

JOESandbox Cloud BASIC



ID: 509788

Cookbook: browseurl.jbs

Time: 22:15:50

Date: 26/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report	
https://docs.google.com/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo/edit?usp=sharing_eip_m&rtpof=true&sd=true&invite=CKvaqcMD&ts=6178419e	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Phishing:	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	7
URLs	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
Private	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	40
No static file info	40
Network Behavior	40
Network Port Distribution	40
TCP Packets	40
UDP Packets	40
DNS Queries	40
DNS Answers	41
HTTP Request Dependency Graph	43
HTTPS Proxied Packets	43
Code Manipulations	84
Statistics	84
Behavior	84
System Behavior	84
Analysis Process: chrome.exe PID: 6564 Parent PID: 476	84
General	84
File Activities	84
Registry Activities	84
Key Value Modified	85
Analysis Process: chrome.exe PID: 6752 Parent PID: 6564	85
General	85
File Activities	85
Disassembly	85
Code Analysis	85

Windows Analysis Report <https://docs.google.com/docu...>

Overview

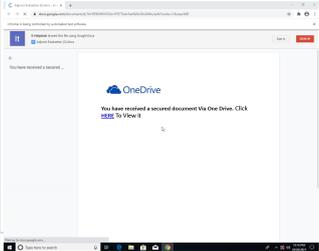
General Information

Sample URL: https://docs.google.com/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo/edit?usp=sharing_eip_m&rtpof=true&sd=true&invite=CKvaqcMD&ts=6178419e

Analysis ID: 509788

Infos:    

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

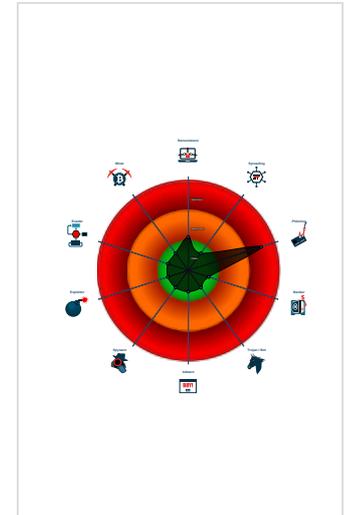
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav...)
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Phishing site detected (based on log...)
- No HTML title found
- HTML body contains low number of ...
- Invalid T&C link found
- Suspicious form URL found

Classification



Process Tree

- System is w10x64
-  **chrome.exe** (PID: 6564 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://docs.google.com/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo/edit?usp=sharing_eip_m&rtpof=true&sd=true&invite=CKvaqcMD&ts=6178419e' MD5: C139654B5C1438A95B321BB01AD63EF6)
 -  **chrome.exe** (PID: 6752 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,8177781781073637063,12308943224005517833,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1912 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Phishing:



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

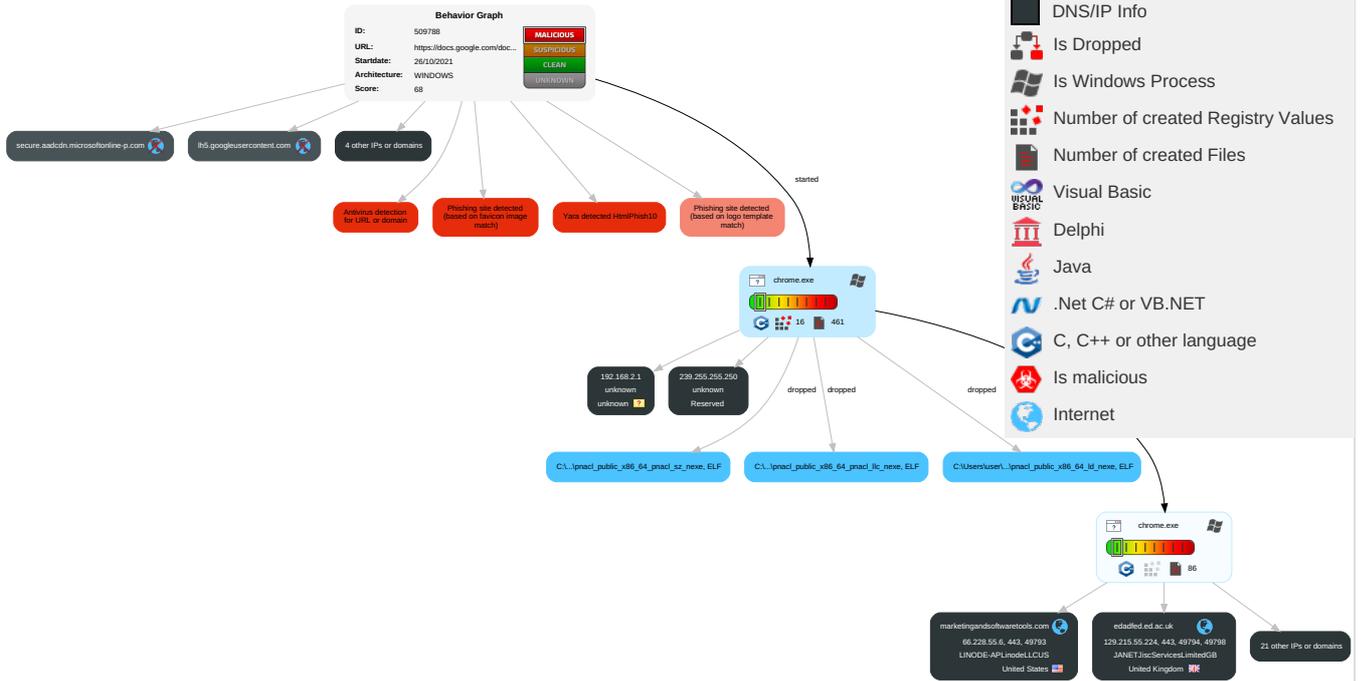
Mitre Att&ck Matrix

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

Behavior Graph

Legend:

-  Process
-  Signature
-  Created File
-  DNS/IP Info
-  Is Dropped
-  Is Windows Process
-  Number of created Registry Values
-  Number of created Files
-  Visual Basic
-  Delphi
-  Java
-  .Net C# or VB.NET
-  C, C++ or other language
-  Is malicious
-  Internet

