535 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:08 UTC	2527	IN	Data Raw: ff d8 ff e1 16 36 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 0c 00 00 01 03 00 01 00 00 00 a8 03 00 00 01 01 03 00 01 00 00 00 f9 01 00 00 02 01 03 00 03 00 00 00 9e 00 00 00 06 01 03 00 01 00 00 00 02 00 00 00 12 01 03 00 01 00 00 00 01 00 00 00 15 01 03 00 01 00 00 00 03 00 00 00 1a 01 05 00 01 00 00 00 a4 00 00 00 1b 01 05 00 01 00 00 00 ac 00 00 00 28 01 03 00 01 00 00 00 02 00 00 00 31 01 02 00 22 00 00 00 b4 00 00 00 32 01 02 00 14 00 00 00 d6 00 00 00 69 87 04 00 01 00 00 00 ec 00 00 00 24 01 00 00 08 00 08 00 08 00 80 fc 0a 00 10 27 00 00 80 fc 0a 00 10 27 00 00 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 30 3a 31 31 3a 32 35 20 31 33 3a 31 34 3a 32 38 00 00 00 04 00 00 90 07 00 04 Data Ascii: 6ExifII*(1"2i$"Adobe Photoshop CC 2019 (Windows)2020:11:25 13:14:28
2022-10-03 14:16:08 UTC	2543	IN	Data Raw: 20 20 20

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	2624	IN	Data Raw: a3 34 ac 14 ab 1d e7 95 6b 4a 12 3e 00 7e 79 f3 df fc 1a 3b 7b b3 f1 66 3a 5d 3c 62 66 36 91 1d 0b e8 7e ce e9 f3 4f 18 9e 42 7d cf 6a 9b e3 53 d4 9c f9 ab 30 da 8b d7 02 a1 6f 65 77 74 19 ad e1 69 11 7e dc 83 65 5f 99 3b 66 2f e5 72 48 58 1b 27 88 20 ae 22 31 b7 1e 6a 48 fb 5c 4d 77 f9 8c c5 9c 48 2c 98 b7 9b 3c bb 0f 9a 34 4b ad 3a 40 05 c0 05 ec e6 ee 92 01 b7 d0 7a 1c e8 3d 9b ed a9 f6 7e a0 4a fd 24 ee 3a 15 9c 78 83 e1 1d 62 ca eb 4f bd b9 b2 bb 43 1c d6 ee 51 e3 3b 10 54 d3 3e 83 d3 6a 63 96 02 51 36 39 fc dd 74 a3 de 94 2d b7 2a 1e c7 33 e1 2d 9a 25 14 15 cd ba 44 49 00 02 72 64 b5 2d b6 9c 8f 84 6f 5e b9 02 db 15 49 cf 31 5a 6e 32 36 d8 17 69 d2 04 b8 0b d0 1a 64 54 73 66 17 16 69 73 6f 56 5a ab 0c 86 e1 b8 f2 79 65 f5 80 b1 bf 24 02 03 1d b2 d0 Data Ascii: 4kJ>~y;{f:]<bf6~OB}jS0oewti~e_;f/rHX' "1jH\MwH,<4K:@z=~J$:xbOCQ;T>jcQ69t-*3-%DIrd-o^I1Zn26idTsfiso VZye$
2022-10-03 14:16:09 UTC	2640	IN	Data Raw: ab ea 6e 08 56 e9 51 d2 b9 74 72 00 c3 85 1b 2c f2 4d 4e 4d b5 28 14 6c a3 e8 c9 4f 2c a7 c9 1c 34 8d b7 d3 5b d3 fa c5 c3 8b 5b 5a 54 4a fb 97 ff 00 8c 6b 50 5b f5 65 32 c6 40 32 96 c1 23 7d 82 0b 56 f3 36 91 e5 cd 36 fb 52 9e f2 db 43 d2 2c 62 32 6a 1a d5 f4 c9 0a 46 83 a9 96 67 21 54 7b 03 f7 e1 d3 61 cb aa 98 86 08 93 66 bc fe 6c c4 78 77 93 f3 2f f3 b3 fe 7e 27 e5 ed 29 ef b4 0f c9 5b 28 fc e1 ad 47 58 65 f3 8d fa 32 e9 b0 b1 db 95 ad b9 e2 f7 05 7b 33 f1 5f 66 19 e9 dd 85 ff 00 03 79 58 cb ad 95 0f e6 f5 f8 b5 fe 6a 17 4f cb ef 37 f9 d3 ce 3f 9a 3a f4 be 61 f3 df 99 6f 7c cd ad 48 4f c5 7c e6 90 0d c8 4b 78 85 12 34 ec 15 00 19 ea 3a 5d 1e 3d 2c 44 30 c4 46 3e 4e 1c f2 d9 45 e8 ba 5d f8 f4 25 d3 6d a7 59 99 f8 dc 4f 14 42 49 e3 5e e1 03 0a 06 39 97 Data Ascii: nVQtr,MNM(lO,4[[ZTJkP[e2@2#}V66RC,b2jFg!T{aflxw/~')[(GXe2{3_fyXjO7?:ao|HO|Kx4:]=,D0F>NE] %mYOBI^9
2022-10-03 14:16:09 UTC	2656	IN	Data Raw: 8b 20 68 d4 ac 83 75 71 51 d2 94 f1 c8 51 5b b6 2c 3f 2f f4 8e 60 c9 65 19 90 54 ab a9 af 00 7b 02 6b 4a fb 60 20 a0 90 c4 b5 8f 20 69 d7 1e a8 9e 06 67 7a 01 e9 a0 62 54 74 15 20 50 0f 0a e5 f8 e4 d3 3e 5b 3c 0a f7 f2 77 53 f3 36 bd a7 f9 7f c9 e5 3c bf aa eb 57 3f 50 d3 ef fd 36 9a 1b 4e 66 82 59 21 47 24 71 dd 9d 94 ec 05 46 e3 37 1a 39 51 75 9a c3 51 7d f3 6f 7b 71 f9 6b e5 0d 2f f2 f7 45 8a fb f3 1b ce b7 77 4b 07 9f 1b 48 0d 10 b6 bf 9e 1e 52 4f 7b 78 ec d1 58 5b c6 48 a3 48 d5 0b b8 04 e6 de 53 04 3c f1 89 b4 83 43 d3 7c bb 79 ae 45 af 49 aa 5a ea 5a a0 77 d2 34 4d 4a 2f 35 ea 77 5e 56 79 a3 ff 00 8f 78 45 cd a2 c3 71 32 98 ea e9 1c a1 89 ad 3c 72 00 96 06 2f 4c 3f 9a 56 70 c4 74 0b 5d 58 5d 6b 57 33 fa 2f 65 63 6f 1b db b3 c6 a1 a6 10 bd b4 92 b3 Data Ascii: huqQQ[,?/`eT{kJ` igzbTt P>[<wS6<W?P6NfY!G$qF79QuQ}o{qk/EwKHRO{xX[HHS<C|yEIZZw4MJ/5w^Vy xEq2<r/L?Vpt]X]kW3/eco
2022-10-03 14:16:09 UTC	2767	IN	Data Raw: 9d 77 af 09 35 cf cc 1d 45 5a 4f 2f f9 2f 4d 01 ee 60 40 3e 29 65 a9 e0 80 12 01 92 42 a8 be e7 3a 1d 1e 88 43 d4 5e 7b 59 af 33 3c 21 e5 5e 7c 9f cd be 67 b8 bb d3 35 3b f4 f3 85 83 eb d1 45 37 90 fc 93 76 ba 2e 89 69 3f a6 23 6f f1 3f 9a 99 44 b2 88 4f 26 36 f6 eb eb 31 61 d2 aa ab b4 84 43 a9 27 a1 28 8f a9 ea 4f 77 a5 e9 b7 30 69 c9 a6 79 66 78 e2 f2 b6 9b 67 1b 69 da 76 9c d1 46 a5 7f 46 d8 54 7a 44 29 08 b3 4a 5e e9 c9 79 0b db 25 15 af 11 ea d4 5e b3 e5 cd 0a e3 5a 63 a8 7a 36 f6 69 2b 11 7d 74 89 c9 c9 db 9a ab 3d 39 b3 6d 52 42 81 b6 c6 80 64 b8 1a cc c3 d6 ac 26 b0 b1 7b 7d 27 49 82 19 f5 18 93 e3 b2 88 86 e1 13 35 01 72 68 03 1f bf e8 c9 53 59 36 98 de 6a 50 3c ef a4 59 da ad e6 b5 6b 09 b9 ba b0 86 e1 21 08 83 64 77 94 c6 dc b7 34 02 9d 7f 67 Data Ascii: w5EZO//M`@>)eB:C^{Y3<!^|g5;E7v.i?#o?DO&61aC'(Ow0iyfxgivFFTzD)J^y%^Zcz6i+}t=9mRBd&{}'I5rh SY6jP<Yk!dw4g
2022-10-03 14:16:09 UTC	2783	IN	Data Raw: 45 7b 6b af 41 40 55 6f 07 d5 67 a7 88 96 20 d1 b5 7a 8f dd 8f 9e 58 38 58 7a 87 9a 11 b5 af 42 e6 1b 2d 6a 17 d2 66 b8 7e 16 b1 dd 85 58 e4 3f cb 14 ea 5a 37 3e dc 83 7f 93 88 8f 72 f1 77 ec 89 d5 50 5b c7 04 b1 ec cb 20 52 bd 29 5c 43 24 a7 53 4f 56 36 9d 76 78 a8 65 5e ff 00 31 80 24 a6 9a 52 99 ed 88 7a 7c 23 6f 91 c0 50 a3 c7 d0 92 9c 43 71 22 80 f4 23 2b 93 6e 2e 6f 0c b4 6d 43 44 f3 66 af 63 cb f7 16 77 87 d1 04 1f 8a 09 3f 79 19 03 be cd 4c 96 c4 57 7a 40 22 5b 77 b0 cf cc ad 36 58 2f 57 52 b5 8c 3d a5 f8 2e ac bd 15 81 dc 1c e5 7b 43 4e 71 ce de d7 b2 75 7e 24 2b a8 78 fb 5c 4d cb 8d 68 3b 11 9a 62 ef 03 2f d1 24 2a 55 9d ba 8a 50 e4 82 bd 02 13 13 c4 4b 32 a8 3d 2b df 12 8a 56 82 48 60 23 75 2a 4f 6c bf 11 0d 73 09 d1 bd b5 58 c8 56 52 e4 6c 32 Data Ascii: E{kA@Uog zX8XzB-jf~X?Z7>rwP[R)\C$SOV6vxe^1$Rz|#oPCq"#+n.omCDfcw?yLWz@"[w6X/WR=.{CNqu~$+ x\Mh;b/$*UPK2=+VH`#u*OlsXVRl2
2022-10-03 14:16:09 UTC	2799	IN	Data Raw: 07 a6 20 31 29 e7 a0 e5 02 91 5f a3 2d 01 ac d2 1c 69 81 8d 40 a6 1f 0a d1 c4 42 b3 e9 e5 57 c6 99 2f 06 d7 8d 4a 38 9d 5c 28 1b 77 c9 0c 05 07 20 7f ff d2 86 69 7a 19 e7 57 41 c4 6e d5 cf 4a 0f 17 c4 59 97 38 ac e2 e2 a0 0a 0d ce 21 8a 54 f7 e6 46 a8 04 9c 95 24 21 24 b8 0c 4a b3 54 9f 11 81 42 4d 75 5b 79 03 83 58 df ad 70 5a 40 dd 5e d2 ed 59 a8 bb 8e f4 c0 19 10 c8 d2 64 e2 3b e5 8c 55 52 7a 93 51 41 db 05 2d ab 9b 86 23 8e c4 60 4a 51 78 ea 4e fb 53 7c 90 62 94 06 45 ab 56 95 ed 84 b2 56 b7 62 d2 02 86 83 e7 81 14 ca e0 0b c5 49 dd bc 71 54 53 5c 05 42 2b f0 d3 6c 0a 18 26 a3 75 1b 4c ea 06 e3 a9 a6 21 b4 04 aa 28 21 94 b4 86 31 51 d0 ff 00 66 27 74 9d 93 1d 23 4e 12 49 2c da 64 ed a6 e a 88 6b 14 d1 ec af 4e ce bd 08 38 b1 25 e8 fa 2e bb 05 fa c9 a7 Data Ascii: 1)_-i@BW/J8\(w izWAnJY8!TF$!$JTBMu[yXpZ@^Yd;URzQA-#`JQxNS|bEVVbIqTS\B+l&uL!(!1Qf't#NI,d kN8%.
2022-10-03 14:16:09 UTC	2815	IN	Data Raw: a1 27 2e c7 12 0a 72 4e 32 0f 45 29 01 3f dd f1 e4 77 2b 99 0e 38 92 30 58 16 03 8b 90 3c 3a e4 0c d9 21 de 49 f4 f6 45 0c 84 39 f8 7a 83 82 84 95 36 b1 d6 db ec 11 cd 81 dd 41 ca 27 80 23 89 38 5d 50 8a b4 b0 b5 36 dd 77 ca 7c 24 82 98 09 12 45 e4 8c 08 61 5c ae 88 55 27 24 ff 00 03 92 0a 86 63 5a 8a 0f 96 4a 95 0b 2c 4a d5 3d 0f b6 58 36 62 42 56 b7 34 97 d0 75 7a 50 71 72 3e 1f bf 2d ab 0c 6a 95 23 92 41 7b 00 42 8e bc d6 aa 0d 18 6f 91 90 f4 95 1c d9 0d f5 b5 98 73 24 ab 23 3b b0 22 8c 6b 5f a0 e6 26 22 4f 26 47 9a 8b ca 2b 50 cd 96 88 b1 25 48 39 ea cc 7d 8d 30 d2 2d 77 38 c6 c6 55 df 02 b9 ee 12 35 67 69 14 2a f5 3b e2 22 4a 54 e0 d4 23 99 f8 46 c8 cc 05 48 04 d6 9f 76 13 0a 54 41 91 fd 8e 46 95 44 ca d5 ea aa 7e fc 69 52 fd 49 cb 5b 1f 8b 70 c3 b6 Data Ascii: '.rN2E)?w+80X<:!IE9z6A'#8]P6w|$Ea\U'$cZJ,J=X6bBV4uzPqr>-j#A{Bos$#;"k_&"O&G+P%H9}0-w8U5gi *;"JT#FHvTAFD~iRI[p
2022-10-03 14:16:09 UTC	2831	IN	Data Raw: c4 b6 77 41 e9 42 7f 71 e9 82 7a d4 d7 29 22 71 e8 ca a1 23 ba db 6f cc 0d 06 55 33 49 e5 cb 5d 2e 64 1c 1a 3b d8 2f e7 8d 14 93 f0 98 84 f2 2b 7d 35 19 1f cc cd ba 3a 6c 5d 59 57 97 7f 31 f4 4d 36 69 6e 92 d2 eb ce 91 da 40 f2 47 e5 cd 2a c2 4b 3b 48 88 dd 49 69 55 15 b8 6f 40 49 a7 6c 89 cb 92 62 9b 40 c3 8f 92 6b 27 e6 de a5 e7 2d 2a 69 b4 d6 9b 43 87 52 89 ed dd da 8b 3c 50 30 e2 f1 5b 2a 33 7a 7c 86 cd 21 6e 47 a0 e3 92 c5 87 7d da 35 1a a1 54 12 6b 1d 35 9a 28 e2 b5 b7 8a 28 55 02 89 9e 8a a1 57 6a 57 36 42 1b 3a c3 35 19 bc b9 a7 c6 1a 6b 9d 48 39 53 f1 08 76 5f ed cb 44 1a 65 30 58 7e a3 a8 59 39 6b 7b 09 4a 5b c6 6a ec 49 ab 11 b6 e7 c3 2c 10 6b e3 be 4c 66 eb cc 69 68 aa a6 53 46 22 35 40 0b 33 3b 1a 2a a2 2d 4b 12 4d 00 1b d7 27 1c 77 c9 06 74 Data Ascii: wABqz)"q#oU3I].d;/+}5:I]YW1M6in@G*K;HIiUo@Ilb@k'-*iCR<P0[*3z|!nG}5Tk5((UWjW6B:5kH9Sv_De0 X~Y9k{J[jI,kLfihSF"5@3;*-KM'wt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.6	49860	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2462	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_mov.mp4 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" Accept-Encoding: identity;q=1, *;q=0 sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: video Referer: https://kawanakajima.co.jp/ Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1 Range: bytes=0-
2022-10-03 14:16:08 UTC	2526	IN	HTTP/1.1 206 Partial Content Date: Mon, 03 Oct 2022 14:16:08 GMT Server: Apache Last-Modified: Tue, 17 Nov 2020 00:16:40 GMT ETag: "56b901-5b44268a46a00" Accept-Ranges: bytes Content-Length: 5683457 Content-Range: bytes 0-5683456/5683457 Connection: close Content-Type: video/mp4
2022-10-03 14:16:09 UTC	2560	IN	Data Raw: 00 00 00 20 66 74 79 70 69 73 6f 6d 00 00 02 00 69 73 6f 6d 69 73 6f 32 61 76 63 31 6d 70 34 31 00 00 00 08 66 72 65 65 00 56 47 65 6d 64 61 74 00 00 02 af 06 05 ff ff ab dc 45 e9 bd e6 d9 48 b7 96 2c d8 20 d9 23 ee ef 78 32 36 34 20 2d 20 63 6f 72 65 20 31 36 30 20 72 33 30 30 20 20 33 33 66 39 65 31 34 20 2d 20 48 2e 32 36 34 2f 4d 50 45 47 2d 34 20 41 56 43 20 63 6f 64 65 63 20 2d 20 43 6f 70 79 6c 65 66 74 20 32 30 30 33 2d 32 30 32 30 20 2d 20 68 74 74 70 3a 2f 2f 77 77 77 2e 76 69 64 65 6f 6c 61 6e 2e 6f 72 67 2f 78 32 36 34 2e 68 74 6d 6c 20 2d 20 6f 70 74 69 6f 6e 73 3a 20 63 61 62 61 63 3d 31 20 72 65 66 3d 33 20 64 65 62 6c 6f 63 6b 3d 31 3a 30 3a 30 20 61 6e 61 6c 79 73 65 3d 30 78 33 3a 30 78 31 31 33 20 6d 65 3d 68 65 78 20 73 75 62 6d 65 3d Data Ascii: ftypisomisomiso2avc1mp41freeVGemdatEH, #x264 - core 160 r3000 33f9e14 - H.264/MPEG-4 AVC codec - Copyleft 2003-2020 - http://www.videolan.org/x264.html - options: cabac=1 ref=3 deblock=1:0:0 analyse=0x3:0x113 me=hex subme=
2022-10-03 14:16:09 UTC	2576	IN	Data Raw: 99 3b 09 d4 cf 7b 63 6d 29 4a 5b f1 75 db 06 60 5a c3 ed e6 8a e5 41 38 a0 b1 d9 7b 0d 69 eb 4f c7 31 0a 86 d3 29 49 4b 45 10 bb e3 29 e8 2b a7 45 73 49 38 90 e6 07 3e fa 56 cc 8c 5b 71 62 57 5c 8e dd b9 aa 92 3a a2 19 22 9e 9f e2 19 7f c2 05 66 be 4e 46 83 43 ee 20 7e 5f 9f 28 6a 60 44 5e be 3d a8 c2 59 e7 2d b3 94 df 61 30 12 71 06 44 4c 8c 07 33 6f 4b 54 54 da 42 07 13 3b 19 95 d4 e9 8c 4c 63 e4 c1 ce 34 91 54 a6 a0 e4 fb fa a5 5f 27 df d5 dc 8d ac cc f9 45 36 38 4c 8b 3a e2 0f c1 17 3b d3 90 8a bd 22 60 0a fc 45 6f e6 f0 1c 64 ab fd a5 bd 35 a4 a6 54 3b 49 be 2c dd 25 37 60 dc 83 54 71 11 25 b3 3e c8 54 4d 52 ff b4 c5 bc 02 c1 6b f0 60 3e fe 92 b7 83 53 af 3d 56 aa 1e 4a cd 9a c2 0c ef 95 c8 7c 8c b8 31 b8 45 02 73 37 7d 45 d6 88 68 c8 a4 c1 9b a0 38 Data Ascii: ;{cm)J[u`ZA8{iO1)IKE)+EsI8>V[qbW\:"fNFC ~_(j`D^=Y-a0qDL3oKTTB;Lc4T_'E68L:;"`Eod5T;I,%7`T q%>TMRk`>S=VJ|1Es7}Eh8
2022-10-03 14:16:09 UTC	2705	IN	Data Raw: c7 42 3f fc 73 ae fa 60 6b 2d 02 96 7e 8a fb 1b 7f df 77 c3 59 02 22 e2 90 86 8d 6a 77 31 03 6f 7c f2 7a 4c b9 29 25 4f 51 4d da 50 5f 44 ea b0 7d 72 13 fe b7 84 cd 28 f9 19 69 52 e3 22 f4 a6 e6 85 34 0a f2 2e 8d 65 ec 10 00 ba 65 fc c5 ab bc df 28 87 a2 93 d2 18 1d fb 0f 95 de bb 7a c3 b7 26 f6 66 af f8 51 1e 77 cd 02 d0 be 50 5c 7d a4 43 58 1b a9 c4 e3 2c 78 20 ec 36 1e d0 7b 58 ce db 16 24 f6 ea 6b f9 88 c7 52 04 d6 a3 1d f5 e6 26 ce 28 cc 3c c9 c1 b1 e7 c3 14 0a e4 6b dc 58 6c 04 f5 bd c5 bc 07 63 c1 ac 07 88 95 ff 44 4b 73 f6 a1 f2 77 0c fe 51 df b8 76 ad 56 85 0e 98 4b 61 b6 3f 7d 78 ca 86 ab 1b 90 7b 82 fe 83 d7 ea 9e b7 00 19 1d 14 dc 90 a0 a2 3d ef d4 3d 46 21 91 fd 4f 0d 7e 9c 16 6e fd b2 97 f5 ba a2 79 dc 0d 4a ff 5f 8c 65 52 fa ec a7 50 49 22 Data Ascii: B?s`k-~wY"jw1o|zL)%OQMP_D}r(iR"4.ee(z&fQwP\}CX,x 6{X$kR&(<kXlcDKswQvVKa?}x{==F!O~nyJ_eRPI"
2022-10-03 14:16:09 UTC	2721	IN	Data Raw: e4 54 25 68 95 80 c2 4c 21 92 ce 64 ec 01 33 d9 69 3e 69 3a 80 72 a2 c0 a8 22 f3 b0 01 8c d1 fd a1 bf e5 c5 57 27 1b a1 bd 5c 61 50 0a bc 5f ed cd 68 8f 7b b1 84 d1 5c d6 be 2f 59 a3 61 a4 cb 25 70 24 dc 50 59 1c a4 38 1a 8d c4 d8 e7 3f 65 6c 54 e7 52 4a 54 0e 16 43 bf 53 84 0a 80 8e 8a fb 34 ff 61 e9 1f 65 3d 62 fe cb 2b 56 4e c7 e1 b6 6f df 65 e8 ad b2 c6 17 1e 3c 3b c1 94 c7 8b 4a cc b1 7b 15 aa 75 4c 7b a6 6a d1 00 c4 bc 90 93 01 12 5e 90 17 a6 25 7a cc 15 97 ce e3 7d 29 75 4d b4 4f a1 92 dc d7 c2 4f d1 7e d0 14 7e 12 4a 2e 2e 0b 24 f2 63 8f ed 29 2e ca 2f ec ad aa 45 ce e2 5c cf aa fe af 8b 10 e1 2a 1f 48 c2 20 df 32 7a 23 75 38 98 f0 25 eb 41 74 4d c2 a3 1a 16 a7 b5 11 dd 20 cc a1 e7 83 06 33 ba 2e ce 5b 28 cc 0c ee 4d 5b d2 f6 a8 6c 36 a9 ca 7c 8b Data Ascii: T%hL!d3i>i:r"W"\aP_h{\VYa%p$PY8?elTRJTCS4ae=b+VNoe<;J{uL{j^%z})uMOO~~J..$c)./E*H 2z#u8%AtM 3. [(M[l6|
2022-10-03 14:16:09 UTC	2737	IN	Data Raw: 49 ea 08 e4 17 7b b9 13 1e ad c4 84 62 ba da 62 16 43 b7 be b4 73 43 b5 79 6a 68 52 3b 13 1d 23 cd 51 62 61 d4 b5 43 88 98 e9 ab dd 22 47 10 2e 30 6c 05 54 0d 69 0f 94 ff 2a 34 f0 54 6e 3a 9d fd 7f b4 1a 29 0d d5 ed 1e 6a 67 c6 71 f8 67 4f 5a 1c 73 a7 ef d7 0e bb 55 b0 2b d8 d2 5d c4 61 aa 60 3e 08 93 e1 95 a2 e3 d5 a1 f6 de 03 e4 97 06 4d cb 4a cc 2a b4 20 8d 05 16 a5 f4 bc 39 9d 3e fe 2f 5a b5 fa 30 1e a2 71 91 9c 59 82 e8 b5 48 8e 6f 85 cd 31 e1 ed 48 74 b5 cc 89 25 22 74 0e 97 69 ba ea 85 06 fb 0b 8c 22 6c 74 f1 f6 1b 2b 9b a0 6e 1b e2 7e 2a ba 5f 12 c8 12 08 78 f2 ef 4c 46 1f fb 2e c7 75 e0 d1 fc 67 66 ea 13 25 e2 dc e6 65 f7 43 9a 06 09 02 62 58 40 1b 1e 40 bb cd 85 4d 31 ac 78 ab 97 2d 1e 9e d9 72 5e 41 50 49 e1 5f 7b 90 0e 7c 4b 4c aa 82 64 65 8d Data Ascii: I{bbCsCyjhR;#QbaC"G.0lTi*4Tn:)jgqgOZsU+]a`>MJ* 9>/Z0qYHo1Ht%"ti"lt+n~*_xLF.ugf%eCbX@@M1x-r^APl_{|KLde
2022-10-03 14:16:09 UTC	2893	IN	Data Raw: 1e a5 3b b0 00 53 83 78 0c 19 a6 90 59 5f f9 78 cf a4 4d cc 5a aa 6b 58 c5 8d 59 fc 6c 8a 77 90 98 b6 34 8a d1 6f a0 04 25 40 21 34 dc 8b 9e ad f7 d7 a6 df ce 10 79 d8 92 9d b2 b9 63 71 03 63 79 52 7e dd 1e 53 47 8b 53 af 4b 98 37 2f e2 1a 7f 8d 15 b3 a2 70 11 44 c4 24 21 77 43 b4 fa fb c6 6c 57 c8 4e b0 57 a4 24 af 6b 7a b4 93 75 56 d2 7b 7d 83 33 2a 11 63 3b db 7f 7e 35 d3 e3 5e 27 a1 0a a5 3b e1 1b 6a 3f 9c dc 67 9c 5e 83 8f 80 9e de ea fd ac 2c bd c1 53 a1 1e 75 69 2b 84 4e c8 a2 23 b1 5e 34 cc f7 2f 19 a8 0f 2d 46 be 59 67 05 ed 8f 93 07 bb 62 bb 40 db 15 17 88 7d 95 d9 57 f4 ce aa aa 29 5b 7c d2 75 0b 11 48 95 08 9a 36 66 13 a2 7c 79 1d e8 11 b8 95 e7 e9 5c c2 bf dd 43 ee a3 36 f6 c9 d9 a1 78 1e 09 55 f2 4b e6 5a 31 a4 9d f0 54 dc 7d 46 8f 15 d5 04 Data Ascii: ;SxY_xMZkXYlw4o%@!4ycqcyR~SGSK7/pD$!wClWNW$kzuV{}3*c;~5^';j?g^,Sui+N#^4/-FYgb@}W)[|uH6f| y\C6xUKZ1T}F

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	2909	IN	Data Raw: 3a a8 c5 a0 a3 ed b8 f3 df ba 7f cd d2 e8 b7 f0 f2 34 ff 02 e8 f3 95 f3 9d 51 d2 62 fc b8 a6 e3 4a 50 3c 50 e9 fe 78 63 49 65 6b 9c 88 9e 61 a5 4e a7 80 c0 68 a8 52 f5 86 55 f8 02 b3 fd 34 2e a9 87 73 ef ec 3a e6 6d 1b a0 ba b9 f5 e2 d3 69 ae 91 bd 64 97 78 5c 42 9b 01 0c 47 cc 55 33 0a b2 a0 99 73 2b 4b f5 a1 99 08 77 11 8d 06 24 9a 81 6d 0c 46 d9 e7 d6 6d ec da 59 fc 39 44 37 88 14 7c 53 d6 60 e4 b0 d2 1e 15 fb f0 d4 42 83 6b 70 f7 e7 ad 85 49 96 a1 6c e6 84 04 15 28 57 56 0e 6d 2a 8f 4c d7 ca a5 f7 d9 cb 40 e5 4c 6d b0 7d 4c ab 24 1c 14 06 7a 3b a4 cd 21 2e 35 4e fe d6 62 41 b1 59 82 6f f2 a9 95 c3 e7 3f 54 0b 70 78 cb 09 aa 33 5d a0 d2 30 a0 ff 3c 42 52 04 3a 87 0e 63 b6 d2 e1 61 2a 01 0d 36 cb 20 70 34 74 f9 ba ea 2b a6 e5 c1 31 29 26 04 08 25 f3 47 Data Ascii: :4QbJP<PxclekaNhRU4.s:midx\BGU3s+Kw$mFmY9D7\|S`BkpII(WVm*L@Lm}L$z;!.5NbAYo?Tpx3]0<BR:ca*6 p4t+1)&%G
2022-10-03 14:16:09 UTC	2925	IN	Data Raw: d5 1b 62 67 e4 a6 b0 a9 8d ca 2a 1e a5 75 bc 36 07 d2 2f b9 70 be 54 f5 1c c9 a3 56 32 57 66 b3 6d 99 0c 9a d0 75 e0 b3 c4 e0 a3 7f 3f 15 d3 56 7a d0 d4 01 78 cf ad 1f bc c6 1b a3 b8 9c 68 40 b5 0b 86 a3 35 01 4f 56 08 4d 71 ee c1 56 8a 8e df e3 67 a4 a6 70 7e 03 f0 41 68 47 2c 17 d7 e1 15 d1 d6 26 b6 dc 49 0d e0 5d 12 33 68 67 4b 06 0c 4e b2 2c 2c d5 e2 08 72 a5 46 ad 6d 12 dd bc 50 b4 32 15 92 07 e6 96 11 13 88 9a 73 ba 5d 01 41 e4 62 77 e9 d0 ad dd 9b 0f 1c aa 95 00 db d9 c7 61 87 46 94 ef c0 98 d0 01 19 f2 a3 cf 08 be e9 90 ce 5e 9a 4d 84 2b cf a4 d6 c4 ad f4 59 91 cf 92 5f 9a 4f 65 b8 6d 6e c8 b8 75 23 34 b1 56 63 a0 8f 29 ef 30 47 25 b8 ae f7 c4 48 c4 6e 91 c5 88 d8 58 37 b9 15 3a c5 c7 b8 9c d4 93 9f 63 fd 1c 09 e8 d2 d8 69 9e 8f e3 11 3d 25 3e 13 Data Ascii: bg*u6/pTV2Wfmu?Vzxh@5OVMqVgp~AhG,&I]3hgKN,,rFmP2s]AbwaF^M+Y_Oemnu#4Vc)0G%HnX7:ci=%>
2022-10-03 14:16:09 UTC	2941	IN	Data Raw: 5b 97 c9 32 37 6c 7a c5 82 d6 81 e7 4d 65 e1 86 50 9f 9b 7c 1d 5d 7a d7 fc fe 93 98 a2 b3 16 ed e4 b7 ee 97 a3 98 20 dd 61 9a 39 20 91 6e 43 fd 97 8d c1 17 bf 4b 92 52 3d 85 f0 f6 e5 05 06 fd 13 7a aa cc af 58 00 a2 8e 5b 6b 58 28 9b 22 69 55 69 52 c8 26 a4 28 78 84 7f 10 74 c6 9c 2e 67 34 c0 7b 23 39 f9 22 bc 51 a7 67 55 81 ff 6f 0d 1c de ac d5 66 8e be 5f be 31 a7 10 69 70 db af 0a a4 62 7e fb 81 04 cf 39 91 cb 2c 24 71 2a dc ec 88 9c 11 b7 82 28 42 08 b9 20 b7 0a 16 97 01 8c 0e 0c 5c 97 73 21 ab ab 17 fb a3 b1 a6 00 43 62 9e 9b f0 7a 4c ad 96 45 7b c5 d6 f0 b7 23 f5 38 4f 03 0e 07 8e fc 60 5a 86 cd 3f 41 2c c0 a8 cb 4c c6 5a db fd 65 d4 72 ce 54 d1 28 d4 7a de a3 98 bc 3a 3a 46 8b c6 59 2c 33 8f 3b 65 bd 2b 35 17 00 f3 a3 36 cd 4f 11 68 40 68 02 ee e5 Data Ascii: [27lzMeP|]z a9 nCKR=zX[kX("iUiR&(xt.g4{#9"QgUof_1ipb~9,$q*(B \s!CbzLE{#8O`Z?A,LZerT(z::FY,3;e+56Oh @h
2022-10-03 14:16:09 UTC	2957	IN	Data Raw: da 06 ef 54 7f 95 fb b5 1e 19 8e 62 d3 1a 9d bd d6 24 b6 a2 14 86 1e 81 f4 9c b3 08 40 a5 66 16 2b ff 3d 1d 13 da 9d 22 c6 2f 2f c3 a6 e4 0a d7 0e 4e 52 25 2f 56 3e 37 2e 46 a1 b2 65 0c 23 13 cc 3f f8 d3 fd 5d 65 8e d6 d8 70 2a db a9 23 4b be 14 13 8b 60 3e a4 45 a0 ca db a2 23 ba 56 4a cd 5c 85 2e 91 d3 ec c1 ab 7a d3 ff 2a 55 82 c6 54 be 99 84 03 55 34 dc 9a c2 96 14 0c f5 b0 93 d5 d2 d3 61 26 c3 8e c6 57 cf 48 00 f0 7c 0d 32 1c 8d a4 e1 21 1a dc 3f 1c cd 34 d8 fe ec e5 0b f9 43 9e d3 a6 61 cf 07 02 92 06 aa 97 60 d5 c5 30 46 77 8a d6 5f f9 10 b6 ea e2 3a c3 e4 48 8d e4 9f 70 b2 8a 4b 77 17 d6 ff 7b 21 ed 3f b5 b3 33 d8 3e 61 ba 09 f4 35 ad 1c 8c 52 fd 0a dd 75 e4 ef 9b 10 9d b1 b8 fd da 0c b0 f6 1f e9 89 57 87 ad 8f 56 ce 8b d6 64 aa 69 bd c2 bc 95 bf Data Ascii: Tb$@f+="//NR%/V>7.Fe#?]ep*#K`>E#VJ\.z*UTU4a&WH|2!?4Ca`0Fw_:HpKw{!?3>a5RuWVdi
2022-10-03 14:16:09 UTC	2973	IN	Data Raw: 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 79 00 00 02 b0 01 9f 0d 6a 4f ff 00 00 03 00 00 03 00 00 0f 26 38 e8 fc c5 47 ac 8a cc 74 50 a0 74 a3 72 3e 7c 0c cd 73 e5 61 0f 80 8a bd d5 35 6e 89 ac 96 d6 08 a1 0b d1 e9 02 c0 1c c7 16 a1 64 2e 3b 5d 44 87 d5 b7 6b 97 96 06 52 f3 49 f5 8b ad 75 ed 77 4a ca ae 09 1a 8f 9d 80 01 68 d0 d0 b3 91 05 cd ae c3 e9 78 6a 2b e5 05 ee 72 2e c0 08 0c 10 d3 4a 8e c9 5b 17 6a 48 fe d1 aa 0e 47 2b c0 88 a6 b8 78 3b d7 1f 0a 9b de fc 54 e3 16 73 5f fd 35 07 f1 34 b6 27 5b 26 2c c6 e9 68 f2 e7 57 2a 46 4f db a3 20 b8 18 8a b0 ea 5f e4 ad 9b 4f 14 92 cc 0e ed b8 de 69 6b ee f9 73 18 25 41 c4 22 00 b0 5d da a1 11 4c 8d 15 6c 7f cf c2 4f a4 9e 69 99 b5 53 7c c4 16 15 59 06 af 93 fd ed 59 Data Ascii: yjO&8GtPtr>|sa5nd.;]DkRIuwJhxj+r.J[jHG+x;Ts_54'[&,hW*FO _Oiks%A"]LlOiS|YY
2022-10-03 14:16:09 UTC	3086	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	3166	IN	Data Raw: 9c 94 a8 0d da 6e 57 aa 61 ae d5 04 62 64 88 1e 90 04 69 67 ec 8d 40 16 99 c3 11 80 2b 08 e4 5b 80 d5 65 cc 53 30 ee 93 cb fb bb 89 cd b2 47 c9 a7 43 91 c7 43 ec 95 19 18 aa 01 78 5c 6f 40 71 13 84 4a c4 e1 d7 eb 30 ac aa a8 e2 7a cc 4e 09 c0 7a fe 12 39 ed 1c c1 5b c8 2a a8 59 5c f6 57 12 53 0e b8 bc f1 f5 28 66 fd 77 ff 28 9f 32 88 46 84 25 fe 9e 7e 9a 0f 30 56 ee a7 1c 2a d2 72 9d 60 fe d5 0e db e3 4d d6 02 44 ec 43 1d bb ab 5e 66 5d e4 a1 de 03 6e 92 21 78 c6 94 65 ac 50 be e1 c0 bf 0e 7e 58 e4 25 f1 bd be de b2 11 b0 ec 5c a6 2c 5f 98 13 1a 74 ce 51 2c 49 cd 83 a5 ad 23 78 7a 1c a8 31 d9 c4 e4 ed 7f b7 c4 3d e6 05 dd 6e 72 55 ec e5 53 a5 23 69 ae fa 39 48 7a 63 55 92 b7 2b 85 c3 78 0a 1d 63 28 d3 88 c2 bf b7 1e b4 8d ad 13 42 7b b2 e0 28 d3 b5 4a 25 Data Ascii: nWabdig@+[eS0GCCx\o@qJ0zNz9[*Y\WS(fw(2F%~0V*r`MDC^f]n!xeP~X%\,_tQ,I#xz1=nrUS#i9HzcU+xc(B{(J%
2022-10-03 14:16:09 UTC	3182	IN	Data Raw: 15 9a d9 96 5f 92 ba b5 8c 03 4e 01 94 b1 c5 a8 9e 11 0e af 3e 34 9b dc 1f ee 59 a9 41 49 b7 7d 5b e3 3d e1 3f 77 2a d1 25 de 7d 38 27 8d 6e 61 b0 4c 95 85 dc eb 92 9d de 2d 61 7c 95 6c 1f 06 00 71 b6 9f d6 57 10 57 4b 29 0c 31 05 09 37 ee 9e bd 60 9a 65 e2 1c 66 0e 4e ea 55 5f e7 8c 25 ef 94 ff f0 11 2a ec 1b a8 76 5a 23 3e d4 b0 35 3a 1e cd aa 69 20 15 ce 08 4f 25 99 30 94 4f 70 ba f7 23 98 58 bf d3 a2 3d b6 d6 a8 e6 da 41 2c cd 29 e1 a8 97 97 35 47 fb 72 55 92 1f 56 ec 5a 6d 7a a8 dc a9 2b 04 84 9d 2d 6e 6c 6f b1 e0 31 eb 34 2d ac be 06 aa 18 1f f2 88 65 15 08 4d d0 32 a2 82 1e 8a 32 23 8c d4 62 71 fb 8d d9 21 d8 3a 5d e8 9d a1 69 ea bf 07 d4 89 44 cc 3b 67 a5 31 90 25 75 9b ae d1 c8 6b a9 6d be 06 d6 0d ba 99 03 c9 c8 01 20 1b 2e 73 f9 9a 16 86 d2 7b Data Ascii: _N>4YAI}[=?w*%}8'naL-a|qWWK)17`efNU_%*vZ#>5:i O%0Op#X=A,)5GrUVZmz+-nlo14-eM22#bq!:]iD;g 1%ukm .s{
2022-10-03 14:16:09 UTC	3198	IN	Data Raw: 8c 6b b4 cb 7b 88 10 5f cb 28 d0 08 21 a0 f8 da e9 9b 1f 7a c8 b3 eb 1c 23 27 44 05 b9 9a 89 5c 24 e2 f9 e6 a2 92 06 84 df 32 16 69 40 cf 84 a8 28 78 da 39 e9 61 bb ed c4 72 c9 a9 ad 6d 49 84 d9 56 66 f9 60 29 9f 6b fc 1b 24 ec b6 fe ea e9 c2 3e 87 bb d0 8a be c3 61 af fc 33 47 69 a5 4b b5 59 61 38 51 c9 b0 6e cd 49 ea 41 14 15 4e e0 af 8d ed a5 6e d3 6a 35 19 98 83 a5 d6 2e 08 75 65 6c 59 c0 5f 65 ad a3 1d a3 73 55 41 c4 1b 74 bb 67 63 5a 52 2e b8 ea 73 bf ce 85 ff 04 53 9f d9 b5 7b 7b ca d8 e0 6f 6b e4 ff 47 34 e9 4e 67 a2 80 bb 02 4d a5 04 a7 af 25 77 36 92 30 06 ef 77 bf 05 8e 02 88 19 30 eb db c9 02 5a 3c 9b 52 34 00 8b ce 8f ed 91 8d 78 fa fa 62 78 1e 6d 80 4d 94 a1 a6 d4 25 4d 34 7e 8f e2 f4 9f ed 0f 62 34 8a ba 89 b1 f4 32 54 7a 60 0a bb 6e 5a bf Data Ascii: k{_(!z#'D\$2i@(x9armIVf`)k$>a3GiKYa8QnIANnj5.uelY_esUAtgcZR.sS{{okG4NgM%w60w0Z<R4xbxmM%M 4~b42Tz`nZ
2022-10-03 14:16:09 UTC	3214	IN	Data Raw: 7b 3b e7 c7 b6 f2 d5 18 ae a1 6b a4 0c 52 be 28 5b 2a 6d 2d 71 d3 63 dd a4 14 fc 1d df 29 e2 5d b5 fb ef 1e 42 f5 11 f6 de 30 8d 0f b0 65 47 c7 b2 99 ae df 40 62 2b 40 c2 16 2d 31 75 3a 56 8c ba e8 ff d9 0a b1 5e 51 66 74 cf 97 67 93 3b 7f 97 bc 17 d1 ef 3b 46 18 19 80 93 89 ef 78 3c 56 61 97 a9 d1 af 12 87 17 e5 23 a4 f8 2f e8 17 7d 2d 4c f4 94 40 9f 48 a3 9a cf 29 97 f6 c6 72 0a d9 08 54 78 0e 44 7e d7 0f bf 48 24 3b d4 73 d6 c8 aa 29 9c cd 8a 25 50 5d 0f 79 d6 1f c0 f0 f2 98 f3 a9 27 b6 8e 43 d5 21 c0 1a d0 1d b5 e9 a0 bd 51 9a b7 e3 1d ef 8a 33 4e 1e cb 81 5d 0e 46 59 df 8f 1a 0c 62 9e c5 2d 61 1c c0 bb a9 f0 34 49 2f 7b 82 3a 1d d1 3b 7a 4c 45 5a 58 ed e0 33 9e 81 db c6 6c 02 93 c3 de 4d e1 55 4a df 36 e0 1b b9 c5 1a 7e f1 84 ec 64 8d d5 84 72 ca 88 Data Ascii: {;kR([*m-qc)]B0eG@b+@-1u:V^Qftg;;Fx<Va#/}-L@H)rTxD~H$;s)%P]y'C!Q3N]FYb-a4I/{:;zLEZX3lMUJ6~dr
2022-10-03 14:16:09 UTC	3230	IN	Data Raw: 10 38 29 37 ee 9f 5e ff 3d 4c e3 ab 33 76 6b bc 40 66 55 54 00 33 83 76 1f 22 fe f2 d5 d0 1d 97 e6 d3 30 ec 63 9a 04 9e 88 2c 3f ed 5a 71 be 99 f9 08 58 6a df 3a 63 6c cb 81 25 7e 08 82 a8 04 50 0e a3 7f ec ac 13 63 dd 1a 05 0c bb b9 30 a5 c8 84 e4 2d 25 82 e6 cb ae 9f a2 09 ea 59 e9 ca 79 0a 34 11 4f 04 95 f1 34 84 ba 59 df 11 e0 d5 c8 74 b3 34 bf 97 35 70 b6 d3 d9 6c 7c 33 56 03 07 1d 6f 9a 49 27 66 c3 db b5 b6 18 db 1c 9d 06 50 6a 5d 2e 28 43 83 72 73 af bd 0b 5a 90 b5 3c dd 51 0b 05 3c d0 38 9f e6 bc 6f 96 27 4d 48 cc 2e 63 6c e1 b0 d8 69 6e a9 61 fb 96 41 5d f6 fb fe 99 35 ad 10 f3 09 64 2b 76 b4 a1 c5 bc cf eb 56 9e f8 de a1 d8 65 ea 98 cb 1f 94 44 bd 94 d1 5f 00 13 fb e0 cb 56 e2 3e cc 8f a5 7f ce e3 69 1c 5d f0 c2 47 38 72 dc 97 e3 de ee 06 db c9 Data Ascii: 8)7^=L3vk@fUT3v"0c,?ZqXj:cl%~Pc0-%Yy4O4Yt45pl|3VoI'fPj].(CrsZ<Q<8o'MH.clinaA]5d+vVeD_V>i]G8r
2022-10-03 14:16:09 UTC	3246	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2463	OUT	GET /wordpress/wp-content/themes/kawaken/images/ttl_business.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:08 UTC	2527	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:08 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "b9b9-5b252e8011240" Accept-Ranges: bytes Content-Length: 47545 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:09 UTC	2592	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 31 30 2e 31 37 20 31 32 33 2e 38 36 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 64 32 64 32 64 32 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 34 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 34 35 2e 34 36 2c 31 30 34 2e 34 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 310.17 123.86"><defs><style>.cls-1{fill:#d2d2d2;}</style></defs><title> 4</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M45.46,104.4
2022-10-03 14:16:09 UTC	2608	IN	Data Raw: 2c 30 2d 2e 38 34 2e 35 37 41 37 2e 38 31 2c 37 2e 38 31 2c 30 2c 30 2c 31 2c 33 37 2e 37 36 2c 39 37 2e 31 33 5a 6d 33 2e 35 31 2d 32 35 2e 37 31 2d 2e 30 39 2d 2e 30 36 61 36 2e 37 2c 36 2e 37 2c 30 2c 30 2c 31 2d 31 2e 32 34 2e 31 37 63 2e 30 35 2d 2e 32 37 2e 31 32 2d 2e 34 32 2e 32 32 2d 2e 34 34 61 31 2e 36 33 2c 31 2e 36 33 2c 30 2c 30 2c 31 2c 2e 35 36 2d 2e 32 6c 2e 36 35 2d 2e 31 33 61 31 2e 31 2c 31 2e 31 2c 30 2c 30 2c 30 2c 2e 35 37 2d 2e 33 35 2e 34 36 2e 34 36 2c 30 2c 30 2c 30 2c 2c 2e 30 39 2d 2e 33 34 2e 32 33 2e 32 33 2c 30 2c 30 2c 31 2d 2e 31 37 2c 30 68 2d 2e 30 38 61 34 2e 39 33 2c 34 2e 39 33 2c 30 2c 30 2c 30 2d 2e 39 34 2e 34 33 2c 33 2c 33 2c 30 2c 30 2c 31 2d 31 2e 32 2e 34 31 2e 39 2e 39 2c 30 2c 30 2c 31 2d 2e 33 31 2e 32 32 2c Data Ascii: ,0-.84.57A7.81,7.81,0,0,1,37.76,97.13Zm3.51-25.71-.09-.06a6.7,6.7,0,0,1-1.24.17c.05-.27.12-.42.22-.44a1.63,1.63,0,0,1,.56-.2l.65-.13a1.1,1.1,0,0,0,.57-.35.46.46,0,0,0,.09-.34.23.23,0,0,1-.17,0h-.08a4.93,4.93,0,0,0-.94.43,3,3,0,0,1-1.2.41.9.9,0,0,1-.31.22,
2022-10-03 14:16:09 UTC	2753	IN	Data Raw: 37 37 2e 35 36 2c 31 2c 2e 32 33 2e 33 34 2e 34 37 2e 37 34 61 33 2e 36 37 2c 33 2e 36 37 2c 30 2c 30 2c 30 2c 2e 37 35 2e 39 32 6c 2e 31 31 2e 31 34 61 31 2e 34 36 2c 31 2e 34 36 2c 30 2c 30 2c 30 2c 2e 34 36 2e 37 2c 33 2e 39 31 2c 33 2e 39 31 2c 30 2c 30 2c 30 2c 31 2c 2e 35 32 2e 36 31 73 2e 31 34 2c 30 2c 2e 34 2c 30 61 36 2e 30 35 2c 36 2e 30 35 2c 30 2c 30 2c 31 2c 2e 36 35 2d 2e 35 33 63 2e 33 2d 2e 32 32 2e 35 34 2d 2e 34 2e 37 32 2d 2e 35 35 6c 33 2e 31 36 2d 32 2e 34 37 61 31 33 2e 35 34 2c 31 33 2e 35 34 2c 30 2c 30 2c 31 2c 31 2e 36 2d 31 2e 31 32 41 31 30 2e 32 33 2c 31 30 2e 32 33 2c 30 2c 30 2c 30 2c 32 37 35 2e 31 35 2c 34 33 6c 2e 32 36 2d 2e 30 39 61 2e 36 37 2e 36 37 2c 30 2c 30 2c 2e 32 35 2d 2e 31 37 71 31 2e 34 38 2d 2e 38 37 2c 31 Data Ascii: 77.56,1,.23.34.47.74a3.67,3.67,0,0,0,.75.92l.11.14a1.46,1.46,0,0,0,.46.7,3.91,3.91,0,0,1,.52.61s.14,0,.4,0a6.05,6.05,0,0,1,.65-.53c.3-.22.54-.4.72-.55l3.16-2.47a13.54,13.54,0,0,1,1.6-1.12A10.23,10.23,0,0,0,0,275.15,43l.26-.09a.67.67,0,0,0,.25-.17q1.48-.87,1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.6	49863	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2496	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_01.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2559	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:08 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "2ff37-5b252e7c40940" Accept-Ranges: bytes Content-Length: 196407 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:09 UTC	2672	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 03 04 02 05 00 01 06 07 08 ff da 00 08 01 01 00 00 00 00 f6 55 c5 bc d2 e4 93 9a dc e3 b1 8a 41 8a 6f 40 9b 3e 6a 11 86 2f 92 13 27 1e f7 2d 6e 23 c7 46 1c 86 4a 38 28 9b 79 a9 64 8a Data Ascii: JFIF"#"" ""#>1++1>H<9<HWNNWmhm"#"" ""#>1++1>H<9<HWNNWmhmt"UAo@>j/'-n#FJ8(yd
2022-10-03 14:16:09 UTC	2688	IN	Data Raw: cc 54 44 d3 d8 07 9d 31 94 2a 15 b4 b3 e3 ec b1 35 13 6d 90 d9 e7 72 aa eb 3b 69 34 96 70 03 d2 c6 84 da a6 d3 cf 5a 97 96 1b d0 d1 31 74 a5 53 7c fe 7e 46 9e a0 d4 a7 ac 46 63 d6 8e 9c 84 95 0c 30 ba d5 b8 cf 1d ac 41 31 6c 99 6e fa 33 f3 b9 fd 8b e5 52 80 d1 19 d8 ce ce 7b 40 53 53 29 6f 09 67 1b 50 09 45 eb 9a 90 ad ee 5c ae 60 80 aa 4c 01 4e c2 a5 5a b1 67 0d c6 cb 97 3e 9b 42 14 55 96 4c 2d 5d 3c b3 81 c9 26 a2 74 a6 36 4b 43 42 61 b4 e0 34 5c ef 5a 4d 25 14 ed 48 54 3d 16 72 a7 0d b1 bd aa d4 da c5 76 43 6d bb 11 cc f8 f7 cb b5 73 56 cc 49 11 41 a4 b2 70 6e ec 89 4a 9b 0a e5 da d4 ec b3 57 9e bd b6 73 65 e5 fa 16 b5 8e 6d 6d 82 0c e9 59 3a 4f 2c 05 de 9d 1c e8 61 34 d5 d1 12 2d 7b 29 66 a3 27 5e 47 7e fc 96 b4 a6 02 51 4b 47 0f 3c f2 2f 64 51 6b 6c Data Ascii: TD1*5mr;i4pZ1tS|~FFc0A1In3R{@SS)ogPE\`LNZg>BUL-]<&t6KCBa4\ZM%HT=rvCmsVIApnJWsemmY:O,a4-{)f'^G~QKG</dQkl
2022-10-03 14:16:09 UTC	2845	IN	Data Raw: 55 3d 93 43 a8 ed 75 7c 7c 6b 9c 7e 1d 2d 56 f8 63 ed 3b 5f 81 13 ec 58 d5 56 55 e3 fa 7e bf b3 75 0e 46 df c6 06 bc 7f be 3d d1 73 ff 00 73 64 06 d2 18 fd ee 6d d7 ed a3 3a fa 91 44 5c ac 6b 81 f2 14 a4 d9 aa 9f 92 ea 36 b5 ee 0a 3c 36 a0 d3 a9 ed 6d 09 67 91 8e 5b 9f 8a b2 5f 7d bd ae f5 38 8d 71 e0 82 2e 25 77 02 5a cf 4f a9 14 15 7f 22 9d 41 e4 65 21 8d 09 ae ec 7a 40 50 bc d7 b1 15 c7 40 55 7b 9e 22 2e 47 1f bb eb 06 c4 fa b5 d8 9f 55 68 3b 5f 23 98 42 b1 04 db 8a 86 d2 60 7a ab 40 8b f5 09 d9 9e 51 61 ee a7 53 a5 1d 6a 2d 6d d1 9e de 5a 36 e2 ab 7c 3e 15 c9 f1 c1 97 ee 55 13 db a8 09 f9 8b 64 f2 6f 73 69 d6 99 d4 c0 4f e7 92 88 2d f8 82 ce e6 90 fd 9a d4 e4 44 5a dd 94 b4 fa 0c 9e 3c d4 0f 76 8f 03 b1 32 08 b1 8e cd 57 2d 65 cf 27 20 19 67 f7 6c 9a Data Ascii: U=Cu||k~-Vc;_XVU~uF=ssdm:D\k6<6mg[_}8q.%wZO"Ae!z@P@U{".GUh;_#B`z@QaSj-mZ6|>UdosiO-DZ<v2W-e' gl
2022-10-03 14:16:09 UTC	2861	IN	Data Raw: b9 52 9d cb 7c 81 87 35 71 d8 2d f4 b6 54 ad 03 ae 35 16 dd 57 36 62 5c b3 75 0f a4 23 92 e3 d3 31 2a c5 cb db 65 dc 72 32 6c b2 28 2e 00 95 fd 42 07 58 97 5e 61 c9 e0 3d e9 99 4b 9f 6e cf cc f2 2f e4 10 7f 5c 3a 79 37 90 fa 8d 21 b2 6b 31 68 41 02 a8 f8 27 40 93 8b 51 be d0 46 4e 4e 35 79 37 22 5d 6f dc 07 a7 5d 98 29 75 c6 f5 82 cd ea 54 8c 8c 5a f1 de d4 b4 2d 27 64 b5 98 a7 81 2b ea 19 16 51 6e 35 69 8c a5 30 a9 07 97 b1 a6 5f 1f a6 5d 58 02 a2 2c f5 86 ff 00 9c c2 2e a6 b7 b9 c7 e6 07 50 06 f9 2f 62 55 c8 27 5c 0f 6a cb f7 0d b0 13 91 fc 91 d4 de a6 a7 a3 13 f5 17 01 98 37 e8 b9 12 a0 3b 76 c3 63 f5 78 ec 69 3b c5 ae 5e 4a ee 06 04 41 b2 77 11 f8 89 4b d3 4f 91 ef c9 a1 50 ba d8 9e 41 f0 f7 d7 e4 b0 40 e7 7e e2 fc 4c 6b 1d 81 9c 63 68 08 b5 95 3b ac Data Ascii: R|5q-T5W6b\u#1*er2l(.BX^a=Kn/\:y7!k1hA'@QFNN5y7"]o])uTZ-'d+Qn5i0_]X,.P/bU'\j7;vcxi;^JAwK OPA@~Lkch;
2022-10-03 14:16:09 UTC	2877	IN	Data Raw: d1 dc a8 eb eb b2 03 6e 7a 7e 43 d9 61 99 46 ea bd 33 2a b1 7d b5 b5 64 d6 99 36 a5 45 43 65 25 eb 62 92 f4 0f 69 44 4d 42 ab f9 c3 a5 38 05 0e f8 d4 d9 c1 b2 f2 d6 c4 f0 d7 89 69 5a 96 33 0e 13 1f 69 5a ce 8e e3 50 96 d4 9c b2 30 58 76 d8 f9 86 b7 5a af fa a4 6f 19 9f 5c b5 66 0e 55 58 ae a1 97 97 f7 0c b3 1c f3 52 9e a1 e9 d5 e5 37 21 5e 26 46 35 ce 2d 18 79 16 5c cf 13 08 9f bd 2a 08 34 35 fa 96 8c d1 8c bb 10 7c a1 04 31 56 df e8 bd 8e 21 86 e7 f9 03 2b d8 74 9e 24 2a 0d 3c 49 f8 6f b8 c4 f8 96 e4 56 a1 8b 7a c8 5c 8f 4c 76 a8 59 8d 58 00 59 6d b7 0e 2e a2 70 63 2b c8 77 df 3f da 38 75 1b 73 0d 1c 94 51 fd 37 f2 f0 81 32 2c ad 10 f3 c9 6c 3f 38 ca 02 f7 a3 1d 15 74 cd 8d 2e eb 80 9c 1d b4 17 20 5f 5b 15 7e 25 8e 87 a2 00 36 0b 29 66 b6 5d 85 92 48 28 Data Ascii: nz~CaF3*}d6ECe%biDMB8iZ3iZP0XvZo\fUXR7!^&F5-y*45|1V!+t$*<IoVz\LvYXYm.pc+w?8usQ72,l?8t. _[~%6)f]H(
2022-10-03 14:16:09 UTC	2990	IN	Data Raw: 5b 4c 31 50 6b 58 a1 57 da 63 0c 50 07 92 6b 87 08 50 ed e9 a2 11 b1 d8 23 5c 93 49 23 c5 34 4d ba 8a ba 11 e6 21 02 8c 23 28 23 1e fc 15 4d f7 7e e0 fb e5 08 d3 66 7c 74 4d e7 92 62 1e e0 94 10 53 b4 60 b3 5d 90 96 c3 b3 8d 73 5f 3b bd 76 05 ff 00 d7 ff 00 6c a1 9a f8 44 84 33 42 0d f7 3b b0 55 bb 67 ea 53 46 c0 87 bb f3 0f 55 f3 b8 6c 8a 67 35 43 07 14 49 38 c4 ab 4a 68 76 e9 44 5c 4d d0 6b 68 31 14 30 11 24 22 25 62 29 82 f9 de 76 8c 9b f5 4f 96 de e6 3b 26 98 cd cd 3f 45 6f 7a b8 1a 7e 8a c7 aa a4 91 e8 a7 c2 50 44 90 5d 87 45 4f 3f 54 f3 2d 31 ba 63 d5 7b 33 1d 4c 7c 0e fd 55 ab ac de 0d 2f 09 1d c2 6b 6d 46 ad aa 31 54 ee 4b e5 42 0e 12 9f 7b f9 be e8 16 ce 9b c8 8e 94 3d 8a 3e 23 15 09 c4 4b d8 3d 4a 79 74 c9 de 4c f3 95 00 f2 4e 46 78 44 a6 94 d9 Data Ascii: [L1PkXWcPkP#\I#4M!#(#M~f|tMbS`]s_;vlD3B;UgSFUlg5CI8JhvD\Mkh10$"%b)vO;&?Eoz~PD]EO?T-1c{3L |U/kmF1TKB{=>#K=JytLNFxD
2022-10-03 14:16:09 UTC	3006	IN	Data Raw: f0 35 1a 0e 98 af 88 9a f5 58 3a d2 cd bf 45 a8 08 ff 00 e3 3e 74 55 1e e0 d8 e5 a7 ee 72 b4 3e 8b f2 fa ad 41 f2 d9 9d 97 fe d5 78 d3 e5 94 0f fe 99 59 b7 e5 23 d5 65 07 cf dd f0 97 80 79 1a 15 37 43 5c da f3 9d 8e 21 b3 54 04 c0 08 5e 9f 85 3b 84 66 15 41 2a 4b 6a 61 56 95 4c 16 96 6e 93 74 fd 16 fb 18 0c b3 e2 1f 74 77 af 1a 22 a8 74 d9 94 a2 40 24 61 c1 32 ba e2 51 85 54 26 aa 6d 6c ff 00 d6 3e e9 d2 dd 3f cc 16 3a 7e ed bc b8 72 5b ec f3 ed b3 04 51 a1 34 5f 03 07 dd 38 92 e7 9c 78 6d 12 49 34 d5 09 bb 92 af aa 17 a3 3d 17 ed 2d 78 65 cd 1b ce c9 a3 00 be 5f 4a ad c6 ea 46 3c 91 1c 4e 7b 30 0d 26 8a c5 cf 82 6e 5a 78 80 e6 02 b4 16 9c 41 a0 fd cb a1 6e 37 e4 3f 17 34 c8 f4 44 0f da c4 9c a8 bd a5 af 6f 88 01 92 05 f1 f2 89 56 0f af 0d 98 28 32 08 e0 Data Ascii: 5X:E>tUr>AxY#ey7C\!T^;fA*KjaVLnttw"t@$a2QT&ml>?:~r[Q4_8xml4=-xe_JF<N{0&nZxAn7?4DoV(2
2022-10-03 14:16:09 UTC	3022	IN	Data Raw: 70 80 1a 6b 6e a1 c3 0f 92 3e de 23 c1 6a 69 af a3 2c 6c 01 ba 09 ec b7 22 c2 e1 bb 15 39 04 88 f9 d8 9f 23 a6 8b 47 c4 d0 44 72 5f 04 a1 c1 76 ae 0d 00 2d 57 0f 3c 46 e0 93 4a b2 d0 e4 be 96 07 dc aa e2 b6 cc 67 34 85 7f 14 2e 15 7b b8 14 91 1d 89 4f ea 53 52 ae 9c fa 00 44 ee 90 e8 ad 08 36 04 df b8 5f 24 05 3a 4d 40 91 92 ea 55 8b 56 97 08 e9 fb 4b 71 f3 f1 09 de 90 56 c1 05 30 0d 34 f9 a8 35 b6 5b 11 c0 83 85 bd 42 a3 15 1d 31 45 dc e5 7f e2 14 c4 0c 08 ba a1 c8 52 e1 b9 6b 42 90 71 16 8a 3a 1c 0b 8a e8 fa c5 2d 75 77 63 b2 b1 7a 6d c0 1d 8e 5d 1c 22 52 39 07 05 83 5f 69 96 50 ec 34 95 55 b3 7d 5f 4b 13 28 fc d8 61 d2 fa 83 09 48 b7 a3 91 4c 27 41 14 71 a4 ec 8f a0 eb 73 7f 31 2b b0 b8 95 5d 50 4a 14 d3 7b 7a cb e7 62 30 b7 db 2d 8a 9a a2 9f 29 01 45 Data Ascii: pkn>#ji,l"9#GDr_v-W<FJg4.{OSRD6_$:M@UVKqV045[B1ERkBq:-uwczm]"R9_iP4U}_K(aHL'Aqs1+]PJ{zb0-)E

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	3038	IN	Data Raw: 2f 86 2c 50 b9 5a ee 36 c5 25 57 56 d7 52 a6 ad 88 1b 17 eb 55 c1 9a aa 87 60 4c 43 f2 69 3d ca 4d 1b 74 e7 9b ad 25 cd 12 59 54 3d 64 bb 2c f0 a0 33 25 57 7a c0 48 ed 85 d5 79 85 55 0a 28 8e 0c 8f 20 2f 30 52 2c 5c 00 c3 00 e1 7a d1 2f 65 01 35 80 e1 17 37 76 9e b1 49 7e 11 c4 46 82 2a e5 45 7e a1 d6 fa 27 bf 44 21 c0 ea 62 da 95 e9 47 ba 1f cb 2e 5f 44 b5 fe aa 65 a9 4f 5d 6f 55 2d 6d 0f 6c 54 2f 29 fe 93 01 a5 a5 e5 01 f5 2b a1 a7 0a 45 50 93 ce 0f e8 8e a8 77 75 af e6 56 b6 3b 56 d6 35 7c 2a cd 35 a2 5b d6 fc 13 9a 6c b7 8f e5 3a ca 9b 04 3e 84 9b b1 81 00 7a 42 12 13 6e aa cc f7 73 27 e3 4e 5f 94 2c 95 91 49 d7 4d 65 d8 c3 b9 34 e8 73 cc 68 a3 65 99 fc cf 37 37 50 b6 4a ca 73 2d 35 39 ee 16 ae 5e 1a f1 1d d7 c0 65 f9 54 e6 03 49 16 01 44 01 17 06 c0 Data Ascii: /,PZ6%WVRU`LCi=Mt%YT=d,3%WzHyU(/0R,\z/e57vI~F*E~'D!bG._DeO]oU-mIT/)+EPwuV;V5|*5[!:>zBns 'N_,IMe4she77PJs-59^eTID
2022-10-03 14:16:09 UTC	3054	IN	Data Raw: 38 81 3e e2 05 04 3f 17 2e 96 48 b1 c0 06 44 9c 9e 94 7e 84 85 2c 12 35 94 39 36 b8 f9 82 05 63 c8 c4 5a d3 40 a0 a4 b4 28 a7 40 a7 f3 0a eb 9d 07 96 15 34 71 8a fa ee 15 30 d6 23 64 62 93 7d bd b9 a4 f8 bb 6b ee 54 a2 d7 51 ec 40 3a 05 5f ab 85 8a 0f c4 3f 6c 95 f0 43 a3 91 9c 14 ff 00 e8 77 36 4f a1 ec b6 54 91 ed 4d 4c ac 81 29 65 f0 c7 ed 9c 80 7c ff 00 00 81 c0 bb 84 b7 c2 fd 4f 21 79 9e e0 25 f6 1e 47 f6 44 dd 76 d5 96 97 cd f1 3b fc 6d 66 76 b7 81 81 a4 43 c3 9a 89 d5 74 b3 6a 81 0f 00 c2 c4 e8 57 80 7e 22 18 de f0 f4 9e 12 29 28 0e 2f fd 20 ea d1 f6 40 f7 37 af 4f 3e bf 11 0d 56 dd 1f ea 17 6e 7c 94 45 28 65 72 61 03 f2 57 fe 0c 5d a7 40 6b fd 97 e1 a5 ab 0c 66 90 d1 48 57 d5 c5 20 10 d0 51 f2 6d 45 0e 34 ec d5 c5 2a cb 00 59 c8 37 69 b6 d5 51 2e Data Ascii: 8>?.HD~,596cZ@(@4q0#db}kTQ@:_?ICw6OTML)e|O!y%GDv;mfvCtjW~")(/ @7O>Vn|E(eraW]@kfHW QmE4*Y7iQ.
2022-10-03 14:16:09 UTC	3070	IN	Data Raw: 22 84 97 0e 8d 5d 9e 48 ec 8f 91 51 28 2b cc 34 8d 6e 6d 41 a5 e2 e5 9f 8a 2d 47 b5 af 8b 85 27 c3 a5 3b 85 c1 48 25 00 4a c5 2e 97 20 6a 83 37 d1 25 05 aa 6d b0 b1 54 04 1a 2d 30 45 74 70 e8 1b 49 1e 57 7d 4d b5 56 ed ce 25 e9 70 4c 6a e6 9f 60 8f e4 85 c3 4b e4 bc 95 08 07 cb f8 2f 72 5c ce 1e 7f fa 4b 9d 92 e8 dd a7 53 df 80 bf 0d 95 06 cd 6e e2 20 b4 a9 f1 48 c8 51 ab 67 08 c4 be 81 08 c1 01 48 3a b5 e5 83 67 86 5c 4e 38 73 29 7a a9 4d c2 97 b4 03 29 0f 97 16 cb 6f 0b 2b dc 10 e6 cb 69 b8 41 62 cf 92 c3 82 30 22 72 c2 61 cf 25 2d a2 b2 59 77 ff 00 c5 08 71 e4 7f 70 ad 13 9e e0 3f 6e 25 03 a7 fb 21 db 29 9f c4 c7 80 0b 72 26 cf 44 82 87 d4 ad aa 8a d3 d9 bc 3e a6 4c 22 27 9f 0f 86 57 50 92 af 8c 45 68 6b a1 35 65 8f 99 82 c0 3d 0a 3c c2 c0 ed 63 78 a0 Data Ascii: "]HQ(+4nmA-G';H%J. j7%mT-0EtpIW}MV%pLj`K/r\KSn HQgH:g\N8s)zM)o+iAb0"ra%-Ywqp?n%!)r&D>L"' WPEhk5e=<cx
2022-10-03 14:16:10 UTC	3278	IN	Data Raw: cb 72 2f 41 56 42 82 86 09 d9 74 de da 35 1e a1 47 8c 28 47 d1 7d 50 0e 90 f7 2f f6 28 bf b9 9f 3a ed af cd 43 68 82 77 17 7b 16 9b 11 c2 f7 8d 04 3f 21 b0 d8 7c 6e 34 41 03 51 73 a3 44 04 21 87 40 d7 15 75 14 95 51 e4 90 37 d4 48 d1 49 4f 1b fe 40 27 22 be 4a 18 ef 11 00 b3 be 20 52 ee 46 dc 71 f2 46 85 41 73 91 11 2d 54 a7 0a 7f 64 ae 85 5a dd 0e 5f dc ef b0 0d 35 a7 87 a0 87 45 2c 23 62 79 18 8a 01 47 fb 88 e0 93 c0 0a 5b bb 95 60 61 4f 9f 8f 64 73 6a da 03 76 ca 8e b5 0e 8f 78 09 fc 49 f9 58 10 07 8a c1 87 ac a3 c4 ea 19 c4 76 2a 35 cb 1f a8 08 e7 1f 87 f7 2b 9d ae ef 27 90 e1 37 9c 7f 10 5e b4 4b 16 c7 07 3f 71 29 61 69 e7 b2 6a 2d 0b 70 78 ea 14 93 5a da 1f 4f e6 5b af 69 fd 5c 9e e7 32 92 7e ca 7f 3c 47 a1 5a 1f c1 1e 55 5a b1 ce b1 75 e4 0b 6c be Data Ascii: r/AVBt5G(G}P/(:Chw{?!|n4AQsD!@uQ7HIO@'"J RFqFAs-TdZ_5E,#byG[`aOdsjvxIXv*5+'7^K?q)aij-pxZO[i\2~ <GZUZul

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49720	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:35 UTC	31	OUT	GET /wordpress/wp-content/plugins/wp-pagenavi/pagenavi-css.css?ver=2.70 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:35 UTC	32	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:35 GMT Server: Apache Last-Modified: Thu, 01 Sep 2022 09:44:21 GMT ETag: "176-5e79a753a4b16" Accept-Ranges: bytes Content-Length: 374 Connection: close Content-Type: text/css
2022-10-03 14:15:35 UTC	32	IN	Data Raw: 2f 2a 0a 44 65 66 61 75 6c 74 20 73 74 79 6c 65 20 66 6f 72 20 57 50 2d 50 61 67 65 4e 61 76 69 20 70 6c 75 67 69 6e 0a 0a 68 74 74 70 3a 2f 2f 77 6f 72 64 70 72 65 73 73 2e 6f 72 67 2f 65 78 74 65 6e 64 2f 70 6c 75 67 69 6e 73 2f 77 70 2d 70 61 67 65 6e 61 76 69 2f 0a 2a 2f 0a 0a 2e 77 70 2d 70 61 67 65 6e 61 76 69 20 7b 0a 09 63 6c 65 61 72 3a 20 62 6f 74 68 3b 0a 7d 0a 0a 2e 77 70 2d 70 61 67 65 6e 61 76 69 20 61 2c 20 2e 77 70 2d 70 61 67 65 6e 61 76 69 20 73 70 61 6e 20 7b 0a 09 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 09 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 42 46 42 46 42 46 3b 0a 09 70 61 64 64 69 6e 67 3a 20 33 70 78 20 35 70 78 3b 0a 09 6d 61 72 67 69 6e 3a 20 32 70 78 3b 0a 7d 0a 0a 2e 77 70 2d 70 Data Ascii: /*Default style for WP-PageNavi pluginhttp://wordpress.org/extend/plugins/wp-pagenavi/*/.wp-pagenavi {clear: both;}.wp-pagenavi a, .wp-pagenavi span {text-decoration: none;border: 1px solid #BFBFBF;padding: 3px 5px;margin: 2px;}.wp-p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.6	49867	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:08 UTC	2497	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_01_w.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:09 UTC	2559	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:08 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "351-5b252e7c40940" Accept-Ranges: bytes Content-Length: 849 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:09 UTC	2559	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 33 2e 35 33 20 35 31 2e 39 31 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 2e 63 6c 73 2d 32 2c 2e 63 6c 73 2d 33 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 63 61 70 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 77 69 64 74 68 3a 32 70 78 3b 7d 2e 63 6c 73 2d 32 7b 73 74 72 6f 6b 65 3a 23 66 66 66 3b 7d 2e 63 6c 73 2d 33 7b 73 74 72 6f 6b 65 3a 23 30 31 35 38 39 61 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 53.53 51.91"><defs><style>.cls-1{fill:#fff;}.cls-2,.cls-3{fill:none;stroke-linecap:round;stroke-linejoin:round;stroke-width:2px;}.cls-2{stroke:#fff;}.cls-3{stroke:#01589a;}</style></defs><title>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.6	49878	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	2704	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_circle_arrow.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:09 UTC	2989	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:09 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "1d5-5b252e7c40940" Accept-Ranges: bytes Content-Length: 469 Connection: close Content-Type: image/svg+xml

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:09 UTC	2989	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 33 2e 33 33 20 32 33 2e 33 33 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 37 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 68 6f 76 65 72 22 3e 3c 63 69 72 63 6c 65 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 63 78 3d 22 31 31 2e 36 37 22 20 63 79 3d 22 31 31 2e 36 37 22 20 72 3d 22 31 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 23.33 23.33"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 7</title><g id="_2" data-name=" 2"><g id="hover"><circle class="cls-1" cx="11.67" cy="11.67" r="11.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.6	49881	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:10 UTC	3294	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_01.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:11 UTC	3299	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "354-5b252e7c40940" Accept-Ranges: bytes Content-Length: 852 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:11 UTC	3299	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 35 33 2e 35 33 20 35 31 2e 39 31 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 61 3b 7d 2e 63 6c 73 2d 32 2c 2e 63 6c 73 2d 33 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 63 61 70 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3a 72 6f 75 6e 64 3b 73 74 72 6f 6b 65 2d 77 69 64 74 68 3a 32 70 78 3b 7d 2e 63 6c 73 2d 32 7b 73 74 72 6f 6b 65 3a 23 30 31 35 38 39 61 3b 7d 2e 63 6c 73 2d 33 7b 73 74 72 6f 6b 65 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 53.53 51.91"><defs><style>.cls-1{fill:#01589a;}.cls-2,.cls-3{fill:none;stroke-linecap:round;stroke-linejoin:round;stroke-width:2px;}.cls-2{stroke:#01589a;}.cls-3{stroke:#fff;}</style></defs><title>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.6	49880	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:10 UTC	3294	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_02.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3298	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "72497-5b252e7c40940" Accept-Ranges: bytes Content-Length: 468119 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:11 UTC	3300	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 06 06 06 07 07 06 09 0a 09 0a 09 0d 0c 0b 0b 0c 0d 14 0e 0f 0e 0f 0e 14 1f 13 16 13 13 16 13 1f 1b 21 1b 19 1b 21 1b 31 26 22 22 26 31 38 2f 2d 2f 38 44 3d 3d 44 56 51 56 70 70 96 01 06 06 06 06 06 06 07 07 06 09 0a 09 0a 09 0d 0c 0b 0b 0c 0d 14 0e 0f 0e 0f 0e 14 1f 13 16 13 13 16 13 1f 1b 21 1b 19 1b 21 1b 31 26 22 22 26 31 38 2f 2d 2f 38 44 3d 3d 44 56 51 56 70 70 96 ff c2 00 11 08 04 74 03 84 03 01 11 00 02 11 01 03 11 01 ff c4 00 1c 00 00 03 01 01 01 01 01 01 00 00 00 00 00 00 00 00 00 04 05 06 03 07 02 01 00 08 ff da 00 08 01 01 00 00 00 00 9d 51 43 e3 f0 0e 89 30 0d b2 f5 a0 6d 91 2e 2b 43 d3 3b 04 35 76 6e a4 7f 1c d9 4e e9 04 67 23 44 c7 4d 07 f8 bd b7 9c f7 c5 Data Ascii: JFIF!!1&""&18/-/8D==DVQVpp!!1&""&18/-/8D==DVQVpptQC0m.+C;5vnNg#DM
2022-10-03 14:16:11 UTC	3316	IN	Data Raw: 0a ea bc f1 74 cf 9b 3d 31 1f 1c 86 4d ef a6 ad fe 0e 3a 14 ce d3 9d 1e b7 8c e6 b9 af 98 c5 ef f3 2a e9 29 96 43 dc df 53 d5 4c 16 59 a2 df 11 97 14 2b f7 7c 57 fb d1 17 9f 5f af 9f 1d e9 fa a8 57 a3 e5 d6 67 e6 04 d7 0d 12 ae 57 b2 99 da 98 e7 a5 d3 b9 e0 71 7b 1e 59 4d d7 ec ce 77 9b b0 f3 15 4a 64 b3 d0 39 fc 8d 21 21 6e 11 a2 4a ea 57 ad 22 a3 2b 42 cd 18 22 7c b5 3b 9d 27 a4 7e 9a 5d e5 5a d0 2f 3e f8 a6 ab 93 77 91 71 a8 ac 33 fa 6d f3 04 a7 8e 2a 73 5d 1c cd a3 81 fe 25 f3 62 7d 0f 3a ed 6b 1b a9 8e bc 5c 96 df e6 40 0f 24 07 b1 e1 7b bf 45 f3 91 42 8a 81 14 46 ca d5 3d 2b ad ba 09 15 97 a0 32 fa 40 68 7a 61 aa 7b bd 23 f3 aa 75 75 79 49 7e 46 0e 8a 1b 6c 44 14 1f 91 f4 cb 6d a7 65 10 94 30 ef 19 3b ca 7b 3c 8f 68 fe 43 df a2 39 3d 9f 23 d6 e0 69 Data Ascii: t=1M:*)CSLY+|W_WgWq{YMwJd9!!nJW"+B"|;'~]Z/>wq3m*s]%b}:k\@${EBF=+2@hza{#uuyI~FIDme0;{<hC9 =#i
2022-10-03 14:16:11 UTC	3339	IN	Data Raw: 76 e9 46 8b 2e 15 1c 1e 83 bf 3c b2 61 d1 93 3d ed e7 60 f9 53 62 c3 6c db 14 08 6f 80 c0 31 01 f3 ba 3c e4 bb a8 a8 11 04 ea d4 be 45 4b 4f 6a 44 2d 88 7c c8 89 7e 8e 05 20 5c e5 22 49 6a f1 1b e4 74 96 c6 8c 87 76 9e 0d b6 93 b6 28 a4 02 30 1a 97 d8 c9 90 ec 33 ea 8a 4f 34 4d c7 4f 0a 6c 0d 8a bc 16 8f 91 75 b9 45 2c b4 07 34 2a 8a b9 f0 e8 bf 13 a0 2d 1b f1 4b aa 5b ab 99 d9 15 ee bb 57 a5 bc 86 61 2a 38 dc eb b6 db 6d 9f ab 10 af 14 a0 c1 73 5d 99 72 b9 5a 34 4e 81 c4 85 66 38 42 af 29 bb e7 65 03 ae 33 a9 9c 49 6a a6 ca 0b d8 78 dd a6 7d 5c d1 bc 5a ad 99 f9 c1 b2 ac 05 dc ee 1c 41 18 9d 8e d6 29 41 a4 0e 1b 6d 4b b6 95 4e 77 e9 e1 10 62 fc ed 4d 2b 1c a9 b1 04 e4 6b cd 6c 8e 24 8f 92 c1 54 67 7a f9 ab dd 69 27 2b 3a 37 64 f8 aa ba d9 72 91 78 47 6d Data Ascii: vF.<a=`Sblo1<EKOjD-|~ \"|jtv(03O4MOluE,4*-K[Wa*8ms]rZ4Nf8B)e3|jx}\ZA)AmKNwbM+kl$Tgzi'+:7drxGm
2022-10-03 14:16:11 UTC	3355	IN	Data Raw: c3 c9 92 bc 5a f5 d4 9f e9 f5 92 4c a6 94 a4 e1 33 0b 01 39 5c eb 03 62 b7 b5 ec 39 6d 8f f0 b8 c6 65 26 96 fe ed c9 c7 db a6 57 11 54 c1 f0 26 46 71 01 ff 00 48 59 a5 83 f6 72 44 c3 11 0b eb d4 5b 7f e6 b1 18 0d b6 8b 55 4b dc b3 8c 43 dd e3 f1 dd 50 ad da d6 e2 e5 f1 68 ad 2b 4b 2a b1 d9 5b 0e 55 36 ac 39 44 50 aa 0e 01 c5 4c b6 26 0a ea 79 27 09 f4 2d a2 93 e3 b6 8a ce c2 df 36 1a 28 7c a9 9e 7d 8f 8e 0d 73 98 5a bc 92 03 95 1e a9 62 7b 08 59 7f c0 92 d9 68 14 b3 cd 3a 18 55 c0 33 e9 f6 06 3d 38 c0 8b 75 8b ea 7d 6d fc db 8d ea 59 36 76 72 5b cc ec 44 d9 40 3b 63 25 82 57 52 3a 8d be 82 b6 20 ca d4 a2 bc 71 69 2b 12 90 8d d5 dc 6a ce 5d 6b b1 aa 68 b6 06 ec db 8c 00 b5 d8 2b 21 df 9a 68 b3 d9 6d 75 f5 2b e5 c7 c8 60 d3 f5 81 5d 79 b0 ab 55 5e 6e f1 9e Data Ascii: ZL39\b9me&WT&FqHYrD[UKCPh+K*[U69DPL&y'-6(|)sZb{Yh:U3=8u}mY6vr[D@;c%WR: qi+j]kh+!hmu+`]yU^n
2022-10-03 14:16:11 UTC	3371	IN	Data Raw: 40 bf 84 93 99 dd 1b 41 33 89 ff 00 cb 34 b3 9f 7b cf aa ba 79 18 cc b4 da 6e b3 61 36 13 65 9b 2c ca 4f 49 aa ce bf 8e 38 cd f5 cb 57 4f 80 cf fa 0c ad f3 e5 20 81 2b bf c3 7f 24 8b 2c 36 bf 7c 34 f7 69 77 e0 2b 96 31 5c a4 b5 cf c4 ae b2 7d bf e0 c9 86 ce b3 0b a4 7b 35 23 02 ef 81 28 5f 55 32 fe 4d 34 0f 77 e6 0b 01 01 c3 35 85 e3 bb 11 ee 9c 80 a2 1b 05 89 99 4f 22 bb 14 23 d9 59 5c ce 45 9a aa d4 7e 98 64 67 3f 49 6a 9a c5 db 10 0b 60 40 32 23 8f 78 dc 90 8b aa fc ce e6 25 60 31 ed ec 06 54 09 65 24 bb 45 6c c5 5d a2 55 93 1e b0 13 be 84 3c 94 0a 25 8e b6 76 71 e4 5e 9b 65 f9 5d 5c e2 53 5e 88 d1 f6 66 85 58 99 f4 e3 5c b5 03 03 31 dd b5 c9 77 63 f8 8d d4 c1 b3 46 4e a6 ae 33 9a fd 60 3d e4 7d 41 12 cf 5b 2e 46 65 0d bc ac 66 83 b5 55 9c e6 00 fd 92 Data Ascii: @A34{yna6e,OI8WO +$,6\|4iw+1\}{5#(_U2M4w5O"#Y\E~dg?Ij`@2#x%`1Te$El]U<%vq^e]\S^fX\1wcFN3`= }A[.FefU
2022-10-03 14:16:12 UTC	3420	IN	Data Raw: 8f 4c da 5d 05 97 96 d9 74 fa 76 f9 82 84 45 cb 2d 48 4b 6a 9f 8e a1 46 55 94 a9 ae 91 17 0f 61 78 b6 05 ad 44 e4 5a c8 06 0b 17 ec e2 62 71 fa 69 83 3a 85 b1 1b 42 73 2a b4 c7 7c fe 59 39 e8 e3 fc ad d1 a6 ac 17 bc 8f 50 30 0e 35 a7 8d bd 5a 4a 4f 2f 8e 02 59 6f 23 60 41 4a 6d bc 1f 1a d5 7d 00 b3 a5 bf 53 b8 96 f1 ae 11 5b 49 e7 cc 0a 7a 2c 49 51 80 6d 6e e6 e6 6f 36 9b 7f 05 2a 6f 9f 13 2f f6 a9 52 9f 22 90 cb b2 b8 bb 38 1f ac 4d 40 84 60 91 05 0a 6c bc 93 e3 55 ca 38 1d 18 b6 78 76 d1 6f 67 5a eb 96 51 5a 92 eb 50 a1 c1 dc d1 89 5f 12 de f5 6a 1a a5 20 27 1a d1 d9 b3 ef 3e b1 91 d2 d0 92 ca 8f cc 3e 23 d1 50 81 70 c7 c6 4e b3 53 b0 81 14 1f 4a 6c 2f f6 e6 5d 5b d9 0e 47 57 db d0 13 61 6a be 45 76 58 32 98 62 46 b4 54 e7 65 8d 45 8e 47 96 c0 85 bc 23 Data Ascii: L]tvE-HKjFUaxDZbqi:Bs*|Y9P05ZJO/Yo#`AJm}S[Iz,lQmno6*o/R"8M@`lU8xvogZQZP_j '>>#PpNSJl/][G WajEvX2bFTeEG#
2022-10-03 14:16:12 UTC	3436	IN	Data Raw: 84 09 a0 09 a8 1b aa 36 05 f5 46 6a 89 84 0f a8 0b f9 9d 8f f7 5c 33 bd 63 f5 59 5b d0 94 75 bb 56 67 0e a9 a6 da d5 0c a7 a5 14 76 1b a2 64 6e 68 b8 4d ea b8 6d ed 28 76 85 27 78 b2 0e 0e a4 99 4c 64 d6 a4 4a 6e c8 1c 01 24 45 13 5e 32 de a0 20 e0 37 2b f8 91 23 45 c4 67 41 9a 17 16 7b 4e 19 fa 27 3e 00 f9 8d c2 e2 4a e3 41 69 b2 37 73 48 3b 52 57 15 8e 73 85 41 5c 31 dc 27 3b 29 d3 f5 56 1e c8 c8 26 bd 93 7e 6b 77 46 bb e8 13 c9 8a ec 15 76 41 b1 34 1a af 50 ab d3 75 cb 16 ae a5 65 ce d1 a5 20 7b 26 49 26 47 95 13 be 58 8e 9d 53 e0 e6 34 db a2 88 cc 08 4d 9f 38 5c 39 d8 0a 28 8a c6 d0 d4 67 c9 0b a2 8d 5a 7c aa 85 91 3d 54 f9 e8 84 02 8d 74 c3 78 5f d4 4a a9 1a ce 8b e6 33 69 47 28 9f 34 4c ef 72 8f 8f 87 3e a8 0a 01 1d 13 49 b5 67 74 26 54 4e 55 a2 24 Data Ascii: 6Fj\3cY[uVgvdnhMm(v'xLdJn$E^2 7+#EgA{N'>JAi7sH;RWsA\1';)V&~kwFvA4Pue {&I&GXS4M8\9(gZ\|=Tt x_J3iG(4Lr>Igt&TNU$
2022-10-03 14:16:12 UTC	3452	IN	Data Raw: 4c 98 25 42 a4 09 09 97 b2 15 43 45 a5 d1 4d a8 56 43 0a e0 53 54 60 50 a7 dd 6d 83 95 7e 0a 14 ec 4a e1 d7 39 5a 58 68 86 a8 d1 49 11 1b 20 a3 cd 16 f9 20 13 14 28 a6 89 e2 e9 c2 01 1e ca c4 d7 b2 74 82 ad f6 56 df ff 00 81 b4 fa e1 a9 85 a7 fa 07 00 50 41 70 c0 ea 11 95 44 20 47 aa 15 36 42 a8 4b 76 54 c6 c0 61 a2 94 13 a1 32 9d 0a f7 51 f0 0c 44 c9 54 c3 44 53 93 97 cb 46 ab ca d7 54 ed 7b ad 56 a8 21 0d 08 27 08 c0 05 52 82 14 55 f8 61 46 03 cf 03 64 31 f4 4d 3f 74 5a b8 23 c6 66 65 70 db 42 01 71 34 46 e5 36 7c d0 b5 d3 eb b2 04 9d 6a 9a 00 ec a2 73 5b 75 c3 b9 52 4c 6c 9a 6a b9 5b 09 a1 a0 c7 52 50 6b 43 44 cc ca e0 70 f2 90 39 a2 b8 ef 80 4c 2b 84 57 0d 37 dd 47 fa 1d 30 d0 ad 70 2b 6f f4 02 8c 1c 8a 9b 5d 15 18 3a 07 c3 28 51 32 b8 42 12 54 f5 44 Data Ascii: L%BCEMVCST`Pm~J9ZXhI (tVPApD G6BKvTa2QDTDSFT{V!'RUaFd1M?tZ#fepBq4F6|js[uRLlj[RPkCDp9L+W7G0p+o]:(Q2BTD