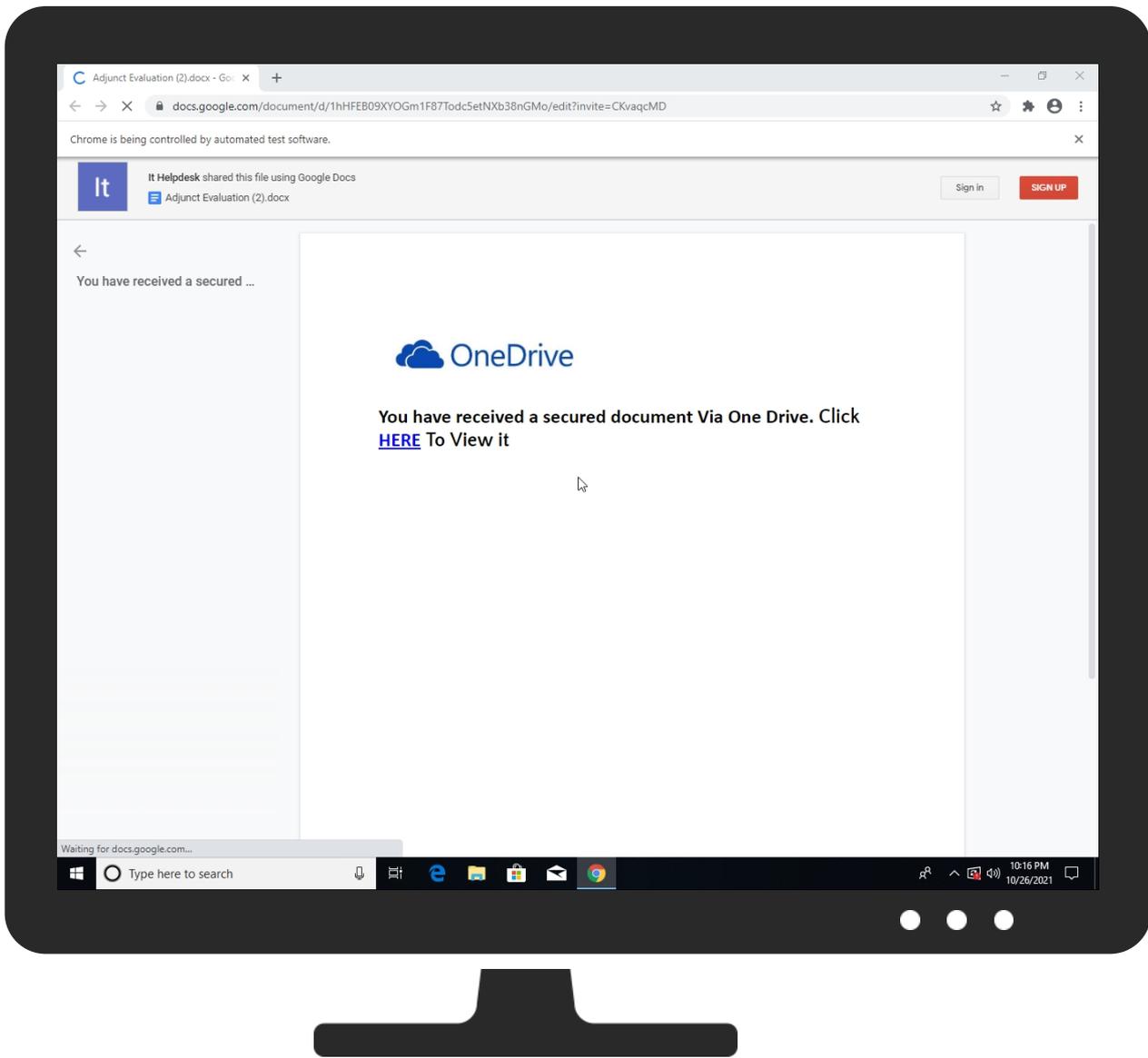


Screenshots

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://docs.google.com/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo/edit?usp=sharing_eip_m&rtopf=true&sd=true&invite=CKvaqcMD&ts=6178419e	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6564_637119584\platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://csp.withgoogle.com/csp/report-to/docs_	0%	Avira URL Cloud	safe	
http://https://edadfed.ed.ac.uk/adfs/portal/illustration/illustration.jpgl-	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/apps-themes	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/docs	0%	Virustotal		Browse
http://https://csp.withgoogle.com/csp/report-to/docs	0%	Avira URL Cloud	safe	
http://https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.htmlRefe	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/QqFxbi9M48c.cr10	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/product-feedback-gathering	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-6ybrougjmfqxw910ieyohr7wb4x4-yvoixrlaidmz4/app	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/QOvJON1sT2A.cr10	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/product-feedback-gatheringCross-Origin-Resource-Policy:	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/apps-themesO	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.cr10W	0%	URL Reputation	safe	
http://https://marketingandsoftwaretools.com/	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://edadfed.ed.ac.uk/	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/social-frontend-mpm-access	0%	URL Reputation	safe	
http://crl.pki.goog/gsr1/gsr1.cr10;	0%	URL Reputation	safe	
http://https://edadfed.ed.ac.uk/adfs/portal/illustration/illustration.jpg	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/apps-themesCross-Origin-Resource-Policy:	0%	URL Reputation	safe	
http://https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/365.php	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/docscross-origin-resource-policy:cross-origincross-origin-opener-poli	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/docs	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/zdATt0Ex_Fk.cr10	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.cr10	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/apps-themescross-origin-resource-policy:cross-origincross-origin-open	0%	URL Reputation	safe	
http://https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html3	0%	Avira URL Cloud	safe	
http://https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.htmlSign	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/social-frontend-mpm-access	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.35	true	false		high
docs.google.com	172.217.168.78	true	false		high
accounts.google.com	172.217.168.13	true	false		high
plus.l.google.com	142.250.203.110	true	false		high
marketingandsoftwaretools.com	66.228.55.6	true	false		unknown
play.google.com	172.217.168.14	true	false		high
browserchannel-sites.l.google.com	74.125.143.189	true	false		high
fc6y67oygyo8.wpeproxy.com	141.193.213.21	true	false		unknown
bit.ly	67.199.248.11	true	false		high
clients.l.google.com	142.250.185.206	true	false		high
people-pa.clients6.google.com	172.217.168.10	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
edadfed.ed.ac.uk	129.215.55.224	true	false		unknown
lh3.googleusercontent.com	unknown	unknown	false		high
0.docs.google.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
lh5.googleusercontent.com	unknown	unknown	false		high
contacts.google.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown
apis.google.com	unknown	unknown	false		high
lh4.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://docs.google.com/document/d/1hHFEB09XYOGm1F87T0dc5etNXb38nGMo/edit?invite=CKvaqcMD	false		high
https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
https://lh3.googleusercontent.com/a/AATXAJyEMzWYioPomGpTeso8L__wKY3bPrTHT3se5MVA=s50-c-k-no	false		high
https://apis.google.com/js/api.js	false		high
https://bit.ly/3me0XGn	false		high
https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegcagldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
https://lh4.googleusercontent.com/-6DRE7a5AcB4/AAAAAAAAAAI/AAAAAAAAAKM/5K1J4UolszQ/s0-c-k-no-ns/photo.jpg	false		high
https://edadfed.ed.ac.uk/adfs/portal/illustration/illustration.jpg	false	• Avira URL Cloud: safe	unknown
https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
129.215.55.224	edadfed.ed.ac.uk	United Kingdom		786	JANETJiscServicesLimitedGB	false
66.228.55.6	marketingandsoftwaretools.com	United States		63949	LINODE-APLinodeLLCUS	false
74.125.143.189	browserchannel-sites.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	plus.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.13	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.35	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.78	docs.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
67.199.248.11	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509788
Start date:	26.10.2021
Start time:	22:15:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://docs.google.com/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMO/edit?usp=sharing_eip_m&rtpof=true&sd=true&invite=CKvaqcMD&ts=6178419e
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@35/257@23/13
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Browse: https://bit.ly/3me0XGn
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBIESBw4p6:NfOCzvRKhGwwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.....6.....".Z..4g....6.2...{...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDXS.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDsgNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d907e79-e240-4ace-a0e8-cf5886bdbcca.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	185872
Entropy (8bit):	6.077082168941572
Encrypted:	false
SSDEEP:	3072:8rdxF5Kc8ps5XPvPwTAfoErslZhVPiszKh17QFcbXafIB0u1GOJmA3iuRI:ldz57AcvPCEllZhBiNjiaqfllUOoSiuu
MD5:	099D283D78922BC8C99F2329C0E7E31A
SHA1:	352FBBE861FB77D7E864E829DEF199F8938E76C3
SHA-256:	164189CF8989ABC8F445C7CA66E38C4DD40856AC473A0A48AA1F1E3A0DAFCBB4
SHA-512:	4B0D0BB911EC3012E93C0E7AF4F9E737CD2BC9BF0FE23986739BB039702E7369CFA6EEA03A035CA4BA91C03B4C3101DA0750DA1D24251066237DF798840A36E
Malicious:	false
Reputation:	low
Preview:	{ "browser": { "last_redirect_origin": "", "shortcut_migration_version": "85.0.4183.121", "data_use_measurement": { "data_used": { "services": { "background": {}, "foreground": {} }, "use_r": { "background": {}, "foreground": {} } }, "hardware_acceleration_mode_previous": true, "intl": { "app_locale": "en", "legacy": { "profile": { "name": { "migrated": true } }, "network_time": { "network_time_mapping": { "local": "1.635311805284615e+12", "network": "1.635279406e+12", "ticks": "132274050.0", "uncertainty": "3963250.0" }, "os_crypt": { "encrypted_key": "RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WK194zTZq03WydZHLcAAAAAIAAAAAABmAAAAQAIAAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppN r2ZbBFie9UAAAAA6AAAAAGAAIAAAABDv4gJLq1dOS7lkrG21YVxojnHhsRhNp8/D1zs78mXMAAAAB0450d5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfjw4oXIE4R7I0AAAAABlt36FqChftM9b7EtaPw98XR5Y944rq1WsgWcOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYpP4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13276832799258787", "plugins": { "metadata": { "adobe-flash-player": { "disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\37470408-1879-4908-9848-7b84876422d9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7471010920667513
Encrypted:	false
SSDEEP:	384:lvHhUZpX8OPsvv4+IENtrexv73CV7+Hv6GOxrcfVhCrDr/SrApm4zcb1FISO//i:NBhK+59CX+Oge7OcD3Q3rG/KxPNB2

C:\Users\user\AppData\Local\Google\Chrome\User Data\37470408-1879-4908-9848-7b84876422d9.tmp

Table with 2 columns: Field Name (MD5, SHA1, SHA-256, SHA-512, Malicious, Reputation, Preview) and Value. Preview shows a partial hex dump of a file.

C:\Users\user\AppData\Local\Google\Chrome\User Data\4aa76b95-007a-4a0a-8c33-217d8793ff03.tmp

Table with 2 columns: Field Name (Process, File Type, Category, Size, Entropy, Encrypted, SSDEEP, MD5, SHA1, SHA-256, SHA-512, Malicious, Reputation, Preview) and Value. Preview shows a JSON object representing browser state.

C:\Users\user\AppData\Local\Google\Chrome\User Data\69f1fb30-d8a3-49fe-838b-ee8259cd1559.tmp

Table with 2 columns: Field Name (Process, File Type, Category, Size, Entropy, Encrypted, SSDEEP, MD5, SHA1, SHA-256, SHA-512, Malicious, Reputation, Preview) and Value. Preview shows a JSON object representing browser state.

C:\Users\user\AppData\Local\Google\Chrome\User Data\7bd5c86a-7b96-47d6-acb4-a27163bab98b.tmp

Table with 2 columns: Field Name (Process, File Type, Category, Size, Entropy, Encrypted, SSDEEP) and Value. Preview is empty.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b5d6b28-abc9-4340-9ff7-41e8f309b77f.tmp

Preview:	<pre>{\"net\":{\"http_server_properties\":{\"servers\":{\"isolation\":[],\"server\":\"https://www.google.com\",\"supports_spdy\":true},\"isolation\":[],\"server\":\"https://ogs.google.com\",\"supports_spdy\":true},\"isolation\":[],\"server\":\"https://www.googleapis.com\",\"supports_spdy\":true},\"isolation\":[],\"server\":\"https://dns.google\",\"supports_spdy\":true},\"alterative_service\":{\"advertised_versions\":{\"expiration\":\"13282377405311650\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"server\":\"https://redirector.gvt1.com\"},\"alternative_service\":{\"advertised_versions\":{\"expiration\":\"13282377405360981\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"server\":\"https://accounts.google.com\",\"supports_spdy\":true},\"alternative_service\":{\"advertised_versions\":{\"expiration\":\"13282377405607589\",\"port\":443,\"protocol_str\":\"quic\"},\"advertised_versions\":{\"expiration\":\"13282377405607592\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"server\":\"https://r4--sn-h0jeln7l.gvt1.com\"},\"alternative_servic</pre>
----------	---

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2c6a0c24-8c93-4014-9329-732aa4582676.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHbKsvxMHVzspxMHbsIH/soBDysKqnsIzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC48472F7F165BBCA3EB2E4DFB0177D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	<pre>{\"net\":{\"http_server_properties\":{\"servers\":{\"alternative_service\":{\"advertised_versions\":{\"expiration\":\"13248543677350473\",\"port\":443,\"protocol_str\":\"quic\"},\"advertised_versions\":{\"expiration\":\"13248543677350474\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"network_stats\":{\"srtt\":31344},\"server\":\"https://dns.google\",\"supports_spdy\":true},\"alternative_service\":{\"advertised_versions\":{\"expiration\":\"13248543501474403\",\"port\":443,\"protocol_str\":\"quic\"},\"advertised_versions\":{\"expiration\":\"13248543501474403\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"network_stats\":{\"srtt\":31656},\"server\":\"https://clients2.googleusercontent.com\",\"supports_spdy\":true},\"alternative_service\":{\"advertised_versions\":{\"expiration\":\"13248543501454993\",\"port\":443,\"protocol_str\":\"quic\"},\"advertised_versions\":{\"expiration\":\"13248543501454994\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"network_stats\":{\"srtt\":39369},\"server\":\"https://www.googleapis.com\",\"supports_spdy\":true},</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3ae53830-345a-498e-8294-eb5615a7a569.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5777008660891205
Encrypted:	false
SSDEEP:	384:FMBtSLiTX+1kXqKf/pUZNCgVLH2HfDprUoRB48:PLIP+1kXqKf/pUZNCgVLH2HftrUSBb
MD5:	F846FBAE3ACAFDE6EC5E3A0490333640
SHA1:	0916D3AD92354C35ADDA9823B489874D7EAEBD34
SHA-256:	AF30BD5F37106E7661C8F2E0CE7BA6F14A2956BC2865A61338C7B2277EED58A
SHA-512:	F77E922788A50B2D8540BBA6895BB5839A32126012914059FF1405282477389A836894516272B578CB1801A7BCAFA451B53F93FEA4B0C456810E34B3C2FC4FB2
Malicious:	false
Reputation:	low
Preview:	<pre>{\"extensions\":{\"settings\":{\"ahfgeienlhkcgomhjhadjkgooble\":{\"active_permissions\":{\"api\":{\"management\",\"system.display\",\"system.storage\",\"webstorePrivate\",\"system.cpu\",\"system.memory\",\"system.network\"},\"manifest_permissions\":[]},\"app_launcher_ordinal\":\"t\",\"commands\":{},\"content_settings\":[],\"creation_flags\":1,\"events\":[],\"from_bookmark\":false,\"from_webstore\":false,\"incognito_content_settings\":[],\"incognito_preferences\":{},\"install_time\":\"13279785403217627\",\"location\":5,\"manifest\":{\"app\":{\"launch\":{\"web_url\":\"https://chrome.google.com/webstore\"},\"urls\":{\"https://chrome.google.com/webstore\"},\"description\":\"Discover great apps, games, extensions and themes for Google Chrome.\"},\"icons\":{\"128\":\"webstore_icon_128.png\",\"16\":\"webstore_icon_16.png\"},\"key\":\"MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQCtI3t00osjuzRsfxtD2SKpITfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLbWLalBPYeXbzIHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB\"},\"name\":\"Web Store\",\"pe</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.234182902702216
Encrypted:	false
SSDEEP:	6:mao8Dq2PWXp+N23iKkKdK9RXXTZIFUtno82F4ZmwBo8AZkwOWXp+N23iKkKdK9RXXH:pXDva5Kk7XT2FUtnX9/BXM5f5Kk7XVJ
MD5:	04F100BC1FC70CD9E2D4EAE39B5E2FB
SHA1:	CBE429B1C8ED4E4A081CE6C005BC7AAA539E55B6
SHA-256:	52841604C612C4B7FB5A8C5EFC1BDC2D1A1E6828A1F18624AE63C2C0E3F70EFA
SHA-512:	D0506F428463DD775D9E85F77AD197C89D4ACE4A6ECC3DB78F5351F0A5D57EAF1B395BE3DD6AD00FDE69F0A34A982401D905084AAA4D663F97430754D999738
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Preview:	2021/10/26-22:16:55.196 1c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/10/26-22:16:55.197 1c90 Recovering log #3.2021/10/26-22:16:55.198 1c90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old8. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.234182902702216
Encrypted:	false
SSDEEP:	6:mao8Dq2PWXp+N23iKkKdK9RXXTZIFUtno82F4ZmwBo8AzkOWXp+N23iKkKdK9RXXH:pXDva5Kk7XT2FUtX9/BXM5f5Kk7XVJ
MD5:	04F100BC1FC70CD9E2D4EAEA39B5E2FB
SHA1:	CBE429B1C8ED4E4A081CE6C005BC7AAA539E55B6
SHA-256:	52841604C612C4B7FB5A8C5EFC1BDC2D1A1E6828A1F18624AE63C2C0E3F70EFA
SHA-512:	D0506F428463DD775D9E85F77AD197C89D4ACE4A6ECC3DB78F5351F0A5D57EAF1B395BE3DD6AD00FDE69F0A34A982401D905084AAA4D663F97430754D999738C
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.196 1c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/10/26-22:16:55.197 1c90 Recovering log #3.2021/10/26-22:16:55.198 1c90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.180268103719233
Encrypted:	false
SSDEEP:	6:mao8pq2PWXp+N23iKkKdKyDZIFUtno8qZmwBo8WkwOWXp+N23iKkKdKyJLJ:pXpva5Kk02FUtXq/BXW5f5KkKwJ
MD5:	E99E2E1EC94EA7FBCF45A21C3B762D05
SHA1:	00E8217679462B7027AD5ADC69CDCE4B271803E0
SHA-256:	491D698AA25F692E3106424E90393FA0E13EBF90CF5C6F44530B2E0C69C49B28
SHA-512:	C25110C8AF44031A78B61999691A7815BE9B1C0AAD30FBB24C909F6D8CC29B328D0DA8EF33DAB217F7DE5758CAE32E8BABB444D7D33469DB3F554C56FD4154
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.190 1c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/10/26-22:16:55.192 1c90 Recovering log #3.2021/10/26-22:16:55.192 1c90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.180268103719233
Encrypted:	false
SSDEEP:	6:mao8pq2PWXp+N23iKkKdKyDZIFUtno8qZmwBo8WkwOWXp+N23iKkKdKyJLJ:pXpva5Kk02FUtXq/BXW5f5KkKwJ
MD5:	E99E2E1EC94EA7FBCF45A21C3B762D05
SHA1:	00E8217679462B7027AD5ADC69CDCE4B271803E0
SHA-256:	491D698AA25F692E3106424E90393FA0E13EBF90CF5C6F44530B2E0C69C49B28
SHA-512:	C25110C8AF44031A78B61999691A7815BE9B1C0AAD30FBB24C909F6D8CC29B328D0DA8EF33DAB217F7DE5758CAE32E8BABB444D7D33469DB3F554C56FD4154
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.190 1c90 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/10/26-22:16:55.192 1c90 Recovering log #3.2021/10/26-22:16:55.192 1c90 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0

Size (bytes):	45056
Entropy (8bit):	0.7083525984225677
Encrypted:	false
SSDEEP:	96:xJmxZqUkKbQDnpM/121sOeCX1ljehFcqIPeIDtBT:xQZI3CWCx1lc+qIGlft2
MD5:	D7936E082B3FA6BD0E681C1071DAAC2D
SHA1:	335DF01E298C6613599490D4EE55FD0EB4FC3F41
SHA-256:	E22C0C607AEB1726FB27EE44CA0EBBEA19B93DE3A6371B8360E81D6BAC1FA94
SHA-512:	4FE54F66216E382BEDC42FE50D1DB0460F4B32EA3C9982F1F8747E8641EE1902338426D867EA00DE98EEEEABF786E4872ECADF8AD664575A51318777917043778
Malicious:	false
Reputation:	low
Preview:\$.l.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.7087672164733044
Encrypted:	false
SSDEEP:	768:wPxjVYk3seJ1mIVZVRVq1VqlmAAxasnMwYJ7JeDiDKcRZ:cVYMFVZVRVGVTKldgUJ
MD5:	61FA6E261C1D17AB0044C1E4F2E43000
SHA1:	6DC298D6D7A4419CE8176AFD714CCCCFD0A07E4F
SHA-256:	219825C23827C29786FC167A78E654E2B819E6E0BD341AA5B6956878AE0B1BDA
SHA-512:	ACF2706E8C1AE0F690A0791803060E39B954EE81D49183B9BA4870FA122D0FDAEC05FFD86DA2F04EEF41AADCC5FA9D3DFDD2D533D38CB10B75C0C646AA550BA
Malicious:	false
Reputation:	low
Preview:S.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1056768
Entropy (8bit):	1.0550192397653997
Encrypted:	false
SSDEEP:	768:VLJt3LJfLJfLJt3bLJt7aBS2dD6hRz2VC/+T8LgP22/bdcUSLF6wQ3TWXWuUJx:AL+64mTF22RsL4wiTWhP8zbd
MD5:	07C02C557EBB0332D5D20006EE7A96DA
SHA1:	73CA2116E5663FEC471AD23DD3ABB0BB6E147EF8
SHA-256:	C2EE3E36836D8D17D7ABA2A9F5F824831E2C9CA9C114BB801F07788C8FEDD06A
SHA-512:	2B7EEB8C56B7876E441E48C4CF2109C0CE7079C8CF2DD098EC9EE1C5F668E802EDA02051EDA29D58D069FD15EC513D60A483D81678D0282D95E6D7AA5468619
Malicious:	false
Reputation:	low
Preview:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4202496
Entropy (8bit):	1.9711399216453733
Encrypted:	false
SSDEEP:	6144:PwAfBcrBL4AA9AjQgGwV2AJOWIA+APyfe6WzLjgkTqt9rreSsJFA690WdAgPk7f:SrKwZMz/N2Z
MD5:	737965BB3F452B787A3889A9196ACF6D
SHA1:	97A7B6A36EF7C657B220E1F7DEE50ABFC6D96230

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	
SHA-256:	CAD51BE7225C785FC1246D02E862336150676507447D4DE5EF4B75E32D6C9590
SHA-512:	12D4577E9B8CFFDF1471F77FEBD2165773CE5FE9137A4CB9DAF7B6DCF57C905126382A1A6914A7CCC6E91F0B6087F08D98A19280A6EFB59EC792ED50AF29F4
Malicious:	false
Reputation:	low
Preview:n.....W..W.....WW..W?.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.3412489427560823
Encrypted:	false
SSDEEP:	48:TZLLOpEO5J/Kn7U1uBXW0YwTzTzzKSR8U9HWGf3pdfE1g6nZ7yd:tNw4m0YwTzuS+7HWMpdd6Z7yd
MD5:	94110347F2A22564D16DB248184F5F0A
SHA1:	62084E6B4BB970CB3508DB0C992781E68E9093DB
SHA-256:	6B65A96CF5B46B856ED128708CBB835ED8D89F9F7DCE13EC99310A85B13A2E5
SHA-512:	8136B6CBF7A715106C083087C23E0FF06503FACCB73896644BAD061EF7A7D7901446662818D0BD1E32A4A9544F78B207B40D16B064B386347A0BE31BB59D58DB
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@C.....g...8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10148
Entropy (8bit):	3.500711655052152
Encrypted:	false
SSDEEP:	96:34/NqG501Zc5L5q8ZuMDb9+k5VFijzJKmH5uSPsvTc8rPsWc/c6ZC:3LPLfYbAkZRxPFOPUED
MD5:	3FF541E2E25AFC12AC89619D5DD0BD67
SHA1:	DC7019C502286DABFD7478941895B99928D0685F
SHA-256:	0BA02760AFBBD36C84CD13D4AA0E8891281EAE9BA91C0410E21BCD1097C14EC
SHA-512:	91D598D0CAB265685A22DF2A0F1631A31A26394C476A63CE14E3FFEB5EB3E837F80175BA2986C54514032784613AB1505484569FD418872B5BCFBD45E4877C7E
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.....\$.84f4db4d_7acf_4634_a927_34ef6a330aac.....`.....5..0.....&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.....Y...https://docs.google.com/document/d/1hHFEB09XYOGm1F87T0dc5etNXb38nGMo/edit?invite=CKvaqcMD...).A.d.j.u.n.c.t..E.v.a.l.u.a.t.i.o.n..(2)...d.o.c.x..G.o.o.g.l.e..D.o.c.s...<...8.....0...h.....`.....0.....H.....@.....3.J.N..4.J.N.....Y...https://.d.o.c.s...g.o.o.g.l.e..c.o.m./d.o.c.u.m.e.n.t./d./1.h.H.F.E.B.0.X.Y.O.G.m.1.F.8.7.T.o.d.c.5.e.t.N.X.b.3.8.n.G.M.o./e.d.i.t.?i.n.v.i.t.e.=C.K.v.a.q.c.M.D.....0...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dt:n:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F97A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkgccagldgiimedpiccmgmieda1.0.0.6_0\metadata\computed_hashes.json