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3468	IN	Data Raw: 2e 8d 27 88 2e 42 8e 35 2f 79 de 83 fd 78 81 b9 69 8a f1 5c 44 54 0c cc d1 d1 be 15 96 52 18 1e 40 37 fb 22 a8 8d 39 63 e9 89 4c c0 7e 01 39 61 05 03 5a 9c f3 50 a5 2d 61 f5 29 9c 01 43 66 d1 97 6a fc c1 68 30 ac 55 71 f1 2d 6d b1 9b 0a 13 75 e2 1f 36 4c de fb 7f a8 e8 c1 91 9b 75 02 c5 6c 9f 4f 51 50 d1 b5 3e 1f 24 b1 51 49 74 c6 7c eb d4 21 7c 0c 0c 59 e7 ea 28 81 1b 34 e6 39 25 5b 46 87 9d ca 14 0f 04 76 9d 38 be 7e a3 97 8b 54 5e 4c 43 50 69 9d 17 6f 05 13 70 83 b1 3f 33 3e 4c cf 5a 23 57 3c ed 76 2e 5e ea 3a ae 7f ea b8 ba ae 57 6d af 72 8b f6 2e 25 55 2c e9 c1 d3 f2 96 60 2a 3a a3 c9 9a 45 c4 b8 27 0b e4 f5 3a 37 29 a8 1e 49 9c 98 97 4c b2 28 5b 05 fe 7c 4c 6f db 0f 8b e1 01 2f b6 00 c0 ac bd f1 2d a7 86 53 50 e2 ab ea 0e e1 40 4c 07 6c 11 45 8b 3a Data Ascii: .'.B5/yxi\DTR@7"9cL~9aZP-a)Cfjh0Uq-mu6LulOQP>$QIt|!|Y(49%[Fv8~T^LCPiop?3>LZ#W<v.^:Wmr.%U ,`*:E':7)IL([|Lo/-SP@LIE:
2022-10-03 14:16:12 UTC	3484	IN	Data Raw: a8 53 b6 e5 e3 76 f9 96 73 1e 36 17 5f 6f 70 63 65 d8 d6 99 c7 37 08 e6 68 40 57 f1 13 54 13 fd ef a4 62 69 33 6c 0f 5e c6 79 49 6e d8 4d 95 db 95 12 b1 ca ac 85 fc b0 a9 16 29 e2 22 ed 4f 0a 6a 00 54 2d 26 38 e2 73 ef 7d 42 f2 04 15 56 90 f5 9f e6 26 7f a2 b0 71 a7 b7 58 ce e6 f8 05 a0 dd db b8 ec 6d f1 da ff 00 51 29 68 b7 c8 83 62 bc fe 06 51 e8 ab 02 dd ab 3c 54 ca 30 14 c5 1a cf cc 3b e0 15 97 cc 24 2d 4f 03 ed 60 2f 88 2b 0e 53 6e cf ed 29 70 1d 18 25 95 dc 0a 5f 1e 63 45 e9 99 40 01 2e bc 45 da 3e 65 85 d4 2d b1 e8 33 32 64 f7 03 42 3e 49 84 61 e5 18 37 ea 27 dd 5c 0b 11 48 63 cc 2b e8 89 d6 1e 7f f2 5f 88 15 6a a4 7b f5 2f c6 c2 b3 36 e8 ec 7b 83 56 7c 30 f7 ca a5 1d 79 80 4f 1c 46 49 23 00 ad d4 27 a8 39 39 57 83 3b fb 38 c3 95 e0 cf 1b 3d e9 9a Data Ascii: Svs6_opce7h@WTbi3l^yInM)"OjT-&8s}BV&qXmQ)hbQ<T0;$-O`/+Sn)p%_cE@.E>e-32dB>Ia7\Hc+_j{/6{V |0yOFI#'99W;8=
2022-10-03 14:16:12 UTC	3500	IN	Data Raw: 05 d9 e2 56 d0 05 bc e2 2c 1b af ce f0 b8 08 1c 59 71 9f ee 07 e4 5a fb f3 18 60 72 a3 4f 0c cc 13 54 31 e3 fa 25 25 1b 1f f7 98 80 a2 b5 2e de b3 04 56 95 3a 3e a5 27 24 2b 7a ac 3f 71 9f 4b 81 79 c1 4e 25 c6 a9 50 53 8f cc 28 65 6f 6d 99 94 c5 b5 5c e2 ef 88 9b a6 85 d2 bc 46 00 16 6d bd 90 d1 5e 48 70 6a a0 35 73 1a dd c0 30 55 2b a5 79 21 2d c0 30 0f 51 18 d4 75 36 6a ba da 50 b4 9d bf 78 8d e8 ec 6d d2 5b d7 0c 3c ce 58 27 24 1d ea ff 00 73 24 7e 90 11 de e1 0e 38 a5 2b fb 5e 22 d0 6c b2 f1 d5 93 b3 8e 59 b5 84 4c 4d e5 96 5e 73 77 71 38 25 6b a7 55 4c 40 01 c0 e6 fb f8 86 af 41 0d 8b c7 9b 88 30 38 95 82 5e 94 51 7f dc 29 c5 81 5e 8e 7e 66 21 ae 0a ea 54 03 de 74 1c dd 11 2c 65 7f 18 07 79 cf 99 cf 88 5d e3 07 dc 52 f3 0e 5a 37 33 1b 9c d9 d3 17 03 Data Ascii: V,YqZ`rOT1%%.V:>'$+z?qKyN%PS(eom\Fm^Hpj5s0U+y!-0Qu6jPxm[<X's~8+^"lYLM^swq8%kUL@A08^Q)^ ~f!Tt,ey]RZ73
2022-10-03 14:16:12 UTC	3566	IN	Data Raw: e7 99 11 07 ba 43 8a 98 7e cb fe 23 29 19 54 ac 0e 6a 70 f5 4c 4d 4b dc 0e 21 6e b0 63 6c 54 60 85 84 3d 12 d8 8d 55 71 7b 8a 22 b7 79 66 f2 9f 25 cb 82 dc 84 0c b2 c5 03 cb c7 52 ab 58 53 41 c4 75 e7 2d 57 27 07 98 db 45 cc a8 ea e2 80 64 bd 6e 59 c9 f6 65 b2 a1 4c 61 f7 10 2b ef 98 f2 1a dc c6 cd 34 79 94 32 ed 2c 1a 32 2b cf 10 cb 45 33 00 39 bd 54 d2 a8 46 9f ca 5b 68 a5 58 a4 ad 90 4a ad 2d fe 12 f6 e6 3c 4a 96 10 78 8a f3 2b cb 2f 73 a7 52 f9 97 cb fd ca d3 66 10 40 a6 b7 8c c3 c2 d7 92 d2 92 52 ba 1b 19 8f 6c e6 ed be ee d8 58 a8 5e d2 8d 6a 68 e1 d4 67 36 8c d0 b3 10 59 64 b4 59 a8 05 78 f0 23 f3 13 08 5b 63 99 a4 e4 4a f1 ff 00 88 5a d1 2d b9 ea 19 6a 6e 49 42 d8 fe 88 d3 3f f7 91 86 07 e4 09 4c 72 01 18 ba ca 9c 73 8e 60 de ec 47 f7 3d 65 3a ff Data Ascii: C~#)TjpLMK!nclT`=Uq{"yf%RXSAu-W'EdnYeLa+4y2,2+E39TF[hXJ-<Jx+/sRf@RlX^jhg6YdYx#[cJZ-jnIB? Lrs`G=e:
2022-10-03 14:16:12 UTC	3582	IN	Data Raw: 30 7e 2c fe 20 f7 01 3a 98 8c d0 d4 c9 3b 99 24 53 c8 64 19 3e 65 36 38 cc c8 78 ad d9 04 32 77 24 c1 78 fb a9 6d 53 a2 8f ba 8a cd 5a b1 6a 7c 42 e5 31 25 48 e2 9d 4c 8a e2 33 47 a3 7f 73 9b f2 54 eb 85 80 7e a7 d7 8b 98 c2 60 ed 77 e6 19 b7 96 50 2d 4b f8 3f 30 02 c2 b8 e6 31 5b a2 de 78 96 f3 0c 33 8f f1 0b b9 c9 48 ed e6 d7 22 74 f4 d5 33 f1 1d db 6b 3d 3e e6 55 b8 14 36 4c 75 b2 bc a7 ea 50 e5 98 c0 d7 30 8c e2 58 1d ee 53 79 02 af 82 dd 4e 0f 0c 2e 7c 12 f3 3a f5 1b 53 33 7c 04 42 30 05 b6 df 51 e4 78 6d e1 ea 1d b2 c5 b1 d3 b0 19 ac 45 e0 80 66 3e a8 53 80 55 59 6f 94 a2 a9 bc e7 53 01 75 bc 78 8d ec db ea 02 e2 d5 2e ae aa 5a 0f 32 e8 dc bb 00 18 37 6e c5 d4 43 90 a7 46 2a 83 7b 5b ee 28 90 f1 f7 33 16 5c 70 c5 8f 52 80 05 05 47 02 6c f9 3e a1 0b Data Ascii: 0~, :;$Sd>e68x2w$xmSZj|B1%HL3GsT~`wP-K?01[x3H"t3k=>U6LuP0XSyN.|:S3|B0QxmEf>SUYoSux.Z27nC F*{[(3\pRGI>
2022-10-03 14:16:12 UTC	3598	IN	Data Raw: a6 3f 10 cd d1 d7 3c 25 ec b7 00 ac ea 08 b2 0d b5 69 8f 21 f4 58 35 ad 07 ca 98 c9 83 04 7c b6 15 3e f1 86 0b 43 2d e4 04 ab e5 7e f0 5c dc 9f ea 8b 0c 23 a8 f0 88 eb a2 ff 00 dc 93 02 56 ed 76 2b bc 57 4b d3 02 6f 4d fe 98 f1 50 48 6a 79 f7 fc 62 99 10 db 6e b8 08 18 26 47 9a cf b3 dc c1 0b 35 57 e4 ee 43 c6 69 cd c0 a8 c0 37 42 82 8a 1f e6 44 11 3a 6f de 6e 54 c7 df 5c 48 d6 cf 63 70 6a e5 40 3b d1 c0 5c 00 32 01 f4 83 a7 79 88 4c b9 86 bc e0 41 45 c1 db 34 4c 62 fc 81 42 83 91 89 d3 41 f2 ad fc 8e 04 da 8e df 96 05 c5 a8 24 f5 66 86 b2 cb 20 52 2c 55 d5 6b b8 09 76 1a 8b e4 d1 3b 70 01 6b 21 a1 69 bc 1a c2 7c b5 fb d3 42 fe ce 8c aa e6 40 56 ba c4 d9 b3 98 f4 5a 7c 24 f4 0f fb 8c 3d 11 e5 81 ec fa c4 87 77 69 68 a7 ac 60 68 ce a4 2d 53 08 ae 37 6f 37 Data Ascii: ?<%i!X5|>C-~\#Vv+WKoMPHjybn&G5WCi7BD:onT\Hcpj@;\2yLAE4LbBA$f R,Ukv;pk!i\|B@VZ\|$=wih`h-S7o7
2022-10-03 14:16:12 UTC	3614	IN	Data Raw: 9e 15 ab b4 60 12 e0 4d 4a 6b 12 b2 d1 c2 ca 66 62 4a 74 3e 8a a9 ac 5f 43 61 6a b4 f0 84 f7 7d c3 7b 18 3c 8e fa f0 c5 e5 0c ee 8b 5a ac 38 21 95 c1 55 e1 d5 6a 72 e2 eb a9 08 bb 23 a7 61 fd 30 44 a4 6c 89 eb 75 a5 1a 67 20 3f ae dc 6d c1 5e 86 0a 3a 1e 83 da 1e 38 d6 d6 33 e2 ce bb 8d 48 fd e4 f8 1f 97 dd ca 4d ac 94 df e7 c6 48 0a 0d ee b4 4f 82 99 4e 65 a0 06 5f cb 31 b2 8a 07 ab 6e 06 5d 40 84 86 f1 bd cf ce 0a 38 1a 14 4b 03 28 77 1c 5d 00 43 e6 17 2c cc b0 0d 67 7f 1b 5d 62 f6 a6 84 a4 a5 b8 77 1e 5d 33 f1 05 61 08 30 da d4 37 cc 75 4d b5 a0 63 bc 8a da 13 35 ef be 3e 99 40 18 15 57 11 7c 58 e4 92 31 50 6b ed f2 e6 f0 9b 0a 1e 59 d9 18 32 9c 50 88 a9 4f d7 86 11 00 08 c2 0d 93 65 ef c6 35 85 68 b0 99 a1 89 80 9b e6 ee 78 61 4f 44 c8 1a d2 d3 05 8d Data Ascii: `MJkfbJt>_Caj}{<Z8!Ujr#a0Dlug ?m^:83HMHONe_1n]@8K(w]C,g]bw]3a07uMc5>@W|X1PkY2POe5hxaOD
2022-10-03 14:16:12 UTC	3630	IN	Data Raw: 61 e7 85 15 10 9b 50 2f 0a 63 0e 18 82 31 d2 b2 ee 73 e7 25 95 de dc 5d a0 9c 35 bc 91 2c 8d b3 95 e9 51 f4 e4 84 49 87 3b 4d 30 71 59 1a 31 22 aa bc 9e b3 59 b2 53 35 58 06 25 42 a2 15 d9 67 87 86 34 89 9a 6c 59 b2 e8 d7 d6 14 ab 68 23 c3 35 ef e3 98 d0 65 0c 36 d5 54 05 0f 17 04 fa 39 57 0d bf 28 40 c5 10 89 18 cd 05 27 99 b9 dc 0e 74 42 50 ac 4a 15 c1 4b d1 2a 88 96 99 b7 49 15 05 5d 93 78 22 b5 5b 7c d0 43 d0 f8 c1 2f 58 9a 36 32 37 2c fb 5a 8d 5b 46 34 9d f5 62 ed 01 57 ec 70 85 21 34 3c 48 bd 07 93 3e 7c ad ba d3 ae 4e 83 ba 9f 58 bf b8 3d 5f 5f d1 ee 21 7b 5c 48 bb 09 ca 2e 48 b8 44 68 00 23 e6 d1 c9 fb 25 97 5f d6 c3 1c 47 c9 6d a8 18 4a 44 f7 85 24 0e 9f a3 e7 26 4b d0 b5 56 0f 8e 1f 79 27 9f 12 9b 97 c8 c7 95 10 02 dd c7 e3 78 20 18 37 7c ce 7b Data Ascii: aP/c1s%]5,QI;M0qY1"YS5X%Bg4lYh#5e6T9W(@'tBPJK*I]x"[|C/X627,Z[F4bWp!4<H>|NX=__!{\H.HDh#%_ GmJD$&KVy'x 7|{
2022-10-03 14:16:12 UTC	3646	IN	Data Raw: 51 d2 c4 46 fa dc dd 31 15 4a 4a 06 98 9e 31 a0 ab 60 d7 5f 70 31 26 aa 00 91 79 1f eb 84 b3 70 83 42 97 ed 70 68 a3 c2 e4 dd 82 62 46 6e b6 80 45 fc 0c 97 2d 00 e1 18 17 98 f1 81 14 50 b8 51 00 1d be 5d fd 99 ab 55 22 28 1f 5f 97 08 3d a1 7c 21 6e fc 70 2b 29 78 97 07 c7 16 89 8c 9e 4f b8 3e 44 c1 2b 28 ec 5f 92 c0 28 4e 9a 7b 0b c7 36 dd a5 e8 f8 b8 13 10 29 a8 f1 fa 71 33 8d 25 7a 5e fb 85 44 ab 5f 07 b2 62 25 10 53 c6 1c d7 75 da 87 70 7d 8d 20 e0 e9 36 62 41 99 44 47 ce 3d f9 b8 40 aa 1a f9 3f 79 2f a1 c5 ef fa d1 cf 80 88 60 4f 30 6a c2 7c f7 b5 69 83 07 74 5d 39 b1 40 f2 e3 94 bc 2a 6f 61 30 ce 43 3d a4 cf 02 70 dd 18 90 53 f9 93 0b 71 aa 22 9e 28 9f 8c 2e 03 4a c9 c7 26 09 f6 e1 99 2d 82 b4 ba e2 3b 6e 20 16 5b 5e 8a 20 03 58 7c e6 a0 33 5b 38 69 Data Ascii: QF1JJ1`_p1&ypBphbFnE-PQ]U"(_=|!np+)xO>D+(_(N{6)q3%z^D_b%Sup} 6bADG=@?y/`O0j|it]9@*oa0C=p Sq"(.J&-;n [^ X|3[8i

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3662	IN	Data Raw: ff 00 c7 ff 00 83 e9 7f d3 12 c8 38 3f c4 72 01 3d ff 00 ac 92 82 fb fb 73 98 e4 77 82 87 f4 c0 9e b4 16 6b ec b9 27 fa c4 b6 fc e1 27 31 98 87 51 67 bb 98 c5 53 a9 3f 79 10 0d cb 54 df e8 c5 2f 0b 7f 06 03 10 0a d3 e1 a7 0b 4a af 3b 35 c5 89 52 43 12 47 57 cc 04 fc ec 5a c2 1b 20 7b 29 ea b0 e0 db ef 7f b9 74 27 10 71 fe 36 1c 91 79 83 00 9a c0 35 8b a4 4e 43 d9 80 93 2f e3 66 99 c7 fb d8 c6 7f ab 41 c4 bf f8 63 0f 51 5f 78 0c 41 3c 5a c1 f2 92 2c 4a d4 31 78 22 1e 18 63 80 08 70 01 f6 e5 81 40 4e 13 5f 8c 66 42 10 bf e3 f4 bb ca bb a0 5f 90 6f 2a ca 21 38 b7 4d 4b 69 fb b9 44 46 e3 90 1e 0d c7 ef 37 79 5f 54 b4 fd 63 3a 91 00 95 ea 6d 26 39 60 17 01 86 2d 09 45 aa c8 f0 cf 90 28 ef ae b4 66 b5 7c 48 aa 28 fa 67 31 5d 74 87 47 9f 3b 81 8c 74 95 ab c3 02 Data Ascii: 8?r=swk"1QgS?yT/J;5RCGWZ {)t'q6y5NC/fAcQ_xA<Z,J1x"cp@N_fB_o*!8MKiDF7y_Tc:m&9`-E(f|H(g1]tG;t
2022-10-03 14:16:12 UTC	3678	IN	Data Raw: ba aa 8a 57 9f 32 c7 47 31 03 d1 fa 7c 60 5d 0f 0e 01 01 4d fd b8 2a 6c 6f 1f 35 23 90 ed 04 74 34 8e 57 78 53 37 77 d0 da 38 68 34 22 30 7f 23 58 be 41 04 1d ad ce 69 f6 e1 bd 48 ca 69 3c 34 b1 29 db 92 a2 fa da 63 87 6a c5 ae 0a fd e3 d4 31 ec 28 7e 24 71 eb fa db fa f3 1d 5c 74 a7 19 e8 e0 e6 0b 42 01 77 16 1f 24 13 34 a8 a3 5c df 98 23 4a 24 50 f3 41 0d e0 93 82 98 92 d5 03 f3 87 3a f5 21 1c d0 3d c4 59 08 02 fb b0 3b 92 b1 0b 1e bd 50 c2 22 31 7c 0e 2f 19 48 40 6d 40 fa 3c 66 3b 56 b3 dc fa ac 5e 8e c5 46 a4 bf 03 02 8e 61 5a 7c 03 ca 60 45 24 a6 e7 c9 8f 4f aa a1 a4 0d fc 60 d2 ed 1f 0e 8c b5 fb c2 5d a2 cf 56 3a 52 d8 a0 3f 74 93 16 8d 45 d5 07 de bb 93 ad 2d a0 f4 2a 16 4c ba 08 a1 df b2 cd b3 d5 4d 17 84 37 8f 0e 8d c9 df 71 25 34 3f f7 dc 24 19 Data Ascii: W2G1|`]M*lo5#t4WxS7w8h4"0#XAiHi<4)cj1(~$q\tBw$4\#J$PA:!=Y;P"1|/H@m@<f;V^FaZ|`E$O`]V:R?tE-*LM7q%4?$
2022-10-03 14:16:12 UTC	3694	IN	Data Raw: cf 03 8c fe 18 e4 62 0f 27 89 2a 04 47 72 d2 72 e2 7d a3 49 a4 49 38 f3 37 95 91 f9 64 a3 2b 18 d8 2c 9f 28 13 92 8a 77 7d ce d3 29 a3 c3 4c 31 2c d2 39 93 81 46 4e 37 e9 df 26 97 8a 01 9b 86 1f be 3b 8f 19 e1 cf c6 b6 50 c7 25 e4 19 9b 79 4b b0 83 85 bc 3e 58 e1 0a ae 25 43 e3 41 ab 99 51 f8 89 12 5a 37 3e 44 91 63 46 82 8a c4 a1 63 61 28 55 f1 c8 6d 19 83 01 b1 8d 42 c2 01 57 90 af ca ce 0e 44 69 d0 a5 75 f1 4e 51 9d cc 65 85 30 0e 55 97 97 3c 46 54 3f 31 27 f1 27 14 ea 91 b8 91 c4 07 e7 c7 8c e0 1c 67 5f 27 9a 40 78 f1 c0 41 75 9d cc 93 44 8d 33 1d 5a d8 04 34 15 70 c2 4a 86 14 48 61 0a 86 61 d8 77 9c ca f6 43 f0 9e 60 b4 62 17 30 57 67 57 25 1f 89 c9 5f 07 f1 cc 29 7c 6e 27 1e 24 df 91 35 38 6e 2c 34 91 22 b3 ca dc 99 11 95 49 5c 1c 49 8b a6 cc 72 58 Data Ascii: b'*Grr}II87d+,(w})L1,9FN7&;P%yK>X%CAQZ7>DcFca(UmBWDiuNQe0U<FT?1"g_'@xAuD3Z4pJ HaawC`b0WgW%_)|n'$58n,4"I|rX
2022-10-03 14:16:12 UTC	3710	IN	Data Raw: 71 25 40 6a fa 8e 1f e5 96 05 92 e4 45 45 00 ae ce ef ab 8d d8 80 a4 0d 48 2a 40 88 f2 59 14 8a 1c ce 3a 70 b8 88 53 94 58 90 39 28 a1 5f 46 87 82 92 f2 63 8d 94 da 7e 90 93 3d 21 55 89 f8 0c b3 68 00 d4 24 89 4c f1 d8 f0 a1 56 67 5c 87 88 c5 b6 77 72 04 f2 71 d8 28 01 91 39 4c 1c 17 4b 8d 8a 36 f2 13 59 0b cc c5 40 7b 1c e9 c1 69 22 57 05 a3 fd 55 78 ee bc 79 21 b2 dc ae 31 99 27 4e 33 03 3c b0 ce 4e 90 78 c4 1c 98 f4 48 e7 8a c2 04 9f 98 80 13 1c 63 c5 1c 87 6f 50 a2 bb 2b 24 2b b3 cf 3a 72 36 8b 53 8b 34 ce 5d 40 2a 63 97 c3 bb 14 2e 44 92 ce 43 3a 2a 8f 02 b4 a0 17 f8 cc 8c ac e0 1a 58 97 90 84 6c 93 53 18 8a 44 5e f2 68 23 f1 6c 85 46 24 60 14 8e 40 fa c7 0b 26 c5 3f 0e 67 19 8a 96 1a 1c 45 21 2f 70 4c 23 68 3e 41 70 42 e7 73 dd 78 5e 7e 91 4e c2 4e Data Ascii: q%@jEEH*@Y:pSX9(_Fc~=!Uh$LVg\wrq(9LK6Y@{i"WUxy!1'N3<NxHcoP+$+:r6S4]@*c.DC:*XlSD^h#lF$`@&?gE!/pL#h>ApBsx^~NN
2022-10-03 14:16:12 UTC	3726	IN	Data Raw: 4d 47 af 3a 96 a5 14 55 98 9e ff 00 7f bc 2c 06 1e d4 d6 43 0f 91 cb b6 52 eb 59 a0 ff 00 c3 c5 04 6e e4 bf cb 9e c6 35 8e 58 9c 95 dc f2 a4 0a c8 48 e4 4c ca d1 a1 86 98 b3 aa b5 fc 8a 24 9f 97 97 63 40 b2 a2 c5 d4 bd b2 2a 20 cd 16 34 60 df 98 57 88 dd 5a f1 ca c8 c7 41 ab 34 6c 15 77 23 54 92 18 55 50 30 18 ee 24 90 e9 ed 60 92 77 1f 3d 57 95 03 2b 80 f3 a1 5a 62 e5 d1 2b 08 10 49 4d 4c 57 8f 23 6c c2 a9 b9 29 13 23 c5 11 da 5e 5c fc 92 03 b5 2c 72 33 8d 3c 60 e4 28 b0 a7 fb 0c 48 8d 98 06 57 58 39 11 aa 06 c4 74 4f 81 3d f2 99 83 fc eb 57 e4 c2 57 fc 60 87 8a 74 e4 22 47 24 9f 36 fe 6c 4e c5 06 c2 19 d6 63 e2 78 0a 37 23 83 be ce 9d e7 1d 51 44 a1 ff 00 10 8a 01 a1 4a fc 52 54 10 30 a3 3b 04 41 6c 20 78 10 31 75 db 67 1c 8d 64 7c 8a 45 d5 e2 62 31 85 Data Ascii: MG:U,CRYn5XHL$c@* 4`WZA4lw#TUP0$`w=W+Zb+IMLW#l)#^\,r3<`(HWX9tO=WW`t"G$6lNcx7#QDJRT0;Al x1ugd|Eb1
2022-10-03 14:16:12 UTC	3742	IN	Data Raw: 47 d6 78 98 93 87 8d 7e db 3f 8b 18 fa ec 46 40 ac d0 e5 1a a3 84 5d 00 b9 2a 15 88 e4 23 fc 71 e4 ca 1f 93 02 b2 d8 1c 58 2f fe 2c 8e 0e 33 b3 8f 16 3f 1b 8e 8a 58 44 32 05 0b 0c 60 67 23 b9 b8 ca 7f 6e 30 06 4e 4b 7d f2 ff 00 e0 61 8a 29 50 64 3f ff 00 26 63 9c 83 50 3e 40 2a 08 86 4f dc fc 65 c7 e9 58 e7 08 54 19 cc ef c2 32 5f c5 b3 8c 14 c7 64 77 43 00 17 9d 03 d6 7b 3f 58 7d 64 79 78 30 8b 18 bd f7 9f fe 33 d9 cb c6 ec fe f7 96 32 ba bb cd b1 8f 58 c2 d1 b1 ac ad e0 62 3a cd 88 36 0e 29 2c c8 4f a7 6b f5 89 2f b0 05 e0 91 ec 28 f5 e9 6f 25 25 80 1e b3 51 f7 8c a0 82 05 e6 a0 2e 1b 2d d7 78 aa 83 b3 83 de 1a db 14 01 8e 18 b1 51 81 18 7d 67 63 a3 fb 55 8b c5 03 d8 cd ab eb 36 d9 a8 af 50 a9 0c 4f d1 c3 3c 6a c1 4f 46 41 b0 a1 e9 e2 3f 58 8a ce 6a ab Data Ascii: Gx~?F@]*#qX/,3?XD2`g#n0NK}a)Pd?&cP>@*OeXT2_dwC{?X}dyx032Xb:6),Ok/(o%%Q.-xQ}gcU6PO<jOFA?Xj
2022-10-03 14:16:12 UTC	3838	IN	Data Raw: 59 b5 fa 5a 62 47 ac dd 22 b6 ec e2 f2 61 65 2e 6c 67 96 c6 c8 09 06 72 09 24 1c 49 96 46 a1 ee 7e 64 91 1a 54 b6 88 4e 50 33 bf 6b 13 01 63 b0 e9 2b b2 69 2e aa dc 69 a4 7f 9b 92 21 55 8d 34 18 e2 fb 19 e8 76 b9 77 85 98 1e b0 bf f7 d9 3d 25 fd f6 ea 18 f5 93 33 21 d8 63 3b 4a 36 28 d5 12 ec 59 ca d6 34 a1 4d 2f 78 9c 97 88 f5 e9 39 42 41 44 d6 68 87 b1 ef e5 9d de 15 ac 03 1b fa c0 d4 73 6a f7 de 52 9f 5d 19 e0 2f db 0c 82 17 12 77 e8 44 83 00 00 74 b9 63 ff 00 58 cd d7 59 b5 fd 67 47 3d 77 88 ae fd d7 5c 88 1c 0d bd 84 76 47 b5 16 7f 55 9f 90 52 34 58 88 c8 e2 94 2b 92 84 88 78 dc 34 8d 27 0a 70 cc 8c 7e 2b 58 8c 9e 55 23 db 15 2d 79 12 30 62 d5 8c 2a 4b ee cb d1 a7 bc b0 45 83 84 e0 ec 65 d8 bc 42 3b bc e8 fd e1 0f f5 94 c0 d9 c0 a1 ff 00 1c 31 90 30 Data Ascii: YZbG"ae.lgr$IF~dTNP3kc+i.i!U4vw=%3!c;J6(Y4M/x9BADhsjR]/wDtcXYgG=w\vGUR4X+x4'p~+XU#-y0b*K EeB;10
2022-10-03 14:16:12 UTC	3854	IN	Data Raw: cc ab 78 98 10 f2 44 5f 62 6e 28 b1 4b 55 2f a1 b3 6b 03 c7 4d 91 b3 59 42 70 61 b6 ec 74 1b c8 fe 84 4e 8f 2a 64 56 b9 ec 48 fe da 21 63 dc 9d 38 d7 8d 16 90 31 3f cf a4 e6 62 33 dc fb 13 8e c7 ab f5 11 3e a4 b1 79 37 36 66 ed 6e 2e 22 4a 9d e6 1a 66 f4 27 1d 5e f2 2b b4 ea 75 53 23 d9 d8 8f 09 1b 45 3d 43 c7 e9 bb d4 c7 c3 b0 b2 96 5e 8e ff 00 51 ff 00 42 44 af c9 3c 64 cc 4a 6a 18 84 ad 3b b1 5e 24 da e6 cf 91 93 9b 18 27 3c 90 6d c8 96 e5 54 d8 58 7e e3 ae de 20 6b 62 6c b4 e0 cc c8 ee 9e 9e f6 d5 0f 4c 77 c6 a9 0d ea bb a0 cf a8 ff 00 65 30 47 7a ec 97 33 88 37 9c 8f 83 de 18 fe a3 ce c2 bc 9e 26 09 6d 2d e6 66 49 85 24 d9 3a da 5f 83 a1 fc 34 c6 46 93 69 e5 49 ca 70 8f b9 4a db 28 e8 51 d5 cb 1a b2 d8 e2 9d 8c fd 11 9c e0 78 85 24 c3 9f 85 b1 7f 6b Data Ascii: xD_bn(KU/kMYBpatN*dVH!c81?b3>y76fn."Jf'^+uS#E=C^QBD<dJj;^$'<mTX~ kblLwe0Gz37&m-fI$:_4FiI pJ(Qx$k
2022-10-03 14:16:12 UTC	3870	IN	Data Raw: 24 80 ac 3f 97 0d 9c a5 c3 e2 bb 02 7e 82 92 a4 0e 75 93 c7 64 c6 1d ab 8b a8 0e 8a 80 4f 1f 12 e7 04 3b 85 88 10 3d be 3b 04 e0 0c 59 70 54 a5 20 93 1b 62 7c e7 12 85 18 c9 99 b2 be 35 b4 40 67 f5 25 f0 ff 00 07 c6 ca 31 f3 37 64 e4 24 ef ac ed c5 16 ac 9c 4d c1 79 9a 13 16 45 f2 13 98 6d a2 71 db 8d a3 b0 06 cd 4b 7c 84 ea 80 5f e6 63 e0 0a b9 c7 51 73 2b bb e3 0b 19 55 87 b4 7c c9 e3 e4 a3 66 65 f3 db 97 11 ea 3c 5f 29 0e 62 96 5a 11 5d c1 45 aa 21 37 35 5b 82 c3 7f 82 75 31 83 41 8c 5d cf ba 88 40 6b 0d 32 a9 05 58 8b 87 10 74 66 fd 63 82 1b 70 45 34 38 76 38 5e c3 40 59 d4 81 40 e7 52 7b dc c9 8d 95 a8 f5 6c 36 4e 94 a8 3f cc 4c 43 2f be 31 51 c3 10 14 a4 45 e0 d6 63 6d a7 72 d8 8d 74 01 63 b1 50 71 1a 11 19 03 f7 63 23 0c 8d d8 11 97 e3 25 5f 64 9a Data Ascii: $?~udO;=;YpT b\|5@g%17d$MyEmqK|_cQs+U|fe<_)bZ]E!75[u1A]@k2XtfcpE48v8^@Y@R{l6N?LC/1QEcmrtc Pqc#%_d

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3886	IN	Data Raw: 76 14 1a a9 dc 97 0f c0 d1 b0 de a6 86 44 a2 a4 dc 18 b1 f1 15 0a 10 95 5a 6e b5 31 aa 22 d1 26 38 c6 86 d5 e8 a3 29 4a 5b b0 d7 c4 2f 65 ce c5 dc 5e 45 ac 91 4f ed 97 8a 18 88 18 b8 76 a3 8f 1a 63 62 c1 6e 64 cb 6e 35 53 91 de a2 f0 2a 2e cc 3c 80 e5 ba ca e1 95 38 20 00 97 cc b7 54 31 9a 83 30 3b 75 89 98 f1 63 a0 17 32 1d 9e d9 91 97 d7 64 2b 13 4a 0c f1 ec 59 7d 0c a5 48 ba a8 9f 11 73 c8 13 18 00 c6 8d 04 52 14 cc 6a fc ba d2 3b 16 2a 16 3f 12 34 de d6 0f d4 0b 5b fa cb 5c 4d 45 fd 0f f2 b6 16 8c a3 ce c0 84 33 b0 0b 73 3d ae 30 03 6f 17 57 f7 fe 62 a9 7c 9e ed a5 c3 85 5b 95 9a 20 df a1 04 b6 12 31 92 7b c0 3d 89 33 e8 54 c9 7c 66 15 0e d6 65 d0 96 a4 31 8d 7b b8 10 1d c5 14 61 60 65 df 73 fe a2 a3 13 40 c7 2e 82 aa 37 23 b3 03 b0 3d 4c 79 6c fb 45 Data Ascii: vDZn1"&8)J[/e^EOvcbndn5S*.<8 T10;uc2d+JY}HsRj;*?4[\ME3s=0oWb|[1{=3T|fe1{a`es@.7#=LyIE
2022-10-03 14:16:12 UTC	3902	IN	Data Raw: 32 50 22 c4 2c c4 05 27 66 c0 e2 77 08 20 c6 52 14 90 27 16 fe 25 42 20 16 67 1f f3 0d 85 81 58 6c c0 2e 50 a8 05 0b 9d 4b a3 1c df dc 02 cc e8 c0 3e e2 ff 00 33 b1 1f b8 1a 85 47 e2 cb 6a 36 03 00 1a a2 b5 fd 4e 54 b5 c7 6a 68 cd 77 0d cb e2 36 37 90 e4 6e 16 b4 19 6e 87 41 f4 07 f1 a9 40 88 58 81 eb 19 de f6 61 2f 36 37 70 39 1d c1 ec 74 20 54 43 47 bb 03 ee 31 b6 52 04 66 fa 12 89 1b 8d a1 3e ae 5d 42 20 a3 d8 99 4a d6 86 ce 36 00 31 eb 85 8e e7 00 04 65 d6 a5 50 a8 2e 7b 90 38 1b 9c 9d 80 62 25 93 94 6a a6 30 a0 55 d4 72 1c 05 05 04 38 38 21 f6 06 70 75 5e 40 5c f1 f1 ae 4b 2e d5 33 70 42 46 27 0d 30 0c 25 79 3b d1 76 c7 ed 46 06 5b 5a dc 2d 5d 45 76 af b9 4f c4 30 16 42 60 66 47 3e a7 2a a7 22 55 ee 37 53 7c c5 c3 fd d3 b6 52 7b e7 90 be c4 ff 00 73 Data Ascii: 2P",'fw R'%B gXl.PK>3Gj6NTjhw67nnA@Xa/67p9t TCG1Rf>]B J61eP.{8b%j0Ur88!pu^@\K.3pBF'0%y;vF[Z-]EvO0B`fG>*"U7S|R{s
2022-10-03 14:16:12 UTC	3918	IN	Data Raw: de 04 2d cb 3a 27 34 75 54 7c 2a b3 a4 ba d9 6e 26 89 a2 1e a6 c2 d0 e0 7a 41 fe 97 64 e8 c7 47 73 e4 5b 2a 23 61 d8 54 42 a6 e7 17 63 cd 8e c9 1a cb 20 76 48 8d 6e 2f 91 2c ba ef 98 92 cb fd 8d ea fe 0d d1 ca 16 90 35 39 b3 6d c7 44 4b c9 6c 67 7c b3 12 37 a5 87 ad 15 9d 5d 27 32 72 67 56 b9 0e 9b 21 7d e0 5d 64 64 3d d5 84 71 45 7c 76 15 11 b9 78 a2 16 87 03 d0 58 2c 2b ba 6a a8 96 aa ab 4c 87 67 4b 8c 56 f0 6a c5 6c 08 dd 53 61 51 6f 45 3e e2 dc f1 3a 0c b9 e0 7a 24 49 a5 56 b9 9b 08 d4 6f 27 c1 ab b8 ee f2 26 3d 8d cf b2 da 1b 88 74 59 34 ef 47 fa 38 d8 45 f2 d0 55 79 1c 60 7b 0b e4 5d 13 0a f8 11 79 13 54 b4 da 8c e9 d5 f3 4d ec 59 cc a1 d8 6a f7 8a 2a 2d ab 7c 2b 0c 5f 91 fd e1 de 8a 8c 67 24 7b 1c 2b d1 ba 72 5a ad 1b 1b f1 47 96 59 16 a6 f4 b2 4c Data Ascii: -:'4uT|*n&zAdGs[*#aTBc vHn/,59mDKlg|7]'2rgV!}]dd=qE|vxX,+jLgKVjlSaQoE>:z$IVo'&=tY4G8EUy`{]yTMYj*-\|+_g${+rZGYL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.6	49882	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3295	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_02_w.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:11 UTC	3332	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "8dc-5b252e7c40940" Accept-Ranges: bytes Content-Length: 2268 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:11 UTC	3332	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 36 2e 32 32 20 35 37 2e 36 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 39 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 32 2e 32 36 2c 31 32 2e 35 32 61 36 2e 32 36 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 66.22 57.64"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 9</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M32.26,12.52a6.26

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.6	49885	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3296	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_02.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:11 UTC	3334	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "8df-5b252e7c40940" Accept-Ranges: bytes Content-Length: 2271 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:11 UTC	3335	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 36 2e 32 32 20 35 37 2e 36 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 61 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 38 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 32 2e 32 36 2c 31 32 2e 35 32 61 36 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 66.22 57.64"><defs><style>.cls-1{fill:#01589a;}</style></defs><title> 8</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M32.26,12.52a6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.6	49883	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3297	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_03.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:11 UTC	3334	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "2773e-5b252e7c40940" Accept-Ranges: bytes Content-Length: 161598 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:12 UTC	3388	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 6d 57 02 b8 07 00 0a a0 00 00 38 55 14 07 28 0a ae 01 c0 02 a8 00 00 aa 08 03 80 15 40 1c 00 00 00 00 00 0a 80 73 f5 55 c0 0a Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmt"mW8U(@sU

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3404	IN	Data Raw: b1 f3 35 6c ea 93 84 48 73 44 8c c7 b4 37 73 6f bb c1 f5 0c 11 b6 eb b5 5d 65 d6 94 07 26 d9 dd b6 59 6e f3 dd bc 9d 1e 24 67 47 6f cd 74 fb 38 a3 28 cb 3d 15 41 40 cc bd e5 71 c5 b2 1e 3f d0 75 f2 f2 31 ce ed 57 d9 6d ae 86 46 8c f9 f5 66 e8 ae 27 aa 84 6e c9 5e 5d 9c 98 4f 55 f7 d3 8e 85 b3 15 70 33 2f 7d 55 9c eb e9 f2 de 83 af 43 cf c1 bf 4d d6 5b 74 b3 c8 bb 17 0b 77 7b 83 bf 2d 32 b7 4d b7 e2 be d3 95 96 3b a8 aa ca 23 d3 e7 52 19 63 ec 76 e8 e2 ea cf e5 bb 9d e8 ac 7c 3e ff 00 36 56 dd 7c b3 48 9e 4e 24 bd 37 3a c7 2e 27 6e ec b7 65 d1 66 9b 6b cd 9b 36 0d 3b 23 4e 38 41 e5 8d ba ba 9a 35 51 e5 bd 07 a3 cb 8a 8e 67 ae cf 46 1b b4 14 48 ca e3 93 a9 0b ab 87 0b d1 0f 25 b2 b9 10 b7 26 d2 8a f2 f3 e3 18 bc f0 6d dd d0 d3 c2 ef fa 2c f9 31 73 bd 64 57 Data Ascii: 5lHsD7so]e&Yn$gGot8(=A@q?u1WmFf'n^]OUp3/}UCM[tw{-2M;#Rcv|>6V|HN$7:.'nefk6;#N8A5QgFH%&m,1 sdW
2022-10-03 14:16:12 UTC	3516	IN	Data Raw: d9 22 ec 4b c7 32 3a 34 27 63 93 fe 7e e6 7f a4 71 fd a7 c9 3f ea 73 fc d3 60 fe 24 59 1f bd 4c 1f c3 8f 24 fe 1c f9 c6 ff 00 3f 4f 63 63 a4 6e 40 38 ef 81 69 00 b5 dd d8 c4 9d a9 9f 8e 9a 0b 12 de e2 dc 41 66 9d e8 ad b1 88 ab d7 bb f2 3a 3a 32 2b 23 43 67 8e 00 57 8d ec d5 47 8a 78 c4 b0 c8 25 8f 9d e9 5a f7 59 ae 52 61 15 c9 a1 9e 0b 2f 14 f1 1a f7 78 ee 69 b4 b0 58 3d ab d1 d6 4c 3d 49 cf 4a 9a 21 79 1a de 80 73 28 06 c7 2b 62 62 d1 ae 91 78 98 25 16 a3 99 87 68 bd 20 48 a4 d6 73 ec 3e 1a ce 5f 82 3b 04 d7 b0 9b 51 66 7a 6e 91 de 7f 52 0b 31 55 9e 26 ad 77 d1 58 4c f3 d2 94 45 7a 5f 96 cd 28 6c c4 2b d8 8d c0 5b 13 c7 32 57 bc 57 d4 e7 e8 c3 34 50 97 53 ea 44 10 9d b4 20 b5 fe 1b 8b e4 d0 c5 6e 01 9c 9d 2e 43 84 bf 35 39 08 66 12 d5 93 e5 95 0c 6d 2f Data Ascii: "K2:4'c~q?s`YL?Occn@8iAf::2+#CgWGx%ZYRa/xiX=L=lJ!ys(+bbx%h Hs>_:QfznR1U&wXLEz_(l+[2WW4 PSD n.C59fm/
2022-10-03 14:16:12 UTC	3532	IN	Data Raw: bf 3c 8d dc d5 69 59 b9 fc 04 2b 1d 1e 36 a5 62 1b b4 4d 2d ee 62 a5 21 b9 a5 2c f7 79 3b 36 67 7f 40 18 c5 0e 98 b1 2a fa b6 08 89 2b c5 5a 92 fa 71 42 b1 e5 ee 7e 9d 73 d9 1e e6 90 59 e4 b9 6b 51 22 b3 32 f2 68 f1 f2 37 a3 7d 77 20 d2 43 83 fc d9 2f d3 63 1b fe a7 1b eb 93 07 86 8b 23 f6 ad 8f fc 39 32 32 03 f9 07 3a 21 5d 7a 3b 8a c2 d2 02 48 25 4d ae 2e 94 cf eb a2 1a d6 3a fe 5e 46 a7 4e 18 2e 34 76 63 e9 39 26 8f 87 e3 8c 6e 46 43 7d 1b 62 45 2a dc da 7a 93 c6 ca 41 ce 9b 52 bc 4a aa b7 9b 1c 5d 3b 83 b9 e0 54 7e ab e0 e7 ab 04 2c ce b2 45 d0 a0 c5 7e c1 39 04 e7 db 64 1e 4e 53 2f 60 fc 07 46 af 2b 5a 6b 55 27 48 ac 50 e7 fa 97 a6 2c 7c 34 e1 a4 83 88 ea ce 0b 98 29 14 53 35 5b 0c ce 92 a0 20 83 6a 84 52 48 25 84 bd 5b 26 e4 d5 75 fa c5 3b 55 4b a8 Data Ascii: <iY+6bM-b!,y;6g@*+ZqB~sYkQ"2h7}w C/c#922:!]z;H%M.:^FN.4vc9&nFC}bE*zARJ];T~,E~9dNS/`F+ZkU 'HP,|4)S5[jRH%[&u;UK
2022-10-03 14:16:12 UTC	3548	IN	Data Raw: 87 db 09 1d c7 17 f0 c1 9f e7 38 3e 91 8f 9f 89 c4 f7 4c 1e cb 8d ef 26 7e 39 fe 7d e0 fa 62 c2 46 9f 3c 80 e3 59 bd c8 3c e2 ff 00 97 34 7b 46 1f 66 c7 ff 00 36 31 07 d4 f3 9d c3 67 c8 c0 47 74 7e 71 7d a1 c4 23 71 64 7e cb f2 9c ec 72 ab a8 db 0c 72 1e ed 44 d8 d1 4b f3 fd d1 c9 20 95 bd 42 13 1e 19 07 ad e0 61 42 de a0 25 46 32 f7 99 3e f1 71 ca b7 ab b9 90 63 fa 5a 93 56 13 1f e1 8f 7e ec 0c 66 a7 dc fb 9c 9c f5 a9 7e 2e d8 d6 68 7c de 1c e1 b7 4c 16 d4 4c 70 5e ac 3c 0a f9 fa c6 30 7c 40 b9 fa c8 8f 68 93 3f 59 4a 06 82 45 83 92 b1 b5 3a 8f 0f 25 68 ff 00 99 46 1b d6 cf 8f 57 0d eb 47 fd 66 c3 72 c7 fd d7 c3 62 73 ef 2b 61 96 5f fb 8d 9d ef f8 b3 66 db ed f4 d8 e7 a4 d9 e9 1d 7b 1c 5a ed da 0f 9c 75 28 dd bb 18 96 66 88 ed 24 65 35 ba 8b 93 af ad 4c Data Ascii: 8>L&~9}bF<Y<4{Ff61gGt~q}#qd~rrDK BaB%F2>qcZV~f~.h|LLp^<0|@h?YJE:%hFWGfrbs+a_f{Zu(f$e5L
2022-10-03 14:16:12 UTC	3760	IN	Data Raw: 5b b9 b6 80 0d 3f 83 24 7e 47 78 c5 74 50 74 3c 52 ba e7 d4 13 4c 44 31 a5 54 86 26 13 46 f1 72 15 ae 41 3c 4b 2e da 3a 10 72 73 24 91 d2 89 5a 26 90 c3 f2 47 31 2b 14 75 ae 4d 12 f7 fa 69 3b 76 4b 2c 29 29 95 19 13 d3 67 54 db 3c 2c 17 50 ca ee 38 7b 0f 04 28 82 ca cf 0b 5f 45 6a a6 b4 60 4c f2 46 b6 bd 3b 8a 12 62 55 25 96 ec 8e b0 94 3c 7f 1d 2c d3 fc 23 b4 a8 c9 7c cc 5a 92 6f 98 e9 ce 4b d3 7b 5f 13 f1 31 cd c3 ac 48 2c 89 96 6a fc 8c 37 2c 1a b1 76 17 10 46 f5 27 90 4b 53 bc b8 8a 74 f5 3d 52 25 78 2b 34 09 2f ab eb c9 c7 f1 a2 dc be 93 5b 4a e6 a7 00 8f 2e a4 b5 f7 b3 9e 46 32 ed db b5 ab 27 23 ea 77 29 43 21 ad 4a 5a cf 66 f2 48 d6 63 e5 62 58 24 8c 44 d1 c1 31 e5 ab 2f ae cc 7b 69 7c 7f ac 2c 89 e3 73 ca d9 8a 6e 3b 8f 85 2c c9 dc 62 27 61 5b b7 Data Ascii: [?$~GxtPt<RLD1T&FrA<K.:rs$Z&G1+uMi;vK,))gT<,P8{(_Ej`LF;bU%<,#|ZoK{_1H,j7,vF'KSt=R%x+4/[J .F2'#w)C!JZfHcbX$D1/{i|,sn;,b'a[
2022-10-03 14:16:12 UTC	3776	IN	Data Raw: 82 e9 e3 34 78 a9 d3 15 33 28 b0 35 28 01 75 7e 2e 87 d9 84 0f 00 87 73 07 85 40 ce 3d 20 bd 13 a5 38 2a 18 26 41 1a 2b e3 56 f5 a9 54 19 06 5f e6 9f fc bf 4a 5c 97 a4 8d cb 0d 9e 0b 9e 93 44 0f 1c 1e 34 d7 04 b1 98 3a 84 61 9e 57 06 5a c5 90 e2 53 e7 3f ce a3 f7 58 c2 e2 93 0e f4 3b 7f 67 ed 9f eb 13 c4 5b c3 0e 4d d2 0e d1 b5 6e 06 70 e1 07 ad c2 6e f0 ea 7d 2d d7 8f a0 da 6e cd 07 78 74 7d be 26 20 b0 a4 4d b0 81 c0 c1 ea e8 44 1a 3e e3 f7 1b 7e f0 e9 c6 53 4b d2 a4 e2 ef 56 76 ab 48 df 60 62 9b be 21 62 9c ed 3f 39 fe 5a 9d 3d e8 3c 2a 99 2a f5 81 7c e5 ac 6a 18 4f 7a a4 b8 9f 8a 1f a5 67 68 25 d6 60 13 b2 9d 9b 7d e5 da 76 a6 62 13 b4 5f a4 1d 25 85 5e 8c a2 d5 53 f9 d0 e7 f2 b4 7b 85 6e 2c 32 2a 78 30 3a ca 4d 8a 8d 54 36 7a 2d b9 58 c8 3b 1e 98 a3 Data Ascii: 4x3(5(u~.s@= 8*&A+VT_J\D4:aWZS?X;g[Mnpn}-nxt}& MD>~SKVvH`b!b?9Z=<**|jOzgh%`}vb_%^S{n,2*x 0:MT6z-X;
2022-10-03 14:16:12 UTC	3792	IN	Data Raw: 8b 25 f5 73 e3 37 ec 87 70 f9 a8 b4 c3 31 ce ce 94 b4 ec 68 fd 5e 76 8b 07 49 f0 b8 ee 1f 39 ea 93 9a 1f 75 b2 87 a1 93 71 09 06 c6 1e 92 c5 91 b7 0c aa 25 44 07 06 c9 72 73 59 50 5c 11 93 fd ef 14 66 ba 32 f9 88 da db 46 b7 19 c3 8f 55 b5 87 f7 58 8f 57 6e 3e ab 3b 0a bf 53 33 ea ac 18 11 b2 31 16 9f 8a 5f 88 2d d7 79 81 be 91 a9 ff 00 fe 49 9f e9 32 f0 e5 f3 ca 2b 25 15 ff 00 4a a9 87 a4 25 e5 e0 8d ab 01 9c 2e ac 4c bb cc 7a f5 0d 49 12 d9 70 10 66 58 69 30 83 6e a3 98 22 0a 4c 0e 13 9d ce 99 41 43 7c 8e b1 08 0c 3e f1 85 f3 9a 90 20 d2 72 ea e2 2c 0c e0 eb 71 06 ae b7 84 2d ae 22 74 a7 37 f3 0b 15 5f d0 bc be c6 d0 9b 59 89 30 d5 2a 96 e4 04 a9 4f 10 bf 22 65 fd 58 2a be 67 79 8e 76 f3 b6 12 eb 3b 15 9d 91 9d ff 00 bc ed a7 38 bd ad aa 54 5b 52 6b d4 Data Ascii: %s7p1h^vI9uq%DrsYP\f2FUXWn>;S31_-yI2+%J%.LzIpfXi0n"LAC|> r,q-"t7_Y0*O"eX*gyv;8T[Rk
2022-10-03 14:16:12 UTC	3808	IN	Data Raw: 8d 72 24 ca a6 cc db 60 b6 d1 2a 92 c2 fa ad f5 39 4e 93 76 46 6c b0 93 9e 5c 63 a1 55 e8 ea 2c 41 5f 58 9c e5 44 01 31 69 7e 0b 1b 26 0d a0 b6 77 10 2d c3 d3 97 fd 88 de c3 63 30 96 3c de fb 41 dd 56 3e 13 17 05 31 63 98 73 2c c2 99 55 ee 04 3a c5 b9 0c e6 c7 bd bc 0e e2 ed dd b3 65 df b4 a6 6f 59 ea 1d 78 01 2b 1c 35 15 ce 40 ae a0 1b 0d 6f 00 5e fb 64 58 08 c8 0a 81 eb 8d 84 09 85 1c 7a ed c2 36 c0 7e 62 5f c4 c2 06 19 da 2d 5b b5 48 46 65 b4 b8 95 19 45 97 c3 6b c7 c5 76 e0 08 b5 e5 2a c1 4b ec c3 29 50 14 a5 48 7e af 28 ca b4 c7 10 0b 1b 9f ce 52 0c 98 ce ea 49 b9 97 b0 23 52 0c 73 81 0f b0 e4 e4 0c 03 bc 36 37 80 dc 12 db 09 55 40 b0 dc a8 89 5b 13 02 3c 24 6a 04 6c 66 a9 7d cd cd ad 0a 78 81 f1 38 37 59 42 ea 78 b1 83 ba aa 75 37 36 94 90 f6 80 66 Data Ascii: r$`*9NvFl\cU,A_XD1i~&w-c0<AV>1cs,U:eoYx+5@o^dXz6~b_-[HFeEkv*K)PH~(RI#Rs67U@[<$jlf)x87YBxu76f
2022-10-03 14:16:12 UTC	3824	IN	Data Raw: f3 1e bc 0b 89 8f 3e a3 f7 91 f1 85 7b c6 84 2d b5 6d 8f 36 f2 46 86 89 24 bb 08 99 6e c9 2f a9 eb 38 5a ec 5d 0e e0 b4 17 90 fb 47 43 1e 5d 05 86 bc 6f 21 dc f0 42 cd 31 53 b8 ff 00 24 3b 96 e1 a0 b5 33 22 ea ce e4 78 f5 13 4e 2e 9b 25 6d bc 84 f2 89 ff 00 90 76 df 64 f3 5a 60 f2 e3 d7 06 86 bc c6 de 08 bb 34 e1 44 a9 b9 52 1b 4a 85 66 48 83 93 7d 09 56 6a 90 b4 db 46 3f 22 2d a7 05 77 9f 21 d3 a1 ad d3 42 39 9a 2e 3c 85 4f 93 43 6e 17 6a c8 dc ea 88 e4 3b 54 b5 e1 6b 85 e0 d8 ad 3d 07 4d 8e f8 18 ef c0 d3 81 70 a1 a6 2b 90 ff 00 dc 8b f9 58 bd 25 0b ff 00 02 ba 65 c2 1d 45 f9 92 aa b2 4d 5b 54 97 41 5d ed 63 21 7e a3 86 43 d7 a6 66 50 ea f2 2d c9 f4 59 0b 2e c9 2a 5a 1c 88 69 c0 f0 75 42 cb 17 c1 14 ec 6d 32 a4 65 2e 68 92 35 a1 f6 7f 45 a9 24 e5 c9 27 Data Ascii: >{-m6F$n/8Z]GC]o!B1S$;3"xN.%mvdZ`4DRJfH}VjF?"-w!B9.<OCnj;Tk=Mp+X%eEM[TA]c!~CfP-Y.*ZiuBm2 e.h5E$'

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.6	49884	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3298	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_03_w.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:11 UTC	3337	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:11 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "7a6-5b252e7c40940" Accept-Ranges: bytes Content-Length: 1958 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:11 UTC	3337	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 35 2e 39 37 20 35 35 2e 35 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 38 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 30 2e 34 2c 35 35 2e 35 34 48 36 2e 35 33 61 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 65.97 55.54"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 8</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M30.4,55.54H6.53a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.6	49886	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:11 UTC	3387	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_03.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:12 UTC	3758	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:12 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "7a9-5b252e7c40940" Accept-Ranges: bytes Content-Length: 1961 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:12 UTC	3758	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 35 2e 39 37 20 35 35 2e 35 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 61 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 38 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 30 2e 34 2c 35 35 2e 35 34 48 36 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 65.97 55.54"><defs><style>.cls-1{fill:#01589a;}</style></defs><title> 8</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M30.4,55.54H6.

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.6	49887	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3516	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_04.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:12 UTC	3927	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:12 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "d4da-5b252e7c40940" Accept-Ranges: bytes Content-Length: 54490 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:13 UTC	3933	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 f6 54 b6 c9 03 1b 06 c6 0c 6c 01 b1 80 30 18 c1 0c 00 00 00 04 00 00 08 04 02 01 08 00 04 20 00 04 21 67 a5 8d 8d 8d b6 31 92 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmt"Tl0 !g1
2022-10-03 14:16:13 UTC	3949	IN	Data Raw: 68 51 a1 c6 28 da 50 a1 42 af a8 50 e1 6a 7a 4f 95 a0 27 12 51 a2 26 3c 1a 3c 64 38 1c 6b 81 f0 f5 e3 88 d1 34 45 22 8a 32 28 7c 6b e0 73 ae 05 1a d0 ad 8f 83 f0 47 07 e2 7a b9 e0 d6 85 5d 33 dd 4c 52 a4 9d e4 81 5d 3f 32 c3 76 67 a8 29 c1 06 98 75 22 8d 0a 3c 0a c4 d5 a7 22 af e8 50 e1 6a 7a 4f 95 a1 57 15 25 1a 6a 9a 8f 06 8f 19 0e 07 c0 e0 1e 1a bc 59 1a 26 88 c0 b0 2d 01 43 86 a0 35 ad 00 78 ee 65 f6 89 1a 51 70 5d ee 61 9c 8f e4 7e 27 ab 8f 81 59 01 2d 76 f6 fb 4b 24 cf 73 04 8c d7 66 6a 82 9e 8d 10 c3 4c 34 40 a6 e0 1c 4d 5a d0 a1 42 af a8 50 e1 6a 7a 4f 95 a0 2e 04 9c 35 4d 47 83 44 d6 43 81 f0 28 72 28 d7 89 23 45 e9 16 d2 5b d2 d0 a3 46 e1 ef 06 40 4c 27 f7 89 cd c9 bb fd 7f a8 dd 35 cf bc b4 88 96 76 96 c3 e0 fc 1e 4f c4 f5 71 c8 e2 e8 35 ab 59 Data Ascii: hQ(PBPjzO'Q&<<d8k4E"2(|ksGz]3LR]?2vg)u"<"PjzOW%jY&-C5xeQp]a~'Y-vK$sfjL4@MZBPjzO.5MGDC(r(#E[F@L'5vOq5Y
2022-10-03 14:16:13 UTC	3967	IN	Data Raw: 36 7b 1b 4f d5 a5 4e e4 1c ac 2f 47 11 5b 46 a4 75 89 55 aa 6c a4 59 12 93 56 2a d2 dc 57 ab 2c f7 12 a2 8f 48 f5 9e 84 93 1b 65 38 d1 b3 65 29 e2 d2 44 a3 46 29 18 69 a9 3a 8c c3 df 61 e4 51 95 27 18 fb 46 2e 94 3d 24 53 31 ea 7b 6e 56 bf 32 7a 91 cd 92 8c d6 ab 36 14 e6 61 95 65 15 21 4a 37 5a 2e 77 91 36 17 43 27 d0 fe ad 3f 99 1e 16 8f cb 1f 23 24 64 6d 17 89 de b3 65 19 96 42 65 a4 5e 12 e8 78 c7 d4 ee 3f 63 c7 c7 a9 9a e9 eb fb 89 f4 36 e5 d5 f6 5e ab e8 6c be c3 43 1e 86 78 bc 57 ea cf cf b4 d0 d9 78 58 69 8c ee 99 df 7e e7 75 72 f8 a4 5e 76 36 57 62 f3 7e ae d4 19 2f 4b b9 90 95 28 a1 19 89 50 68 5a d7 65 a5 72 31 8e 6c 53 62 b9 61 32 cb 2d 19 3d 1a d2 d5 23 46 b2 90 e7 08 ab 8d 64 87 1a 72 d6 de 6b 63 62 a7 b8 c3 7d c6 2d 5b 7f fe cf b3 de 1a 29 Data Ascii: 6{ON/G[FuUlYV*W,He8e)DF)i:aQ'F.=$S1{nV2z6ae!J7Z.w6C'?#$dmeBe^x?c6^lCxWxXi~ur^v6Wb~/K(PhZ er1lSba2-=#Fdrkcb}-[)
2022-10-03 14:16:13 UTC	3983	IN	Data Raw: 41 5a 25 d9 3e 09 f0 74 dd b8 9c 10 ed a4 7e 25 c7 ec fc 7e cd 8d bb eb 77 fe c9 27 65 1d 3f ea 32 5f ac c6 d5 22 18 38 72 5b a1 74 50 97 06 27 46 d3 74 cf 42 48 71 6b 91 50 b9 34 b1 45 8a 2d 8a 06 82 0a a1 da 84 62 b2 9d 98 7b 44 7c f6 4b 82 67 4b e4 de b3 46 20 b3 66 33 92 8e c7 ad 8a 7a 93 7f c8 d5 7e 45 26 b7 52 16 24 ff 00 c8 f5 a5 1f 36 2e a1 fd 0b 1d 0b 1a 27 a9 16 29 44 b4 37 bb 2f 71 b3 a7 fd 46 4b f5 99 f4 61 a5 a4 82 db 92 56 24 8e ad 28 b5 42 5f 8a 21 f2 42 4a b3 57 94 7e 3d ed 26 68 42 54 3e c9 70 48 e9 76 6c d5 b1 65 89 98 9c 8b 24 58 d5 8e 09 f8 1e 06 1b 1f 4d 01 f4 bf 47 a1 21 e1 4a 23 52 fa 37 ca d9 aa 46 b9 0f 97 93 3a 7f 9b 24 ef 15 8b 94 43 e2 84 da 1b b9 0a 8e bf 98 88 87 cc d3 b2 34 e6 8f e3 da bb 18 fb 24 48 c1 91 a8 53 46 a4 6c 62 Data Ascii: AZ%>t~%~w'e?2_"8r[tP'FtBHqkP4E-b{D|KgKF f3z~E&R$6.')D7/qFKaV$(B_!BJW~=&hBT>pHvle$XMG!J#R 7F:$C4$HSFlb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49726	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:37 UTC	237	OUT	GET /wordpress/wp-content/themes/kawaken/js/scrolltopcontrol.js HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:38 UTC	238	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:38 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "e73-5b252e8011240" Accept-Ranges: bytes Content-Length: 3699 Connection: close Content-Type: text/javascript
2022-10-03 14:15:38 UTC	238	IN	Data Raw: 2f 2f 2a 2a 20 6a 51 75 65 72 79 20 53 63 72 6f 6c 6c 20 74 6f 20 54 6f 70 20 43 6f 6e 74 72 6f 6c 20 73 63 72 69 70 74 2d 20 28 63 29 20 44 79 6e 61 6d 69 63 20 44 72 69 76 65 20 44 48 54 4d 4c 20 63 6f 64 65 20 6c 69 62 72 61 72 79 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 64 79 6e 61 6d 69 63 64 72 69 76 65 2e 63 6f 6d 2e 0a 2f 2f 2a 2a 20 41 76 61 69 6c 61 62 6c 65 2f 20 75 73 61 67 65 20 74 65 72 6d 73 20 61 74 20 68 74 74 70 3a 2f 2f 77 77 77 2e 64 79 6e 61 6d 69 63 64 72 69 76 65 2e 63 6f 6d 20 28 4d 61 72 63 68 20 33 30 74 68 2c 20 30 39 27 29 0a 2f 2f 2a 2a 20 76 31 2e 31 20 28 41 70 72 69 6c 20 37 74 68 2c 20 30 39 27 29 3a 0a 2f 2f 2a 2a 20 31 29 20 41 64 64 73 20 61 62 69 6c 69 74 79 20 74 6f 20 73 63 72 6f 6c 6c 20 74 6f 20 61 6e 20 61 62 73 6f Data Ascii: //** jQuery Scroll to Top Control script- (c) Dynamic Drive DHTML code library: http://www.dynamicdrive.com. //** Available/ usage terms at http://www.dynamicdrive.com (March 30th, 09')//** v1.1 (April 7th, 09'):// ** 1) Adds ability to scroll to an abso

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.6	49888	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3564	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_04_w.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:12 UTC	3927	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:12 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "925-5b252e7c40940" Accept-Ranges: bytes Content-Length: 2341 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:12 UTC	3928	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 37 32 2e 39 33 20 35 36 2e 38 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 38 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 37 31 2e 39 33 2c 33 30 2e 36 35 48 33 35 2e 33 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 72.93 56.84"><defs><style>.cls-1{fill:#fff;}</style></defs><title> 8</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M71.93,30.65H35.3

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.6	49889	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:12 UTC	3565	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_business_04.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:13 UTC	3930	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:12 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "928-5b252e7c40940" Accept-Ranges: bytes Content-Length: 2344 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:13 UTC	3930	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 37 32 2e 39 33 20 35 36 2e 38 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 61 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 38 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 37 31 2e 39 33 2c 33 30 2e 36 35 48 33 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 72.93 56.84"><defs><style>.cls-1{fill:#01589a;}</style></defs><title> 8</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M71.93,30.65H3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.6	49896	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3932	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "621a-5b252e7d34b80"
2022-10-03 14:16:13 UTC	3990	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:13 GMT Server: Apache Connection: close ETag: "621a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.6	49897	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3933	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_img_sp.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:13 UTC	3990	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:13 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "16c87-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 93319 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:14 UTC	3992	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 02 8a 02 ee 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 f4 10 01 50 14 41 40 00 10 00 00 11 40 41 40 01 00 01 14 01 0 0 04 00 44 51 10 01 00 40 10 09 80 50 15 00 01 44 51 00 00 00 11 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm"PA@@A@DQ@PDQ
2022-10-03 14:16:14 UTC	4008	IN	Data Raw: 9d 32 95 e5 58 4b a8 36 85 71 55 96 54 31 16 fb 1a 0b df 88 3a 86 05 a5 dd 49 71 89 d4 9b 42 7e 9d 81 2e e9 e2 d7 49 ad 21 e9 86 32 0f 4a 67 da d9 3b 17 09 62 5c a5 58 f5 25 d4 b6 3a 4b c9 ce 7a 9b 57 6d 67 af 7b 7f 05 cc af bb 91 0d 69 10 7f ea 41 f8 3d dc c3 b0 10 58 44 47 2c 09 98 3f 3c 01 31 31 31 fc e5 c7 10 9c fb d4 91 90 50 f1 3b 62 0f 73 fe 9b d8 c3 5a c4 09 b9 87 88 ab b8 e7 8f 4a 5c e2 2d af f2 a3 3c ce 73 36 f8 9b 99 99 99 dc 20 89 9f a0 4c ce c1 9d 8f e7 b2 25 bf a4 67 89 1e 3e 0b ed ad ce 71 87 f8 fb 8d 6b 0a 3d fb 00 7b 9d c2 06 05 5d 3b db 42 ed d3 74 d5 6f 71 37 9a 8f 85 75 5d 6e 55 05 fb 3b 98 ec 88 bb 44 ef 58 aa e2 cb 0f 6a b0 d5 f4 d9 4c 8d 0e c3 b5 d4 5b a2 ca 9b 5a 81 36 91 65 9c da 95 94 2c bd f7 ad 5a 53 66 55 59 ed 2a 54 06 f0 4f Data Ascii: 2XK6qUT1:lqB~.I!2Jg;b\X%:KzWmg{iA=XDG,?<111P;bsZJ\-<s6 L%g>qk={];Btoq7u]nU;DXjL[Z6e,ZSfUY*TO
2022-10-03 14:16:14 UTC	4089	IN	Data Raw: 4e e9 a6 75 d7 11 6a f7 bd a2 a5 59 6b 43 a8 f4 c6 26 2b 8a ca fe d0 76 1c bd 13 8b 62 11 16 4a 0e 4d 93 82 2b 75 72 e4 4a 09 70 41 c5 db f7 80 1e 97 78 cc 5b a8 68 be 5d f9 8b c3 55 0c be d6 46 a9 8e 3f 6a 58 32 a2 80 bf 30 7b 07 57 ed 00 a9 ca 6d a8 86 61 c0 15 9e b0 cb fa 58 07 d9 9e 93 72 3e d0 aa f2 e0 fc 4b 43 52 73 1c 77 c9 16 19 5d 27 10 46 cb fc ca dd 8a ee c0 d1 ba f1 04 55 eb 63 ed 2a b1 e9 cb 28 a0 b6 7a ff 00 52 ca 7a e9 0a d1 eb 68 06 50 bb 6d fb 83 b4 49 4c 62 39 f4 2d 92 0d 75 33 3f 10 8a f7 dc 37 71 d0 fd ce 04 f6 db 1d 71 6b 7f cb 94 ac ad ec 59 6c 94 bf 0b e3 31 c5 8a 31 46 e2 70 be 20 55 e6 61 b0 1b f5 78 97 44 d6 02 5a de d3 08 1a 50 5e 9d aa 0c 69 be f4 fa 4b 21 4c af 93 e6 e2 72 5f 12 fc 42 8d d9 df 13 d5 be ed cc d7 5b 85 b0 79 aa Data Ascii: NujYkC&+vbJM+urJpAx[h]UF?jX20{WmaXr>KCRsw]'FUc*(zRzhPmILb9-u3?7qqkYl11Fp UaxDZP^iK!Lr_B[y
2022-10-03 14:16:14 UTC	4105	IN	Data Raw: 00 01 3f 10 ff 00 55 9f ee b3 6f fe ac ff 00 7d 9f ef b3 fd f6 7f ba cf f7 d9 fe eb 3f dd 67 fa ec 3f fd d6 7f be cf f7 59 fe fb 3f dd 67 fa ec ff 00 7d 9f eb b3 fd d6 7f be cf f7 5c ff 00 7d 9f ef b3 fd f6 7f be cf f7 d9 fe eb 3f df 67 fa 6c 3f fd f6 7f be cf f7 58 7f fb ac ff 00 75 9f ee b3 fd f6 7f ae cf f7 d9 fe eb 3f df 67 fb ec ff 00 75 9f ef b3 fd d6 7f be cf f7 59 fe eb 3f df 67 fb ac ff 00 75 9f ee b3 fd d6 7f be cf f7 59 fe eb 3f dd 67 fb ac ff 00 5d 9f ef b3 fd d6 7f ba cf f7 d9 fe eb 3f df 67 fb ac ff 00 75 9f ee b3 fd f6 7f be cf f7 59 fe eb 3f dd 63 ff 00 ea b3 fd d6 3f fe fb 39 ff 00 ea cf f6 59 fe eb 3f dd 67 fb 2c 7f fd 96 3f fe cb 3f d9 67 fb 2c ff 00 7d 9f ec b3 fd d6 7f a2 cf f4 59 fe eb 3f d9 67 fb 2c ff 00 45 91 c9 93 26 4c 99 32 7c Data Ascii: ?Uo}?g?Y?g}\}?gl?Xu?guY?guY?g]?guY?c?9Y?g,??g,}Y?g,E&L2|
2022-10-03 14:16:14 UTC	4121	IN	Data Raw: bc 81 07 16 82 b8 93 08 36 3b 99 c9 70 54 ce ea 80 12 68 e2 4d 64 f5 02 51 89 da 82 0c 27 38 24 65 85 50 f1 c1 96 d7 a2 8a a3 a6 9a 1c 2b cb 04 f5 ed a0 61 e1 7a b9 0e 9a 55 c7 4b 80 65 38 6f 26 54 62 a1 9e 00 b8 16 c3 1b d1 6c 56 cc bf 89 d1 46 eb 5b 93 07 dc 0d c6 1e 12 c3 23 6c ca ea e0 07 0c 19 05 49 aa 38 4c 37 8a 28 da 92 a8 a6 5d 8b 04 0e 48 07 07 1b c6 c7 80 55 41 70 31 84 c9 9f fe 89 c3 9b f6 c4 ad ea f0 3c 05 39 c7 a9 6e 91 bc 08 cd 27 a2 84 c0 f3 d2 9a 07 43 a2 bb e5 c6 23 d9 b5 ca 91 8e 6e 23 80 03 83 4d 46 ae 6e 24 e6 cb cc 8b 97 c4 d9 01 f2 d4 03 00 14 e1 93 5 e 65 79 c6 6b 49 a5 17 12 b3 ef 39 4a a5 1a dc 26 a8 e1 d3 3f 4e dd e5 76 22 a9 aa e0 53 8c 01 27 04 7f e0 73 9d ec 9a b6 2e 81 c2 45 99 c1 82 5d 15 31 8c 86 44 0b 4d 8d 84 4f 66 2b 18 Data Ascii: 6;pThMdQ'8$eP+azUKe8o&TblVF[#II8L7(]HUAp1<9n'C#n#MFn$^eykl9J&?Nv"S's.E]1DMOf+
2022-10-03 14:16:14 UTC	4266	IN	Data Raw: 92 08 1c 85 24 0c a6 08 ec 43 86 69 22 95 d1 e3 fc 8b 16 bc 66 73 90 04 59 36 a7 c0 f0 28 20 ce 4c 8b 91 a4 b9 36 44 a6 16 92 5d 83 32 bc 49 b3 3f e8 55 59 44 91 c8 ed 45 46 31 57 e8 15 c3 03 80 51 d8 8c 54 68 42 46 5e 65 01 40 50 24 f5 fd 10 ce db 7d ac ad bc 0b b4 30 c6 89 a8 bf cf d7 c6 23 f9 cf a0 8a d0 36 b2 9b 58 c2 3a a1 2a f1 36 08 d5 83 be 24 69 33 28 93 d0 38 25 dc 02 58 e0 66 1f 06 73 20 0f 60 49 83 68 07 68 9c b9 31 49 7c 33 3c 9e 69 8a b9 3e 5f 4b 23 e1 ca 8d 4a 2b 95 89 ca 05 f2 79 28 30 d8 57 c5 0b 96 5b 06 12 56 f0 12 0b 02 85 e4 20 c6 98 5c 8e 5b 08 0f 72 b5 01 d8 91 f1 5a 05 93 13 0a 2a f2 a6 36 28 47 31 86 89 14 61 c2 d9 58 47 40 3a 16 12 06 6c 55 fc d2 e4 43 00 4c 8f 46 25 d9 50 c7 38 29 d3 ec 49 22 4c d2 41 34 d8 e1 71 b1 dd 09 68 33 Data Ascii: $Ci"fsY6(L6D]2l?UYDEF1WQThBF^e@P$}0#6X:*6$i3(8%Xfs `Ihh1I|3<i>_K#J+y(0W[V \[rZ*6(G1aXG@ :IUCLF%P8)I"LA4qh3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.6	49898	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3965	OUT	GET /wordpress/wp-content/themes/kawaken/images/ttl_about.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:13 UTC	3990	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:13 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "15f35-5b252e8011240" Accept-Ranges: bytes Content-Length: 89909 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:14 UTC	4024	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 34 38 2e 32 38 20 31 34 34 2e 33 36 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 64 32 64 32 64 32 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 32 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 31 2e 31 33 2c 31 32 33 2e 34 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 348.28 144.36"><defs><style>.cls-1{fill:#d2d2d2;}</style></defs><title> 2</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M31.13,123.4
2022-10-03 14:16:14 UTC	4040	IN	Data Raw: 34 2e 36 37 71 2e 32 37 2d 2e 32 31 2e 33 2d 2e 30 36 5a 6d 2e 33 36 2d 31 61 2e 33 35 2e 33 35 2c 30 2c 30 2c 30 2c 30 2c 2e 32 35 6c 2d 2e 31 38 2d 2e 31 32 2e 31 32 2d 2e 31 39 5a 6d 2e 32 38 2d 33 35 2e 33 32 63 2d 2e 33 32 2e 32 38 2d 2e 34 32 2e 34 36 2d 2e 32 39 2e 35 34 5a 6d 2e 31 34 2c 34 37 2e 39 2d 2e 32 38 2e 32 31 2e 30 36 2e 33 31 2e 33 36 2d 2e 32 33 5a 6d 2d 2e 31 35 2c 32 2e 34 31 2d 2e 31 31 2d 2e 35 33 61 31 2e 31 2c 31 2e 31 2c 30 2c 30 2c 30 2c 30 2c 2e 34 37 5a 6d 2e 30 37 2c 31 2e 31 61 2e 31 2e 31 2c 30 2c 30 2c 30 2c 30 2d 2e 31 35 6c 2d 2e 31 34 2e 31 31 5a 6d 30 2c 31 2e 31 32 63 2e 30 35 2c 30 2c 2e 30 37 2d 2e 30 35 2e 30 35 2d 2e 31 33 73 2d 2e 30 35 2d 2e 31 31 2d 2e 31 2d 2e 31 6c 2d 2e 30 38 2c 30 5a 6d 2e 30 35 2d 33 2e Data Ascii: 4.67q.27-.21.3-.06Zm.36-1a.35.35,0,0,0,0,.25l-.18-.12.12-.19Zm.28-35.32c-.32.28-.42.46-.29.54Zm.14,47.9-.28.21.06.31.36-.23Zm-.15,2.41-.11-.53a1.1,1.1,0,0,0,0,.47Zm.07,1.1a.1.1,0,0,0,0-.15l-.14.11Zm0,1.12c.05,0,.07-.05.05-.13s-.05-.11-.1-.1l-.08,0Zm.05-3.
2022-10-03 14:16:14 UTC	4137	IN	Data Raw: 5a 6d 2e 36 32 2d 33 33 2e 32 34 61 2e 35 37 2e 35 37 2c 30 2c 30 2c 30 2d 2e 35 2e 36 36 41 2e 36 34 2e 36 34 2c 30 2c 30 2c 30 2c 37 31 2e 37 35 2c 36 33 2e 30 36 5a 6d 31 2e 31 31 2c 33 32 2e 33 33 61 34 2e 34 31 2c 34 2e 34 31 2c 30 2c 30 2c 30 2c 31 2d 31 2e 35 37 2e 38 38 41 34 2c 34 2c 30 2c 30 2c 31 2c 37 33 2e 31 2c 39 35 2c 2e 32 38 2e 32 38 2c 30 2c 30 2c 30 2c 31 2c 37 32 2e 38 36 2c 39 35 2e 33 39 5a 6d 2d 31 2e 34 33 2c 31 31 2e 37 35 61 31 2e 34 34 2c 31 2e 34 34 2c 30 2c 30 2c 30 2c 31 2e 30 39 2d 2e 39 33 41 31 2e 31 2c 31 2e 31 2c 30 2c 30 2c 30 2c 37 31 2e 34 33 2c 31 30 37 2e 31 34 5a 4d 37 34 2e 35 37 2c 38 30 6c 2d 2e 30 39 2e 33 34 2d 32 2e 31 2c 31 2e 33 39 61 2e 32 2e 32 2c 30 2c 30 2c 31 2c 2e 31 38 2d 2e 32 38 41 34 2e 30 35 2c 34 2e 30 35 Data Ascii: Zm.62-33.24a.57.57,0,0,0-.5.66A.64.64,0,0,0,71.75,63.06Zm1.11,32.33a4.41,4.41,0,0,1-1.57.88A4,4,0,0,1,73.1,95,.28.28,0,0,1,72.86,95.39Zm-1.43,11.75a1.44,1.44,0,0,0,1.09-.93A1.1,1.1,0,0,0,71.43,107.14ZM74.57,80l-.09.34-2.1,1.39a.2.2,0,0,1,.18-.28A4.05,4.05
2022-10-03 14:16:14 UTC	4153	IN	Data Raw: 30 36 63 2d 2e 30 39 2e 30 38 2d 2e 30 37 2e 31 35 2e 30 35 2e 32 33 43 32 32 31 2e 37 38 2c 35 30 2e 38 31 2c 32 32 31 2e 38 2c 35 30 2e 37 35 2c 32 32 31 2e 38 35 2c 35 30 2e 37 34 5a 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 32 37 32 2e 35 32 2c 33 34 2e 32 6c 2e 30 35 2d 2e 31 37 63 30 2c 2e 31 2c 30 2c 2e 31 36 2d 2e 30 35 2e 31 37 2e 34 31 2d 2e 30 39 2e 36 32 2d 2e 30 38 2e 36 34 2c 30 61 31 2e 35 2c 31 2e 35 2c 30 2c 30 2c 30 2d 2e 34 37 2e 38 32 2e 34 34 2e 34 34 2c 30 2c 30 2c 31 2d 2e 30 39 2e 33 33 63 2d 2e 30 39 2e 30 38 2d 2e 31 33 2e 31 34 2d 2e 31 32 2e 31 39 2d 2e 31 38 2e 31 34 2d 2e 33 37 2e 31 2d 2e 35 38 2d 2e 31 32 6c 2d 2e 33 31 2e 30 36 61 31 2c 31 2c 30 2c 30 2c 31 2c 2e 34 33 2d 31 6c 2d 2e Data Ascii: 06c-.09.08-.07.15.05.23C221.78,50.81,221.8,50.75,221.85,50.74Z"/><path class="cls-1" d="M272.52,34.2l.05-.17c0,.1,0,.16-.05.17.41-.09.62-.08.64,0a1.5,1.5,0,0,0-.47.82.44.44,0,0,1-.09.33c-.09.08-.13.14-.12.19-.18.14-.37.1-.58-.12l-.31.06a1,1,0,0,1,.43-1l-.
2022-10-03 14:16:14 UTC	4169	IN	Data Raw: 2e 33 35 2e 33 32 2d 2e 33 38 2e 35 34 2d 2e 31 31 5a 6d 2e 34 39 2c 35 39 2d 2e 31 38 2d 2e 31 32 61 2e 32 31 2e 32 31 2c 30 2c 30 2c 31 2c 2e 31 34 2d 2e 31 31 5a 6d 2d 2e 30 38 2d 35 37 63 30 2c 2e 32 2e 31 33 2e 32 34 2e 32 36 2e 31 43 32 36 35 2c 31 38 2e 37 38 2c 32 36 34 2e 39 31 2c 31 38 2e 37 34 2c 32 36 34 2e 38 39 2c 31 38 2e 36 34 5a 6d 2e 32 35 2c 33 32 2e 38 32 63 2e 30 36 2e 33 31 2c 30 2c 2e 34 38 2d 2e 32 31 2e 35 33 43 32 36 34 2e 38 36 2c 35 31 2e 36 38 2c 32 36 34 2e 39 34 2c 35 31 2e 35 31 2c 32 36 35 2e 31 34 2c 35 31 2e 34 36 5a 4d 32 36 35 2e 30 39 2c 37 35 6c 2e 30 37 2e 33 2d 2e 32 33 2c 30 43 32 36 34 2e 38 38 2c 37 35 2e 31 39 2c 32 36 34 2e 39 34 2c 37 35 2e 30 37 2c 32 36 35 2e 30 39 2c 37 35 5a 6d 30 2d 35 37 2e 30 38 63 2e Data Ascii: .35.32-.38.54-.11Zm.49,59-.18-.12a.21.21,0,0,1,.14-.11Zm-.08-57c0,.2.13.24.26.1C265,18.78,264.91,18.74,264.89,18.64Zm.25,32.82c.06.31,0,.48-.21.53C264.86,51.68,264.94,51.51,265.14,51.46ZM265.09,75l.07.3-.23,0C264.88,75.19,264.94,75.07,265.09,75Zm0-57.08c.
2022-10-03 14:16:14 UTC	4277	IN	Data Raw: 32 2c 30 2c 30 2c 31 2c 30 2d 2e 31 36 63 30 2d 2e 30 39 2c 30 2d 2e 31 39 2e 31 36 2d 2e 33 6c 2d 2e 31 2d 2e 30 37 2e 31 31 2d 2e 30 39 2e 30 39 2c 30 63 2d 2e 30 35 2e 31 31 2d 2e 30 38 2e 33 33 2d 2e 31 33 2e 34 37 6c 30 2c 30 63 30 2d 2e 30 39 2c 30 2d 2e 32 2e 30 35 2d 2e 32 35 73 2e 31 35 2d 2e 30 36 2e 31 39 2c 30 6c 2d 2e 30 37 2d 2e 30 38 61 31 2e 31 35 2c 31 2e 31 35 2c 30 2c 30 2c 31 2c 2e 32 39 2d 2e 35 34 68 2d 2e 30 35 63 30 2d 2e 30 37 2c 30 2d 2e 31 34 2e 30 36 2d 2e 31 33 61 2e 37 39 2e 37 39 2c 30 2c 30 2c 31 2c 2e 33 36 2d 2e 34 6c 2d 2e 31 2d 2e 30 37 73 2e 32 2c 30 2c 2e 30 35 2d 2e 31 6c 30 2d 2e 31 73 30 2d 2e 31 2e 30 36 2d 2e 31 33 68 30 63 2e 30 39 2d 2e 31 2d 2e 31 2c 30 2c 30 2d 2e 31 34 73 2d 2e 31 32 2d 2e 31 2d 2e 30 37 2d Data Ascii: 2,0,0,1,0-.16c0-.09,0-.19.16-.3l-.1-.07.11-.09.09,0c-.05.11-.08.33-.13.47l0,0c0-.09,0-.2.05-.25s.15-.06.19,0l-.07-.08a1.15,1.15,0,0,1,.29-.54h-.05c0-.07,0-.14.06-.13a.79.79,0,0,1,.36-.4l-.1-.07s.2,0,.05-.1l0-.1s0-.1.06-.13h0c.09-.1-.1,0,0-.14s-.12-.1-.07-