Preview:	{ "file_hashes": { "block_hashes": ["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBxp3hN2slp0=", "WSOpQRkYHjPSIG9Zif2a7Tnhy43NDcG1Zg5Nv0UbH0=", "jDctR8lmG5KZrQKm4kDjUB7FokSjfo/pmvFowRVlaY=", "LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=", "nZ9zLb2By96AkKXALRM+C0Eu1XUjPIMXEKjJCpdtHE=", "wifibc1QfMBN2jrtUtlgsCefvuceTpAatmLvul11RJA=", "dHjWSIlidj7MWgg3T8MG58RuuqRXk32vqi/13JqEgA=", "zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTi=", "DpjXcO85FFY9KJFPkGNfUtdQIOsGwO5jUckiUwY14=", "gqid6l1+mk/6yWgUECRofl9IMipXgXh2jEN2+CxmPE0=", "prDB91X2Mmfg/MtxVMITWBMEGBOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOsthVFWn8EzCM=", "EPQ3jzdrLkAHyvf3920B5Y3aAkO1Jdn/UtbnAmq6T0=", "+oOc6ca+ChkUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=", "3mBGNAIRITANEQkqzU3TEI+5wJ0ubR5uwtS4/9OOM7w=", "1A9N Nawxuhu95H5eThv1rewJ4QQWhhPNxJXO1C/n68=", "E3vWLQxzmj+e5QxYbUscIJ5n0lTpw5JBHV1Kph3/KM=", "i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsmTlRpg=", "R8B8qYabnMSILPhrtu0hGyRhn3llsMHqBbi70gkljEE=", "rhizuEvv2KRAF Mms896x FwkNgPrw6WvmgPn6xrBSa2Y=", "LAMXv6sRb0VZrY34aVXF3Fftxs
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm18520.615.0.5_1\metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6lcafusK4H1IIGRIhKikIALQWdynQh2RX4K6M1tvtzr7XSNyZ:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{ "file_hashes": { "block_hashes": ["DOZdV3jFvk12AM2JNDYK03KZrVrPrmJ+sVgWkqE4Q=", "rVEIW3Hu3T52SzDDUqGT5YjJTBGUv2h3pNuBKFlhZ1U=", "X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxS=", "VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=", "EchCwCbQHbHQ7oDdGT2qNyiRj0yck2YC2emNGq4whTE=", "block_size":4096,"path":", "_locales/fw/messages.json", {" "block_hashes": ["xkkoZ7iSU1+7cd6DAteMUC5IPFd+EgcbnzxkOifWlk=", "3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=", "o9+TsohquaCMj+70zeinRG/hBhA2uL0Dl/WoC1uokME=", "xv/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=", "p/mvJm2wuCl32Rx3it654MjKAsMe3S9IDEabc1A8mE=", "j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=", "nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDXTxc=", "eToQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=", "Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihEkM=", "VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=", "iDgLXQqXJp8nCZxgLuC9LXM45DGufuGnXvmHsn18wc=", "g+RfdRfWtUK0Pkcsbot7NJ4SC9wVRV/dvVMuHAteJ8=", "2oC4HcCuXU3VjF6wnKlZnt9uqQNaebcuWp/mWj69U=", "aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWszCnvk=", "L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	2.3297795927158162
Encrypted:	false
SSDEEP:	96:EBCyGkPslR5W553fVpTPsV5+5i5z+5vTjAhGvKkvgGxzbPTDbmxl8ITXXSh:WN1PcfPwMTjaUvgGdXmxl8Za
MD5:	8C5E6D22D9CBAFBC84EB8EA6C5233B37
SHA1:	F1E240183B308AD110333472AB611300EDEB8AC4
SHA-256:	B66536A8FD37195113119090E26A5F547C6AA5C38A86269B0860AD2FB6AEFF87
SHA-512:	67463A04CF377F92287AB25639133969B6EBB1205889AB7A0EB181CD3A5E2E83FD29CB680803BDA5275580B506F27337942332BF9B7E21868BB31556C96F84
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@C.....g....._c.....~2.....s...;+...indexfavicon_bitmaps_icon_idfavicon

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxIXNqXlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45C8B569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.205798500431973
Encrypted:	false
SSDEEP:	6:mao8r+q2PWXp+N23iKkDk25+Xqx8chl+IFUtno81EIWZmwBo81EIVkwOWXp+N23U:pXr+va5KkTXfchl3FUtnX1E4/BX1EIV6
MD5:	AC1079BC1136D36892290E946BB064D6
SHA1:	34915BB00B95A980620EE79D39183CCAE17F2BEF
SHA-256:	55184BEEBD56069E993EA6CB7212D1159EF8E7D70C82BA050E3AC3D993EDDA09
SHA-512:	0BD9922A72EA1865CD7A93508F46BEF4A07D60499CAB42A014EF325E9512D08155FBEA1546EBDCA8121C5AB573AF8A1BA97F2CA21E24B32A4555CBA36E110B:F
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.122 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/10/26-22:16:55.124 1a0c Recovering log #3.2021/10/26-22:16:55.124 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.205798500431973
Encrypted:	false
SSDEEP:	6:mao8r+q2PWXp+N23iKkDk25+Xqx8chl+IFUtno81EIWZmwBo81EIVkwOWXp+N23U:pXr+va5KkTXfchl3FUtnX1E4/BX1EIV6
MD5:	AC1079BC1136D36892290E946BB064D6
SHA1:	34915BB00B95A980620EE79D39183CCAE17F2BEF
SHA-256:	55184BEEBD56069E993EA6CB7212D1159EF8E7D70C82BA050E3AC3D993EDDA09
SHA-512:	0BD9922A72EA1865CD7A93508F46BEF4A07D60499CAB42A014EF325E9512D08155FBEA1546EBDCA8121C5AB573AF8A1BA97F2CA21E24B32A4555CBA36E110B:F
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.122 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/10/26-22:16:55.124 1a0c Recovering log #3.2021/10/26-22:16:55.124 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.166477469641953
Encrypted:	false
SSDEEP:	6:mao80+q2PWXp+N23iKkDk25+XuoIFUtno8eQAWZmwBo8eQ3VkwOWXp+N23iKkDkL:pX0+va5KkTXYFUtnXf/BXfV5f5KkTXHJ
MD5:	E3758A8E4804307F04BEA1375DA53FCA
SHA1:	7FA45A0D80FC86A8598895F61575AB485383E831
SHA-256:	CFB07E4FC25F41ED5FE4A973C46C55DF75EF5A2702BAE94CC1C3CF42FDC96992
SHA-512:	ECE21FBEBB601F1B3F904117A7B25FE06558FD65F0EF3C29EE8362B09847D671D68B0CF16CB6CA5FAF3978C4EEBA44B9E5C839BE66BF6F67E60CA090E58A060A
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.116 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/10/26-22:16:55.117 1a0c Recovering log #3.2021/10/26-22:16:55.117 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Entropy (8bit):	5.166477469641953
Encrypted:	false
SSDEEP:	6:mao80+q2PWXp+N23iKKdK25+XuoIFUtno8eQAWZmwBo8eQ3VkwOWXp+N23iKKdKl:pX0+va5KkTXYFUtnXf/BXfV5f5KkTXHJ
MD5:	E3758A8E4804307F04BEA1375DA53FCA
SHA1:	7FA45A0D80FC86A8598895F61575AB485383E831
SHA-256:	CFB07E4FC25F41ED5FE4A973C46C55DF75EF5A2702BAE94CC1C3CF42FDC96992
SHA-512:	ECE21FBEBB601F1B3F904117A7B25FE06558FD65F0EF3C29EE8362B09847D671D68B0CF16CB6CA5FAF3978C4EEBA44B9E5C839BE66BF6F67E60CA090E58A060A
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.116 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/10/26-22:16:55.117 1a0c Recovering log #3.2021/10/26-22:16:55.117 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.187708719667054
Encrypted:	false
SSDEEP:	6:mao8D+q2PWXp+N23iKKdKWT5g1ldqIFUtno8mWZmwBo8NVkwOWXp+N23iKKdKWTk:pXD+va5Kkg5gSRFUtnXZ/BXNV5f5Kkgk
MD5:	6021708A7551D4F4228A80EC5B5E3A8B
SHA1:	F7919ADA45204594482076986FF7A07BB0D3CD56
SHA-256:	52B66731DD973F6B7FB3443229ED8C41D92511B395FB85282BD054B66B8122F7
SHA-512:	9B34F1193460E2E9E5736B932C3B1A02FE03F497EF5CDC450B8B0F7E674CA3C233D26778BFA329211C0421B3337FB2EEBF0B240443449DC5A78D8A4F32492677
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.016 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/10/26-22:16:55.018 1a0c Recovering log #3.2021/10/26-22:16:55.018 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old.d (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.187708719667054
Encrypted:	false
SSDEEP:	6:mao8D+q2PWXp+N23iKKdKWT5g1ldqIFUtno8mWZmwBo8NVkwOWXp+N23iKKdKWTk:pXD+va5Kkg5gSRFUtnXZ/BXNV5f5Kkgk
MD5:	6021708A7551D4F4228A80EC5B5E3A8B
SHA1:	F7919ADA45204594482076986FF7A07BB0D3CD56
SHA-256:	52B66731DD973F6B7FB3443229ED8C41D92511B395FB85282BD054B66B8122F7
SHA-512:	9B34F1193460E2E9E5736B932C3B1A02FE03F497EF5CDC450B8B0F7E674CA3C233D26778BFA329211C0421B3337FB2EEBF0B240443449DC5A78D8A4F32492677
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:55.016 1a0c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/10/26-22:16:55.018 1a0c Recovering log #3.2021/10/26-22:16:55.018 1a0c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCachedata_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	270336
Entropy (8bit):	0.0018238520723782249
Encrypted:	false
SSDEEP:	3:MsEIIllkEthXllkIzEfi:/M/xT0Zz
MD5:	B4AC901F20E52934CE21731FD3F61DC8
SHA1:	ED65F9491D6D3900936E0E1397EBB1C6C1084725
SHA-256:	ED989B289938933622AA5EFF180AB8445FB12F035B2B29BEA50DA8A568375B40
SHA-512:	E04577FDCCB16D5144E5E91C29567AFC6A4F6D4CA4DD93320D23760846B2BA7C5106B77750FDE5DDEE5B1217B8889D102DEF95780DEF467830CBA1B9E2D4F3F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1

Table with 2 columns: Reputation: low, Preview: [dotted lines]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History

Table with 2 columns: Process: C:\Program Files\Google\Chrome\Application\chrome.exe, File Type: SQLite 3.x database, last written using SQLite version 3032001, Category: dropped, Size (bytes): 118784, Entropy (8bit): 0.6042432996215225, Encrypted: false, SSDEEP: 96:rPs95b553z50c0U+bDoYysX0uhnydVjN9DLjGQLBE3uyPsk5v5j3:rPKp2Xf+bDo3irhnydVj3XBBE3uyPp, MD5: 030711ACF444E42DC22BFF5394B40086, SHA1: DAE5D5B25A7AFFB3FBA1B7C7AD49242B8A48395B, SHA-256: C087EBC4A913C774EBDB1354EFAFC30EA9AFA78A121B9FB252F479D6DC99E87, SHA-512: 0C0CABAC2B910ED069827E389DECAAC3BF2F830FE7938ECA543E09F34D6FD8CE45C187ED3322E664B0E0ED5ECCC2D88EE6DBA4DBEE665C7F45742FDB691E9708, Malicious: false, Reputation: low, Preview: SQLite format 3.....@C.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Table with 2 columns: Process: C:\Program Files\Google\Chrome\Application\chrome.exe, File Type: data, Category: dropped, Size (bytes): 1801, Entropy (8bit): 5.974118310558968, Encrypted: false, SSDEEP: 48:vvTVgLR2D84dZ5M6CYwXt6EwH5et675qB5gORo:vwZgLyXFM6QwN5ey5qB5Zy, MD5: F796D133E316CA119F7A531B4BE4364E, SHA1: 62430B64B2A023C59AFEF907FF2C40582FDCC8A4, SHA-256: 90D1DBD6D0F405FB4F17A659FDB5B4D1C3440FEBA89AD1EF6B0C1325AA936E28, SHA-512: 7FA8271AECA3BA1B676FA65EFAF4A2AC5F4B6937DDB5D0AADF2F7044420B01E774B38D89F29A67457FE434AAD45ABA0227E2F5E25A2816B51D34C5D1196417F3, Malicious: false, Reputation: low, Preview: ".....!1hhfeb09xyogm1f87todc5etnxb38ngmo..2..adjunct..ckvaqcmd..com..d..docs..document..docx..edit..evaluation..google..https..invite..rtprof..sd..true..6178419e..eip..m..sharing..ts..usp*....%!.!1hhfeb09xyogm1f87todc5etnxb38ngmo.....2.....6178419e.....adjunct.....ckvaqcmd.....com.....d.....docs.....document.....docx.....edit.....eip.....evaluation.....google.....https.....invite.....m.....rtprof.....sd.....sharing.....true.....ts.....usp..2..."...0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....x.....y.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal