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.6	49899	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3966	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_circle_arrow_blue.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:13 UTC	3991	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:13 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "202-5b252e7c40940" Accept-Ranges: bytes Content-Length: 514 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:13 UTC	3991	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 33 2e 33 33 20 32 33 2e 33 33 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 61 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 39 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 63 69 72 63 6c 65 20 63 6c 61 73 73 3d 22 63 6c 73 2d Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 23.33 23.33"><defs><style>.cls-1{fill:#01589a;}.cls-2{fill:#fff;}</style></defs><title> 9</title><g id="_2" data-name=" 2"><g id=""><circle class="cls-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.6	49900	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3966	OUT	GET /wordpress/wp-content/themes/kawaken/images/ttl_contents.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3991	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:13 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "c1ec-5b252e8011240" Accept-Ranges: bytes Content-Length: 49644 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:14 UTC	4057	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 32 37 2e 38 20 31 33 31 2e 35 39 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 64 32 64 32 64 32 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 33 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 32 37 2e 37 37 2c 31 31 39 6c 2d 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 327.8 131.59"><defs><style>.cls-1{fill:#d2d2d2;}</style></defs><title> 3</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M27.77,119l-.
2022-10-03 14:16:14 UTC	4073	IN	Data Raw: 2e 34 36 2d 2e 30 37 2c 30 61 32 2e 38 33 2c 32 2e 38 33 2c 30 2c 30 2c 31 2d 31 2e 33 35 2e 36 33 6c 2d 31 2e 31 2e 32 37 61 33 2e 31 37 2c 33 2e 31 37 2c 30 2c 30 2c 30 2d 31 2e 33 33 2e 35 31 6c 2d 2e 36 31 2e 31 32 2d 2e 39 35 2e 32 33 63 2d 2e 34 32 2e 31 32 2d 2e 37 34 2e 32 2d 2e 39 34 2e 32 34 61 32 2e 32 2c 32 2e 32 2c 30 2c 30 2c 30 2d 31 2c 2e 33 35 2c 31 2c 31 2c 30 2c 30 2c 31 2d 2e 34 34 2e 31 37 6c 2d 31 2e 38 33 2e 33 38 61 2e 36 32 2e 36 32 2c 30 2c 30 2c 30 2d 2e 34 33 2e 32 34 2c 32 2e 31 39 2c 32 2e 31 39 2c 30 2c 30 2c 31 2d 2e 39 33 2e 33 35 2c 33 2e 35 39 2c 33 2e 35 39 2c 30 2c 30 2c 30 2d 2e 38 36 2e 32 36 2c 31 2e 32 36 2c 30 2c 30 2c 30 2c 30 2d 2e 34 34 2e 31 37 2c 31 2e 35 37 2c 31 2e 35 37 2c 30 2c 30 2c 31 2d 2e 37 Data Ascii: .46-.07,0a2.83,2.83,0,0,1-1.35.63l-1.1.27a3.17,3.17,0,0,0-1.33.51l-.61.12-.95.23c-.42.12-.74.2-.94.24a2.2,2.2,0,0,0-1,.35,1,1,0,0,1-.44.17l-1.83.38a.62.62,0,0,0-.43.24,2.19,2.19,0,0,1-.93.35,3.59,3.59,0,0,0-.86.26,1.26,1.26,0,0,0-.44.17,1.57,1.57,0,0,1-.7
2022-10-03 14:16:14 UTC	4250	IN	Data Raw: 35 6c 2d 2e 32 31 2e 33 36 61 2e 37 35 2e 37 35 2c 30 2c 30 2c 30 2d 2e 30 39 2e 37 33 2e 33 32 2e 33 32 2c 30 2c 30 2c 30 2d 2e 32 37 2e 32 32 6c 2e 30 39 2e 30 36 43 32 36 31 2e 38 37 2c 33 35 2c 32 36 31 2e 39 31 2c 33 35 2c 32 36 31 2e 38 34 2c 33 34 2e 38 36 5a 6d 2d 31 34 2e 31 38 2c 35 63 2e 31 36 2c 30 2c 2e 32 33 2d 2e 30 37 2e 32 32 2d 2e 31 32 6c 2d 2e 31 31 2d 2e 31 34 2d 2e 33 38 2e 30 38 2d 2e 30 37 2e 30 39 61 2e 32 32 2e 32 32 2c 30 2c 30 2c 31 2d 2e 31 33 2e 31 31 2e 38 35 2e 38 35 2c 30 2c 30 2c 30 2c 2e 33 39 2c 30 5a 6d 31 2e 31 35 2d 2e 32 33 2e 38 34 2d 2e 31 38 61 2e 33 36 2e 33 36 2c 30 2c 30 2c 31 2c 2e 32 31 2d 2e 31 32 2e 33 36 2e 33 36 2c 30 2c 30 2c 31 2d 2e 32 31 2c 30 2c 2e 33 39 2e 33 39 2c 30 2c 30 2c 30 2d 2e 32 2c 30 6c Data Ascii: 5l-.21.36a.75.75,0,0,0-.09.73.32.32,0,0,0-.27.22l.09.06C261.87,35,261.91,35,261.84,34.86Zm-14.18,5c.16,0,.23-.07.22-.12l-.11-.14-.38.08-.07.09a.22.22,0,0,1-.13.11.85.85,0,0,0,.39,0Zm1.15-.23.84-.18a.36.36,0,0,1,.21-.12.36.36,0,0,1-.21,0,.39.39,0,0,0-.2,0l
2022-10-03 14:16:14 UTC	4266	IN	Data Raw: 31 37 63 2d 2e 31 2c 30 2d 2e 32 34 2e 31 32 2d 2e 33 33 2e 30 38 61 31 2c 31 2c 30 2c 30 2c 31 2d 2e 34 38 2e 35 68 30 6c 2d 2e 30 37 2e 30 38 2c 30 2c 30 63 30 2c 2e 31 36 2d 2e 32 35 2e 31 38 2d 2e 34 2e 32 32 68 30 61 31 34 2e 34 37 2c 31 34 2e 34 37 2c 30 2c 30 2c 31 2d 32 2e 30 35 2c 31 2e 34 33 63 2d 2e 34 34 2e 30 36 2d 2e 36 2e 35 34 2d 31 2e 31 33 2e 36 37 43 33 31 37 2e 33 32 2c 31 39 2e 38 35 2c 33 31 36 2e 36 32 2c 32 30 2e 34 36 2c 33 31 36 2e 35 38 2c 32 30 2e 35 36 5a 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 33 31 35 2e 35 36 2c 32 31 2e 34 38 68 30 43 33 31 35 2e 35 34 2c 32 31 2e 34 33 2c 33 31 35 2e 35 34 2c 32 31 2e 34 35 2c 33 31 35 2e 35 36 2c 32 31 2e 34 38 5a 22 2f 3e 3c 70 6f 6c 79 67 6f Data Ascii: 17c-.1,0-.24.12-.33.08a1,1,0,0,1-.48.5h0l-.07.08,0,0c0,.16-.25.18-.4.22h0a14.47,14.47,0,0,1-2.05,1.43c-.44.06-.66.54-1.13.67C317.32,19.85,316.62,20.46,316.58,20.56Z"/><path class="cls-1" d="M315.56,21.48h0C315.54,21.43,315.54,21.45,315.56,21.48Z"/><polygo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.6	49901	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3988	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_rekishi.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:14 UTC	4056	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:14 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "12782-5b252e8011240" Accept-Ranges: bytes Content-Length: 75650 Connection: close Content-Type: image/jpeg

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:14 UTC	4185	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 04 05 02 03 06 07 01 00 08 ff da 00 08 01 01 00 00 00 00 00 16 99 17 ee c6 a0 bf 4d 50 bd b8 d8 36 07 e8 26 bb 4c 2f c6 04 55 03 9d 3c cb 55 0c 8c 90 e5 13 59 c1 e6 9e 04 2a bd b0 6a Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"MP6&L/U<UY*j
2022-10-03 14:16:14 UTC	4201	IN	Data Raw: 91 52 73 b3 f2 35 2d ec 51 b7 51 fa 2a df a7 98 74 63 85 4d ad f4 4a 2b 0c 43 09 92 72 d0 95 04 78 25 3e 18 30 c1 4e 2e 93 74 57 1d c4 3e 15 39 45 7d dd 31 09 f5 18 af c7 34 57 28 6e ba 7c dd 50 6a bc 68 e1 15 3d 11 e6 2d 74 2b a6 c4 0c eb da 10 66 58 aa 12 c5 a9 ce 66 2d 9f 9f d0 84 3a 32 27 42 9f f2 2a 7d 0f ea 1a a4 c0 d9 60 30 50 31 a5 be 2c 89 cf 96 61 56 e1 06 95 55 2d 05 ce a4 74 a9 cc 2d 64 8c c0 25 6f d7 00 8b 0e 65 11 be 70 00 85 46 aa ba 03 9b 83 f9 e0 4c 79 9b d3 93 43 22 a0 c1 53 d7 32 c5 aa 56 9e a9 fa 9e 61 d5 1d 48 7a dc 77 4d 48 34 d8 cd c0 46 6b 54 2a 1f 1a d5 67 89 ff 00 cb e1 0e 63 0f 44 bc c0 c6 e0 7f ee 48 3f b6 ce 8d 25 31 c8 bd d9 1b 9f 92 9d 5f 66 f7 a7 95 d9 cc de 47 50 c4 7d 7a df 8f fb 75 df 50 f5 a6 6e 67 ab 2b 7c 5f ad 4c bf Data Ascii: Rs5-QQ*tcMJ+Crx%>0N.tW>9E}14W(n|Pjh=-t+fXf-:2'B*}`0P1,aVU-t-d%oepFLyC"S2VaHzwMH4FkT*gcDH?%1_fGP}zuPng+|_L
2022-10-03 14:16:14 UTC	4285	IN	Data Raw: 3f f2 b4 a6 8e 4f b0 b1 f0 f2 c8 15 9c 08 0f 4f 99 c4 d3 a7 b1 ce e7 94 1d f9 69 5e 77 79 44 5f e6 22 26 6f b2 f1 e7 d7 fb 0f 3d 99 55 01 5a ae e0 4d 4d 2a e3 2f ca 39 d4 21 69 a3 47 5b ae 60 d4 7d 37 15 5e 99 6d 0e ab 8e 1c e6 f6 d8 f9 5b cf 67 4e e9 3d 74 be bc e3 a0 07 7f 74 7d 7d 93 f3 68 21 00 0b e3 a1 c9 ea e2 70 ba a6 b1 5f 9a 7a 27 29 fd d7 5f e4 33 eb c5 d2 d7 9f 9e f3 34 bf c8 e7 d0 83 17 3e 3f 9e 7f 76 ef fa 3c cc 1f 3f d6 e6 0f ca 3b ad eb bb d9 2e cf 63 85 a8 a9 bb e2 db f2 54 26 33 3e 6f 36 60 ee 76 14 87 d3 2c df d2 a1 1f d6 e8 15 f0 29 01 93 33 03 d3 59 99 12 a8 dc c3 76 97 8a 69 67 9e ee f4 83 bd 7b a6 8d 07 74 91 9e 74 3d 9a 19 9b 79 ba 8b cf a4 a6 2b d6 64 7d 1d 1f 63 8d 6a 93 e2 86 a1 9c d7 42 11 d6 1f da b1 f2 43 5d 26 15 a9 8f a6 78 Data Ascii: ?OOi^wyD_"&o=UZMM*/9!iG[`}7^m[gN=tt}}h!p_z')_34>?v<?;.cT&3>o6`v,)3Yvig{tt=y+d}cjBC]&x
2022-10-03 14:16:14 UTC	4301	IN	Data Raw: b7 e4 34 6a 26 53 85 77 15 ee 79 b0 62 ba 30 26 7a c6 f0 9c 6f 76 26 4c 6f 3f 7b ab 95 87 9e 23 a9 c6 0b fb 43 8f 20 a2 0c fd c3 cc 39 0b f3 ec 23 17 3c 08 f9 d3 8d bc 5c 7d cf 75 33 32 f6 01 9f b8 de 91 2f 1f 3f 32 b1 12 0c 6c 41 6f 24 fd 4e 42 79 e4 08 8a f9 1b 65 89 8b 16 db a8 80 80 26 cc 7c d4 50 3a b8 b0 23 1a 33 c9 84 f3 0e 2c ab cc 51 b7 90 66 97 0a 0b a0 60 2f dc 65 da 25 29 e0 19 87 1e 3e 87 71 59 cf 26 70 6e 00 e2 63 da bc 46 cc af fd d9 91 5f e6 2e 34 82 06 ab 96 80 06 9b 9b 95 30 32 0a 58 db 3e aa 99 31 b8 2d 8c 98 0a 0a 06 0c 55 eb 32 d3 21 53 0e 4c 87 76 d1 2c 09 5e f3 7f c4 2a de d1 99 c7 02 1c 58 5b 99 e2 6e 09 8c a4 71 ec 66 f5 6f 7e a2 a3 ad 1a 84 df 12 d3 20 0c 63 0b e4 f4 66 fc b9 89 53 3d 11 b1 e4 1c 1e a1 62 d7 08 44 84 39 e0 c5 64 Data Ascii: 4j&Swyb0&zov&Lo?{#C 9#<\}u32/?2lAo$NBye&|P:#3,Qf`/e%)>qY&pncF_.402X>1-U2!SLv,^*X[nqfo~ c fS=bD9d
2022-10-03 14:16:14 UTC	4317	IN	Data Raw: 39 3e 91 1c 66 e1 80 31 f8 e2 e6 4c 8a 7e 98 cd 90 46 0a bc 08 e0 2d 28 30 b2 70 a6 2a 1e cc bc 9e f0 36 1e 4c fd 33 e1 1b 05 81 0e 65 ec 9e a1 39 0d 35 4c ec 58 dd 19 b0 bd b5 c5 ae 16 20 c7 97 88 2c 1b 22 1c ca 29 6e 6e cf 9b 69 f7 8f 8d 06 f3 1c 62 c6 00 13 19 2d 56 b0 96 72 4c 5c 6a f4 83 98 71 a1 a4 f9 8a 87 ea f7 94 4d 13 00 c2 58 93 17 16 37 65 11 77 ea 0c 57 19 6e a2 87 c5 c8 94 b8 84 74 2c 81 e6 a1 c1 b0 4b 54 64 cc 2d 59 a6 45 d3 6a 4a a3 93 5c c6 cf 9b 3f 95 9e 63 7c 58 8b 9d e2 60 c4 10 62 01 7b 83 1e bb 54 5f 35 f4 a4 41 a7 c5 a4 07 00 1c 1a 8e 18 13 85 54 da 4d 6f 8f 11 50 19 36 89 8b 0b 69 8d fc c7 ce 4b 51 be 26 a7 1e 52 c7 75 cc 08 ca b7 8c 42 43 2d a8 e8 47 5c 7a 7f 48 99 31 e9 57 63 54 3a 5c ea 4b 89 7b 49 73 37 ea 30 db cf 26 7c 7b 14 Data Ascii: 9>f1L~F-(0p*6L3e95LX ,")nnib-VrL\jqMX7ewWnt,KTd-YEjJ\?c|X`b{T_5ATMoP6iKQ&RuBC-G\zH1WcT:\K{Is70&|{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.6	49902	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:13 UTC	3989	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_hyosho.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:14 UTC	4057	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:14 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "18ab2-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 101042 Connection: close Content-Type: image/jpeg

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:14 UTC	4218	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1b 00 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 04 05 00 02 03 01 06 07 ff da 00 08 01 01 00 00 00 00 fa 56 52 49 27 64 92 4e c9 24 92 76 49 24 92 49 27 64 92 49 27 64 92 76 4e c9 24 9d 92 49 d9 24 92 49 24 9c ec 92 73 b2 49 24 93 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"VRI'dNvII'dI'dvNIIsI
2022-10-03 14:16:14 UTC	4234	IN	Data Raw: a3 31 02 cd 1c b4 1f 22 c7 01 ac b3 6e 90 5a 69 ab c4 6c 4c 37 be aa 82 38 b3 6c 8b 83 75 f8 00 ac 26 74 ec 57 da 23 cd 70 4e 2f 66 c8 58 94 75 ed 65 65 7a 11 7b 32 b0 3d 65 4e 3f 95 b0 00 66 7f 99 67 21 14 8c b1 0c 06 14 18 06 20 4c 93 14 63 a9 e4 40 4a cc af dc c0 26 38 1e a2 1e 84 03 bc c3 32 3f 80 d8 38 9e 53 66 60 52 70 61 3e 87 0f 5e 1e b2 6a 18 60 25 3a b6 c5 4b 1e a3 bb 85 63 38 b7 ed be 45 a4 05 c7 90 eb 96 dd 70 49 f2 0f a8 08 0d 15 89 db 3e 5c 2e 21 b7 0b 98 b7 da f8 02 c2 dd 4b 6c d9 fb 4c 1c b1 1a b2 83 12 bf 2f d9 4d 57 55 db c7 85 8c 96 17 38 55 54 00 2a a3 b7 64 33 1c a8 0a 49 39 ad 30 bd 3f 89 4e 59 5e b7 ce 29 b3 2b ef 7b ff 00 09 59 61 eb 1b 15 12 49 f6 99 6e b6 6d 54 c3 df 67 65 b3 d9 01 5d 3a 24 7a 80 55 5a 05 56 f5 9a a9 24 4d 53 ec Data Ascii: 1"nZilL78lu&tW#pN/fXueez{2=eN?fg! Lc@J&82?8Sf`Rpa>^j`%:Kc8EpI>\.!KlL/MWU8UT*d3l90?NY^)+{ YaInmTge]:$zUZV$MS
2022-10-03 14:16:14 UTC	4327	IN	Data Raw: 58 c8 46 60 fc 57 be a3 55 a6 bb 1b 95 b5 13 d5 89 8d 56 46 52 bb 6c af 35 4e 31 02 9a c0 20 6b 89 80 06 21 f6 c4 c0 04 c2 00 18 8a 08 02 2d d6 f7 b1 71 d0 86 df 15 de 18 35 c9 8a 9b 1c cc b0 04 ce 51 de d9 c4 40 6c 6d ef 6f e2 17 ad 01 25 b9 47 fa 6c 36 14 25 a8 a2 cb 3f e2 4f 81 e5 dc 17 cb 5f c7 7c 57 08 12 e7 e5 97 fe 3e 27 36 d3 60 1f 9f 3f 25 c6 a3 ae 1f 23 9b c9 e4 9c db 99 47 c7 f3 39 07 d3 f2 1f 1d c4 ff 00 bb 6f 98 35 0d 78 76 5b 6d cc 5e cc 4e 3f 03 93 c8 60 2a e3 7f 87 2b 4e f9 55 27 13 88 a0 55 cd f9 6e 25 2a c2 53 cb ba 8b 2c f1 96 7b 31 2b e2 93 fb 96 9a d6 75 31 ff 00 d0 63 fd 03 b8 99 3c 3e 34 ea 63 bc 4b 57 50 25 67 d3 31 5d 4b 4e 42 e8 a4 ca a8 63 77 92 30 0b 63 19 c9 f4 60 c2 b5 0d e7 22 bc b6 d0 f5 f6 87 0d 03 b2 fd 58 c7 10 a6 da e9 Data Ascii: XF`WUVFRl5N1 k!-q5Q@lmo%Gl6%?O_|W>'6`?%#G9o5xv[m^N?`*+NU'Un%*S,{1+u1c<>4cKWP%g 1]KNBcw0c`"X
2022-10-03 14:16:14 UTC	4343	IN	Data Raw: bd 97 f7 15 0d e1 90 52 a3 61 e0 b4 8f 9a 36 45 0a 84 f7 77 38 8d b8 38 33 63 89 ca ba 22 9b d3 bb 67 17 9e af a6 93 80 b8 5c 3f ae a3 f1 75 fe 26 bf a2 9b 2f 73 85 47 02 9e ca 6a f7 65 4e a7 d5 b9 d7 8f 4f 0a 9a 77 67 03 f8 fc 4f af 89 8f 62 b7 0b f2 af 0a fb 18 d1 4b e8 7f 65 4f dc 49 d5 f5 55 7f b1 4f 37 73 8a e3 a6 c5 8e 1b ad 9c 57 33 ff 00 09 1c 3a 78 54 f6 cf b9 4b e2 56 c7 35 7d 1b 2f 87 a1 bb ff 00 15 f9 9a 8d 56 be da 2b 49 b0 ee c4 3b 8a 7e 0c b2 53 1e c7 cc c5 31 8f 3d 2d 23 91 e6 c5 51 6f 09 17 f4 29 f1 22 6a de 05 3d 8c 66 0a 6f d0 e1 de 07 7e 9a 53 b9 e2 ea 36 8a 3d 4c 7d cf 15 ec 5b a1 83 dc c9 4f ae bb 8c 9d 22 3a b2 b9 ee 7c af 49 14 be b8 3f ff c4 00 28 10 01 00 03 00 00 02 02 02 03 01 00 00 03 00 03 01 00 00 01 00 11 21 31 41 51 61 71 81 10 Data Ascii: Ra6Ew883c"g\?u&/sGjeNOwgObKeOIUO7sW3:xTKV5}/V+I;~S1=-#Qo)"j=fo~S6=L}[O":|I?(!1AQaq
2022-10-03 14:16:14 UTC	4359	IN	Data Raw: 63 c0 3d 8e c9 52 c3 b9 cd c4 37 12 9d a8 ec 38 eb 7c 3c 54 6e 1d 73 72 e3 52 57 4e 5f 98 15 d1 d2 5b c4 ad c7 5f 22 03 5d b9 74 54 08 2a d0 6e f1 8f b6 cf 23 65 e6 49 41 b5 f9 0f 0f 86 52 68 a3 5c fc 1a 02 b4 bd 5a 75 d1 0d d1 f8 6e a1 f6 41 75 48 e5 60 3d dc 27 7d a0 c2 0f 06 da 0b d6 0e bb ce 2d d3 f1 0c 19 39 66 17 d6 ca 5d 32 97 c8 8c 2a 16 07 c7 72 db 0d 48 39 65 eb 18 25 f0 c0 c4 b7 36 c3 b9 63 40 03 4f 71 ad c0 e0 79 a8 e9 d2 65 a0 ea f4 b1 6d 32 38 63 88 5d de c0 63 42 c7 74 58 b7 86 80 5d 51 71 d0 d7 77 18 a9 12 9f 88 9b 2e f5 52 ad 4d 14 7b 25 79 6d 6e 8d d9 b7 c5 b4 4b 2c 3b 5c b7 32 22 3b ca 1e 27 26 85 1e 88 e0 58 2c 53 f8 55 47 73 04 b1 c9 70 49 08 05 54 b3 8a 5a b7 d7 11 9d be 18 fb 62 d9 0f 21 28 b8 dd 6f fe a5 bc 15 ea 08 4c 97 87 13 1f Data Ascii: c=R78|<TnsrRWN_[_"]tT*n#eIARh\ZunAuH`='}-9f]2*rH9e%6c@Oqyem28c]cBtX]Qqw.RM{%ymnK,;\2";'& X,SUGsplTZb!(oL
2022-10-03 14:16:15 UTC	4408	IN	Data Raw: 4d 85 dd 7e 09 7f 94 63 3f ac 8d 67 8b 13 e2 91 2a d5 6a 96 75 0d 33 a0 17 72 d8 8f a5 ea 95 90 8d ff 00 a5 17 f7 87 0b 82 6e c2 e9 82 2b 0d 09 f1 1b 38 21 c1 f6 57 2e 79 61 53 99 a8 b7 f2 a3 67 9f 83 ff 00 58 8f b6 c3 fe be 62 02 00 07 04 61 d8 88 f1 f8 d3 62 c2 d1 73 da 2f dc 6d bf 84 63 1e 32 27 b9 67 5f c1 86 c8 bc b8 b8 27 0a 60 2b 6b 10 e2 1f 8b 25 cb fc 2c fb fc 22 04 af c1 71 c0 46 1f 42 22 03 91 52 02 0f 64 52 6e a0 dd 55 c8 a2 1b 39 62 ba b4 d6 46 bb 0b 6c 83 7f 89 7d 32 c0 00 7a 74 91 14 94 e8 55 4a 03 29 fe 30 c3 42 f4 96 18 c2 62 2c ec 12 a3 40 75 a4 c0 25 df 99 51 ab 41 ce e3 0b cc 57 c4 aa 13 23 a8 a0 47 d3 28 6d 13 3e c8 ac aa 70 1c 32 b8 ab d8 d3 b1 89 52 cb 7a 89 cb 50 2e aa b0 ee 3b 6b b9 47 81 28 9d 25 1c 04 a7 ac ab ff 00 e9 89 b1 c4 Data Ascii: M~c?g*ju3rn+8!W.yaSgXbabs/mc2'g_`+k%,"qFB"RdRnU9bFl}2ztUJ)0Bb,@u%QAW#G(m>p2RzP.;kG(%
2022-10-03 14:16:15 UTC	4424	IN	Data Raw: a5 a6 df 91 d2 a8 b8 59 4c 93 8e ef 04 46 f0 ce 29 11 59 bc 09 2b a2 52 7c 60 6b 14 35 72 ec c7 54 ee 98 92 c7 06 c5 2c 2c 92 78 74 db 1e ec 92 e1 13 50 8b 71 69 19 13 c1 47 2c 6e 69 51 11 c6 eb fb 33 62 4c a4 5d 31 38 b3 04 2a da 4b dc bb 57 86 4b 62 49 25 81 2a 52 cb 3b b7 45 c5 b4 d6 07 74 66 ef 83 1c 8a dd ff 00 44 16 6c 69 47 aa f9 29 a6 9d 99 59 ab 1d 4e c5 b5 51 9c 15 29 8f 06 2e 8c 47 b6 45 19 5c 95 9b 95 98 67 dc e8 ea 52 f6 2e 2d 91 70 77 11 6d 96 3b 21 ee 9f bb 29 af ca 3a 25 5e 62 ff 00 27 fd 11 c9 e7 e9 91 50 66 57 bb 9f fe 04 a1 97 cf 82 78 68 e5 5f 0c 8e e5 5c 9c 0a 6b 24 ac dd 81 ee 46 c8 ed 48 a9 26 3c 33 70 9c 1d 1d 28 c5 21 6e ca 12 59 62 8c fd 89 41 79 8f 92 95 57 24 95 26 bb da 1e 6c 93 93 5c 11 ac f2 3d b1 43 9d 8d 78 74 e4 56 4a 2e Data Ascii: YLF)Y+R|`k5rT,,xtPqiG,niQ3bL]18*KWKbI%*R;EtfDliG)YNQ).GE\gR.-pwm;!):%^b'PfWxh_\k$FH&<3p(!nYbAyW$&I\=CxtVJ.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.6	49903	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:14 UTC	4056	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_blog.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:14 UTC	4285	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:14 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "eed1-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 61137 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:14 UTC	4376	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 f2 bc ea 77 0a 13 f4 1e af 28 e0 50 01 40 05 14 46 31 82 00 80 8c 8b 3b 9d ab 34 34 e4 a8 e9 f2 6a c4 e9 a6 6c fb 7d c7 77 d3 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"w(P@F1;44jl}w
2022-10-03 14:16:14 UTC	4392	IN	Data Raw: 2c d4 d4 53 dd d1 45 52 aa ac ae 9c 6b 46 f3 55 35 27 55 41 60 0d 39 aa eb 51 54 e2 00 a0 3e 2b 1f 8b f8 9e 12 7c 47 da 68 dc fe 73 a2 24 9b 9d 7a 62 61 91 ed 60 d4 ad 8b 85 10 e1 f3 d3 b5 66 ff 00 28 fa ce 37 e9 78 9f bd 7f bf a0 15 a8 41 54 2e c9 46 e1 3c 12 de f4 c7 12 3b c2 6b 93 99 5b a9 59 95 d5 56 af 8a 61 ba 36 20 8e 29 aa 22 87 cc 85 45 82 c1 3e 77 f7 73 50 40 c8 18 1a d1 fe 86 4d 35 5b 4b 6f c1 86 ab 22 df 7a c5 e3 b1 18 b7 e6 95 f5 ee e1 d0 c8 dc ff 00 04 dc 0e 2e 9f 27 87 7f 89 b2 66 c8 c7 3c 8a b3 2f 89 58 7c 1b 61 6b 41 ab c8 e2 56 f7 82 cb cd 50 04 5c 13 9e 11 90 20 e6 ac 4e 06 1c 4f 6a b5 ee 2b 69 60 8e 18 b4 b2 33 96 9a f7 a0 d2 6e 54 d8 38 06 1d b2 75 e0 b8 f0 4c 7e 2a 16 d1 8f 21 ae 42 99 ae 6e 9b 1c 32 61 5c 7a a7 54 71 0a 88 fa 2e 8d Data Ascii: ,SERkFU5'UA`9QT>+|Ghs$zba`f(7xAT.F<;k[YVa6)"E>wsP@M5[Ko"z.'f</X|akAVP\ NOj+i`3nT8uL~*!B n2a\zTq.
2022-10-03 14:16:15 UTC	4459	IN	Data Raw: 76 69 47 37 80 ff 00 da 8a 4a b4 72 3a 13 ee 3d e9 cd 74 4f 74 83 33 81 e1 aa 95 91 c8 04 ac bd 39 71 ee 4f 6e 47 bd e2 ed 77 69 ba f9 26 3b 40 4f 81 fc 91 15 1a d0 f0 3c 93 4c b8 79 b2 65 f9 3a 55 ce 2b 75 ed e6 0a c6 60 19 23 4d 96 33 67 3e 22 4b 45 91 0b 65 47 bd 23 b9 58 26 84 d4 3a 69 e8 17 29 1c b6 ce 28 c6 c0 c6 9d e7 7b 94 4c aa 63 68 3e aa 5a 0f 8f 35 2c 6d 7f ed 1b fd 41 66 9a 0d 7e 51 9c f8 a1 2b a6 dd 8c 10 38 b8 fe 48 0c a3 ab 8e dc cf f9 c5 35 a1 a2 83 4e 9a a8 e3 00 75 8f 06 9c b9 a8 e3 93 11 28 b5 f8 72 68 58 6c 3b 62 6d 00 f1 ef 5b 47 64 66 ac b0 f1 d4 27 32 58 5d 70 41 41 cc 77 68 50 f3 0a 48 2d 52 2a 39 84 d7 4e c0 5a 1e 1c ce 4e bd 3c 10 2d b3 9e f7 97 0e 00 52 9e 09 98 fc c3 26 25 99 b9 3b 8a f8 33 b4 1f 2c 93 61 8b c9 60 65 58 1c 6e Data Ascii: viG7Jr:=tOt39qOnGwi&;@O<Lye:U+u`#M3g>"KEeG#X&:i)({Lch>Z5,mAf~Q+8H5Nu(rhXl;bm[Gdf'2X]pAAw hPH-R*9NZN<-R&%;3,a`eXn
2022-10-03 14:16:15 UTC	4475	IN	Data Raw: 7c 1e a7 b9 83 0a 00 b7 37 50 e1 96 bc b4 95 a9 eb d9 f0 cb f6 f4 61 2e b2 8d 86 28 05 57 a1 85 ef f6 fe 65 53 ff 00 53 0c a4 fa 58 10 be 58 e2 dd f7 5b e6 1f 03 37 61 07 e6 df bc be 95 7f d4 1f c9 1e 3d 14 5f e5 bf 11 00 79 d1 74 fc 19 27 e5 80 c9 2f 01 00 80 98 f1 00 32 bd 45 0c 89 c4 c5 36 df 10 1a 15 e3 86 02 0d 43 0d ae 29 dc 4c f8 04 0b ed 65 e5 1d 50 7e 32 84 06 c4 b1 32 24 a9 52 a0 42 58 f3 5f 4e 27 fa 8e f0 c4 ad 30 79 80 b8 2f 86 a1 c1 2e a8 91 f9 20 13 51 29 82 92 85 c3 9f 92 6d 34 c1 5e 88 a1 b8 7e 87 0c ac 78 88 1e 2a 1d 45 c8 c0 5b 45 64 30 d1 92 55 90 61 88 0a 04 02 d7 0e e1 1c fd c4 09 06 0d f6 21 c5 55 c0 6a 28 5b 43 7a 29 b8 d5 88 9a 8a d9 b7 87 18 3f f7 f3 1a 04 9e 85 ac 79 21 ed 5b 13 2b f6 5e 09 68 21 07 43 fa 9a cd 7f 88 08 d8 7d 96 Data Ascii: |7Pa.(WeSSXX[7a=_yt'/2E6C)LeP~22$RBX_N'0y/. Q)m4^~x*E[Ed0Ua!Uj([Cz)?y![+^h!C}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49730	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:39 UTC	242	OUT	GET /wordpress/wp-content/themes/kawaken/js/base.js HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:40 UTC	242	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:40 GMT Server: Apache Last-Modified: Tue, 10 Nov 2020 03:09:34 GMT ETag: "1099-5b3b802177780" Accept-Ranges: bytes Content-Length: 4249 Connection: close Content-Type: text/javascript
2022-10-03 14:15:40 UTC	242	IN	Data Raw: 24 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 09 24 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 27 6c 6f 61 64 27 2c 20 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 09 09 24 28 27 2e 6c 6f 61 64 69 6e 67 27 29 2e 66 61 64 65 4f 75 74 28 29 3b 0a 09 7d 29 3b 0a 7d 29 3b 0a 0a 2f 2f e3 82 a2 e3 83 b3 e3 82 ab e3 83 bc e3 83 aa e3 83 b3 e3 82 af 0a 24 28 77 69 6e 64 6f 77 29 2e 6c 6f 61 64 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0a 09 24 28 22 23 74 6f 70 5f 74 78 74 22 29 2e 61 64 64 43 6c 61 73 73 28 22 66 61 64 65 49 6e 44 6f 77 6e 5f 74 6f 70 5f 30 31 22 29 3b 0a 09 24 28 22 23 74 6f 70 5f 74 78 74 32 22 29 2e 61 64 64 43 6c 61 73 73 28 22 66 61 64 65 49 6e 44 6f 77 6e 5f 74 6f 70 5f 30 32 22 29 3b 0a 0a 09 76 61 72 20 68 65 61 64 65 72 48 69 67 68 74 20 3d 20 30 3b 20 2f 2f e3 Data Ascii: $(function(){$(window).on('load', function(){$('.loading').fadeOut();});});//$(window).load(function(){$("#top_txt").addClass("fadeInDown_top_01");$("#top_txt2").addClass("fadeInDown_top_02");var headerHight = 0; //

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.6	49904	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:14 UTC	4137	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_ttl.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:14 UTC	4375	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:14 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "160fb-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 90363 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:15 UTC	4426	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 6d 6c 6e 73 3a 78 6c 69 6e 6b 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 6c 69 6e 6b 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 36 38 36 2e 30 31 20 31 39 34 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 69 73 6f 6c 61 74 69 6f 6e 3a 69 73 6f 6c 61 74 65 3b 7d 2e 63 6c 73 2d 32 7b 6f 70 61 63 69 74 79 3a 30 2e 36 3b 6d 69 78 2d 62 6c 65 6e 64 2d 6d 6f 64 65 3a 6d 75 6c 74 69 70 6c 79 3b 7d 2e 63 6c 73 2d 33 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" viewBox="0 0 686.01 194"><defs><style>.cls-1{isolation:isolate;}.cls-2{opacity:0.6;mix-blend-mode:multiply;}.cls-3{fill:#fff;}</style></defs><title>1</title><g
2022-10-03 14:16:15 UTC	4442	IN	Data Raw: 32 6b 5a 6b 58 4d 33 65 69 72 44 6c 65 47 58 67 75 73 6a 36 54 61 47 73 6f 34 6a 66 44 73 4d 66 73 7a 46 73 48 75 4d 2b 64 46 66 31 44 70 34 56 55 7a 6b 72 37 34 4d 43 64 79 7a 4b 62 49 2b 71 54 46 77 6a 5a 50 33 75 4e 43 75 65 5a 55 47 50 30 39 64 39 58 42 61 2f 59 4e 65 2b 6a 47 63 65 50 36 54 76 7a 37 48 78 57 4d 64 4a 57 78 66 62 74 6f 41 54 2f 69 31 63 4a 35 2f 52 64 4a 67 31 54 56 73 73 48 5a 5a 44 2f 6f 6f 2f 6d 46 7a 6b 4d 63 38 55 78 6d 76 5a 78 63 76 67 66 55 78 65 56 37 46 6a 66 63 50 49 34 7a 76 73 47 6f 66 74 62 78 37 51 2b 46 33 68 64 2f 5a 2b 5a 72 42 45 43 69 36 37 47 37 6a 38 67 2b 75 2b 7a 72 76 4c 2f 6d 52 37 75 2b 37 7a 49 53 50 33 72 63 72 71 4b 7a 69 4d 77 57 59 65 32 4f 38 7a 57 45 49 65 46 53 43 71 6a 31 46 2b 63 41 66 76 62 78 55 Data Ascii: 2kZkXM3eirDleGXgusj6TaGso4jfDsMfszFsHuM+dFf1Dp4VUzkr74MCdyzKbI+qTFwjZP3uNCueZU GP09d9XBa/YNe+jGceP6Tvz7HxWMdJWxfbtoAT/i1cJ5/RdJg1TVssHZZD/oo/mFzkMc8UxmvZxcvgfUxeV7FjfcPI 4zvsGoftbx7Q+F3hd/Z+ZrBECi67G7j8g+u+zrvL/mR7u+7zISP3rcrqKziMwWYe2O8zWEIeFSCqj1F+cAfvbxU

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:15 UTC	4520	IN	Data Raw: 6a 38 4a 37 6c 61 2b 56 71 64 62 31 36 2f 6f 57 73 58 46 54 38 43 2b 6e 76 49 48 4a 2b 6b 5a 34 76 78 57 2b 6b 2b 4d 57 67 5a 53 39 56 64 59 6e 42 75 34 31 64 76 77 39 6d 73 54 78 4d 38 33 65 33 2f 74 73 62 36 49 65 4b 69 6a 52 75 49 4e 64 4e 39 6a 34 61 69 36 4f 43 64 55 42 37 6f 6d 2f 65 41 67 49 65 70 2f 72 77 69 68 2f 72 30 55 79 71 4a 75 63 6c 4e 78 53 6c 6c 75 42 36 49 50 42 6f 79 43 50 4d 4e 53 78 4c 57 43 54 49 6d 4f 30 6a 35 63 34 6c 6a 41 42 6b 49 50 74 6e 48 58 4d 6b 51 6c 56 7a 47 72 6f 32 48 6c 66 54 74 65 73 6f 78 43 64 58 59 7a 36 72 7a 4d 39 61 62 6b 54 78 7a 30 4d 77 61 48 6e 54 6a 59 61 4f 6d 58 56 74 72 44 78 4f 63 58 4c 71 68 39 34 77 47 6e 39 53 64 46 43 49 45 57 43 56 49 61 56 55 59 70 6c 6b 44 57 61 6d 63 63 32 6f 74 49 35 30 39 56 Data Ascii: j8J7la+Vqdb16/oWsXFT8C+nvIHJ+kZ4vxW+k+MWgZS9VdYnBu41dvw9msTxM83e3/tsb6leKijRuINdN9j4ai6O CdUB7om/eAgIep/rwih/r0UyqJuclNxSlluB6IPBoyCPMNSxLWCTImO0j5c4ljABkIPtnHXMkQlVzGro2HlfTtesox CdXYz6rzM9abkTxz0MwaHnTjYaOmXVtrDxOcXLqh94wGn9SdFCIEWCVIaVUYplkDWamcc2otI509V
2022-10-03 14:16:15 UTC	4536	IN	Data Raw: 54 7a 50 2f 4c 31 6e 7a 6a 75 70 5a 56 4d 48 6a 75 44 6c 61 35 39 6b 71 7a 39 42 6e 79 7a 69 58 71 6f 43 57 41 44 34 51 54 4e 6b 67 73 35 7a 6e 51 5a 59 68 61 6b 50 76 50 42 43 78 4b 70 4b 58 5a 68 50 74 58 66 68 49 33 78 68 5a 71 6d 50 42 63 39 73 31 6d 6b 63 61 33 71 33 75 37 38 75 45 67 72 63 4b 32 58 36 6e 5a 69 38 30 67 44 56 4b 75 6c 42 55 48 4c 6f 4b 76 45 56 75 65 4e 46 59 7a 70 4e 6a 65 57 73 30 33 66 59 31 57 73 37 37 6b 31 44 75 50 38 68 2b 71 48 64 63 45 4e 44 59 55 4d 33 77 50 53 4b 69 34 4d 65 73 66 67 4e 62 6c 62 4e 61 42 71 73 67 56 57 72 48 70 4f 4f 61 6c 67 30 2f 4c 61 6c 2f 48 38 67 48 68 34 2f 6f 6c 36 2f 62 37 4d 68 4d 57 71 49 4e 51 48 37 55 31 68 51 7a 4e 47 5a 73 71 76 4e 74 76 32 4d 47 38 68 49 5a 37 41 73 77 57 6e 42 55 6e 62 4b Data Ascii: TzP/L1nzjupZVMHjuDla59kqz9BnyziXqoCWAD4QTNkgs5znQZYhakPvPBCxKpKXZhPtXfhI3xhZqm PBc9s1mkca3q3u78uEgrcK2X6nZi80gDVKulBUHLoKvEVueNFYzpNjeWs03fY1Ws77k1DuP8h+qHdcENDYUM3wPSKi 4MesfgNblbNaBqsgVWrHpOOalg0/Lal/H8gHh4/ol6/b7MhMWqINQH7U1hQzNGZsqvNtv2MG8hIZ7AswWnBUnbK
2022-10-03 14:16:15 UTC	4552	IN	Data Raw: 75 72 2b 33 79 44 55 30 41 71 38 6c 48 49 32 6d 6a 71 72 58 54 33 46 57 36 68 54 4c 53 4e 6a 73 6f 32 73 4f 4d 59 64 39 51 75 6b 30 51 72 57 4d 4b 43 2b 72 6b 61 2f 6b 2f 34 4c 49 6c 73 62 4e 36 79 78 71 6a 61 63 5a 48 77 4f 6c 45 78 35 4e 75 38 41 5a 53 4d 65 36 52 37 39 30 34 77 35 67 44 59 63 38 55 45 59 2b 45 54 4c 79 6b 73 77 34 2f 6b 4c 49 38 52 4d 6d 51 63 34 36 78 6c 39 35 74 6c 66 2b 72 32 44 34 48 61 46 37 6e 37 72 33 36 6c 71 72 2f 77 66 64 39 32 75 2f 35 70 50 75 37 33 63 55 4a 37 65 41 66 4e 59 31 2f 45 53 57 78 52 79 44 36 2b 6d 35 6a 6e 65 49 70 2f 38 69 65 50 70 50 30 67 46 62 4d 76 55 36 36 74 45 71 79 50 45 63 6b 4c 72 5a 79 71 5a 4f 2b 44 50 35 67 50 69 32 2f 4f 36 31 57 6a 34 49 78 73 33 6f 72 47 72 63 38 36 67 47 42 6a 73 45 71 48 6c Data Ascii: ur+3yDU0Aq8lHI2mjqrXT3FW6hTLSNjso2sOMYd9Quk0QrWMKC+rka/k/4LIlsbN6yxqjacZHwOlEx 5Nu8AZSMe6R7904w5gDYc8UEY+ETLyksw4/kLl8RMmQc46xl95tlf+r2D4HaF7n7r36lqr/wfd92u/5pPu73cUJ7eA fNY1/ESWxRyD6+m5jneIp/8iePpP0gFbMvU66tEqyPEckLrZyqZO+DP5gPi2/O61Wj4lxs3orGrc86gGBjsEqHl
2022-10-03 14:16:15 UTC	4600	IN	Data Raw: 30 2c 2e 30 36 2c 30 6c 30 2c 30 63 2e 30 38 2d 2e 30 36 2e 31 37 2c 30 2c 2e 32 32 2c 30 68 30 6c 30 2c 30 2c 30 2c 30 68 30 6c 2e 30 38 2d 2e 31 31 2e 30 37 2c 30 63 2d 2e 31 2d 2e 31 35 2e 34 35 2d 2e 32 37 2e 35 31 2d 2e 33 35 73 2e 30 38 2d 2e 31 39 2e 31 39 2d 2e 32 36 2e 31 35 2c 30 2c 2e 32 36 2c 30 2d 2e 30 39 2c 30 2d 2e 30 37 2d 2e 30 38 6c 2e 31 37 2c 30 63 30 2c 2e 30 37 2c 30 2c 2e 30 36 2e 30 37 2e 30 37 73 2e 33 31 2d 2e 31 38 2e 31 38 2d 2e 33 63 2e 31 36 2d 2e 30 39 2e 32 31 2d 2e 30 36 2e 32 36 2d 2e 31 31 48 36 35 39 63 2e 31 2c 30 2c 30 2c 30 2c 30 73 2e 35 33 2d 2e 32 38 2e 33 39 2d 2e 33 39 68 30 63 2d 2e 31 31 2d 2e 30 39 2d 2e 32 34 2d 2e 31 33 2d 2e 32 37 2d 2e 32 32 68 2e 30 38 6c 30 2d 2e 30 39 2e 31 2c 30 63 30 2d 2e 31 Data Ascii: 0,.06,0l0,0c.08-.06.17,0,.22,0h0l0,0,0,0h0l.08-.11.07,0c-.1-.15.45-.27.51-.35s.08-.19.19-.26.15,0,.26,0-.09,0-.07-.08l.17,0c0,.07,0,.06.07.07s.31-.18.18-.3c.16-.09.21-.06.26-.11H659c.1,0,0,0,0,0s.53-.28.39-.39h0c-.11-.09-.24-.13-.27-.22h.08l0-.09.1,0c0-.1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.6	49905	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:14 UTC	4217	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_ini.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:15 UTC	4408	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:14 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "ff70-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 65392 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:15 UTC	4488	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 03 04 02 05 06 01 00 07 08 ff da 00 08 01 01 00 00 00 00 f5 46 85 9a aa ab 1b 7a 77 45 25 41 61 e5 9c 9a f6 9d 10 82 17 18 2d 4b 53 3c 65 5d d7 cc 43 57 47 cd 4b a0 e9 00 63 8e ac be Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"FzwE%Aa-KS<e]CWGKc

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:15 UTC	4504	IN	Data Raw: 3c cc 9f 51 d4 e3 a2 6f 4e f3 73 15 5e d6 56 ef 91 b6 d1 a0 44 f2 8a 1f a7 84 9c 5b 1d ab dd 2c 66 9f c8 88 3c 2c d1 0d 3f 33 59 e0 ca 94 b7 73 cd cf 66 6f c6 75 33 07 c6 e9 b8 35 a6 07 4d 09 39 0d 9b 32 e8 6f 19 6e be ca 8b c1 1f 82 c7 e1 82 5e 17 87 bf e0 e6 79 a3 30 b0 08 3e a6 2f 09 78 40 b3 22 f9 99 a6 d8 e9 9b 2a bf 2c cb 76 c2 a8 db f4 ec 45 c8 ce 36 f2 03 92 de 46 f2 b2 25 ca e9 5a 00 79 49 d7 b5 2a bf d0 74 65 8b a4 df f7 f5 05 8e c6 cd 42 d9 32 67 f2 c5 c3 cd 05 06 e8 a9 44 7a cc 3c 02 f1 21 3f 3c 26 21 a8 de 02 ac 4b 10 4b 9d 68 54 13 75 d8 07 f1 76 93 f3 ce a7 a7 49 19 e3 05 9e 75 26 3f 3d 33 d4 d6 fd a8 98 10 c9 1a 86 cd cd 9b b7 df e3 e4 f2 17 28 f9 d9 cb 44 3b e2 a7 e8 cd 33 0f 59 e6 9f b0 78 ac df 0c 81 ee a1 0d c3 32 cd 0f 37 7c 32 c3 33 Data Ascii: <QoNs^VD[,f<,?3Ysfou35M92on^y0>/x@"*,vE6F%ZyI*teB2gDz<!?<&!KKhTuvIu&?=3(D;3Yx27|23
2022-10-03 14:16:15 UTC	4568	IN	Data Raw: 76 e0 7a 9e 04 d3 a7 bf 61 73 e8 bc 0f de 66 8f 41 59 b2 eb aa d3 27 a9 38 26 76 65 21 be 8d 5b de df 78 f8 41 9f d2 2d 6e 45 7a 81 a6 4f 4a 86 0f cd 35 3a ab 0b df 73 da e7 cd 98 b1 97 be 98 de fe 11 e4 0c 47 4b 4b dc 11 97 1b 57 d7 32 d4 b0 d6 47 22 5b 50 1b d4 8c f4 8e dc aa c7 5d 4d ae e3 dd af 1f 34 00 19 b3 49 4a e3 9c 67 f5 6e 65 76 a8 ca ca ec d5 d4 38 03 70 30 e9 f5 ce be 79 cc 5e d0 d3 9d ec ab aa 54 da a4 ff 00 78 07 00 7f 98 4d b4 ea 2b 75 04 36 14 83 d0 f3 05 08 42 56 15 03 7d 91 81 0b 76 5e a8 7a 85 fe 61 37 76 15 6b e8 cf fc c6 7d 62 7b 28 be 94 72 5c 31 19 3c cd 1d 94 1b 81 b7 03 3c 1e bc 4d 21 40 e1 ac e4 7a ce 27 d5 b8 9b 74 f7 b7 a2 18 5a db 4f ab 98 4f 68 69 80 eb be 5f 4b 9d f6 31 18 c4 d4 3d ac cb d2 6a 3d 44 d4 7a 89 7f c2 5e 3d 25 Data Ascii: vzasfAY'8&ve![xA-nEzOJ5:sGKKW2G"[P]M4IJgnev8p0y^TxM+u6BV}v^za7vk}b{(r\1<<M!@z'tZOOhi_K1=j=Dz^=%
2022-10-03 14:16:15 UTC	4584	IN	Data Raw: 04 40 fd 0f 31 6e 4c 13 d2 15 b4 a0 82 a6 c8 eb 03 1c b4 ee dd 5c 75 56 06 53 6e 08 27 7e 3a 7e 73 3a dd 32 fd 95 b5 3f 81 85 f5 24 fa 19 97 da 3a 2f 10 b6 21 03 d0 44 04 a8 25 8f a2 8c c6 d8 0e 00 cc f0 01 ec e2 73 3e ac 7e 46 72 66 26 1b 98 59 28 c3 85 20 64 66 2d c6 ca 0f bf 56 19 4f 9b 23 42 63 2c 18 da 60 60 51 b9 59 de 6a ac ad 06 11 0e 3f 32 3c e1 ef 1c 93 c6 e2 a4 4a 3b 4a 87 6b 2d 74 28 fb 57 6e 3c c4 d3 8c 95 d7 9f cb bb 94 d1 a5 d4 de 35 d9 35 56 5b 67 77 d7 d0 75 81 28 1d e8 e4 f5 00 c7 de 15 46 15 47 48 5c 78 a1 b8 1d b7 32 1f 80 9d 9f a6 6d ef 9b ec fb d6 1c ca c2 15 06 77 76 6e c7 9f 5c cd 32 1c bd a8 3f 59 ae 7a 0d da 7d 2d cf 56 3d e0 bc 4e d2 ed 14 67 d3 52 5d 47 52 08 18 cf ae 66 ae 9a 19 b5 29 b9 be e0 20 e0 08 12 dd 0e b9 50 ae 41 ad Data Ascii: @1nL\uVSn'~:~s:2?$:/!D%s>~Frf&Y(df-VO#Bc,``QYj?2<J;Jk-t(Wn<55V[gwu(FGH\x2mwvn\2?Yz}-V=N gR]GRf) PA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.6	49907	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:15 UTC	4458	OUT	GET /wordpress/wp-content/themes/kawaken/images/scrolldown.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:15 UTC	4608	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:15 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:11 GMT ETag: "c3a-5b252e7e28dc0" Accept-Ranges: bytes Content-Length: 3130 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:15 UTC	4609	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 37 37 2e 30 33 20 33 34 2e 32 35 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 66 66 66 3b 7d 2e 63 6c 73 2d 32 7b 66 69 6c 6c 3a 6e 6f 6e 65 3b 73 74 72 6f 6b 65 3a 23 66 66 66 3b 73 74 72 6f 6b 65 2d 6d 69 74 65 72 6c 69 6d 69 74 3a 31 30 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 33 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 177.03 34.25"><defs><style>.cls-1{fill:#fff;}.cls-2{fill:none;stroke:#fff;stroke-miterlimit:10;}</style></defs><title> 3</title><g id="_2" data-name=" 2"><g id="

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.6	49906	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:15 UTC	4486	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_rakuseki.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:15 UTC	4608	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:15 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "1ce59-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 118361 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:16 UTC	4612	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1d 00 00 02 03 01 01 01 01 01 00 00 00 00 00 00 00 00 04 05 02 03 06 01 00 07 08 09 ff da 00 08 01 01 00 00 00 00 fb 60 9e 59 94 fa 2b df 7a 33 ef 28 ba 30 b7 c3 46 57 0b 7d 94 dd 55 54 93 74 17 dc ad 91 31 27 96 55 1e f6 cf 23 6e ba f0 Data Ascii: JFIF"#"" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"`Y+z3(0FW}UTt1'U#n
2022-10-03 14:16:16 UTC	4628	IN	Data Raw: fa ed a0 c4 01 3d 37 67 85 55 37 67 e7 05 82 25 e7 ba 75 6b 4e 49 bf 46 76 33 e2 38 7a 90 ed a3 5e 69 c6 fa 59 89 2d a3 b4 b4 3d 66 ca dd 67 cc f5 90 2d 5c f3 cd 23 e3 83 c5 54 da 9b ee 1f 41 9b 6e 24 51 50 e9 f2 a5 03 ac ac 55 3c 19 2c 47 6e e3 45 59 98 81 e3 38 81 29 1a 17 2d 4c 8b 99 4b af 57 af 1f 17 0c 12 d3 2e 9e 7b 2e a9 00 7a c3 a6 e6 ec eb a6 af 7b 13 d4 c3 b3 32 9b da 9e 6c a3 a7 1e cc 6a fd 4d 29 42 02 ac 07 70 1f 84 9c 19 f6 85 d2 82 b6 55 6d ba 7c cf f3 24 42 a7 cd e0 0f 30 9d 72 0d db 4c bc b8 d6 ce d5 af d8 d1 a1 06 50 13 6d 3c 91 01 ce 85 c3 00 88 b2 93 2f 45 99 80 50 d0 35 92 f9 66 66 6c bc 9f 79 83 dd 48 e2 b1 24 71 8b 52 07 de 8f 47 4e e8 94 49 9f 06 55 e9 b3 67 44 ef d3 8e fe 09 7d 39 84 c7 41 0b 30 ee 00 3e 2c 65 19 25 3c 94 3a 24 c3 Data Ascii: =7gU7g%ukNIFv38z^iY-=fg-\#TAn$QPU<,GnEY8)-LKW.{.z{2ljM)BpUm\|$B0rLPm</EP5ffIyH$qRGNIUgD}9 A0>,e%<:$
2022-10-03 14:16:16 UTC	4676	IN	Data Raw: 7e 5e f1 fc 48 31 da cb 35 49 e0 3e 0d de ba 8a 05 84 73 ec 51 40 cd 97 90 a4 25 a5 ca 8a 16 66 ea 85 db bf 93 0e fe 3d 19 ba 15 f2 2e b1 ce 54 8b 57 bb 39 9b c8 d5 63 36 65 95 9e 7d 62 0a 43 9a e9 13 61 d8 1f ec a4 d9 93 d3 4a 75 c7 fc 7b 7f 26 95 b6 7b e6 7c b7 79 53 0e 96 85 8b 50 6d bb e9 36 58 1a ec ca d7 a6 f8 44 66 21 31 6f 10 ce 44 f7 56 ba 28 08 c1 98 ea a6 79 5f 4f 1b 04 66 f1 cd 2a 38 67 4d 98 f6 2e 43 df d0 44 fc 93 3e 19 2b 31 d3 af 54 84 84 ba b5 f2 53 3c d6 67 1e c1 da ca 42 80 a4 d3 76 5d 39 fd 54 ad 97 32 2a 74 3b bf f4 fb d3 d6 be 15 21 c3 77 18 ef 51 dc 16 de 41 00 5f c8 30 7d 24 95 26 8b 0d 5f be 3d 50 15 f1 61 25 72 09 1b 25 7a 4d 28 5e 9d 99 ba f6 ff 00 ce cd 47 63 dc d1 c6 32 dd eb 78 46 02 a6 df 23 ce ad fd 66 d3 53 c7 cd d7 91 e5 Data Ascii: ~^H15I>sQ@%f=.TW9c6e}bCaJu{&{|ySPm6XDf!1oDV(y_Of*8gM.CD>+1TS<gBv]9T2*t;|wQA_0} $&_=Pa%r%zM(^Gc2xF#fS
2022-10-03 14:16:16 UTC	4692	IN	Data Raw: d1 1e 56 b9 46 be 5a f4 22 40 4b 29 bd 1f a4 31 66 52 a3 36 51 b6 15 a4 ed 96 7a 82 65 e4 64 a6 1a 3c f3 e4 ad 5d eb d6 af 16 12 e9 f5 6f 67 fd 8e b6 75 09 49 e8 a2 ba 99 1e 4f 69 51 3e b0 6c a8 9f d6 eb e4 ee c0 c2 52 8d e9 77 88 be cd 72 d4 dc 7c 1f 92 df c2 6d bc 99 39 0b 71 8f a6 19 e5 ca 72 b0 cd 15 4c 4a e1 c3 d1 e7 7b 68 f1 02 b6 d3 82 ad e7 5d 94 a6 98 d1 eb ef a0 2a d2 0b f5 92 86 6c 49 b1 18 b9 3f ac 4b 75 a2 dd 82 74 d2 90 bd 15 89 5f 6b f9 66 02 73 2c 3d e5 14 b8 7d 8e 60 26 de 7e 4b d2 a9 56 52 61 a8 4b 37 79 cb 3c fb f6 a4 67 29 50 f6 d0 c1 3b 3f 5f f9 3f 8f 50 41 92 4c 5e e0 36 25 23 15 3f b0 8b 6a 16 50 04 68 8e 8f 01 9b 24 68 4f 70 89 db c5 f5 8c 4d fc 8a 8c ff 00 5a 66 26 b7 0a 13 a7 d7 a3 bf 81 72 18 aa 07 58 a5 10 29 1a 56 a5 d5 d2 54 Data Ascii: VFZ"@K)1fR6Qzed<]oguIOiQ>lRwr|m9qrLJ{h]*II?Kut_kfs,=}`&~KVRaK7y<g)P;?_?PAL^6%#?jPh$hOpMZ f&rX)VT
2022-10-03 14:16:16 UTC	4708	IN	Data Raw: 43 a0 0d 75 8f c8 b3 10 54 9b a1 18 5a ad b1 3f 31 88 bd 9d d0 d7 4a 88 be 9f 1e 1b 2a 10 51 62 de 66 42 38 8b 23 b1 13 d2 a9 f5 0f 76 c9 a2 26 12 cc f6 14 3f 99 88 62 b0 47 10 2f a4 f6 71 ef 38 b8 07 db 7b a0 23 e3 75 c9 8c 83 5d 83 4c b7 c5 40 08 57 ac 5a 1a 25 06 b7 33 b5 e4 fb b7 2e f2 16 ca ce 3c 1d 47 05 3a 05 fc ce 6f f5 3d a0 31 b0 23 93 ea 7d 4a 70 c6 be 07 76 9c 4b d1 e4 ed f7 35 cf 56 b9 32 65 17 ff 00 f4 8f 13 38 c9 94 9b 03 c1 3e 63 d5 1f b8 77 9e 99 b2 1e 7a ef 66 32 a8 41 c8 d2 81 52 d4 01 51 f8 8c 38 cb 1b f8 95 cb 28 f7 54 ca aa d9 0f b3 18 1f ee 63 1c 99 4f df 31 9b 40 28 93 d2 69 0b 16 24 1e a6 29 a0 c0 08 96 7f d8 43 7f 88 c7 94 d1 f3 1a e7 4b a9 d6 71 a6 36 a6 66 e5 92 ac 28 1a 11 d8 0b e4 67 fa 61 aa 13 7b 8e 2c dd 29 88 03 de da 2f Data Ascii: CuTZ?1J*QbfB8#v&?bG/q8{#u]L@WZ%3.<G:o=1#}JpvK5V2e8>cwzf2ARQ8(TcO1@(i$)CKq6f(ga{,)/
2022-10-03 14:16:16 UTC	4752	IN	Data Raw: 90 67 37 70 a8 0b 13 74 04 4e 07 d4 1e 54 07 b8 03 e0 f6 98 89 4e 5e dd f5 66 f3 00 08 28 f1 5e ff 00 98 47 5e 91 e8 dc 37 f9 ea 2a 65 be 3a 73 39 15 7d 24 e4 7d f7 47 a1 02 2f 03 c6 a8 74 2a 65 ae 3f 23 a6 e6 64 e3 90 05 c6 bd 58 0e e6 06 d6 1e 1c 88 ff 00 57 5b 95 f4 94 9b 27 a9 61 16 d5 30 52 a9 1d 88 98 f1 ff 00 6c eb 19 f2 4f 89 9c 8c 09 45 c0 1b 62 60 50 41 d5 0a 84 37 36 a0 dd 6a 61 fb 8e dc 0d 12 23 b7 d6 7d 82 4d a8 fc 01 30 65 63 c4 d3 2f db 7f 37 08 67 bd b1 ed f0 00 99 39 10 76 58 e8 47 b2 52 b9 26 a2 36 4c aa 2c 91 ba 1e 77 de 63 19 73 e7 07 e8 a9 3c 98 7c 99 f5 32 3e 53 c7 e1 49 ed 1f 1f 0c 1b cc e7 ab 64 ad cc bf db 42 59 a8 5e c7 4d 4c cc d8 03 92 09 d6 c4 c8 c1 dd c0 17 ad 1d 6a 62 2e 31 3d 16 e8 69 7b 98 a2 de c1 af 35 d4 c3 45 b1 2e c8 Data Ascii: g7ptNTN^f(^G^7*e:s9}$}G/t*e?#dXW['a0RlOEb`PA76ja#}M0ec/7g9vXGR&6L,wcs<|2>SIdBY^MLjb.1=i{5E.

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:16 UTC	4768	IN	Data Raw: 8c f1 04 7c 89 7c d3 1d 93 e0 46 d9 6e 64 f7 11 90 65 71 ee 1e 4f 63 3d 2e 31 9f 3f b7 31 53 4a 2f a1 23 bc a6 c6 83 88 d0 a9 8c 97 c4 3a 5d 72 98 3d 46 34 04 9e 3f 50 99 9b 36 3e 05 af ea 36 8a 91 1f 97 ff 00 8b 39 6b 3e 6c cc 98 b0 80 2a 82 d9 df 7b 33 3b 64 67 d9 66 30 92 7e 20 37 14 72 f2 22 ff 00 1e 20 a7 55 34 67 1c 78 f1 1e 2b 90 fd da 8a ee c8 79 1c dd 61 39 0e 21 48 b3 d3 7d 16 1f bf 64 4f 54 b9 91 ba a8 a8 95 91 7a 0b 99 b8 b8 e8 35 3e 93 2a 8f ba e8 b5 c0 3e 9a 65 75 5a 8e e1 f0 fb b2 22 9a 0c 86 03 ef ea b7 60 19 76 c8 47 4a b9 ad db 1b a9 ea 4b 87 5b 7c 67 6b 5e 37 07 f6 89 a0 a1 47 b4 1f 1a 83 23 58 02 f8 eb 70 63 14 7b 9b 26 7b 54 b7 45 99 9f ee e3 f1 1c 96 1a 35 d0 13 32 af 02 2c 5c c4 00 3f b8 1d 46 df 11 46 31 3a be 60 ec 42 19 8d 51 8f Data Ascii: ||FndeqOc=.1?1SJ/#:]r=F4?P6>69k>I*{3;dgf0~ 7r" U4gx+ya9!H}dOTz5>*>euZ"`vGJK[|gk^7G#Xpc{&{TE52,\?FF1:`BQ
2022-10-03 14:16:16 UTC	4784	IN	Data Raw: 19 dd 14 32 42 a6 84 92 2d 18 d5 7a 13 5a 61 18 6d 96 9c 8d 91 cb eb 02 8d 24 ae c4 e6 ad d3 22 d5 21 ee a4 4a ea ec 6e d3 6c 8c 78 24 92 7c 0a 09 37 c8 a9 b7 fd a8 db e5 72 53 1c e7 27 27 48 52 b4 96 4c 0c 54 36 f2 c8 22 36 b2 c8 e6 ac 69 6e 7c 09 c7 72 19 6b 82 e9 24 25 9d 3e bf 04 d6 48 c7 a4 77 84 ac 4d e0 b4 25 2a 69 65 0d 3e 7b 14 bb 3a b1 d2 72 c2 64 17 8d 51 36 db 48 6b f6 64 2d d7 fa 12 54 71 83 1c 91 8e 25 1d c2 77 b4 5f b8 fa 4c 75 c1 c8 ac 4a a9 69 96 67 27 d1 24 a9 c4 6d f2 34 c4 3d 10 a9 a2 5e cc 64 55 49 19 c1 81 5e 8e b4 43 7c 70 53 76 f4 dc e8 4b e2 cf 92 56 c4 9d a7 94 5c ad e5 8f 22 fd 4b 62 94 e4 c9 7b 2d 50 9e 19 36 d2 25 16 9c 7f d9 6e ec da 89 26 24 c8 a4 92 2b 0b 93 81 b4 92 45 5d 0d ac a1 6d ab 12 ac ea ab 56 dd 25 f8 38 ae 09 4a Data Ascii: 2B-zZam$"!Jnlx$|7rS"HRLT6"6in|rk$%>HwM%*ie>{:rdQ6Hkd-Tq%w_LuJig'$m4=^dUI^C|pSvKV\"Kb{-P 6%n&$+E]mV%8J

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.6	49908	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:15 UTC	4487	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_newsletter.jpg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:15 UTC	4612	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:15 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "eee1-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 61153 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:16 UTC	4644	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 b8 05 3c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 01 05 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 e5 6c 84 80 01 4d 90 9a 8b 8b 24 44 00 01 a0 04 a4 04 81 82 19 20 68 64 13 94 63 6b e9 9c eb 86 33 05 85 c2 eb 78 2b 76 e4 89 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm<"lM$D hdck3x+v
2022-10-03 14:16:16 UTC	4660	IN	Data Raw: 1b db f0 99 18 2b 2b 5c 31 4a 8e 24 8f b2 02 cf 31 ad 93 73 0f 41 37 48 65 f4 90 7e aa d2 d0 ab ce c9 e0 bd 61 71 59 3f 86 97 aa 15 79 03 2a a8 32 b3 62 b2 cc 73 41 24 34 b6 d3 1a 16 4f f9 82 df 88 93 f0 16 00 64 97 40 b9 3e d7 06 54 54 92 08 d7 71 e7 fb b3 1c dc 8c 71 33 c8 b8 09 09 95 9a 3d df a7 bd da 06 77 05 8c 71 c9 ba 5d ac ea 98 dd 15 c2 8d f5 37 52 f8 8a 32 1b 14 91 48 9b cd 70 37 1e d0 6d 89 02 9a 04 6c 6e 10 42 b8 c0 45 03 03 d4 f5 ae d4 64 8e 9e f6 d5 3b fb d6 db 70 01 b5 31 bd d4 3e a9 37 4d 8d a8 de d2 dd dc 9e b4 b2 3f 52 55 91 f3 42 52 ad 84 9a 56 18 c2 b8 5e c0 a3 01 52 47 9a 58 8e ec d7 4f c6 fe b8 a1 b9 5b 15 27 94 d1 97 ca 6b 72 ed 34 b9 27 03 c8 bd d2 52 3a 54 98 da c4 74 5e a5 3e ee 82 53 9e be d0 0f dc 26 3d 83 f9 db 35 a4 f4 95 d7 Data Ascii: ++\1J$1sA7He~aqY?y*2bsA$4Od@>TTqq3=wq]7R2Hp7mlnBEd;p1>7M?RUBRV^RGXO['kr4'R:Tt^>S&=5
2022-10-03 14:16:16 UTC	4724	IN	Data Raw: a1 30 b2 4f 36 4f 91 86 7a 99 10 7c b6 41 74 4b 55 a4 c1 2b e8 95 34 33 bc e5 26 1b e9 4e 40 c9 c1 de 34 45 bd 36 3b 6e b5 a0 d3 ad d0 92 73 6a 68 de ba db 78 78 d0 d6 a3 a4 4a b7 95 35 19 c3 25 ec e5 4b fd 8d b1 46 5a 89 a9 81 93 57 90 2b e9 47 af e5 a4 c6 58 1d 4e 07 9d e8 45 f4 b6 f4 56 2a bb b4 35 fa 14 cb 49 7e b8 2d c2 fa 10 8d 7f 40 b3 c9 f7 e4 9a ed 1b a2 59 0a 17 3c a0 64 b2 dc 81 ce 5a 1c c7 dd d8 6d 88 6a 65 61 88 ee 51 2d 91 ad e5 f9 4e 4e 36 a6 97 51 c2 94 6b 0e c7 10 44 e1 a0 fd 96 e2 76 93 98 68 4f 51 d1 1c ea 10 d6 a6 a9 13 93 52 a8 b4 af 09 2a 0a 6d 9a f9 ef c8 1d 8d 2e dd f0 9e 44 0d cd 0a 22 38 5a e3 af 8b 41 e3 ad c4 4b 79 70 f8 7f 21 d9 86 c7 26 4d 69 2a 9a 4f c9 7a 9d f4 f9 1d da 46 b1 76 2a 68 f3 bc 05 81 48 d0 8a 72 a6 78 35 a7 2e Data Ascii: 0O6Oz|AtKU+43&N@4E6;nsjhxxJ5%KFZW+GXNEV*5I~-@Y<dZmjeaQ-NN6QkDvhOQR*m.D"8ZAKyp! &Mi*OzFv*hHrx5.