Table with 2 columns: Process: C:\Program Files\Google\Chrome\Application\chrome.exe, File Type: data, Category: dropped, Size (bytes): 8720, Entropy (8bit): 0.3283577581710296, Encrypted: false, SSDEEP: 6:Gq4/fMt76Y4QZVRtRex99pG/MCcqR4EZY4QZv8FOY:H4nMWQA9LdcBQZ8FOY, MD5: 75D25CAC20D754B06B177DF64C707612, SHA1: 7BF92DE32899EEDF7B567A41478014D371FBD4FC, SHA-256: DE193E2152E6648051AF35F705EAB8FA6ECBB11035485C72B49FEF2FB2BC70, SHA-512: 5747490EC6FF62D32832757E06DE64FCED0149F6C596D7FBB405D508020120C41DB636F32BDED688BB2E84C2344E14B955FF939EDDEC50DFEA7CD45449EDD01, Malicious: false, Reputation: low, Preview: [dotted lines]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10148
Entropy (8bit):	3.500711655052152
Encrypted:	false
SSDEEP:	96:34/NqG501Zc5L5q8ZuMDb9+k5VFijZjKMH5uSPsvTc8rPsWc/c6ZC:3LPLfYbAkZRxPFOPUED
MD5:	3FF541E2E25AFC12AC89619D5DD0BD67
SHA1:	DC7019C502286DABFD7478941895B99928D0685F
SHA-256:	0BA02760AFBBED36C84CD13D4AA0E8891281EAE9BA91C0410E21BCD1097C14EC
SHA-512:	91D598D0CAB265685A22DF2A0F1631A31A2639AC476A63CE14E3FFEB5EB3E837F80175BA2986C54514032784613AB1505484569FD418872B5BCFBD45E4877C7E
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.....\$.84f4db4d_7acf_4634_a927_34ef6a330aac.....5..0.....&...{AE32626E-B2F7-4664-89C4-2B2C2DB60905}.....Y...https://docs.google.com/document/d/1hHFE09XyOGm1F87Toc5etNXb38nGmO/edit?invite=CKvaqcMD...).A.d.j.u.n.c.t..E.v.a.l.u.a.t.i.o.n..(2)...d.o.c.x..-..G.o.o.g.l.e..D.o.c.s...<...8.....0...h.....`.....0.....H.....@.....3.J.N..4.J.N.....Y...h.t.t.p.s://.d.o.c.s...g.o.o.g.l.e...c.o.m/.d.o.c.u.m.e.n.t./d./1.h.H.F.E.B.0.9.X.Y.O.G.m.1.F.8.7.T.o.d.c.5.e.t.N.X.b.3.8.n.G.M.o./e.d.i.t.?i.n.v.i.t.e.=C.K.v.a.q.c.M.D.....0...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last TabsOC (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8066
Entropy (8bit):	5.410912158770678
Encrypted:	false
SSDEEP:	192:olXgdczDpE5fgnwKHgQryytdorlRgE5fghg:bsowsp8g
MD5:	D3D2B9618743D1A9407E9086C6B1839B
SHA1:	0249D5909709210BF583F079F1908C6226544614
SHA-256:	1909477A61C98E9F09C9C9BD463F0F3CB942794618A3B67C24982D83C81FC45
SHA-512:	5581C4D02B3F81B5BDB5ACFA1F5AD60D739CD8534FFCDE6368C3466EA55B46F74988A7DF5CB26560527D15B7C7132EBABB484DAE350C967AFF33FFF4E10CFE12
Malicious:	false
Reputation:	low
Preview:	...5.....VERSION.1.8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Q_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.CloudProvider7.{"cloudEnabled":false,"notifiedHangoutsPrivacy":false}.S_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.IdentityService6.{"signedIn":false,"userEmail":null,"kioskAuth":false}.Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..826992000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2020-09-30 07:58:17.19][INFO][mr.Init] MR instance ID: eed8a5c4-c410-41ec-8296-fe0906655421\n","[2020-09-30 07:58:17.20][INFO][mr.Init] Native Cast MRP is disabled.\n","[2020-09-30 07:58:17.20][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2020-09-30 07:58:17.21][INFO

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.156872068447172
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:mao8af3+q2PWXp+N23iKkdk8a2jMGIFUtno8C4WZmwBo8YVkwOWXp+N23iKkdk8N:pXaf3+va5Kk8EFUtnXC4W/BXYV5f5Kkw
MD5:	C1F5FC0AD3857B3FBB628142DA053E56
SHA1:	F35D426EB4C9E5074E52CA4D63A50548D2E643B6
SHA-256:	C21C02C7239476B8B644B85C61B2BDCEC8A24DFBD7A532F6CAB4F638BA621655
SHA-512:	9C90E4747FC55149255AD35E11009A8EC834456FD0BD890AC1E649CC327DC4AF1391212C2772E695D5291E08F239011E1F3B54B00414ADD1620F648877DEC775
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.260 1a3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/10/26-22:16:43.268 1a3c Recovering log #3.2021/10/26-22:16:43.271 1a3c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.156872068447172
Encrypted:	false
SSDEEP:	6:mao8af3+q2PWXp+N23iKkdk8a2jMGIFUtno8C4WZmwBo8YVkwOWXp+N23iKkdk8N:pXaf3+va5Kk8EFUtnXC4W/BXYV5f5Kkw
MD5:	C1F5FC0AD3857B3FBB628142DA053E56
SHA1:	F35D426EB4C9E5074E52CA4D63A50548D2E643B6
SHA-256:	C21C02C7239476B8B644B85C61B2BDCEC8A24DFBD7A532F6CAB4F638BA621655
SHA-512:	9C90E4747FC55149255AD35E11009A8EC834456FD0BD890AC1E649CC327DC4AF1391212C2772E695D5291E08F239011E1F3B54B00414ADD1620F648877DEC775
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.260 1a3c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/10/26-22:16:43.268 1a3c Recovering log #3.2021/10/26-22:16:43.271 1a3c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	0.5027784235225523
Encrypted:	false
SSDEEP:	48:Tbw/qALihje9kqL42WOT/9FLRFPxmPyPIVYFP+:fOqAuhjspnWov9FPkPyPIVYFP+
MD5:	37B337AEA3C2A2B21AE00CD51374A9DB
SHA1:	DB5D4AD4812EADA55CF099460316A11C492ACDB7
SHA-256:	52DDC8CFC46D0F84EDF77E72AF54E06CCB8F2882D700233BE4B91195D27BE094
SHA-512:	49F3B3AA3365098EF11F17DF9FC62CA786D9EB06E7D28D042333C406037D5633E406017A08B983AE410D0D3976E12123865B848220E79BC1654B2FC8F28F60
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@C.....\t+>.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBSvxMHVzspxMHbsIH/soBDysKqnsilzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC48472F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State. (copy)

Preview:	{ "net": { "http_server_properties": { "servers": [{ "alternative_service": [{ "advertised_versions": [], "expiration": "13248543677350473", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543677350474", "port": 443, "protocol_str": "quic" }, { "isolation": [], "network_stats": [{ "srtt": 31344 }, { "server": "https://dns.google", "supports_spdy": true }, { "alternative_service": [{ "advertised_versions": [], "expiration": "13248543501474403", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543501474403", "port": 443, "protocol_str": "quic" }, { "isolation": [], "network_stats": [{ "srtt": 31656 }, { "server": "https://clients2.googleusercontent.com", "supports_spdy": true }, { "alternative_service": [{ "advertised_versions": [], "expiration": "13248543501454993", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [], "expiration": "13248543501454994", "port": 443, "protocol_str": "quic" }, { "isolation": [], "network_stats": [{ "srtt": 39369 }, { "server": "https://www.googleapis.com", "supports_spdy": true },
----------	---

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State7f (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3947
Entropy (8bit):	4.895085022128005
Encrypted:	false
SSDEEP:	96:JnDHaz42ZrCxZO5pGRGcGcGbGGGGeGyGhGNGGGGH:JnDHaz42ZexZO5pyL14UvL1O83J
MD5:	9A2DA8A1A7CE0783A1488AA87EC16A4F
SHA1:	A54A0B17D41403E9B2E8B608F7459113BFC55968
SHA-256:	70AC9E3D6B32E9BA67A1E9DDE13EC1A3ED84CF22EEB5E7FFC8CCE05AEE0E6717
SHA-512:	808269EC02D76F71B4119BE8E7C12D4E043251D4CF7B15D50168394B41E6C898CEE68C8E9C6DC8CC990A4A1A9750F5695CE9D9CB2E41C2736D683D02422A52
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": [{ "isolation": [], "server": "https://www.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://ogs.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://www.googleapis.com", "supports_spdy": true }, { "isolation": [], "server": "https://dns.google", "supports_spdy": true }, { "alternative_service": [{ "advertised_versions": [50], "expiration": "13282377405311650", "port": 443, "protocol_str": "quic" }, { "isolation": [], "server": "https://redirector.gvt1.com", "alternative_service": [{ "advertised_versions": [50], "expiration": "13282377405360981", "port": 443, "protocol_str": "quic" }, { "isolation": [], "server": "https://accounts.google.com", "supports_spdy": true }, { "alternative_service": [{ "advertised_versions": [50], "expiration": "13282377405607589", "port": 443, "protocol_str": "quic" }, { "advertised_versions": [50], "expiration": "13282377405607592", "port": 443, "protocol_str": "quic" }, { "isolation": [], "server": "https://r4--sn-h0jeln7l.gvt1.com", "alternative_servic

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.230889035760275
Encrypted:	false
SSDEEP:	6:mao83M+q2PWxp+N23iKkKdKgXz4rRIFUtno82EmZmwBo8GMVkwOWxp+N23iKkKdKgi:pX8+va5KkgXiuFUtnXK/BXbV5f5KkgXS
MD5:	D1F224838D6E2336A09689F1A911B7F9
SHA1:	6DBA108BD882ACBBA51A047E21F30319006D072
SHA-256:	E56753E97AC6839D0C4827094C1D8AC6120C0F8552BB6E404DFC236B545945D0
SHA-512:	38CE809B4E8553D3DE6E087E1DA6AB6EAEC552D87CA7F314FFD5FD56401F4DC3DD717FADED66FF0CD70B23B00AEB288F9049C208D0B36B76A480BD3ACB9DBC3
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.893 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\MANIFEST-000001.2021/10/26-22:16:43.895 1aac Recovering log #3.2021/10/26-22:16:43.896 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.oldMP (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.230889035760275
Encrypted:	false
SSDEEP:	6:mao83M+q2PWxp+N23iKkKdKgXz4rRIFUtno82EmZmwBo8GMVkwOWxp+N23iKkKdKgi:pX8+va5KkgXiuFUtnXK/BXbV5f5KkgXS
MD5:	D1F224838D6E2336A09689F1A911B7F9
SHA1:	6DBA108BD882ACBBA51A047E21F30319006D072
SHA-256:	E56753E97AC6839D0C4827094C1D8AC6120C0F8552BB6E404DFC236B545945D0
SHA-512:	38CE809B4E8553D3DE6E087E1DA6AB6EAEC552D87CA7F314FFD5FD56401F4DC3DD717FADED66FF0CD70B23B00AEB288F9049C208D0B36B76A480BD3ACB9DBC3
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.893 1aac Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\MANIFEST-000001.2021/10/26-22:16:43.895 1aac Recovering log #3.2021/10/26-22:16:43.896 1aac Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences\ (copy)

Table with 2 columns: Property Name (e.g., Size, Entropy, Encrypted) and Value (e.g., 5190, 4.985071692974357, false). Includes a large JSON preview for the 'Preferences' file.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\QuotaManager

Table with 2 columns: Property Name (e.g., Process, File Type, Category) and Value (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe, SQLite 3.x database). Includes a preview of the SQLite database content.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL

Table with 2 columns: Property Name (e.g., Process, File Type, Category) and Value (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe, SQLite 3.x database). Includes a preview of the SQLite database content.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)

Table with 2 columns: Property Name (e.g., Process, File Type, Category) and Value (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe, UTF-8 Unicode text). Includes a preview of the text file content.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Reputation:	low
Preview:	2021/10/26-22:16:43.764 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000001.2021/10/26-22:16:43.765 1a08 Recovering log #3.2021/10/26-22:16:43.766 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.184734106558647
Encrypted:	false
SSDEEP:	6:mao8h3t+q2PWXp+N23iKkKdKrQmXiFUtno8h0X5ZmwBo8hD3VkwOWXp+N23iKkKdKf:pXhYva5KkCFUtnXh0J/BXh55f5KktJ
MD5:	0B0C8A0ADD90AABC059A2EE44D68CC1D
SHA1:	E45631CAA5A0C5599D43527EC5BD955E06849601
SHA-256:	B0ACCFD4751AF14F963A63C6624AA84755CD50614239B28B0FEA7BB785692AE1
SHA-512:	556A244FB1F3BEA73DD766C8895471CB87BD9AD9741AA992492CD63C8ECACB163CED2EE2F00789BD56CFDF8A97290DCF09A7638684D9B557E83C3AF5F171A4AB
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.764 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000001.2021/10/26-22:16:43.765 1a08 Recovering log #3.2021/10/26-22:16:43.766 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.142282300770209
Encrypted:	false
SSDEEP:	6:mao8UHlq2PWXp+N23iKkKdK7Uh2ghZIFUtno85YZmwBo80EekwOWXp+N23iKkKdK7w:pXUova5KklhHh2FUtnXa/BXg5f5Kklh9
MD5:	1B9683EAAE083EAB64A7361B24271890
SHA1:	BFAAC91503BFE2F318D4A5AEC2AC4B40F263E58E
SHA-256:	F8713F26CE6FD4AEA498FA9AC3E78328BE50E468A8C9D3ECEC5E4256739B1E1A
SHA-512:	B2A2387646DC9975478A9A6008FA908EBA7A3E8B1542F745F769BA75C13B13E6CAC13A9E89670FE92D8C20CAC2A7C8DA6F7BF0F8CD70A86F2440CFA5B28183A0
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.245 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/10/26-22:16:43.258 1a30 Recovering log #3.2021/10/26-22:16:43.263 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.142282300770209
Encrypted:	false
SSDEEP:	6:mao8UHlq2PWXp+N23iKkKdK7Uh2ghZIFUtno85YZmwBo80EekwOWXp+N23iKkKdK7w:pXUova5KklhHh2FUtnXa/BXg5f5Kklh9
MD5:	1B9683EAAE083EAB64A7361B24271890
SHA1:	BFAAC91503BFE2F318D4A5AEC2AC4B40F263E58E
SHA-256:	F8713F26CE6FD4AEA498FA9AC3E78328BE50E468A8C9D3ECEC5E4256739B1E1A
SHA-512:	B2A2387646DC9975478A9A6008FA908EBA7A3E8B1542F745F769BA75C13B13E6CAC13A9E89670FE92D8C20CAC2A7C8DA6F7BF0F8CD70A86F2440CFA5B28183A0
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.245 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/10/26-22:16:43.258 1a30 Recovering log #3.2021/10/26-22:16:43.263 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcphaombhimeihdjnejgic\def1a9e076c-5189-4c0f-ad8f-53604d4503d9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def1a9e076c-5189-4c0f-ad8f-53604d4503d9.tmp

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBDD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{\"net\":{\"http_server_properties\":{\"servers\":{\"alternative_service\":{\"advertised_versions\":[50],\"expiration\":\"13248543490879170\",\"port\":443,\"protocol_str\":\"quic\"},\"advertised_versions\":[73],\"expiration\":\"13248543490879171\",\"port\":443,\"protocol_str\":\"quic\"},\"isolation\":[],\"server\":\"https://dns.google\",\"supports_spdy\":true}},\"version\":5},\"network_qualities\":{\"CAASABiAgICA+P///8B\":\"4G\",\"CAESABiAgICA+P///8B\":\"4G\"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\defGPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIIkEthXllk2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\defLocal Storage\leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.259535259476688
Encrypted:	false
SSDEEP:	6:mao81Oq2PWxp+N23iKKdKusNpV/2jMGIFUtno8L7ZZmwBo83WFkOWXp+N23iKKZ:pXgva5KkFFUtnX3Z/BXmF5f5KkOJ
MD5:	D0BC86514B3018133C3FD87DD2927A92
SHA1:	39ADA531487BA5A06AA2675853063566E7B4124D
SHA-256:	46314C863C0620E1E1E08FA8B92F97827607824E453B21A730AAC619DEF8387C
SHA-512:	F5CADD45CE650F7A99005C686B8CBB6DE115E66E637CFA1CB29DF49EB65A051C75F93F144ACEE874C7BCCB7343391EC4121E50E8A00517A580130CA1341DFC4
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.839 1a34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\defLocal Storage\leveldb\MANIFEST-000001.2021/10/26-22:16:43.840 1a34 Recovering log #3.2021/10/26-22:16:43.841 1a34 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\defLocal Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\defLocal Storage\leveldb\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.259535259476688
Encrypted:	false
SSDEEP:	6:mao81Oq2PWxp+N23iKKdKusNpV/2jMGIFUtno8L7ZZmwBo83WFkOWXp+N23iKKZ:pXgva5KkFFUtnX3Z/BXmF5f5KkOJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Local Storage\leveldb\LOG.old (copy)

MD5:	D0BC86514B3018133C3FD87DD2927A92
SHA1:	39ADA531487BA5A06AA2675853063566E7B4124D
SHA-256:	46314C863C0620E1E1E08FA8B92F97827607824E453B21A730AAC619DEF8387C
SHA-512:	F5CADD45CE650F7A99005C686B8CBB6DE115E66E637CFA1CB29DF49EB65A051C75F93F144ACEE874C7BCCB7343391EC4121E50E8A00517A580130CA1341DFC4
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.839 1a34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Local Storage\leveldb\MANIFEST-000001.2021/10/26-22:16:43.840 1a34 Recovering log #3.2021/10/26-22:16:43.841 1a34 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Network Persistent StateMP (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":{"alternative_service":{"advertised_versions":{"[50],"expiration":"","13248543490879170","port":443,"protocol_str":"quic"},"advised_versions":{"[73],"expiration":"","13248543490879171","port":443,"protocol_str":"quic"},"isolation":[],"server":"https://dns.google","supports_spdy":true},"version":5},"network_qualities":{"CAASABiAgICA+P///8B":"4G","CAESABiAgICA+P///8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.306963014036674
Encrypted:	false
SSDEEP:	12:pXYuL4va5KkmiuFUtnXSJ\BXwD5f5Kkm2J:Zka5KkSgXCof5Kkr
MD5:	A96BEB54F9A2976EA61519F61507E359
SHA1:	73C35B730E3C3439272DF64346E27AA280FBD6BD
SHA-256:	6EC42A0E6B17765613E7B3D69FAE2F9D400697106693CD918B83B50886C239E6
SHA-512:	C2B3F01833D94C486DCE7724144DB94A4A45B620F0AD657242EC1F12400320E6FE9815E8EE380F322F3C370688CE110AAD9F102DC16F1D5A8729BAD24C6695B
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.887 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Platform Notifications\MANIFEST-000001.2021/10/26-22:16:43.891 1ab4 Recovering log #3.2021/10/26-22:16:43.893 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpaahaombhbimeihdjnejgic\def\Platform Notifications\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.306963014036674
Encrypted:	false
SSDEEP:	12:pXYuL4va5KkmiuFUtnXSJ\BXwD5f5Kkm2J:Zka5KkSgXCof5Kkr
MD5:	A96BEB54F9A2976EA61519F61507E359
SHA1:	73C35B730E3C3439272DF64346E27AA280FBD6BD
SHA-256:	6EC42A0E6B17765613E7B3D69FAE2F9D400697106693CD918B83B50886C239E6
SHA-512:	C2B3F01833D94C486DCE7724144DB94A4A45B620F0AD657242EC1F12400320E6FE9815E8EE380F322F3C370688CE110AAD9F102DC16F1D5A8729BAD24C6695B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\LOG.old (copy)