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:16 UTC	4740	IN	Data Raw: 0b 57 56 d1 7b 4c cc 9e 10 45 b2 0c 2a a2 ec 9c 01 da 93 fc 1f c0 47 a3 c2 78 f2 61 7d de a5 92 c8 e3 44 be d8 bc f3 2c 0d b7 0a 42 2d 80 d6 e2 3d 1c c7 52 8e 5b 96 89 b9 e5 2f ec a3 38 3b 58 db 11 3e 15 db b2 c8 9f e0 2e f0 44 21 c2 a0 a6 78 f0 6b 53 c5 46 b4 60 03 7a b2 61 22 c3 a4 51 14 61 1e d6 2a e0 e9 fd 40 9b 6a 9d e9 43 2c f8 34 6d 50 b1 02 4a 08 56 47 37 00 10 20 5e c1 4f 94 b4 f9 6c c1 ab 5b 12 56 96 ed 8f d4 b6 ef 9e f0 51 51 a7 bc 12 f4 f5 50 c0 96 e4 a5 e6 7d 67 bc 2a d6 92 9e ec 1a 3f cf 30 0a 3e 35 d0 f9 d9 02 eb 1c cb 35 b8 b0 33 01 50 c6 17 d3 12 8b e2 e5 68 bc ab 09 56 aa fb 95 49 67 86 b3 6b 16 20 dd c7 42 66 f0 5b c5 45 f1 48 d0 2e 60 c1 9c 60 45 f9 b8 14 d0 79 31 5f ee 6f 7c d0 29 a3 4d ca 25 4a e8 4a 94 75 a9 52 a5 75 b9 71 96 fc 8f Data Ascii: WV{LE*Gxa}D,B-=R[/8;X>.D!xkSF`za"Qa*@jC,4mPJVG7 ^Ol[VQQP}g*?0>553PhVIgk Bf[EH.``Ey1_o|)M %JJuRuq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.6	49911	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:17 UTC	4787	OUT	GET /wordpress/wp-content/themes/kawaken/images/ttl_recruit.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1
2022-10-03 14:16:17 UTC	4789	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:17 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:13 GMT ETag: "d83c-5b252e8011240" Accept-Ranges: bytes Content-Length: 55356 Connection: close Content-Type: image/svg+xml
2022-10-03 14:16:18 UTC	4821	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 38 39 2e 31 32 20 31 33 31 2e 31 32 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 65 61 65 61 65 61 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 34 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 39 2e 37 32 2c 38 39 2e 32 35 63 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 289.12 131.12"><defs><style>.cls-1{fill:#eaeaea;}</style></defs><title> 4</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M9.72,89.25c
2022-10-03 14:16:18 UTC	4837	IN	Data Raw: 63 2e 32 2c 30 2c 2e 32 37 2d 2e 31 31 2e 32 2d 2e 32 5a 4d 31 36 2e 33 35 2c 37 31 61 2e 32 38 2e 32 38 2c 30 2c 30 2c 30 2c 30 2d 2e 32 34 2e 33 37 41 2e 38 39 2e 38 39 2c 30 2c 30 2c 30 2c 30 2c 31 36 2e 33 35 2c 37 31 5a 6d 2e 32 35 2d 2e 33 37 61 2e 32 38 2e 32 38 2c 30 2c 30 2c 30 2c 30 2d 2e 32 35 2e 33 37 73 30 2d 2e 31 31 2e 31 32 2d 2e 31 38 53 31 36 2e 36 31 2c 37 30 2e 37 2c 31 36 2e 36 2c 37 30 2e 36 35 5a 6d 2d 2e 30 39 2c 32 32 2e 32 33 61 2e 33 31 2e 33 31 2c 30 2c 30 2c 30 2c 30 2d 2e 32 34 51 31 36 2e 33 39 2c 39 32 2e 36 37 2c 31 36 2e 35 31 2c 39 32 2e 38 38 5a 6d 2e 33 34 2d 2e 33 31 2d 2e 30 36 2d 2e 33 61 2e 32 34 2e 32 34 2c 30 2c 30 2c 30 2d 2e 31 31 2d 2e 31 34 76 2e 30 38 6c 2d 2e 30 36 2e 30 39 2e 30 37 2e 33 5a 6d 2e 37 31 2d 32 35 2e 33 38 2d Data Ascii: c.2,0,.27-.11.2-.2ZM16.35,71a.28.28,0,0,0-.24.37A.89.89,0,0,0,16.35,71Zm.25-.37a.28.28,0,0,0-.25.37s0-.11.12-.18S16.61,70.7,16.6,70.65Zm-.09,22.23a.31.31,0,0,0,0-.24Q16.39,92.67,16.51,92.88Zm.34-.31-.06-.3a.24.24,0,0,0-.11-.14v.08l-.06.09.07.3Zm.71-25.38-
2022-10-03 14:16:18 UTC	4867	IN	Data Raw: 2e 33 39 2c 32 2e 31 37 2c 32 2e 31 37 2c 30 2c 30 2c 30 2c 2e 36 38 2d 2e 35 37 71 33 2e 38 37 2d 34 2e 34 35 2c 36 2d 36 2e 35 36 6c 38 2d 38 2e 36 33 61 33 2e 36 37 2c 33 2e 36 37 2c 30 2c 30 2c 31 2c 31 2e 34 38 2d 2e 39 34 71 30 2d 2e 30 38 2e 31 35 2c 30 61 2e 31 38 2e 31 38 2c 30 2c 30 2c 31 2c 2e 31 33 2c 30 2c 2e 31 36 2e 31 36 2c 30 2c 30 2c 2e 31 32 2c 30 2c 2e 36 37 2e 36 37 2c 30 2c 30 2c 30 2c 2e 34 34 2e 31 39 2c 31 2e 31 39 2c 31 2e 31 39 2c 30 2c 30 2c 31 2c 2e 34 32 2e 31 32 63 2e 37 36 2e 31 31 2c 31 2e 30 38 2e 34 39 2c 31 2c 31 2e 31 35 61 34 2c 34 2c 30 2c 30 2c 31 2c 30 2c 31 2e 32 2c 33 2e 36 32 2c 33 2e 36 32 2c 30 2c 30 2c 30 2c 30 2d 2e 35 37 2c 31 2e 32 37 2c 33 2e 33 31 2c 33 2e 33 31 2c 30 2c 30 2c 31 2d 2e 35 32 2c 31 2e 31 Data Ascii: .39,2.17,2.17,0,0,0,.68-.57q3.87-4.45,6-6.56l8-8.63a3.67,3.67,0,0,1,1.48-.94q0-.08.15,0a.18.18,0,0,1,.13,0,.16.16,0,0,0,.12,0,.67.67,0,0,0,.44.19,1.19,1.19,0,0,1,.42.12c.76.11,1.08.49,1,1.15a4,4,0,0,1,0,1.2,3.62,3.62,0,0,0-.57,1.27,3.31,3.31,0,0,1-.52,1.1
2022-10-03 14:16:18 UTC	4883	IN	Data Raw: 38 32 2c 36 2e 36 35 2c 32 37 35 2e 30 35 2c 31 34 2c 32 37 30 2e 38 38 2c 32 30 2e 33 22 2f 3e 3c 70 6f 6c 79 67 6f 6e 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 70 6f 69 6e 74 73 3d 22 32 37 36 2e 38 20 31 33 2e 34 36 20 32 37 36 2e 38 20 31 33 2e 34 37 20 32 37 36 2e 38 34 20 31 33 2e 35 32 20 32 37 36 2e 38 20 31 33 2e 34 36 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 32 37 36 2c 31 34 2e 34 68 30 5a 22 2f 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 32 37 38 2e 33 31 2c 31 31 76 30 5a 22 2f 3e 3c 70 6f 6c 79 67 6f 6e 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 70 6f 69 6e 74 73 3d 22 32 38 32 2e 38 31 20 35 2e 35 31 20 32 38 32 2e 38 20 35 2e 35 32 20 32 38 32 2e 38 32 20 35 2e 35 Data Ascii: 82,6.65,275.05,14,270.88,20.3"/><polygon class="cls-1" points="276.8 13.46 276.8 13.47 276.84 13.52 276.8 13.46"/><path class="cls-1" d="M276,14.4h0Z"/><path class="cls-1" d="M278.31,11v0Z"/><polygon class="cls-1" points="282.81 5.51 282.8 5.52 282.82 5.5

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.6	49909	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:17 UTC	4788	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_mov.mp4 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" Accept-Encoding: identity;q=1, *;q=0 sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: video Referer: https://kawanakajima.co.jp/ Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1 Range: bytes=5636096-5683456 If-Range: "56b901-5b44268a46a00"
2022-10-03 14:16:17 UTC	4789	IN	HTTP/1.1 206 Partial Content Date: Mon, 03 Oct 2022 14:16:17 GMT Server: Apache Last-Modified: Tue, 17 Nov 2020 00:16:40 GMT ETag: "56b901-5b44268a46a00" Accept-Ranges: bytes Content-Length: 47361 Content-Range: bytes 5636096-5683456/5683457 Connection: close Content-Type: video/mp4
2022-10-03 14:16:18 UTC	4789	IN	Data Raw: aa e7 ea 48 38 c9 17 47 c0 a7 6c 16 c5 61 3f 56 de 85 2f 0f d0 60 64 f2 75 aa b7 89 b6 db 8f 9e c9 f3 81 76 5c d8 ab 66 d7 a2 ae 65 68 d5 5c b5 c9 d0 d1 5d 3e 4c d9 b2 7d 7f 81 ea 56 66 30 49 55 0d 46 5e d8 47 85 e8 26 a8 fa e4 96 7b 7b 89 85 27 86 e8 25 d7 92 b3 6a 6b ed 80 74 6d b9 d3 cc a6 b1 03 f9 26 32 41 da a3 83 0d 2b ab d8 ec b5 3b a6 74 8a b9 a1 1c c3 03 3b 51 8e d6 00 d3 95 ad d0 5e 8b 1a bf 25 9a 85 8c e4 aa fc 9c 3b a8 56 06 23 e6 66 ac 47 d8 9b e9 91 c1 81 05 ca 5b fc 54 bd 03 19 89 55 f5 9d 6c b0 1e 7c fb 03 0b 38 46 b4 08 51 e8 9b 00 34 57 ff f6 cc 13 22 6a ea 43 d9 7f d4 4d 03 4d e3 4f 92 43 b5 fa 8a e0 3c 5f 5a 56 f8 db 9d 67 79 77 6f 47 12 a3 a3 55 49 3e cb b2 98 b9 ae 91 f1 ef 44 b1 ea b2 c0 03 dd 9f cb 97 c7 a7 6f 46 57 97 b6 78 b8 d9 Data Ascii: H8Gla?V/`duv\feh\]>L}Vf0IUF^G&{{'%jktm&2A+;t;Q^%;V#fG[TUl|8FQ4W"jCMMOC<_ZVgywoGUI>DoFWx
2022-10-03 14:16:18 UTC	4805	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:20 UTC	4889	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_top_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:20 UTC	4890	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:20 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:08 GMT ETag: "f2fc-5b252e7b4c700" Accept-Ranges: bytes Content-Length: 62204 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:20 UTC	4890	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 03 84 04 b0 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 02 01 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 fa ea c1 02 80 b0 45 69 ca f3 f5 04 09 e7 f0 2c ca be cd 80 3c cb 77 2d e3 d3 d8 ee 62 b5 68 e5 dd dc ca 70 7c ea 7a 3e ef 33 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhm"Ei,<w-bhp|z>3
2022-10-03 14:16:20 UTC	4906	IN	Data Raw: ba 35 a3 5a 3c c3 59 ac c2 4b ea 44 78 ff 00 a3 c4 18 67 b0 f8 27 ee 17 b4 c4 7b be c1 f2 fd 67 95 6e 07 d4 ca dd 70 17 53 12 dc a4 54 e0 71 19 87 67 63 49 a0 91 21 94 ce c7 72 45 67 f5 32 44 4a 6f 64 43 82 b6 56 34 dc 71 68 50 6c f2 91 e5 40 54 e0 59 21 24 3d b2 b1 63 48 97 d2 4b 66 53 99 8b 96 99 27 fb 1a 94 52 7f 27 99 62 bc ed 21 54 e0 d6 6a 1c 8b b2 f9 dc b9 84 f7 22 3e d5 e9 bf b8 c4 18 61 f0 54 f7 11 e0 c4 7b be c1 f2 fd 76 54 e0 7c f5 32 b1 df aa 02 e3 ae 1c 94 f8 36 2a 8f 82 87 28 5c 67 22 59 40 8d ac 36 ae 36 ac 55 4e 47 91 26 2c 33 21 4e c4 0a c5 84 99 11 a2 c5 8b 22 d1 2c 98 d5 89 f6 13 43 91 2a a7 98 4a b5 90 b1 6e ff 00 27 99 a3 ea bf d2 cc 4c f5 d2 ba 7c 32 87 d5 16 8a 95 6d b0 9f 99 15 fb 0e 36 48 43 91 72 fd 58 4f 79 0f 6a fb a5 e8 e2 0c Data Ascii: 5Z<YKDxg'{gnpSTqgcl!rEg2DJodCV4qhPl@TY!$=cHKfS'R'b!Tj">aT{vT|26*(\g"Y@66UNG&,3!N",C*Jn'L |2m6HCrXOyj
2022-10-03 14:16:21 UTC	4955	IN	Data Raw: 8e 9a 97 cb e3 3e df e4 f9 1f 27 e5 3b 9f 27 63 b8 b8 27 ed 23 d4 b2 59 cf 82 3c 66 91 11 23 c3 6a ed a7 d0 79 33 b1 58 a2 4b a2 47 71 66 fa 9e 52 e5 ff 00 39 4b 26 c7 93 19 22 5c 13 e5 0f 66 5c b9 a8 4e c4 a5 b1 27 b0 d8 fa 25 c7 d9 77 c9 f0 70 ce c8 7b f4 77 3b 1c a2 db 74 fc e7 c9 46 7a 6a 45 fc 32 9c af bf ca 20 21 0d 97 c9 ac e1 bb 7d 33 8e 99 d8 59 ac 9a 3c 5a 9f d2 d9 f9 7a 3b 7f 93 e4 ee 76 3b e4 f9 47 cb 3b 13 e0 8f a7 31 71 92 17 04 4f 83 03 2d 35 50 f7 b1 7e b6 f3 aa 52 25 d0 c7 c8 b3 7d 4f 29 72 ff 00 91 8c 63 65 f3 68 91 27 b1 27 bf 4b 65 f7 1b df a2 f9 3f 4b b1 db aa e5 f3 91 17 93 cf b5 fd 45 d8 c0 d4 d7 4a 2c 80 8b ec 36 5c 4f 29 0c a6 fe a9 7f 02 e8 ae bb 8b 34 21 9e 29 0f e8 c8 97 0b a3 b7 f9 1f e6 3b 9d 8f 93 b0 f9 3b 3c a6 2f 4e 5d 84 Data Ascii: >';'c'#Y<f#jy3XKGqfR9K&"\f\N'%wp{w;tFzjE2 !}3Y<Zz;v;G;1qO-5P~R%}O)rceh"Ke?KEJ,6\O)4!);;</N]
2022-10-03 14:16:21 UTC	4971	IN	Data Raw: 40 eb 26 fd 92 ef 17 bd f1 d3 af bd b8 e5 a9 74 b7 7f c5 bb 2d ee df 9b a7 b6 5e fb 2d be 3f 92 9e 49 90 8d 97 8e e8 f2 23 a2 75 74 60 9f 8c e4 8b 3e f1 2f 7f 90 06 3c 63 cf ef 0f d8 31 a0 7a e8 fe c9 cb c9 9f e1 16 0e b0 84 3b af 97 d8 2e 8d 1d 78 de f7 0e 3d bf b8 8f 2f 87 f7 7f c6 22 de ae d3 a0 2c bb 3c 06 74 b6 22 2f 8e 03 13 db 32 de 1f 18 f5 bf 9b 5b 73 fc 16 61 f8 72 35 5f 63 87 f8 01 e7 11 cd eb fb bc ff 00 5c 06 d9 e2 f2 6f 9c 33 11 e7 2c c4 df e5 41 be 16 67 90 8f dc c8 78 18 b0 de ef be 81 ee d2 bb 2b ea de d7 12 d1 18 10 12 61 c3 68 65 d9 3c 36 bf 40 99 f3 97 94 be 0f a8 4a e6 6d 9d 67 0f 0d 8d af de ee d2 3d ba df c5 f3 3c fc 67 4f 67 d4 34 e1 e3 6e ed 98 1b df 53 fa 7c 43 af db ec 5b bd ad a5 fb 29 28 63 7a 03 d8 ac c3 14 3a df 47 ac 9b 0f Data Ascii: @&t-^-?!#ut`>/<c1z;.x=/",<t"/2[sar5_c\o3,Agx+ahe<6@Jmg=<gOg4nS|C[)(cz:G

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.6	49914	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:20 UTC	4890	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_company_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:20 UTC	4890	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:20 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:08 GMT ETag: "1344f-5b252e7b4c700" Accept-Ranges: bytes Content-Length: 78927 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:20 UTC	4922	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 03 84 04 4c 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 06 03 04 05 07 08 ff da 00 08 01 01 00 00 00 00 f4 c8 83 90 e4 04 80 6c 24 c0 90 e4 39 01 20 90 12 64 87 20 24 06 bf 24 0e 7e dc 9a c7 8f 43 7a 1c 8e c4 50 07 1b c0 ab f0 87 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmL"l$9 d $$~CzP

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:20 UTC	4938	IN	Data Raw: 85 43 f4 00 6d 2a 57 01 6b bb 8a c5 ab fd 32 a1 f6 ee 33 40 9d b9 34 6a 49 ee 35 0c cf 75 ee 9d be c0 2c 1b 0d 14 54 a6 67 8f bd 7b 75 fc aa 31 9c 36 fd d1 a9 f3 2b 5d 2f ea 1e e0 c0 4b 8d 80 51 0c ed 75 43 87 ba 72 37 90 54 d6 65 2b 2f b8 5c fe aa a6 67 54 55 99 0f c5 fb 22 ee d1 55 79 5c d8 da de f1 59 1a 1d 61 b9 a3 f5 51 46 09 cc fe eb 75 2a 47 17 3c df 7e cb 70 58 1e 1c 29 a1 e9 e4 1f 78 f1 b9 72 f5 97 b0 ba a8 63 2a 72 87 8d 1a 6e 13 63 63 45 80 55 33 c5 4b 1f 48 ff 00 f6 8e 6a 0a 69 27 95 b5 35 5f ec 8f e1 0a bb b3 2c 2f f9 26 9b b1 87 c0 26 ab fe 0c 77 9f c3 de ec a0 a3 ab 91 db 88 ce 20 a7 7b fd e3 a0 44 07 8b 15 94 fc f8 29 9a 5a 04 63 e6 b2 e4 62 fb 3d 87 7a 4c e6 79 3b 8c e7 cd 4f 52 f7 bb a2 11 16 e6 36 29 a1 ad 68 68 dd ea 39 eb ff 00 d2 d2 Data Ascii: Cm*Wk23@4jl5u,Tg{u16+]/KQuCr7Te+/\gTU"Uy\YaQFu*G<~pX)xrc*rnccEU3KHji'5_,/&&w {D)Zcb=zLy; OR6)hh9
2022-10-03 14:16:21 UTC	4984	IN	Data Raw: 95 df c1 61 d1 35 a1 ad 00 70 fd ba 9d e3 61 f3 5f 68 ea 84 b5 1d 00 3d 98 ff 00 74 73 03 62 57 d9 7a 2e 96 b1 d3 1d d1 8d 3c d1 db 8b d4 19 6b 1f c9 ba 04 4d 9a 4a 63 75 6b 7e 6a 77 5d e0 2c 0e 8c 43 4a cc d7 cd 2b b3 9f 20 8e 55 51 50 e2 e1 04 3a ca ed e7 e0 1c d4 14 f1 d3 b0 86 9d 4f 79 df 16 d7 1c ad 2e e4 0a a7 6e 58 1b f9 b5 d9 7b 93 b0 75 ab 9d 96 99 d6 f7 b4 4d 68 63 03 47 0d 3a a4 d9 4d 88 4d 33 fa 2a 32 3f 34 a7 87 92 a7 a3 6d 3d 37 40 1c 7c 4f 32 84 10 53 d3 c8 03 74 b6 aa bf 19 a6 a2 89 ad 88 87 c9 97 b2 de 01 51 d4 54 e2 18 a4 0e 94 dc 66 f9 0d 13 98 c7 f7 85 d4 b2 c3 0c 65 f2 3c 31 a1 62 7f 68 a4 94 ba 3a 63 92 3d d9 ad ab 93 dc fd e4 11 e2 51 a9 75 88 05 53 30 97 5c a8 80 ba 71 ff 00 15 0d bd d6 85 4f 23 cb 05 d5 d5 45 5c 34 cd cf 23 b7 fe Data Ascii: a5pa_h=tsbWz.<kMJcuk~jw],CJ+ UQP:Oy.nX{uMhcG:MM3*2?4m=7@|O2StQTfe<1bh:c=QuS0\qO#E\4#
2022-10-03 14:16:21 UTC	5000	IN	Data Raw: 59 bc ee ac 32 ab 35 be a5 3b 72 0f 32 d1 1e 83 76 d3 19 f2 68 7a 2d 7c b1 b0 f8 c4 77 69 5a 25 21 e5 da 1c 2b b3 2e 05 e4 28 27 66 3b b1 b5 5f 0d 0c 4d d4 a8 ef 37 cf 1b 95 62 df a1 28 40 c4 74 b6 bd c5 7d fa 3e 13 3e f6 c3 99 ba 2a f2 27 f1 0c 3b 68 08 f2 e0 d9 c0 45 da f5 f2 79 a2 08 b1 01 c6 89 78 f6 be a6 3a ba bf 81 8c 4b 86 dd 8c a9 de e1 18 6f a3 f9 9f f0 ff 00 61 e8 3f 29 a9 a9 a9 d6 4e 77 0c 44 56 dd 63 96 32 ad cb 41 97 d1 1c 45 ab 22 ac c2 84 d2 a2 83 fa 28 61 23 b5 3b 12 95 32 8b 16 a5 e4 62 b3 41 a6 a3 39 54 1c cd db be f6 af 94 6d 0d 2d cb 27 6a 1e e9 97 c6 f6 fb 45 56 85 47 a5 d4 61 a9 df 7e c1 03 7c 25 23 56 d4 67 31 1f 39 f0 c2 3a ac 57 e0 c4 b9 a7 6c 5f 6a 82 75 89 d9 ab d2 c7 57 57 f0 31 d7 6a ec be e7 9b 83 ab 0e a3 d6 ff 00 87 fb 0f Data Ascii: Y25;r2vhz-|wiZ%!+.('f;_M7b(@t}>>*';hEyx:Koa?)NwDVc2AE"(a#;2bA9Tm-'jEVGa~|%#Vg19:Wl_juWW1j
2022-10-03 14:16:21 UTC	5016	IN	Data Raw: 1b 7e a1 10 a7 3b b2 d7 72 f5 e2 14 2e 2d 18 19 9b df b4 26 1e f2 bf 03 d5 71 12 96 5e 62 48 ac 8f 32 a5 0d 86 c7 7d 0b 36 d9 82 33 29 84 b6 82 5e 80 d5 dc 45 ef 32 a1 88 1a 6f f0 4c 7d 27 41 3d ca ed 03 43 a1 ae 48 27 23 2a 07 46 27 a9 4f 26 95 bc 4b 61 1d b4 20 5d 1d d5 4b 1b 17 e6 5f 8b 2b f0 2e 31 db 45 81 2e 52 da 07 bd 12 8f 29 8e 83 a3 03 a8 de c8 56 f8 84 9e 30 62 dd e5 07 97 41 75 2a 12 1b 1b c6 50 38 e8 44 ec 05 10 f1 72 de 63 00 2d 5a 3d ad 4c 2d 08 b5 4d c7 10 e1 03 b3 95 8a 64 bc 54 af 62 71 33 d5 4c 9f 82 29 5e 58 60 09 17 44 0c 6a 45 bf 3a 6f 0a 89 2d 58 d9 77 b7 06 a3 9f 25 27 b6 77 06 07 96 9b 98 50 62 bd ee a1 1c 02 e2 6d 7e cf b5 c5 e2 14 16 be 4c c3 51 ea f7 30 3a b8 f5 92 95 0d 45 82 0f 8b 39 a6 08 9c ec 20 58 3e c0 37 87 8d 15 35 29 Data Ascii: ~;r.-&q^bH2}63)^E2oL}'A=CH'#*F'O&Ka]K_+.1E.R)V0bAu*P8Drc-Z=L-MdTbq3L)^X`DjE:o-Xw%'wPbm~ LQ0:E9 X>75)

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.6	49917	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:21 UTC	4954	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_mov.mp4 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" Accept-Encoding: identity;q=1, *;q=0 sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: video Referer: https://kawanakajima.co.jp/ Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1 Range: bytes=81920-5636095 If-Range: "56b901-5b44268a46a00"
2022-10-03 14:16:21 UTC	5029	IN	HTTP/1.1 206 Partial Content Date: Mon, 03 Oct 2022 14:16:21 GMT Server: Apache Last-Modified: Tue, 17 Nov 2020 00:16:40 GMT ETag: "56b901-5b44268a46a00" Accept-Ranges: bytes Content-Length: 5554176 Content-Range: bytes 81920-5636095/5683457 Connection: close Content-Type: video/mp4
2022-10-03 14:16:21 UTC	5030	IN	Data Raw: 1e a5 3b b0 00 53 83 78 0c 19 a6 90 59 5f f9 78 cf a4 4d cc 5a aa 6b 58 c5 8d 59 fc 6c 8a 77 90 98 b6 34 8a d1 6f a0 04 25 40 21 34 dc 8b 9e ad f7 d7 a6 df ce 10 79 d8 92 9d b2 b9 63 71 03 63 79 52 7e dd 1e 53 47 8b 53 af 4b 98 37 2f e2 1a 7f 8d 15 b3 a2 70 11 44 c4 24 21 77 43 b4 fa fb c6 6c 57 c8 4e b0 57 a4 24 af 6b 7a b4 93 75 56 d2 7b 7d 83 33 2a 11 63 3b db 7f 7e 35 d3 e3 5e 27 a1 0a a5 3b e1 1b 6a 3f 9c dc 67 9c 5e 83 8f 80 9e de ea fd ac 2c bd c1 53 a1 1e 75 69 2b 84 4e c8 a2 23 b1 5e 34 cc f7 2f 19 a8 0f 2d 46 be 59 67 05 ed 8f 93 07 bb 62 bb 40 db 15 17 88 7d 95 d9 57 f4 ce aa aa 29 5b 7c d2 75 0b 11 48 95 08 9a 36 66 13 a2 7c 79 1d e8 11 b8 95 e7 e9 5c c2 bf dd 43 ee a3 36 f6 c9 d9 a1 78 1e 09 55 f2 4b e6 5a 31 a4 9d f0 54 dc 7d 46 8f 15 d5 04 Data Ascii: ;SxY_xMZkXYlw4o%@!4ycqcyR~SGSK7/pD$!wClWNW$kzuV{}3*c;~5^';j?g^,Sui+N#^4/-FYgb@}W)[|uH6f| y\C6xUKZ1T}F

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:21 UTC	5046	IN	Data Raw: 3a a8 c5 a0 a3 ed b8 f3 df ba 7f cd d2 e8 b7 f0 f2 34 ff 02 e8 f3 95 f3 9d 51 d2 62 fc b8 a6 e3 4a 50 3c 50 e9 fe 78 63 49 65 6b 9c 88 9e 61 a5 4e a7 80 c0 68 a8 52 f5 86 55 f8 02 b3 fd 34 2e a9 87 73 ef ec 3a e6 6d 1b a0 ba b9 f5 e2 d3 69 ae 91 bd 64 97 78 5c 42 9b 01 0c 47 cc 55 33 0a b2 a0 99 73 2b 4b f5 a1 99 08 77 11 8d 06 24 9a 81 6d 0c 46 d9 e7 d6 6d ec da 59 fc 39 44 37 88 14 7c 53 d6 60 e4 b0 d2 1e 15 fb f0 d4 42 83 6b 70 f7 e7 ad 85 49 96 a1 6c e6 84 04 15 28 57 56 0e 6d 2a 8f 4c d7 ca a5 f7 d9 cb 40 e5 4c 6d b0 7d 4c ab 24 1c 14 06 7a 3b a4 cd 21 2e 35 4e fe d6 62 41 b1 59 82 6f f2 a9 95 c3 e7 3f 54 0b 70 78 cb 09 aa 33 5d a0 d2 30 a0 ff 3c 42 52 04 3a 87 0e 63 b6 d2 e1 61 2a 01 0d 36 cb 20 70 34 74 f9 ba ea 2b a6 e5 c1 31 29 26 04 08 25 f3 47 Data Ascii: :4QbJP<PxclekaNhRU4.s:midx\BGU3s+Kw$mFmY9D7\|S`BkpII(WVm*L@Lm}L$z;!.5NbAYo?Tpx3]0<BR:ca*6 p4t+1)&%G
2022-10-03 14:16:22 UTC	5062	IN	Data Raw: d5 1b 62 67 e4 a6 b0 a9 8d ca 2a 1e a5 75 bc 36 07 d2 2f b9 70 be 54 f5 1c c9 a3 56 32 57 66 b3 6d 99 0c 9a d0 75 e0 b3 c4 e0 a3 7f 3f 15 d3 56 7a d0 d4 01 78 cf ad 1f bc c6 1b a3 b8 9c 68 40 b5 0b 86 a3 35 01 4f 56 08 4d 71 ee c1 56 8a 8e df e3 67 a4 a6 70 7e 03 f0 41 68 47 2c 17 d7 e1 15 d1 d6 26 b6 dc 49 0d e0 5d 12 33 68 67 4b 06 0c 4e b2 2c 2c d5 e2 08 72 a5 46 ad 6d 12 dd bc 50 b4 32 15 92 07 e6 96 11 13 88 9a 73 ba 5d 01 41 e4 62 77 e9 d0 ad dd 9b 0f 1c aa 95 00 db d9 c7 61 87 46 94 ef c0 98 d0 01 19 f2 a3 cf 08 be e9 90 ce 5e 9a 4d 84 2b cf a4 d6 c4 ad f4 59 91 cf 92 5f 9a 4f 65 b8 6d 6e c8 b8 75 23 34 b1 56 63 a0 8f 29 ef 30 47 25 b8 ae f7 c4 48 c4 6e 91 c5 88 d8 58 37 b9 15 3a c5 c7 b8 9c d4 93 9f 63 fd 1c 09 e8 d2 d8 69 9e 8f e3 11 3d 25 3e 13 Data Ascii: bg*u6/pTV2Wfmu?Vzxh@5OVMqVgp~AhG,&I]3hgKN,,rFmP2s]AbwaF^M+Y_Oemnu#4Vc)0G%HnX7:ci=%>
2022-10-03 14:16:22 UTC	5078	IN	Data Raw: 5b 97 c9 32 37 6c 7a c5 82 d6 81 e7 4d 65 e1 86 50 9f 9b 7c 1d 5d 7a d7 fc fe 93 98 a2 b3 16 ed e4 b7 ee 97 a3 98 20 dd 61 9a 39 20 91 6e 43 fd 97 8d c1 17 bf 4b 92 52 3d 85 f0 f6 e5 05 06 fd 13 7a aa cc af 58 00 a2 8e 5b 6b 58 28 9b 22 69 55 69 52 c8 26 a4 28 78 84 7f 10 74 c6 9c 2e 67 34 c0 7b 23 39 f9 22 bc 51 a7 67 55 81 ff 6f 0d 1c de ac d5 66 8e be 5f be 31 a7 10 69 70 db af 0a a4 62 7e fb 81 04 cf 39 91 cb 2c 24 71 2a dc ec 88 9c 11 b7 82 28 42 08 b9 20 b7 0a 16 97 01 8c 0e 0c 5c 97 73 21 ab ab 17 fb a3 b1 a6 00 43 62 9e 9b f0 7a 4c ad 96 45 7b c5 d6 f0 b7 23 f5 38 4f 03 0e 07 8e fc 60 5a 86 cd 3f 41 2c c0 a8 cb 4c c6 5a db fd 65 d4 72 ce 54 d1 28 d4 7a de a3 98 bc 3a 3a 46 8b c6 59 2c 33 8f 3b 65 bd 2b 35 17 00 f3 a3 36 cd 4f 11 68 40 68 02 ee e5 Data Ascii: [27lzMeP|]z a9 nCKR=zX[kX("iUiR&(xt.g4{#9"QgUof_1ipb~9,$q*(B \s!CbzLE{#8O`Z?A,LZerT(z::FY,3;e+56Oh @h
2022-10-03 14:16:22 UTC	5094	IN	Data Raw: da 06 ef 54 7f 95 fb b5 1e 19 8e 62 d3 1a 9d bd d6 24 b6 a2 14 86 1e 81 f4 9c b3 08 40 a5 66 16 2b ff 3d 1d 13 da 9d 22 c6 2f 2f c3 a6 e4 0a d7 0e 4e 52 25 2f 56 3e 37 2e 46 a1 b2 65 0c 23 13 cc 3f f8 d3 fd 5d 65 8e d6 d8 70 2a db a9 23 4b be 14 13 8b 60 3e a4 45 a0 ca db a2 23 ba 56 4a cd 5c 85 2e 91 d3 ec c1 ab 7a d3 ff 2a 55 82 c6 54 be 99 84 03 55 34 dc 9a c2 96 14 0c f5 b0 93 d5 d2 d3 61 26 c3 8e c6 57 cf 48 00 f0 7c 0d 32 1c 8d a4 e1 21 1a dc 3f 1c cd 34 d8 fe ec e5 0b f9 43 9e d3 a6 61 cf 07 02 92 06 aa 97 60 d5 c5 30 46 77 8a d6 5f f9 10 b6 ea e2 3a c3 e4 48 8d e4 9f 70 b2 8a 4b 77 17 d6 ff 7b 21 ed 3f b5 b3 33 d8 3e 61 ba 09 f4 35 ad 1c 8c 52 fd 0a dd 75 e4 ef 9b 10 9d b1 b8 fd da 0c b0 f6 1f e9 89 57 87 ad 8f 56 ce 8b d6 64 aa 69 bd c2 bc 95 bf Data Ascii: Tb$@f+="//NR%/V>7.Fe#?]ep*#K`>E#VJ\.z*UTU4a&WH|2!?4Ca`0Fw_:HpKw{!?3>a5RuWVdi
2022-10-03 14:16:22 UTC	5110	IN	Data Raw: 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 79 00 00 02 b0 01 9f 0d 6a 4f ff 00 00 03 00 00 03 00 00 0f 26 38 e8 fc c5 47 ac 8a cc 74 50 a0 74 a3 72 3e 7c 0c cd 73 e5 61 0f 80 8a bd d5 35 6e 89 ac 96 d6 08 a1 0b d1 e9 02 c0 1c c7 16 a1 64 2e 3b 5d 44 87 d5 b7 6b 97 96 06 52 f3 49 f5 8b ad 75 ed 77 4a ca ae 09 1a 8f 9d 80 01 68 d0 d0 b3 91 05 cd ae c3 e9 78 6a 2b e5 05 ee 72 2e c0 08 0c 10 d3 4a 8e c9 5b 17 6a 48 fe d1 aa 0e 47 2b c0 88 a6 b8 78 3b d7 1f 0a 9b de fc 54 e3 16 73 5f fd 35 07 f1 34 b6 27 5b 26 2c c6 e9 68 f2 e7 57 2a 46 4f db a3 20 b8 18 8a b0 ea 5f e4 ad 9b 4f 14 92 cc 0e ed b8 de 69 6b ee f9 73 18 25 41 c4 22 00 b0 5d da a1 11 4c 8d 15 6c 7f cf c2 4f a4 9e 69 99 b5 53 7c c4 16 15 59 06 af 93 fd ed 59 Data Ascii: yjO&8GtPtr>|sa5nd.;]DkRIuwJhxj+r.J[jHG+x;Ts_54'[&,hW*FO _Oiks%A"]LlOiS|YY
2022-10-03 14:16:22 UTC	5126	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:22 UTC	5238	IN	Data Raw: 9c 94 a8 0d da 6e 57 aa 61 ae d5 04 62 64 88 1e 90 04 69 67 ec 8d 40 16 99 c3 11 80 2b 08 e4 5b 80 d5 65 cc 53 30 ee 93 cb fb bb 89 cd b2 47 c9 a7 43 91 c7 43 ec 95 19 18 aa 01 78 5c 6f 40 71 13 84 4a c4 e1 d7 eb 30 ac aa a8 e2 7a cc 4e 09 c0 7a fe 12 39 ed 1c c1 5b c8 2a a8 59 5c f6 57 12 53 0e b8 bc f1 f5 28 66 fd 77 ff 28 9f 32 88 46 84 25 fe 9e 7e 9a 0f 30 56 ee a7 1c 2a d2 72 9d 60 fe d5 0e db e3 4d d6 02 44 ec 43 1d bb ab 5e 66 5d e4 a1 de 03 6e 92 21 78 c6 94 65 ac 50 be e1 c0 bf 0e 7e 58 e4 25 f1 bd be de b2 11 b0 ec 5c a6 2c 5f 98 13 1a 74 ce 51 2c 49 cd 83 a5 ad 23 78 7a 1c a8 31 d9 c4 e4 ed 7f b7 c4 3d e6 05 dd 6e 72 55 ec e5 53 a5 23 69 ae fa 39 48 7a 63 55 92 b7 2b 85 c3 78 0a 1d 63 28 d3 88 c2 bf b7 1e b4 8d ad 13 42 7b b2 e0 28 d3 b5 4a 25 Data Ascii: nWabdig@+[eS0GCCx\o@qJ0zNz9[*Y\WS(fw(2F%~0V*r`MDC^f]n!xeP~X%\,_tQ,I#xz1=nrUS#i9HzcU+xc(B{(J%
2022-10-03 14:16:22 UTC	5254	IN	Data Raw: 15 9a d9 96 5f 92 ba b5 8c 03 4e 01 94 b1 c5 a8 9e 11 0e af 3e 34 9b dc 1f ee 59 a9 41 49 b7 7d 5b e3 3d e1 3f 77 2a d1 25 de 7d 38 27 8d 6e 61 b0 4c 95 85 dc eb 92 9d de 2d 61 7c 95 6c 1f 06 00 71 b6 9f d6 57 10 57 4b 29 0c 31 05 09 37 ee 9e bd 60 9a 65 e2 1c 66 0e 4e ea 55 5f e7 8c 25 ef 94 ff f0 11 2a ec 1b a8 76 5a 23 3e d4 b0 35 3a 1e cd aa 69 20 15 ce 08 4f 25 99 30 94 4f 70 ba f7 23 98 58 bf d3 a2 3d b6 d6 a8 e6 da 41 2c cd 29 e1 a8 97 97 35 47 fb 72 55 92 1f 56 ec 5a 6d 7a a8 dc a9 2b 04 84 9d 2d 6e 6c 6f b1 e0 31 eb 34 2d ac be 06 aa 18 1f f2 88 65 15 08 4d d0 32 a2 82 1e 8a 32 23 8c d4 62 71 fb 8d d9 21 d8 3a 5d e8 9d a1 69 ea bf 07 d4 89 44 cc 3b 67 a5 31 90 25 75 9b ae d1 c8 6b a9 6d be 06 d6 0d ba 99 03 c9 c8 01 20 1b 2e 73 f9 9a 16 86 d2 7b Data Ascii: _N>4YAI}[=?w*%}8'naL-a|qWWK)17`efNU_%*vZ#>5:i O%0Op#X=A,)5GrUVZmz+-nlo14-eM22#bq!:]iD;g 1%ukm .s{
2022-10-03 14:16:22 UTC	5270	IN	Data Raw: 8c 6b b4 cb 7b 88 10 5f cb 28 d0 08 21 a0 f8 da e9 9b 1f 7a c8 b3 eb 1c 23 27 44 05 b9 9a 89 5c 24 e2 f9 e6 a2 92 06 84 df 32 16 69 40 cf 84 a8 28 78 da 39 e9 61 bb ed c4 72 c9 a9 ad 6d 49 84 d9 56 66 f9 60 29 9f 6b fc 1b 24 ec b6 fe ea e9 c2 3e 87 bb d0 8a be c3 61 af fc 33 47 69 a5 4b b5 59 61 38 51 c9 b0 6e cd 49 ea 41 14 15 4e e0 af 8d ed a5 6e d3 6a 35 19 98 83 a5 d6 2e 08 75 65 6c 59 c0 5f 65 ad a3 1d a3 73 55 41 c4 1b 74 bb 67 63 5a 52 2e b8 ea 73 bf ce 85 ff 04 53 9f d9 b5 7b 7b ca d8 e0 6f 6b e4 ff 47 34 e9 4e 67 a2 80 bb 02 4d a5 04 a7 af 25 77 36 92 30 06 ef 77 bf 05 8e 02 88 19 30 eb db c9 02 5a 3c 9b 52 34 00 8b ce 8f ed 91 8d 78 fa fa 62 78 1e 6d 80 4d 94 a1 a6 d4 25 4d 34 7e 8f e2 f4 9f ed 0f 62 34 8a ba 89 b1 f4 32 54 7a 60 0a bb 6e 5a bf Data Ascii: k{_(!z#'D\$2i@(x9armIVf`)k$>a3GiKYa8QnIANnj5.uelY_esUAtgcZR.sS{{okG4NgM%w60w0Z<R4xbxmM%M 4~b42Tz`nZ
2022-10-03 14:16:22 UTC	5286	IN	Data Raw: 7b 3b e7 c7 b6 f2 d5 18 ae a1 6b a4 0c 52 be 28 5b 2a 6d 2d 71 d3 63 dd a4 14 fc 1d df 29 e2 5d b5 fb ef 1e 42 f5 11 f6 de 30 8d 0f b0 65 47 c7 b2 99 ae df 40 62 2b 40 c2 16 2d 31 75 3a 56 8c ba e8 ff d9 0a b1 5e 51 66 74 cf 97 67 93 3b 7f 97 bc 17 d1 ef 3b 46 18 19 80 93 89 ef 78 3c 56 61 97 a9 d1 af 12 87 17 e5 23 a4 f8 2f e8 17 7d 2d 4c f4 94 40 9f 48 a3 9a cf 29 97 f6 c6 72 0a d9 08 54 78 0e 44 7e d7 0f bf 48 24 3b d4 73 d6 c8 aa 29 9c cd 8a 25 50 5d 0f 79 d6 1f c0 f0 f2 98 f3 a9 27 b6 8e 43 d5 21 c0 1a d0 1d b5 e9 a0 bd 51 9a b7 e3 1d ef 8a 33 4e 1e cb 81 5d 0e 46 59 df 8f 1a 0c 62 9e c5 2d 61 1c c0 bb a9 f0 34 49 2f 7b 82 3a 1d d1 3b 7a 4c 45 5a 58 ed e0 33 9e 81 db c6 6c 02 93 c3 de 4d e1 55 4a df 36 e0 1b b9 c5 1a 7e f1 84 ec 64 8d d5 84 72 ca 88 Data Ascii: {;kR([*m-qc)]B0eG@b+@-1u:V^Qftg;;Fx<Va#/}-L@H)rTxD~H$;s)%P]y'C!Q3N]FYb-a4l/{::zLEZX3lMUJ6~dr
2022-10-03 14:16:22 UTC	5302	IN	Data Raw: 10 38 29 37 ee 9f 5e ff 3d 4c e3 ab 33 76 6b bc 40 66 55 54 00 33 83 76 1f 22 fe f2 d5 d0 1d 97 e6 d3 30 ec 63 9a 04 9e 88 2c 3f ed 5a 71 be 99 f9 08 58 6a df 3a 63 6c cb 81 25 7e 08 82 a8 04 50 0e a3 7f ec ac 13 63 dd 1a 05 0c bb b9 30 a5 c8 84 e4 2d 25 82 e6 cb ae 9f a2 09 ea 59 e9 ca 79 0a 34 11 4f 04 95 f1 34 84 ba 59 df 11 e0 d5 c8 74 b3 34 bf 97 35 70 b6 d3 d9 6c 7c 33 56 03 07 1d 6f 9a 49 27 66 c3 db b5 b6 18 db 1c 9d 06 50 6a 5d 2e 28 43 83 72 73 af bd 0b 5a 90 b5 3c dd 51 0b 05 3c d0 38 9f e6 bc 6f 96 27 4d 48 cc 2e 63 6c e1 b0 d8 69 6e a9 61 fb 96 41 5d f6 fb fe 99 35 ad 10 f3 09 64 2b 76 b4 a1 c5 bc cf eb 56 9e f8 de a1 d8 65 ea 98 cb 1f 94 44 bd 94 d1 5f 00 13 fb e0 cb 56 e2 3e cc 8f a5 7f ce e3 69 1c 5d f0 c2 47 38 72 dc 97 e3 de ee 06 db c9 Data Ascii: 8)7^=L3vk@fUT3v"0c,?ZqXj:cl%~Pc0-%Yy4O4Yt45pl|3VoI'fPj].(CrsZ<Q<8o'MH.clinaA]5d+vVeD_V>i]G8r
2022-10-03 14:16:22 UTC	5318	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:22 UTC	5398	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	5590	IN	Data Raw: 83 0f 31 ae d5 10 b9 8a 8d e7 90 f8 a5 4b b1 77 20 72 c5 a0 f2 a5 15 1e 93 bc 9f 73 f8 aa b4 d2 e6 83 b3 72 6b 37 7d 81 d8 b5 4b 27 be 2f ab fd 3f d7 5f e9 a5 5e 39 81 a1 63 87 9b c8 6e cd e1 b2 72 4f 74 6a e7 b9 64 39 4e bc b3 7d 35 30 a7 b4 8a 42 c2 55 80 c0 4b 88 db c1 7d 6f 19 77 8a 47 4f fc 8d 22 4a 4d 11 86 30 26 81 03 0e 82 66 61 cf 75 5f d5 6a 04 69 3b f8 be 00 b9 14 2b 02 b1 1f 14 4e 3b 07 16 f5 8e a7 25 90 56 ad 10 12 c7 58 ca 43 ab b1 c6 c9 55 06 5d f2 f3 82 01 b9 69 e5 9f 3e 72 f1 78 bf b3 67 4b 7a 21 6d 57 81 15 d2 0f c0 94 ed 62 15 f4 50 31 ab 5f 2d a3 5e 36 b1 32 dd 15 62 1c 87 e6 87 9f d1 b4 1c 83 b5 8b d9 b9 2e eb 41 3f 87 08 33 f8 4a af cb 0a b4 6b 5d 56 d5 33 ef 04 a7 48 b5 1b 95 d6 ae 98 25 a3 08 be f4 56 d8 5e 19 40 96 ae be 2b c3 68 Data Ascii: 1Kw rsrk7}K'/?_^9cnrOtjd9N}50BUK}owGO"JM0&fau_ji;+N;%VXCU]i>rxgKz!mWbP1_-^62b.A?3Jk]V3H% V^@+h
2022-10-03 14:16:23 UTC	5606	IN	Data Raw: fb 59 09 26 fb 4c 85 26 83 82 90 d4 78 f1 bd 41 2e ef 1a 01 37 7c 1e a8 63 4a ca 28 c7 09 08 69 55 f3 69 13 74 d6 0e b9 8c 76 b4 8b 5f 12 4c 29 94 e3 be 60 51 70 30 44 f7 16 46 3a be b8 6a 33 f4 54 cd 2e ab ba 3b 67 f6 78 99 21 8e 93 70 b2 5a 9e 34 13 3a 22 99 05 a8 65 f5 f2 b5 67 45 26 a0 6f b1 14 ea 38 17 3f f4 9d 43 78 ff 3a 0a 87 8a 92 19 80 99 db 4d 6f 93 01 13 8b 58 7b ce 7b 2c 4c 21 65 42 f4 9e 63 23 21 d0 af 78 0a dc 49 17 d2 c5 b2 a4 31 5b cc 3b eb aa 5b 5c e4 47 6e d6 8d b9 9c 8b ca 1d c5 92 c3 9f 96 1e 94 5f 49 b9 b5 ad 33 66 b6 84 b0 71 c9 4d 70 0b 55 40 f1 69 27 2c c9 b0 06 ee 18 b5 fa 6d 9a 0f a2 37 3c 26 24 23 6d 8f 3a cb c3 b7 23 f6 14 96 3a 9b 7b ca 74 db 3d 39 e4 95 90 b6 41 20 07 d4 6e 49 da 4c 18 37 e5 4c eb eb 95 0a 5b 82 14 07 08 c3 Data Ascii: Y&L&xA.7|cJ(iUitv_L)`Qp0DF:j3T.:gx!pZ4:"egE&o8?Cx:MoX{{,L!eBc#!xI1[;[\Gn_I3fqMpU@i',m7<&$#m:#:{t=9A nIL7L[
2022-10-03 14:16:23 UTC	5622	IN	Data Raw: 5d c1 7f 00 d6 9c fb 1c 56 c1 e7 51 e2 1a f5 3d 2c 95 f2 57 f0 da 66 50 27 91 83 3b 4b 2e 28 71 2a 9a d3 3c 2e c7 8c c0 48 8d 0f 50 f2 05 25 c5 81 67 d4 33 ca 6e 63 81 9d 16 37 ff 84 01 27 a8 d4 db af b6 61 1d be 98 49 88 56 ef a0 d9 bd 39 77 cd 31 6c 23 97 08 60 14 ed c1 a2 4e c3 1f 84 c3 39 b8 c7 58 83 5d 78 86 ca 1b 05 b3 e0 ae 35 c0 ac fc fd 0c 56 95 cd 40 56 d7 e8 13 6b 4b 50 30 5f f4 1d 95 24 44 af 96 8f 4c 55 f3 3e 92 3c ba 2b d4 d5 71 59 03 2a 8e c5 7e 84 2b 2c f7 5f b4 bf 3b 65 cf 67 3f 86 ab 3f d0 9b 7e be 7e 1f b8 42 63 28 64 32 cd be 71 22 4b 36 c3 3c 43 cf f7 76 97 68 23 7f 8e ae be 93 ce 24 b2 cf ff 5f 62 01 c4 55 ce 2c 02 29 57 15 3d 8f 55 94 3a d6 f1 83 92 fe 78 b3 41 db bd f6 75 92 7c 20 c0 38 ed 03 84 52 f4 7d 1d a2 9d 4a 7f 92 63 2c ac Data Ascii:]VQ=,WfP';K.(q*<.HP%g3nc7'aIV9w1I#`N9X]x5V@VkKP0_$DLU><+qY*~+,_;eg??~~Bc(d2q"K6<Cvh#$_bU ,)W=U:xAu| 8R}Jc,
2022-10-03 14:16:23 UTC	5638	IN	Data Raw: c3 3e 00 d9 dc 4f 9b 22 4f a8 aa 64 6a 1d 7a de 8e 9e c4 07 fc 6d 93 2b 52 96 a7 7d a7 de 31 e9 c3 76 f6 f9 db a9 74 56 ff b8 c0 04 15 5c b6 47 43 d9 23 a8 ae f2 22 fc c2 84 96 4d 8e c7 1d d2 9c 50 80 0e 48 47 03 a9 f8 8c ab 5b ff 83 0e ad f1 89 db cd ac 21 2f 9e d9 44 f7 e6 6c 0e bc 5d b3 57 47 61 77 c8 5d a8 0c 93 88 9d cd 83 7d 02 a8 0c f6 79 d5 4c 8e 08 38 f0 23 49 60 ac 95 94 4c e7 1b 09 a6 dc 31 43 f8 75 93 9f f2 2d d7 58 45 9d 59 67 56 cc 0d 74 73 89 8c 0f b5 df 17 57 b0 55 6c 10 f8 30 56 8b c4 32 c6 15 70 b8 71 86 61 54 87 2a 17 8f a7 55 81 e6 80 fb 04 ae 46 ed 80 de bf 4e 51 79 a6 b2 2c 51 12 4a b9 04 58 a1 f3 87 b2 a7 76 34 c5 e9 45 d8 fd f0 4e d5 8e e9 6f 37 07 d4 02 8b d2 20 c6 4a 42 42 4f 63 a2 47 76 66 4f be f0 ad 3d fe fe 23 2d 99 c2 47 75 Data Ascii: >O"Odjzm+R}1vtV\GC#"MPHG[!/Dl]WGaw]}yL8#l`L1Cu-XEYgVtsWUl0V2pqaT*UFNQy,QJXv4ENo7 JBBOcGvfO=#-Gu
2022-10-03 14:16:23 UTC	5718	IN	Data Raw: b0 ec 7d 88 a9 0d ce 6d 05 08 86 25 b9 e1 51 d1 9c 8e eb 8e a9 f9 00 fc 4f 94 bc 60 ff 74 71 74 4a 6c ab 33 bb 9a 53 37 c0 0f 37 de 6d 8e f9 cf c6 97 cc de 4e 67 ff c7 98 e8 11 59 6f 44 cb 7c fe b9 5a 24 b7 4b 36 15 1d 06 60 df 5e 21 6f 74 e0 53 2e 42 09 21 f8 5c a4 3b e7 2e 16 4c 17 cb 05 6b 1a d6 16 11 ff 66 6f d5 10 70 fa a8 57 5c b6 ad 52 d6 57 ee b0 db 62 81 12 00 38 8f 07 59 04 76 98 05 f9 b8 7f 1e 98 e7 3b 5f af 73 93 6c 6e ab 0e e0 ed 2e cb 5d 43 21 24 c1 23 b9 82 a0 5f f2 66 6f 4c 2f 97 d8 b3 56 56 4e 39 b1 82 8d 22 24 23 27 14 6f bf ab cc eb 2d 98 b0 81 a0 f0 08 1c c6 60 69 c8 99 1e 44 09 73 54 ea 86 3c 48 87 75 18 27 8f b2 94 db 9c 35 8d 73 5b 7a 72 c7 c2 25 32 94 a9 ec 1d 78 11 37 e8 45 4c 65 b2 d9 d4 0b 14 36 ec 04 25 fd cc 73 f3 58 20 46 01 Data Ascii: }m%QO`tqtJl3S77mNgYoD|Z$K6`^!otS.B!\;.LkfopW\RWb8Yv;_sln.]C!$#_foL/VVN9"$#'o-`iDsT<Hu'5s [zr%2x7ELe6%sX F
2022-10-03 14:16:23 UTC	5734	IN	Data Raw: b7 11 02 54 21 88 17 99 72 f1 11 04 29 ad fb a1 1b 24 0e 00 0b ff 27 4a 69 e2 09 e5 20 e0 5e d2 07 42 92 61 77 63 98 61 a6 3e 0f 02 10 11 07 08 11 cc 36 57 12 c9 63 11 5c ad 35 6e 4f b7 33 f2 bb 75 a7 7b 63 61 e1 cc 27 7b e9 0a e9 a0 22 b8 d3 11 da 18 51 da b6 19 ff ca 82 7e 07 c5 a4 4b b3 3c f4 ad 4f 8f fa 6c 09 0a a9 db a0 dc 1f 08 f9 72 30 d8 f6 19 b6 9a 02 f3 d5 49 46 f8 67 e7 fb 2a 3d 36 04 25 49 55 fb 9d 76 a6 1d 1b 9d 8e f6 29 6e d4 4f d1 34 75 68 b2 e7 4b 17 20 a4 4b 0e 28 b5 bd 8b f8 94 73 4e bf 8b 32 b6 7c b8 32 da ef 38 0f 6d b6 fa 93 48 11 89 89 28 fa 48 86 f1 9b 26 6d 1e fd cc 83 03 86 1c 25 44 e5 33 50 dc 62 e4 0b 68 13 72 52 62 b5 ea 62 96 40 c1 d5 08 32 6b 94 9b da 0c 88 76 59 9b a6 c7 c2 66 3a 83 80 69 ba bd 3d 50 bc 43 18 10 74 99 dc 88 Data Ascii: T!r)$'Ji ^Bawca>6Wc\5nO3u{ca'{"Q~K<Olr0IFg*=6%IUv)nO4uhK K(sN2|28mH(H&m%D3PbhrRbb@2kvYf: i=PCt
2022-10-03 14:16:23 UTC	5764	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	5812	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	5972	IN	Data Raw: 24 bd a5 69 7f 48 31 11 64 c6 7f de 84 9f 5a 86 a3 d3 dd 81 76 21 12 54 62 0c 8f a1 d9 74 68 72 13 70 e6 6e d5 2a 14 c3 b8 51 26 24 33 fd 78 4f 8d bb 6d 38 4e 24 4e 20 96 30 7d a7 8b ca 01 92 ca 3f 96 42 6f a9 46 15 1a f8 69 14 88 0e f3 60 02 f5 b8 8d ea ab 97 b8 b5 d7 e9 8a 0a 90 0b 49 ef 45 b4 9c c3 dc 5f 37 03 72 a5 33 d7 61 23 30 a8 68 d5 8a e1 b1 47 10 a6 e4 04 bb ee ae 9f 6a 24 ce c5 b7 0f 3d ad 05 cc d0 6f 98 5d 6f a0 ff 20 f6 7c 10 dd ff 09 96 df a2 d0 e9 c9 1e f2 82 1d a3 8a 9a 06 64 0e 22 da a1 b0 75 e3 b2 c8 e1 89 3a 11 f9 6f 15 2d 7c 09 0d a6 f4 a6 a7 d1 24 cf 43 93 53 27 3e 62 78 d7 d5 2a 2e bd 44 60 09 d1 e2 e9 1d 4d 6b 68 17 37 32 86 c3 59 76 18 02 aa 93 f8 19 b2 d2 db 5c 27 f0 14 50 7b 98 5c bd 17 2b a0 58 39 42 c6 10 19 46 67 a0 43 ab 5f Data Ascii: $iH1dZv!Tbthrpn*Q&$3xOm8N$N 0}?BoFi`IE_7r3a#0hGj$=o]o \|d"u:o-\|$CS'>bx*.D`Mkh72Yv\'P{\+X9BFgC_
2022-10-03 14:16:23 UTC	5988	IN	Data Raw: a9 5e a9 cf c7 ed 69 5c ff de 6d 10 a4 b7 d8 74 c6 1c 80 8d 9d c3 e2 88 f1 fa d3 b8 25 b7 43 58 69 95 9d 2e 94 17 11 2f ee e9 4f 85 2f 24 c4 16 1a 64 88 d7 19 f4 6e 46 ce 11 c4 f3 cc e6 7b 0c a6 cb 96 a5 cb 1f 7d b9 85 d2 2b f0 5e ec 16 61 a4 c8 61 ee c7 96 57 24 89 ae 15 8a 4b 62 16 27 48 c2 35 ea b3 83 36 80 61 72 0e fc bd 4f b5 bf bd 01 7e 1e 1a 09 61 35 39 21 a1 77 27 92 af 8f a1 c1 42 b4 80 62 88 9f 38 71 60 7b 7d 9a 93 64 e1 54 9b 48 67 50 74 b6 3e 2c 25 5e fc 3d 1b da f0 ce 06 f3 31 cb 30 85 d7 b3 3a e3 19 4f 9a c6 d9 d3 31 98 82 0c 11 d1 99 c9 59 d8 7e 96 d4 99 80 77 b7 42 14 7e 79 17 f4 5b 17 6a 39 73 c3 17 bd eb f7 a6 5d 6d a3 fc 4f 0b 8b f5 66 13 84 d8 25 cc 5d 67 ee 9e 28 a0 cd 87 b5 94 33 f3 c4 2a 76 0c 18 5b 3c 9f 35 85 e8 c2 f8 62 40 fe 20 Data Ascii: ^i\mt%CXi./O/$dnF{}+^aaW$Kb'H56arO~a59!w'Bb8q`{}dTHgPt>,%^=10:O1Y~wB~y[j9s]mOf%]g(3*v[<5b@
2022-10-03 14:16:23 UTC	6004	IN	Data Raw: 32 9e bb b3 79 dd 52 a5 47 12 1e ff 29 ea e1 27 13 6a 9b 81 19 72 c4 ba f7 7b d0 07 f7 fd 9c f3 41 82 b3 5b f3 71 d0 a8 38 a7 0a d0 55 de dd 17 27 3b b4 51 25 f5 2d 04 77 60 01 92 f1 f7 e0 d3 54 58 44 c7 fe 07 c7 63 fc ff f9 d1 c0 2a 56 b4 a3 cc b3 8c fc f7 d2 4c f1 f6 ba 40 72 3b 2a c1 51 00 14 b2 ce 59 97 e0 c1 a8 ca 61 13 f5 a2 eb 63 93 51 42 ac 9a c3 42 6f 17 48 ea 01 3a a1 26 12 13 52 9f 2e 34 bd 13 73 9c 60 c0 5e 13 65 55 6d 8c 86 2b 65 3c 60 bb 37 91 b1 5d e8 cc b6 39 e0 bb 4f 20 74 c3 b5 5f 98 8a 4c f5 b1 68 f6 48 9f bd 58 71 c0 b5 d2 54 7a d4 d4 15 78 57 ee 88 f9 3f c3 5b 95 b1 99 ba 93 09 61 25 bb b2 e5 f6 ce b9 44 e3 5f 9e ee 05 e1 b4 9d c7 ab de 3c d9 ae 4a 9b fd 65 da ad 4b be c9 cf ff 44 31 62 a4 b0 05 7b b8 58 05 2a 80 c7 e8 c1 0d 16 86 1d Data Ascii: 2yRG)'jr{A[q8U';Q%-w`TXDc*VL@r;*QYacQBBoH:&R.4s`^eUm+e<`7]9O t_LhHXqTzxW?[a%D_<JeKD1b{X*
2022-10-03 14:16:23 UTC	6020	IN	Data Raw: b1 16 2f 63 e1 ef 9d b2 14 c9 f9 5f 7f 18 eb ed e4 e5 7a cd da c2 c1 27 75 93 7a ed 43 03 c9 58 8d 32 84 63 1c 4b 40 62 55 cd f1 98 09 75 60 af c3 82 62 1a a0 01 c4 95 71 1b bd 2c a4 f9 f6 87 f8 6d 15 40 8e b0 73 bd fe aa 6b 3c f2 89 e0 f9 1a 62 d0 54 ac 29 9c 61 49 12 3e 7c 74 b0 be 95 ab 0d 2d e7 4c 63 cd 34 24 a9 fd 76 af 8d 7f 47 15 bf b5 0e a9 25 2d 76 b8 26 0f 1a 5c 69 70 6b e7 29 03 87 83 ba 17 23 d3 6e 49 c5 5b 48 48 16 c1 7a 49 e8 ca 98 70 7a d9 8f 47 20 62 22 78 76 c8 10 6d a9 fd c1 ab 1b b8 65 0d f8 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6132	IN	Data Raw: 3f 80 35 cf 9d 22 0a 00 a3 87 a3 b4 6c e6 9b 93 27 ee 9f 37 7f ae da 65 4a 71 22 f3 74 d2 45 98 d7 fc 07 37 5d d7 de bf 0a f6 90 ce 5e 63 2e eb 52 74 ad 02 2e 90 db f7 ea 37 39 22 d6 f8 b5 e3 ee 13 b9 41 a3 f7 27 18 72 b9 6a 8f 83 58 6b 50 f2 17 98 46 93 1f 41 28 dc 55 d7 e0 e1 5d ec a6 f7 d3 31 18 83 35 9a 54 e2 fe d9 89 b6 3b 8f b6 1b 9b e9 db fb fa 8b 76 c8 af 7b b1 d0 b3 71 5e 31 38 b1 9a 74 d4 89 c1 33 84 b1 5f c5 8c 2f 38 da 36 56 89 b7 fd c4 8c 55 ee b2 fc 8f 45 0c 63 81 a3 18 69 4c bf 5a 96 2d 8b 27 7a ba 0a 85 eb c6 8d 87 22 d7 47 05 a7 2a a4 c5 da 8a 6d f5 8c 65 eb 41 60 33 ef da 09 b0 f3 80 28 e7 5e 6f 5b 11 e2 f6 28 05 a2 c7 38 95 d3 ec 44 f7 bb 0a 87 e0 34 ef 53 f5 ed 08 da 73 f5 1e ae 38 2c c8 d7 5e 42 ee 78 2d db f9 cc b3 53 ed ab af 08 27 Data Ascii: ?5"l'7eJq"tE7]^c.Rt.79"A'rjXkPFA(U]15T;v{q^18t3_/86VUEciLZ-'z"G*meA`3(^o[(8D4Ss8,^Bx-S'
2022-10-03 14:16:23 UTC	6148	IN	Data Raw: d8 88 68 3c 6c f5 98 5f 0c 23 26 b5 e3 6f 59 53 5c 31 87 cb ea 29 66 80 4d 63 10 c7 1a bd 34 a1 28 0b bf 58 71 b0 5d 96 62 57 34 80 30 b7 22 7e 4b 5c 81 ba bf dc 28 8c 94 5f 12 2b e6 bb ba 6b 90 8a 4e 46 6d cd ac 69 ed e0 52 b3 97 9e 58 af aa b2 61 ee 7f 25 91 c6 e1 98 e9 d8 d6 81 4b 8a f9 db 69 2b ed ec 07 91 20 9e d1 61 53 e8 0d df 8e 72 9c 56 6f f4 59 8e 2d 19 6e fc 51 43 33 00 56 dd 06 32 71 f4 2e c5 a9 f6 90 c5 82 14 17 bf 79 a9 c6 fd 94 f3 1a 1e 16 04 5a 0a 46 8e d0 ce 39 99 79 26 8e 68 ed f4 f7 d9 b7 20 e5 c3 d1 9f df 58 62 c1 3a 24 85 c0 38 09 be bf b4 47 02 13 57 f2 74 44 bc bf b1 7f b7 83 62 ea fb a5 ac 08 0b 57 8e 48 76 ec f9 7b 1b 0d 12 bf 05 8b 85 7f 26 b0 8f f6 34 df 76 15 16 f9 a5 39 dc ef 96 bf e4 9b d0 e8 c1 9f 1f d2 a3 c4 4f ed 0c 52 97 Data Ascii: h<l_#&oYS\1)fMc4(Xq]bW40"~K\(_+kNFmiRXa%Ki+ aSrVoY-nQC3V2q.yZF9y&h Xb:$8GWtDbWHv{&4v9OR
2022-10-03 14:16:23 UTC	6164	IN	Data Raw: 8f 59 2b 92 08 b7 7b 85 e1 fb 83 84 af e4 33 b3 75 80 00 e0 56 e0 e1 8b 12 5b a4 54 28 66 79 5d ec 76 7c 87 90 82 45 bd db 73 e1 2e 29 b0 6f b9 7b f7 92 f2 71 9e 78 22 91 ba 65 d3 b9 29 98 e6 74 17 92 75 14 a4 e6 51 86 7b 3b bc 22 82 da bd 3b 8d 51 e2 1e e4 fb fe a2 25 8a b1 6f 95 b7 99 06 9e 22 87 26 fe 4c 92 df 5b 4e f0 bb 15 92 99 56 dc 06 39 ce aa d4 89 a0 3e 51 81 3f cb a0 3f 65 c9 1a f4 9b 18 78 23 24 56 77 51 c3 3f ac bb d4 ea 75 cd 31 8f 9c ba fb 47 dc 6a 42 d6 32 b6 cd 56 26 6f 32 34 c4 3f 49 a6 c3 1a 72 1d 31 ae 24 56 87 f9 5e 28 17 b3 23 a3 d6 5b e1 fa 1f 23 65 cf 38 ac af b4 2c ee 05 2d a4 c9 29 63 47 87 cf 19 14 cf 86 2f 00 79 08 45 0b a1 90 61 f2 2d ad 4c 17 c3 05 32 cb a3 14 20 6e c4 57 10 14 1a 0b 8e 5f 10 f4 76 65 6b 1c 22 9c 23 59 00 30 Data Ascii: Y+{3uV[T(fy]v|Es.)o{qx"e)tuQ{;";Q%o"&L[NV9>Q??ex#$VwQ?u1GjB2V&o24?lr1$V^(#[#e8,-)cG/yEa-L2 nW_vek"#Y0
2022-10-03 14:16:23 UTC	6180	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6276	IN	Data Raw: 48 66 e1 ed 83 68 20 b5 15 d5 0a 92 c8 ed 8d 87 c4 df 4f c2 89 86 83 4a ef bb 53 9a ba 2d ea 57 27 b8 e9 79 0c 9e 5b 17 ac 6f 19 91 49 35 96 2c 01 23 74 90 dc 2a 7f ff ea 51 a1 1f 9b 04 dc 10 64 9d 62 20 9f 05 19 74 65 cf a5 a5 cb 00 18 20 ce 76 93 7d 94 0b 5c 17 5a ac aa 3e 51 eb b7 94 ae cf da 5e c4 57 4c 64 cf ae e8 3f 08 b7 72 e5 fe fe 79 03 7e 3a eb 6a 2b cf 5d f2 be 32 c2 ef 81 c8 b0 53 1c 70 7d 6e b3 eb 4e ce 10 9a 7c 9e c5 a5 dd f8 05 cf 8c ca 7f 89 0c 13 07 c8 28 df c1 90 d0 27 9e 7b 56 9e 4a 22 5d bc 86 e2 85 09 52 0f 57 7d 57 87 fb b4 46 d5 f0 d3 2d 32 fa 17 c6 64 79 26 e1 1d 00 05 ee d6 86 56 b0 68 3d 2a 7d 0c e3 29 b2 b9 55 1a c7 ff f0 46 1a e0 ff dc 3f 36 bb 68 41 5b 00 d6 22 b4 85 54 19 f4 d2 11 b0 f1 07 94 b1 1d 32 60 30 a4 fd 51 8e d6 86 Data Ascii: Hfh OJS-W'y[oI5,#t*Qdb te v}\Z>Q^WLd?ry~:j+]2Sp}nN|('{VJ"]RW}WF-2dy&Vh=*})UF?6hA["T2`0Q
2022-10-03 14:16:23 UTC	6292	IN	Data Raw: 1c f7 8d bd 0b e9 38 76 95 fe f9 9b 3c 03 46 5b 75 d0 82 99 fb ce 8d c2 4a e0 70 c7 23 7f c0 63 07 de 4c 2a 57 2c 37 18 28 6b 41 f8 fd 82 fe f0 a1 fa f4 7d 45 fc 80 33 6f df d4 ac 5c 8d df b5 e8 68 44 ae 85 25 f5 b8 41 e0 de a4 f1 f1 b8 8b 82 bc 8e 4f 46 95 ee 43 f6 62 65 92 55 41 10 d2 e2 a6 ae d4 d5 41 cd 92 14 e6 ea b6 8e b5 37 ab 1f 61 4d 96 81 dc ed 5c 1c 68 e0 45 15 e2 14 8b 7f b3 01 53 d9 93 6d 51 ca 08 01 53 41 b0 b9 dc f4 fe 6d 62 c4 77 9d 06 ef af 52 7e d2 46 eb c7 8c da 9f cd 4b 98 d2 f3 5d 11 3d 84 f5 27 07 be 5f 2a 6d 95 93 31 73 8d cc cb 01 d2 ec a0 a5 26 35 bf b2 40 dc 99 33 5b 05 21 9b c7 e5 c8 40 97 ba 44 b3 97 bf d5 46 21 96 11 63 df 8a e7 7c 2a 38 13 fb 95 1c 26 d6 31 41 ed f3 59 9a ac 6c 05 d9 45 bf 2f 90 ac 6d 66 07 ef 49 59 4d 57 b1 Data Ascii: 8v<F[uJp#cL*W,7(kA}E3o\hD%AOFCbeUAA7aM\hESmQSAmbwR~FK]='_*m1s&5@3[!@DF!c|*8&1A YIE/mfIYMW
2022-10-03 14:16:23 UTC	6308	IN	Data Raw: 4e d4 61 50 7f 65 68 07 52 10 a0 9c bb 1f 90 36 e4 9b 32 db 63 d5 47 af 3b c3 0f 22 a2 12 ad 6b 8e b3 c5 77 e1 68 19 3a cf 91 47 ab 9f 9e ae 36 92 75 09 9c 3d 0c 46 93 41 b5 34 a4 32 ef d9 39 ef 1d 95 b3 a2 d0 79 93 11 ab c4 75 fd b5 4d 95 80 f9 2c a4 5d a4 d7 fd 93 9f d0 e6 ed c5 71 eb a0 a0 88 46 4b 2f c9 8b 73 3a a3 5c 94 12 6c 95 97 9d 00 c2 35 4a 2c d4 19 c0 58 24 be 84 93 9b 12 05 44 af 81 d9 77 ee b5 57 16 54 30 77 73 eb f5 52 56 64 5b 16 52 43 48 51 b4 e4 9e 06 09 a0 1f 22 c5 8e 8b b6 b8 22 64 e5 cc ed a6 8b ea 5c 84 c5 37 ae dc 26 2d f9 74 bf 68 ba 15 a9 cb 39 c6 15 9e 5d b5 bc a3 f3 dc e8 8c ab 8a 46 e1 e2 ec 62 a2 d3 1b cd 11 4d 01 c3 33 89 c5 b8 bc 86 c2 bb 9d 3f fb 72 7a a7 67 89 1d 6c c9 3c 0a 3d 28 43 cd 40 be 44 1e 7e eb 0b 09 01 04 5c 98 Data Ascii: NaPehR62cG;"kwh:G6u=FA429yuM,]qFK/s:\l5J,X$DwWT0wsRVd[RCHQ""d\7&-th9]FbM3?rzgl<=(C@D~\
2022-10-03 14:16:23 UTC	6324	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6420	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6564	IN	Data Raw: a9 cb 0c d0 d7 19 9d 9f e1 96 9b d5 95 a7 7c fd de 1e 89 1a 89 cb 75 80 3d 80 69 dc 70 69 ab 2f 5e d7 a7 b0 b7 bd ba de c5 d7 86 f2 de b7 46 10 08 85 e6 37 5f 79 05 84 07 2f 6f f3 26 c7 1a 7a 20 f4 ce a5 dd 17 91 04 6b 65 c4 5a d5 00 6d 91 91 cb ea 1a 82 04 f5 77 ea a1 8e 2f bc 8f 2f 23 c9 1f 0f 0e fb 9b 77 10 c8 4e 1b 16 51 56 cd 66 ec de dc 41 df 0f 8d 86 cf 3e 25 57 87 c5 e3 e8 98 72 1b 23 5c ae 50 57 61 5f 3e b9 b2 96 72 64 16 15 b4 30 3f ab 0a 2c 58 56 a1 8b 6e b0 53 10 ab c9 02 65 ea cb 9c 45 ce a8 7d 34 38 c7 4f c8 63 2b 34 28 af 27 29 53 e5 ed b6 d4 b7 f5 74 8a b2 25 a3 7f fe 45 3b 83 32 ca e1 a4 9a ac 13 a8 c1 34 61 89 13 30 f0 71 48 f5 25 a7 f1 e2 de c5 c6 aa 1b 5b 36 11 60 2c 0c 65 e7 a9 ff c4 5f 41 23 22 bb e0 34 b5 74 c8 43 cf 82 c3 7a 3a eb Data Ascii: |u=ipi/^F7_y/o&z keZmw//#wNQVfA>%Wr#\PWa_>rd0?,XVnSeE}48Oc+4(')St%E;24a0qH%[6`,e_A#"4tCz:
2022-10-03 14:16:23 UTC	6580	IN	Data Raw: 5b c1 f6 f3 c1 b2 33 d3 3d fd 5c ea 25 60 d7 08 a8 14 65 73 31 aa 59 0f 8b 1e 93 f5 8a 9a dc f7 e0 01 58 41 97 4b 2e c8 c0 e6 5f 2e 40 46 4b 6a c8 25 92 aa c8 dc e5 a9 87 92 a6 e8 22 41 b0 8e 56 64 45 f7 d1 7c fa c8 e6 b8 6a 1d a6 fc 8a d8 d5 a8 cf a5 02 e1 c5 f4 de 9c 53 7a e2 a9 b0 92 1b 40 f9 68 fc 0c 80 8e d4 8a 76 b5 40 8f 14 ef 96 bb 8c 4c da 6d 4f d4 cf ac 8f d3 45 c8 98 e5 4d 5e 81 0c ca ac 6e 7a 19 da b1 8c 30 98 53 35 a8 68 07 bd b8 52 be eb c0 88 2e 2f e0 aa 51 37 d3 41 5d 0b b7 e9 53 1b c7 fd 25 cb 84 63 2f b8 56 6f 10 b8 c9 dc 5f 0a d7 07 51 48 66 9e 82 86 19 7b 9e 79 ef 1c 85 42 e1 67 da ac 4d b8 49 6c a7 f6 65 c5 ee b5 e3 8a 45 27 35 1e d2 ed 03 92 03 68 c2 4b a3 42 b4 39 33 86 b4 78 e8 bd 6c ca d0 30 0a 41 33 c9 ce a8 c7 27 d2 b4 2a 72 cd Data Ascii: [3=\%`es1YXAK._.@FKj%"AVdE|jSz@hv@LmOEM^nz0S5hR./Q7A]S%c/Vo_QHf{yBgMIleE'5hKB93xl0A3'*r
2022-10-03 14:16:23 UTC	6596	IN	Data Raw: 4f f8 f2 fa 15 29 6a 7d 05 fb 5f 29 00 5f ad 57 ce 84 46 36 11 32 2d de 62 72 7c 68 ac 37 8a 3a 3a 29 f8 0b b5 0e 9b 6e 20 90 eb 96 cd 2a 22 19 74 4c 9b 93 c7 54 7c 79 5f 0b 70 5d 75 87 f8 b7 b9 25 73 df 9c 17 84 22 6a de 1c 2e 92 b6 a0 d8 3c 99 f8 80 69 63 62 e6 a4 ba 53 d8 de c3 d5 61 e4 1d 34 f0 71 be 26 27 b8 d7 7f fc d5 9c fc 77 45 85 85 5c b1 6a 8d 28 61 87 38 5b 3c 64 76 3c 27 16 00 8a 77 ff f5 c0 e1 25 a5 94 e2 27 71 04 e2 65 77 c6 7b 02 aa c8 d0 14 63 a5 a6 bb 54 63 d1 8e f7 e4 2c 7c 10 66 b2 1c 70 f0 d0 f9 29 6b 24 9d c1 a2 63 9a 38 1d c7 3e 0c ff a7 80 6b de 80 e7 88 5a 99 8f 63 ec ae 64 8e df 6e c4 cf 8e d5 36 2e 7e 69 5f 88 be d1 92 1d 9d be f1 86 7b 51 1d e5 cc 4d 8e 22 9b 37 6e 73 37 e5 22 4d e1 4a 8f e8 0b bf aa 32 07 c8 71 c7 da 69 77 6e Data Ascii: O)j}_)_WF62-br|h7::)n *"tLT|y_p]u%s"]j.<icbSa4q&'wE\j(a8[<dv<'w%'qew{cTc,|fp)k$c8>kZcdn6.~i_{QM"7ns 7"MJ2qiwn
2022-10-03 14:16:23 UTC	6612	IN	Data Raw: a3 e4 cc 25 a5 1c b3 b2 a0 fb df 09 96 f4 4f e1 80 ee 77 5e 87 47 e0 e7 19 70 54 bd 1c 46 00 dc 93 52 6e e7 bf 98 a7 4a 48 cd 28 47 72 59 5f 5c 51 b4 f4 e9 bf 15 d7 d8 1a cb c1 5b b1 d3 62 49 d4 e2 38 ae 3f a6 dd bc 39 e3 47 c0 df 97 2c aa 91 33 04 c6 d7 f5 17 b7 f0 8e 4c 54 e4 7d 65 6b 03 05 78 f8 bd 1c e1 e8 80 87 87 d4 7e f9 47 98 8b db 3f 89 9e ec ee 1e 81 a4 57 47 0b fc 25 97 37 2b 8d 7a cd 71 5f 73 3b b3 59 e6 2e f9 a3 0d 74 59 b4 a7 4f f3 a8 57 f7 57 67 9d 4f 35 0f b5 2c 06 7c b6 eb 9f ee fb 5a 90 ff cf 12 e6 a8 cf 84 75 6a f1 54 7c 62 6a e0 08 ac 89 69 92 58 af ad fa 7b b4 8f ee 74 c9 b1 f2 b4 03 e3 68 ed 67 21 d2 b5 ab 15 8a ab 63 9c a8 0d 16 fe 40 67 51 aa d8 e2 50 cf f3 8a ba 21 99 ab 93 5b 30 3e 49 4a 75 0d 96 4b 53 00 a5 09 e6 39 a8 c4 4c a9 Data Ascii: %Ow^GpTFRnJH(GrY_\Q[bl8?9G,3LT}ekx~G?WG%7+zq_s;Y.tYOWWgO5,|ZujT|bjiX{thg!c@gQP![0>lJuKS9L
2022-10-03 14:16:23 UTC	6628	IN	Data Raw: de 5e 8f e3 f3 82 03 70 14 eb f5 8f 9a d4 93 32 41 78 9c cd 5a 27 c9 1f 17 63 43 87 f0 26 a5 7b ca ca 2b b2 01 45 56 5c a2 c1 d7 7a 61 7e bd f2 a6 e5 77 06 34 44 7d c3 3e 16 d0 36 c4 37 34 9c 37 b9 5b 7d ac 59 4a 45 a2 63 8d f2 a7 ee 5b 4a 39 4c c3 29 8c 7b 52 c4 e4 a3 97 db e8 80 cb 6e cd ee 37 1f 5c 6c d1 a9 46 2c c2 85 59 dd 2e 60 92 39 7f cf 6c d6 1b c2 12 14 42 72 94 d5 2b 62 ed 36 bc e6 37 51 a0 f2 dd 36 f3 c8 d8 ad 11 95 d0 37 32 40 f2 eb 22 d8 69 fd f6 9b 4d f6 2d 2a 75 61 53 e0 dd 43 af f4 c2 a0 2e 1b 35 8c 5c cb e1 03 6e cb 63 10 a2 7f 6a 14 e8 ad 1b f6 4b 28 92 80 7d de 34 a3 5e 0d e2 4a ee 6b f6 11 b1 79 61 e7 b0 b7 c5 07 7a ec 3a 54 9b 53 59 84 44 f1 d3 b2 05 c0 92 88 0b 20 e5 2e 5d 28 11 7e c8 eb 1c ba eb 48 7e 28 4e 15 bd 7c b0 fa 8e 99 56 Data Ascii: ^p2AxZ'cC&{+EV\za~w4D}>6747[}YJEc[J9L){Rn7\lF,Y.`9lBr+b67Q672@"iM-*uaSC.5\ncjK(}4^Jkyaz:TSYD .](~H~(N|V
2022-10-03 14:16:23 UTC	6644	IN	Data Raw: 71 85 2b d5 61 85 08 8d 23 42 67 28 67 58 f4 6a b7 1a 22 c5 f6 52 0a af 8b e8 29 4e 91 9b 5a 9f 40 59 29 47 d6 67 cb b5 5a ef b7 39 b6 50 99 a7 22 7d de 15 53 ec cd b3 bd 57 55 1e 07 d6 63 af 8b b3 ab 37 43 ce e4 87 50 e8 b0 56 3d 8c e7 3a b7 00 9a 3a 7c 7a 47 a4 b5 55 ed a4 69 07 b1 75 15 8c eb 34 43 23 cc 0a 95 ff 26 24 82 d7 5e 90 67 2a 93 73 da e6 52 a1 34 13 fb ad 9d cc b0 cc e0 af e4 07 59 47 75 75 02 99 ca b9 20 d7 ba 55 13 27 16 f8 4f d9 28 a3 33 3b db 86 88 1f 3f 02 a5 50 b8 28 93 08 c1 53 14 b4 93 be cf 66 42 ff 34 c2 49 0e 45 81 bc d0 a5 fd 2e f3 27 58 7a e0 f9 e4 bf 67 e5 db c9 52 62 eb e6 75 e5 54 8b 3e 03 57 5a 2a 0e 84 cb 59 7f c0 8b aa 58 5c 6d 77 ef f8 e6 1e 5f e9 aa 02 44 b6 2a 6e 0f 4e 76 ba f1 52 07 ca b4 a4 eb ba c1 14 f2 1f 2d eb 35 Data Ascii: q+a#Bg(gXj"R)NZ@Y)GgZ9P"}SWUc7CPV=::|zGUiu4C#&$^g*sR4YGuu U'O(3;?P(SfB4IE.'XzgRbuT>WZ*YX \mw_D*nNvR-5
2022-10-03 14:16:23 UTC	6660	IN	Data Raw: d0 5b 63 83 7f 9c 44 78 49 b1 61 0f b3 e6 6e 1d b9 90 d7 0a c8 c4 aa a6 34 03 3d ad 10 04 65 4a 13 28 00 43 60 22 74 41 66 1c 0f a2 68 bc 1e 43 88 cd 6f 7b b0 ce 75 53 bf a3 f3 66 32 ee 01 36 38 56 7d b0 13 64 7c f0 56 65 c7 79 f7 c6 b2 03 6c e6 f0 86 7f 89 82 27 6e 8d 3d 6f 28 45 f6 7a d2 93 b6 70 e1 b7 81 0c 3a d4 29 0a f0 12 33 ae db 9c f0 36 ce ec 2f d0 29 6e bb 32 c8 4c e1 fd 78 97 62 65 72 c5 e5 29 98 00 e2 1d 48 21 c7 8e 90 c8 6a 51 d8 ae 84 0a bf d1 1a 0c 7a 26 0f df 5e 98 e9 eb 39 4c 97 2d 02 f7 7d 95 26 56 84 53 de 0c 4d c8 38 61 fc ef 82 20 29 17 61 7d d8 0c be 50 9e 75 19 54 96 77 42 bd 58 61 18 01 f4 d2 93 1f 4b f4 a4 a1 a7 8d b3 6f 81 60 e7 5c 04 3c 0f e9 55 96 51 13 86 e6 4b 4c 59 fe b3 4f 48 56 59 ca 8e 82 f8 fc 03 79 98 ea f8 f7 bc e0 dc Data Ascii: [cDxIan4=eJ(C`"tAfhCo{uSf268V}d|Veyl'n=o(Ezp:)36/)n2Lxber)H!jQz&^9L-}&VSM8a )a}PuTwBXaKo`\ <UQKLYOHVYy
2022-10-03 14:16:23 UTC	6676	IN	Data Raw: ce 05 7c 26 2b 36 a8 a2 e7 63 2a 7d 7a b6 a5 eb cf b9 5f de 64 94 b3 42 b8 ef fd 61 4b e3 98 e4 15 44 66 42 3a a2 3a dd 23 fe d5 c1 a2 9c a7 19 0f 6f 05 df 87 d7 fa e0 b6 31 7d 40 fd 68 30 36 b3 ad cb 1d 76 ad 1b 48 bc 6c b7 52 d3 7a e8 2e fc 81 f9 6b bb d8 64 bd ce 9a 43 e4 1b 5f cc 59 a1 eb 63 88 5f 14 14 d3 ce 36 de a5 f0 fc f0 6f 25 70 e0 83 18 df ce a8 c9 ea 84 98 98 83 52 64 78 ee 60 3e 22 ea 67 31 6e 10 a6 0e ab 12 db bc 77 2e 64 c0 f7 1a 45 09 fc c9 ce 7e 39 fd b8 e9 a0 80 4b d6 d3 cc 51 d1 66 66 76 a6 bc d5 c3 94 a6 71 12 fd 67 40 ef 2a 31 6f 86 40 28 b2 8d c7 aa 5f d5 d7 89 b0 8a ea c9 15 56 6c d6 73 d5 96 60 0c f9 71 6a a5 cb 46 b4 93 30 45 c1 64 f4 37 9d ef 63 f2 c0 53 e5 2f be 60 e8 b7 c3 8e 6f ab 4f 05 83 fd 8d 03 b0 75 f4 04 a8 3c 9e 07 40 Data Ascii: |&+6c*}z_dBaKDfB::#o1}@h06vHIRz.kdC_Yc_6o%pRdx`>"g1nw.dE~9KQffvqg@*1o@(_Vls`qjF0Ed7cS/`o Ou<@
2022-10-03 14:16:23 UTC	6692	IN	Data Raw: 3b 7c f2 47 d8 98 c2 e7 ee 7e 7d 7b 82 37 ee bd dc e2 d9 1b 5c 52 4a 13 7f 2a 3f e7 fa 84 93 fd 67 bd cb 30 6d 2d 29 62 15 ad ba 78 04 5a 3c 2a 52 64 6a e9 2b 11 63 06 b3 bc d2 c7 b6 35 23 25 94 80 9f 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6708	IN	Data Raw: f6 1c 60 75 c9 0f 36 8b 26 ca 9f 09 f4 20 06 0e 67 12 16 41 26 97 ca ea aa 58 e3 50 c0 13 eb 69 f0 bb ed 06 62 6d bd 3e 7e d7 de 6d e2 42 77 20 6a 0c 56 7a d6 f5 57 f9 12 cd 28 1e c0 5d 09 be 3a 7d 2a d2 9a 97 f1 45 b4 ef a3 a5 b8 e6 24 d6 a2 c2 c9 bf 60 8d 12 78 22 ec db 4a 84 1b 28 13 7d 75 aa 91 10 0e 2c d7 e9 16 81 c1 94 53 bd 5d dd 7d 06 5d 58 32 25 4a 4c 63 0d 17 fe a9 92 c5 ae 78 72 ab 59 5b 80 cc 68 39 7a ae 12 02 37 64 64 6a 6b 62 ef 77 88 34 ab 03 6c ba 05 53 9c da 5c 15 8c 33 8e e0 f3 c4 3c df 6c 7c 22 93 7c a8 dd d0 fc 3c 8a 4c 0a a3 75 22 db 00 a3 04 12 13 02 cd ad 33 e4 be db 0b 92 e9 aa c7 28 23 ec 08 e8 61 b7 31 3b 45 d9 d4 03 d2 80 b2 f4 7b a2 14 63 15 a1 50 f6 2f c2 b1 d3 af 0e 01 6c c6 a0 de d7 27 89 14 c6 e5 12 07 4e 11 c2 57 35 39 2e Data Ascii: `u6& gA&XPibm>~mBw jVzW(]:}*E$`x"J(}u,S]}]X2%JLcxrY[h9z7ddjkbw4lS\3<l|"|<Lu"3(#a1;E{cP/l'NW59.
2022-10-03 14:16:23 UTC	6724	IN	Data Raw: cc 04 43 d6 a0 03 9d ef a1 00 cd c2 7c 73 d9 53 d8 1e 3b c8 43 59 ce 74 35 b6 83 8c cd c6 63 61 03 a9 5b d4 1c a8 25 8b a9 bd c0 44 25 a2 e0 8a 50 82 cf 54 4f 31 38 60 a6 69 7f 63 9b 5e ce bf 2f 98 98 df 19 27 d2 ec df 01 5c 5b a8 b4 31 11 80 21 0c a8 da 0d e8 6d ac a3 19 1f 85 f4 51 4c 48 38 ef f3 4d 88 c6 18 a8 81 b2 ff f0 2a 04 dc dd 45 22 f5 57 b1 0b 46 b9 e7 d3 c7 44 66 d2 f8 18 c7 72 bf ba 56 00 e6 e3 b4 64 8e 6d f9 93 32 81 2b e4 8f d7 6d 18 b2 2d 04 5c 4a a6 6c 50 cc 51 b0 f3 d4 47 c0 6f c7 9c 3d cd ae 76 10 f8 c3 20 db d2 61 14 59 1c 46 da 9e 32 4a b0 81 64 91 1a 98 61 40 38 3b de b6 47 1b 53 2f fe e1 4f e1 c2 d2 2b 2e 0d 86 8e 48 c2 ac ed 4f 6f 92 bb 15 7e e5 b8 a2 1b cd 4f 57 12 8f 6b 4c b9 71 72 07 93 42 e9 1f 6f d6 23 6c 41 8e 5e 9b 02 13 f5 Data Ascii: C|sS;CYt5ca[%D%PTO18`ic^/'\[1!mQLH8M*E"WFDfrVdm2+m-\JlPQGo=v aYF2Jda@8;GS/O+.H Oo~OWkLqrBo#lA^
2022-10-03 14:16:23 UTC	6740	IN	Data Raw: eb c7 42 51 b9 b1 5b e2 eb e6 4f 78 74 7a 3d 09 a0 49 98 a5 d7 0a 9a c5 04 56 06 94 3e c8 c1 6e 7f 8d 9b 87 bf 7a 8c 8d fd 73 12 ac f6 b9 e5 4d 3b e5 07 91 84 ef 5f 94 66 9d 67 e5 b3 ce 40 31 aa ed 22 6e 38 69 4f a9 a0 5e 58 21 f1 9a fa c4 71 60 6a 90 ac 8c ea 16 fb 9f 7c 99 88 3b c4 66 fc be 4d e6 08 94 29 3a fc 62 0c 17 c4 e1 5e 4d 14 35 05 5b e8 02 08 fe ab 34 b1 0a c1 b3 b4 f4 15 85 99 2d b3 74 1a 97 c9 be c3 84 bb 82 7d 01 c3 3d a2 fc 2c 43 fd 96 ca 18 3a 6a 6c d5 51 a1 3a a6 84 bc f6 10 73 75 39 8b cd 0c 1c 10 f0 db 2e cb 75 d7 97 97 62 9a a5 24 08 99 8d 72 eb cb 58 fd f7 f8 89 18 8e 9e 83 dd ae 9b f6 13 1f 77 67 09 bf 1c 00 14 dd da 9d a7 70 17 b1 c7 69 be ec da f4 a4 d9 0c 28 aa 77 55 10 20 ad 2c 0d 98 99 c3 1d 20 8c af f0 99 da 53 0b 79 1a 67 bf Data Ascii: BQ[Oxtz=IV>nzsM;_fg@1"n8iO^X!q`j|;fM):b^M5[4-t}=,C;jlQ:su9.ub$rXwgpi(wU , Syg
2022-10-03 14:16:23 UTC	6756	IN	Data Raw: 96 60 02 0d 77 23 92 31 fa 17 29 e2 7f c8 f4 86 05 13 09 e3 08 a3 eb 98 91 4a fd 38 c7 2e 11 f6 12 f8 68 88 1d 35 0b d2 9e ff 01 69 c5 e8 5b 57 42 a3 ec ae 9a a4 4a 21 0b 2b 48 2b 5e bd 45 36 8a b0 de fe ae c6 d7 63 02 a0 a7 be e4 63 5b af 61 e1 3e d7 25 88 32 61 1d 41 99 df 38 96 c3 3d 7e 69 9b e1 2e de 46 f3 ce 00 6f a0 c9 a9 c6 2b e9 b5 02 10 2f dc 92 d9 f7 ab cc 6d 55 64 4d 62 c8 bb 1d 06 67 50 3a 56 39 cc fd 9c 3d 44 6d c6 3a a0 4a de 18 f5 9b cc 2b 86 bf 33 94 01 8b 57 fa 42 e6 c1 7d 97 9b bf d1 9e 45 7e b4 ae 54 7d 00 58 36 de 08 3d fb 85 d1 34 60 4b 18 37 24 c5 10 5d 3c 18 f1 15 a2 05 c5 ee 2f 24 e3 ae 57 96 5f 3f d2 9c ca 27 44 48 84 e6 98 d4 43 ad 24 e9 68 64 21 11 c7 69 8d f9 93 46 68 b6 fe d8 fa 6a 65 04 0e cb cc 71 61 40 df fd cb e6 00 ec c2 Data Ascii: `w#1)J8.h5i[WBJ!+H+^E6cc[a>%2aA8=~i.Fo+/mUdMbgP:V9=Dm:J+3WB}E~T}X6=4`K7$]</$W_?'DHC$hd!i Fhjeqa@
2022-10-03 14:16:23 UTC	6772	IN	Data Raw: 1c 5a 97 01 ac d6 3f 55 e3 5b 67 27 97 b8 7d 1d c9 55 68 41 c7 8b 4f 5b 60 0a 36 4e da 4d 18 e2 65 2b e8 1d 38 a9 95 b9 d6 85 26 d3 3c 45 b0 73 b6 8d d5 3e 78 69 f5 3e 63 de 4f e0 4b 6b cd 8e d8 89 39 38 b9 3f 7a d3 94 b2 47 bb fd 2a dc 05 7c 87 cc ae f9 aa 2b 53 63 12 34 1b 5c 08 d8 39 88 96 bd d5 44 a2 18 58 c9 bb 81 65 1c 64 29 c9 1c 1d 48 d9 d2 a9 31 93 a5 d0 c8 97 3d b0 a2 6d 36 2d 88 20 0a 87 5f 8a 3c 07 27 ff 56 c0 08 b1 e7 9b 13 57 c9 80 2c 9b 66 75 23 ba 54 9a 1e e3 63 60 16 87 34 b3 7c a1 b3 28 70 dd 31 81 2f bb a2 f8 e8 0d dc a5 0f 10 fe af 03 c8 4b 05 ec 4e f5 08 e4 29 db 9d fd 0e 43 30 4c bf 67 96 25 bd 9a 89 af b6 8b 76 e2 58 45 f3 9d da 83 79 19 d1 36 64 b3 43 aa 65 30 25 36 5c ff f2 ee 7d b4 61 2e 8b 6e 0a 8e b4 04 a2 98 e2 7f ec 25 7e 85 Data Ascii: Z?U[g'}UhAO[`6NMe+8&<Es>xi>cOKk98?zG*|+Sc4\9DXed)H1=m6- _<'VW,fu#Tc`4|(p1/KN)C0Lg%vXEy6d Ce0%6\}a.n%~
2022-10-03 14:16:23 UTC	6788	IN	Data Raw: 40 73 a0 08 d6 43 54 77 73 4f 6d 43 ea 00 24 34 20 26 1e c0 81 38 36 bf aa 22 df ea ac 1e 48 5f 8e 12 a0 1c 05 68 db 06 bb 5d 4b 30 be d8 78 f6 2d a0 90 9b ec 74 7c 56 e0 7e 4b 71 14 c7 1d aa 03 b4 85 a5 f8 fd d3 d9 7b 50 69 46 09 91 6f 7e d1 34 ae ef 99 82 2c 45 db 2d e9 d9 86 75 fe 33 c1 3b 2a 08 2c 56 f4 66 77 83 8c e6 97 c9 c5 4d 15 95 1b 19 f6 7a 4b d2 53 a6 56 56 97 68 cb 68 21 6f ca 07 a1 01 e6 ca 34 9e ed 14 31 c4 90 02 9a aa 08 ad be da 36 cd fc 18 01 33 90 81 95 c6 60 08 d7 1f 6b 35 73 0b b9 a0 ff f9 16 f4 c1 c0 58 7b aa 90 50 fd 7d 17 52 5d 02 cc dd 16 87 16 e7 5d 95 dd 1f 35 84 92 6c 86 ec 0f 64 35 7a a0 c0 4e 99 95 99 d7 10 a3 7b 47 2c fa 20 ea 1a 82 75 18 c9 45 51 8b c9 30 25 4c 0c a0 72 94 72 8c 36 ba c8 1e 3a ac 1a aa 3f 68 ba 6c cf 7d 6d Data Ascii: @sCTwsOmC$4 &86"H_h]K0x-t|V~Kq{PiFo~4,E-u3;*,VfwMzKSVVhh!o4163`k5sX{P}R]]5ld5zN{G, uEQ0% Lrr6:?hl}m
2022-10-03 14:16:23 UTC	6804	IN	Data Raw: 62 82 4e 4e e7 e3 ab fa 38 af c3 8b 2c 94 e1 d3 46 d0 22 c2 bf 92 35 f5 94 7e f6 98 49 af 3a 09 a0 d3 56 35 8b cc 00 12 0f 86 2c b8 13 15 2a a6 3d 21 49 0b d5 9b d5 af 0e fc ac 2c a8 ce 1b 7b 8d 13 29 05 dd d8 5c e5 e5 43 ff 6b 4e bc b2 21 d8 6a d1 67 1c a1 d5 65 d2 56 39 9c 30 b1 e6 8c 46 d4 16 0b a3 db 86 8f f8 aa 6d fd 5f 2a 75 6d b4 c4 c7 31 53 ae a9 4b 0f 2b 92 32 73 99 25 ba 65 b2 3f f1 54 38 a0 4f 7e a1 23 1a d2 23 c8 b5 1e 38 0e 11 31 66 73 09 50 6a 45 b8 97 ac 70 73 5d 6e 62 b9 ee d2 f6 5f dc a4 1c c1 be 67 68 2c 8a 65 3e 81 d3 73 3e 3f 5d b4 6d 68 b5 c7 ad 38 74 1d b5 8a 5b 28 aa 2b 77 c0 90 67 d3 3e c4 ef e3 75 31 d0 0b d3 8c 4a b3 87 f9 4a ee 3c b3 a5 f1 74 e0 ae 5f 3e b6 04 7d 88 01 84 45 51 5b 44 20 65 ad 2a a1 58 ec 4f 2f 71 dc fe 14 d3 53 Data Ascii: bNN8,F"5~I:V5,*=!I,{}\CkN!jgeV90Fm_*um1SK+2s%e?T8O~##81fsPjEps]nb_gh,e>s>?]mh8t[(+wg>u1J J<t_>}EQ[D e*XO/qS
2022-10-03 14:16:23 UTC	6820	IN	Data Raw: 34 1f 44 90 50 00 af f1 d5 1d 2d 53 76 cc a7 43 d1 28 9f bb a4 57 1e 08 cc 61 6b b3 bd a1 20 19 d2 93 1b 5d 9f 67 26 2e e1 e6 b7 cb b0 c0 e7 6f e8 7e 32 94 f0 c4 1f d1 d0 dc 10 08 69 65 40 3a c4 56 03 f5 fb 75 aa 7e a1 37 10 26 56 86 5c c9 27 a4 72 7c b9 97 17 56 70 15 dd 1f 15 0c 09 da 3a 8b 8c 7f 8c d1 ea e0 00 fc 56 17 bd 9f a9 ec 27 ff 99 8d 94 c8 7e 5d 99 64 d2 d6 74 b2 ad ad 30 3e ca 4e 81 f0 00 d7 a2 70 e1 a3 c1 47 41 6a 70 75 c3 26 4d 71 3e 24 b9 30 9e 37 28 b2 12 97 51 c5 ec 2c de a0 e8 8e 82 2f 26 f9 c5 86 50 9c d2 bf 62 1a 49 6c 1e bb ce 94 8a 9a c9 31 f4 e2 b7 7f 39 db 6f 9d b2 2f 2a 92 e3 ea 4b cf e5 65 87 56 f7 ef a4 39 ed 5c 81 c8 ca a8 6a 1d 4c 58 cb ef 7f 28 2f 11 83 24 72 8b 3e b3 45 88 86 d9 c4 39 b6 9a 8f a3 bb ce 04 04 4c c4 36 6e 58 Data Ascii: 4DP-SvC(Wak]g&.o~2ie@:Vu~7&V\'r|Vp:V'~]dt0>NpGAjpu&Mq>$07(Q,/&PbII19o/*KeV9\jLX(/$r>E9L6nX
2022-10-03 14:16:23 UTC	6836	IN	Data Raw: c8 15 38 e0 12 cc 6c e3 a8 18 c8 68 ae 2e 39 af 31 22 4b f5 fc eb aa ed 81 0a 24 c2 22 d1 04 7f 1a dd e2 6f 18 c7 49 2c 97 a0 64 60 16 fa d1 d5 64 96 33 21 57 c0 ac de 74 64 b7 a7 fc 97 d0 1f e1 28 d8 99 cb 20 c4 04 38 b8 52 88 86 5a f6 48 7a 6c 0d 07 4c 87 8f 73 06 5a 2b af f3 ee 10 fb 8f 78 64 9f b7 f8 5a 92 6a 40 77 56 08 21 dd 90 27 be 65 e9 8e 35 d3 92 6a c7 fe d5 b4 21 bf 9c e0 fa 76 0e 2a 89 85 1c 74 33 ed 98 a7 2e 47 05 bd 7f 96 8b 12 3c 8b 37 d1 5e ea 0e a5 d7 a5 5c ea 5b d7 11 70 87 ba bc ee 82 29 da 5d f6 8a a1 06 97 e6 4d a1 09 93 aa 96 14 8f 11 4e e1 04 4e 8c 4e 9e 6d 33 1c b9 07 63 a6 be d2 0e 94 e9 3b 1d 50 e4 ba 98 85 d0 69 f8 ed 7e 2a a6 16 35 aa 92 bb 40 eb 88 e5 c2 09 1a 56 b8 c1 ca d9 4f b9 28 e2 fd f2 ca 85 fe 9d ef c8 d4 48 0f 2d 02 Data Ascii: 8lh.91"K$"oI,d`d3!Wtd(8RZHzlLsZ+xdZj@wV!'e5j!v*t3.G<7^\[p)]MNNNm3c;Pi~*5@VO(H-