Preview:	2021/10/26-22:16:43.887 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\MANIFEST-000001.2021/10/26-22:16:43.891 1ab4 Recovering log #3.2021/10/26-22:16:43.893 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\000003.log .
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHIS+QUI1ASEGhTFjIj:S85aEFjIj
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.274335440803419
Encrypted:	false
SSDEEP:	6:mao8rhFN+q2PWXp+N23iKkKdKusNpZQMxIFUtno81ZmwBo8sv3VkwOWXp+N23iKkK+:pXrhOva5KkMFUtnX1/BXs95f5KkTJ
MD5:	100DD7C2457DF7214F2FA8724D2373B2
SHA1:	B2B72EBC4170A308DF649509D6CB6265DD065D25
SHA-256:	4387F4A36E8342A92046D73008800A0F2251A0C09E3C90646BA6EE7299103F2C
SHA-512:	3CB583A68093D0831CE8C9259DBA815EFD731C6FEB676677BFF43FA0CFDC81455F72CF9733DCFA842FE47B1C12A2D61E6791BEEBD1C285AE1B694495878A315
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:59.339 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\MANIFEST-000001.2021/10/26-22:16:59.340 1aa8 Recovering log #3.2021/10/26-22:16:59.341 1aa8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.274335440803419
Encrypted:	false
SSDEEP:	6:mao8rhFN+q2PWXp+N23iKkKdKusNpZQMxIFUtno81ZmwBo8sv3VkwOWXp+N23iKkK+:pXrhOva5KkMFUtnX1/BXs95f5KkTJ
MD5:	100DD7C2457DF7214F2FA8724D2373B2
SHA1:	B2B72EBC4170A308DF649509D6CB6265DD065D25
SHA-256:	4387F4A36E8342A92046D73008800A0F2251A0C09E3C90646BA6EE7299103F2C
SHA-512:	3CB583A68093D0831CE8C9259DBA815EFD731C6FEB676677BFF43FA0CFDC81455F72CF9733DCFA842FE47B1C12A2D61E6791BEEBD1C285AE1B694495878A315
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:59.339 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\MANIFEST-000001.2021/10/26-22:16:59.340 1aa8 Recovering log #3.2021/10/26-22:16:59.341 1aa8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lmmhkkegcccagldgiimedpiccmgmedaldefl2e3c3ba8-5ab9-48ca-a3ea-849bb783bcfa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefl2e3c3ba8-5ab9-48ca-a3ea-849bb783bcfa.tmp	
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECF3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BF
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": { "alternative_service": { "advertised_versions": [50], "expiration": "13248543498399332", "port": 443, "protocol_str": "quic" }, "advertised_versions": [73], "expiration": "13248543498399332", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "https://dns.google", "supports_spdy": true }, "version": 5 }, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "4G" } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflGPUCachedata_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIIkEthXllkI2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflLocal Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.203723459708745
Encrypted:	false
SSDEEP:	12:pX74va5KkkGHArBFUtnXG3J/BXVD5f5KkkGHArJ:ZGa5KkkGgPgXoPf5KkkGga
MD5:	353C8293AD74991DAF6AE849B8DC2CF3
SHA1:	7E5D2D4270BEEE5427BBAFA730A57A8E26C1B87A
SHA-256:	15B1AACB757EF53756B021A334A1A4BBC868EDFE2773953CD5912A7EA4D8EB07
SHA-512:	D7147B32F095A4A8152529D72846B47AB7620A248AEFF56A9C88994B73607E35D3AD45639DD82DF78981B4AED69E1B5C8E3D8738D8C87AF69E68AC8E39C5D3
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:29.068 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflLocal Storage\leveldb\MANIFEST-000001.2021/10/26-22:17:29.069 1ab4 Recovering log #3.2021/10/26-22:17:29.071 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflLocal Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflLocal Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.203723459708745
Encrypted:	false
SSDEEP:	12:pX74va5KkkGHArBFUtnXG3J/BXVD5f5KkkGHArJ:ZGa5KkkGgPgXoPf5KkkGga
MD5:	353C8293AD74991DAF6AE849B8DC2CF3
SHA1:	7E5D2D4270BEEE5427BBAFA730A57A8E26C1B87A
SHA-256:	15B1AACB757EF53756B021A334A1A4BBC868EDFE2773953CD5912A7EA4D8EB07

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefLocal Storage\leveldb\LOG.old (copy)	
SHA-512:	D7147B32F095A4A8152529D72846B47AB7620A248AEFF56A9C88994B73607E35D3AD45639DD82DF78981B4AED69E1B5C8E3D8738D8C87AF69E68AC8E39C5D3
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:29.068 1ab4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefLocal Storage\leveldb\MANIFEST-000001.2021/10/26-22:17:29.069 1ab4 Recovering log #3.2021/10/26-22:17:29.071 1ab4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefLocal Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefNetwork Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/y
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECF3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BF
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":{"alternative_service":{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},"isolation":[],"server":["https://dns.google","supports_spdy":true],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.239880762294583
Encrypted:	false
SSDEEP:	12:pXwN4va5KkkGHArqiuFUtnXdJ/BXcD5f5KkkGHArq2J:ZwMa5KkkGgCgXZsf5KkkGg7
MD5:	0FCFA5EC632BED947BC7BA772622A158
SHA1:	C0613F2B893F1163CE9FF0B3D79B3F2388A5BE75
SHA-256:	E2FC3D5D0A7BDD1DB2F9DA68AA266D8F1F7108BD08B066D977C743445C5959E3
SHA-512:	38A9884F2FBD0D541D2051970E7539FB1310A8C2FBAF967EB991623A1151A83A6C0CEA0A530237AAD809089AFD23B1EBEABDD32733A7BDB1193E2FF225BF5C10
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:29.084 1bf0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\MANIFEST-000001.2021/10/26-22:17:29.085 1bf0 Recovering log #3.2021/10/26-22:17:29.086 1bf0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.239880762294583
Encrypted:	false
SSDEEP:	12:pXwN4va5KkkGHArqiuFUtnXdJ/BXcD5f5KkkGHArq2J:ZwMa5KkkGgCgXZsf5KkkGg7
MD5:	0FCFA5EC632BED947BC7BA772622A158
SHA1:	C0613F2B893F1163CE9FF0B3D79B3F2388A5BE75
SHA-256:	E2FC3D5D0A7BDD1DB2F9DA68AA266D8F1F7108BD08B066D977C743445C5959E3
SHA-512:	38A9884F2FBD0D541D2051970E7539FB1310A8C2FBAF967EB991623A1151A83A6C0CEA0A530237AAD809089AFD23B1EBEABDD32733A7BDB1193E2FF225BF5C10
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:29.084 1bf0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\MANIFEST-000001.2021/10/26-22:17:29.085 1bf0 Recovering log #3.2021/10/26-22:17:29.086 1bf0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldefPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHIS+QUI1ASEGhTFjji:S85aEFjji
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.189992682787136
Encrypted:	false
SSDEEP:	12:pXwnva5KkkGHArAFUtnXwK1/BXwj5f5KkkGHArfJ:ZCa5KkkGgkgXpX4f5KkkGgV
MD5:	FDF40CA4C09C58B075577F86D530467F
SHA1:	B901AA5383BD559915FEBE1C9734A95CE2F32768
SHA-256:	590EAF63EA70A5DA3D4F38697CDEE4E598349E789D7C09E181FC02358F2BCB11
SHA-512:	67C66EF464BB467ECEC043B6F10051A2C9053E589CB14BC1B415A805A25CD6425F2F7BE94010746625C330B5EFF29CC3FB9B5DB3788F5E6701B06646B460205A
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:44.815 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\MANIFEST-000001.2021/10/26-22:17:44.817 1aa4 Recovering log #3.2021/10/26-22:17:44.818 1aa4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\LOG.olde/ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.189992682787136
Encrypted:	false
SSDEEP:	12:pXwnva5KkkGHArAFUtnXwK1/BXwj5f5KkkGHArfJ:ZCa5KkkGgkgXpX4f5KkkGgV
MD5:	FDF40CA4C09C58B075577F86D530467F
SHA1:	B901AA5383BD559915FEBE1C9734A95CE2F32768
SHA-256:	590EAF63EA70A5DA3D4F38697CDEE4E598349E789D7C09E181FC02358F2BCB11
SHA-512:	67C66EF464BB467ECEC043B6F10051A2C9053E589CB14BC1B415A805A25CD6425F2F7BE94010746625C330B5EFF29CC3FB9B5DB3788F5E6701B06646B460205A
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:17:44.815 1aa4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\MANIFEST-000001.2021/10/26-22:17:44.817 1aa4 Recovering log #3.2021/10/26-22:17:44.818 1aa4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	160
Entropy (8bit):	3.0217164415295743
Encrypted:	false
SSDEEP:	3:sLollttz6sjGXU2tk0lkGgGgGgGg:qolXtWswXU2tkEttt
MD5:	DE92AD90BE6D3364745B2F73F4C3CF73
SHA1:	9158681463BD30E5AF4DDA4BAAC81F93CEDBDA77
SHA-256:	0025A3E0D3B834401B3B5F820E1991EF7E810D9A4B8B6B579E6301C94E7031A0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
SHA-512:	9E81CEFC195439439F4B23EE7696309D7BC3C08E5B444D2ABDE26D2F12B2D3BCFD124FB9A2D40C6389E9F787741676FAD366A2E9982674E7B931028C014D8A7
Malicious:	false
Reputation:	low
Preview:	...n'....._mts_schema_descriptor.....F.....F.....F.....F.....F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.22230067346204
Encrypted:	false
SSDEEP:	6:mao839+q2PWXp+N23iKkKpIFUtno80E1ZZmwBo8hVkwOWXp+N23iKkKdKa/WLJ:pX34va5KkmFUtnX3Z/BXv5f5KkaUJ
MD5:	0EAACD20E20AB9DDAB746A2D9D4B4DCD
SHA1:	DCE436C152B65382FC84F9D04C1C387A2E36109E
SHA-256:	316083B1F0BCBCB92C978855358F56D0E6960AFAF0128B819DCFA40E9306D932
SHA-512:	1D07C7783372A5FE5E5E593491301128FA41EF6A2BBA9F35771BA58198ED1B2FBBAC5F2AE2C299F5308411D0702A326CD49C55EA4B4C0616D767B0109E62F6D7
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.256 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/10/26-22:16:43.263 1a08 Recovering log #3.2021/10/26-22:16:43.267 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.22230067346204
Encrypted:	false
SSDEEP:	6:mao839+q2PWXp+N23iKkKpIFUtno80E1ZZmwBo8hVkwOWXp+N23iKkKdKa/WLJ:pX34va5KkmFUtnX3Z/BXv5f5KkaUJ
MD5:	0EAACD20E20AB9DDAB746A2D9D4B4DCD
SHA1:	DCE436C152B65382FC84F9D04C1C387A2E36109E
SHA-256:	316083B1F0BCBCB92C978855358F56D0E6960AFAF0128B819DCFA40E9306D932
SHA-512:	1D07C7783372A5FE5E5E593491301128FA41EF6A2BBA9F35771BA58198ED1B2FBBAC5F2AE2C299F5308411D0702A326CD49C55EA4B4C0616D767B0109E62F6D7
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:43.256 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/10/26-22:16:43.263 1a08 Recovering log #3.2021/10/26-22:16:43.267 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.276404583728472
Encrypted:	false
SSDEEP:	12:pXfva5KkkOrsFUtnXTHZ/BXE5f5KkkOrzJ:Zna5Kk+gXTjuf5Kkn
MD5:	26BFAC701ADCFD5402201DDA71603F16
SHA1:	BCE0974C77FC288F7AF3D92EB9ACC70A2A09B2D4
SHA-256:	778300A6FBF6C8BD8039FF47F0CD51C2538BA642E62924817589416587654E0AD
SHA-512:	71353AFB4A08094955946A9E4A5C339A463063016F017B18897ECABFD2E71FB677355A6578D724DBE8066A553FE009F23611D84B8121B8D2CE74D34B7B9E4ED7
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:18:16.819 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\MANIFEST-000001.2021/10/26-22:18:16.821 1a08 Recovering log #3.2021/10/26-22:18:16.822 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Size (bytes):	402
Entropy (8bit):	5.276404583728472
Encrypted:	false
SSDEEP:	12:pXfva5KkkOrsFUtnXTHZ/BXE5f5KkkOrzJ:Zna5Kk+gXTjuf5Kkn
MD5:	26BFAC701ADCFD5402201DDA71603F16
SHA1:	BCE0974C77FC288F7AF3D92EB9ACC70A2A09B2D4
SHA-256:	778300A6FBF6CBD8039FF47F0CD51C2538BA642E62924817589416587654E0AD
SHA-512:	71353AFB4A08094955946A9E4A5C339A463063016F017B18897ECABFD2E71FB677355A6578D724DBE8066A553FE009F23611D84B8121B8D2CE74D34B7B9E4ED7
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:18:16.819 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\MANIFEST-000001.2021/10/26-22:18:16.821 1a08 Recovering log #3.2021/10/26-22:18:16.822 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurityOi (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.43295139687735
Encrypted:	false
SSDEEP:	6:YAQNCTIsoz7kqUCHD8wXwlmUUAnIMOb3AAh/FV15Rc3YRpdVqhR8wXwlmUUAnIM4:Y6sMkq/HH+UAnI25h/FnowpdM9+UAnIz
MD5:	7EFCB4FE53EDCD76B3C16A938D785D33
SHA1:	48B9A039466AE1D98AE2839E2AE31286FE87CA69
SHA-256:	6888D003479E1F8BF786A64BE60FEA3469788452987C9DEB3BF341DE6370E363
SHA-512:	D36AB793E847C7032C0A486F9BF5A945DF3736C1ACE2E08C596899020ACDA53121D4412CE7CEB4567DD8C2778ACBD0680B8FA469EBE70B76C2B57C67AFC046E8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct": [], "sts": [{"expiry": "1666847810.802245", "host": "0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=", "mode": "force-https", "sts_include_subdomains": false, "sts_observed": "1635311810.802251"}, {"expiry": "1646198209.100961", "host": "+IPeEeU664E5hmZDsZ8+6O9RnpLxT6WoswFwUoLm6aw=", "mode": "force-https", "sts_include_subdomains": true, "sts_observed": "1635311809.100968"}], "version": "2"}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.007647183052057029
Encrypted:	false
SSDEEP:	3:ImtV+T+T/Mn/tT560m/Ybb//lsUTll7B:iiV+T+EqzgeUp
MD5:	093DDFD9F4DAA600586DEC2345FCC49E
SHA1:	04C0818E729ED26A845FC6C6C03560D5EF6349A4
SHA-256:	871272B59D82AE7F11168FE54209B9397539BC05314C6465B0503D10EECF464
SHA-512:	214051E0E72BA0D902E568B71BE3EDAD18460C2851447F6E4E510A81A056B93C5E0FD370169162D60A18163CF2C43D6C2A8FA7E8E07640CE555015A6FDA8886
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....{ _lKx.<.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d9bbc3-d6a0-418b-a6be-6263029a82f7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5217
Entropy (8bit):	4.989512287040006
Encrypted:	false
SSDEEP:	96:nyC03ix9pcKIqok0JCKL8RkK1HAbOTQVuwvn:nyCJ9pcR4KQkKU
MD5:	B9DF7C310609ED6A1F39FF42BA1B46AC
SHA1:	A6942AD6357F6028E2023DE87105447A7C6D0A1E
SHA-256:	EA300C9EFFF4C43EB86933FB1BE6960D114FDDFE178EDAE924465B96D7D0CBA6
SHA-512:	F7F2880E4442DBF3D4E466D7A77FA4C45D129D6F945211D521785F69A1334E3B21BCED331EF0E8E93FB8D3F732E4F7BDDA9A131AFA68547C68BA4666460730E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.543094092501018
Encrypted:	false
SSDEEP:	3:tUKjo8gkFN2WZmwv2So8gmHJkbhR1V8tSo8gmlmFhhR1WGV:mao8g8XZmwBo8gSml7Vho8gEv7tv
MD5:	FC7B4013319ED18FA4212C4A948DC751
SHA1:	EA22F9A95FD2DB20F78CD955EAACA355905B2765
SHA-256:	A3748C4D5EC74F6F5C7F0774D7817145B99FB3D3CE76B86ED4AB44C23AEAF9FC
SHA-512:	BB113DDE1319A9FE26709701254381C777CE1AC9E738FA59E1CC2E7975741EF94C588EE954F35D0356ED6A9122BAE22848121CDB282D52B21EAB7328583A8D4!
Malicious:	false
Reputation:	low
Preview:	2021/10/26-22:16:54.527 1c90 Recovering log #3.2021/10/26-22:16:54.757 1c90 Delete type=0 #3.2021/10/26-22:16:54.758 1c90 Delete type=3 #2.