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6852	IN	Data Raw: a0 5b 89 20 87 9a 88 4d bc 35 59 d1 c0 17 89 69 bc 37 77 eb f3 30 98 f1 8e b1 27 06 2d c8 d5 55 e3 f7 b9 3d 72 4b dd 63 50 13 5c da f3 3d f6 72 c2 df 8a 35 a3 2d d0 3b 52 ed bf 80 b3 56 3f 40 c6 f1 f7 98 22 2e b5 5d d1 72 66 69 c1 2e c3 eb fb 65 5c 28 30 ba f8 0d e2 3d b5 82 1d 7d 82 30 f3 30 15 b2 c3 45 e1 88 b0 81 39 95 1e b1 13 c2 30 24 7d 87 a9 67 ef e2 74 98 ee 8e c5 c8 2d db 1a 88 cf 28 7c 21 26 ee 24 bd a9 70 d6 fe 33 bc a3 7e a9 40 5a 2a ae e5 7b 9a 76 0b 3d 82 1d 0a 85 7b 3d 0c ba 53 58 a5 ff e5 f1 0b f5 90 2f 51 eb 93 00 be 81 6c cd b8 e1 52 5e 4c 70 91 05 74 21 2a 5f 37 9b b1 d5 31 a2 6e 9b 31 07 eb 88 40 1b 03 cc cb 02 cf c6 b5 12 99 0f 2f e9 70 cd 15 af 0c df e7 aa 93 71 10 65 7b e1 db 94 8f ba ae 73 fd 97 4c 2e 07 58 36 93 6c 72 d5 a3 b1 4e Data Ascii: [M5Yi7w0'-U=rKcP\=r5-;RV?@".]rfi.e\(0=}00E90$}gt-(\|!&$p3~@Z*{v={=SX/QlR^Lpt!*_71n1@/pqe{sL.X6lrN
2022-10-03 14:16:23 UTC	6868	IN	Data Raw: 9b 95 3d 09 9e 83 bf 77 fe 23 06 32 e5 9f 57 7e cf 76 41 a5 a2 13 46 33 06 e5 00 d2 fe 23 8a 67 7d 73 49 f5 3e 58 4e 50 19 09 58 83 9a c2 03 08 c2 02 17 fe 82 58 4d e8 d5 44 17 12 75 79 eb f5 7b 61 72 1e 03 9b e5 08 0c 67 92 c2 27 67 09 75 40 c5 67 2e e6 27 a4 72 71 a3 bb b9 fc 30 23 25 c4 04 58 6c cc df 5f 25 ae 34 a8 65 fd f8 70 02 25 bb 49 65 c8 bd 02 1d 22 f8 96 05 6c 56 57 4e be 81 33 3c 86 2b 2d 5b c1 58 dc 51 3a e1 06 f7 97 07 84 fe b6 c6 f5 ae 33 cc 95 ef be 72 44 fb d8 98 ba 6f 6c a5 61 ed 2e 35 26 40 a5 c0 44 18 7c 08 e4 73 0f 26 d2 e9 9f 63 38 d6 e0 02 94 71 34 16 6d 7b 2e 0c 53 76 0b a8 22 00 bb 89 ea d2 ea 31 49 85 07 cc 83 79 0e 1c 18 ca fe 2c 7c e1 48 21 a0 99 07 a3 7b 53 fe 2c 32 e7 79 b6 ab d1 d1 f0 09 4e ed 75 26 59 c9 7f de 3b 5e f6 96 Data Ascii: =w#2W~vAF3#g}sI>XNPXXMDuy{arg'gu@g.'rq0#%Xl_%4ep%Ie"lVWN3<+-[XQ:3rDola.5&@D|s&c8q4m{.Sv" 1Iy,|H!{S,2yNu&Y;^
2022-10-03 14:16:23 UTC	6884	IN	Data Raw: 60 ae 0c 83 5a 20 97 8b a9 f2 dd 7c a2 03 76 00 bd 0c 6c 4c 23 b1 db 57 40 cc f4 e0 d3 97 b0 9e ee 33 e3 d7 51 39 3d d6 3d 9c 7c 4c 66 93 bb c1 c1 40 f0 27 51 1d 86 e4 b7 81 38 b7 73 30 c9 94 77 54 06 63 36 69 d4 d7 97 b6 12 ef 5a b8 1f 29 28 03 72 80 67 e6 24 4d 6c 8a 60 1e c7 3e 8f 9d d9 fa 5e de 10 2f 26 c4 8f 7e d7 8d 97 22 f2 7d a9 49 6b 35 bc 33 33 a6 cb 18 ba e1 d7 d2 97 94 ce ef 37 c7 3c 6d 86 68 a0 03 74 f2 4a 65 69 21 02 2b ae 4a ac da e7 d3 a0 01 e6 74 ed d3 ef 7a 62 14 35 9c 06 2f 7f ba d0 9a 8c 83 98 4e b1 8b 53 6f 53 74 92 92 5f 6d 52 96 24 57 2e 8c d9 5f d5 f2 33 36 26 5d 69 f2 75 49 ed f4 b3 15 96 99 3f ed 22 7a d3 01 d1 c3 db 1f 20 16 ef d0 63 0b d6 44 2b 28 45 7c 34 87 b1 84 96 b7 36 1b 8a be 84 c5 0a d3 84 20 bc 70 6c d1 92 af 55 8d b9 Data Ascii: `Z |vlL#W@3Q9==|Lf@'Q8s0wTc6iZ)(rg$Ml`>^/&~"}Ik5337<mhtJei!+Jtzb5/NSoSt_mR$W._36&]iuI?"z cD+ (E|46 plU
2022-10-03 14:16:23 UTC	6900	IN	Data Raw: 3c 6a b0 e3 58 fc e2 b6 95 dc ce 6e 15 e4 8a 85 be 2b 92 a8 9c 4a d8 22 ac 08 71 9b 5c 75 93 36 14 b3 d5 98 f1 df 7d 1d ce 32 61 98 cf de be 46 0d b5 84 db a5 88 4b bb c7 aa 06 98 5b fc cd 0c 27 b9 e0 2c 1b 11 a6 df 0d 97 04 94 db 6d aa 2f 33 32 1e f0 7f e0 87 e3 9a 54 19 7b b0 2e f3 9a 4c 5e ca 56 ad c2 8a 04 5e 7a cf 7a ac 34 fb 05 84 ff 3d 51 c0 76 e7 e9 05 ec 1f 69 24 c7 08 76 54 98 c6 f8 81 3b 1d 07 c6 9d 66 db f2 91 ec dd fb 80 ae 2a 64 71 be 33 a8 ea aa db bb bf e7 69 67 16 4a e6 ad 11 57 53 4a 21 37 b7 62 19 d4 3e 55 bf bf da 29 a2 27 72 01 a6 3c 2f 92 83 07 76 67 e8 27 1f 97 61 94 4d e8 9e 71 29 55 e3 c1 ef 6d 52 40 ce 9e 1d a7 bb 01 78 a9 32 13 a2 2a 7f 10 f1 40 94 7f 93 48 af ba 44 fb 42 2e 58 e8 8c d0 fc af f1 39 c9 59 0c fc 2b ef b3 87 30 51 Data Ascii: <jXn+J"q\u6}2aFK[',m/32T{.L^V^zz4=Qvi$vT;f*dq3igJWSJ!7b>U)'r</vg'aMq)UmR@x2*@HDB.X9Y+0Q
2022-10-03 14:16:23 UTC	6916	IN	Data Raw: 92 2f 61 34 02 1e a8 c0 1a f3 aa 1e ae ef 27 50 ca f4 c6 66 7b af 24 7b 79 f8 55 8b e6 b0 f9 48 f1 83 cf c4 7f 3d ac d9 5a e9 69 ac 29 13 65 82 d0 45 c3 7a 1a b4 09 63 5d 41 4f 05 09 8a ca 2f dc 9a 89 b4 0e aa 86 e7 1f 5b 29 b2 52 57 ae bc cf f3 df 4f 4d 8f 6f cb c0 c4 ca 4b f8 d6 88 a5 b8 30 4a bc c1 d0 95 b8 97 53 17 77 a4 1d 41 a0 cb a7 cc ee db ad 9a 33 ac 4d 51 5e ca c5 9c be f8 25 fa 09 b2 34 39 4b 8a 10 73 ab 8b 4b da e1 3a 2a 78 8a ff 83 18 df b0 6b 21 eb bc b7 62 9d 51 8b 07 ec 62 dd be 59 c9 3a ad 03 2e ca 39 db 22 96 54 bf b3 ed b4 72 e7 64 ce 69 73 91 dc 78 02 61 2c 8e 5a 6b ff d5 6c 57 ab ce d1 78 0f 8f 2c e0 32 90 2e c3 d8 c1 35 07 0e fc c8 10 ab 82 98 ab 00 19 f7 43 8f 21 4a 12 c8 47 aa e6 a2 7b 78 c4 23 83 7c 04 23 5b a4 04 4a 69 e8 80 79 Data Ascii: /a4'Pf{${yUH=Zi)eEzc]AO/[)RWOMoK0JSwA3MQ^%49KsK:*xk!bQbY:.9"Trdisxa,ZklWx,2.5C!JG{x#|#[Jiy
2022-10-03 14:16:23 UTC	6932	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	6996	IN	Data Raw: 70 99 7f 2a 30 77 4b ff 2b fd e5 58 fe 88 4d 38 6b 88 5f 7d 7e e3 57 50 7b 68 b4 36 26 52 60 02 c5 8c 19 3e 96 29 e7 d0 82 f9 5e 7d 04 27 38 c1 30 d5 b9 3c 25 44 f3 f2 9a 5f 47 d3 48 e8 3f 2f 81 43 ca 34 ba 48 11 5b 55 6e 05 0c 08 43 c9 a8 58 e4 6f 81 0a a5 35 6b 8c 32 0f 2d db ca a7 62 e0 15 d9 c0 a0 6e c6 11 ec 29 e0 41 a3 b7 35 2c 44 50 84 3a 31 81 a4 b4 f4 26 08 b9 c0 44 ef 8b 70 40 b7 2e e3 0b fc 99 40 7f 8b de 66 cc 5b 1c b9 42 9f 7d ff 78 3d a8 6c ea 0f a0 e3 0d 73 25 49 b8 a7 6b cd ea e6 b4 24 f3 57 f8 0a b7 07 d2 19 b8 2f 9d 27 be 44 59 2c e7 10 15 e6 9b 71 d2 18 d9 e6 a3 bc 4b 1b 67 a3 ab 98 cc fd 89 10 37 8a 00 cd 81 2f 79 80 c6 a3 a6 ca c9 74 6f 4a 50 cb 42 af c4 db d8 b5 a1 60 55 b6 77 93 3a 10 1b 1d c1 20 6d f0 e4 44 38 65 1f c2 a5 e8 82 88 Data Ascii: p*0wK+XM8k_}~WP{h6&R`>)^}'80<%D_GH?/C4H[UnCXo5k2-bn)A5,DP:1&Dp@.@f[B}x=ls%Ik$W/'DY,qKg7/ytoJPB`Uw: mD8e
2022-10-03 14:16:23 UTC	7012	IN	Data Raw: 3f a3 65 f2 e6 aa 33 61 f4 47 bc 31 65 76 c3 5a a2 93 96 86 71 f8 74 bc bf 2b 2a 25 30 75 38 21 11 7f b6 78 da 4b e6 c8 95 8a 5d 88 a0 e8 5a 1f 5e fa 66 64 7b 8c 2d 9a 0b 50 14 d5 f9 a3 75 2f e2 73 70 b7 38 e2 4f 0a 15 e1 da 94 0c 59 b6 92 ba 54 fb ad c5 c3 4e a1 e4 c8 91 11 71 84 c8 3f 6f d7 a0 c8 a5 d3 8a d5 ef 01 a3 e0 dd be 05 e2 82 db 0d fc 57 6e 83 15 d9 bd 3e d8 6e d2 0e 6d d3 ea 84 f5 8e b0 7c c5 6b 44 94 96 dd 3b 38 5f a1 b4 3b d4 c8 e7 d3 fa 0c ed 1c 7b 6c b1 c4 b8 fc cf 4b f3 04 74 ad 63 03 22 88 29 09 bb 91 c7 1f c5 bd 4b 3d 24 7b da 12 bb ab c0 ee 3d 08 ee 44 60 f4 c4 86 28 ee 24 2b 33 79 66 00 7e 3e 2f 9f bb 75 33 d9 a1 81 24 39 ce b9 a1 7b 1d 83 25 03 e5 02 94 02 35 d5 e1 48 41 a8 53 31 4a bd a4 6b bc 61 86 65 58 68 7a 18 a9 6e 26 11 48 8c Data Ascii: ?e3aG1evZqt+*%0u8!xK]Z^fd{-Pu/sp8OYTNq?oWn>nm|kD;8_;{IKtc")K=${=D`($+3yf~>/u3$9{%5HAS1JkaeXhzn&H
2022-10-03 14:16:23 UTC	7028	IN	Data Raw: ba 12 68 9e f9 27 7f 68 f1 ca a4 99 98 0d e6 8f 2e a3 e5 99 62 3b 13 57 af 54 ff eb bf de 8b 1c 34 2a 58 c6 35 c2 3f 05 97 f1 d7 cd a1 aa 0e 1b c0 09 ab 72 40 83 ce e3 93 0f fd b9 49 67 8e 55 3b a0 f7 21 a6 82 74 11 83 a9 ca ec 76 cc c5 70 fe 92 c8 75 8b 4e e3 60 23 5a b0 54 41 57 62 f0 30 5e 5b 66 b5 b9 29 f9 ff c1 0e 10 ba d2 45 aa 30 e9 fe c2 64 b1 50 f6 39 dc 45 e9 64 77 55 cf bd 95 84 5b 75 1b c2 28 b3 b2 e9 ae 07 f9 64 a8 c6 ec 1a bc da 49 6b 8d 61 b6 42 4b f3 95 4a 5e f0 6a 57 8d 57 d8 f4 df a9 c4 b1 2f 52 c0 20 41 df 2b d2 dd d9 46 ab 76 de 09 4e eb 8a f4 ac 9a 48 54 4a b6 b0 e1 9b ca 63 50 13 c0 1f b3 58 4e 56 96 9f f8 af 09 4c 1f c8 76 d7 15 26 c1 11 dc 45 de f8 ee 77 15 21 6f fa 66 1c 56 e0 61 94 39 72 b8 93 ad 02 bb 5f 06 48 16 c6 c1 c3 74 0e Data Ascii: h'h.b;WT4*X5?r@IgU;!tvpuN`#ZTAWb0^[f)E0dP9EdwU[u(dIkaBKJ^jWW/R A+FvNHTJcPXNVLv&Ew!ofVa9r_Ht
2022-10-03 14:16:24 UTC	7044	IN	Data Raw: d6 f2 7d 95 f6 ef 41 00 f8 61 f0 cd 93 81 fa fb c9 32 21 23 a9 f5 ed a8 e6 e4 c1 e7 41 31 b4 41 33 d9 51 12 c1 23 9d 48 84 34 ed 4e bc 3f dc f7 98 02 dc db c7 ca 91 84 36 44 36 21 38 9d 96 af 64 ee f8 5c 18 01 eb 8b 16 9c 70 59 b0 e3 75 76 6d 8f fd 73 2a 71 6c e8 5e 3e 88 17 88 8e 2c 75 84 09 7f 2a 80 01 6f c6 44 7c 7c 45 a4 5a 57 58 7a 9b d1 96 96 f2 7c 3f b9 eb f2 5c c0 6f 46 90 7e 9c 82 f2 4b 2a 19 21 5b ac 1b 19 8a 48 d2 90 70 f4 78 da ff de 39 03 73 84 55 a0 db 82 50 92 bd 3d 2d b7 ee 0d 9b 0b a5 9c d2 d0 91 cb ba dc 91 32 23 90 31 6f b9 4a 24 c4 f5 fe 96 eb fe fa 0c 1e 0c 97 a4 46 17 8b 2d 37 37 37 7c d6 bb 9e 81 dc 07 e8 5f 55 e7 5c 20 e8 41 65 98 15 20 ca 5e 9e ea 5f 04 bd ab 78 dc 04 69 97 d0 56 8c 9a 0a 6a 06 32 c6 a7 47 c5 f0 7a fd 70 d1 e1 60 Data Ascii: }Aa2!#A1A3Q#H4N?6D6!8d\pYuvms*ql^>,u*oD||EZWXz|?\oF~K*![Hpx9sUP=-2#1oJ$F-777|_U\ Ae ^_xi Vj2Gzp`
2022-10-03 14:16:24 UTC	7060	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:24 UTC	7140	IN	Data Raw: 03 2c b2 55 90 9b f6 56 7d 4e 8e f0 f6 df 21 23 01 6a 62 53 17 11 f2 27 78 07 46 f0 d6 9c 7f 11 e0 fb 0b de ed 50 46 f1 e2 73 b0 ac 04 b7 6d c4 8e 26 04 56 28 93 fd 6e 56 1b fc bb 6f d1 75 f2 16 d2 51 6b 96 e9 9c 19 1c 8d 23 7c db 30 63 6b 24 0e 05 83 c0 4f 10 f9 86 e9 36 39 17 1a d6 55 3a 3a e3 64 bd fd db bb a8 41 04 71 86 a1 b6 08 9f f6 06 de 6d 16 36 ff cd 74 2d 23 6f dc 7d ad 47 06 97 88 d1 4c 0b ff 15 8b b8 0b ee 97 ba 38 f9 c9 16 fc 2d 39 92 dd 38 98 b4 b5 f6 21 00 7e 5b 58 a5 81 6e 0a 9f 9b 2b a7 e0 d2 fb 23 20 f3 43 19 2c 7d 48 cf 50 91 d1 d9 50 e1 0c 7c ad 8d a0 0a 34 2b 65 86 58 b8 34 04 b4 48 e4 00 d2 25 64 55 48 2d 99 9c 8a 97 0c a1 c6 d7 b4 64 29 19 8d df ec 5a f9 e6 aa 04 2d c8 ad 09 4a ce 7a 71 b8 8d 87 b5 ed 8d ea 68 27 d4 d1 37 21 1d 16 Data Ascii: ,UV}N!#jbS'xFPFsm&V(nVouQk#|0ck$O69U::dAqm6t-#o}GL8-98!~[Xn+# C,}HPP|4+eX4H%dUH-d)Z-Jzqh'7!
2022-10-03 14:16:24 UTC	7156	IN	Data Raw: b0 66 83 39 e0 8b ed d1 d3 41 a1 55 c5 20 66 4c 8a 5c b1 e9 0f ee 0e 70 0c ce 02 cb b6 80 de a3 0e de 2c b2 3d 4d d7 23 4d fb 4d 66 f7 2c 15 37 ff f4 b3 40 b5 9a 87 1f c8 1d 6f 0c 5a b8 60 d6 67 db ee a3 92 d0 f7 87 69 06 57 8a 78 99 62 1e d9 b3 a8 f3 99 83 3c f9 2b d2 53 45 78 77 dd 1f 50 ac 65 d0 83 07 b2 7a ff 08 5e d7 a3 1f 35 f4 80 bd 03 f6 f7 53 1b 9a 39 d0 4c 3d 32 15 04 08 ab 82 48 9c 1d bc 8b 01 47 3d a6 45 79 93 cc e4 c9 5e bc f2 12 31 a7 29 71 25 95 85 e5 99 80 99 ec e6 f2 f8 7e e2 48 d3 a9 07 b5 cd f7 98 31 13 9c 8e 91 54 f7 87 f2 ee b0 37 26 61 fc 88 3d dd f1 eb 30 f3 f2 38 4a a7 37 ee cc 65 e0 38 37 91 ea 64 4a f8 d3 3e 1f c6 c4 d1 2a c2 6b d9 ab 88 04 62 06 3d f1 2c ce 83 2d c0 74 ae ef 84 24 56 12 80 3c 69 3f 07 76 70 84 bf 0e 20 4a ac e8 Data Ascii: f9AU fL\p,=M#MMf,7@oZ`giWxb<+SExwPez^5S9L=2HG=Ey^1)q%~H1T7&a=08J7e87dJ>*kb=,-t$V<i?vp J
2022-10-03 14:16:24 UTC	7172	IN	Data Raw: 80 59 c2 61 c6 9c 8a 80 a5 87 b6 a2 92 a5 9d 11 b5 e6 9a 53 f8 63 10 f9 20 41 27 a6 7c ac 03 2b 22 6f 6a a3 4f 41 a7 24 28 af 30 8c 26 2c 3e fc 35 84 22 02 c6 05 1a a5 fe 2b 35 5a 0a 47 6c 4f 7f 32 21 01 28 b1 1e 35 90 af 26 6a 68 ed 9f fd b5 2b 53 fc e8 6e ef 28 34 67 3a e5 59 54 79 4d 8c bd cf 7c 72 c0 db de 81 ba a5 42 81 db 95 95 0c c0 46 a3 6c 06 5d 91 49 fd 8d 90 fb 15 72 80 ff 5b 77 cd 0d a0 42 b1 2e d9 e0 7c da b2 1e c2 b9 a1 c4 a5 d8 c3 30 be 80 d1 bb 78 9f ca 3b fa 7e d0 2a 09 7b 65 6d a7 d2 02 3e 42 f9 8b ee af e7 de f0 c6 8d 43 9a c9 94 92 08 78 d1 5f 95 ee 53 08 cb 71 e5 d7 06 db 90 9a cf e6 99 b8 03 69 98 1d 3d 15 f8 ec 17 a4 57 c1 82 ab d7 0f 96 73 6e a2 a8 bc 01 cc 8f a4 0d 56 d2 fe 00 84 6e eb b4 25 d5 ed 87 50 8b 49 25 fd 79 01 e7 2b 98 Data Ascii: YaSc A'|+"ojOA$(0&,>5"+5ZGlO2!(5&jh+Sn(4g:YTyM|rBFl]Ir[wB.|0x;~*{em>BCx_Sqi=WsnVn%PI%y+
2022-10-03 14:16:24 UTC	7188	IN	Data Raw: 86 72 4f 37 da 8f fe c1 4d 05 2d d5 ed f8 54 52 49 01 ca 2e b3 02 a1 94 cb 2a d1 84 af 25 74 8f 15 9e 72 26 4b f9 13 43 40 c9 f2 ca ac 2b a6 c7 f5 a8 e0 18 34 99 3d 42 11 3f a7 c0 2a f3 31 c6 a1 92 b5 e4 57 30 74 d1 5f b1 c2 a0 6c 20 b6 9b ed 64 87 7f 0a 96 6c 13 3d 9f 3c 63 33 b7 93 6e 60 42 9b 9a b3 9a 71 28 94 24 a3 7a 40 95 4d 33 58 9e e8 fe 41 03 90 00 22 a9 ff 18 4f b9 c6 c1 8a cf 54 59 90 ea 8e 2f 69 28 d4 37 c7 fe 36 63 84 14 7b 2b 34 9a 3e 07 9e 21 75 9b 8d 37 bf 16 55 1e 4d c2 44 5c e3 34 d7 28 3e 19 ec 1c 65 60 4f 55 6b 41 95 9f 9e fb 80 43 f7 ff 9e 4f 08 2d 79 b4 20 a0 ee fc a4 fe d8 7f 72 37 ad 86 e9 5a 1b 82 0a 54 00 88 68 c2 91 c2 06 94 b5 42 3b 3d a8 45 f2 df 46 2d 5f 56 fb 67 06 89 78 9c fe 2f fc e5 e7 0a 7e fc ac 36 dc 94 68 26 ff b4 e9 Data Ascii: rO7M-TRI.*%tr&KC@+4=B?*1W0t_l dl=<c3n`Bq($z@M3XA"OTY/i(76c{+4>!u7UMD\4(>e`OUkACO-y r7ZTh B;=EF-_Vgx/~6h&
2022-10-03 14:16:24 UTC	7204	IN	Data Raw: 7e 1d c1 93 a0 69 e6 e3 bc 04 1d aa 09 0d da eb db bd 80 b1 98 94 42 4a ff cd de 03 b4 57 5a 09 94 76 ab 29 35 35 04 57 d3 7f 36 a9 2d 66 e9 5e 73 71 c0 c4 d5 37 e7 6a 73 10 b6 4f 3c b0 87 4c 9e d6 c6 6a 90 29 a5 47 47 fc 34 f4 b5 f8 fa c8 d1 53 97 33 36 97 1c b2 60 15 43 ed cd 7f 9b 4d 12 f4 48 51 c5 ca c5 08 28 d3 cc 22 08 7e f3 c4 60 03 fe 04 1a 29 26 92 3c 37 56 37 ae 30 76 03 ac 73 25 b0 93 7d 55 c9 b3 d9 dd 7c d4 52 52 cf ed e7 dc 2e 13 8a 3a 73 88 13 41 8b ea e0 bf 2b 1b 29 6c 0b 67 3b d3 07 2f bd 1a 50 2e ee 99 d8 f2 d5 cf a9 a3 10 8d 3d 0b 30 a4 9e 73 ac d0 f4 94 a5 fa f7 81 bb 8c 19 7c c6 fe 8d e1 da 8c 98 96 93 4d b1 26 56 46 b2 91 fc 82 87 77 4c c4 bb 26 98 73 93 3d e0 00 3b 5e 13 17 98 96 2b ab 3e 4f d2 ab ee 62 08 06 2e 6b 6d 1c 63 8d 3e c7 Data Ascii: ~iBJWZv)55W6-f^sq7jsO<Lj)GG4S36`CMHQ("~`)&<7V70vs%}U|RR.:sA+)lg;/P.=0s|M&VFwL&s=;^+>Ob.kmc>
2022-10-03 14:16:24 UTC	7220	IN	Data Raw: 7c 1e 12 84 5f e6 f3 81 2b 87 f8 28 d9 27 1d e1 44 75 e7 e4 f2 4a 6e 0b 59 4f 4f dc 76 c2 81 0d 8e 42 48 26 6d 83 b3 bd 2d 5d 7d 03 d3 ef 9d c4 10 b4 ce e1 63 0a 34 6b 94 98 c1 9d 0f 6a 1f 40 e5 f8 df b9 eb 0c 4a 08 25 40 fd 1e 90 f4 af e3 69 08 b8 cd ce f7 96 25 b7 de 2a 05 60 9f 64 de c4 48 6b 4b bc fe cb 9e 2c 04 2e 1e bc a7 59 7f 7c 1a d4 e6 58 dc 6c 21 6d cf 91 03 49 1d 62 44 04 54 bf b5 f8 b8 f4 1f eb f7 37 82 8a a2 96 b5 31 fb 30 fe 15 74 73 7a 0b 43 8e 8d db e4 6a 13 f2 2c 5e 3d 6b f7 da 12 60 6d 72 5b 14 81 46 7f 9c 4e f7 fe 6f 8e cf d4 36 50 21 be 5c cf 7a 9b db 6d 49 23 b5 51 5d df 6f 76 83 f2 2c 95 37 2f 1b f0 14 e4 91 83 80 83 e7 d4 9c 2a 83 f3 1c 21 c8 9c 98 ee 23 e6 4b 27 9c 87 e3 c1 e2 e0 ec 98 7f e7 b2 13 9c 5f 5a 63 36 8f ee c3 68 5e 1e Data Ascii: |_+('DuJnYOOvBH&m-]}c4kj@J%@i%*`dHkK,.Y|Xl!mIbDT710tszCj,^=k`mr[FNo6P!\zmI#Q]ov,7/*!#K'_Zc6h^
2022-10-03 14:16:24 UTC	7236	IN	Data Raw: 5e 29 db df 9e 12 58 df fd 61 f3 a2 2b 98 0a d9 76 9d 8f 79 9b 94 15 7e 02 c4 0a 4c 44 67 11 11 0c f8 86 0b 46 ec d7 c1 5d 25 45 16 18 4e 40 b3 72 d5 fd 5e c3 59 f5 3b 3c 9f 84 b9 af 99 c5 7c 1f 59 99 64 38 6d 75 75 d8 5d d7 2a 64 72 f0 0f 70 23 4a b2 b4 1f 5e 91 a0 8b 5f b2 88 a2 d2 0f a1 62 ab fb 22 07 33 0f a8 77 43 63 0a e9 d5 bc 1a 73 26 a9 a1 98 dc f1 47 31 3d bd c7 d1 1f 97 60 9d 9e 09 57 4b 7b 6a 13 98 d1 56 ee 00 87 43 29 cc 7a ed 8b fb dd 7b f5 82 15 ab 0e d8 3f 23 f0 c0 61 dc 5c ff 93 41 e6 7f f2 f0 bc c3 9a b9 f7 dc 9a af 23 eb f6 c5 a7 5d 7d 99 3c 03 b7 49 20 26 18 dc 2d c1 b2 05 46 cd 15 c3 5b 75 f1 33 68 07 22 50 d2 35 50 19 22 dd ed 43 4b 3c fd 4b ca d5 6f f8 b2 9e 90 2b aa 7e 1c c5 51 72 06 ef 39 7e a0 81 00 94 48 52 ed 2b f0 d2 45 27 63 Data Ascii: ^)Xa+vy~LDgF]%EN@r^Y;<|Yd8muu]*drp#J^_b"3wCcs&G1=`WK{jVC)z{?#a\A#]}<I &-F[u3h"P5P"CK<Ko+ ~Qr9~HR+E'c
2022-10-03 14:16:24 UTC	7252	IN	Data Raw: 44 47 09 55 36 e3 c7 f8 98 1b 06 15 ba 4f a4 0a 14 63 a1 b5 b6 98 10 64 d4 bf 9d 17 19 0a 18 f5 45 2d a6 60 a1 72 f2 ec 36 19 d8 34 3d be 7b a5 10 f7 94 99 a8 93 29 31 36 a2 3a 32 16 6c c1 39 73 a5 a2 4c ba c9 46 da 2f e8 c9 b6 27 60 69 e6 32 d3 eb a5 76 b2 45 33 77 78 35 2f 36 7e e2 f5 7f cc 94 e6 e3 a5 52 40 66 07 7c 7b 91 a0 38 5f 49 10 e8 e3 f2 2f 70 f7 92 2d 7d 51 21 44 3c 94 20 0e 64 04 3d 2b 66 ed e6 60 c7 b8 3d db 9e ad db e2 4e 5f c6 ab c0 6a d7 8a 8b 8a 42 29 e8 c3 8b 02 22 e7 9e 23 07 d8 63 86 94 ef 92 5c 4c 9f da 33 bb 45 84 3c 69 18 0a fb f0 c0 40 cc 04 f9 a7 5e 7d b4 d2 bc fa 0d 6f cc 2e ae c0 92 bd 0e c0 b2 53 a1 24 82 72 30 62 00 63 3c f4 28 ee 33 e4 27 38 27 c3 30 89 b2 90 73 e0 3a 94 28 dc 7d bf 56 95 30 fb 61 4b 66 53 0b 8b b5 34 80 1d Data Ascii: DGU6OcdE-`r64={}16:2l9sLF/"`i2vE3wx5/6~R@f|{8_l/p-}Q!D< d=+f`=N_jB)"#c\L3E<i@^}o.S$r0bc<(3'8'0s:{} V0aKfS4
2022-10-03 14:16:24 UTC	7268	IN	Data Raw: 7a dd 64 b5 5e c9 1e 38 13 4d 95 1f bc c0 97 67 e7 36 3c 87 17 37 52 1a 7b 8e d5 e6 12 b0 c7 f4 ea 9f 7a e8 2d d8 64 6f 15 de 49 03 ff f8 2f 1e a2 32 41 ea 63 4d 16 3b c1 af 3a 6d e5 0c 5c 54 7f 66 8b 08 1e 00 36 b9 95 81 56 3a 12 59 0b b5 b9 83 ca 61 49 d2 8a 30 7f 58 79 74 a5 35 2d 2b ad 2b c1 8a 54 2b e5 f7 9b c9 ec 74 fb 46 5b 48 f2 ae 9d 6d 4f e6 2e ac 1f be 43 5b 8f 55 de ad a1 27 9e d1 59 9f fa e2 6e 47 c6 df c4 48 36 38 e4 79 5d 90 f8 ac 4f ff d9 c7 28 25 a2 cd 02 ca e6 10 cc 20 d9 58 e6 46 96 a8 f1 b3 e2 01 ff d7 21 66 55 15 7b 18 0a b1 cb 77 ae 00 6b 72 4a 0f e1 43 bb 40 08 24 e8 66 3b a9 95 65 d9 8d d5 78 20 23 ce b3 4c d2 da 87 63 df 58 66 9b 10 ea dd 66 54 61 73 92 ec 93 4a fc 21 41 0f 1b 99 f0 e8 f4 da 6d 14 17 27 44 69 c5 06 f6 1e 54 9c 14 Data Ascii: zd^8Mg6<7R{z-dol/2AcM;:m\Tf6V:YaI0Xyt5-++T+tF[HmO.C[U'YnGH68y]O(% XF!fU{wkrJC@$f;ex #LcX ffTasJ!Am'DiT

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:24 UTC	7284	IN	Data Raw: 3f 2a 1d 7d f4 ef 2e 7c e3 52 33 29 fe 9d 22 fc 35 46 5e 9c c4 73 1e 34 4b f3 08 5b 61 f1 95 5d aa 4d 0f 0e f7 fe 38 6e 87 09 ab e5 c7 e5 73 ed f5 d5 2d 0f 49 d2 08 ac 4f 8a 3e 61 de 91 8e 2f e6 df 76 aa 59 a4 f8 ba c2 a7 db e5 0a 83 42 bb be 26 4c 51 31 56 67 cb 67 15 f2 9a f3 42 86 38 4d 6d 55 85 3e fd 9c 82 d7 0b e4 a5 52 84 89 e8 c0 1c a4 e1 81 a7 2d da db 2d 87 01 0f 6d 9b 40 78 a4 82 62 b8 d5 65 c8 f2 08 a9 b5 7e a6 44 c0 59 89 8d 6b 9a 23 c9 35 1c b1 35 56 b3 5c c6 03 ad 32 1d 42 0c 80 20 81 5b 06 40 99 dc 3d b9 9a f7 02 80 90 2a d9 44 96 a1 e2 12 68 67 a9 58 53 a6 21 db ba 0a 4b e3 39 37 a8 97 3c d6 af 75 5d d9 1b fa a6 72 85 9a 20 71 39 68 9b 37 d2 ff 7c 0d 43 59 6e cb ad 88 d4 7f 4e 3f 3a 5d 04 9a 5c d5 ad d5 0a d9 49 e7 94 97 0b c1 94 f4 96 bd Data Ascii: ?*}.|R3)"5F^s4K[a]M8ns-IO>a/vYB&LQ1VggB8MmU>R--m@xbe~DYk#55V\2B [@=*DhgXS!K97<u]r q9h7|C YnN?:]\l
2022-10-03 14:16:24 UTC	7300	IN	Data Raw: c1 64 c6 c5 c2 c5 aa 4b ad e4 65 02 a3 bc 40 d1 41 08 d6 5d 4e 0f 4b e2 ef 46 ba 4b d8 c8 9e cc fc 37 b6 8b db a9 c1 66 ba c9 21 e5 08 85 26 56 87 17 9a c7 de ec 2b 40 fe 07 99 3a 90 c3 21 22 5c 75 bf c6 6f 95 21 ab 79 2e 30 8f 20 5e d9 b0 4e 75 45 9f 18 99 ab 2a ef 4b 82 ca fa 83 f7 bf 7f 9b 30 9f a6 a8 e7 10 52 04 d3 c3 8b 94 bf 68 b0 ab 61 15 5f 43 90 63 e4 89 87 09 8a ff 53 c4 f1 85 ac 7c ee df fe 00 3c c7 48 34 26 10 9b be 70 96 e1 63 50 a0 09 e4 36 16 be b4 29 63 38 33 81 e0 12 9e 52 4b f0 83 16 93 0f 07 96 e5 85 62 f0 73 32 ac 95 53 ce 5e b6 c5 7b 0a 19 84 75 6d 98 55 5e ac 4c dc 04 34 c9 65 2d 9d f1 82 61 5b 36 83 cc ed b0 39 48 e9 0d dd a0 71 9f e8 bc ad 5f e5 46 fb 99 81 0e 31 ce 6c fb c1 09 b5 be ba 61 b5 a8 c8 e7 e5 31 4b 37 86 71 60 c9 1c 69 Data Ascii: dKe@A]NKFK7f!&V+@:!"\uo!y.0 ^NuE*K0Rha_CcS|<H4&pcP6)c83RKbs2S^{umU^L4e-a[69Hq_F1la1K7q`i
2022-10-03 14:16:24 UTC	7316	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:24 UTC	7428	IN	Data Raw: f4 ad df ec f5 df 98 16 60 87 3e f7 7d 8c cb a9 66 7d 95 65 47 a8 a7 1b b3 99 aa a7 2a 26 0c 25 25 87 33 41 c1 c4 68 89 80 af e4 79 82 b2 49 cc d3 ab 72 95 1e 3c 5c 7a b8 0e 7f 6d bc 2c 63 bc 22 c3 0b a7 f1 e0 8f d7 04 01 73 55 29 30 66 d2 bd f7 53 97 12 31 f4 8b 50 af 6b 1b 49 cb 90 ac c0 4b 54 a3 15 49 b4 6a b6 b7 86 9e 92 bc c5 5b a1 df ea e9 3c d8 e2 9a 84 ea b9 c8 6b ff 37 1d 34 15 75 9e d5 16 42 b1 f3 09 f2 01 9b 51 7f 4f 8b 2f 7c d6 e7 94 17 8a c5 6f 75 9a fc 13 12 4e 3c 22 5a fe c6 c1 fa 9f 1e 64 46 ee 01 5a d8 35 c9 ef 67 66 d7 23 11 3f 81 7d 29 08 e0 e6 97 df 9e e3 e7 ea 52 48 94 54 e6 fb 1d ea d7 7b ef 19 4f 9e 0e 52 2f a9 89 78 bf cd 70 57 7c a2 c4 9c 19 f4 71 1a 2d 6a 1a 2e 68 39 b8 ce 67 a6 47 7c 9a cd 1f 10 d6 05 09 ef c1 c8 40 f2 71 24 10 Data Ascii: `>}f}eG*&%%3AhyIr<\zm,c"sU)0fS1PkIKTIj[<k74uBQO/|ouN<"ZdFZ5gf#?})RHT{OR/xpW|q-j.h9gG|@q$
2022-10-03 14:16:24 UTC	7444	IN	Data Raw: 05 7e 0b d6 27 cf 52 ca 6a 2b c9 24 b8 f4 bc 65 f7 9b fa 46 6b b5 d0 f7 f2 14 f3 a8 35 ec 8c a0 e5 be 7a b7 22 00 54 d3 37 28 43 5c f6 2d 1d 3d 5f 23 b8 c6 cc 18 5b 32 c9 11 f7 74 c4 06 a9 53 10 16 b3 d7 7b 3a de a2 27 03 c5 f1 76 8f 65 09 4c ea bc 17 47 c8 d9 35 56 4a 89 80 71 e7 f7 d9 49 af a1 32 92 bd cc 12 0c 8d e4 41 79 18 bb f3 42 7a 3a 7c e0 89 67 f0 ff 5e fc 54 c9 5e 69 d2 96 dd dc 9a bd 07 3e f4 0e f1 ba c9 3e 19 87 18 0f 92 d5 11 e6 84 09 4f a8 8d 78 ee e8 4e 40 6a 88 ed b4 74 d9 a4 b3 36 0c 9a 63 30 52 b8 05 a0 e0 cd f2 9d 34 83 35 d4 5a db 80 2e 2f a4 0a 26 18 ae 3f 18 7a f4 42 7e 9b dd 7c 16 98 dc 8d 44 a3 d2 02 30 60 31 7a e9 16 65 49 cf 5c 92 48 fd 5f c3 1e a3 b3 53 f0 02 5a 73 99 c8 e8 df 68 0c 6c b5 d4 0f ad 41 55 13 60 46 2b 4f ea 75 15 Data Ascii: ~'Rj+$eFk5z"T7(C\-=_#[2tS{:'veLG5VJqI2AyBz:|g^T^i>>OxN@jt6c0R45Z./&?zB~|D0`1zeI\H_SZshIAU`F+Ou
2022-10-03 14:16:24 UTC	7460	IN	Data Raw: ea dc 30 d0 c0 4e ef 1f d4 33 80 c9 67 f3 86 43 c0 ab 68 a1 f9 43 b7 00 76 f0 f1 5e 16 08 81 0c 41 fc 10 e9 69 de 50 4f 71 62 89 dc 61 24 cd f1 51 e1 85 5d 2b e1 2b c8 99 be 95 94 f5 a4 d8 3c ea 4f 1f 6a 41 11 6d d0 a9 25 40 a7 25 33 04 c4 16 50 4b 3a 81 53 89 43 2b ea a7 bc ac 7a 6e 9a 3b 41 b9 1a e5 2a f3 11 e2 08 67 b3 2a a3 7c b2 42 a0 a3 d3 e2 79 5d b0 a0 95 10 5d da a4 8a ab 04 5f 2d 0b 1c 5d cd 33 bd 74 92 68 87 de d5 84 1f 3d d9 52 f9 60 b1 65 98 d0 a6 68 49 4c 93 54 bd 6f 68 cb bb ee 13 c2 3b 6c e4 9b b1 b5 eb 60 15 b9 28 c7 7d c7 4b 3c 42 13 c7 a4 60 10 7d 51 3b da 5c d8 4d 89 2a 50 6c 62 8a b8 d9 4d 20 3d ed cc e4 d3 9c 29 b2 28 d2 24 3f 87 bb ca e4 c2 69 22 03 c0 2b 0f 84 51 1a 47 6f 1e 0f d9 89 9b 31 40 c9 99 75 2e 28 64 cf 4c 8d e2 95 a1 ee Data Ascii: 0N3gChCv^AiPOqba$Q]++<OjAm%@%3PK:SC+zn;A*g*\|By]]_-]3th=R`ehILToh;\|`(}K<B`}Q;\M*PlbM =)($? i"+QGo1@u.(dL
2022-10-03 14:16:24 UTC	7476	IN	Data Raw: 59 68 71 38 c6 a2 dc 9d 2d 6d e3 cc 13 7a 7b 5d 6d 95 98 27 ac 56 0e 98 31 f6 a2 d1 b2 d7 36 57 ff c9 ec d5 ce be eb 3e 4c 12 8b 7f 80 ba 7e e3 7d 44 4c e8 b8 1d 10 0d 07 17 9e 7b 71 99 60 97 16 c9 6c 98 9a 0a 63 40 2a be 84 90 73 1a c6 1d 07 37 b6 cb 99 ac fa a0 59 a1 4b 57 43 40 e5 56 40 f2 79 ae 22 8b 13 4a 41 5a 9f 62 f9 4e 75 7c 18 00 81 7b e1 e6 27 62 65 6d af 84 4b 45 8b 1f f5 49 32 c8 67 4f e0 49 d5 1b d1 70 66 da 2a 61 92 3c 24 f0 c3 94 83 eb f7 9a ff 5d 7a 3e 27 7d bb b3 93 cd 4e f8 54 04 fa 43 3a c9 f0 da 0e 13 cc fc 4a a4 c4 e0 13 b1 39 f2 af f0 51 4f 46 36 a0 c3 82 6b f7 49 d6 ec 60 4a 6a b3 83 9d f1 83 63 48 a5 59 99 c7 16 1a 55 99 d5 97 b4 48 e1 c6 3a 53 50 b6 07 ae 30 8e 86 26 4b fa b6 e8 8a 0f 3d 86 3b 24 56 e1 b4 a6 cd 67 2a 33 4c c9 bb Data Ascii: Yhq8-mz{]m'V16W>L~}DL{q`lc@*s7YKWC@V@y"JAZbNu|{'bemKEI2gOlpf*a<$]z>'}NTC:J9QOF6kl`JjcHYU H:SP0&K=;$Vg*3L
2022-10-03 14:16:26 UTC	7493	IN	Data Raw: 91 6b 32 55 06 56 7e 74 42 c3 8a 58 62 69 fd a4 f3 67 14 a6 36 55 5f 36 ee ee 43 eb 44 c3 c1 d1 b1 de fb e3 c8 57 37 e9 5a ba 8e bc df 93 b1 42 21 a0 18 49 5d 15 1d 82 c0 81 ac 1d aa 4a 09 ce 60 a5 8d 11 c1 0c 4f fe 96 9f 8f 16 7c 13 03 2e 1a 30 4e 47 99 4e ca d0 4a e2 0d a8 ba b5 f1 af 8c ab 94 24 42 50 10 7e 8c cb 80 5b 8a ef 14 f6 44 04 6c ab 0d f6 13 88 ac 7f a3 b7 bd 59 cd ce 31 b2 47 52 61 c0 b6 ad bf 52 21 b6 d6 8e a6 c3 38 61 2f 84 7e 56 f8 4c 82 d0 7b 69 e2 25 dd ac 36 a2 75 9e 8d 90 a4 94 0f f7 05 d7 46 ac e0 84 67 71 84 a0 5a f8 83 6c c4 39 20 4d 49 f0 2f 66 45 b1 b7 cd f5 b4 67 26 ab 09 1a 2e 5f fe fb e2 04 3c 7d ac 6f 58 29 b4 96 3e 5a 5d 3a 97 db d4 53 72 24 98 b3 0a 17 4c 33 27 2e 31 00 45 af aa 50 36 08 c2 89 96 5f c5 81 56 cb ec 22 d2 1f Data Ascii: k2UV~tBXbig6U_6CDW7ZB!IJ`O|.0NGNJ$BP~[DIY1GRaR!8a/~VL{i%6uFgqZl9 MI/fEg&._<}oX)>Z]:Sr$L 3'.1EP6_V"
2022-10-03 14:16:26 UTC	7509	IN	Data Raw: f2 b8 b5 1c 6c a8 0e 9e f0 05 a3 a5 dc 89 08 76 8f e8 cd f2 b4 9f 81 c5 3e 7b 08 b7 ea 9d e2 a9 c2 a5 35 b4 56 fb 1f d7 5c f0 27 c1 ed 03 42 05 e2 d4 b5 90 56 c2 91 68 3a fe 81 4a 55 9e 7c e8 08 43 42 5c c0 e5 fd ad 9b 56 34 aa e6 76 aa 17 47 cb ee 92 71 47 f9 aa b6 1a 4d 13 ff 5a 71 04 9d 3e ce 39 bd 51 e6 67 c3 4d a4 f2 b4 ec 64 06 80 bb e0 72 af 7f 75 3d 8c e6 ae 8a 45 5c 28 c2 f5 18 87 67 d2 ee 0a 83 9e 87 55 74 7f d3 c1 7d 33 5d 18 8a 7c 0c 7a dc b5 d4 9b d5 74 91 13 d3 26 c5 df 6f c8 c5 78 4b fd 6d 61 e1 3e 73 38 11 4a 47 68 d5 e1 f4 dc 38 e0 0c 5a c4 c0 22 ad 83 48 16 b0 a9 90 52 cd ff af d8 f1 8d 2c b9 45 67 4a 0a 6f ac b0 ef 91 26 41 5c 9f 36 8f 85 27 e2 bb 58 fa 1e 96 44 ea fc 06 37 20 5e 99 fb 75 79 37 70 ad ef b8 94 b2 24 2e 8a e2 58 dd b9 83 Data Ascii: lv>{5V\'BVh:JU|CB\V4vGqGMZq>9QgMdru=E\(gUt}3]|zt&oxKma>s8JGh8Z"HR,EgJo&A\6'XD7 ^uy7p$.X
2022-10-03 14:16:26 UTC	7525	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	7573	IN	Data Raw: fe 19 7d 64 f8 4e a7 29 cc 19 7c 38 1e cd 33 7a 76 e4 09 70 07 2e 56 b9 a6 99 53 d0 37 93 04 18 cc e6 e3 b9 45 90 62 b5 2d 32 df f1 d6 81 df c5 10 fd 70 48 44 3e bd 7e 27 01 8f 7f 76 c9 c4 2d fb b7 fc 50 cf 8d e1 18 3b d3 49 43 fc 6f 46 f3 54 a6 f1 e9 07 15 af 0c 7b 1a 1d 29 3e ae 2e ac f7 42 a3 40 a8 52 ef 04 ea cc 96 81 e5 2e 10 2d 89 ae 4b b2 3e f6 7d 0a 9b 1f 3c f6 94 82 f7 a6 87 28 09 0f 75 f3 53 93 ac 0d c6 de 49 cc 3a de ac 69 55 14 41 8d e9 42 86 3b 2c 90 95 0f c1 c6 5f 8f 74 85 4d 7f c9 85 40 8b eb 0a 3f 15 60 a6 5c 94 30 6b 10 77 03 f6 78 18 c0 e3 6b 14 7f e3 47 b9 ed 50 b1 b1 0d 47 5b 9a 7a 7a 6b e2 dd 78 f0 c3 ea 5d 65 4f 19 69 9d 5e 8b 67 95 7b 58 ba 48 85 c6 61 20 30 09 71 b6 c9 1c 46 58 19 d7 37 92 c4 bb 8d eb 68 55 6f 4e 23 ed 2f 1d ab 28 Data Ascii: }dN)|83zvp.VS7Eb-2pHD>~'v-P;ICoFT{)>.B@R.-K>}<(uSI:iUAB;,_tM@?`\0kwxkGPG[zzkx]eOi^g{XHa 0qFX7hUoN#/(
2022-10-03 14:16:26 UTC	7589	IN	Data Raw: bb 71 b0 29 bf 1c 8c 33 e7 55 26 7f 78 99 b0 22 07 6d 99 4a dc c7 15 2e e3 9a 72 56 7b 64 fc 24 fc 3c 66 ab f9 14 b8 d8 32 84 ca da 1b 8d 62 d1 be 96 7f f2 8f 7c 4c 22 7a 8f 67 9e ce 73 d9 7e c7 56 83 b7 91 7b b4 b8 f4 21 2d b5 e8 f3 1c b8 bd 3e 6d fe b8 e4 63 ba 20 d6 d7 ef 98 37 7b db 68 9b e7 a8 92 36 5d 48 16 0d d1 35 7f 59 e6 48 94 01 b4 0b b6 be 04 be 64 2f 14 ab 8e 3c 03 92 cc f0 3e af 8a 98 63 9f 2d 6b 95 31 12 7f 57 98 86 10 59 cb b5 9a fb 04 1a 3f c4 ad cd db 61 30 98 f3 81 70 ca 8b 48 8c ef 77 85 8f 09 ad 1d d6 7f 67 eb 74 c5 d5 11 63 79 ed 36 ba 68 c6 f2 35 fe cf 5c e2 99 30 ec 96 cc 82 eb 81 22 a2 0b 33 55 c8 d9 64 4b 06 0f 09 5d 61 80 48 46 2a 73 40 5b fd 8e 6f 1d 9f 45 66 47 97 74 5c 62 7b 1b 97 38 e7 fe 1d d5 4e b1 7f ff 39 76 48 62 ed 3f Data Ascii: q)3U&x"mJ.rV{d$<f2b|L"zgs~V{!->mc 7{h6]H5YHd/<>c-k1WY?a0pHwgtcy6h5\0"3UdK]aHF*s@[oEfGt\b {8N9vHb?
2022-10-03 14:16:26 UTC	7605	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	7717	IN	Data Raw: 20 3b 8c 38 ed 31 ba c3 94 b7 9a 57 37 92 2a e8 15 85 9d a3 d5 5b aa c5 59 51 a3 42 36 0c c8 b6 e4 dd e5 a8 dd c0 d8 5a f3 aa b6 b9 21 a3 41 ac ca 91 37 f9 16 77 3e fe 77 3e ab 4e 09 d7 27 ea f2 67 3b e6 f5 5a 14 4a c6 b1 53 15 f4 f4 40 7d 72 5b e3 fd 07 08 34 9b 0d 5b c1 89 91 cc 13 3e a9 45 f7 fa d7 87 66 f6 12 0c 6a 19 71 81 cd de 9f 30 5d a0 47 03 46 29 a8 bb ad 2c 48 8c d1 5e 55 43 7f fb a2 17 03 79 06 6f a1 64 65 1c d8 32 13 b4 ff 1f 46 b5 ff a3 c6 1e e1 9d e6 7e 31 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	7877	IN	Data Raw: e5 0d 8d 06 db 8d 8f 77 23 f5 05 b6 0f e0 d0 8b bf 2e fc 15 80 f6 aa ad f1 67 67 2b 43 6b 50 ed 76 0e dc 35 ea 2d a3 7b 7a 7d a6 2c 65 21 c0 6a 56 e7 01 e4 04 f6 13 03 a6 42 33 2c f4 40 b2 50 bf f6 90 38 eb b9 c1 03 db 07 fb e2 98 07 61 e3 1a 15 b0 e6 da f5 8a c0 d0 5b ee 80 57 09 c1 34 98 7c 51 3e ee 3f c2 89 db 06 6e b0 ec 9b e9 99 9f 00 de 23 3b 25 bf 89 f5 c0 2d 0f 90 63 b0 91 0f 25 b0 0b 07 20 e7 a9 ec de 0b 76 38 1c f0 2c 9f 7c 73 ae 91 16 9e 0f b0 f7 c1 b5 db db 84 7b 41 26 a7 30 c5 df ef 00 92 30 f9 1d 5b 87 56 61 19 cb 92 2a cf ce 68 84 b9 2d b8 dc 8b 41 37 bd d6 75 99 3c 09 27 e9 da 0e 77 f1 d0 e2 95 76 e6 e8 5e 25 08 ed 81 89 a8 2c bc b6 23 5b 01 78 21 be 5a 6d af f3 31 d0 61 67 b5 b9 0b 30 f3 0a 3d e3 f7 8b d3 28 16 5f b0 3a 4d d9 c9 70 9e 91 Data Ascii: w#.gg+CkPv5-{z},e|jVB3,@P8a[W4|Q>?n#;%-c% v8,|s{A&00[Va*h-A7u<'wv^%,#[x!Zm1ag0=(_:Mp
2022-10-03 14:16:26 UTC	7893	IN	Data Raw: 33 1a 51 e3 2c b9 f9 9d bb ad 20 63 50 d2 3e a8 73 90 4b 83 bd e5 e6 b4 20 ce dd 34 1f ed f4 a9 cd f1 7e 7b 28 e0 db b4 d6 57 d7 81 5a b8 02 36 f6 89 17 10 fa 5c 02 77 bf a6 c8 7b 59 34 6d f3 3d 6c 4e 65 0f 32 4f ef 73 d6 55 f6 e1 84 5b cb 02 6e 6f 2c c7 6c a0 51 29 33 6f 9e 18 a4 21 28 f8 bc 81 04 1e 30 f9 c7 f8 fa 61 e2 61 c8 ac 20 13 3e 28 74 02 34 24 ee c8 7d 88 9b 7e 5b 36 3c df 38 e2 40 82 de 40 cf e7 bc ff c9 e4 d7 fd b1 5c a3 6b 1a e0 99 81 31 19 3d 75 15 ba 64 4d 88 a1 f4 4a b1 4f 7f 45 9b 21 17 c9 d2 df 6e a9 5c 51 20 16 c0 e1 6a ff f7 c0 82 63 69 2c 15 60 d5 a2 af 53 83 f1 b9 8d 86 65 52 83 6d b9 96 89 8a 45 b2 b2 28 33 01 b9 23 02 55 7f f0 8a 98 b2 3b 27 d2 72 2a 54 3f 6f 5a 30 09 18 1c 20 e2 4b 36 27 6d c8 f2 f3 a1 e2 ad dd 58 1a bf f3 7c f7 Data Ascii: 3Q, cP>sK 4~{(WZ6\w{Y4m=lNe2OsU[no,lQ)3o!(0aa >(t4$}~[6<8@@\k1=udMJOE!n\Q jci,`SeRmE(3#U;'r*T?oZ0 K6'mX|
2022-10-03 14:16:26 UTC	7909	IN	Data Raw: 01 f2 bc 17 4e 6c 56 9f e5 20 a3 1f 25 ad 30 d2 7e 19 87 a6 da fe 47 3c bb 9f 1b f2 49 53 cb ff 82 51 b8 d3 bc 27 0f 81 60 56 59 e6 a3 63 2b 57 60 19 2f 14 59 24 e6 80 75 17 27 4c e3 35 a0 86 9d 67 0c 2b 56 c1 98 ed ea 40 03 d3 9c 60 4c 38 11 d1 3d 14 12 f3 e9 f2 5d a6 ce 17 e6 54 f8 1d 2e d9 90 46 7f 85 bc 4a 06 26 6f 53 86 fc bf a6 c4 dd 89 00 20 77 9c b9 95 22 50 d4 43 0d 33 5f ef e9 60 af 92 5a ba dd 39 21 8d c0 15 ad 2d 24 16 b9 36 c7 e4 9e b3 a3 b8 cb c1 87 23 51 e9 4e 70 00 00 03 00 00 03 00 00 4b 84 56 4f 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8021	IN	Data Raw: 40 4d 50 33 ea 49 75 af 76 57 ff 88 5e 84 9c c9 9b 5c 01 7a 3b 91 53 35 cf 5b b1 eb 85 f7 2f d4 0d 94 d8 91 38 47 fc fb 39 8b 11 95 0e 2a 30 1a 4e 1f 32 e2 19 1b 1c 0d a3 0c f5 04 71 28 3c 76 c1 c9 00 ed e6 a9 7d 2e da ed 96 fc 91 52 db 4c 5a 91 80 17 ec 63 40 ec e6 18 21 31 16 7f 93 c3 ec 17 2d 15 d8 f8 4e 84 d6 a6 4e a7 08 09 30 9c e4 7e f9 7b 05 17 63 06 68 45 d8 e5 d4 88 99 cc 53 d6 2b 91 b8 21 8b df fa f4 46 6c 48 97 7e 9f b5 08 79 b1 14 5d 69 46 e7 38 fc d1 93 04 08 ea ff ff a4 8e da b8 38 8a 15 fa 9b 52 15 47 2b de 31 41 02 f8 5e 70 45 ff 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8165	IN	Data Raw: c2 70 30 3d a6 ac 7c bd 9a f2 ee 24 f8 51 79 1b cd a9 56 6d 60 b6 a9 a2 60 0f 8d 92 bd 4d 52 c0 27 3b 30 24 6a f4 23 25 ea 8f 02 9f ff 52 9a a6 79 60 8a a9 c4 f2 39 88 a9 f8 5b 84 50 42 b7 84 c5 91 3f 14 dd 48 0b 75 b2 3b a8 64 18 32 03 16 39 0e 78 63 10 83 ec af a8 46 2a 01 72 b2 41 8f d5 5d 51 40 75 30 ca cc 90 f3 ff 2d 9a 93 52 a7 aa 01 32 df 8e 5f 75 1d 61 b3 27 b5 73 bb 14 49 cd e3 42 69 20 0a de 1a cc 5f 07 fb 2b 1e 72 5e e3 b1 a7 17 85 4b ab f9 b8 8f 84 a4 e8 f3 38 e8 da 17 ff 41 9e e3 c0 b7 ae 67 d9 5a 30 19 a3 78 5a e8 bb af 88 fe 8c b3 45 51 85 02 a1 ef 37 77 c8 fc f3 78 50 21 43 dc 1c a4 be 84 3d 2c 36 d6 6e e9 76 e4 1a b5 5e d8 77 00 50 be 25 3d 57 58 d1 a7 80 94 ca 01 86 6a 74 ea 75 74 89 c1 e0 50 52 aa 97 92 bf d2 91 cc 4d f6 11 ee c4 64 14 Data Ascii: p0=|$QyVm``MR';0$j#%Ry`9[PB?Hu;d29xcF*rA]Q@u0-R2_ua'sIBi _+r^K8AgZ0xZEQ7wxP!C=,6nv^wP%=W XjtutPRMd
2022-10-03 14:16:26 UTC	8181	IN	Data Raw: 94 1f f1 1a 5f b4 a0 92 84 bb 74 47 26 81 3a 11 96 57 d7 a0 a5 5d 16 98 db 36 24 e5 c0 33 ea c8 9b 3c c0 f8 39 bb 1f 72 e3 86 c2 98 e3 ff 1b 28 41 05 94 c8 14 5c 2d 36 c4 b3 8d 10 da 7e 6c 7d 7c 13 81 2d c8 73 1d 80 bc 8b 06 dd c3 43 2f cf 7d 0b 05 93 25 ec 8e dd be 64 c3 4f 8c d7 a6 e7 e8 91 8e bf 1d 86 77 69 6c c3 86 2d c9 3f 75 66 50 73 1f 13 af 6d 2e 6a 9b b9 17 b9 30 79 4a a0 9a f6 18 84 d6 c9 c6 74 c9 c1 91 bb c3 e1 33 2e 9b c1 df a6 cd 07 ea db 30 35 c5 64 c3 8d 6e b7 c2 dd fa 9d 0c 60 0c 5e d4 31 20 26 e5 26 37 97 e9 50 eb 0d f8 c9 92 61 13 2c db da b2 0f c3 d3 62 09 60 e2 2b 9c 21 0e ef a4 d8 71 70 7c c2 bc ac 82 52 df b7 e1 d7 b1 64 e7 1f 37 bf 6b e1 d5 68 33 eb c8 3d 64 a8 4d 3d b4 5d bb 62 ad 82 da b6 c7 68 82 8d 6c 3f 10 cf e0 12 a3 0c 2a ca Data Ascii: _tG&:W]6$3<9r(A\-6~l}|-sC/}%dOwil-?ufPsm.j0yJt3.05dn`^1 &&7Pa,b`+!qp|Rd7kh3=dM=]bhl?*
2022-10-03 14:16:26 UTC	8197	IN	Data Raw: 56 65 ab 61 75 4e 44 07 51 d4 2d 43 f7 53 ff 1f 07 fd ce cf 4d 13 73 40 30 69 9f 16 6b 43 6d 87 10 ab 2d b4 8f 6b e6 59 e0 1d 86 f8 f7 91 02 ef 3a d6 94 be 89 d6 1f c6 c8 f3 03 25 9c 56 fb 89 f4 20 cc a5 b1 5b bc 2b 1e 53 38 f0 5a ee 43 f0 3c e2 f6 c9 3f f0 33 02 da 1c ca 8a 3a 5f 16 d0 b7 b5 03 28 e5 43 95 63 95 50 70 9b 86 b0 80 18 9b 2c 78 d1 d4 11 77 30 6f 1e fa 05 71 35 53 12 11 05 d3 22 b7 4f c6 5e 83 d3 35 84 1e 1c c6 8c c3 38 59 42 da 1f 3c 34 c6 02 27 3c c7 3d d3 64 c0 e3 42 cb 67 97 a0 2d b1 d9 fd 25 41 71 f9 f8 34 30 79 eb 64 5c ea 79 c1 fb 25 b9 88 1d ae 05 17 de ad 7e c2 15 eb 5e 1e f9 46 38 fe 54 85 89 c6 ca 5e e0 40 18 87 05 fb f4 9e 6e 19 1a 37 20 b8 45 2d c2 c5 b3 2d d3 9a 24 6f 8b f9 77 8b bf e6 8d eb f4 9b 06 fb e1 cb aa c7 0f c7 9c c1 Data Ascii: VeauNDQ-CSMs@0ikCm-kY:%V [+S8ZC<?3:_(CcPp,xw0oq5S"O^58YB<4'<=dBg-%Aq40yd\y%~^F8T^@n7 E--$ow
2022-10-03 14:16:26 UTC	8213	IN	Data Raw: 15 65 1d 08 2b b8 f3 e6 cb 95 1b 4f da de 1b 76 59 76 3e be 11 14 35 78 cb bf 32 40 c5 02 c8 ef e3 91 30 9c f6 64 d5 2c 8f f1 84 3c 5c aa 29 bf 7d e0 3a bb ed bd f9 a3 39 d3 49 fc 29 2f a1 12 a1 94 62 71 b2 85 35 14 49 e1 f3 c4 19 d5 8e 77 ef d7 74 b1 e1 da 0b 8e ff 28 65 23 b7 00 fe 79 c6 91 35 30 3a 3b 5b 5b da 73 5c 11 c8 62 16 aa a7 3e ea dc a9 0b e4 7f 73 b3 0f b4 ea d8 85 ca 3b e9 2f 01 a4 35 1d 41 4f 4f 8a 12 66 cc 15 c8 db d3 35 34 aa ff 56 65 51 3e b7 ab 67 a3 ca 73 3c 79 4d 8d 40 3c b5 be 5e 18 05 92 70 b1 c8 73 36 84 81 e9 c4 55 06 57 6c 27 86 5b 58 e8 25 ee bf c6 fc 16 e4 2c 5a af cd c9 67 6e d8 75 e0 a5 2e a8 c8 77 27 6f 8a 33 91 66 8b 1d 3f 21 ec f1 0c 9f 72 46 93 a7 09 d1 15 3b 9a df e6 fb 52 5b a5 2f f9 b9 f3 68 f9 3b 88 c3 74 77 66 17 d2 Data Ascii: e+OvYv>5x2@0d,<\)}:9I)/bq5Iwt(e#y50:;[[s\b>s;/5AOOf54VeQ>gs<yM@<^ps6UWl'[X%,Zgnu.w'o3f?! rF;R[/h;twf
2022-10-03 14:16:26 UTC	8229	IN	Data Raw: 8d 29 49 7f 69 51 1d 53 cd e1 26 90 71 d3 ec c9 a3 ac 05 dc 5c 4b d2 00 16 a7 67 4e ee 45 16 ff 6a f5 fb 9d cf ff a2 66 7c 02 73 bc ae 90 81 26 04 d5 b2 f7 5b 8b 6f 86 88 3e d3 3d 37 04 9d 29 c5 7b c5 23 77 e2 3f 27 ff 87 3d 6b a1 57 fd 01 fd af 21 13 90 b5 7e 5b 91 d2 b2 4f 8c 30 2b b4 5c 33 a4 8e a8 04 c8 6f cb 1e 3b be c5 65 59 d0 17 74 2f c1 1b e9 af 5d 37 55 6a dd 9b 18 4b 8f 9d dd 53 55 d4 a2 9c 3f 69 34 ee a0 75 bb 55 7d 08 3a 8e e8 7d 34 6f 81 9a 5c 23 73 3c 5e 97 88 d8 36 98 9c de 0d 15 93 8e ff af cd 7b cc 35 82 ea 84 56 c6 75 22 bd e9 48 8d 2e 06 6b dc a4 3e 95 72 a4 7a a0 b9 5f f5 e5 2d a8 42 f8 fb 31 7a 78 e6 08 46 b3 a7 90 19 e3 c7 b0 9a 6a 3e de 25 1d 09 9b 19 8e 22 b4 fe 2c 43 c0 ec d0 19 e5 97 14 b0 5c 0d b8 83 47 82 3c ba 5e 8e f6 cb 1e Data Ascii:)IiQS&q\KgNEjf|s&[o>=7){#w?'=kW!~[O0+\3o;eYt/]7UjKSU?i4uU}:}4o\#s<^6{5Vu"H.k>rz_-B1zxFj>%",C\G<^
2022-10-03 14:16:26 UTC	8245	IN	Data Raw: 4c 1b c7 5d 55 a9 ee f2 bf db a7 c7 62 47 a1 2e 9e e5 33 7e 7c 5c 04 39 31 dc 10 c2 42 31 77 22 a5 95 52 33 e1 ff 5b 43 1c 9a 07 e4 dd 9b 8c 00 79 3e 69 0f 7e 07 6c 22 93 89 85 2a 28 c0 d7 cf 6d f4 67 4a df d7 7e 48 a9 ee 7f 45 42 72 2f 2d 95 3f d6 39 82 95 17 70 cd a1 b2 59 1b b0 6e d7 21 ad 34 71 c8 d0 eb 6a ff ed 9c ff 32 c2 c9 ec c6 1e 96 96 d7 95 80 23 9c f0 56 15 0a 7f fb db c3 78 3e 20 c9 1a 4e 39 ad 68 01 3d 92 21 96 17 53 b4 c5 43 fb 8c a0 df c3 21 e9 72 57 8f b5 d8 a9 01 05 02 73 4e 85 92 ea 0d c7 8e 54 99 30 97 01 5d 14 58 b0 3b 92 7b 93 4c 61 cb 9a 59 91 14 7f 5b ad e4 2a c8 e3 f5 73 ed 7b 6b 77 0d d9 76 41 44 2a 0c 2a 1a 11 55 6c 0e 63 08 ab 1a 02 29 76 c9 62 22 e4 93 a3 b8 d9 19 30 a1 52 72 0e f7 55 78 cd 87 69 1e f9 1e d6 bd 15 91 c9 0e 76 Data Ascii: L]UbG.3~|\91B1w"R3[Cy>i~l"*(mgJ~HEBr/-?9pYn!4qj2#Vx> N9h=!SC!rWsNT0]X;{LaY[*s{kwvAD**Ulc)vb"0RrUxiv
2022-10-03 14:16:26 UTC	8261	IN	Data Raw: 0a f2 ec a0 86 05 e1 79 d1 96 a9 25 44 bd e5 5a 4c fa 02 e0 1d cd d0 0d ea 58 93 30 9d e8 05 06 12 6a ab bf b7 23 8b 42 32 d1 24 f1 74 f5 bc 94 7c de aa 4a 2b 25 f6 2c da ee 4d cd 12 21 f5 41 4f 18 f9 eb ef cb f8 b7 a5 d6 0f 22 14 b0 fb 13 3f 2f bf ea bc d5 8f 83 4d 6f b5 54 5d 1d 50 8a b0 18 13 de 58 ef 89 8f 8f db 22 72 34 23 9c 0d 94 9b ea 96 ab c5 8b fe 41 5d a3 6f ad 56 92 d5 d5 52 15 25 3b d3 ef d0 a3 04 f3 9f 92 39 3c 60 34 7e cd ea 83 9c 2c 8a c4 bc a7 a0 5f 95 2a 5c 7f bd f7 cc 68 71 cb f4 2c 3e e5 13 44 93 2e fa cf ef 35 85 06 ec bb 83 ae 1e 58 6e 13 7c da 45 42 42 a9 60 66 c6 92 9c 9e 78 12 54 92 38 d8 29 e4 59 dd 99 d8 79 ab 67 4f 12 8e 69 2e d1 99 25 cb 2c a7 80 a2 62 28 a0 2f 5a bb cb 3e 66 a5 d7 89 ef a4 d6 ab 12 0d fb bb 2c 1e ef 20 a3 1b Data Ascii: y%DZLX0j#B2$t|J+%,M!AO"?/MoT]PX"r4#A]oVR%;9<`4~,_*\hq,>D.5Xn|EBB`fxT8)YygOi.%,b(/Z>f,
2022-10-03 14:16:26 UTC	8277	IN	Data Raw: 0b 48 70 e6 c0 32 e9 fa a2 d2 ae de 19 cd ef 9d a8 52 56 53 66 c0 db c0 8d b2 25 5f 71 ab 22 8a e3 93 43 50 37 f0 92 63 0c e0 85 f4 2b a1 e8 07 6b fd 9a 58 ce 65 eb cb 3b e0 7f 67 37 81 c2 61 d2 a3 ad a9 67 34 91 b9 9a 66 48 9b b3 c4 db 34 33 af 04 a0 5e 33 88 85 b5 5f 90 ad df 01 90 95 81 1b 70 ee ac 9e c4 84 be 96 59 ad e8 7f 91 90 75 17 3d 3c c1 9a 0e c9 36 11 bc 94 cf 77 d1 0f bb e2 83 e9 f4 f2 da cf 0b d7 55 1e d2 77 be 68 0a f8 ac 6d 59 d7 f8 d8 11 79 f4 05 89 4f 8a ea 17 35 0f 62 ca 59 7f 3b b5 ed 62 31 69 57 41 21 5c 3b 5e 59 15 45 4e 51 89 66 40 7e 3d 80 10 bb 52 38 50 9a 1e ae b5 dd d2 59 40 1c b3 9e 87 1f 45 90 43 3f 1a 6e 89 7b 05 52 c6 be 12 a8 51 43 17 48 11 62 4c d9 73 46 35 4c 85 31 c2 47 fa 5b fd 27 bf 50 d9 00 01 2f ed c2 31 a0 9b a6 0c Data Ascii: Hp2RVSf%_q"CP7c+kXe;g7ag4fH43^3_pYu=<6wUwhmYyO5bY;b1iWA!\;^YENQf@~=R8PY@EC?n{R QCHbLsF5L1G['P/1
2022-10-03 14:16:26 UTC	8293	IN	Data Raw: 6f 9a d9 6e 56 2a 8b af 4a c2 09 3a 46 6e 75 43 7c c5 a3 1d 35 7b 1a fe 6b 52 74 23 5a 94 a7 68 56 ef 2c b8 20 a3 0a f0 60 ab c5 d8 ee d5 d7 5e d9 de 0a f2 59 02 5d 38 b2 85 44 5d 9b 6e d7 c7 ba 19 0e 8d fe 43 10 d3 c4 1d 56 9c df 1d ae 03 aa 73 ea a3 b9 6f 28 c8 99 1e 7a 83 26 cf 3e 30 99 9c a9 b7 e7 92 b7 ad b2 62 52 b5 f6 0b 01 10 f9 0b 7c 15 85 0f 81 90 07 10 e4 f1 5a 2a 33 69 2d d0 5e 35 9c fa 3b a1 d5 0f b2 c0 bb 57 20 6e d9 00 be 07 cb eb 0c ac c2 65 9b 8e dd 54 23 8f 58 9d 8f 4f 5e cc 70 77 22 53 f7 6e 53 c1 c0 3a dd 3d d9 bc 5f 52 77 0b 64 2c 21 c1 3d 2f eb 22 eb bd 14 2a 35 dd 37 2e 96 1a 21 77 05 08 14 da 13 8f 4e d7 a2 bd eb 9c 64 e6 28 0c 60 e3 09 90 de 1b fc 7e 25 da d7 ef 49 a1 cc 2b 4f 4a 6a 0d 9a f9 eb 2d a2 c7 8d 7e 94 73 f0 fb 29 d4 a7 Data Ascii: onV*J:FnuC|5{kRt#ZhV, `^Y]8D]nCVso(z&>0bR|Z*3i-^5;W neT#XO^pw"SnS:=_Rwd,!=/"*57.!wNd(`~%I+OJj-~s)

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8309	IN	Data Raw: 77 09 11 6d 69 19 0d 99 32 0e 84 a5 5d 4b 24 b6 87 b6 41 58 0f 54 4a 83 23 3d 33 56 56 0a 83 1d 48 d8 3c e9 97 f1 4a 71 dd 37 11 19 26 03 7f 01 cc e2 11 5c b6 9e fd b9 6b 22 73 5d 94 31 91 1c 4e be 53 8b f5 62 64 5c 1f 47 cc 98 3c 0f f2 d1 3b e2 95 fa e6 e2 32 cb 4a be dd cc 31 04 ed fa a0 79 d9 88 30 7b a1 03 02 3f 4a 19 0c 74 ed 41 bd 45 48 c8 26 9b 97 89 df f5 4f 45 54 05 79 90 31 2d c7 a6 ed 53 cc 8d 05 29 36 36 48 ac 36 18 a1 ed b4 9b 5d dc 92 3e b1 89 a6 54 15 65 5c 31 b0 73 98 67 60 45 26 6b ed 12 7f 32 27 20 df 8c 28 59 ce 7c 3f fa fe 39 3a 0f f9 fe 8a 12 f6 03 db 1e 32 70 f3 6e 30 09 54 4b 39 af e5 50 4d 10 34 1b 23 e5 59 ab 9b 2f 4a 9c 42 86 43 d5 d7 c0 6f 6f 84 a6 1f ed ad 7b eb 00 05 ca ed d8 34 ae c8 d6 97 5c 89 39 bf e9 04 28 48 e4 8a 65 c9 Data Ascii: wmi2]K$AXTJ#=3VVH<Jq7&\k"s]1NSbd\G<;2J1y0{?JtAEH&OETy1-S)66H6]>Te\1sg`E&k2' (Y|?9:2pn0TK 9PM4#Y/JBCoo{4\9(He
2022-10-03 14:16:26 UTC	8325	IN	Data Raw: b3 47 80 f7 c0 82 4e ca a4 86 4f 78 39 4a f4 f8 45 da 8f 68 f8 74 ff 1c d2 07 64 13 6e 86 e6 75 09 e4 31 4b d0 61 92 94 ed 55 03 66 d1 ca 5b d1 8d 74 f5 db dc a6 af fe 6f 32 4a 65 64 52 76 8d bf a3 25 86 6a 57 cb 8c bf ce 49 17 3e cf 90 d4 c7 52 55 bd ac 1a 55 a3 e1 81 c2 91 a9 26 25 a9 08 51 0f 87 03 cd b7 d9 d2 6c 47 29 5e 78 3f 8f c0 bb bc 67 36 16 23 70 74 df bd 2e 97 36 22 9a f0 26 a1 f0 97 91 ed 97 ca 50 a6 f9 32 3c f1 35 f8 44 03 88 a1 a6 5d 54 6a b8 32 86 26 15 f6 48 b6 ac 74 56 04 4a a5 32 ea 1e 5f 77 e4 13 d4 1e bf ef ae 1f d2 24 d2 c9 dd eb 13 f9 ac 47 ee da b2 93 b2 6c 3e 80 5f 94 a7 5c 2d a6 a6 90 75 db f2 36 e4 13 b4 f7 76 78 c3 dd 42 57 0a aa ac 24 e5 06 88 0d b8 e3 d2 08 3d ea 39 fc f9 86 15 cb 01 11 73 df 1c 93 b6 29 70 e3 4e 93 9f 50 11 Data Ascii: GNOx9JEhtdnu1KaUf[to2JedRv%jWI>RUU&%QIG)^x?g6#pt.6"&P2<5D]Tj2&HtVJ2_w$GI>_\-u6vxBW$=9s)p NP
2022-10-03 14:16:26 UTC	8341	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8453	IN	Data Raw: a1 3f 70 da 6d b6 4b cb b0 43 f2 53 65 64 44 00 ed c6 f4 88 33 00 71 d9 96 b8 a2 33 7a 4c f0 c4 3f 0c 39 08 eb d9 42 a5 d6 14 9d 4e 74 dd fb bd bb b6 f7 53 a7 45 46 eb 46 74 16 6d a4 6e bb 1e 79 af 27 c2 ee 1a c2 c1 e2 60 8b 1c f2 43 23 72 a1 b1 31 b3 51 0c 5e 04 fe a5 6f 47 55 14 41 66 78 27 fb 0b e2 ae ea 14 21 78 b4 3e 1a 9a c6 8b 67 96 9e d5 99 31 0c 05 8e 78 d3 65 c2 46 4a ca a3 89 29 9c 2d 14 4f 91 19 e9 7a c8 a0 ea 87 ce d3 ec 8a ef 47 d5 03 e1 44 a1 ec f8 be 16 d8 c7 69 3d fd 11 cb 27 00 8f 66 c7 ab 98 48 06 6c 47 6a 8f 4a cc 5a 39 7e 59 1e 98 c2 2c 17 ba fa aa d2 8a 70 fb 4d ac 99 be ca bb 6f bc d3 9c db 0e 35 ba 7a 99 91 6e 5d 6b 98 18 cd b5 8c dc 64 87 e3 99 01 94 c2 ec fb 7b aa d8 4e ed 38 20 c8 24 0a bf 1e cf 9b 39 92 6d b1 f9 c9 e6 2a db fd Data Ascii: ?pmKCSedD3q3zL?9BNtSEFFtmny`C#r1Q^oGUAfx'!x>g1xeFJ)-OzGDi='fHlGjJZ9~Y,pMo5zn]kd{N8 $9m*
2022-10-03 14:16:26 UTC	8469	IN	Data Raw: 7e 6f 25 d2 b0 5b 08 92 32 24 7d f4 d6 86 56 3f 74 0a fd 10 29 67 c7 f5 a0 2d 2f 2e e5 1d 07 9c 4d 40 b5 99 19 ba 0e fc 79 8d 70 24 77 5f 0e 1a b5 83 4e dc e1 2c d1 37 34 b5 fe 17 08 d2 bc 1e 87 ba 23 3d 72 eb 42 f4 a7 fa ab 78 95 73 2b c5 89 85 f8 c0 8c 23 ea 9e 9c bf 74 80 75 61 a4 b6 7c 3f 56 1f 7c 89 cd 16 4d d9 b3 0c 58 11 cd a1 72 a5 d5 31 92 17 a4 cb 07 f8 cd 82 63 f0 5f 38 26 01 86 32 a5 99 96 ca a1 ac dd b4 c6 75 b2 53 fd ca 54 c8 37 71 3c 9c 63 17 81 d8 8f 19 3d 75 53 f0 ea fd d3 cf b4 14 9b cb b5 9d ce 65 f0 f6 9a 3a 9f 47 3c d1 d3 d2 22 34 f9 ea 41 e1 d8 99 e1 00 b5 6e f2 8a 32 15 ad 4d 5a da 4c 04 95 18 c5 af 20 61 74 c9 d8 cd ae f1 19 b5 c0 34 96 3b 6d 74 ab f6 db 6e de 72 c0 b0 08 9c f6 65 9d 99 a0 e9 f3 74 13 75 66 11 12 4a 82 a0 7d 8f 94 Data Ascii: ~o%[2$}V?t)g-/.M@yp$w_N,74#=rBxs+#tua|?V|MXr1c_8&2uST7q<c=uSe:G<"4An2MZL at4;mtnretufJ}
2022-10-03 14:16:26 UTC	8485	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8613	IN	Data Raw: 18 fc 71 a7 c2 57 c3 22 da 3e e5 e6 e1 f9 82 1b 41 fd 3b e5 0c 4c a3 e6 ba a7 b0 33 1f 31 c6 99 1e 46 4a f8 68 ea bb bb e8 d6 aa 1d 5f ef b0 13 59 80 fe ef dc d7 db 14 e4 b4 d2 54 9d 08 a3 f2 6f 4e a9 54 fd 16 ca 32 0e 23 79 71 2f a1 c4 bf d1 ce b6 d0 b6 34 bb 28 48 39 14 4f 03 1f 1e 9a 3f 18 e9 3e 81 84 5a e6 a7 10 dd 70 ba 60 76 23 ae f5 5a 45 26 c0 55 77 e5 d6 28 9e 1f 6e a4 e7 a9 8c e0 1e 84 51 9f ca 26 4e 70 18 56 05 a7 a1 0b b1 80 31 6f 73 f6 b0 41 c2 cd 07 2a 10 2e 15 7f 80 c8 73 17 d2 db b1 60 89 f2 4d 2e d1 1b e1 5e bb 0f 8f 88 6e c3 33 f6 4f 20 83 e1 63 1a 6b b3 13 67 9b dd 7f 0f 3d 45 8e 93 9d f9 4b 3e 08 00 dc 49 8d c3 d8 45 f9 2f 60 b9 6e 1a 11 f7 ef 80 c2 f1 94 e7 9e 09 7e 1e d5 ca 72 1d 71 20 01 92 90 f2 0e 3c 1f a7 e3 b9 7b 64 84 ae b6 be Data Ascii: qW">A;L31FJh_YToNT2#yq/4(H9O?>Zp`v#ZE&Uw(nQ&NpV1osA*.s`M.^n3O ckg=EK>IE/`n~rq <{d
2022-10-03 14:16:26 UTC	8629	IN	Data Raw: be 6f 28 5f e7 6d 58 4e 86 c9 a9 9c e9 16 60 1c af 9f 8c 7f d4 fc df e0 72 ba d9 12 f2 72 6c 50 73 d4 fd 8d 5b 9a 5e be 87 ab 8d 91 8d f1 8b 2e 34 27 87 a9 82 b2 4e 95 2a e4 38 b2 b2 ca a1 0f 77 6b 04 fd 49 ec 15 44 53 b0 08 7d 03 1c a3 af 4b 2e ca 2e 83 ba ee 1c e1 23 40 a0 fe 1b a2 36 dc bf 9a 37 35 5a 49 27 54 43 b6 06 87 87 a7 92 1b eb ab a7 27 42 a3 d0 6e e5 80 22 05 17 1e d8 c2 25 31 9e 89 e6 a3 b4 7a 18 35 c1 cf a6 aa af fb c7 83 e3 a6 84 17 09 5a 34 12 87 81 87 a8 17 4a ad b2 34 46 4f 8f f4 f7 aa 75 73 c1 59 84 9f fd e4 3a a8 73 e8 15 54 e8 c8 59 5c b2 52 d1 3d c4 43 9c d8 98 7b 6f dd 49 7c de 89 ee 8e 70 c6 50 e7 56 ad 5a 4f 63 c7 30 cb e7 1f b7 23 a1 8a 36 40 9d a3 4a 6f 03 9c 7c 07 ab 5a 58 0d 0e 03 88 7f cc eb b7 d5 c5 88 76 2c 4d 81 89 89 53 Data Ascii: o(_mXN`rrlPs[^.4'N*8wkIDS}K..#@675ZI'TC'Bn"%1z5Z4J4FOusY:sTY\R=C{oI|pPVZOc0#6@Jo|ZXv,MS
2022-10-03 14:16:26 UTC	8645	IN	Data Raw: b0 c5 d5 6d 66 88 6b 85 b5 09 6d a5 44 21 c4 88 85 a7 52 d9 31 1b e0 01 50 ca 47 34 03 22 43 af 36 20 6f 4c dd 08 00 8e 54 ec 88 97 86 c6 90 4d 8f b1 d9 51 88 eb 30 82 fe 23 3b 2c b3 99 e7 06 e6 95 6b 7b 1b a2 0c 8b 34 72 16 3c bd 04 3a 43 b5 f4 c0 be 1f f7 d0 c9 ac 7c dc cc 6a ef 18 2c dd c1 ba 15 fb b2 8e d2 5e 15 56 f2 a4 29 1a f4 e7 fe 7d 3b 2b ab 4e 8c b9 f0 44 2f 6f 27 06 d8 37 cf fa dc 7c ce 25 a7 16 1c 5e b2 0c e3 25 23 09 97 4f 6c 2c 82 89 99 cf ff 37 d2 1e 49 bb 67 fd a9 f1 7f 5a b6 56 6b 9d cd 1d b1 e1 9b 25 46 bc 91 44 6f 69 b3 8a 35 aa b8 12 a0 5f dc 7d 4e ba 88 1a eb b1 c4 6a 64 47 11 5a 50 16 ed 8a 38 62 42 1c 57 10 2f 3c 9b 53 08 2e 82 d0 70 bc 4b f9 45 dc 23 5c 64 32 e6 af c8 40 e1 0a fb 51 cd 68 fe 82 61 46 f9 05 61 7a a3 ac 6e 86 ec b3 Data Ascii: mfkmD!R1PG4"C6 oLTMQ0#;,k{4r<:C|j,^V)};+ND/o'7|%^%#Ol,7IgZVk%FDoi5_}NjdGZP8bBW/<S.pKE#\d 2@QhaFazn
2022-10-03 14:16:26 UTC	8661	IN	Data Raw: 90 7e ca d0 5a af b8 a3 b1 36 a6 0d 87 fe 18 77 51 9a c2 77 38 6e 9a ca b7 e2 8f 8e fd 85 95 7c c7 fa 26 9d 27 af 2d d9 2c b3 75 2e fb 56 df 74 52 56 e1 83 86 e8 ee 19 6c 10 1b 28 7f 35 5c 35 2c 6e 38 47 45 09 49 11 6c f0 7b de 84 e2 12 6c 47 45 19 19 bd f9 52 86 d3 f8 8d 73 e7 d6 4f 78 c0 aa de bd f6 d1 3d eb 06 d2 c9 c3 12 cc 55 5a 95 0c 31 25 e7 37 bd 1b fa 02 18 a2 35 cb e5 66 3a 43 72 49 f4 4e ea e4 f7 5f b0 d7 93 3c ae 33 55 4e 82 85 d6 e8 84 c5 77 b7 02 3e 60 7a ef df ce 92 d5 7e a0 d6 1d 9f c5 67 1a 19 c3 c7 58 6f ee 71 a1 74 d2 48 11 90 d0 a1 e8 9c b6 e3 d4 3c 2e a3 30 76 7e b2 94 a0 d2 18 c2 fe fc 2d 32 71 f3 be 39 94 81 6b f3 e4 9b 9f a9 3e 3d 6f aa 9c d8 5f bf 8f 08 c4 65 2a 2f 99 27 ae 09 58 26 90 ea b7 8f 5b 6f 04 17 da 20 69 c2 e9 c8 eb de Data Ascii: ~Z6wQw8n|&'-,u.VtRVl(5\5,n8GEIl{lGERsOx=UZ1%75f:CrIN_<3UNw>`z~gXoqtH<.0v~-2q9k>=o_e*/'X&[o i
2022-10-03 14:16:26 UTC	8677	IN	Data Raw: 87 89 a7 73 46 92 a6 af 41 98 eb 0e 8b 24 07 45 ba 1f 08 65 85 46 9a 09 68 58 56 be d8 5f 19 86 8d 4d f0 74 6e ce 96 79 02 78 1e ce 31 08 bf fb d2 98 71 55 fe 82 e2 59 9a 18 aa b4 75 ad 8a c9 58 92 5c 6d c1 f6 bd 97 dd 9b 7a df 28 4a d6 5c a2 7c 71 d9 3b de 65 74 b4 6a 52 3e 80 d9 24 0a 8b 51 95 2e 88 82 7a 19 2b 65 08 db 8c 64 04 7e e1 48 f3 46 b7 b0 2f a8 e5 31 e0 b3 54 62 70 75 25 78 2d 98 89 b5 ce a2 9c 37 12 a8 f5 b9 c6 3a 00 40 51 bc af 5f 4e 01 ca 88 4c 22 9b c9 4e 88 f2 1f 2c 54 6f a7 62 75 bd 29 37 70 ac 99 8e 0f 21 4c ba 22 ff a5 21 a2 d7 9b 58 e7 e0 46 67 25 9a 44 a3 87 4a d6 e2 83 b5 6f 14 40 f3 91 65 ed 26 56 be b5 5c ee ab 85 33 8b 7c 2c 8f 04 64 cc 61 f1 32 32 1e ca f1 ef 1f 70 74 e5 f4 35 ed 6c 64 bb 28 03 10 95 b1 13 ab b3 c5 40 cd fe df Data Ascii: sFA$EeFhXV_Mtnyx1qUYuX\mz(J\|q;etjR>$Q.z+ed~HF/1Tbpu%x-7:@Q_NL"N,Tobu)7p!L"!XFg%DJo@e&V\ 3|,da22pt5ld(@
2022-10-03 14:16:26 UTC	8693	IN	Data Raw: 10 c2 92 8c 58 18 7b 86 94 f6 9e f8 45 f1 55 aa 32 ff 12 0f 35 ee d5 57 39 2b 41 79 ba fe a2 80 79 41 77 9a e9 f0 83 2f ff 52 2d 8e b6 db a1 a6 a4 19 b2 66 ff 0b ac e7 2a 35 30 c8 a8 fe 5a 81 8d d0 3d a2 4f 77 61 17 4d 7e 38 75 d4 04 d2 f7 71 ed 15 71 8d a3 ba 74 cf 15 17 a3 2d fb 36 da ed ad 6e 81 7c 1f 10 1f 9e 4f b4 b5 f0 4f f9 77 0e f2 3a 16 73 68 d0 3b 10 fe 12 2a 7b 7e 6c b1 6d 36 fc 6f 91 db 92 03 f0 92 77 e3 3f 98 48 e6 db 2f 18 6f f4 64 62 bb 5f 0a c2 81 fa 67 29 39 3a 06 7e e4 58 4e fb 49 35 8e b5 19 98 38 1d 04 62 dd 44 f6 82 72 5b 69 42 8b bb b8 b9 1a e9 a2 fc 55 93 c3 bd 21 fa 50 f0 c3 63 06 b8 af 4d c1 15 be bd a6 be 9b 11 d7 95 15 a2 c5 4e 88 52 5d 53 5f 9d b2 2e 56 80 bf 7e af 52 d6 fd 5f eb 20 3e d9 1f 47 d9 f3 d4 43 7b dc c5 20 27 83 d5 Data Ascii: X{EU25W9+AyyAw/R-f*50Z=OwaM~8uqqt-6n|OOw:sh;*{~lm6ow?H/odb_g)9:~XNI58bDr[iBU!PcMNR]S_.V~ R_ >GC{ '
2022-10-03 14:16:26 UTC	8709	IN	Data Raw: 3f be 8e bc 63 40 c1 f4 0e 9a 35 4a 90 5e d2 cc 5b 92 b3 88 e1 d0 cc bc 59 f6 ac c3 92 8b cd ed 0f 2e aa 3d be 53 4b 46 b6 e7 80 c4 15 5b 8e a0 09 ce fa 34 47 01 fd 27 b8 8f 47 e4 73 3d 1a ee 1b b9 d9 08 72 ec 74 e2 fc 8a 89 27 b6 0e 13 fc e9 69 97 c3 59 2d 96 70 1a 45 cc 68 70 7c 86 68 d6 e8 63 f6 60 c1 ce db 70 d0 8a 2c c9 2e f6 c6 b4 45 3a 36 d5 32 6a d9 21 7a 37 a9 31 0c d7 12 28 c7 dd a4 bf ab 2d 92 5a 41 95 6b 03 98 85 5c 9c 13 e4 43 93 7e 58 c7 d6 3d f9 1c 23 85 fa 76 f8 eb ce d2 39 68 13 83 2e 17 89 da 91 bf d2 10 82 db ee 5b 0e de a0 bb fb 17 c7 24 89 98 f6 2c fb d4 f2 a4 4d c9 dd 00 f2 d8 19 47 44 6f d3 65 3a f4 f9 c7 e8 a6 6c f3 cc 93 b6 9a 3e 61 57 3f 5a 3d 0c df e4 8a a7 1f b7 23 c4 08 ba 51 e4 f2 84 74 e3 11 fa d8 7a 7e d6 16 49 6b ce c3 9e Data Ascii: ?c@5J^[Y.=SKF[4G'Gs=rt'iY-pEhp|hc`p,.E:62j!z71(-ZAk\C~X=#v9h.[$,MGDoe:l>aW?Z=#Qtz~Ik
2022-10-03 14:16:26 UTC	8725	IN	Data Raw: 18 fb cb 9a a3 ab 7d c3 81 7c dd 39 62 36 19 55 b0 8b 56 06 18 ba ca 48 85 53 d9 6d c8 bf 9c 40 f4 51 a1 db 63 79 91 5a 3d 7c de 6e 8f ab 05 f8 95 4a df bb 32 6e d8 98 66 5e 12 c6 70 d5 d8 7a 90 af 60 69 fd 1b 60 d7 d8 8d 66 54 c7 b5 f0 30 0b c5 13 e9 b6 99 a0 1e 81 f2 ed b5 99 7c b0 18 44 dc 68 7d 1c a4 06 10 0c f1 d3 6e 14 be d0 4b 22 fc fc 53 ca 6c 13 cb b8 93 b1 a4 c6 ed 59 65 5f 28 26 b2 ca 08 a0 88 dc 8b 76 83 5c 26 1e 4a 62 aa 7f b3 3d 65 71 61 d4 bb 9d 3b 89 b5 6e 0e c5 ed 72 14 56 f2 04 b4 09 75 8e 1a 54 16 1e 09 7c d2 64 b3 47 00 43 19 bf 3b 2b b5 5f 36 30 9a f5 2f ae f0 fe bc 83 c7 bb b6 26 c9 8d 1b 77 14 3a ee 27 0f 20 12 c1 87 a8 d7 94 6a b2 b5 27 46 0e 08 15 dd 27 58 22 ff a1 c1 ea 04 60 6d 2b c5 1a 8f d6 d1 25 bb f6 64 35 a6 5e b1 99 20 d1 Data Ascii: }|9b6UVHSm@QcyZ=|nJ2nf^pz`i`fT0|Dh}nK"SlYe_(&v\&Jb=eqa;nrVuT|dGC;+_60/&w:' j'F'X"`m+%d5^
2022-10-03 14:16:26 UTC	8741	IN	Data Raw: 06 36 2b eb 3d b8 5d 40 c8 44 80 1a 2c 2b fd 30 be 6f 19 32 c8 98 53 fb da ef 42 0d 75 3d ca ea 5b e0 ce c2 80 9a 93 5d 41 56 85 75 30 3b a4 f5 bd af d1 46 fc 61 99 ec c2 1d 80 66 01 d6 a5 24 57 9b 99 7b d9 32 4f b4 7a b1 7a 52 0d 96 22 8c f5 fc 0f ee 78 43 ee 71 ce 23 87 9a 99 0a e1 fa e9 e5 0e 49 5f 40 1a df bc 84 1f 1b 75 6f 3d eb 0b f7 77 61 88 47 89 a9 43 47 cc 46 9f 6e a4 b0 b8 71 1e bf 2b e7 6d 09 f1 04 50 98 c2 b6 4c 79 17 4d 3d 1a 80 d7 9e c5 ab 2d 0c aa 18 bb 94 f4 cf 96 eb 73 1e 99 1f 47 1f 9b 87 0c 3a 3b ef cb de a4 e7 77 b1 9e 9c f4 4b d5 d2 ad 88 e8 15 07 35 3b 5c 21 fc a0 a7 58 e0 07 f9 b8 85 57 ff 1e 24 56 9e e6 7e a0 a2 f3 92 0f 3e 2e d4 b6 43 96 37 87 5c c2 15 eb d7 19 09 2c 69 2b 26 52 1b 87 2f f6 68 64 13 77 53 d3 ba bd 96 d1 2e 56 d4 Data Ascii: 6+=]@D,+0o2SBu=[]AVu0;Faf$W{2OzzR"xCq#I_@uo=waGCGFnq+mPLyM=-sG:;wK5;\!XW$V~>.C7\,i+&R/hd wS.V

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8757	IN	Data Raw: 12 03 75 6b fe 67 97 5a 64 85 07 26 18 d1 40 b9 47 59 85 86 fb 9a a2 8f 61 ab c7 f5 9b 41 57 49 27 ae 9f 05 23 52 29 ae aa 79 73 0d 15 23 3c 94 94 81 85 7c 05 ee ce 5c 77 93 6b b4 2d 6c a5 ee e1 7b 72 60 0b 28 90 ea 77 7f d7 51 eb 48 c7 c8 23 a5 07 dd 21 83 30 74 53 5b e8 80 c7 7c 74 b8 61 80 10 3e 74 07 38 88 8b 15 1d 5a 68 23 77 99 28 10 43 6a f9 cb 5d 86 b7 4b 8c 93 6a 1c 47 49 83 ca da 89 aa 75 e1 37 ae d0 02 b3 9a eb 8e 89 de cc 87 b1 5c 25 f5 1b c4 d0 85 12 fe 86 39 c6 b6 ff cc f4 10 54 3d 61 23 13 18 8e ad 57 37 86 00 3f 7b e9 ea 0a d5 71 38 c7 52 d1 a4 b3 3f bd 2d ec 8a 87 cf 9d 75 c9 5c 18 52 1a af 97 b7 c9 87 a3 0c a1 c7 d2 b4 c7 5a 8e 6f e1 b2 72 a1 97 46 24 ad 8f 7d 5c 2b 8a a7 2b 04 78 6c 3c 84 8c 1b 6a 1a c0 c2 e6 e4 6e 3b 8a c7 b9 10 2a be Data Ascii: ukgZd&@GYaAWI'#R)ys#<|wk-l{r`(wQH#!0tS[|ta>t8Zh#w(Cj]KjGIu7\%9T=a#W7?{q8R?-u\RZorF$}\++xl<jn;*
2022-10-03 14:16:26 UTC	8773	IN	Data Raw: ef d3 36 c3 a2 58 9a 1e b3 06 85 e1 c6 2e 40 2b a2 56 0d 5f 41 48 97 a0 40 13 19 6a 65 31 f7 57 6d 5f 22 c7 35 ea 3f 42 bf 1a 22 70 c1 38 a9 41 05 fa fa 15 7f d3 a1 a1 bf 3c aa 43 b0 d7 67 71 55 64 6e 1d 7b 1d e4 5f f2 08 8b 7e 5a 87 a8 69 74 be 64 78 74 a9 15 fb 06 b4 a8 36 cd ba 7c 9b ee 6f 5c 45 41 07 28 e6 3b c1 d4 22 57 f2 8a 60 c4 a7 2a 1f e2 54 ff cb e5 dd 94 aa 14 35 ca 8b cd 7c ad 0b b8 98 5a 37 f5 0f ab 34 87 b9 55 72 89 a7 25 86 9d 65 e6 6e 65 12 73 14 2a 93 8a 0e b9 a4 ce 79 35 31 d3 95 f0 5e ef d9 e6 99 d7 4b 93 16 f2 08 9b 46 0d b6 eb 7d c2 3d a1 c4 a1 94 17 48 81 41 26 4a 09 6d 6f 39 5c 82 5c 45 8d e4 f5 0e 7d 45 5f bc 6f 71 0c b0 a8 93 e0 df 0a 91 bf 9f 38 4f d4 53 cd 7d 52 dd 53 fa 52 fc f0 79 33 52 1d 50 f0 46 bb af c9 4b 3a 14 11 cc 9b Data Ascii: 6X.@+V_AH@je1Wm_"5?B"p8A<CgqUdn{_~Zitdxt6|o\EA(;"W`*T5|Z74Ur%enes*y51^KF}=HA&Jmo9\\E}E_o q8OS}RSRy3RPFK:
2022-10-03 14:16:26 UTC	8789	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	8901	IN	Data Raw: 8e f3 44 9f 12 12 17 87 dd 18 a9 a2 a6 b4 fd f3 9a 61 e0 5b 9f f3 85 ec a1 31 d4 05 d7 21 01 ee 4c 6d f6 1a e2 99 fe 66 bb bb b7 25 69 11 6f 51 15 b6 9f 8d 2b b5 c9 d4 37 78 64 e8 67 75 b8 04 38 74 46 bb 76 ae a3 eb 3c 5a d5 4b 45 ba 18 e3 39 b3 e1 ac 8b c7 6e 8c e6 da 79 b1 cd b9 34 17 80 68 68 17 00 9f 8f 6c 16 6c 5d 4e 83 97 f0 2b 33 5f 90 76 08 0a 82 16 d1 eb 54 89 16 c8 d7 b9 03 4f 2d 10 fa 23 b2 13 fd db 16 90 02 ec 05 b0 aa ab fc 71 fd 72 9e 68 55 6b 38 5e 1f 6f 88 62 35 2f 1c aa bc 4a 48 b7 2e 27 6d f8 67 12 db 46 16 c0 38 92 ec d4 d3 03 83 e2 20 0b 49 40 1d 31 56 9a 92 0e ab be a4 37 74 28 df 4f c9 44 46 c0 e1 54 d4 df 05 bf 82 be e4 82 86 88 78 91 50 00 31 45 e5 7d 66 33 fc 7f 7d e8 8b 3f 3f cf cb 59 08 e6 3d 9d f1 66 a9 4e 88 34 34 79 2f dc 3e Data Ascii: Da[1!Lmf%ioQ+7xdgu8tFv<ZKE9ny4hhll]N+3_vTO-#qrhUk8^ob5/JH.'mgF8 l@1V7t(ODFTxP1E}f3}??Y=f N44y/>
2022-10-03 14:16:26 UTC	8917	IN	Data Raw: 47 43 35 54 d0 ab e7 60 9a 1d 5a ef 0d 7e bc 60 6f 87 23 cb 6c 1b 63 06 43 d6 8b d6 48 75 64 e6 86 87 74 fd c0 4d bc b5 eb db a0 35 0d fe ca c6 ee 5c be 4f a2 0e f0 f1 5c d7 5c 26 28 36 b8 ec 05 2c a3 ab 07 fe d7 13 47 29 2c 8a 65 fc 99 0d 63 0f 1a 78 ea f9 d6 33 0c 23 1d 17 96 31 66 03 bf 1d e3 4d 00 b3 26 9a 54 32 94 69 2b 96 9e 4b 21 f7 89 43 9a 76 15 2c 95 23 13 d3 1e 24 3c 11 84 58 37 dc f0 2e 6a eb be 0e 48 e2 8b 58 e8 eb 6a 3e 76 e2 16 9c 6c b7 81 d3 6b 2d b0 7c 3c 8f bf 78 e5 9b c0 c8 c0 ce 25 d8 d2 50 c4 b4 bf c2 97 6c ca 63 fa b5 17 f5 59 45 93 56 1b 18 f9 d0 34 39 50 f6 9d 0e 76 26 db b3 07 32 7d b0 9d e8 a3 8b d4 be 83 55 6c a9 82 36 34 9c 3b 44 1d 09 24 37 49 9f 75 99 7a 26 4f 24 7b e7 00 86 0d 85 a7 69 6f 7d 5a 77 cf 11 79 66 ab 2c 40 5b 09 Data Ascii: GC5T`Z~`o#lcCHudtM5\O\\&(6,G),ecx3#1fM&T2i+K!Cv,#$<X7.jHXj>vlk-|<x%PlcYEV49Pv&2}Ul64;D$7 luz&O${io}Zwyf,@[
2022-10-03 14:16:26 UTC	8933	IN	Data Raw: 0a f4 55 c6 74 1d cd 75 6a 0d f5 b4 fc 74 21 df 28 83 89 47 48 ca 5f c4 31 c1 1d 59 36 3a 88 ce 69 81 c0 6b 6f 16 76 b5 18 aa c5 02 a4 c6 a9 55 c1 80 54 0d 86 76 82 6b 87 56 3b 2c 94 a2 74 67 2f e0 30 cb 48 d9 0b 97 67 0b 64 5d c0 ea d1 89 44 e0 ef 4b 09 fd ea d7 09 60 82 d8 f5 bb 69 64 d5 c4 cd fa 31 c2 76 d6 c2 18 06 a2 30 df e4 80 0d ae 63 4d 66 09 3d f9 ff 58 a8 82 2c 38 3c 0f dd de 6b 33 e4 23 68 8e 27 f8 d5 fe c2 6a a8 85 5c 0a a4 0f 41 7f 18 1c 11 fa 16 32 61 a0 18 26 43 5e f1 07 20 79 69 98 a2 f8 f4 65 dd f4 b6 a6 99 83 6b 95 ad fc 08 c1 38 8f 12 2b a0 9a 12 2a 35 02 38 a7 d6 f9 a6 9f 9a f6 82 18 05 ef 87 d2 8e d7 7a c7 8a 5c 92 a9 25 6c 09 eb 65 39 f2 c4 15 ba f4 15 59 5e ed 12 20 52 4a 31 94 c0 8b 92 85 c0 91 e0 9b 7c b7 47 c3 ee 9d 56 90 74 db Data Ascii: Utujt!(GH_1Y6:ikovUTvkV;,tg/0Hgd]DK`id1v0cMf=X,8<k3#h'j\A2a&C^ yiek8+*58z\%le9Y^ RJ1|GVt
2022-10-03 14:16:26 UTC	8949	IN	Data Raw: eb 6e 15 60 bf 06 91 9c 82 59 b1 fb 22 39 a2 51 ce 5e 65 ba ad 7c 20 45 14 9b 67 eb 4e cc 0d c9 99 05 1d 8d f5 17 51 3c e1 1a ad 4c d2 a4 8c 00 f9 ef d7 be 00 4e 26 02 fd 14 5a be ee 1f a9 6e bd 8c 72 32 b0 30 52 5d 87 88 ea d9 75 3c 96 df 02 c2 9a 75 dd 16 e1 54 1d 94 f2 1d 37 9b 7a ce 7c b3 c2 19 a3 d9 18 c2 4a 8d a4 08 a1 c5 97 07 7d 58 68 1a 30 fd d6 cf 81 02 2d be 4c 66 19 fd 36 43 40 a4 a4 89 c0 b0 3d 2f 7c 4f 89 18 ca d7 6a e0 dd 5a 15 b0 f5 2c f2 77 0b 99 cc 9d c8 a1 54 63 57 51 86 ee c2 20 48 b7 eb 34 18 4f 43 0b 02 04 c3 74 a9 f7 41 aa 02 9e 9f f6 ec 31 fb 4f 01 df c2 14 6a 1a dd 95 40 a0 1f 80 22 52 00 94 65 f3 0e 0e 58 39 16 1d e2 47 15 fb b5 1f 87 29 a5 b9 37 e5 a4 ac 26 9c 6d 86 24 6e b1 3e 65 99 54 3b c9 ce a0 9e e1 76 62 b6 e3 a6 13 d6 3c Data Ascii: n`Y"9Q^e| EgNQ<LN&Znr20R]u<uT7z|J}Xh0-Lf6C@=/|OjZ,wTcWQ H4OCtA1Oj@"ReX9G)7&m$n>eT;vb<
2022-10-03 14:16:26 UTC	8965	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	9045	IN	Data Raw: 5e fd 37 15 5c d5 60 48 5b f3 cb 43 6c c6 bc 47 0c a9 e4 55 76 47 4e 2e a7 c8 7b 58 f8 35 f0 9f a6 b8 77 87 31 0d 79 4c ab 16 73 d7 f8 df 4a 36 93 38 5e e0 22 b9 cc 8d 03 7d 59 c0 48 e1 d3 1f 77 1a 7a 3e 31 aa 11 43 9f 15 5f bd bd 28 97 29 96 0b e1 cb 1a f0 6d 2d d4 2e 5e c4 6d 44 72 7e 58 cb 3a 4e 66 e6 32 5d 96 a1 e7 fa 93 e8 df 52 36 ea e0 69 46 a6 d7 f0 fd f9 bd 89 1c 13 28 75 8c 44 6d 82 7a 8f 60 06 47 25 eb e0 c0 68 1d 09 ee f0 e8 eb d8 4e 7f 2b 88 ea 13 02 a6 dd 5f d2 f6 d5 e2 12 ce 9c 03 38 d1 26 6b 4c b4 39 57 4e 52 3a 50 36 f6 af 3d bd 9a 61 70 70 0d af f2 80 80 99 13 34 38 7d aa 73 14 ed 88 29 0e 5c 7c 96 f2 f7 ff e1 d2 c4 be f5 d8 fd cc bd c8 dc 6c 2a 1a 8d f7 5c 4b 9c 6c ac 97 eb 9d ab 3f 1d 39 8a 93 46 6d bb 61 21 2a bb 23 fc 9b 95 6f f4 a3 Data Ascii: ^7\`H[ClGUvGN.{X5w1yLsJ68^"}YHwz>1C_()m-.^mDr~X:Nf2]R6iF(uDmz`G%hN+_8&kL9WNR:P6=app48}s) |I*\Kl?9Fma!*#o
2022-10-03 14:16:26 UTC	9061	IN	Data Raw: b4 97 6e 89 8a 68 92 e9 b0 f0 a9 a1 fc c7 2f bd 9c 9c 4d 67 8d ec 43 5f 48 83 98 5a 90 41 98 28 7a 3a eb 94 2a 82 55 cc 0c f0 de 3a 29 98 5b 62 c5 2f c1 4e f0 9e 53 08 41 61 06 1f 19 a8 7b e0 13 2f 6e eb fe 64 e3 53 7d 4b 83 ef b8 e2 ca 0c 95 18 6e cd 50 cc 33 2c 6c 5d af 60 72 bc b6 10 5d 2b 22 b3 cb 24 64 bd b8 80 f5 ed 2a c5 e3 5e 17 ee 18 14 0b 6d b7 4d 83 a5 e5 f3 62 2a cd 07 8d 6d 34 b3 d6 9c 3b 6f 41 78 24 9f e0 57 dd 86 ec df bc 5d 35 5b ba 8e 35 a6 13 22 7d 2e 16 90 79 a1 b4 8f 48 0d 93 b8 b1 a6 81 cb da b4 4f da 4e 59 f6 37 4c a8 c0 48 9b 5b 83 c7 3d 85 ec 59 67 9b ab 3f 6a 29 59 75 97 88 75 f5 13 5b 7c 13 79 e0 ec 7e 63 43 8c 5d 18 e3 56 0b ca a5 40 71 92 b2 9f b8 2b 8e 8f 15 b4 29 07 60 14 6b fb 4d 8b 27 00 08 99 6e 2b fb 52 99 a5 1d 3c 80 b4 Data Ascii: nh/MgC_HZA(z:*U:)[b/NSAa{/ndS}KnP3,l]`r]+"$d*^mMb*m4;oAx$W]5[5"}.yHONY7LH[=Yg?j)Yuu[|y~c C]V@q+)`kM'n+R<
2022-10-03 14:16:26 UTC	9077	IN	Data Raw: 93 3f 1a 47 8d 3e 4d 21 c7 c1 7b f9 d2 fe fe c5 70 f6 fb 6f e2 43 cf 31 8a a7 ff f0 d8 f3 b2 00 82 60 07 ad 48 51 d5 68 da 74 0d f2 a0 28 eb 27 55 f3 39 8c d6 52 f7 1e 77 9d 8e d3 56 3a e2 0c 1a 2f 3d 27 a3 71 70 10 89 ca 0a 8c f5 67 c7 41 82 77 e4 65 79 13 1e 98 a8 7b 36 69 6a d2 0d 93 46 34 6a 7e ac 4f a7 13 ff 54 f7 f8 29 b8 b7 f2 1a 71 db ac 21 68 2c 1b d6 60 87 f7 20 59 2b 5c a7 8d 8b 38 b5 81 ba 6f 56 0f 1a 28 de cf 4c 78 fe 6c b5 df de d4 84 a3 6e 16 42 29 e2 67 0d a9 f1 5a 76 ee 0a 21 93 6a b9 51 af 13 80 9b 9a 36 4a 3f b3 cd 0c 1a 03 9a e5 47 20 12 f1 cb 5a 34 1d 93 11 03 01 30 bf 11 d4 56 bb 85 59 d5 b3 fe cf db 73 30 c3 f9 ab d7 e5 20 27 c2 dc 22 7a e6 95 48 f0 2c f7 e6 83 49 1e 20 d1 0a 60 87 a0 ca 3b 69 93 52 32 84 84 94 23 d1 4b 2e 2f e0 32 Data Ascii: ?G>M!{poC1`HQht('U9RwV:/='qpgAwey{6ijF4j~OT)q!h,` Y+\8oV(LxlnB)gZv!jQ6J?G Z40VYs0 '"zH,I `;iR2#K./2
2022-10-03 14:16:26 UTC	9093	IN	Data Raw: 9c 96 7e 98 12 88 62 8c f7 d5 52 c1 de 22 f8 de 5f 21 48 b9 fc 11 1e e5 99 f9 bc 90 97 81 48 c4 10 72 e4 dd 20 52 5c 14 e0 c6 b2 a1 16 cd 7c ee 87 8f b3 41 77 bc 8f e9 c8 8e 9b 5d d4 38 71 bb ef a3 f8 e2 3d db 64 2c fe 9d 85 a9 ef b5 1a 2d 2e 4d 50 d8 e6 df 4b 20 8c f2 96 8e de 3a 6e cf 08 fc 24 21 a0 37 19 c6 45 f6 b0 72 87 25 9d 84 55 eb 64 4a 53 50 34 df e8 51 ca ee 1e ab 13 d7 4d 26 8e 2a bd b8 cf ce 56 37 70 fe 9f b9 4f 10 93 79 2c 16 14 d5 8a e0 11 59 87 a7 61 8f ad d0 e7 99 5c 1d 2c 74 0b bb cf 02 84 13 0c 85 5f 37 60 c2 59 20 dc d7 18 c6 a0 bf 2d 42 51 68 2d 1d b2 75 9f 8e 8c c4 a8 0d b0 3a ae f5 c9 7c 54 8b e7 2a e1 3f 5a fe 79 e7 7e 52 c0 d8 59 37 28 24 eb 67 df 57 64 cb fe 8d 83 66 1c b5 78 40 20 44 2b 21 97 09 c4 57 c9 65 07 67 4b fd 61 42 2b Data Ascii: ~bR"_!HHr R|Aw]8q=d,-.MPK :n$!7Er%UdJSP4QM&*V7pOy,Ya\,t_7`Y -BQh-u:\|T*?Zy~RY7($gWdfx@ D +!WegKaB+
2022-10-03 14:16:26 UTC	9109	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	9189	IN	Data Raw: 1c f8 a2 fc ff 1c bb ab 81 11 8d 04 56 e1 a0 97 10 0b 61 54 d0 85 24 ab b7 23 94 18 00 44 f9 f0 9f 3e 59 a6 ab de de ca eb 59 1e 13 f7 9b 91 d1 bd f0 14 93 91 1d fb 1b a8 38 37 c1 c7 c0 2f e3 cb d8 dd 45 79 fb af 4d 60 2d 36 b1 07 6c a6 17 ea 2a 21 91 92 4a e4 52 e3 71 d3 21 12 c4 67 c8 81 64 c9 4c 90 44 63 0d 5d 39 ca 24 dd 83 36 80 51 c6 55 3d 82 d5 14 82 0b 68 89 6a 85 26 89 01 f1 6c a3 9d 10 87 91 5c 38 c4 dc e6 17 ed 38 06 63 d7 ea e4 60 06 e2 1b 7e ed 88 a6 b9 e6 c2 b7 d7 7d 40 4e 6e 0c a4 50 37 20 e3 14 58 60 87 36 6c 9d 00 93 70 36 7c 07 10 01 f9 46 8d ad 3d dc 39 19 8d b6 5d 23 e5 c1 ed ac ce 67 a8 35 aa 5e d5 14 33 2c 5d b9 de 11 67 1e 0d a9 90 cf 8f c7 ae 05 97 e2 15 2e 8c aa 7d 00 ec 4a c9 c0 4a 2f 9d 99 a1 ee e4 21 b2 c1 50 5f 2a e6 e9 54 51 Data Ascii: VaT$#D>YY87/EyM`-6l*!JRq!gdLDc]9$6QU=hj&l\88c`~}@NnP7 X`6lp6|F=9]#g5^3,]g.}JJ/!P_*TQ
2022-10-03 14:16:26 UTC	9205	IN	Data Raw: 4d ae f7 f7 1f db 5f e9 00 4b fe 6e 83 bb 24 66 84 a1 47 e9 d2 e4 84 d2 75 a0 62 9e a0 3c a0 40 ee 49 90 d2 de 75 22 8b 05 07 71 27 d7 46 8c 7f c9 8f cd b8 74 f1 29 06 92 c9 59 9e 4b 07 1b 4e dc 06 0c 9f 87 eb 95 93 4d 5b b9 7b ab 27 fb dc 3f 59 5c fa cd b3 fa 6b f8 1e a9 f6 44 42 ff 67 7a e4 cd 0c 33 8a f6 6f d9 6e 16 df 36 2f 32 cc 5e bb 8d f0 2a b0 92 33 3e ae 03 b6 62 ef c6 59 ad b1 13 7d 7b ea eb 29 a8 47 72 d1 c5 75 58 e2 8b cb 90 99 88 9a ae 6b 62 61 1c 7a 3e 1d 27 1e 32 7d 00 4d b6 f1 d7 d2 2e 6d 85 99 cd dc 52 5e e9 52 c2 57 fd 92 47 c3 29 d8 f2 2b e4 3f 15 79 63 48 e7 6d ab ef 4e 85 62 06 e0 3b 2a 3f 59 3f 08 e7 69 29 da 35 a5 49 29 95 90 f9 8b c3 2b 03 0e b5 0d b5 ce a6 ba 09 b3 27 91 60 b3 e9 6b 35 bf e7 fe 51 cf cf c9 eb 1a 64 1b a0 4b ba d5 Data Ascii: M_Kn$fGub<@lu"q'Ft)YKNM[{'?Y\kDBgz3on6/2^*3>bY}{)GruXkbaz>'2}M.mR^RWG)+?ycHmNb;*?Y?i)5I) +`k5QdK
2022-10-03 14:16:26 UTC	9221	IN	Data Raw: 9e d7 ff ef 86 24 f2 eb 2a f9 82 bb 34 c6 86 08 d7 ea 88 34 fe b9 70 da 29 e7 50 81 c5 47 f0 31 96 33 3a b0 9b 67 1d ea bd 12 c6 22 81 7a 83 11 c7 18 0b b1 03 fb 75 4a df 00 34 67 90 a2 0c 1d b9 0b dd 6d b9 90 fc b5 ab 72 a7 09 c4 95 fb 27 4d b2 8a 9e 02 2a c8 b2 17 a9 a0 e4 a5 59 2d 1b b4 bc 7e 7d 8b 11 7d 6c 87 13 7b 5f 4a e1 d0 c7 53 6c 5a 82 e5 9d d4 f2 11 6f 86 84 7b 3b ef ac ef ef 15 78 d9 21 ec b8 f0 7c d4 c4 da 8d 70 dc 34 04 fb bb 0e 1e 72 31 e4 7a 68 4f 09 c2 50 93 56 50 97 5b 79 af bc 7d 8b bd 01 90 7a ef 9c 0c ed 5a fe d6 d6 d6 15 f5 50 a4 77 d0 db 1c 5a ae 66 1f 32 e4 88 df b2 8a f7 61 ea 21 77 c2 9c c3 0d de 8f 8a 93 f6 a2 a1 ec b8 dc 83 10 25 df ef a1 65 be 3d 4e 35 e9 e8 af 20 a5 8f 6f f1 9f ad b5 6c 1c 5f b8 db 1f 59 65 62 1b 54 80 db 0e Data Ascii: $*44p)PG13:g"zuJ4gmr'M*Y-~}}l{_JSlZo{;x!|p4r1zhOPVP[y}zZPwZf2a!w%e=N5 ol_YebT
2022-10-03 14:16:26 UTC	9237	IN	Data Raw: 9d f1 cd 6a 01 2d 92 99 09 f6 9d cc 13 ee e7 b0 43 31 37 d5 16 ec 59 f4 56 b2 e7 30 e0 e4 5e ca f8 81 90 20 b4 b2 46 1b 72 e0 45 a1 52 34 3e 05 ca 3a be 0a f0 cb 53 d5 03 72 77 a4 c2 4b f5 fd 1b 61 72 37 6a 89 27 65 97 c2 42 c8 42 06 eb aa a1 85 0b dc 46 8f b9 7d 40 ba 52 a3 a7 54 5d 7d dc 50 2f 20 53 3c f4 79 8e 88 5d e7 c4 fe cb 6e b7 58 4d 82 7d 91 ef 49 ab 12 3a e2 c0 65 22 00 cc 1c 18 90 42 38 29 f0 b5 fa a6 4d c0 cb cc eb 89 af 09 d9 a7 30 65 33 ae 40 0a 49 23 c8 6a 31 a3 86 6b 52 81 c2 f9 3d cd 55 c9 2d f0 d1 4e 67 cc 12 3d 4b d1 4a eb 4f 38 41 ca 20 97 d4 88 c7 1b df 07 6e 33 b6 0f e9 63 32 a6 d9 c2 96 db a9 58 32 80 69 37 36 c8 29 2c 29 9b 45 0a 8a 15 49 22 a9 c5 08 8b 01 70 cc f7 66 12 1e aa 5b 07 95 90 86 9a 4c ef 73 e0 ad f1 61 3b a9 1f 1f 02 Data Ascii: j-C17YV0^ FrER4>:SrwKar7j'eBBF}@RT]}P/ S<y]nXM}I:e"B8)M0e3@I#j1kR=U-Ng=KJO8A n3c2X2i76),)EI"pf[Lsa;
2022-10-03 14:16:26 UTC	9253	IN	Data Raw: ac 20 ce 14 45 04 67 80 78 46 5d cc 78 d4 01 3e 27 f9 ba ef 75 10 85 fa 9d d1 14 7d 81 13 3e 14 82 f4 2b 3b 3e c9 bb eb 6a 80 f4 48 bc 9e 75 f3 23 6e 9a e3 07 a4 53 a3 12 cd 2a 43 1f a1 ab cc 4e 8a fc 77 ff 67 e8 34 d1 03 12 d1 e2 7a 50 26 22 b6 10 a5 d9 6f 8c 75 c4 53 72 31 4d 03 6a 23 62 ea d5 bc 56 7a f5 b6 c4 97 dc ac ab 96 b5 91 81 4e 54 e9 b2 02 af 32 0f 58 5a 0c b9 0f 03 9e 23 44 2a 2e f4 fc 02 d2 8c cb 10 77 10 cc 80 ae 98 28 7a 9c 31 4b 27 39 97 29 45 dc b2 dc 93 bd 19 1d ad bb 56 3b 04 ba 8f ff 50 95 ce 82 76 af 2f 0f 90 03 4e cf cb 96 65 0c f7 77 39 75 14 3d 53 70 d5 28 a3 9f c1 f4 72 0e ad 52 c3 e3 ad fc 77 c6 ac b5 1f 2f e2 dc 37 64 8c 93 4e a4 9b c3 61 8d bc ad 2a 36 34 e1 d9 3e 12 8d 3d d8 8f 83 10 a3 6a ab 29 25 de fd 9f f4 1a 3f 6b c0 2a Data Ascii: EgxF]x>'u}>+;>jHu#nS*CNwg4zP&"ouSr1Mj#bVzNT2XZ#D*.w(z1K'9)EV;Pv/New9u=Sp(rRw/7dNa*64>=j)%? k*
2022-10-03 14:16:26 UTC	9269	IN	Data Raw: f5 25 2e 4c 20 af 9c 79 fd 44 6e 7d b5 27 d1 fc 98 7d a7 bd c7 94 69 e1 f3 98 83 ce 6c 89 10 e0 65 59 ab 2b 8e 24 bb 1b 86 bf 24 c8 45 ad 0d 86 05 ae 2e 87 3b 92 99 6c 44 18 27 5e d4 99 78 a1 76 45 68 9c ff 2c 1c 7f 29 b8 7f 3c 6f ad 56 11 2b 41 0b c4 4d c1 8e a8 9c 9b fc f1 a7 e7 54 2f 5d 0d 2d c0 29 34 1a e9 95 cd dc 27 e8 93 df c6 6a 27 b6 39 db 02 4b 9e c6 c2 4d c8 be 4f 95 42 07 26 bc 30 8d 65 ee a7 1d 21 90 60 79 9d 35 70 a6 57 7e 51 67 67 2d bc 8e 9c ce 96 c7 2f e1 af 1c f5 2a 8c 57 41 6c c3 54 aa d6 20 25 f5 f9 90 4c a7 fa 03 df ae 93 1e e4 d4 4f b6 6b 54 67 2d 72 fc 74 ba 1f ad a4 46 32 56 53 ba 44 f6 4c 49 f6 82 13 2b 0d 04 c5 97 28 da b8 ee 25 73 d5 2b 91 77 0b 3a 3e 0a 5c f5 97 52 ab 2a 8e 00 23 67 61 32 4a 2e c8 88 4f b1 e1 ee cf ea 05 29 8d Data Ascii: %.L yDn}'}ileY+$$E.;lD'^xvEh,)<oV+AMT/]-)4'j'9KMOB&0e!`y5pW~Qgg-/*WAlT %LOkTg-rtF2VSDLI+ (%s+w:>\R*#ga2J.O)
2022-10-03 14:16:26 UTC	9285	IN	Data Raw: 4d e3 6d 52 fa 79 52 1a 56 48 bf ff b5 66 31 63 9f 6a 60 29 bf c7 3d e7 42 9b d5 38 60 4a fd 15 e0 67 e2 76 bf ea e7 1e 7c d4 95 35 dc 7e 26 80 0b 55 83 1f d1 db 9e 2f 22 79 5a 6d 08 d4 e3 ec 7f 1f 00 cb 3a ed 10 91 8d e9 d5 ee a7 03 9b f5 7c ee f8 12 d5 59 41 ff 17 8d 41 28 be 7e aa 25 52 6b f0 6c a5 5b 76 2b 3a 5a 0c 65 39 e1 83 a5 8b 6e 78 c1 a5 ea 68 e8 c5 45 b6 46 fd 1d 30 00 4a 8a 00 0f 28 ca d3 9f 52 72 44 4c 6f b1 07 a6 40 ce 78 51 c7 96 f6 2a a0 f6 20 d9 a4 81 b4 b9 d7 60 a8 ae ba 45 30 14 1d 2c 91 af 35 25 90 b6 ee 8d 9a bb 23 ae 51 d7 96 60 15 7f bb bd 3e 6a 66 14 f6 fb 60 a8 86 43 df 7b 1f d1 5f 84 ec c2 fd d2 fd c4 f3 63 6f 44 e1 b6 99 92 40 7a 30 25 65 13 f7 3f 36 8b d1 03 59 61 48 39 65 37 d9 bd 54 6b 76 2d ce c2 73 b2 f1 29 e8 d0 b1 7e ed Data Ascii: MmRyRVHf1cj`)=B8`Jgv|5~&U/"yZm:|YAA(~%Rkl[v+:Ze9nxhEF0J(RrDLo@xQ* `E0,5%#Q`>jf`C{_coD@z0 %e?6YaH9e7Tkv-s)~
2022-10-03 14:16:26 UTC	9301	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 79 21 10 05 00 a0 1b ff c0 00 00 00 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	9333	IN	Data Raw: 88 15 37 ee 84 a9 1d b4 8d 3c b1 b0 aa 51 f4 6e 1b d1 22 56 d3 fa a8 5c 29 25 c3 1a 5a 44 44 50 fb c4 cb b0 fc e1 95 59 38 e2 a6 fb e6 31 25 b4 87 e0 4c 60 31 9d f7 c1 f4 64 e8 dd a8 c5 f1 42 44 9e 6f c0 1c b1 bd 15 69 0a 4b 22 84 5b 6b 84 a4 6d 4b 33 7c 5c d8 39 6c f8 60 96 57 ac db 63 e6 02 7f 6f ab 22 bc 1e c6 fd 7c 4d 3f 2c c4 ba fc 98 da 30 3a 95 7a 0e f6 9f 90 9f b4 b8 fd 1c 17 53 8d b0 63 2e cf e6 35 7d 38 32 cc 3c f5 23 e9 cf 3c 71 12 b1 4a 3c 2c bf fe 96 16 97 f8 b7 2b ec e1 0a e5 66 ed bd e1 7b f2 c7 c9 94 8f 9e 31 88 d9 10 8f 0b 84 33 c3 3c e9 34 4d de 92 42 d5 7a f4 0a 09 83 c5 ba 1d d8 51 19 20 45 7a fd 6a 9c 6e fe b2 d6 5a 79 ad 87 95 e2 75 a1 76 81 1f 13 b9 ff 0a 7b 22 7c 7f 7f ed 29 51 ce f8 c1 08 49 0e 42 c4 09 e4 19 28 85 2e cb 99 a6 4d Data Ascii: 7<Qn"V\)%ZDDPY81%L`1dBDoiK"[kmK3|\9l`Wco"|M?,0:zSc.5}82<#<qJ<,+f{13<4MBzQ EzjnZyuv{"|)QIB(.M
2022-10-03 14:16:26 UTC	9349	IN	Data Raw: 11 9c 60 48 8a 84 26 14 05 a9 65 53 7a 9c 70 a1 f8 a4 c4 81 7a 28 3f 08 bf 24 f5 55 62 31 94 b1 f8 01 1b 36 cf 8f a2 d2 0c 24 ac 16 bd 7d fa f6 f5 26 9d d8 80 aa df ff b3 ae 3d de 5b a6 bb 15 fb 6a 1b 39 b4 eb ea 6c 9d 1c a8 ea c7 2a af 34 f1 ae 70 db 1d 15 5c 07 2b f5 8f d2 45 31 a9 ac cb 93 b2 f5 31 a1 de 6d db 15 41 5b d5 1a f8 5f 90 23 d2 f5 50 2a 35 2b 7b be 1f e8 31 0b f7 c8 50 6d e5 0b 9b d6 20 57 d7 c5 5f 23 38 7c e4 ba c2 e6 01 5a e6 5c 28 57 00 e2 2f 59 69 26 3b eb 55 8d ca b2 87 1c 77 18 2c c5 ce d3 14 ae b5 ff c8 ea 21 4a 7f d8 6c 1d 45 bc b6 49 8e cd a0 55 6e 1f 3e 52 59 c1 ba d7 1f af 9e 9a 53 55 51 6d ed 97 e2 87 da c3 87 e1 47 f6 ab 5c a4 04 f4 37 e0 b5 15 4a 7d 2a f5 ac 79 d0 3d 24 c6 5d 25 e6 23 5b 66 0f 38 08 74 f9 3f 6d c9 7d db a3 de Data Ascii: `H&eSzpz(?$Ub16$}&=[j9l*4p\+E11mA[_#P*5+{1Pm W_#8|Z\(W/Yi&;Uw,!JlEIUn>RYSUQmG\7J}*y=$]%#[f8t?m}
2022-10-03 14:16:26 UTC	9365	IN	Data Raw: 7a 19 03 07 a8 e3 8c 05 a4 0c e2 2d 2c f8 db 97 b1 dd 24 0f 87 d7 a7 83 24 41 fd f5 e9 25 c1 25 66 4f 88 16 24 40 a3 e6 d8 e8 34 e7 b0 e6 42 13 3d 7d 93 4b c3 ba d9 7a 3d fe 7e e5 03 48 03 40 02 ad 08 8b e2 eb 01 d3 e8 c2 eb be e0 d6 28 b2 f4 bf 13 c6 ad dd e1 00 cc 3b f7 eb 12 ca a9 84 72 73 67 82 2d 90 24 2b 87 d9 36 21 94 92 74 fa 73 b3 57 62 ff a3 0c 89 9c c3 ac d9 b2 52 81 8b f6 68 d8 e0 5a 95 7e e1 c8 07 3d 62 85 5d 2e b6 c7 53 fb 01 03 bb 43 c3 7b 4a 30 b8 ae 8f 0e e1 d3 bb c0 43 67 f8 b0 f4 51 df b4 9b ff e9 9a d9 5d 81 13 dd be 38 56 de c8 b0 79 cb 5e a7 10 a4 1f 86 cf fa 3d 54 d1 52 e3 c0 c3 29 e8 d1 f6 ba b9 b8 b5 62 3c 7d 90 4a e7 b0 e0 bf 34 67 78 92 45 4f 3f dc 29 bd f5 5a 2e 9d 97 a5 bd cb d3 f5 81 0e 9f 12 8b d2 5b 9f 98 75 04 f0 22 b8 5a Data Ascii: z-,$$A%%fO$@4B=}Kz=~H@(;rsg-$+6!tsWbRhZ~=b].SC{J0CgQ]8Vy^=TR)b<}J4gxEO?)Z.[u"Z
2022-10-03 14:16:26 UTC	9381	IN	Data Raw: 81 82 86 11 d8 84 9f 28 8a af 4b 9f 5a e7 91 51 a1 32 c1 2f 1f e5 c6 34 42 d6 b0 c7 ed 90 54 2e 88 0c 45 cf 4a e5 e3 52 da 9d 1a 08 9b 18 d9 73 b4 92 08 25 98 87 71 30 1f 8b c3 7a ea 5b 93 60 63 07 d0 eb 73 a3 74 a0 0c c0 88 77 07 cb 6c 8b 8e e4 fd 05 2a 22 b2 cc 20 37 44 4b 28 2a 8f 56 3f c1 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	9477	IN	Data Raw: 5b 71 04 ab b9 56 5d bf 70 47 c8 8f f6 b2 de 3e c6 bf 60 14 06 01 3a 2d b8 10 73 a7 44 71 4a c2 0d 1b 32 e1 6c e8 44 ac 45 cb 66 b1 98 9f db 02 23 f3 39 49 d4 8a 7b 12 46 d4 02 9b 50 70 ae 65 c7 e6 a3 30 77 7c 82 ed 5f 26 49 89 e7 29 bd ef af 5f 1f 72 22 92 99 7d 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	9621	IN	Data Raw: 7d 4f 05 da 40 c9 e4 66 5e 92 6b 29 c3 33 22 c4 78 bf 39 53 d5 d5 23 69 e0 47 03 25 81 3e 14 fc c8 bb 23 fc 3d 77 57 2a 34 4e c1 dd 37 a6 c2 a7 35 24 06 64 1c 0e ea 99 21 8a 6a 5d f9 29 ac df 43 94 d8 39 b5 93 8a dc d1 90 83 8f 93 9e 0c 0d f7 57 66 3c f6 e0 22 c0 0c 2f 10 45 dd 90 58 a0 70 7f 5a 84 38 00 5b 96 9f 1e 19 71 85 83 db de 57 48 5e 4c a8 67 22 a0 0f 1c 3a f1 4d 2f 02 28 78 ae eb 8e 63 33 24 e5 c7 17 f8 63 ee 5d f5 c0 4f cd 48 90 c9 09 b8 36 ff 78 d1 a2 65 07 86 14 61 19 14 50 fa f3 ea a5 fc 5f 09 b2 4d 34 34 17 f3 a8 1a e5 69 4d e1 0b 18 e6 5f d1 b0 e2 f8 a4 fe ac 17 d0 5b cb 38 7c 79 f3 49 6f 15 29 6a 96 e7 a7 ec f5 8a cf 2b bf 70 99 5a 4d 96 8c 8e 04 71 9c 0c ef aa 13 ae ed 8b 3b d6 80 2f 2f cf 08 97 86 8f b8 11 db e4 f3 b6 49 4a b1 bf db 38 Data Ascii: }O@f^k)3"x9S#iG%>#=wW*4N75$d!j])C9Wf<"/EXpZ8[qWH^Lg":M/(xc3$c]OH6xeaP_M44iM_[8|yIo)j+pZM q;//IJ8
2022-10-03 14:16:27 UTC	9637	IN	Data Raw: 99 3b 8b c6 c7 5c 64 3a 58 46 02 d2 6b d0 de b8 dc 6b 62 30 05 d2 44 93 3b 05 d9 84 b9 d3 fc 67 40 d8 c3 a2 16 9a 3c 40 46 0e 9f 47 eb a4 72 75 73 0c 42 ee eb 8d d8 67 e3 44 80 58 98 d0 71 0f 4f df fd 4b e1 86 a9 e2 78 27 7d fa e5 90 cd 6d d1 da 66 82 65 51 ac a6 2c 08 f1 3d 2f 6e e9 d7 e9 39 17 9c a6 21 1e e3 8e a9 b0 5f 1a fd 95 07 0a 7d a2 f6 55 e5 c8 c9 9a 7c 6e 2a 9f 59 87 50 d5 b0 1f 38 0e c0 d1 e1 68 22 a0 d6 7d 65 1a 92 e8 61 f9 62 e9 d9 52 7c 3c 4e d6 ed 8f ab 1c ee 98 73 10 2e 4e 7a 60 56 cd 0b 15 a7 75 06 d6 b4 5b cc a8 ba 3a e8 c5 ad 01 3d 38 b4 b3 ef 45 1a fd 9d 67 51 fc 95 41 33 28 6a 9b 66 f4 02 59 1d 6e be bd 47 4c f6 d5 8d 1c cf f3 d5 a5 16 26 1d 48 79 db 94 0a a9 d3 1e cc 83 70 39 0b 1f 62 66 ca b4 57 d8 4b 4e 12 e7 df 6e e7 e6 65 92 ee Data Ascii: ;\d:XFkkb0D;g@<@FGrusBgDXqOKx'}mfeQ,=/n9!_}U|n*YP8h"}eabR|<Ns.Nz`Vu[:=8EgQA3(jfYnGL&Hyp9 bfWKNne
2022-10-03 14:16:27 UTC	9653	IN	Data Raw: 9a 9b bb ca a4 05 85 d8 5f e4 a4 42 a7 f3 62 90 da 55 9c 8b 98 92 6f 2c 0d 35 3d b6 aa 1b 62 6e 7e c8 07 f6 7f ef 0b ee 51 5c c9 2e 87 33 cf c6 8c 23 7b c4 10 54 00 9f 08 be 1b bf 51 2d 3b 52 62 62 90 71 8e a1 b1 59 39 12 37 95 64 93 93 bc 2b c3 71 6b 69 dc 84 3c 50 8c a2 1e 8f 9f 89 26 c1 53 6d 8f 96 49 3f 2c 76 8a 86 dd 57 ce 83 37 e9 70 a5 03 16 4b 05 3f fa e3 73 7f f7 ff 86 dd 5d 02 15 63 e3 89 12 07 35 ac ab 0e cb df d8 7b 1c 62 11 da 5a e8 95 22 b5 94 4f fd c1 6f 65 5e 5d 5e 4e a4 8f 38 d5 9f d2 bb 1e 63 19 5c 51 eb 12 e8 74 13 bc 22 63 9b f3 70 0c c1 1b b8 f9 0a 7c 12 6e ca 6c b3 93 57 3e a3 64 89 8c b3 e6 94 35 0e 1b 96 43 49 9e 4a e4 a9 65 90 1f f8 98 ac 85 7f b9 03 70 c4 b9 e1 d1 06 45 83 0f 47 f5 b8 f6 d4 f9 fb 64 1b c5 31 b8 b0 17 94 9b 21 9a Data Ascii: _BbUo,5=bn~Q\.3#{TQ-;RbbqY97d+qki<P&SmI?,vW7pK?s]c5{bZ"Ooe^]^N8c\Qt"cp|nlW>d5ClJepEGd1!
2022-10-03 14:16:27 UTC	9669	IN	Data Raw: af 61 f3 f7 e9 30 76 4d 9b ff 0b 2f 89 9d 3f 15 02 db 9a 74 2b 76 f6 a6 e9 f4 16 d1 e3 17 94 98 d1 07 83 b7 d2 c6 61 68 e1 a5 dd 2d 1b a6 37 89 59 44 29 96 bc 89 dd 88 f9 66 61 a1 2f dd 52 dc bf 1e ac 05 60 b6 96 09 72 95 f2 43 ba 41 9b 4c b3 fd 1f c3 75 26 06 b2 fe 0a a0 b5 0a 55 a1 e2 f3 e5 f9 1c df 90 85 8b 0d 49 8f 62 07 9d 63 e2 9c 22 36 77 33 fc d8 33 51 2d 63 9f 2f 35 fb c9 11 98 ba e4 2f 8c 00 ff bf 37 6a 23 df d9 7d 70 0d bb f5 b4 cd 7e ba 97 3e a1 e6 36 5d fb a7 ea 6e 19 fb eb 46 3f e3 7f 15 23 d1 02 f8 6d fd 60 4a 1b f2 a5 6f 8c ff f4 d8 10 d2 d2 9c 41 98 06 77 91 c9 66 ae 6a 44 23 8c 41 06 e4 a7 8b c9 7f c7 01 0c 32 64 1e 0c 67 c8 22 f0 5a a5 68 bf 49 81 88 b0 0d fc 28 1a b9 7a 4d 62 5c 55 d3 66 e6 e1 ab e8 ac 47 56 ef 57 e8 86 1d cf 11 cc 1b Data Ascii: a0vM/?t+vah-7YD)fa/R`rCALu&UIbc"6w33Q-c/5/7j#}p~>6]nF?#m`JoAwfjD#A2dg"ZhI(zMb\UfGVW
2022-10-03 14:16:27 UTC	9685	IN	Data Raw: 42 9a 1f 29 85 a0 be 23 fd 94 2b 4d 55 54 bd 99 77 88 b8 a7 05 c1 c1 70 e9 70 1c 8c a7 81 15 49 a4 a1 95 7e 82 12 0a b2 2d 5e 22 31 c9 5a 44 b7 0e 1c fb c4 3b fb 0f 5e dc fe 6a 0c d2 26 3e a0 68 b2 71 0a 40 e0 a0 2f 25 b2 b6 af 2d 58 47 d3 0f 7a 79 9f 8a 15 f7 14 b5 21 96 c4 7e 3d 13 30 29 a9 09 2d 0f 5d 90 64 28 32 eb 01 d3 1f 9d 7c c1 bf 8c 32 a7 d6 3e ab 9f c0 fc aa 82 0b 1f 5e 05 85 02 79 9e 8f 46 01 eb 94 5b ac 54 39 07 e3 a8 f0 0b 8d ae cb 84 90 24 20 a0 96 83 07 58 7c 2f 1c 36 2c 65 3b 02 e9 77 13 7d b8 e2 35 ac ce fd 5f 7a 49 a8 f8 49 6e d0 40 ba cc bb 2f fc 9b 98 8f 57 02 a0 89 f6 b7 a8 56 95 d4 3e 3a 82 fd c4 ed c5 8a a3 f1 ef 6a 46 45 c2 da ab 4e 23 04 f1 27 d8 41 8b 7f b8 23 ba c7 aa 35 e2 b2 a3 60 56 60 00 68 55 d8 ae 90 a6 4e de 4c 49 3c 68 Data Ascii: B)#+MUTwppI~-^"1ZD;^j&>hq@/%-XGzy!~=0)-]d(2|2>^yF[T9$ X|/6,e;w}5_zIIn@/WV>:jFEN#'A#5`V`hUNLI<h
2022-10-03 14:16:27 UTC	9701	IN	Data Raw: 20 54 5c f1 83 35 62 9d e1 c7 c9 7d 7e 92 fb 8d 01 a4 fe e4 8c ac dc 53 18 2d da fe 7b 84 3e 99 78 07 6a 4a d6 09 a7 ae bc 00 ce 91 8d b5 a6 f2 b0 9d 0f be ae 83 b5 54 4f eb a0 44 f5 e2 6d 3c 2f 66 aa 90 2b 20 c2 a0 2d 00 5a 33 f1 9f dd d0 cd 4b 25 df d5 4e 3e a1 ab 9d eb 74 cc 33 ca bd 53 be 84 ed 85 93 86 8f d4 fc f3 95 d5 75 ec 84 f7 68 8e 9b c1 fd 36 63 7d 37 f1 16 f3 05 ce 3c 62 ba 6b 55 d6 dd db f1 cb 26 86 e4 55 9e 6d f2 b0 55 a9 28 5f de b7 37 38 2b a7 8a c0 35 0d 74 aa a0 7d 01 b7 70 6b 1a 37 23 96 8c e1 41 2b d2 61 42 5a e9 84 cb d1 3c ad a8 54 25 66 5a e0 2f c3 53 29 38 a7 d9 83 1c 2f f2 bf f1 9f a7 f4 cc 4d b8 4b 3a 7e c6 d5 9c b5 bd 0b f3 7a b4 4c f6 73 95 52 21 fe 63 67 f4 24 16 8a 41 4e 6c 33 aa 33 63 b4 60 2c 18 9a e1 73 56 9d 71 a5 ed cf Data Ascii: T\5b}~S-{>xjJTODm</f+ -Z3K%N>t3Suh6c}7<bkU&UmU(_78+5t}pk7#A+aBZ<T%fZ/S)8/MK:~zLsR!cg$AN l33c`,sVq
2022-10-03 14:16:27 UTC	9717	IN	Data Raw: e2 01 3b e2 c6 96 95 35 52 d9 e7 12 73 6d 95 b0 a5 58 17 a8 ab c9 cd e5 b9 81 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	9765	IN	Data Raw: 04 7b c5 56 7c 18 62 54 d2 74 b7 f9 4c 77 78 5f 88 13 b1 e7 23 6c 52 fe a1 21 10 04 0e f2 0c 4f 4a d6 06 96 09 0f 3e 0e 13 ef b8 78 18 fd ea 1a c5 7f 62 e2 80 a9 14 40 f0 2b 20 32 c6 2c e9 89 06 2a 96 a9 25 4f 8b c1 28 1f 04 30 92 7f 60 32 0d 07 5a a9 f5 e6 16 91 fe 17 a5 43 d5 85 56 1b 00 d6 26 53 9c 3d f9 bc bd 07 cc 88 1f 23 e3 3c 29 e8 05 b1 4f 70 83 9e 66 4a 51 00 1d f3 00 9f 0b 83 e6 9b 5d e2 aa d2 59 7d 58 18 12 9b e2 16 b3 7c a9 2c 44 c0 c6 a6 78 14 db b5 4f f7 21 e8 a1 f2 29 4c da f0 17 cd b1 85 b9 65 8f 75 6e 78 77 ba 28 16 1c 17 4b b2 ab 23 ae 3c d0 d3 02 ac ec 4a 1a 35 ca 4e 49 6d 34 82 ef ce d4 28 5d 27 1b c6 4b 4b 8b 78 54 ca 6c 7d 19 40 fe 1d 43 c2 93 af 10 80 3b d9 e9 9d 80 36 6d c0 37 ac 7a e5 df 4f 79 5d 0e 95 52 56 6f 99 0f 81 26 d4 bf Data Ascii: {V|bTtLwx_#IR!OJ>xb@+ 2,*%O(0`2ZCV&S=#<)OpfJQ]Y}X|,DxO!)Leunxw(K#<J5NIm4(]'KKxTl}@C;6m7z Oy]RVo&
2022-10-03 14:16:27 UTC	9781	IN	Data Raw: 82 f3 71 aa 68 da 4a 79 c0 2a fe 0c 79 f8 5e b1 82 18 51 93 da 19 b7 80 e5 e8 88 f0 f3 0b 6b 4a 3e d0 92 2c df 8d a2 28 b0 cd 2a 7c b1 4c 4c d3 ab 61 6c 34 8d 30 c5 dd e7 85 43 55 8e 8b 7c 53 b2 fc d0 26 3f 2f ad 11 fe c0 be 80 53 cb 4c 37 81 6f 28 d2 79 c5 cf 42 36 d0 91 af 37 c2 1a 4f a4 aa 63 16 62 0c 98 97 0d 0e 7b b0 79 25 3b 7e 2c 4d f2 32 27 be 81 fe 5d 52 1c 43 fe c6 93 9d 8a 53 ba a7 46 58 38 85 c7 e7 e1 85 63 5d d8 a1 aa c5 25 90 2e 3a 2d 2e 07 86 93 c8 17 fa a4 fe ba a7 07 be 11 9f 39 26 37 f5 f3 1d 7c 22 78 ff f4 28 0b 95 25 38 0e b2 64 0b db 19 49 8d db fb c0 c2 3f c6 af 98 9d cd 11 6e 41 65 ce 03 59 0e fc 69 ee 10 88 e6 bf fd ef f8 23 c8 0a 82 c9 56 54 73 6c 8e c5 43 98 f4 e1 19 8f b5 c1 ec d5 82 ef 51 70 fc 2c 51 ab 19 e4 b4 5e 84 c3 a9 2f Data Ascii: qhJy*y^QkJ>,(*|LLal40CU|S&?/SL7o(yB67Ocb{y%;~,M2']RCSFX8c]%.:-.9&7|"x(%8dI?nAeYi#VTslCQp,Q^/
2022-10-03 14:16:27 UTC	9797	IN	Data Raw: 9a 89 1c 04 77 65 5b ba d7 3d 0f 8c e3 30 27 eb a2 68 c5 78 e7 34 a6 3b 8f e2 b1 ce b0 c1 58 02 2a 46 7d 5e d8 de 6e 85 e1 9d 3b 77 4b d5 e3 9e 0a c5 15 dd 92 45 3c cd 58 13 45 f3 55 31 4d a1 f9 50 cd 07 06 c6 be 14 c2 e4 2e c3 f5 ad c5 dc da 0b 85 e3 88 53 d2 45 a5 2c 23 18 bb 85 f1 b2 8f 12 b2 af 51 b7 15 02 f0 56 65 32 24 6a f6 3b 70 94 c8 d5 0d 03 1c 7d 79 b9 37 cb 1a de c7 23 01 d9 dc 80 9a 62 29 c5 6a 15 5a c7 d1 d6 fe 9c 95 e0 5f ab b0 b5 8f d4 27 8e 9c f6 90 7d 62 a3 55 23 31 46 22 f6 d0 7d 95 5b ca 0b 3c 16 c1 2e e5 76 1f 07 6f 50 f4 8e 33 83 3f ed 46 c6 51 f9 d6 16 af 71 4d ad 8a 83 8b aa 2c c2 65 f8 da be 41 52 05 fa ef ff ad e5 82 94 5c 20 72 6c 81 ee f9 03 a8 7d e4 b3 47 33 bd e2 9b 9e b7 b2 5b 96 ad d5 4f d8 75 79 e5 be 2d 77 ea 2a e8 f9 e7 Data Ascii: we[=0'hx4;X*F}^n;wKE<XEU1MP.SE,#QVe2$j;p}y7#b)jZ_'}bU#1F"}[<.voP3?FQqM,eAR\ rl}G3[Ouy-w*
2022-10-03 14:16:27 UTC	9813	IN	Data Raw: 2f 63 74 65 40 65 e5 52 29 e4 c4 de 37 4f 7d b1 d6 3a 0c 16 a1 fd 6d 4e d3 b9 5a 92 51 2a 0a 9a 00 19 b2 16 94 cb eb cc 35 7a 2e 9f 5e 3f 1b 26 ec 48 37 20 41 a7 fa 6c a1 f8 49 ca e1 bf 02 c0 2e f8 d4 fa a5 d0 65 f0 27 c7 4d d3 ac c0 6c ab c9 57 6b 0d ee 7a cc 1a cc ab 04 94 40 a4 a5 53 18 85 45 4b ee 73 08 45 e6 d8 db 89 0c 70 a6 99 33 dc 6c ea 7b 05 41 2f 7f 1a b6 38 13 5f 07 3d 91 e9 6f 0b e8 68 22 69 5c 02 25 e0 ae 9d ab 37 df e4 ef 06 bb 3a 2c df e8 ba 1c 04 d5 07 3f 94 08 cb cd 48 d0 22 36 b2 19 cf f2 28 e9 87 e3 16 45 f5 6f 31 36 67 a7 b8 42 fe d4 1d 69 bb c6 e2 64 4a 4d 22 68 cd 79 81 44 4f a3 62 53 9b 30 04 8f cd ba 1d f5 d1 7b 1c 45 50 36 ac 3c e1 fa 71 72 c9 2b 92 41 43 49 af fc d6 ab 85 b1 cb 78 f9 35 6c 8e c5 b8 e8 8f d0 ed bd e2 64 58 74 cd Data Ascii: /cte@eR)7O}:mNZQ*5z.^?&H7 AIl.e'MlWkz@SEKsEp3l{A/8_=oh"i\%7:,?H"6(Eo16gBidJM"hyDObS0{EP6 <qr+ACIx5ldXt
2022-10-03 14:16:27 UTC	9829	IN	Data Raw: cb 62 88 79 12 88 f3 77 95 33 1c f7 6d 68 fe be 3f 3b 63 61 0a 00 35 83 2a 12 15 a8 d6 cb 03 a1 6f 8d 6d c4 01 3e 70 c9 29 e9 72 51 af 89 7e 9b 6f 53 3c 6c 4c 81 15 60 17 51 19 f0 40 ad 40 99 e6 b5 ce 20 b5 61 0b 3b 41 dc 60 6b 77 29 c2 cc ad 1e 53 74 05 bf 41 5d 28 9a bf 0a 17 0c ee 3a 08 a7 3f 55 9b 29 ac 5c 87 36 3e 6c df 3f b7 6c db c8 07 a8 7f a0 d3 2f 3b e7 b4 cd 8c 0d dc 2e 87 85 61 e1 ea 2b 1d 0f 63 8e 3e 44 e8 7f 31 6e 80 a3 09 45 90 80 f7 3f 16 62 c8 53 f8 d6 eb 8a 0b 11 48 f3 51 1e ef 14 c8 3d b0 4b 48 f7 fd 3a d9 89 b9 79 c0 d5 49 f8 d9 d5 34 d7 94 c6 01 19 f7 1f 7c 3f 65 b0 55 46 66 3a 06 8a 49 e5 a2 ff 76 9e 27 a5 23 10 be 6c 19 e1 98 f8 3d 1e e0 e8 e9 95 29 45 ac 27 c8 e8 b2 8f 7d 4a 6b e5 c7 56 b0 db c4 cc 84 29 84 64 64 73 18 d2 ac 6f 08 Data Ascii: byw3mh?;ca5*om>p)rQ~oS<lL`Q@@ a;A`kw)StA](:?U)\6>l?l/;.a+c>D1nE?bSHQ=KH:yI4|?eUFf:Iv'#l=)E'}JkV)ddso
2022-10-03 14:16:27 UTC	9845	IN	Data Raw: bc 3b 23 8d d1 b1 c1 0e 46 aa 5f 91 25 e8 48 d1 16 3d cd 5e 9a bf 03 95 63 a9 f9 e0 e4 e1 d4 0e 1c 6b b8 e5 c8 f4 25 65 f3 ea 15 6b 23 df 54 59 5b 78 5a 95 c7 ed a8 20 f2 12 3c 90 25 07 63 6a 4f b4 a2 a0 43 ee 7e 67 ce 6e df cc f7 72 7d 64 66 0e d3 f7 3c 7e 1b 47 f6 d9 d4 c9 d1 89 79 ab da ee 08 c4 74 9d 5b f6 35 ce 15 42 9f ad 2c fb 9f d9 cb 54 6f 90 24 4b be 81 4f 2f 54 12 2e a5 66 d4 cc bb cb 0b 5f 99 09 78 b7 24 b4 f8 55 7c 11 4b 11 e2 cb 56 c3 8b 1e f7 78 d0 02 3e 50 18 88 5a 8c 54 07 6b cd 0b 8d e8 b8 a7 9d eb a3 2a cd 6b 90 19 eb 2c 35 83 c0 8b ec 34 39 e1 dd 38 1a 59 96 65 19 8c 04 92 d7 c9 de 64 a8 ac fd 94 25 b0 61 06 7d 08 31 af bc 73 33 89 be ff c4 fd 81 2a f4 11 d9 bd 8a e6 01 15 e7 81 68 4c 54 e1 dd 07 88 e9 94 6a 65 a3 3d c5 4c 9d 36 3c 79 Data Ascii: ;#F_%H=^ck%ek#TY[xZ <%cjOC~gnr}df<~Gyt[5B,To$KO/T.f_x$U|KVx>PZTk*k,5498Yed%a}1s3*hLTje=L6<y
2022-10-03 14:16:27 UTC	9861	IN	Data Raw: 86 d7 b1 1e b7 74 65 7b 47 2e 04 9f 9c c2 dd 0f 79 a6 16 35 28 d8 a0 63 a6 69 79 79 1a 97 eb dc a2 7c 92 5e 49 79 7d 1d 2f 7c db ee 9e 75 33 4a 30 fa 2b c2 5e e8 74 c8 1f c7 73 3b 7c fc 51 80 77 bb f1 bf 15 47 b6 74 99 0d 68 2b 86 34 db 7d c3 85 d3 cf 2d 6a f1 9a ff d2 3f c4 78 70 18 a8 0c af 67 65 47 d4 bf 35 11 89 54 3b c0 c0 39 ac 8a ae 33 07 31 ff 80 70 f7 76 12 ca 02 72 27 24 ef 40 08 bf fc 69 19 09 a6 d7 fd 2c e4 3b 67 7b 7a ea c8 cc 8c 3a a5 39 5f b1 b5 73 7d 3b 60 1f 51 2e 39 5e d9 fb 16 37 d5 5f 19 23 5f 6c 2f 42 bf 2b 30 23 c1 67 85 10 a9 27 84 f4 3d a8 a4 bc 92 44 ae cc ea 5d 7b d2 02 08 a3 14 9f 34 ac fc 0b 7e cb ce d2 58 d4 8d 53 52 69 37 12 79 7f d6 26 43 79 fe 9b 04 80 a6 18 33 cf 94 cb b5 2b 71 95 74 21 a7 3c 4c 1b 8b eb 00 f4 44 fd ae f8 Data Ascii: te{G.y5(ciyy|^Iy}/|u3J0+^ts;|QwGth+4}-j?xpgeG5T;931pvr'$@i,;g{z:9_s};`Q.9^7_#_l/B+0#g'=D]{4~XSRi7y &Cy3+qt!<LD
2022-10-03 14:16:27 UTC	9877	IN	Data Raw: f1 df b2 e5 56 0b 54 73 20 8c 33 e4 81 ba 11 af 21 9a 83 d9 6d 2e 1a 50 b4 49 b0 c8 00 9e e4 da a2 ad 9b 9b 2d c2 d8 a4 35 3a 0a e8 41 c4 e3 36 49 35 c0 6e 25 fd a9 ef 85 9b e8 18 e0 5d 2a 2d 97 f0 16 ae c6 87 15 58 08 9c 5a 11 7c bc e9 6e eb f0 16 de 83 54 bd f2 fb cc 17 91 63 bf e5 9a fe e4 d8 19 c7 ca a4 2e 18 4f 09 46 e5 5e 8b f8 fc 2e 76 87 01 a1 21 eb c3 c2 0d 20 ac 58 b0 79 db 93 62 b5 31 0e 3b 82 ac c7 17 5d df ee 1a 7b 76 3c d4 4b bc 7d b4 45 21 04 b4 98 b1 c3 5c 78 c3 e5 40 00 ce 79 94 de 35 23 11 3e 70 9c d2 8f e3 1d d2 55 2b a3 a4 4b 27 74 42 c6 3c 52 58 75 fb 8e 5c 06 66 23 29 ee b7 86 f3 86 04 55 99 a5 e8 06 6c 02 af e4 45 37 23 57 59 2e 48 b9 ca 99 64 86 8d 35 2f 99 5b 35 a5 c6 b8 96 8c 0c 0a 8d 4a 5c c8 44 f2 65 55 e8 65 5a 83 c8 53 b3 fc Data Ascii: VTs 3!m.PI-5:A6I5n%]*-XZ|nTc.OF^.v! Xyb1;]{v<K}E!\x@y5#>pU+K'tB<RXu\f#)UlE7#WY.Hd5/[5J\DeUeZS
2022-10-03 14:16:27 UTC	9893	IN	Data Raw: 7d a5 e1 dd 38 55 3c f9 0c 12 40 58 64 d3 52 1c 95 b1 b1 90 24 76 af af 1f 66 5c eb 1c 0c 9c a9 2b ff 28 f5 d4 81 43 b0 04 0c 29 e4 1e cb 17 fc f0 85 fd 82 78 06 12 7e 80 37 f9 14 45 bb 20 17 8c 81 3d bf e4 72 44 06 c8 00 cf 15 b0 fe 3e a6 11 e4 79 48 fe ea 0c 7b eb 2c db 84 d1 d5 60 cc 3a 5d 60 b9 b1 36 5c 9f 26 51 75 17 a0 71 a1 4a 73 f3 3e f9 32 6c de db 73 01 c0 1c 4f 34 0d 82 50 29 5b 14 9a c6 3e f0 2b 4f f2 72 61 e5 47 19 99 1a f0 f4 cb 32 ae 1c 72 7b 8a 24 ff bf 0e ec f6 22 6a eb 2e dd 9b 4a d6 74 9c ab d6 73 a0 5e be 7c f0 98 37 84 12 43 d0 96 f8 84 ff 36 4e 49 a2 9f fe 12 01 1a 2b af eb bd 29 be bf 2b ed cc fe 17 d9 04 98 49 b2 89 c3 81 9d af fa 49 39 11 ca d7 96 83 1a 93 68 36 bb bb 5a 35 e3 32 77 2c 76 b7 50 ac 4c 16 5a c9 42 e6 7c 24 91 2b 58 Data Ascii: }8U<@XdR$vf\+(C)x~7E =rD>yH{,`:]`6\&QuqJs>2lsO4P)[>+OraG2r{$"j.Jts^|7C6NI+)+II9h6Z52w,vPLZB|$+X