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 22:16:44.816459894 CEST	192.168.2.3	8.8.8.8	0xf303	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:44.817760944 CEST	192.168.2.3	8.8.8.8	0xbaa4	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:44.818001032 CEST	192.168.2.3	8.8.8.8	0xc3b0	Standard query (0)	docs.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:46.068486929 CEST	192.168.2.3	8.8.8.8	0x3461	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:47.071774960 CEST	192.168.2.3	8.8.8.8	0xcdcc	Standard query (0)	lh5.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:47.561469078 CEST	192.168.2.3	8.8.8.8	0x84fb	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:48.480464935 CEST	192.168.2.3	8.8.8.8	0xb46b	Standard query (0)	people-pa.clients6.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:48.515523911 CEST	192.168.2.3	8.8.8.8	0xe018	Standard query (0)	0.docs.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:49.664812088 CEST	192.168.2.3	8.8.8.8	0xf502	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.072293043 CEST	192.168.2.3	8.8.8.8	0x9f48	Standard query (0)	contacts.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.263704062 CEST	192.168.2.3	8.8.8.8	0x3b80	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.312258959 CEST	192.168.2.3	8.8.8.8	0x58c	Standard query (0)	lh5.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:54.890546083 CEST	192.168.2.3	8.8.8.8	0x4fd2	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 22:16:54.952629089 CEST	192.168.2.3	8.8.8.8	0xcdcf	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:55.097141027 CEST	192.168.2.3	8.8.8.8	0x285a	Standard query (0)	marketingandsoftwaretools.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:56.356074095 CEST	192.168.2.3	8.8.8.8	0xbf19	Standard query (0)	edadfed.ed.ac.uk	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:56.359100103 CEST	192.168.2.3	8.8.8.8	0x45c3	Standard query (0)	secure.adn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:59.060270071 CEST	192.168.2.3	8.8.8.8	0x1163	Standard query (0)	lh4.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:00.537441969 CEST	192.168.2.3	8.8.8.8	0xb20b	Standard query (0)	lh4.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:00.555650949 CEST	192.168.2.3	8.8.8.8	0xf79f	Standard query (0)	secure.adn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:47.863831043 CEST	192.168.2.3	8.8.8.8	0x56fc	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:47.870500088 CEST	192.168.2.3	8.8.8.8	0x8450	Standard query (0)	docs.google.com	A (IP address)	IN (0x0001)
Oct 26, 2021 22:18:40.922665119 CEST	192.168.2.3	8.8.8.8	0x4ac3	Standard query (0)	0.docs.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 22:16:44.834357023 CEST	8.8.8.8	192.168.2.3	0xf303	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:44.834357023 CEST	8.8.8.8	192.168.2.3	0xf303	No error (0)	clients.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:44.844089985 CEST	8.8.8.8	192.168.2.3	0xc3b0	No error (0)	docs.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:44.844399929 CEST	8.8.8.8	192.168.2.3	0xbaa4	No error (0)	accounts.google.com		172.217.168.13	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:45.959467888 CEST	8.8.8.8	192.168.2.3	0xcb57	No error (0)	gstaticads.l.google.com		172.217.168.35	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:46.095477104 CEST	8.8.8.8	192.168.2.3	0x3461	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:46.095477104 CEST	8.8.8.8	192.168.2.3	0x3461	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:47.098654985 CEST	8.8.8.8	192.168.2.3	0xcdcc	No error (0)	lh5.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:47.098654985 CEST	8.8.8.8	192.168.2.3	0xcdcc	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:47.588434935 CEST	8.8.8.8	192.168.2.3	0x84fb	No error (0)	play.google.com		172.217.168.14	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:48.507356882 CEST	8.8.8.8	192.168.2.3	0xb46b	No error (0)	people-pa.clients6.google.com		172.217.168.10	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:48.554773092 CEST	8.8.8.8	192.168.2.3	0xe018	No error (0)	0.docs.google.com	browserchannel-sites.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:48.554773092 CEST	8.8.8.8	192.168.2.3	0xe018	No error (0)	browserchannel-sites.l.google.com		74.125.143.189	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:49.691487074 CEST	8.8.8.8	192.168.2.3	0xf502	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:49.691487074 CEST	8.8.8.8	192.168.2.3	0xf502	No error (0)	plus.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.099369049 CEST	8.8.8.8	192.168.2.3	0x9f48	No error (0)	contacts.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 22:16:50.099369049 CEST	8.8.8.8	192.168.2.3	0x9f48	No error (0)	plus.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.291081905 CEST	8.8.8.8	192.168.2.3	0x3b80	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:50.291081905 CEST	8.8.8.8	192.168.2.3	0x3b80	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:50.338797092 CEST	8.8.8.8	192.168.2.3	0x58c	No error (0)	lh5.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:50.338797092 CEST	8.8.8.8	192.168.2.3	0x58c	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:54.908595085 CEST	8.8.8.8	192.168.2.3	0x4fd2	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:54.908595085 CEST	8.8.8.8	192.168.2.3	0x4fd2	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:54.970850945 CEST	8.8.8.8	192.168.2.3	0xcdcf	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:54.970850945 CEST	8.8.8.8	192.168.2.3	0xcdcf	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:55.234781027 CEST	8.8.8.8	192.168.2.3	0x285a	No error (0)	marketingandsoftwaretools.com		66.228.55.6	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:56.374308109 CEST	8.8.8.8	192.168.2.3	0xbf19	No error (0)	edadfed.ed.ac.uk		129.215.55.224	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:56.379525900 CEST	8.8.8.8	192.168.2.3	0x45c3	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:56.393471003 CEST	8.8.8.8	192.168.2.3	0xc509	No error (0)	fc6y67oygyo8.wpeprox.com		141.193.213.21	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:56.393471003 CEST	8.8.8.8	192.168.2.3	0xc509	No error (0)	fc6y67oygyo8.wpeprox.com		141.193.213.20	A (IP address)	IN (0x0001)