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	9909	IN	Data Raw: 09 af ff 96 ff a0 79 41 77 3d 89 fe 04 22 75 ae b2 ff 5d 14 b0 f8 ea 53 6e c9 be 9c bf 45 a5 ca d9 ca 01 d4 22 d8 92 e3 c4 6f ab 0a 48 1f ed b6 3a d6 67 8b 32 b5 36 92 19 af 44 eb e1 95 46 90 55 3a 62 4e ec 3c 94 07 7d 5b 60 51 68 45 a0 8a 49 1a 6e bc 57 e6 30 b0 61 34 7c d3 9a c3 ff f8 1d 03 13 d7 94 84 29 49 f5 8b 03 9a 57 76 4b 30 00 b7 0c 12 80 e0 52 1d 11 05 2f 87 50 27 01 2f 16 2d 23 6c 7f 57 af 04 08 cc 3f e6 fc bd a6 e3 ca 5c 14 7b f8 63 d9 4f 8c f3 9a 6a 16 ac c1 72 45 36 7e 27 00 3f 0e fb ae ac bd 89 0c 76 f0 f3 37 93 f1 b8 08 d7 81 ed ba 99 85 a1 ca 37 ec c1 23 87 85 10 5d 6d e0 60 30 0a c1 38 b6 0a a9 61 fa 53 3d 79 18 4c 84 71 d7 5c c9 e4 4f f2 97 cd 33 9f b5 69 24 45 36 96 6e 9a dc a0 a7 24 ac 38 29 b3 b8 9b d8 af 6c 5b 55 12 e8 ea 4d 43 09 Data Ascii: yAw="u]SnE"oH:g26DFU:bN<}[`QhEInW0a4|)IWvK0R/P'/-#lW?\{cOjrE6~'?v77#]m`08aS=yLq\O3i$E6n$ 8)l[UMC
2022-10-03 14:16:27 UTC	9925	IN	Data Raw: f0 5e 49 03 c6 de be 70 18 52 ba 44 b7 54 09 e8 c3 93 f3 69 ed c2 b2 2d e1 2a ca a8 6c 39 16 77 5c b6 78 49 96 48 7c e4 b6 0c 1b 32 41 b7 f3 e2 4c 57 cc 48 c3 98 c0 42 65 6a c8 1a aa e5 aa 9f 7e e5 15 60 37 fc 6c f4 d0 fd de 96 20 bf c4 eb b7 fd 71 ab 2f 81 23 2d cd 84 56 e3 71 df 78 78 e0 9a db bd 0b 7a 99 89 eb 7d b2 9c ec f7 f3 2f 8e d1 15 91 b4 6e db 10 08 f2 6a 66 68 9a e2 15 87 b5 fe c1 04 42 9f 07 5a 87 5f bb 16 05 a2 fd a6 8e 66 8d ce f1 90 0c 13 4a 71 4f 7e 95 5c 9c 5a a4 86 95 be b7 14 80 e0 37 df 23 b3 0c 6f aa f6 96 a1 01 a0 6e 7c 99 fe 02 54 ae fe dd 43 7d f3 c0 10 62 bc 38 91 61 3f d9 b7 aa 31 22 18 de 8d af 9a 42 83 e1 a7 51 31 6b 96 c6 ab ef 1e bc 89 f7 6e ea 1f 7e 8c eb c0 08 af 50 58 f7 d0 60 82 ac 92 20 06 15 2d a6 d1 1f 27 ce fb ec 1e Data Ascii: ^lpRDTi-*l9w\xIH|2ALWHBej~`7l q/#-Vqxxz}/njfhBZ_fJqO~\Z7#on|TC}b8a?1"BQ1kn~PX` -'
2022-10-03 14:16:27 UTC	9941	IN	Data Raw: 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	10053	IN	Data Raw: 6a cb 1c 1b 9f 81 4c c7 49 0b 37 1b 5a b7 2c 6e 88 e2 9a 2c 7d c2 65 37 23 0f 68 5d 1a d9 e0 17 9a b3 c7 ef 00 5c 57 8e 5d de 46 8b 94 8d 57 1d d5 01 25 06 cf 04 d0 ff 18 e7 27 c7 39 1e 9b 89 4f 9c 2a b8 f4 d9 cf e2 b2 b0 00 4b 67 68 ec 93 0b e5 1c 1d f1 89 c8 2e 2e d9 b1 76 be c5 d3 fd 46 38 bc 9c 8b a9 2f e5 fa 83 c4 5e 80 3e 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	10197	IN	Data Raw: b4 43 ac f5 45 6c eb 5a 41 64 c8 95 9c 78 0f 41 2f df 11 ed 04 77 b8 0d bb 8f 3b dd d5 97 71 27 a6 42 2a 74 79 2b b8 79 50 3f 24 cb 51 42 b9 73 25 ce 99 49 56 ee 40 d9 52 dc a6 94 24 c9 e7 52 7a ce 10 1e 34 ad 15 24 27 50 fc c7 5f 05 0e 60 4d 07 c2 d7 65 74 b8 50 8a 6f fa cd 1f dd 4d 57 44 03 f5 8e 1e ad ae 46 ea 9d 37 50 40 27 3e 24 0c 51 84 f9 c3 05 ff 93 4d 75 da d4 2b 79 68 91 39 fb 7e 17 86 4e 5c 88 39 e9 ff 5f 74 1c a6 29 3e 09 16 3b 92 73 aa 87 f1 39 34 1d e8 6f 96 d7 ce 43 9b 81 6a cf 6a f6 c7 9d ba ad 85 27 19 2e 7f 6a e0 55 b6 f7 d6 f2 92 02 58 b3 df d7 7c a7 78 74 6e 2e a9 64 e8 04 1a f1 84 3c 92 db dd 6d 21 62 78 57 b1 26 16 23 7d 74 32 21 17 b7 54 43 5c a1 49 b0 90 c0 6b 6a 18 7d fd 53 1a c3 8d 4f 7c 06 75 60 f9 dc b4 b5 8b a5 a4 eb 06 fb c7 Data Ascii: CEIZAdxA/w;q'B*ty+yP?$QBs%IV@R$Rz4$'P_`MetPoMWDF7P@'>$QMu+yh9~N\9_t)>;s94oCjj'.jUX|xtn.d <m!bxW&#}t2!TC\lkj}SO|u`
2022-10-03 14:16:27 UTC	10213	IN	Data Raw: 9f 25 10 cc 08 92 41 d3 a0 47 15 0a fb 83 16 ca 23 53 12 9e 62 f9 d2 73 54 97 fe 71 40 dd 9d f6 3e 0b 83 0e b6 6d f7 fd 5b a2 7b d4 b9 51 2c 9b c8 9f 75 2b 88 05 d8 77 8d 50 e9 67 3a 73 a2 85 ef 4e ff f3 9d cd 67 3f 5c 74 71 52 2b 20 9a 18 2b 48 16 cf b3 1b 2e 16 79 80 26 24 68 9f 25 e5 aa 3d fe ee e2 2c 8a 1e 31 ef bf 0e 0c bb cd 5a bf f1 c9 64 61 55 b5 88 7b a3 19 8c 4b 60 c7 0b bc 41 e4 cd 5c 45 0a 65 0d c3 f2 69 d9 72 85 c6 32 a9 2e 3b c6 f3 8f e2 86 3c 1b 94 f0 f3 6d d2 17 8b ab ae c0 3c e5 44 1c eb 6b 48 51 c4 52 ca 32 68 65 55 c1 7b a3 c2 f2 f1 21 10 05 00 a0 1b ff c0 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:27 UTC	10357	IN	Data Raw: 25 3f 11 97 99 7d 97 d0 b2 ef 38 e5 87 fd b5 2d 9c 9b e6 94 d8 f9 65 16 72 a6 bc 59 41 c5 ec fc 50 83 6c 87 97 50 e9 25 fa 59 c9 47 0e e7 ac 55 db da bf db e9 4d 90 bd 11 e5 f0 0b cf 74 11 c4 69 89 28 75 84 d8 23 9f 96 a3 e3 59 3c a6 17 06 67 6f 1b fa 3e c8 4a 0c 81 9d 7a 3b 92 37 d5 41 7b 58 81 1e 03 42 8f fe 7c e4 d1 e3 76 e2 37 40 83 a2 c2 00 cd df a7 93 86 57 8a 1e 2b bc 88 c6 8f 21 0d d7 d5 f8 22 3f b0 83 35 12 6a 6f c9 e1 5a ea 68 53 d0 fd b2 7a c0 00 07 26 95 16 66 56 0f 3f 44 8b 2d 96 96 ad 40 b2 72 fb d7 80 0e 2b ac a0 de 77 03 96 2c e9 c6 13 12 aa 55 72 fc d0 cc cc 21 a3 03 69 04 78 47 bb 43 70 79 60 52 95 27 9d 5b f5 a9 3c 0f 56 45 e8 ac 1c 72 a9 c4 a2 c0 26 69 79 3f 4f e0 b2 2d 17 cb 20 47 7f 3d bf 66 87 80 18 bb b3 e2 16 0d 49 9f b2 de 65 ee Data Ascii: %?}8-erYAPIP%YGUMti(u#Y<go>Jz;7A{XB|v7@W+!"?5joZhSz&fV?D-@r+w,Ur!ixGCpy`R'[<VEr&iy?O- G=fIe
2022-10-03 14:16:27 UTC	10373	IN	Data Raw: 45 43 8b 21 7d 63 37 14 64 56 a6 3b f4 55 2d 66 f9 58 96 7a a6 77 5d 00 30 4d b6 ac 4a fa 19 22 74 18 a4 2a f1 92 ed 32 45 96 5e 00 02 c9 b4 3b a2 0b 0e 47 01 96 7c dc 97 78 92 a7 b7 11 76 7e de dd df e3 f3 44 0f 0f cf c3 8f 15 2c ef 81 68 29 81 97 f0 03 d6 91 22 16 01 f4 3f 35 de f2 49 bd 47 ac cb 0d 16 91 84 7a ca 4f 75 4d 25 5d 93 6e e5 dc cf ee 49 11 1c 90 6c 8f 9d a1 01 87 39 f2 e5 99 9f 5b fa d6 73 21 b7 81 87 63 16 4b 9c c3 03 ef 0d 67 10 f3 46 4f 37 ba 05 69 7c e7 c4 2d f7 ba a1 85 ab c6 76 c3 17 c1 ec c2 a6 8b 35 35 ae 2f eb 2a 71 ae 8e 8a ce 9e 20 4d c8 92 ed d1 e2 0a 9d b5 e9 44 9b 91 98 13 33 c1 44 d7 66 12 7c be ac 9e 7c c2 4a 34 e1 44 74 4b 5a de a9 5c 8f 25 26 1b a9 30 0d 24 e9 b3 b4 ad ec 06 58 6d c5 57 65 e4 be ac 86 bb 0d 11 1c 3d b4 df Data Ascii: EC!}c7dV;U-fXzw]0MJ"t*2E^;G|xv~D,h)"?5IGzOuM%]nII9[s!cKgFO7i|-v55/*q MD3Df||J4DtKZ\%&0$XmWe=
2022-10-03 14:16:27 UTC	10389	IN	Data Raw: f9 c9 be b5 cc a3 e6 91 60 02 e0 3e ca ef d1 b1 89 e9 d4 4d 51 ca b3 84 bc 37 9d 43 c4 86 17 35 61 39 b1 89 d5 e7 a1 de fc f3 99 61 fa fa ef a9 3e 8e 4e 56 03 89 cf 99 e4 0c f0 68 88 da 77 c9 03 e5 b6 41 29 9f 79 3a ac e5 a4 dc 4c 7c f2 95 eb f2 c2 ca 22 34 48 6c 24 d2 03 0b b9 f6 75 9a 11 51 ce 14 f4 4c 7a 3d 6a 3d eb 99 8e 79 eb 6d 3c 33 1f 1a 0d 35 84 fb e1 49 e6 46 90 3e 4f 8d 8f 72 fc 56 c6 e3 98 c7 6f 13 f2 6f f5 e9 35 06 c5 34 28 1f 10 15 1d fe 15 ff 17 72 69 61 76 b5 34 98 de df c6 19 15 7f 63 9a f5 31 da 60 1d 16 23 72 24 fb ae bb 5c 42 c8 18 3c 96 37 29 14 93 73 dd 4d 14 ab 79 81 82 ad 0f 72 51 ae 40 d7 4e de 38 c0 de 58 5a ee 71 6e b4 8e c8 81 a2 78 cd cc 08 ee 4a aa bb 2c c3 53 df 68 87 83 2b 9f b8 74 03 8d f3 ef 4c c8 37 b9 a6 f1 35 50 ea 24 Data Ascii: `>MQ7C5a9a>NVhwA)y:L|"4Hl$uQLz=j=ym<35IF>OrVoo54(riav4c1`#r$\B<7)sMyrQ@N8XZqnxJ,Sh+tL75P$
2022-10-03 14:16:28 UTC	10405	IN	Data Raw: 17 fa f2 eb 01 75 06 52 3c 9c 1e 17 47 d8 45 91 44 0b 2e 1f 61 c6 d7 16 fd a0 d1 99 f4 ca 1b 32 b4 a8 3a 2a 17 3f cc fd a2 f6 75 20 e0 2c 20 1d 0f fb 84 41 0f 02 2d ae f1 0d 18 fa 91 0c 81 21 69 a5 a8 40 d9 f1 09 df 84 04 81 b3 b6 4e fb 52 3e 55 e4 f8 ab 99 21 b8 e6 e5 02 9c e1 0c 44 05 c1 6f 5a d4 2b e3 c9 e9 b8 ff a6 1f 85 50 b2 c0 75 12 82 f8 45 6d 69 d9 79 1f 51 f4 99 1c 90 0d fd d2 12 bb b0 07 be 61 e1 71 ea 7e 1f b3 f0 80 46 f7 bc 44 c2 ca d8 23 2b ef c9 9b 73 18 ca 78 87 e3 fe c5 66 d3 8c ca 0e 16 5c 8f 51 9d f0 3d 59 d9 1e 5b c4 c7 75 b3 67 27 50 0c 02 de 60 4b 50 c3 59 5f a7 6b 80 02 97 13 5e 3b 82 fa 3f 91 b8 57 d8 73 b9 ad 3b df 4b bf 93 e2 c3 44 20 95 2e 10 eb a8 0e 98 1a 70 66 27 a0 35 65 c8 31 95 a9 18 c1 3e 2c 41 4a 55 65 4e ed 2a 92 fd a9 Data Ascii: uR<GED.a2:*?u , A-!i@NR>U!DoZ+PuEmiyQaq~FD#+sxf\Q=Y[ug'P`KPY_k^;?Ws;KD .pf'5e1>,AJUeN*
2022-10-03 14:16:28 UTC	10421	IN	Data Raw: ec 0f cb 51 a8 57 12 5f b1 50 d1 99 51 3e 30 a3 b7 a8 28 ed 50 c3 c8 30 d5 74 23 26 93 0d f7 39 0f 92 bd 34 d1 14 28 11 fc 32 7c 19 5a 53 6c 5e d7 32 4d 99 70 81 68 93 44 65 78 dc 62 16 55 27 98 b8 9f 4f 54 eb 50 ae 11 4b 2d 89 73 20 67 c2 a9 f6 97 74 ff 55 f0 02 c6 1d 4a f3 6e d0 c4 f5 7e 42 48 45 e2 02 01 84 b2 35 c6 3f 71 42 1e 83 88 40 1c a8 67 b7 f0 15 4b 78 ec 1d 54 7a 62 9d a2 25 68 0a b5 de db b5 03 a8 60 30 73 ac c2 e5 ac 8c 9b 96 7f 6e 6f b1 20 f8 7a 3f 47 15 5f ea 93 0d 0c 06 38 b7 ab 2f 2a 1d cb c8 da 94 e6 e3 63 b9 39 69 a7 1d e5 fe de 0f e8 0a b7 46 a3 7f 42 06 21 fb ca 87 ae 80 d6 27 9f af 47 7f a2 44 f4 0d dd e2 fb a0 3c 79 38 27 4e bd 17 c1 2c 78 1e 67 45 21 b9 bb e4 31 0a c4 7f 9e 12 14 7e 87 26 32 83 06 bf 5b 4f e5 0b e3 af 83 d8 39 73 Data Ascii: QW_PQ>0(P0t#&94(2|ZSl^2MphDexbU'OTPK-s gtUJn~BHE5?qB@gKxTzb%h`0sno z?G_8/*c9iFB!'GD<y8'N ,xgE!1~&2[O9s
2022-10-03 14:16:28 UTC	10437	IN	Data Raw: c6 ee 7b 3e 3f 14 70 02 f0 d1 92 69 0e 6d 0d 21 13 7a f8 b8 4b 83 bc 62 57 f6 b5 54 3d 37 58 45 e5 8e f3 e4 d0 22 92 e4 55 db 9c c5 a1 d9 3c 72 d8 7f 18 45 c3 63 3b f3 2b 62 75 5b 16 56 a1 d7 f7 c2 d6 7b 02 6e 6f ee 97 4b 4f 85 eb b7 b2 47 6b fe 8d 29 1c c7 64 36 7f 03 06 bf da ed 5f 96 82 7d 54 60 59 e0 00 7f 90 dc 51 15 4c 7f 43 60 d8 3a b3 18 66 b4 76 01 bd 33 e6 13 79 2f 1b 85 b4 b2 73 a6 89 c9 a6 f2 d7 d0 5a 62 13 88 2b 64 f3 56 f4 e3 87 13 ba b2 1c 2d 89 31 c4 e4 ed d1 55 95 54 6a 07 79 49 bd f7 06 9a 1e 42 7c dc b5 31 be a1 cb 39 ae 2c 3d 1b 82 fe 7c 63 22 f9 64 cb 08 98 0d 3e f5 27 2c e7 96 e1 7e 97 d0 ed c5 1a e4 ac d8 f5 6c e4 16 4a ef c6 96 60 cc a7 48 21 7c c1 18 b4 a4 33 b6 e2 98 4d 5a e2 49 1e cd 10 a0 d9 14 61 40 1c 50 57 7e d9 5f 58 fc 35 Data Ascii: {>?pim!zKbWT=7XE"U<rEc;+bu[V{noKOGk)d6_}T`YQLC`:fv3y/sZb+dV-1UTjyIB|19,=|c"d>',~lJ`H!|3M ZIa@PW~_X5
2022-10-03 14:16:28 UTC	10453	IN	Data Raw: 00 00 37 ea 00 00 00

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:28 UTC	10501	IN	Data Raw: b8 84 f9 bc 92 c1 44 07 72 40 df 4a 20 98 d4 4c 41 3f 14 49 83 4e 04 86 0f aa de a9 71 9b 96 af 8f 29 9f b0 8a ca 78 ad b6 2e 68 d0 cb 02 28 83 46 a8 13 72 fd 70 bf 6b f4 3c bb ad 5b ec 85 57 8d e3 e0 8a b8 4b b6 00 61 3d e4 fb 6e 25 87 36 41 7b 0c bc fd 48 95 32 e4 96 2d e3 e7 3d 93 0d ec 79 89 c3 65 bf 74 93 7a 78 25 6f 8b ca ff 16 16 80 22 96 49 3f 47 7e f9 04 18 1a 2a 17 43 89 fa 81 9e 96 95 bf d7 26 53 8c df 7e 8a 7b d2 7e e7 b1 9e 43 b0 26 b4 2c 44 a8 b4 6d ce 42 ce 75 d2 b9 c7 cb 6c ff 2e d9 a3 02 04 2d 3b 98 81 49 63 8b 83 69 54 63 b7 e7 d7 29 53 28 6d 40 64 ff 68 59 94 1e 73 bb 8a 68 91 7e 3c 0b c1 49 6b 0b 43 93 8a af 1c 25 cf 51 2c bf 25 da 9c 36 4e 2f 2d 13 96 c0 7f 45 53 bc 5c 64 09 a8 5a 94 b9 75 a9 f9 09 6a e6 f6 46 50 f1 9c c1 90 ac 5b 38 Data Ascii: Dr@J LA?INq)x.h(Frpk<[WKa=n%6A{H2-=yetzx%o"I?G~*C&S~{~C&,DmBuI.-;lciTc)S(m@dhYsh~<lkC%Q, %6N/-ES\dZujFP[8
2022-10-03 14:16:28 UTC	10517	IN	Data Raw: 77 67 e0 d3 cf 03 34 c3 b2 f0 f0 91 a1 e2 5c 1e 87 d2 47 b7 46 1d 12 16 8f 5f 61 25 fd a2 a4 a9 2f c0 0b 68 02 26 ac a4 82 c6 17 97 9e d6 09 09 41 67 52 20 be 68 31 87 07 0a 83 3b f6 81 fd 07 37 47 60 d6 ae 8d b5 37 5d f4 57 d6 3b 8d 09 6d 6a 90 75 d0 52 8a e4 4a a7 84 eb 7a fb 90 1b 26 84 46 7b 94 a9 7b 69 bf 52 f0 ad cb 8d d0 06 d5 ba e1 ba 6f 20 bc be ae f7 3a 56 c3 fe 78 92 d8 66 7f c9 24 72 61 17 3f 01 f6 00 17 61 3c 56 03 43 2b be b7 7a 28 91 72 6d 01 36 eb 83 b0 15 30 93 2d f5 c0 8d 73 38 b6 66 7f f3 b9 9e 85 9d 35 97 f1 ad 77 76 95 2e 0b 91 37 de 23 66 7d 34 eb 8b 12 b8 d6 50 e8 51 79 60 b8 e8 f0 ac da 1f 3d bc 70 ae 91 b9 4d 98 fd 36 b5 4f 61 ba 98 43 fa 12 87 03 d3 8f 3f 63 5f 75 ca 5f 1f 48 aa 8f 63 f8 25 2d 17 0e 3e 47 a5 86 bc d6 a0 ca d0 2e Data Ascii: wg4\GF_a%/h&AgR h1;7G`7]W;mjuRJz&F{{iRo :Vxf$ra?a<VC+z(rm60-s8f5wv.7#f}4PQy`=pM6OaC?c_u_ Hc%->G.
2022-10-03 14:16:28 UTC	10533	IN	Data Raw: 98 83 43 f9 e3 89 7b 55 72 05 73 8a 14 a9 99 29 64 2c f5 8c 96 7a 97 36 f8 31 20 56 4c e7 23 f9 52 a6 4f 97 cd c9 5d 1a dd 1e 07 f7 9a d3 ae f8 cb 8c 78 0c 82 4d 6e e7 a3 a5 29 c6 9f 2e 61 9a ba b0 9d 6d 9e 9a e0 bc d3 f7 ef 0d 07 52 de 72 fc bb 95 f1 75 df 48 84 99 a3 ef 84 f2 6a eb c3 a3 c0 fa b9 88 91 ff 4d 91 14 d7 ad c5 18 74 8a f2 9f 3f 39 b6 ed 04 dc 30 26 b4 c7 ae bc 2b 05 25 1c ea da 04 b9 6b c4 4c 10 0e c8 23 64 5c 85 dd dd c9 ae 42 fc 44 e2 9f 21 b6 c2 b9 9b 71 59 24 72 bb 67 9b 4f fd bc 8c df bd 03 5a a4 94 da d5 12 eb f7 bf 50 3c 91 c4 7c c8 ad 5e fb fe d2 84 3e 24 cf 11 58 ec ab c1 81 ca 34 1b 37 63 31 99 eb e5 2d a2 39 51 4d 5d 8b 2d 3a 6a dc 7c b2 46 b5 ac 17 f7 37 35 e0 8b 24 b3 a9 64 58 1e 04 2d 30 26 c8 eb 86 8e 07 fb 73 52 04 b1 6d a1 Data Ascii: C{Urs)d,z61 VL#RO]xMn).amRruHjMt?90&+%kL#d\BD!qY$rgOZP<\|^>$X47c1-9QM]-:j|F75$dX-0&sRm
2022-10-03 14:16:28 UTC	10549	IN	Data Raw: 39 63 cc 84 28 8a ff 77 c9 c5 7b 40 fa a5 86 2a a1 87 ca 88 71 41 93 a9 0b 67 5d b9 cc 52 26 35 c6 e7 bd 5f 2f e6 70 38 a7 d5 66 c0 69 80 5c a8 f5 70 2f e9 e9 e1 ac 42 24 8a f2 87 46 df 34 82 31 21 b6 02 fb 17 e4 92 f7 6c f0 e7 da 76 b1 78 d7 ba 20 1a f6 8e 0d fe e1 34 38 43 28 e3 d4 04 51 b3 5d a6 b7 eb ac bb 72 14 e6 cc f2 4a 34 05 24 54 18 59 d9 b6 04 c0 b8 63 05 3a 14 97 9b e5 4a cf 5c 01 73 46 ae f8 6b 8a 65 ad 30 f8 6e 82 f7 a3 7f 4e 8d fb 52 38 09 a5 c0 07 00 34 ac d3 d4 fd 17 5a 29 7a 19 ac 51 30 72 73 c2 a0 24 9a 02 f6 cb 21 9b 60 11 55 1e 99 79 29 17 2a ea 73 e9 ee 45 4c 95 42 d1 46 62 dd 55 88 ff 69 aa 52 96 ea 09 d9 40 33 27 17 e1 44 34 26 2e c7 ec db 21 b3 54 8d d3 f9 30 d2 84 11 eb 50 a0 54 81 15 1d 82 d1 39 f7 9a b5 4c b0 13 32 fa e7 a0 32 Data Ascii: 9c(w{@*qAg]R&5_/p8fi\p/B$F41!lvx 48C(Q]rJ4$TYc:J\sFke0nNR84Z)zQ0rs$!`Uy)*sELBFbUiR@3'D4& .!T0PT9L22
2022-10-03 14:16:28 UTC	10565	IN	Data Raw: 33 fa 5b 72 5c 20 9d 98 94 17 ed 7b 1b 4c 4f 20 ba b0 39 83 07 9e 5a 02 72 58 79 92 a2 71 30 47 48 64 df 44 ca e0 f6 f5 71 d9 98 84 26 3c 82 69 5a 48 6a 8c 7f f6 70 13 c8 41 da e4 be 8f df 85 fd 2b 7d ab fa a9 5c b0 2c 7a 42 5f 46 28 7c e9 89 3c 28 f3 35 95 da 75 b0 32 f6 0f 25 43 fa d0 d9 d9 47 6d 98 8c 75 52 d6 8b fa c5 14 69 fb 1c 84 49 c8 0d 08 ef 5e 1d 81 8f 79 a2 af cd 30 2b ef d7 a5 85 cd 4f 38 ea d7 7f d9 83 37 a1 a9 50 2e 91 12 73 11 28 73 08 66 1c 1e 6c 12 a0 9d fd 61 f1 92 78 08 f3 6a 92 d6 7c dd 45 24 51 1b 82 1e f2 9f 6d 36 bd 32 e6 9e 05 b4 d5 91 51 35 75 e4 e9 3f 14 8c f3 58 27 20 20 b2 b8 38 1e aa db 23 a9 22 de c8 1e df d2 d1 5e 75 35 95 00 fc fb 39 89 9f b0 d4 32 d5 82 42 4f 27 2a c8 f8 e5 97 c3 e4 ec 1d 1e dc ac 17 b2 ff c3 8c 38 1b 46 Data Ascii: 3[r\ {LO 9ZrXyq0GHdDq&<iZHjpA+}\,zB_F(|<(5u2%CGmuRiI^y0+O87P.s(sflaxj|E$Qm62Q5u?X' 8#"^ u592BO'*8F
2022-10-03 14:16:28 UTC	10581	IN	Data Raw: ec 63 26 af bd e8 ee ff f7 3f d1 c8 b8 59 07 26 d0 66 5a 7f a7 58 48 37 86 43 99 c7 6d 67 d8 e4 72 b9 28 67 68 0f dc 55 4d a9 d0 08 04 1b d8 69 31 35 a6 eb a4 44 f7 50 3c cd 91 e4 26 46 60 f3 1b ec c5 43 43 e0 c3 17 47 f4 ee 89 30 f3 ee a3 56 9e 58 ae 3a 82 82 43 00 cd a8 ad 3f f2 9b c0 44 6d 04 ff 9b 2b 46 9c 6a 5b a8 a8 a9 64 73 40 0e 51 20 95 e5 80 13 2a d3 b1 b1 35 68 04 72 7a 74 8f 2b d6 31 90 e5 f7 d9 5c f7 13 9c e7 28 f4 e8 db ee 52 e7 7a 53 1f 33 55 c8 df 06 95 b2 30 45 c1 77 c0 85 17 f6 80 1e 30 08 9d 66 b7 84 30 1a 80 75 ff 74 46 66 4f 59 fb 29 ac e4 34 90 d4 c2 93 47 e4 18 62 41 39 83 c0 60 88 26 f1 6f 98 d3 d1 bf af 45 35 64 fb ff ef aa 1c 2e f1 22 ab 3b 60 65 0d f0 20 9d b7 da b5 4e f0 97 eb 6b 43 60 54 8f c8 65 0e 20 d0 45 bc 25 0b e1 4a f5 Data Ascii: c&?Y&fZXH7Cmgr(ghUMi15DP<&F`CCG0VX:C?Dm+Fj[ds@Q *5hrzt+1\(RzS3U0Ew0f0utFfOY)4G bA9`&oE5d.";`e NkC`Te E%J
2022-10-03 14:16:28 UTC	10597	IN	Data Raw: d9 92 c5 77 ee b2 bb 5c fa 50 82 92 3b 35 44 47 3c b8 b2 dc 29 0b c2 77 68 28 22 8d 91 25 54 4d a7 9a 42 43 ed e6 d4 22 a5 88 7c 48 63 58 0c d3 36 b7 1c 63 46 3f ba 5c e5 06 25 cb 59 0d f3 38 a5 22 57 e5 4e e8 41 04 cd f3 6c 4f 72 9e b5 6a 38 52 0a c2 94 6d 17 93 17 f1 bc 2f 1e d7 97 07 68 16 8e 95 5e b6 c6 5e bc 37 6f 50 1d 9c 2f 64 72 ac cb 88 61 fc 81 b4 02 8b 63 a2 7f 82 00 fc ea 76 72 93 e5 b4 3e b4 93 93 94 e7 96 04 90 eb 89 c8 fc 2b 7f cf 29 61 a5 18 f1 49 07 fe c4 52 a1 7c e8 e3 f2 ca b5 c8 e8 d7 96 60 41 86 e6 be c2 e9 f6 42 fc eb a5 bb 7b ce 5b ed a5 d7 27 40 7a 27 95 80 f6 ae e3 ff 78 7b a0 28 68 7e c8 91 58 32 95 07 38 b4 3b cd 0a 52 e8 6f 16 02 76 73 30 ba 61 49 63 2d 80 58 c9 d9 67 f6 f6 f1 49 21 91 d1 ba 6d ef 89 c2 22 eb 19 86 13 c1 f5 51 Data Ascii: w\P;5DG<)wh("%TMBC"|HcX6cF?\%Y8"WNAlOrj8Rm/h^^7oP/dracvr>+)aIR|`AB{['@z'x{(h~X28;Rovs0aIc-Xg!Im"Q

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49731	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:41 UTC	247	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo.png HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/collinesredshare666.htm Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:41 UTC	247	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:41 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:10 GMT ETag: "621a-5b252e7d34b80" Accept-Ranges: bytes Content-Length: 25114 Connection: close Content-Type: image/png
2022-10-03 14:15:42 UTC	247	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 02 04 00 00 00 72 08 06 00 00 00 2c e6 c9 63 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 61 bc 49 44 41 54 78 da ec 5d 05 78 14 c7 db df dd 73 8d bb 02 c1 5d 8a 4b a0 04 d7 16 2f 14 68 71 28 4e 81 e2 14 2b 5e 1c 5a 08 14 28 4e d0 e2 4e d0 40 d0 40 48 88 7b 2e c9 5d ce ef 56 be d9 fc 09 5f 08 77 61 f7 6e 03 49 bb bf e7 b9 27 97 bd 99 d9 f1 f7 f7 be f3 ce 0c 04 b1 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 b0 60 c1 82 05 0b 16 2c 58 fc 0f f0 7f b1 d0 13 ef fc ec 75 2c e1 94 a7 23 df d1 89 0b Data Ascii: PNGIHDRr,ctEXtSoftwareAdobe ImageReadyqe<aIDATx]xs]K/hq(N+^Z(NN@@H{.]V_wanl`,X`,X`,X`,X`,X`,X`,X`,Xu,#
2022-10-03 14:15:42 UTC	263	IN	Data Raw: 10 c4 26 2f 17 ce c9 29 7d e4 3a 06 87 47 2b 5b 22 39 c9 91 9b 74 e3 e0 38 51 15 2a 85 73 60 04 3c 38 a5 6e 25 fe c8 ec 13 01 ab a8 68 8e 54 71 ea 8e d6 8f c7 81 aa 43 e5 1c 6e 0e 48 f8 d5 b5 de 56 d7 b7 b7 9f ca 17 67 ab f0 9a 94 3b 21 0a bd 1d d3 c3 21 cd de 7c dd 7e 6e f0 d1 19 09 0f 3a 71 44 02 38 27 c0 93 43 e9 86 e0 2f 4e 08 36 86 a9 85 0d 47 a5 54 ab f4 5d d2 84 df 0e 28 c3 9e bd 35 85 e5 a9 f1 6e 80 08 94 da ad 74 e4 56 ae 2a 7e fc 79 b3 06 39 ee ef dd 42 8a 59 0a 33 2e 7c 9a 43 ba 2e 7d 93 11 37 d2 de ee a3 31 6b 7b ec 7a b3 df af 3c 0f 88 ac 5d bb 5c 09 14 ad 63 4b 5c 84 cf 7f af e1 49 6b d5 3a c3 11 8b 6d ba ba d8 94 95 d5 e3 f9 b7 df da 7c f6 b8 48 88 d8 94 7f 1e 17 3a c4 64 5d 6a 0d 78 5b 1b 26 75 bc b2 2f ef 21 d5 c0 19 b9 58 75 aa de f7 1a Data Ascii: &/)}:G+["9t8Q*s`<8n%hTqCnHVg;!!|~n:qD8'C/N6GT](5ntV*~y9BY3.|C.}71k{z<]\cK\Ik:m|H:d]jx[&u/!Xu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.6	49925	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:21 UTC	5029	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo_footer.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "e43c-5b252e7d34b80"
2022-10-03 14:16:22 UTC	5110	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:22 GMT Server: Apache Connection: close ETag: "e43c-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.6	49924	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:21 UTC	5030	OUT	GET /wordpress/wp-content/themes/kawaken/images/top_recruit.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:22 UTC	5110	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:22 GMT Server: Apache Last-Modified: Wed, 25 Nov 2020 04:14:36 GMT ETag: "276ff-5b4e6aa49e300" Accept-Ranges: bytes Content-Length: 161535 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:22 UTC	5206	IN	Data Raw: ff d8 ff e1 16 36 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 0c 00 00 01 03 00 01 00 00 00 a8 03 00 00 01 01 03 00 01 00 00 00 f9 01 00 00 02 01 03 00 03 00 00 00 9e 00 00 00 06 01 03 00 01 00 00 00 02 00 00 00 12 01 03 00 01 00 00 00 01 00 00 00 15 01 03 00 01 00 00 00 03 00 00 00 1a 01 05 00 01 00 00 00 a4 00 00 00 1b 01 05 00 01 00 00 00 ac 00 00 00 28 01 03 00 01 00 00 00 02 00 00 00 31 01 02 00 22 00 00 00 b4 00 00 00 32 01 02 00 14 00 00 00 d6 00 00 00 69 87 04 00 01 00 00 00 ec 00 00 00 24 01 00 00 08 00 08 00 08 00 80 fc 0a 00 10 27 00 00 80 fc 0a 00 10 27 00 00 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 39 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 30 3a 31 31 3a 32 35 20 31 33 3a 31 34 3a 32 38 00 00 00 04 00 00 90 07 00 04 Data Ascii: 6ExifII*(1"2i$"Adobe Photoshop CC 2019 (Windows)2020:11:25 13:14:28
2022-10-03 14:16:22 UTC	5222	IN	Data Raw: 20 20 20

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	5702	IN	Data Raw: a1 27 2e c7 12 0a 72 4e 32 0f 45 29 01 3f dd f1 e4 77 2b 99 0e 38 92 30 58 16 03 8b 90 3c 3a e4 0c d9 21 de 49 f4 f6 45 0c 84 39 f8 7a 83 82 84 95 36 b1 d6 db ec 11 cd 81 dd 41 ca 27 80 23 89 38 5d 50 8a b4 b0 b5 36 dd 77 ca 7c 24 82 98 09 12 45 e4 8c 08 61 5c ae 88 55 27 24 ff 00 03 92 0a 86 63 5a 8a 0f 96 4a 95 0b 2c 4a d5 3d 0f b6 58 36 62 42 56 b7 34 97 d0 75 7a 50 71 72 3e 1f bf 2d ab 0c 6a 95 23 92 41 7b 00 42 8e bc d6 aa 0d 18 6f 91 90 f4 95 1c d9 0d f5 b5 98 73 24 ab 23 3b b0 22 8c 6b 5f a0 e6 26 22 4f 26 47 9a 8b ca 2b 50 cd 96 88 b1 25 48 39 ea cc 7d 8d 30 d2 2d 77 38 c6 c6 55 df 02 b9 ee 12 35 67 69 14 2a f5 3b e2 22 4a 54 e0 d4 23 99 f8 46 c8 cc 05 48 04 d6 9f 76 13 0a 54 41 91 fd 8e 46 95 44 ca d5 ea aa 7e fc 69 52 fd 49 cb 5b 1f 8b 70 c3 b6 Data Ascii: '.rN2E)?w+80X<:!lE9z6A'#8]P6w|$Ea\U'$cZJ,J=X6bBV4uzPqr>-j#A{Bos$#;"k_&"O&G+P%H9}0-w8U5gi *;"JT#FHvTAFD~iRl[p
2022-10-03 14:16:23 UTC	5750	IN	Data Raw: c4 b6 77 41 e9 42 7f 71 e9 82 7a d4 d7 29 22 71 e8 ca a1 23 ba db 6f cc 0d 06 55 33 49 e5 cb 5d 2e 64 1c 1a 3b d8 2f e7 8d 14 93 f0 98 84 f2 2b 7d 35 19 1f cc cd ba 3a 6c 5d 59 57 97 7f 31 f4 4d 36 69 6e 92 d2 eb ce 91 da 40 f2 47 e5 cd 2a c2 4b 3b 48 88 dd 49 69 55 15 b8 6f 40 49 a7 6c 89 cb 92 62 9b 40 c3 8f 92 6b 27 e6 de a5 e7 2d 2a 69 b4 d6 9b 43 87 52 89 ed dd da 8b 3c 50 30 e2 f1 5b 2a 33 7a 7c 86 cd 21 6e 47 a0 e3 92 c5 87 7d da 35 1a a1 54 12 6b 1d 35 9a 28 e2 b5 b7 8a 28 55 02 89 9e 8a a1 57 6a 57 36 42 1b 3a c3 35 19 bc b9 a7 c6 1a 6b 9d 48 39 53 f1 08 76 5f ed cb 44 1a 65 30 58 7e a3 a8 59 39 6b 7b 09 4a 5b c6 6a ec 49 ab 11 b6 e7 c3 2c 10 6b e3 be 4c 66 eb cc 69 68 aa a6 53 46 22 35 40 0b 33 3b 1a 2a a2 2d 4b 12 4d 00 1b d7 27 1c 77 c9 06 74 Data Ascii: wABqz)"q#oU3I].d;/+}5:l]YW1M6in@G*K;HIiUo@Ilb@k'-*iCR<P0[*3z|!nG}5Tk5((UWjW6B:5kH9Sv_De0 X~Y9k{J[jI,kLfihSF"5@3;*-KM'wt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.6	49926	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:23 UTC	5654	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_comsys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "31e7-5b252e7c40940"
2022-10-03 14:16:23 UTC	6676	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:23 GMT Server: Apache Connection: close ETag: "31e7-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.6	49929	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	7492	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_tosys.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "2982-5b252e7c40940"
2022-10-03 14:16:26 UTC	7989	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:26 GMT Server: Apache Connection: close ETag: "2982-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.6	49930	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	7493	OUT	GET /wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:09 GMT If-None-Match: "4356-5b252e7c40940"

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:26 UTC	9285	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:26 GMT Server: Apache Connection: close ETag: "4356-5b252e7c40940"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.6	49931	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:28 UTC	10485	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_facebook.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "28a-5b252e7d34b80"
2022-10-03 14:16:28 UTC	10614	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:28 GMT Server: Apache Connection: close ETag: "28a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.6	49932	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:28 UTC	10613	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_twitter.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "3db-5b252e7d34b80"
2022-10-03 14:16:28 UTC	10614	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:28 GMT Server: Apache Connection: close ETag: "3db-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.6	49934	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:31 UTC	10614	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:31 UTC	10614	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:31 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "2ff37-5b252e7c40940" Accept-Ranges: bytes Content-Length: 196407 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:32 UTC	10615	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 03 04 02 05 00 01 06 07 08 ff da 00 08 01 01 00 00 00 00 f6 55 c5 bc d2 e4 93 9a dc e3 b1 8a 41 8a 6f 40 9b 3e 6a 11 86 2f 92 13 27 1e f7 2d 6e 23 c7 46 1c 86 4a 38 28 9b 79 a9 64 8a Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmt"UAo@>j/'-n#FJ8(yd

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:32 UTC	10631	IN	Data Raw: cc 54 44 d3 d8 07 9d 31 94 2a 15 b4 b3 e3 ec b1 35 13 6d 90 d9 e7 72 aa eb 3b 69 34 96 70 03 d2 c6 84 da a6 d3 cf 5a 97 96 1b d0 d1 31 74 a5 53 7c fe 7e 46 9e a0 d4 a7 ac 46 63 d6 8e 9c 84 95 0c 30 ba d5 b8 cf 1d ac 41 31 6c 99 6e fa 33 f3 b9 fd 8b e5 52 80 d1 19 d8 ce ce 7b 40 53 53 29 6f 09 67 1b 50 09 45 eb 9a 90 ad ee 5c ae 60 80 aa 4c 01 4e c2 a5 5a b1 67 0d c6 cb 97 3e 9b 42 14 55 96 4c 2d 5d 3c b3 81 c9 26 a2 74 a6 36 4b 43 42 61 b4 e0 34 5c ef 5a 4d 25 14 ed 48 54 3d 16 72 a7 0d b1 bd aa d4 da c5 76 43 6d bb 11 cc f8 f7 cb b5 73 56 cc 49 11 41 a4 b2 70 6e ec 89 4a 9 b 0a e5 da d4 ec b3 57 9e bd b6 73 65 e5 fa 16 b5 8e 6d 6d 82 0c e9 59 3a 4f 2c 05 de 9d 1c e8 61 34 d5 d1 12 2d 7b 29 66 a3 27 5e 47 7e fc 96 b4 a6 02 51 4b 47 0f 3c f2 2f 64 51 6b 6c Data Ascii: TD1*5mr;i4pZ1tS|~FFc0A1ln3R{@SS)ogPE\`LNZg>BUL-]<&t6KCBa4\ZM%HT=rvCmsVIApnJWsemmY:O,a4-{}f^G~QKG</dQkl
2022-10-03 14:16:32 UTC	10647	IN	Data Raw: 55 3d 93 43 a8 ed 75 7c 7c 6b 9c 7e 1d 2d 56 f8 63 ed 3b 5f 81 13 ec 58 d5 56 55 e3 fa 7e bf b3 75 0e 46 df c6 06 bc 7f be 3d d1 73 ff 00 73 64 06 d2 18 fd ee 6d d7 ed a3 3a fa 91 44 5c ac 6b 81 f2 14 a4 d9 aa 9f 92 ea 36 b5 ee 0a 3c 36 a0 d3 a9 ed 6d 09 67 91 8e 5b 9f 8a b2 5f 7d bd ae f5 38 8d 71 e0 82 2e 25 77 02 5a cf 4f a9 14 15 7f 22 9d 41 e4 65 21 8d 09 ae ec 7a 40 50 bc d7 b1 15 c7 40 55 7b 9e 22 2e 47 1f bb eb 06 c4 fa b5 d8 9f 55 68 3b 5f 23 98 42 b1 04 db 8a 86 d2 60 7a ab 40 8b f5 09 d9 9e 51 61 ee a7 53 a5 1d 6a 2d 6d d1 9e de 5a 36 e2 ab 7c 3e 15 c9 f1 c1 97 ee 55 13 db a8 09 f9 8b 64 f2 6f 73 69 d6 99 d4 c0 4f e7 92 88 2d f8 82 ce e6 90 fd 9a d4 e4 44 5a dd 94 b4 fa 0c 9e 3c d4 0f 76 8f 03 b1 32 08 b1 8e cd 57 2d 65 cf 27 20 19 67 f7 6c 9a Data Ascii: U=Cu||k~-Vc;_XVU~uF=ssdm:D\k6<6mg[_}8q.%wZO"Ae!z@P@U{".GUh;_#B`z@QaSj-mZ6|>UdosiO-DZ<v2W-e' gl
2022-10-03 14:16:32 UTC	10663	IN	Data Raw: b9 52 9d cb 7c 81 87 35 71 d8 2d f4 b6 54 ad 03 ae 35 16 dd 57 36 62 5c b3 75 0f a4 23 92 e3 d3 31 2a c5 cb db 65 dc 72 32 6c b2 28 2e 00 95 fd 42 07 58 97 5e 61 c9 e0 3d e9 99 4b 9f 6e cf cc f2 2f e4 10 7f 5c 3a 79 37 90 fa 8d 21 b2 6b 31 68 41 02 a8 f8 27 40 93 8b 51 be d0 46 4e 4e 35 79 37 22 5d 6f dc 07 a7 5d 98 29 75 c6 f5 82 cd ea 54 8c 8c 5a f1 de d4 b4 2d 27 64 b5 98 a7 81 2b ea 19 16 51 6e 35 69 8c a5 30 a9 07 97 b1 a6 5f 1f a6 5d 58 02 a2 2c f5 86 ff 00 9c c2 2e a6 b7 b9 c7 e6 07 50 06 f9 2f 62 55 c8 27 5c 0f 6a cb f7 0d b0 13 91 fc 91 d4 de a6 a7 a3 13 f5 17 01 98 37 e8 b9 12 a0 3b 76 c3 63 f5 78 ec 69 3b c5 ae 5e 4a ee 06 04 41 b2 77 11 f8 89 4b d3 4f 91 ef c9 a1 50 ba d8 9e 41 f0 f7 d7 e4 b0 40 e7 7e e2 fc 4c 6b 1d 81 9c 63 68 08 b5 95 3b ac Data Ascii: R|5q-T5W6b\u#1*er2l(.BX^a=Kn/\:y7!k1hA'@QFNN5y7"]o])uTZ-'d+Qn5i0_]X,.P/bU'\j7;vcxi;^JAwK OPA@~Lkch;
2022-10-03 14:16:32 UTC	10679	IN	Data Raw: d1 dc a8 eb eb b2 03 6e 7a 7e 43 d9 61 99 46 ea bd 33 2a b1 7d b5 b5 64 d6 99 36 a5 45 43 65 25 eb 62 92 f4 0f 69 44 4d 42 ab f9 c3 a5 38 05 0e f8 d4 d9 c1 b2 f2 d6 c4 f0 d7 89 69 5a 96 33 0e 13 1f 69 5a ce 8e e3 50 96 d4 9c b2 30 58 76 d8 f9 86 b7 5a af fa a4 6f 19 9f 5c b5 66 0e 55 58 ae a1 97 97 f7 0c b3 1c f3 52 9e a1 e9 d5 e5 37 21 5e 26 46 35 ce 2d 18 79 16 5c cf 13 08 9f bd 2a 08 34 35 fa 96 8c d1 8c bb 10 7c a1 04 31 56 df e8 bd 8e 21 86 e7 f9 03 2b d8 74 9e 24 2a 0d 3c 49 f8 6f b8 c4 f8 96 e4 56 a1 8b 7a c8 5c 8f 4c 76 a8 59 8d 58 00 59 6d b7 0e 2e a2 70 63 2b c8 77 df 3f da 38 75 1b 73 0d 1c 94 51 fd 37 f2 f0 81 32 2c ad 10 f3 c9 6c 3f 38 ca 02 f7 a3 1d 15 74 cd 8d 2e eb 80 9c 1d b4 17 20 5f 5b 15 7e 25 8e 87 a2 00 36 0b 29 66 b6 5d 85 92 48 28 Data Ascii: nz~CaF3*}d6ECe%biDMB8iZ3iZP0XvZo\fUXR7!^&F5-y*45|1V!+t$*<loVz\LvYXYm.pc+w?8usQ72,l?8t. _[~%6)f]H(
2022-10-03 14:16:32 UTC	10695	IN	Data Raw: 5b 4c 31 50 6b 58 a1 57 da 63 0c 50 07 92 6b 87 08 50 ed e9 a2 11 b1 d8 23 5c 93 49 23 c5 34 4d ba 8a ba 11 e6 21 02 8c 23 28 23 1e fc 15 4d f7 7e e0 fb e5 08 d3 66 7c 74 4d e7 92 62 1e e0 94 10 53 b4 60 b3 5d 90 96 c3 b3 8d 73 5f 3b bd 76 05 ff 00 d7 ff 00 6c a1 9a f8 44 84 33 42 0d f7 3b b0 55 bb 67 ea 53 46 c0 87 bb f3 0f 55 f3 b8 6c 8a 67 35 43 07 14 49 38 c4 ab 4a 68 76 e9 44 5c 4d d0 6b 68 31 14 30 11 24 22 25 62 29 82 f9 de 76 8c 9b f5 4f 96 de e6 3b 26 98 cd cd 3f 45 6f 7a b8 1a 7e 8a c7 aa a4 91 e8 a7 c2 50 44 90 5d 87 45 4f 3f 54 f3 2d 31 ba 63 d5 7b 33 1d 4c 7c 0e fd 55 ab ac de 0d 2f 09 1d c2 6b 6d 46 ad aa 31 54 ee 4b e5 42 0e 12 9f 7b f9 be e8 16 ce 9b c8 8e 94 3d 8a 3e 23 15 09 c4 4b d8 3d 4a 79 74 c9 de 4c f3 95 00 f2 4e 46 78 44 a6 94 d9 Data Ascii: [L1PkXWcPkP#\l#4M!#(#M~f|tMbS`]s_;vlD3B;UgSFUlg5Cl8JhvD\Mkh10$"%b)vO;&?Eoz~PD]EO?T-1c{3L |U/kmF1TKB{=>#K=JytLNFxD
2022-10-03 14:16:32 UTC	10711	IN	Data Raw: f0 35 1a 0e 98 af 88 9a f5 58 3a d2 cd bf 45 a8 08 ff 00 e3 3e 74 55 1e e0 d8 e5 a7 ee 72 b4 3e 8b f2 fa ad 41 f2 d9 9d 97 fe d5 78 d3 e5 94 0f fe 99 59 b7 e5 23 d5 65 07 cf dd f0 97 80 79 1a 15 37 43 5c da f3 9d 8e 21 b3 54 04 c0 08 5e 9f 85 3b 84 66 15 41 2a 4b 6a 61 56 95 4c 16 96 6e 93 74 fd 16 fb 18 0c b3 e2 1f 74 77 af 1a 22 a8 74 d9 94 a2 40 24 61 c1 32 ba e2 51 85 54 26 aa 6d 6c ff 00 d6 3e e9 d2 dd 3f cc 16 3a 7e ed bc b8 72 5b ec f3 ed b3 04 51 a1 34 5f 03 07 dd 38 92 e7 9c 78 6d 12 49 34 d5 09 bb 92 af aa 17 a3 3d 17 ed 2d 78 65 cd 1b ce c9 a3 00 be 5f 4a ad c6 ea 46 3c 91 1c 4e 7b 30 0d 26 8a c5 cf 82 6e 5a 78 80 e6 02 b4 16 9c 41 a0 fd cb a1 6e 37 e4 3f 17 34 c8 f4 44 0f da c4 9c a8 bd a5 af 6f 88 01 92 05 f1 f2 89 56 0f af 0d 98 28 32 08 e0 Data Ascii: 5X:E>tUr>AxY#ey7C\!T^;fA*KjaVLnttw"t@$a2QT&ml>?:~r[Q4_8xml4=-xe_JF<N{0&nZxAn7?4DoV(2
2022-10-03 14:16:32 UTC	10727	IN	Data Raw: 70 80 1a 6b 6e a1 c3 0f 92 3e de 23 c1 6a 69 af a3 2c 6c 01 ba 09 ec b7 22 c2 e1 bb 15 39 04 88 f9 d8 9f 23 a6 8b 47 c4 d0 44 72 5f 04 a1 c1 76 ae 0d 00 2d 57 0f 3c 46 e0 93 4a b2 d0 e4 be 96 07 dc aa e2 b6 cc 67 34 85 7f 14 2e 15 7b b8 14 91 1d 89 4f ea 53 52 ae 9c fa 00 44 ee 90 e8 ad 08 36 04 df b8 5f 24 05 3a 4d 40 91 92 ea 55 8b 56 97 08 e9 fb 4b 71 f3 f1 09 de 90 56 c1 05 30 0d 34 f9 a8 35 b6 5b 11 c0 83 85 bd 42 a3 15 1d 31 45 dc e5 7f e2 14 c4 0c 08 ba a1 c8 52 e1 b9 6b 42 90 71 16 8a 3a 1c 0b 8a e8 fa c5 2d 75 77 63 b2 b1 7a 6d c0 1d 8e 5d 1c 22 52 39 07 05 83 5f 69 96 50 ec 34 95 55 b3 7d 5f 4b 13 28 fc d8 61 d2 fa 83 09 48 b7 a3 91 4c 27 41 14 71 a4 ec 8f a0 eb 73 7f 31 2b b0 b8 95 5d 50 4a 14 d3 7b 7a cb e7 62 30 b7 db 2d 8a 9a a2 9f 29 01 45 Data Ascii: pkn>#ji,l"9#GDr_v-W<FJg4.{OSRD6_$:M@UVKqV045[B1ERkBq:-uwczm]"R9_iP4U}_K(aHL'Aqs1+]PJ{zb0-)E
2022-10-03 14:16:32 UTC	10743	IN	Data Raw: 2f 86 2c 50 b9 5a ee 36 c5 25 57 56 d7 52 a6 ad 88 1b 17 eb 55 c1 9a aa 87 60 4c 43 f2 69 3d ca 4d 1b 74 e7 9b ad 25 cd 12 59 54 3d 64 bb 2c f0 a0 33 25 57 7a c0 48 ed 85 d5 79 85 55 0a 28 8e 0c 8f 20 2f 30 52 2c 5c 00 c3 00 e1 7a d1 2f 65 01 35 80 e1 17 37 76 9e b1 49 7e 11 c4 46 82 2a e5 45 7e a1 d6 fa 27 bf 44 21 c0 ea 62 da 95 e9 47 ba 1f cb 2e 5f 44 b5 fe aa 65 a9 4f 5d 6f 55 2d 6d 0f 6c 54 2f 29 fe 93 01 a5 a5 e5 01 f5 2b a1 a7 0a 45 50 93 ce 0f e8 8e a8 77 75 af e6 56 b6 3b 56 d6 35 7c 2a cd 35 a2 5b d6 fc 13 9a 6c b7 8f e5 3a ca 9b 04 3e 84 9b b1 81 00 7a 42 12 13 6e aa cc f7 73 27 e3 4e 5f 94 2c 95 91 49 d7 4d 65 d8 c3 b9 34 e8 73 cc 68 a3 65 99 fc cf 37 37 50 b6 4a ca 73 2d 35 39 ee 16 ae 5e 1a f1 1d d7 c0 65 f9 54 e6 03 49 16 01 44 01 17 06 c0 Data Ascii: /,PZ6%WVRU`LCi=Mt%YT=d,3%WzHyU(/0R,\z/e57vI~F*E~'D!bG._DeO]oU-mIT/)+EPwuV;V5|*5[I:>zBns 'N_.IMe4she77PJs-59^eTID
2022-10-03 14:16:32 UTC	10759	IN	Data Raw: 38 81 3e e2 05 04 3f 17 2e 96 48 b1 c0 06 44 9c 9e 94 7e 84 85 2c 12 35 94 39 36 b8 f9 82 05 63 c8 c4 5a d3 40 a0 a4 b4 28 a7 40 a7 f3 0a eb 9d 07 96 15 34 71 8a fa ee 15 30 d6 23 64 62 93 7d bd b9 a4 f8 bb 6b ee 54 a2 d7 51 ec 40 3a 05 5f ab 85 8a 0f c4 3f 6c 95 f0 43 a3 91 9c 14 ff 00 e8 77 36 4f a1 ec b6 54 91 ed 4d 4c ac 81 29 65 f0 c7 ed 9c 80 7c ff 00 00 81 c0 bb 84 b7 c2 fd 4f 21 79 9e e0 25 f6 1e 47 f6 44 dd 76 d5 96 97 cd f1 3b fc 6d 66 76 b7 81 81 a4 43 c3 9a 89 d5 74 b3 6a 81 0f 00 c2 c4 e8 57 80 7e 22 18 de f0 f4 9e 12 29 28 0e 2f fd 20 ea d1 f6 40 f7 37 af 4f 3e bf 11 0d 56 dd 1f ea 17 6e 7c 94 45 28 65 72 61 03 f2 57 fe 0c 5d a7 40 6b fd 97 e1 a5 ab 0c 66 90 d1 48 57 d5 c5 20 10 d0 51 f2 6d 45 0e 34 ec d5 c5 2a cb 00 59 c8 37 69 b6 d5 51 2e Data Ascii: 8>?.HD~,596cZ@(@4q0#db}kTQ@:_?ICw6OTML)e|O!y%GDv;mfvCtjW~")(/ @7O>Vn|E(eraW]@kfHW QmE4*Y7iQ.

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:33 UTC	10775	IN	Data Raw: 22 84 97 0e 8d 5d 9e 48 ec 8f 91 51 28 2b cc 34 8d 6e 6d 41 a5 e2 e5 9f 8a 2d 47 b5 af 8b 85 27 c3 a5 3b 85 c1 48 25 00 4a c5 2e 97 20 6a 83 37 d1 25 05 aa 6d b0 b1 54 04 1a 2d 30 45 74 70 e8 1b 49 1e 57 7d 4d b5 56 ed ce 25 e9 70 4c 6a e6 9f 60 8f e4 85 c3 4b e4 bc 95 08 07 cb f8 2f 72 5c ce 1e 7f fa 4b 9d 92 e8 dd a7 53 df 80 bf 0d 95 06 cd 6e e2 20 b4 a9 f1 48 c8 51 ab 67 08 c4 be 81 08 c1 01 48 3a b5 e5 83 67 86 5c 4e 38 73 29 7a a9 4d c2 97 b4 03 29 0f 97 16 cb 6f 0b 2b dc 10 e6 cb 69 b8 41 62 cf 92 c3 82 30 22 72 c2 61 cf 25 2d a2 b2 59 77 ff 00 c5 08 71 e4 7f 70 ad 13 9e e0 3f 6e 25 03 a7 fb 21 db 29 9f c4 c7 80 0b 72 26 cf 44 82 87 d4 ad aa 8a d3 d9 bc 3e a6 4c 22 27 9f 0f 86 57 50 92 af 8c 45 68 6b a1 35 65 8f 99 82 c0 3d 0a 3c c2 c0 ed 63 78 a0 Data Ascii: "]HQ(+4nmA-G';H%J. j7%mT-0EtpIW}MV%pLj`K/r\KSn HQgH:g\N8s)zM)o+iAb0"ra%-Ywqp?n%!)r&D>L"' WPEhk5e=<cx
2022-10-03 14:16:33 UTC	10791	IN	Data Raw: cb 72 2f 41 56 42 82 86 09 d9 74 de da 35 1e a1 47 8c 28 47 d1 7d 50 0e 90 f7 2f f6 28 bf b9 9f 3a ed af cd 43 68 82 77 17 7b 16 9b 11 c2 f7 8d 04 3f 21 b0 d8 7c 6e 34 41 03 51 73 a3 44 04 21 87 40 d7 15 75 14 95 51 e4 90 37 d4 48 d1 49 4f 1b fe 40 27 22 be 4a 18 ef 11 00 b3 be 20 52 ee 46 dc 71 f2 46 85 41 73 91 11 2d 54 a7 0a 7f 64 ae 85 5a dd 0e 5f dc ef b0 0d 35 a7 87 a0 87 45 2c 23 62 79 18 8a 01 47 fb 88 e0 93 c0 0a 5b bb 95 60 61 4f 9f 8f 64 73 6a da 03 76 ca 8e b5 0e 8f 78 09 fc 49 f9 58 10 07 8a c1 87 ac a3 c4 ea 19 c4 76 2a 35 cb 1f a8 08 e7 1f 87 f7 2b 9d ae ef 27 90 e1 37 9c 7f 10 5e b4 4b 16 c7 07 3f 71 29 61 69 e7 b2 6a 2d 0b 70 78 ea 14 93 5a da 1f 4f e6 5b af 69 fd 5c 9e e7 32 92 7e ca 7f 3c 47 a1 5a 1f c1 1e 55 5a b1 ce b1 75 e4 0b 6c be Data Ascii: r/AVBt5G(G}P/(:Chw{?!|n4AQsD!@uQ7HIO@'"J RFqFAs-TdZ_5E,#byG[`aOdsjvxIXv*5+'7^K?q)aij-pxZO[i\2~ <GZUZul

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.6	49933	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:32 UTC	10615	OUT	GET /wordpress/wp-content/themes/kawaken/images/icon_Instagram.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "16b4-5b252e7d34b80"
2022-10-03 14:16:32 UTC	10647	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:32 GMT Server: Apache Connection: close ETag: "16b4-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.6	49938	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:34 UTC	10807	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_02.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:35 UTC	10808	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:35 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "72497-5b252e7c40940" Accept-Ranges: bytes Content-Length: 468119 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:35 UTC	10809	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 06 06 06 07 07 06 09 0a 09 0a 09 0d 0c 0b 0b 0c 0d 14 0e 0f 0e 0f 0e 14 1f 13 16 13 13 16 13 1f 1b 21 1b 19 1b 21 1b 31 26 22 22 26 31 38 2f 2d 2f 38 44 3d 3d 44 56 51 56 70 70 96 01 06 06 06 06 06 06 07 07 06 09 0a 09 0a 09 0d 0c 0b 0b 0c 0d 14 0e 0f 0e 0f 0e 14 1f 13 16 13 13 16 13 1f 1b 21 1b 19 1b 21 1b 31 26 22 22 26 31 38 2f 2d 2f 38 44 3d 3d 44 56 51 56 70 70 96 ff c2 00 11 08 04 74 03 84 03 01 11 00 02 11 01 03 11 01 ff c4 00 1c 00 00 03 01 01 01 01 01 00 00 00 00 00 00 00 00 04 05 06 03 07 02 01 00 08 ff da 00 08 01 01 00 00 00 00 9d 51 43 e3 f0 0e 89 30 0d b2 f5 a0 6d 91 2e 2b 43 d3 3b 04 35 76 6e a4 7f 1c d9 4e e9 04 67 23 44 c7 4d 07 f8 bd b7 9c f7 c5 Data Ascii: JFIF!!1&""&18/-/8D==DVQVpp!!1&""&18/-/8D==DVQVpptQC0m.+C;5vnNg#DM
2022-10-03 14:16:35 UTC	10825	IN	Data Raw: 0a ea bc f1 74 cf 9b 3d 31 1f 1c 86 4d ef a6 ad fe 0e 3a 14 ce d3 9d 1e b7 8c e6 b9 af 98 c5 ef f3 2a e9 29 96 43 dc df 53 d5 4c 16 59 a2 df 11 97 14 2b f7 7c 57 fb d1 17 9f 5f af 9f 1d e9 fa a8 57 a3 e5 d6 67 e6 04 d7 0d 12 ae 57 b2 99 da 98 e7 a5 d3 b9 e0 71 7b 1e 59 4d d7 ec ce 77 9b b0 f3 15 4a 64 b3 d0 39 fc 8d 21 21 6e 11 a2 4a ea 57 ad 22 a3 2b 42 cd 18 22 7c b5 3b 9d 27 a4 7e 9a 5d e5 5a d0 2f 3e f8 a6 ab 93 77 91 71 a8 ac 33 fa 6d f3 04 a7 8e 2a 73 5d 1c cd a3 81 fe 25 f3 62 7d 0f 3a ed 6b 1b a9 8e bc 5c 96 df e6 40 0f 24 07 b1 e1 7b bf 45 f3 91 42 8a 81 14 46 ca d5 3d 2b ad ba 09 15 97 a0 32 fa 40 68 7a 61 aa 7b bd 23 f3 aa 75 75 79 49 7e 46 0e 8a 1b 6c 44 14 1f 91 f4 cb 6d a7 65 10 94 30 ef 19 3b ca 7b 3c 8f 68 fe 43 df a2 39 3d 9f 23 d6 e0 69 Data Ascii: t=1M:*)CSLY+|W_WgWq{YMwJd9!!nJW"+B"|;'~]Z/>wq3m*s]%b}:k\@${EBF=+2@hza{#uuyI~FIDme0;{<hC9 =#i

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:35 UTC	10873	IN	Data Raw: 76 e9 46 8b 2e 15 1c 1e 83 bf 3c b2 61 d1 93 3d ed e7 60 f9 53 62 c3 6c db 14 08 6f 80 c0 31 01 f3 ba 3c e4 bb a8 a8 11 04 ea d4 be 45 4b 4f 6a 44 2d 88 7c c8 89 7e 8e 05 20 5c e5 22 49 6a f1 1b e4 74 96 c6 8c 87 76 9e 0d b6 93 b6 28 a4 02 30 1a 97 d8 c9 90 ec 33 ea 8a 4f 34 4d c7 4f 0a 6c 0d 8a bc 16 8f 91 75 b9 45 2c b4 07 34 2a 8a b9 f0 e8 bf 13 a0 2d 1b f1 4b aa 5b ab 99 d9 15 ee bb 57 a5 bc 86 61 2a 38 dc eb b6 db 6d 9f ab 10 af 14 a0 c1 73 5d 99 72 b9 5a 34 4e 81 c4 85 66 38 42 af 29 bb e7 65 03 ae 33 a9 9c 49 6a a6 ca 0b d8 78 dd a6 7d 5c d1 bc 5a ad 99 f9 c1 b2 ac 05 dc ee 1c 41 18 9d 8e d6 29 41 a4 0e 1b 6d 4b b6 95 4e 77 e9 e1 10 62 fc ed 4d 2b 1c a9 b1 04 e4 6b cd 6c 8e 24 8f 92 c1 54 67 7a f9 ab dd 69 27 2b 3a 37 64 f8 aa ba d9 72 91 78 47 6d Data Ascii: vF.<a=`Sblo1<EKOjD-|~ \"|jtv(03O4MOluE,4*-K[Wa*8ms]rZ4Nf8B)e3ljx}\ZA)AmKNwbM+kl$Tgzi'+:7drxGm
2022-10-03 14:16:35 UTC	10889	IN	Data Raw: c3 c9 92 bc 5a f5 d4 9f e9 f5 92 4c a6 94 a4 e1 33 0b 01 39 5c eb 03 62 b7 b5 ec 39 6d 8f f0 b8 c6 65 26 96 fe ed c9 c7 db a6 57 11 54 c1 f0 26 46 71 01 ff 00 48 59 a5 83 f6 72 44 c3 11 0b eb d4 5b 7f e6 b1 18 0d b6 8b 55 4b dc b3 8c 43 dd e3 f1 dd 50 ad da d6 e2 e5 f1 68 ad 2b 4b 2a b1 d9 5b 0e 55 36 ac 39 44 50 aa 0e 01 c5 4c b6 26 0a ea 79 27 09 f4 2d a2 93 e3 b6 8a ce c2 df 36 1a 28 7c a9 9e 7d 8f 8e 0d 73 98 5a bc 92 03 95 1e a9 62 7b 08 59 7f c0 92 d9 68 14 b3 cd 3a 18 55 c0 33 e9 f6 06 3d 38 c0 8b 75 8b ea 7d 6d fc db 8d ea 59 36 76 72 5b cc ec 44 d9 40 3b 63 25 82 57 52 3a 8d be 82 b6 20 ca d4 a2 bc 71 69 2b 12 90 8d d5 dc 6a ce 5d 6b b1 aa 68 b6 06 ec db 8c 00 b5 d8 2b 21 df 9a 68 b3 d9 6d 75 f5 2b e5 c7 c8 60 d3 f5 81 5d 79 b0 ab 55 5e 6e f1 9e Data Ascii: ZL39\b9me&WT&FqHYrD[UKCPh+K*[U69DPL&y'-6(|}sZb{Yh:U3=8u}mY6vr[D@;c%WR: qi+j]kh+!hmu+`]yU^n
2022-10-03 14:16:35 UTC	10905	IN	Data Raw: 40 bf 84 93 99 dd 1b 41 33 89 ff 00 cb 34 b3 9f 7b cf aa ba 79 18 cc b4 da 6e b3 61 36 13 65 9b 2c ca 4f 49 aa ce bf 8e 38 cd f5 cb 57 4f 80 cf fa 0c ad f3 e5 20 81 2b bf c3 7f 24 8b 2c 36 bf 7c 34 f7 69 77 e0 2b 96 31 5c a4 b5 cf c4 ae b2 7d bf e0 c9 86 ce b3 0b a4 7b 35 23 02 ef 81 28 5f 55 32 fe 4d 34 0f 77 e6 0b 01 01 c3 35 85 e3 bb 11 ee 9c 80 a2 1b 05 89 99 4f 22 bb 14 23 d9 59 5c ce 45 9a aa d4 7e 98 64 67 3f 49 6a 9a c5 db 10 0b 60 40 32 23 8f 78 dc 90 8b aa fc ce e6 25 60 31 ed ec 06 54 09 65 24 bb 45 6c c5 5d a2 55 93 1e b0 13 be 84 3c 94 0a 25 8e b6 76 71 e4 5e 9b 65 f9 5d 5c e2 53 5e 88 d1 f6 66 85 58 99 f4 e3 5c b5 03 03 31 dd b5 c9 77 63 f8 8d d4 c1 b3 46 4e a6 ae 33 9a fd 60 3d e4 7d 41 12 cf 5b 2e 46 65 0d bc ac 66 83 b5 55 9c e6 00 fd 92 Data Ascii: @A34{yna6e,OI8WO +$,6\|4iw+1\}{5#(_U2M4w5O"#Y\E~dg?Ij`@2#x%`1Te$El]U<%vq^e]\S^fX\1wcFN3`=}A[.FefU
2022-10-03 14:16:36 UTC	10969	IN	Data Raw: 8f 4c da 5d 05 97 96 d9 74 fa 76 f9 82 84 45 cb 2d 48 4b 6a 9f 8e a1 46 55 94 a9 ae 91 17 0f 61 78 b6 05 ad 44 e4 5a c8 06 0b 17 ec e2 62 71 fa 69 83 3a 85 b1 1b 42 73 2a b4 c7 7c fe 59 39 e8 e3 fc ad d1 a6 ac 17 bc 8f 50 30 0e 35 a7 8d bd 5a 4a 4f 2f 8e 02 59 6f 23 60 41 4a 6d bc 1f 1a d5 7d 00 b3 a5 bf 53 b8 96 f1 ae 11 5b 49 e7 cc 0a 7a 2c 49 51 80 6d 6e e6 6f 36 9b 7f 05 2a 6f 9f 13 2f f6 a9 52 9f 22 90 cb b2 b8 bb 38 1f ac 4d 40 84 60 91 05 0a 6c bc 93 e3 55 ca 38 1d 18 b6 78 76 d1 6f 67 5a eb 96 51 5a 92 eb 50 a1 c1 dc d1 89 5f 12 de f5 6a 1a a5 20 27 1a d1 d9 b3 ef 3e b1 91 d2 d0 92 ca 8f cc 3e 23 d1 50 81 70 c7 c6 4e b3 53 b0 81 14 1f 4a 6c 2f f6 e6 5d 5b d9 0e 47 57 db d0 13 61 6a be 45 76 58 32 98 62 46 b4 54 e7 65 8d 45 8e 47 96 c0 85 bc 23 Data Ascii: L]tvE-HKjFUaxDZbqi:Bs*|Y9P05ZJO/Yo#`AJm}S[Iz,lQmno6*o/R"8M@`lU8xvogZQZP_j '>>#PpNSJl/][G WajEvX2bFTeEG#
2022-10-03 14:16:36 UTC	10985	IN	Data Raw: 84 09 a0 09 a8 1b aa 36 05 f5 46 6a 89 84 0f a8 0b f9 9d 8f f7 5c 33 bd 63 f5 59 5b d0 94 75 bb 56 67 0e a9 a6 da d5 0c a7 a5 14 76 1b a2 64 6e 68 b8 4d ea b8 6d ed 28 76 85 27 78 b2 0e 0e a4 99 4c 64 d6 a4 4a 6e c8 1c 01 24 45 13 5e 32 de a0 20 e0 37 2b f8 91 23 45 c4 67 41 9a 17 16 7b 4e 19 fa 27 3e 00 f9 8d c2 e2 4a e3 41 69 b2 37 73 48 3b 52 57 15 8e 73 85 41 5c 31 dc 27 3b 29 d3 f5 56 1e c8 c8 26 bd 93 7e 6b 77 46 bb e8 13 c9 8a ec 15 76 41 b1 34 1a af 50 ab d3 75 cb 16 ae a5 65 ce d1 a5 20 7b 26 49 26 47 95 13 be 58 8e 9d 53 e0 e6 34 db a2 88 cc 08 4d 9f 38 5c 39 d8 0a 28 8a c6 d0 d4 67 c9 0b a2 8d 5a 7c aa 85 91 3d 54 f9 e8 84 02 8d 74 c3 78 5f d4 4a a9 1a ce 8b e6 33 69 47 28 9f 34 4c ef 72 8f 8f 87 3e a8 0a 01 1d 13 49 b5 67 74 26 54 4e 55 a2 24 Data Ascii: 6Fj\3cY[uVgvdnhMm(v'xLdJn$E^2 7+#EgA{N'>JAi7sH;RWsA\1';)V&~kwFvA4Pue {&I&GXS4M8\9(gZ\|=Tt x_J3iG(4Lr>Igt&TNU$
2022-10-03 14:16:36 UTC	11001	IN	Data Raw: 4c 98 25 42 a4 09 09 97 b2 15 43 45 a5 d1 4d a8 56 43 0a e0 53 54 60 50 a7 dd 6d 83 95 7e 0a 14 ec 4a e1 d7 39 5a 58 68 86 a8 d1 49 11 1b 20 a3 cd 16 f9 20 13 14 28 a6 89 e2 e9 c2 01 1e ca c4 d7 b2 74 82 ad f6 56 df ff 00 81 b4 fa e1 a9 85 a7 fa 07 00 50 41 70 c0 ea 11 95 44 20 47 aa 15 36 42 a8 4b 76 54 c6 c0 61 a2 94 13 a1 32 9d 0a f7 51 f0 0c 44 c9 54 c3 44 53 93 97 cb 46 ab ca d7 54 ed 7b ad 56 a8 21 0d 08 27 08 c0 05 52 82 14 55 f8 61 46 03 cf 03 64 31 f4 4d 3f 74 5a b8 23 c6 66 65 70 db 42 01 71 34 46 e5 36 7c d0 b5 d3 eb b2 04 9d 6a 9a 00 ec a2 73 5b 75 c3 b9 52 4c 6c 9a 6a b9 5b 09 a1 a0 c7 52 50 6b 43 44 cc ca e0 70 f2 90 39 a2 b8 ef 80 4c 2b 84 57 0d 37 dd 47 fa 1d 30 d0 ad 70 2b 6f f4 02 8c 1c 8a 9b 5d 15 18 3a 07 c3 28 51 32 b8 42 12 54 f5 44 Data Ascii: L%BCEMVCST`Pm~J9ZXhI (tVPApD G6BKvTa2QDTDSFT{V!'RUaFd1M?tZ#fepBq4F6|js[uRLlj[RPkCDp9L+W7G0p+o]:(Q2BTD
2022-10-03 14:16:36 UTC	11017	IN	Data Raw: 2e 8d 27 88 2e 42 8e 35 2f 79 de 83 fd 78 81 b9 69 8a f1 5c 44 54 0c cc d1 d1 be 15 96 52 18 1e 40 37 fb 22 a8 8d 39 63 e9 89 4c c0 7e 01 39 61 05 03 5a 9c f3 50 a5 2d 61 f5 29 9c 01 43 66 d1 97 6a fc c1 68 30 ac 55 71 f1 2d 6d b1 9b 0a 13 75 e2 1f 36 4c de fb 7f a8 e8 c1 91 9b 75 02 c5 6c 9f 4f 51 50 d1 b5 3e 1f 24 b1 51 49 74 c6 7c eb d4 21 7c 0c 0c 59 e7 ea 28 81 1b 34 e6 39 25 5b 46 87 9d ca 14 0f 04 76 9d 38 be 7e a3 97 8b 54 5e 4c 43 50 69 9d 17 6f 05 13 70 83 b1 3f 33 3e 4c cf 5a 23 57 3c ed 76 2e 5e ea 3a ae 7f ea b8 ba ae 57 6d af 72 8b f6 2e 25 55 2c e9 c1 d3 f2 96 60 2a 3a a3 c9 9a 45 c4 b8 27 0b e4 f5 3a 37 29 a8 1e 49 9c 98 97 4c b2 28 5b 05 fe 7c 4c 6f db 0f 8b e1 01 2f b6 00 c0 ac bd f1 2d a7 86 53 50 e2 ab ea 0e e1 40 4c 07 6c 11 45 8b 3a Data Ascii: .'.B5/yxi\DTR@7"9cL~9aZP-a)Cfjh0Uq-mu6LulOQP>$QIt|!|Y(49%[Fv8~T^LCPiop?3>LZ#W<v.^:Wmr.%U ,`*:E':7)IL([|Lo/-SP@LIE:
2022-10-03 14:16:36 UTC	11033	IN	Data Raw: a8 53 b6 e5 e3 76 f9 96 73 1e 36 17 5f 6f 70 63 65 d8 d6 99 c7 37 08 e6 68 40 57 f1 13 54 13 fd ef a4 62 69 33 6c 0f 5e c6 79 49 6e d8 4d 95 db 95 12 b1 ca ac 85 fc b0 a9 16 29 e2 22 ed 4f 0a 6a 00 54 2d 26 38 e2 73 ef 7d 42 f2 04 15 56 90 f5 9f e6 26 7f a2 b0 71 a7 b7 58 ce e6 f8 05 a0 dd db b8 ec 6d f1 da ff 00 51 29 68 b7 c8 83 62 bc fe 06 51 e8 ab 02 dd ab 3c 54 ca 30 14 c5 1a cf cc 3b e0 15 97 cc 24 2d 4f 03 ed 60 2f 88 2b 0e 53 6e cf ed 29 70 1d 18 25 95 dc 0a 5f 1e 63 45 e9 99 40 01 2e bc 45 da 3e 65 85 d4 2d b1 e8 33 32 64 f7 03 42 3e 49 84 61 e5 18 37 ea 27 dd 5c 0b 11 48 63 cc 2b e8 89 d6 1e 7f f2 5f 88 15 6a a4 7b f5 2f c6 c2 b3 36 e8 ec 7b 83 56 7c 30 f7 ca a5 1d 79 80 4f 1c 46 49 23 00 ad d4 27 a8 39 39 57 83 3b fb 38 c3 95 e0 cf 1b 3d e9 9a Data Ascii: Svs6_opce7h@WTbi3l^yInM)"OjT-&8s}BV&qXmQ)hbQ<T0;$-O`/+Sn)p%_cE@.E>e-32dB>Ia7'\Hc+_j{/6{V |0yOFI#'99W;8=
2022-10-03 14:16:36 UTC	11049	IN	Data Raw: 05 d9 e2 56 d0 05 bc e2 2c 1b af ce f0 b8 08 1c 59 71 9f ee 07 e4 5a fb f3 18 60 72 a3 4f 0c cc 13 54 31 e3 fa 25 25 1b 1f f7 98 80 a2 b5 2e de b3 04 56 95 3a 3e a5 27 24 2b 7a ac 3f 71 9f 4b 81 79 c1 4e 25 c6 a9 50 53 8f cc 28 65 6f 6d 99 94 c5 b5 5c e2 ef 88 9b a6 85 d2 bc 46 00 16 6d bd 90 d1 5e 48 70 6a a0 35 73 1a dd c0 30 55 2b a5 79 21 2d c0 30 0f 51 18 d4 75 36 6a ba da 50 b4 9d bf 78 8d e8 ec 6d d2 5b d7 0c 3c ce 58 27 24 1d ea ff 00 73 24 7e 90 11 de e1 0e 38 a5 2b fb 5e 22 d0 6c b2 f1 d5 93 b3 8e 59 b5 84 4c 4d e5 96 5e 73 77 71 38 25 6b a7 55 4c 40 01 c0 e6 fb f8 86 af 41 0d 8b c7 9b 88 30 38 95 82 5e 94 51 7f dc 29 c5 81 5e 8e 7e 66 21 ae 0a ea 54 03 de 74 1c dd 11 2c 65 7f 18 07 79 cf 99 cf 88 5d e3 07 dc 52 f3 0e 5a 37 33 1b 9c d9 d3 17 03 Data Ascii: V,YqZ`rOT1%%.V:>'$+z?qKyN%PS(eom\Fm^Hpj5s0U+y!-0Qu6jPxm[<X's~8+^"lYLM^swq8%kUL@A08^Q)^ ~f!Tt,ey]RZ73

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:36 UTC	11143	IN	Data Raw: e7 99 11 07 ba 43 8a 98 7e cb fe 23 29 19 54 ac 0e 6a 70 f5 4c 4d 4b dc 0e 21 6e b0 63 6c 54 60 85 84 3d 12 d8 8d 55 71 7b 8a 22 b7 79 66 f2 9f 25 cb 82 dc 84 0c b2 c5 03 cb c7 52 ab 58 53 41 c4 75 e7 2d 57 27 07 98 db 45 cc a8 ea e2 80 64 bd 6e 59 c9 f6 65 b2 a1 4c 61 f7 10 2b ef 98 f2 1a dc c6 cd 34 79 94 32 ed 2c 1a 32 2b cf 10 cb 45 33 00 39 bd 54 d2 a8 46 9f ca 5b 68 a5 58 a4 ad 90 4a ad 2d fe 12 f6 e6 3c 4a 96 10 78 8a f3 2b cb 2f 73 a7 52 f9 97 cb fd ca d3 66 10 40 a6 b7 8c c3 c2 d7 92 d2 92 52 ba 1b 19 8f 6c e6 ed be ee d8 58 a8 5e d2 8d 6a 68 e1 d4 67 36 8c d0 b3 10 59 64 b4 59 a8 05 78 f0 23 f3 13 08 5b 63 99 a4 e4 4a f1 ff 00 88 5a d1 2d b9 ea 19 6a 6e 49 42 d8 fe 88 d3 3f f7 91 86 07 e4 09 4c 72 01 18 ba ca 9c 73 8e 60 de ec 47 f7 3d 65 3a ff Data Ascii: C~#)TjpLMK!nclT`=Uq{"yf%RXSAu-W'EdnYeLa+4y2,2+E39TF[hXJ-<Jx+/sRf@RlX^jhg6YdYx#[cJZ-jnIB?Lrs`G=e:
2022-10-03 14:16:36 UTC	11159	IN	Data Raw: 30 7e 2c fe 20 f7 01 3a 98 8c d0 d4 c9 3b 99 24 53 c8 64 19 3e 65 36 38 cc c8 78 ad d9 04 32 77 24 c1 78 fb a9 6d 53 a2 8f ba 8a cd 5a b1 6a 7c 42 e5 31 25 48 e2 9d 4c 8a e2 33 47 a3 7f 73 9b f2 54 eb 85 80 7e a7 d7 8b 98 c2 60 ed 77 e6 19 b7 96 50 2d 4b f8 3f 30 02 c2 b8 e6 31 5b a2 de 78 96 f3 0c 33 8f f1 0b b9 c9 48 ed e6 d7 22 74 f4 d5 33 f1 1d db 6b 3d 3e e6 55 b8 14 36 4c 75 b2 bc a7 ea 50 e5 98 c0 d7 30 8c e2 58 1d ee 53 79 02 af 82 dd 4e 0f 0c 2e 7c 12 f3 3a f5 1b 53 33 7c 04 42 30 05 b6 df 51 e4 78 6d e1 ea 1d b2 c5 b1 d3 b0 19 ac 45 e0 80 66 3e a8 53 80 55 59 6f 94 a2 a9 bc e7 53 01 75 bc 78 8d ec db ea 02 e2 d5 2e ae aa 5a 0f 32 e8 dc bb 00 18 37 6e c5 d4 43 90 a7 46 2a 83 7b 5b ee 28 90 f1 f7 33 16 5c 70 c5 8f 52 80 05 05 47 02 6c f9 3e a1 0b Data Ascii: 0~, :;$Sd>e68x2w$xmSZj|B1%HL3GsT~`wP-K?01[x3H"t3k=>U6LuP0XSyN.|:S3|B0QxmEf>SUYoSux.Z27nCF*{[(3\pRGI>
2022-10-03 14:16:36 UTC	11175	IN	Data Raw: a6 3f 10 cd d1 d7 3c 25 ec b7 00 ac ea 08 b2 0d b5 69 8f 21 f4 58 35 ad 07 ca 98 c9 83 04 7c b6 15 3e f1 86 0b 43 2d e4 04 ab e5 7e f0 5c dc 9f ea 8b 0c 23 a8 f0 88 eb a2 ff 00 dc 93 02 56 ed 76 2b bc 57 4b d3 02 6f 4d fe 98 f1 50 48 6a 79 f7 fc 62 99 10 db 6e b8 08 18 26 47 9a cf b3 dc c1 0b 35 57 e4 ee 43 c6 69 cd c0 a8 c0 37 42 82 8a 1f e6 44 11 3a 6f de 6e 54 c7 df 5c 48 d6 cf 63 70 6a e5 40 3b d1 c0 5c 00 32 01 f4 83 a7 79 88 4c b9 86 bc e0 41 45 c1 db 34 4c 62 fc 81 42 83 91 89 d3 41 f2 ad fc 8e 04 da 8e df 96 05 c5 a8 24 f5 66 86 b2 cb 20 52 2c 55 d5 6b b8 09 76 1a 8b e4 d1 3b 70 01 6b 21 a1 69 bc 1a c2 7c b5 fb d3 42 fe ce 8c aa e6 40 56 ba c4 d9 b3 98 f4 5a 7c 24 f4 0f fb 8c 3d 11 e5 81 ec fa c4 87 77 69 68 a7 ac 60 68 ce a4 2d 53 08 ae 37 6f 37 Data Ascii: ?<%i!X5|>C-~\#Vv+WKoMPHjybn&G5WCi7BD:onT\Hcpj@;\2yLAE4LbBA$f R,Ukv;pk!i\|B@VZ\|$=wih`h-S7o7
2022-10-03 14:16:36 UTC	11191	IN	Data Raw: 9e 15 ab b4 60 12 e0 4d 4a 6b 12 b2 d1 c2 ca 66 62 4a 74 3e 8a a9 ac 5f 43 61 6a b4 f0 84 f7 7d c3 7b 18 3c 8e fa f0 c5 e5 0c ee 8b 5a ac 38 21 95 c1 55 e1 d5 6a 72 e2 eb a9 08 bb 23 a7 61 fd 30 44 a4 6c 89 eb 75 a5 1a 67 20 3f ae dc 6d c1 5e 86 0a 3a 1e 83 da 1e 38 d6 d6 33 e2 ce bb 8d 48 fd e4 f8 1f 97 dd ca 4d ac 94 df e7 c6 48 0a 0d ee b4 4f 82 99 4e 65 a0 06 5f cb 31 b2 8a 07 ab 6e 06 5d 40 84 86 f1 bd cf ce 0a 38 1a 14 4b 03 28 77 1c 5d 00 43 e6 17 2c cc b0 0d 67 7f 1b 5d 62 f6 a6 84 a4 a5 b8 77 1e 5d 33 f1 05 61 08 30 da d4 37 cc 75 4d b5 a0 63 bc 8a da 13 35 ef be 3e 99 40 18 15 57 11 7c 58 e4 92 31 50 6b ed f2 e6 f0 9b 0a 1e 59 d9 18 32 9c 50 88 a9 4f d7 86 11 00 08 c2 0d 93 65 ef c6 35 85 68 b0 99 a1 89 80 9b e6 ee 78 61 4f 44 c8 1a d2 d3 05 8d Data Ascii: `MJkfbJt>_Caj}{<Z8!Ujr#a0Dlug ?m^:83HMHONe_1n]@8K(w]C,g]bw]3a07uMc5>@W|X1PkY2POe5hxaOD
2022-10-03 14:16:36 UTC	11207	IN	Data Raw: 61 e7 85 15 10 9b 50 2f 0a 63 0e 18 82 31 d2 b2 ee 73 e7 25 95 de dc 5d a0 9c 35 bc 91 2c 8d b3 95 e9 51 f4 e4 84 49 87 3b 4d 30 71 59 1a 31 22 aa bc 9e b3 59 b2 53 35 58 06 25 42 a2 15 d9 67 87 86 34 89 9a 6c 59 b2 e8 d7 d6 14 ab 68 23 c3 35 ef e3 98 d0 65 0c 36 d5 54 05 0f 17 04 fa 39 57 0d bf 28 40 c5 10 89 18 cd 05 27 99 b9 dc 0e 74 42 50 ac 4a 15 c1 4b d1 2a 88 96 99 b7 49 15 05 5d 93 78 22 b5 5b 7c d0 43 d0 f8 c1 2f 58 9a 36 32 37 2c fb 5a 8d 5b 46 34 9d f5 62 ed 01 57 ec 70 85 21 34 3c 48 bd 07 93 3e 7c ad ba d3 ae 4e 83 ba 9f 58 bf b8 3d 5f 5f d1 ee 21 7b 5c 48 bb 09 ca 2e 48 b8 44 68 00 23 e6 d1 c9 fb 25 97 5f d6 c3 1c 47 c9 6d a8 18 4a 44 f7 85 24 0e 9f a3 e7 26 4b d0 b5 56 0f 8e 1f 79 27 9f 12 9b 97 c8 c7 95 10 02 dd c7 e3 78 20 18 37 7c ce 7b Data Ascii: aP/c1s%]5,QI;M0qY1"YS5X%Bg4lYh#5e6T9W(@'tBPJK*I]x"[|C/X627,Z[F4bWp!4<H>|NX=__!{\H.HDh#%_GmJD$&KVy'x 7|{
2022-10-03 14:16:36 UTC	11223	IN	Data Raw: 51 d2 c4 46 fa dc dd 31 15 4a 4a 06 98 9e 31 a0 ab 60 d7 5f 70 31 26 aa 00 91 79 1f eb 84 b3 70 83 42 97 ed 70 68 a3 c2 e4 dd 82 62 46 6e b6 80 45 fc 0c 97 2d 00 e1 18 17 98 f1 81 14 50 b8 51 00 1d be 5d fd 99 ab 55 22 28 1f 5f 97 08 3d a1 7c 21 6e fc 70 2b 29 78 97 07 c7 16 89 8c 9e 4f b8 3e 44 c1 2b 28 ec 5f 92 c0 28 4e 9a 7b 0b c7 36 dd a5 e8 f8 b8 13 10 29 a8 f1 fa 71 33 8d 25 7a 5e fb 85 44 ab 5f 07 b2 62 25 10 53 c6 1c d7 75 da 87 70 7d 8d 20 e0 e9 36 62 41 99 44 47 ce 3d f9 b8 40 aa 1a f9 3f 79 2f a1 c5 ef fa d1 cf 80 88 60 4f 30 6a c2 7c f7 b5 69 83 07 74 5d 39 b1 40 f2 e3 94 bc 2a 6f 61 30 ce 43 3d a4 cf 02 70 dd 18 90 53 f9 93 0b 71 aa 22 9e 28 9f 8c 2e 03 4a c9 c7 26 09 f6 e1 99 2d 82 b4 ba e2 3b 6e 20 16 5b 5e 8a 20 03 58 7c e6 a0 33 5b 38 69 Data Ascii: QF1JJ1`_p1&ypBphbFnE-PQ]U"(_=|!np+)xO>D+(_(N{6)q3%z^D_b%Sup} 6bADG=@?y/`O0j|it]9@*oa0C=pSq"(.J&-;n [^ X|3[8i
2022-10-03 14:16:36 UTC	11239	IN	Data Raw: ff 00 c7 ff 00 83 e9 7f d3 12 c8 38 3f c4 72 01 3d ff 00 ac 92 82 fb fb 73 98 e4 77 82 87 f4 c0 9e b4 16 6b ec b9 27 fa c4 b6 fc e1 27 31 98 87 51 67 bb 98 c5 53 a9 3f 79 10 0d cb 54 df e8 c5 2f 0b 7f 06 03 10 0a d3 e1 a7 0b 4a af 3b 35 c5 89 52 43 12 47 57 cc 04 fc ec 5a c2 1b 20 7b 29 ea b0 e0 db ef 7f b9 74 27 10 71 fe 36 1c 91 79 83 00 9a c0 35 8b a4 4e 43 d9 80 93 2f e3 66 99 c7 fb d8 c6 7f ab 41 c4 bf f8 63 0f 51 5f 78 0c 41 3c 5a c1 f2 92 2c 4a d4 31 78 22 1e 18 63 80 08 70 01 f6 e5 81 40 4e 13 5f 8c 66 42 10 bf e3 f4 bb ca bb a0 5f 90 6f 2a ca 21 38 b7 4d 4b 69 fb b9 44 46 e3 90 1e 0d c7 ef 37 79 5f 54 b4 fd 63 3a 91 00 95 ea 6d 26 39 60 17 01 86 2d 09 45 aa c8 f0 cf 90 28 ef ae b4 66 b5 7c 48 aa 28 fa 67 31 5d 74 87 47 9f 3b 81 8c 74 95 ab c3 02 Data Ascii: 8?r=swk"1QgS?yT/J;5RCGWZ {)t'q6y5NC/fAcQ_xA<Z,J1x"cp@N_fB_o*!8MKiDF7y_Tc:m&9`-E(f|H(g1]tG;t
2022-10-03 14:16:36 UTC	11255	IN	Data Raw: ba aa 8a 57 9f 32 c7 47 31 03 d1 fa 7c 60 5d 0f 0e 01 01 4d fd b8 2a 6c 6f 1f 35 23 90 ed 04 74 34 8e 57 78 53 37 77 d0 da 38 68 34 22 30 7f 23 58 be 41 04 1d ad ce 69 f6 e1 bd 48 ca 69 3c 34 b1 29 db 92 a2 fa da 63 87 6a c5 ae 0a fd e3 d4 31 ec 28 7e 24 71 eb fa db fa f3 1d 5c 74 a7 19 e8 e0 e6 0b 42 01 77 16 1f 24 13 34 a8 a3 5c df 98 23 4a 24 50 f3 41 0d e0 93 82 98 92 d5 03 f3 87 3a f5 21 1c d0 3d c4 59 08 02 fb b0 3b 92 b1 0b 1e bd 50 c2 22 31 7c 0e 2f 19 48 40 6d 40 fa 3c 66 3b 56 b3 dc fa ac 5e 8e c5 46 a4 bf 03 02 8e 61 5a 7c 03 ca 60 45 24 a6 e7 c9 8f 4f aa a1 a4 0d fc 60 d2 ed 1f 0e 8c b5 fb c2 5d a2 cf 56 3a 52 d8 a0 3f 74 93 16 8d 45 d5 07 de bb 93 ad 2d a0 f4 2a 16 4c ba 08 a1 df b2 cd b3 d5 4d 17 84 37 8f 0e 8d c9 df 71 25 34 3f f7 dc 24 19 Data Ascii: W2G1|`]M*lo5#t4WxS7w8h4"0#XAiHi<4)cj1(~$q\tBw$4\#J$PA:!=Y;P"1|/H@m@<f;V^FaZ|`E$O`]V:R?tE-*LM7q%4?$
2022-10-03 14:16:36 UTC	11271	IN	Data Raw: cf 03 8c fe 18 e4 62 0f 27 89 2a 04 47 72 d2 72 e2 7d a3 49 a4 49 38 f3 37 95 91 f9 64 a3 2b 18 d8 2c 9f 28 13 92 8a 77 7d ce d3 29 a3 c3 4c 31 2c d2 39 93 81 46 4e 37 e9 df 26 97 8a 01 9b 86 1f be 3b 8f 19 e1 cf c6 b6 50 c7 25 e4 19 9b 79 4b b0 83 85 bc 3e 58 e1 0a ae 25 43 e3 41 ab 99 51 f8 89 12 5a 37 3e 44 91 63 46 82 8a c4 a1 63 61 28 55 f1 c8 6d 19 83 01 b1 8d 42 c2 01 57 90 af ca ce 0e 44 69 d0 a5 75 f1 4e 51 9d cc 65 85 30 0e 55 97 97 3c 46 54 3f 31 27 f1 27 14 ea 91 b8 91 c4 07 e7 c7 8c e0 1c 67 5f 27 9a 40 78 f1 c0 41 75 9d cc 93 44 8d 33 1d 5a d8 04 34 15 70 c2 4a 86 14 48 61 0a 86 61 d8 77 9c ca f6 43 f0 9e 60 b4 62 17 30 57 67 57 25 1f 89 c9 5f 07 f1 cc 29 7c 6e 27 1e 24 df 91 35 38 6e 2c 34 91 22 b3 ca dc 99 11 95 49 5c 1c 49 8b a6 cc 72 58 Data Ascii: b'*Grr}II87d+,(w})L1,9FN7&;P%yK>X%CAQZ7>DcFca(UmBWDiuNQe0U<FT?1"g_'@xAuD3Z4pJ HaawC`b0WgW%_)|n'$58n,4"I\IrX

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:36 UTC	11287	IN	Data Raw: 71 25 40 6a fa 8e 1f e5 96 05 92 e4 45 45 00 ae ce ef ab 8d d8 80 a4 0d 48 2a 40 88 f2 59 14 8a 1c ce 3a 70 b8 88 53 94 58 90 39 28 a1 5f 46 87 82 92 f2 63 8d 94 da 7e 90 93 3d 21 55 89 f8 0c b3 68 00 d4 24 89 4c f1 d8 f0 a1 56 67 5c 87 88 c5 b6 77 72 04 f2 71 d8 28 01 91 39 4c 1c 17 4b 8d 8a 36 f2 13 59 0b cc c5 40 7b 1c e9 c1 69 22 57 05 a3 fd 55 78 ee bc 79 21 b2 dc ae 31 99 27 4e 33 03 3c b0 ce 4e 90 78 c4 1c 98 f4 48 e7 8a c2 04 9f 98 80 13 1c 63 c5 1c 87 6f 50 a2 bb 2b 24 2b b3 cf 3a 72 36 8b 53 8b 34 ce 5d 40 2a 63 97 c3 bb 14 2e 44 92 ce 43 3a 2a 8f 02 b4 a0 17 f8 cc 8c ac e0 1a 58 97 90 84 6c 93 53 18 8a 44 5e f2 68 23 f1 6c 85 46 24 60 14 8e 40 fa c7 0b 26 c5 3f 0e 67 19 8a 96 1a 1c 45 21 2f 70 4c 23 68 3e 41 70 42 e7 73 dd 78 5e 7e 91 4e c2 4e Data Ascii: q%@jEEH*@Y:pSX9(_Fc~=!Uh$LVg\wrq(9LK6Y@{i"WUxy!1'N3<NxHcoP+$+:r6S4]@*c.DC:*XlSD^h#lF$`@&?gE!/pL#h>ApBsx^~NN
2022-10-03 14:16:36 UTC	11303	IN	Data Raw: 4d 47 af 3a 96 a5 14 55 98 9e ff 00 7f bc 2c 06 1e d4 d6 43 0f 91 cb b6 52 eb 59 a0 ff 00 c3 c5 04 6e e4 bf cb 9e c6 35 8e 58 9c 95 dc f2 a4 0a c8 48 e4 4c ca d1 a1 86 98 b3 aa b5 fc 8a 24 9f 97 97 63 40 b2 a2 c5 d4 bd b2 2a 20 cd 16 34 60 df 98 57 88 dd 5a f1 ca c8 c7 41 ab 34 6c 15 77 23 54 92 18 55 50 30 18 ee 24 90 e9 ed 60 92 77 1f 3d 57 95 03 2b 80 f3 a1 5a 62 e5 d1 2b 08 10 49 4d 4c 57 8f 23 6c c2 a9 b9 29 13 23 c5 11 da 5e 5c fc 92 03 b5 2c 72 33 8d 3c 60 e4 28 b0 a7 fb 0c 48 8d 98 06 57 58 39 11 aa 06 c4 74 4f 81 3d f2 99 83 fc eb 57 e4 c2 57 fc 60 87 8a 74 e4 22 47 24 9f 36 fe 6c 4e c5 06 c2 19 d6 63 e2 78 0a 37 23 83 be ce 9d e7 1d 51 44 a1 ff 00 10 8a 01 a1 4a fc 52 54 10 30 a3 3b 04 41 6c 20 78 10 31 75 db 67 1c 8d 64 7c 8a 45 d5 e2 62 31 85 Data Ascii: MG:U,CRYn5XHL$c@* 4`WZA4lw#TUP0$`w=W+Zb+IMLW#I)#^\,r3<`(HWX9tO=WW`t"G$6lNcx7#QDJRT0;Al x1ugd|Eb1
2022-10-03 14:16:36 UTC	11319	IN	Data Raw: 47 d6 78 98 93 87 8d 7e db 3f 8b 18 fa ec 46 40 ac d0 e5 1a a3 84 5d 00 b9 2a 15 88 e4 23 fc 71 e4 ca 1f 93 02 b2 d8 1c 58 2f fe 2c 8e 0e 33 b3 8f 16 3f 1b 8e 8a 58 44 32 05 0b 0c 60 67 23 b9 b8 ca 7f 6e 30 06 4e 4b 7d f2 ff 00 e0 61 8a 29 50 64 3f ff 00 26 63 9c 83 50 3e 40 2a 08 86 4f dc fc 65 c7 e9 58 e7 08 54 19 cc ef c2 32 5f c5 b3 8c 14 c7 64 77 43 00 17 9d 03 d6 7b 3f 58 7d 64 79 78 30 8b 18 bd f7 9f fe 33 d9 cb c6 ec fe f7 96 32 ba bb cd b1 8f 58 c2 d1 b1 ac ad e0 62 3a cd 88 36 0e 29 2c c8 4f a7 6b f5 89 2f b0 05 e0 91 ec 28 f5 e9 6f 25 25 80 1e b3 51 f7 8c a0 82 05 e6 a0 2e 1b 2d d7 78 aa 83 b3 83 de 1a db 14 01 8e 18 b1 51 81 18 7d 67 63 a3 fb 55 8b c5 03 d8 cd ab eb 36 d9 a8 af 50 a9 0c 4f d1 c3 3c 6a c1 4f 46 41 b0 a1 e9 e2 3f 58 8a ce 6a ab Data Ascii: Gx~?F@]*#qX/,3?XD2`g#n0NK}a)Pd?&cP>@*OeXT2_dwC{?X}dyx032Xb:6),Ok/(o%%Q.-xQ}gcU6PO<jOFA?Xj
2022-10-03 14:16:36 UTC	11335	IN	Data Raw: 59 b5 fa 5a 62 47 ac dd 22 b6 ec e2 f2 61 65 2e 6c 67 96 c6 c8 09 06 72 09 24 1c 49 96 46 a1 ee 7e 64 91 1a 54 b6 88 4e 50 33 bf 6b 13 01 63 b0 e9 2b b2 69 2e aa dc 69 a4 7f 9b 92 21 55 8d 34 18 e2 fb 19 e8 76 b9 77 85 98 1e b0 bf f7 d9 3d 25 fd f6 ea 18 f5 93 33 21 d8 63 3b 4a 36 28 d5 12 ec 59 ca d6 34 a1 4d 2f 78 9c 97 88 f5 e9 39 42 41 44 d6 68 87 b1 ef e5 9d de 15 ac 03 1b fa c0 d4 73 6a f7 de 52 9f 5d 19 e0 2f db 0c 82 17 12 77 e8 44 83 00 00 74 b9 63 ff 00 58 cd d7 59 b5 fd 67 47 3d 77 88 ae fd d7 5c 88 1c 0d bd 84 76 47 b5 16 7f 55 9f 90 52 34 58 88 c8 e2 94 2b 92 84 88 78 dc 34 8d 27 0a 70 cc 8c 7e 2b 58 8c 9e 55 23 db 15 2d 79 12 30 62 d5 8c 2a 4b ee cb d1 a7 bc b0 45 83 84 e0 ec 65 d8 bc 42 3b bc e8 fd e1 0f f5 94 c0 d9 c0 a1 ff 00 1c 31 90 30 Data Ascii: YZbG"ae.lgr$IF~dTNP3kc+i.i!U4vw=%3!c;J6(Y4M/x9BADhsjR]/wDtcXYgG=w\vGUR4X+x4'p~+XU#-y0b*K EeB;10
2022-10-03 14:16:36 UTC	11351	IN	Data Raw: cc ab 78 98 10 f2 44 5f 62 6e 28 b1 4b 55 2f a1 b3 6b 03 c7 4d 91 b3 59 42 70 61 b6 ec 74 1b c8 fe 84 4e 8f 2a 64 56 b9 ec 48 fe da 21 63 dc 9d 38 d7 8d 16 90 31 3f cf a4 e6 62 33 dc fb 13 8e c7 ab f5 11 3e a4 b1 79 37 36 66 ed 6e 2e 22 4a 9d e6 1a 66 f4 27 1d 5e f2 2b b4 ea 75 53 23 d9 d8 8f 09 1b 45 3d 43 c7 e9 bb d4 c7 c3 b0 b2 96 5e 8e ff 00 51 ff 00 42 44 af c9 3c 64 cc 4a 6a 18 84 ad 3b b1 5e 24 da e6 cf 91 93 9b 18 27 3c 90 6d c8 96 e5 54 d8 58 7e e3 ae de 20 6b 62 6c b4 e0 cc c8 ee 9e 9e f6 d5 0f 4c 77 c6 a9 0d ea bb a0 cf a8 ff 00 65 30 47 7a ec 97 33 88 37 9c 8f 83 de 18 fe a3 ce c2 bc 9e 26 09 6d 2d e6 66 49 85 24 d9 3a da 5f 83 a1 fc 34 c6 46 93 69 e5 49 ca 70 8f b9 4a db 28 e8 51 d5 cb 1a b2 d8 e2 9d 8c fd 11 9c e0 78 85 24 c3 9f 85 b1 7f 6b Data Ascii: xD_bn(KU/kMYBpatN*dVH!c81?b3>y76fn."Jf'^+uS#E=C^QBD<dJj;^$'<mTX~ kblLwe0Gz37&m-fI$:_4FiI pJ(Qx$k
2022-10-03 14:16:36 UTC	11367	IN	Data Raw: 24 80 ac 3f 97 0d 9c a5 c3 e2 bb 02 7e 82 92 a4 0e 75 93 c7 64 c6 1d ab 8b a8 0e 8a 80 4f 1f 12 e7 04 3b 85 88 10 3d be 3b 04 e0 0c 59 70 54 a5 20 93 1b 62 7c e7 12 85 18 c9 99 b2 be 35 b4 40 67 f5 25 f0 ff 00 07 c6 ca 31 f3 37 64 e4 24 ef ac ed c5 16 ac 9c 4d c1 79 9a 13 16 45 f2 13 98 6d a2 71 db 8d a3 b0 06 cd 4b 7c 84 ea 80 5f e6 63 e0 0a b9 c7 51 73 2b bb e3 0b 19 55 87 b4 7c c9 e3 e4 a3 66 65 f3 db 97 11 ea 3c 5f 29 0e 62 96 5a 11 5d c1 45 aa 21 37 35 5b 82 c3 7f 82 75 31 83 41 8c 5d cf ba 88 40 6b 0d 32 a9 05 58 8b 87 10 74 66 fd 63 82 1b 70 45 34 38 76 38 5e c3 40 59 d4 81 40 e7 52 7b dc c9 8d 95 a8 f5 6c 36 4e 94 a8 3f cc 4c 43 2f be 31 51 c3 10 14 a4 45 e0 d6 63 6d a7 72 d8 8d 74 01 63 b1 50 71 1a 11 19 03 f7 63 23 0c 8d d8 11 97 e3 25 5f 64 9a Data Ascii: $?~udO;=;YpT b\|5@g%17d$MyEmqK|_cQs+U|fe<_)bZ]E!75[u1A]@k2XtfcpE48v8^@Y@R{l6N?LC/1QEcmrtcPqc#%_d
2022-10-03 14:16:36 UTC	11383	IN	Data Raw: 76 14 1a a9 dc 97 0f c0 d1 b0 de a6 86 44 a2 a4 dc 18 b1 f1 15 0a 10 95 5a 6e b5 31 aa 22 d1 26 38 c6 86 d5 e8 a3 29 4a 5b b0 d7 c4 2f 65 ce c5 dc 5e 45 ac 91 4f ed 97 8a 18 88 18 b8 76 a3 8f 1a 63 62 c1 6e 64 cb 6e 35 53 91 de a2 f0 2a 2e cc 3c 80 e5 ba ca e1 95 38 20 00 97 cc b7 54 31 9a 83 30 3b 75 89 98 f1 63 a0 17 32 1d 9e d9 91 97 d7 64 2b 13 4a 0c f1 ec 59 7d 0c a5 48 ba a8 9f 11 73 c8 13 18 00 c6 8d 04 52 14 cc 6a fc ba d2 3b 16 2a 16 3f 12 34 de d6 0f d4 0b 5b fa cb 5c 4d 45 fd 0f f2 b6 16 8c a3 ce c0 84 33 b0 0b 73 3d ae 30 03 6f 17 57 f7 fe 62 a9 7c 9e ed a5 c3 85 5b 95 9a 20 df a1 04 b6 12 31 92 7b c0 3d 89 33 e8 54 c9 7c 66 15 0e d6 65 d0 96 a4 31 8d 7b b8 10 1d c5 14 61 60 65 df 73 fe a2 a3 13 40 c7 2e 82 aa 37 23 b3 03 b0 3d 4c 79 6c fb 45 Data Ascii: vDZn1"&8)J[/e^EOvcbndn5S*.<8 T10;uc2d+JY}HsRj;*?4[\ME3s=0oWb|[1{=3T|fe1{a`es@.7#=LylE
2022-10-03 14:16:36 UTC	11399	IN	Data Raw: 32 50 22 c4 2c c4 05 27 66 c0 e2 77 08 20 c6 52 14 90 27 16 fe 25 42 20 16 67 1f f3 0d 85 81 58 6c c0 2e 50 a8 05 0b 9d 4b a3 1c df dc 02 cc e8 c0 3e e2 ff 00 33 b1 1f b8 1a 85 47 e2 cb 6a 36 03 00 1a a2 b5 fd 4e 54 b5 c7 6a 68 cd 77 0d cb e2 36 37 90 e4 6e 16 b4 19 6e 87 41 f4 07 f1 a9 40 88 58 81 eb 19 de f6 61 2f 36 37 70 39 1d c1 ec 74 20 54 43 47 bb 03 ee 31 b6 52 04 66 fa 12 89 1b 8d a1 3e ae 5d 42 20 a3 d8 99 4a d6 86 ce 36 00 31 eb 85 8e e7 00 04 65 d6 a5 50 a8 2e 7b 90 38 1b 9c 9d 80 62 25 93 94 6a a6 30 a0 55 d4 72 1c 05 05 04 38 38 21 f6 06 70 75 5e 40 5c f1 f1 ae 4b 2e d5 33 70 42 46 27 0d 30 0c 25 79 3b d1 76 c7 ed 46 06 5b 5a dc 2d 5d 45 76 af b9 4f c4 30 16 42 60 66 47 3e a7 2a a7 22 55 ee 37 53 7c c5 c3 fd d3 b6 52 7b e7 90 be c4 ff 00 73 Data Ascii: 2P",'fw R'%B gXl.PK>3Gj6NTjhw67nnA@Xa/67p9t TCG1Rf>]B J61eP.{8b%j0Ur88!pu^@\K.3pBF'0%y;vF[Z-]EvO0B`fG>*"U7S|R{s
2022-10-03 14:16:36 UTC	11415	IN	Data Raw: de 04 2d cb 3a 27 34 75 54 7c 2a b3 a4 ba d9 6e 26 89 a2 1e a6 c2 d0 e0 7a 41 fe 97 64 e8 c7 47 73 e4 5b 2a 23 61 d8 54 42 a6 e7 17 63 cd 8e c9 1a cb 20 76 48 8d 6e 2f 91 2c ba ef 98 92 cb fd 8d ea fe 0d d1 ca 16 90 35 39 b3 6d c7 44 4b c9 6c 67 7c b3 12 37 a5 87 ad 15 9d 5d 27 32 72 67 56 b9 0e 9b 21 7d e0 5d 64 64 3d d5 84 71 45 7c 76 15 11 b9 78 a2 16 87 03 d0 58 2c 2b ba 6a a8 96 aa ab 4c 87 67 4b 8c 56 f0 6a c5 6c 08 dd 53 61 51 6f 45 3e e2 dc f1 3a 0c b9 e0 7a 24 49 a5 56 b9 9b 08 d4 6f 27 c1 ab b8 ee f2 26 3d 8d cf b2 da 1b 88 74 59 34 ef 47 fa 38 d8 45 f2 d0 55 79 1c 60 7b 0b e4 5d 13 0a f8 11 79 13 54 b4 da 8c e9 d5 f3 4d ec 59 cc a1 d8 6a f7 8a 2a 2d ab 7c 2b 0c 5f 91 fd e1 de 8a 8c 67 24 7b 1c 2b d1 ba 72 5a ad 1b 1b f1 47 96 59 16 a6 f4 b2 4c Data Ascii: -:'4uT|*n&zAdGs[*#aTBc vHn/,59mDKlg|7]'2rgV!}]dd=qE|vxX,+jLgKVjlSaQoE>:z$IVo'&=tY4G8EUy`{}yTMYj*-\|+_g${+rZGYL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49735	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:15:42 UTC	272	OUT	GET /wordpress/wp-content/themes/kawaken/images/tel_freedial.svg HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/css/layout.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:15:42 UTC	275	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:15:42 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:12 GMT ETag: "627-5b252e7f1d000" Accept-Ranges: bytes Content-Length: 1575 Connection: close Content-Type: image/svg+xml
2022-10-03 14:15:42 UTC	275	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 34 39 2e 39 33 20 33 32 2e 37 36 22 3e 3c 64 65 66 73 3e 3c 73 74 79 6c 65 3e 2e 63 6c 73 2d 31 7b 66 69 6c 6c 3a 23 30 31 35 38 39 36 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 2f 64 65 66 73 3e 3c 74 69 74 6c 65 3e e3 82 a2 e3 82 bb e3 83 83 e3 83 88 20 31 3c 2f 74 69 74 6c 65 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 5f 32 22 20 64 61 74 61 2d 6e 61 6d 65 3d 22 e3 83 ac e3 82 a4 e3 83 a4 e3 83 bc 20 32 22 3e 3c 67 20 69 64 3d 22 e3 83 ac e3 82 a4 e3 82 a2 e3 82 a6 e3 83 88 22 3e 3c 70 61 74 68 20 63 6c 61 73 73 3d 22 63 6c 73 2d 31 22 20 64 3d 22 4d 30 2c 30 56 35 2e 31 31 61 32 39 2e 32 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 49.93 32.76"><defs><style>.cls-1{fill:#015896;}</style></defs><title> 1</title><g id="_2" data-name=" 2"><g id=""><path class="cls-1" d="M0,0V5.11a29.2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.6	49939	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:34 UTC	10807	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_03.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:35 UTC	10809	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:35 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "2773e-5b252e7c40940" Accept-Ranges: bytes Content-Length: 161598 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:35 UTC	10841	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 01 05 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 6d 57 02 b8 07 00 0a a0 00 00 38 55 14 07 28 0a ae 01 c0 02 a8 00 00 aa 08 03 80 15 40 1c 00 00 00 00 00 0a 80 73 f5 55 c0 0a Data Ascii: JFIF"#"" ""*#>1++1>H<9<HWNNWmhm"#*"" ""*#>1++1>H<9<HWNNWmhmt"mW8U(@sU
2022-10-03 14:16:35 UTC	10857	IN	Data Raw: b1 f3 35 6c ea 93 84 48 73 44 8c c7 b4 37 73 6f bb c1 f5 0c 11 b6 eb b5 5d 65 d6 94 07 26 d9 dd b6 59 6e f3 dd bc 9d 1e 24 67 47 6f cd 74 fb 38 a3 28 cb 3d 15 41 40 cc bd e5 71 c5 b2 1e 3f d0 75 f2 f2 31 ce ed 57 d9 6d ae 86 46 8c f9 f5 66 e8 ae 27 aa 84 6e c9 5e 5d 9c 98 4f 55 f7 d3 8e 85 b3 15 70 33 2f 7d 55 9c eb e9 f2 de 83 af 43 cf c1 bf 4d d6 5b 74 b3 c8 bb 17 0b 77 7b 83 bf 2d 32 b7 4d b7 e2 be d3 95 96 3b a8 aa ca 23 d3 e7 52 19 63 ec 76 e8 e2 ea cf e5 bb 9d e8 ac 7c 3e ff 00 36 56 dd 7c b3 48 9e 4e 24 bd 37 3a c7 2e 27 6e ec b7 65 d1 66 9b 6b cd 9b 36 0d 3b 23 4e 38 41 e5 8d ba ba 9a 35 51 e5 bd 07 a3 cb 8a 8e 67 ae cf 46 1b b4 14 48 ca e3 93 a9 0b ab 87 0b d1 0f 25 b2 b9 10 b7 26 d2 8a f2 f3 e3 18 bc f0 6d dd d0 d3 c2 ef fa 2c f9 31 73 bd 64 57 Data Ascii: 5lHsD7so]e&Yn$gGot8(=A@q?u1WmFf'n^]OUp3/}UCM[tw{-2M;#Rcv|>6V|HN$7:.'nefk6;#N8A5QgFH%&m,1 sdW

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:36 UTC	10921	IN	Data Raw: d9 22 ec 4b c7 32 3a 34 27 63 93 fe 7e e6 7f a4 71 fd a7 c9 3f ea 73 fc d3 60 fe 24 59 1f bd 4c 1f c3 8f 24 fe 1c f9 c6 ff 00 3f 4f 63 63 a4 6e 40 38 ef 81 69 00 b5 dd d8 c4 9d a9 9f 8e 9a 0b 12 de e2 dc 41 66 9d e8 ad b1 88 ab d7 bb f2 3a 3a 32 2b 23 43 67 8e 00 57 8d ec d5 47 8a 78 c4 b0 c8 25 8f 9d e9 5a f7 59 ae 52 61 15 c9 a1 9e 0b 2f 14 f1 1a f7 78 ee 69 b4 b0 58 3d ab d1 d6 4c 3d 49 cf 4a 9a 21 79 1a de 80 73 28 06 c7 2b 62 62 d1 ae 91 78 98 25 16 a3 99 87 68 bd 20 48 a4 d6 73 ec 3e 1a ce 5f 82 3b 04 d7 b0 9b 51 66 7a 6e 91 de 7f 52 0b 31 55 9e 26 ad 77 d1 58 4c f3 d2 94 45 7a 5f 96 cd 28 6c c4 2b d8 8d c0 5b 13 c7 32 57 bc 57 d4 e7 e8 c3 34 50 97 53 ea 44 10 9d b4 20 b5 fe 1b 8b e4 d0 c5 6e 01 9c 9d 2e 43 84 bf 35 39 08 66 12 d5 93 e5 95 0c 6d 2f Data Ascii: "K2:4'c~q?s`YL?Occn@8iAf::2+#CgWGx%ZYRa/xiX=L=lJ!ys(+bbx%h Hs>_;QfznR1U&wXLEz_(l+[2WW4 PSD n.C59fm/
2022-10-03 14:16:36 UTC	10937	IN	Data Raw: bf 3c 8d dc d5 69 59 b9 fc 04 2b 1d 1e 36 a5 62 1b b4 4d 2d ee 62 a5 21 b9 a5 2c f7 79 3b 36 67 7f 40 18 c5 0e 98 b1 2a fa b6 08 89 2b c5 5a 92 fa 71 42 b1 e5 ee 7e 9d 73 d9 1e e6 90 59 e4 b9 6b 51 22 b3 32 f2 68 f1 f2 37 a3 7d 77 20 d2 43 83 fc d9 2f d3 63 1b fe a7 1b eb 93 07 86 8b 23 f6 ad 8f fc 39 32 32 03 f9 07 3a 21 5d 7a 3b 8a c2 d2 02 48 25 4d ae 2e 94 cf eb a2 1a d6 3a fe 5e 46 a7 4e 18 2e 34 76 63 e9 39 26 8f 87 e3 8c 6e 46 43 7d 1b 62 45 2a dc da 7a 93 c6 ca 41 ce 9b 52 bc 4a aa b7 9b 1c 5d 3b 83 b9 e0 54 7e ab e0 e7 ab 04 2c ce b2 45 d0 a0 c5 7e c1 39 04 e7 db 64 1e 4e 53 2f 60 fc 07 46 af 2b 5a 6b 55 27 48 ac 50 e7 fa 97 a6 2c 7c 34 e1 a4 83 88 ea ce 0b 98 29 14 53 35 5b 0c ce 92 a0 20 83 6a 84 52 48 25 84 bd 5b 26 e4 d5 75 fa c5 3b 55 4b a8 Data Ascii: <iY+6bM-b!,y;6g@*+ZqB~sYkQ"2h7}w C/c#922:!]z;H%M.:^FN.4vc9&nFC}bE*zARJ];T~,E~9dNS/`F+ZkU 'HP,|4)S5[jRH%[&u;UK
2022-10-03 14:16:36 UTC	10953	IN	Data Raw: 87 db 09 1d c7 17 f0 c1 9f e7 38 3e 91 8f 9f 89 c4 f7 4c 1e cb 8d ef 26 7e 39 fe 7d e0 fa 62 c2 46 9f 3c 80 e3 59 bd c8 3c e2 ff 00 97 34 7b 46 1f 66 c7 ff 00 36 31 07 d4 f3 9d c3 67 c8 c0 47 74 7e 71 7d a1 c4 23 71 64 7e cb f2 9c ec 72 ab a8 db 0c 72 1e ed 44 d8 d1 4b f3 fd d1 c9 20 95 bd 42 13 1e 19 07 ad e0 61 42 de a0 25 46 32 f7 99 3e f1 71 ca b7 ab b9 90 63 fa 5a 93 56 13 1f e1 8f 7e ec 0c 66 a7 dc fb 9c 9c f5 a9 7e 2e d8 d6 68 7c de 1c e1 b7 4c 16 d4 4c 70 5e ac 3c 0a f9 fa c6 30 7c 40 b9 fa c8 8f 68 93 3f 59 4a 06 82 45 83 92 b1 b5 3a 8f 0f 25 68 ff 00 99 46 1b d6 cf 8f 57 0d eb 47 fd 66 c3 72 c7 fd d7 c3 62 73 ef 2b 61 96 5f fb 8d 9d ef f8 b3 66 db ed f4 d8 e7 a4 d9 e9 1d 7b 1c 5a ed da 0f 9c 75 28 dd bb 18 96 66 88 ed 24 65 35 ba 8b 93 af ad 4c Data Ascii: 8>L&~9}bF<Y<4{Ff61gGt~q}#qd~rrDK BaB%F2>qcZV~f~.h|LLp^<0|@h?YJE:%hFWGfrbs+a_f{Zu(f$e5L
2022-10-03 14:16:36 UTC	11065	IN	Data Raw: 5b b9 b6 80 0d 3f 83 24 7e 47 78 c5 74 50 74 3c 52 ba e7 d4 13 4c 44 31 a5 54 86 26 13 46 f1 72 15 ae 41 3c 4b 2e da 3a 10 72 73 24 91 d2 89 5a 26 90 c3 f2 47 31 2b 14 75 ae 4d 12 f7 fa 69 3b 76 4b 2c 29 29 95 19 13 d3 67 54 db 3c 2c 17 50 ca ee 38 7b 0f 04 28 82 ca cf 0b 5f 45 6a a6 b4 60 4c f2 46 b6 bd 3b 8a 12 62 55 25 96 ec 8e b0 94 3c 7f 1d 2c d3 fc 23 b4 a8 c9 7c cc 5a 92 6f 98 e9 ce 4b d3 7b 5f 13 f1 31 cd c3 ac 48 2c 89 96 6a fc 8c 37 2c 1a b1 76 17 10 46 f5 27 90 4b 53 bc b8 8a 74 f5 3d 52 25 78 2b 34 09 2f ab eb c9 c7 f1 a2 dc be 93 5b 4a e6 a7 00 8f 2e a4 b5 f7 b3 9e 46 32 ed db b5 ab 27 23 ea 77 29 43 21 ad 4a 5a cf 66 f2 48 d6 63 e5 62 58 24 8c 44 d1 c1 31 e5 ab 2f ae cc 7b 69 7c 7f ac 2c 89 e3 73 ca d9 8a 6e 3b 8f 85 2c c9 dc 62 27 61 5b b7 Data Ascii: [?$~GxtPt<RLD1T&FrA<K.:rs$Z&G1+uMi;vK,))gT<,P8{(_Ej`LF;bU%<,#|ZoK{_1H,j7,vF'KSt=R%x+4/[J .F2'#w)C!JZfHcbX$D1/{i|,sn;,b'a[
2022-10-03 14:16:36 UTC	11081	IN	Data Raw: 82 e9 e3 34 78 a9 d3 15 33 28 b0 35 28 01 75 7e 2e 87 d9 84 0f 00 87 73 07 85 40 ce 3d 20 bd 13 a5 38 2a 18 26 41 1a 2b e3 56 f5 a9 54 19 06 5f e6 9f fc bf 4a 5c 97 a4 8d cb 0d 9e 0b 9e 93 44 0f 1c 1e 34 d7 04 b1 98 3a 84 61 9e 57 06 5a c5 90 e2 53 e7 3f ce a3 f7 58 c2 e2 93 0e f4 3b 7f 67 ed 9f eb 13 c4 5b c3 0e 4d d2 0e d1 b5 6e 06 70 e1 07 ad c2 6e f0 ea 7d 2d d7 8f a0 da 6e cd 07 78 74 7d be 26 20 b0 a4 4d b0 81 c0 c1 ea e8 44 1a 3e e3 f7 1b 7e f0 e9 c6 53 4b d2 a4 e2 ef 56 76 ab 48 df 60 62 9b be 21 62 9c ed 3f 39 fe 5a 9d 3d e8 3c 2a 99 2a f5 81 7c e5 ac 6a 18 4f 7a a4 b8 9f 8a 1f a5 67 68 25 d6 60 13 b2 9d 9b 7d e5 da 76 a6 62 13 b4 5f a4 1d 25 85 5e 8c a2 d5 53 f9 d0 e7 f2 b4 7b 85 6e 2c 32 2a 78 30 3a ca 4d 8a 8d 54 36 7a 2d b9 58 c8 3b 1e 98 a3 Data Ascii: 4x3(5(u~.s@= 8*&A+VT_J\D4:aWZS?X;g[Mnpn}-nxt}& MD>~SKVvH`b!b?9Z=<**|jOzgh%`}vb_%^S{n,2*x 0:MT6z-X;
2022-10-03 14:16:36 UTC	11097	IN	Data Raw: 8b 25 f5 73 e3 37 ec 87 70 f9 a8 b4 c3 31 ce ce 94 b4 ec 68 fd 5e 76 8b 07 49 f0 b8 ee 1f 39 ea 93 9a 1f 75 b2 87 a1 93 71 09 06 c6 1e 92 c5 91 b7 0c aa 25 44 07 06 c9 72 73 59 50 5c 11 93 fd ef 14 66 ba 32 f9 88 da db 46 b7 19 c3 8f 55 b5 87 f7 58 8f 57 6e 3e ab 3b 0a bf 53 33 ea ac 18 11 b2 31 16 9f 8a 5f 88 2d d7 79 81 be 91 a9 ff 00 fe 49 9f e9 32 f0 e5 f3 ca 2b 25 15 ff 00 4a a9 87 a4 25 e5 e0 8d ab 01 9c 2e ac 4c bb cc 7a f5 0d 49 12 d9 70 10 66 58 69 30 83 6e a3 98 22 0a 4c 0e 13 9d ce 99 41 43 7c 8e b1 08 0c 3e f1 85 f3 9a 90 20 d2 72 ea e2 2c 0c e0 eb 71 06 ae b7 84 2d ae 22 74 a7 37 f3 0b 15 5f d0 bc be c6 d0 9b 59 89 30 d5 2a 96 e4 04 a9 4f 10 bf 22 65 fd 58 2a be 67 79 8e 76 f3 b6 12 eb 3b 15 9d 91 9d ff 00 bc ed a7 38 bd ad aa 54 5b 52 6b d4 Data Ascii: %s7p1h^vI9uq%DrsYP\f2FUXWn>;S31_-yI2+%J%.LzIpfXi0n"LAC|> r,q-"t7_Y0*O"eX*gyv;8T[Rk
2022-10-03 14:16:36 UTC	11113	IN	Data Raw: 8d 72 24 ca a6 cc db 60 b6 d1 2a 92 c2 fa ad f5 39 4e 93 76 46 6c b0 93 9e 5c 63 a1 55 e8 ea 2c 41 5f 58 9c e5 44 01 31 69 7e 0b 1b 26 0d a0 b6 77 10 2d c3 d3 97 fd 88 de c3 63 30 96 3c de fb 41 dd 56 3e 13 17 05 31 63 98 73 2c c2 99 55 ee 04 3a c5 b9 0c e6 c7 bd bc 0e e2 ed dd b3 65 df b4 a6 6f 59 ea 1d 78 01 2b 1c 35 15 ce 40 ae a0 1b 0d 6f 00 5e fb 64 58 08 c8 0a 81 eb 8d 84 09 85 1c 7a ed c2 36 c0 7e 62 5f c4 c2 06 19 da 2d 5b b5 48 46 65 b4 b8 95 19 45 97 c3 6b c7 c5 76 e0 08 b5 e5 2a c1 4b ec c3 29 50 14 a5 48 7e af 28 ca b4 c7 10 0b 1b 9f ce 52 0c 98 ce ea 49 b9 97 b0 23 52 0c 73 81 0f b0 e4 e4 0c 03 bc 36 37 80 dc 12 db 09 55 40 b0 dc a8 89 5b 13 02 3c 24 6a 04 6c 66 a9 7d cd cd ad 0a 78 81 f1 38 37 59 42 ea 78 b1 83 ba aa 75 37 36 94 90 f6 80 66 Data Ascii: r$`*9NvFl\cU,A_XD1i~&w-c0<AV>1cs,U:eoYx+5@o^dXz6~b_-[HFeEkv*K)PH~(RI#Rs67U@[<$jIf}x87YBxu76f
2022-10-03 14:16:36 UTC	11129	IN	Data Raw: f3 1e bc 0b 89 8f 3e a3 f7 91 f1 85 7b c6 84 2d b5 6d 8f 36 f2 46 86 89 24 bb 08 99 6e c9 2f a9 eb 38 5a ec 5d 0e e0 b4 17 90 fb 47 43 1e 5d 05 86 bc 6f 21 dc f0 42 cd 31 53 b8 ff 00 24 3b 96 e1 a0 b5 33 22 ea ce e4 78 f5 13 4e 2e 9b 25 6d bc 84 f2 89 ff 00 90 76 df 64 f3 5a 60 f2 e3 d7 06 86 bc c6 de 08 bb 34 e1 44 a9 b9 52 1b 4a 85 66 48 83 93 7d 09 56 6a 90 b4 db 46 3f 22 2d a7 05 77 9f 21 d3 a1 ad d3 42 39 9a 2e 3c 85 4f 93 43 6e 17 6a c8 dc ea 88 e4 3b 54 b5 e1 6b 85 e0 d8 ad 3d 07 4d 8e f8 18 ef c0 d3 81 70 a1 a6 2b 90 ff 00 dc 8b f9 58 bd 25 0b ff 00 02 ba 65 c2 1d 45 f9 92 aa b2 4d 5b 54 97 41 5d ed 63 21 7e a3 86 43 d7 a6 66 50 ea f2 2d c9 f4 59 0b 2e c9 2a 5a 1c 88 69 c0 f0 75 42 cb 17 c1 14 ec 6d 32 a4 65 2e 68 92 35 a1 f6 7f 45 a9 24 e5 c9 27 Data Ascii: >{-m6F$n/8Z]GC]o!B1S$;3"xN.%mvdZ`4DRJfH}VjF?"-w!B9.<OCnj;Tk=Mp+X%eEM[TA]c!~CfP-Y.*ZiuBm2 e.h5E$'

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.6	49936	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:34 UTC	10807	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_mov.mp4 HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" Accept-Encoding: identity;q=1, *;q=0 sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: video Referer: https://kawanakajima.co.jp/ Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942; _gat_gtag_UA_63283810_1=1 Range: bytes=5683200-5683456 If-Range: "56b901-5b44268a46a00"
2022-10-03 14:16:35 UTC	10808	IN	HTTP/1.1 206 Partial Content Date: Mon, 03 Oct 2022 14:16:35 GMT Server: Apache Last-Modified: Tue, 17 Nov 2020 00:16:40 GMT ETag: "56b901-5b44268a46a00" Accept-Ranges: bytes Content-Length: 257 Content-Range: bytes 5683200-5683456/5683457 Connection: close Content-Type: video/mp4
2022-10-03 14:16:35 UTC	10808	IN	Data Raw: 5b 00 55 9d 6a 00 55 a1 d6 00 55 b3 5b 00 55 c3 5b 00 55 c9 25 00 55 cd 7e 00 55 da cd 00 55 eb 4a 00 55 ee fd 00 55 f5 19 00 56 07 61 00 56 0b 7f 00 56 0f 52 00 56 14 6b 00 56 16 8f 00 56 1e 36 00 56 22 5b 00 56 24 81 00 56 28 9e 00 56 2a c2 00 56 2e e7 00 56 31 0d 00 56 35 2a 00 56 39 47 00 56 3b 8c 00 56 3f a9 00 00 00 1a 73 67 70 64 01 00 00 00 72 6f 6c 6c 00 00 00 02 00 00 00 01 ff ff 00 00 00 1c 73 62 67 70 00 00 00 00 72 6f 6c 6c 00 00 00 01 00 00 05 91 00 00 00 01 00 00 00 62 75 64 74 61 00 00 00 5a 6d 65 74 61 00 00 00 00 00 00 00 21 68 64 6c 72 00 00 00 00 00 00 00 00 6d 64 69 72 61 70 70 6c 00 00 00 00 00 00 00 00 00 00 00 00 2d 69 6c 73 74 00 00 00 25 a9 74 6f 6f 00 00 00 1d 64 61 74 61 00 00 00 01 00 00 00 00 4c 61 76 66 35 38 2e 34 34 2e 31 Data Ascii: [UjUU[U[U%U~UUJUUVaVVRVkVV6V"[V$V(V*V.V1V5*V9GV;V?sgpdrollsbgprollbudtaZmeta!hdlrmdirappl-ilst%toodataLavf58.44.1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.6	49940	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:37 UTC	11424	OUT	GET /wordpress/wp-content/themes/kawaken/images/business_img_04.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp
2022-10-03 14:16:37 UTC	11424	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:37 GMT Server: Apache Last-Modified: Fri, 23 Oct 2020 09:07:09 GMT ETag: "d4da-5b252e7c40940" Accept-Ranges: bytes Content-Length: 54490 Connection: close Content-Type: image/jpeg
2022-10-03 14:16:37 UTC	11424	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 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 04 74 03 84 03 01 22 00 02 11 01 03 11 01 ff c4 00 1c 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 ff da 00 08 01 01 00 00 00 00 f6 54 b6 c9 03 1b 06 c6 0c 6c 01 b1 80 30 18 c1 0c 00 00 00 04 00 00 08 04 02 01 08 00 04 20 00 04 21 67 a5 8d 8d 8d b6 31 92 Data Ascii: JFIF"#*" "*#>1++1>H<9<HWNNWmhm"#*" "*#>1++1>H<9<HWNNWmhmt"Tl0 !g1
2022-10-03 14:16:37 UTC	11440	IN	Data Raw: 68 51 a1 c6 28 da 50 a1 42 af a8 50 e1 6a 7a 4f 95 a0 27 12 51 a2 26 3c 1a 3c 64 38 1c 6b 81 f0 f5 e3 88 d1 34 45 22 8a 32 28 7c 6b e0 73 ae 05 1a d0 ad 8f 83 f0 47 07 e2 7a b9 e0 d6 85 5d 33 dd 4c 52 a4 9d e4 81 5d 3f 32 c3 76 67 a8 29 c1 06 98 75 22 8d 0a 3c 0a c4 d5 a7 22 af e8 50 e1 6a 7a 4f 95 a1 57 15 25 1a 6a 9a 8f 06 8f 19 0e 07 c0 e0 1e 1a bc 59 1a 26 88 c0 b0 2d 01 43 86 a0 35 ad 00 78 ee 65 f6 89 1a 51 70 5d ee 61 9c 8f e4 7e 27 ab 8f 81 59 01 2d 76 f6 fb 4b 24 cf 73 04 8c d7 66 6a 82 9e 8d 10 c3 4c 34 40 a6 e0 1c 4d 5a d0 a1 42 af a8 50 e1 6a 7a 4f 95 a0 2e 04 9c 35 4d 47 83 44 d6 43 81 f0 28 72 28 d7 89 23 45 e9 16 d2 5b d2 d0 a3 46 e1 ef 06 40 4c 27 f7 89 cd c9 bb fd 7f a8 dd 35 cf bc b4 88 96 76 96 c3 e0 fc 1e 4f c4 f5 71 c8 e2 e8 35 ab 59 Data Ascii: hQ(PBPjzO'Q&<<d8k4E"2(|ksGz]3LR]?2vg)u"<"PjzOW%jY&-C5xeQp]a~'Y-vK$sfjL4@MZBPjzO.5MGDC(r(#E[F@L'5vOq5Y

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:38 UTC	11456	IN	Data Raw: 36 7b 1b 4f d5 a5 4e e4 1c ac 2f 47 11 5b 46 a4 75 89 55 aa 6c a4 59 12 93 56 2a d2 dc 57 ab 2c f7 12 a2 8f 48 f5 9e 84 93 1b 65 38 d1 b3 65 29 e2 d2 44 a3 46 29 18 69 a9 3a 8c c3 df 61 e4 51 95 27 18 fb 46 2e 94 3d 24 53 31 ea 7b 6e 56 bf 32 7a 91 cd 92 8c d6 ab 36 14 e6 61 95 65 15 21 4a 37 5a 2e 77 91 36 17 43 27 d0 fe ad 3f 99 1e 16 8f cb 1f 23 24 64 6d 17 89 de b3 65 19 96 42 65 a4 5e 12 e8 78 c7 d4 ee 3f 63 c7 c7 a9 9a e9 eb fb 89 f4 36 e5 d5 f6 5e ab e8 6c be c3 43 1e 86 78 bc 57 ea cf cf b4 d0 d9 78 58 69 8c ee 99 df 7e e7 75 72 f8 a4 5e 76 36 57 62 f3 7e ae d4 19 2f 4b b9 90 95 28 a1 19 89 50 68 5a d7 65 a5 72 31 8e 6c 53 62 b9 61 32 cb 2d 19 3d 1a d2 d5 23 46 b2 90 e7 08 ab 8d 64 87 1a 72 d6 de 6b 63 62 a7 b8 c3 7d c6 2d 5b 7f fe cf b3 de 1a 29 Data Ascii: 6{ON/G[FuUlYV*W,He8e)DF)i:aQ'F.=$S1{nV2z6ae!J7Z.w6C'?#$dmeBe^x?c6^lCxWxXi~ur^v6Wb~/K(PhZ er1lSba2-=#Fdrkcb}-[)
2022-10-03 14:16:38 UTC	11472	IN	Data Raw: 41 5a 25 d9 3e 09 f0 74 dd b8 9c 10 ed a4 7e 25 c7 ec fc 7e cd 8d bb eb 77 fe c9 27 65 1d 3f ea 32 5f ac c6 d5 22 18 38 72 5b a1 74 50 97 06 27 46 d3 74 cf 42 48 71 6b 91 50 b9 34 b1 45 8a 2d 8a 06 82 0a a1 da 84 62 b2 9d 98 7b 44 7c f6 4b 82 67 4b e4 de b3 46 20 b3 66 33 92 8e c7 ad 8a 7a 93 7f c8 d5 7e 45 26 b7 52 16 24 ff 00 c8 f5 a5 1f 36 2e a1 fd 0b 1d 0b 1a 27 a9 16 29 44 b4 37 bb 2f 71 b3 a7 fd 46 4b f5 99 f4 61 a5 a4 82 db 92 56 24 8e ad 28 b5 42 5f 8a 21 f2 42 4a b3 57 94 7e 3d ed 26 68 42 54 3e c9 70 48 e9 76 6c d5 b1 65 89 98 9c 8b 24 58 d5 8e 09 f8 1e 06 1b 1f 4d 01 f4 bf 47 a1 21 e1 4a 23 52 fa 37 ca d9 aa 46 b9 0f 97 93 3a 7f 9b 24 ef 15 8b 94 43 e2 84 da 1b b9 0a 8e bf 98 88 87 cc d3 b2 34 e6 8f e3 da bb 18 fb 24 48 c1 91 a8 53 46 a4 6c 62 Data Ascii: AZ%>t~%~w'e?2_"8r[tP'FtBHqkP4E-b{D|KgKF f3z~E&R$6.')D7/qFKaV$(B_!BJW~=&hBT>pHvle$XMG!J#R 7F:$C4$HSFlb

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.6	49944	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:49 UTC	11478	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_img_sp.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:11 GMT If-None-Match: "16c87-5b252e7e28dc0"
2022-10-03 14:16:50 UTC	11479	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:50 GMT Server: Apache Connection: close ETag: "16c87-5b252e7e28dc0"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.6	49943	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:49 UTC	11478	OUT	GET /wordpress/wp-content/themes/kawaken/images/logo.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:10 GMT If-None-Match: "621a-5b252e7d34b80"
2022-10-03 14:16:50 UTC	11479	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:50 GMT Server: Apache Connection: close ETag: "621a-5b252e7d34b80"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.6	49937	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:50 UTC	11478	OUT	GET /news/ HTTP/1.1 Host: kawanakajima.co.jp Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: _ga=GA1.3.189789998.1664838942; _gid=GA1.3.1735943631.1664838942
2022-10-03 14:16:52 UTC	11480	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:16:50 GMT Server: Apache X-Powered-By: PHP/7.4.5 Link: <https://kawanakajima.co.jp/wp-json/>; rel="https://api.w.org/" Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-10-03 14:16:52 UTC	11480	IN	Data Raw: 38 34 32 65 0d 0a Data Ascii: 842e
2022-10-03 14:16:52 UTC	11480	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 37 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 73 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 69 65 20 69 65 38 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 6a 61 22 0a 09 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 73 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 20 3e 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 21 28 49 45 20 37 29 20 7c 20 21 28 49 45 20 38 29 20 5d 3e 3c 21 2d Data Ascii: <!DOCTYPE html>...[if IE 7]><html class="ie ie7" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if IE 8]><html class="ie ie8" dir="ltr" lang="ja"prefix="og: https://ogp.me/ns#" ><![endif]-->...[if !(IE 7) | !(IE 8)]><!-
2022-10-03 14:16:52 UTC	11488	IN	Data Raw: 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 74 29 7d 66 6f 72 28 6f 3d 41 72 72 61 79 28 22 66 6c 61 67 22 2c 22 65 6d 6f 6a 69 22 29 2c 74 2e 73 75 70 70 6f 72 74 73 3d 7b 65 76 65 72 79 74 68 69 6e 67 3a 21 30 2c 65 76 65 72 79 74 68 69 6e 67 45 78 63 65 70 74 46 6c 61 67 3a 21 30 7d 2c 72 3d 30 3b 72 3c 6f 2e 6c 65 6e 67 74 68 3b 72 2b 2b 29 74 2e 73 75 70 70 6f 72 74 73 5b 6f 5b 72 5d 5d 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 70 7c 7c 21 70 2e 66 69 6c 6c 54 65 78 74 29 72 65 74 75 72 6e 21 31 3b 73 77 69 74 63 68 28 70 2e 74 65 78 74 42 61 73 65 6c 69 6e 65 3d 22 74 6f 70 22 2c 70 2e 66 6f 6e 74 3d 22 36 30 30 20 33 32 70 78 20 41 72 69 61 6c 22 2c 65 29 Data Ascii: etElementsByTagName("head")[0].appendChild(t)}for(o=Array("flag","emoji"),t.supports={everything:!0,everythingExceptFlag:!0},r=0;r<o.length;r++)t.supports[o[r]]=function(e){if(!p||p.fillText)return!1;switch(p.textBaseline="top",p.font="600 32px Arial",e)
2022-10-03 14:16:52 UTC	11496	IN	Data Raw: 6d 65 6e 75 3c 2f 70 3e 3c 2f 61 3e 0a 3c 2f 68 65 61 64 65 72 3e 0a 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 5f 69 6d 67 22 3e 0a 09 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 6f 72 64 70 72 65 73 73 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 6b 61 77 61 6b 65 6e 2f 69 6d 61 67 65 73 2f 6c 6f 77 5f 6d 61 69 6e 5f 69 6d 67 5f 74 6f 70 69 63 73 2e 6a 70 67 22 20 61 6c 74 3d 22 e3 83 88 e3 83 94 e3 83 83 e3 82 af e3 82 b9 22 20 63 6c 61 73 73 3d 22 70 63 22 3e 0a 09 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 6f 72 64 70 72 65 73 73 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 6b 61 Data Ascii: menu</p></header> <img src="https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/low_main_img_topics.jpg" alt="" class="pc"><img src="https://kawanakajima.co.jp/wordpress/wp-content/themes/ka
2022-10-03 14:16:52 UTC	11504	IN	Data Raw: 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 61 74 65 67 6f 72 79 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 e3 82 ab e3 83 86 e3 82 b4 e3 83 aa e5 87 ba e5 8a 9b 73 74 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 e3 83 88 e3 83 94 e3 83 83 e3 82 af e3 82 b9 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 e3 82 ab e3 83 86 e3 82 b4 e3 83 aa e5 87 ba e5 8a 9b 73 74 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 78 74 5f 77 72 61 70 22 3e 44 4b e3 83 9c e3 83 b3 e3 83 89 e5 b7 a5 e6 b3 95 e3 Data Ascii: ... st --> ... st --> DK
2022-10-03 14:16:52 UTC	11511	IN	Data Raw: 0a 09 09 09 09 09 09 3c 6c 69 3e 0a 09 09 09 09 09 09 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 6e 61 67 61 6e 6f 2d 72 6f 61 64 2f 22 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 6f 72 64 70 72 65 73 73 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 74 68 65 6d 65 73 2f 6b 61 77 61 6b 65 6e 2f 69 6d 61 67 65 73 2f 66 6f 6f 74 65 72 5f 62 61 6e 6e 65 72 5f 6e 61 67 61 6e 6f 72 6f 61 64 2e 6a 70 67 22 20 61 6c 74 3d 22 6e 61 67 61 6e 6f 20 72 6f 61 64 22 3e 3c 2f 61 3e 0a 09 09 09 09 09 09 3c 2f 6c 69 3e 0a 09 09 09 09 09 09 3c 2f 75 6c 3e 0a 09 09 09 09 09 09 3c 75 6c 20 63 6c 61 73 73 3d 22 6c 69 73 74 5f 66 5f 73 6e 73 5f 69 63 6f Data Ascii: <img src="https://kawanakajima.co.jp/wordpress/wp-content/themes/kawaken/images/footer_banner_naganoroad.jpg" alt="nagano road"> <ul class="list_f_sns_ico
2022-10-03 14:16:52 UTC	11513	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:16:52 UTC	11513	IN	Data Raw: 61 33 0d 0a Data Ascii: a3

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:52 UTC	11513	IN	Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 68 74 74 70 73 3a 2f 2f 6b 61 77 61 6e 61 6b 61 6a 69 6d 61 2e 63 6f 2e 6a 70 2f 77 70 2d 69 6e 63 6c 75 64 65 73 2f 6a 73 2f 77 70 2d 65 6d 62 65 64 2e 6d 69 6e 2e 6a 73 3f 76 65 72 3d 35 2e 34 2e 31 31 27 20 64 65 66 65 72 20 63 68 61 72 73 65 74 3d 27 55 54 46 2d 38 27 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <script type='text/javascript' src='https://kawanakajima.co.jp/wordpress/wp-includes/js/wp-embed.min.js?ver=5.4.11' defer charset='UTF-8'></script></body></html>
2022-10-03 14:16:52 UTC	11513	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:16:52 UTC	11513	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.6	49946	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:51 UTC	11479	OUT	GET /wordpress/wp-content/themes/kawaken/images/main_ttl.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:11 GMT If-None-Match: "160fb-5b252e7e28dc0"
2022-10-03 14:16:51 UTC	11480	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:51 GMT Server: Apache Connection: close ETag: "160fb-5b252e7e28dc0"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.6	49948	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:51 UTC	11479	OUT	GET /wordpress/wp-content/themes/kawaken/images/scrolldown.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:11 GMT If-None-Match: "c3a-5b252e7e28dc0"
2022-10-03 14:16:51 UTC	11480	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:51 GMT Server: Apache Connection: close ETag: "c3a-5b252e7e28dc0"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.6	49957	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

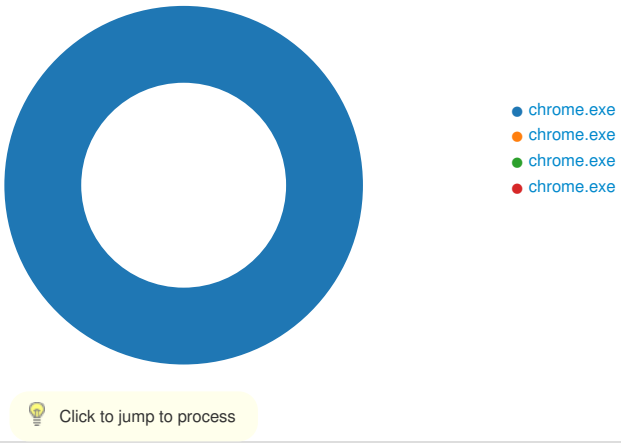
Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:55 UTC	11513	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_top_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:08 GMT If-None-Match: "f2fc-5b252e7b4c700"
2022-10-03 14:16:55 UTC	11514	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:55 GMT Server: Apache Connection: close ETag: "f2fc-5b252e7b4c700"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.6	49956	210.190.150.55	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:16:55 UTC	11514	OUT	GET /wordpress/wp-content/themes/kawaken/images/about_company_img_01.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: kawanakajima.co.jp If-Modified-Since: Fri, 23 Oct 2020 09:07:08 GMT If-None-Match: "1344f-5b252e7b4c700"
2022-10-03 14:16:55 UTC	11514	IN	HTTP/1.1 304 Not Modified Date: Mon, 03 Oct 2022 14:16:55 GMT Server: Apache Connection: close ETag: "1344f-5b252e7b4c700"

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5176**, Parent PID: **4544**

General

Target ID:	0
Start time:	16:15:20
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5228**, Parent PID: **5176**

General

Target ID:	1
Start time:	16:15:21
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1844 --field-trial-handle=1712,i,10524100664618611924,16229694031488129540,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4248**, Parent PID: **4544**

General

Target ID:	2
Start time:	16:15:22
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://kawanakajima.co.jp/collinesredshare666.htm
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: chrome.exe PID: **6920**, Parent PID: **5176**

General

Target ID:	12
Start time:	16:16:21
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=4300 --field-trial-handle=1712,i,10524100664618611924,16229694031488129540,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly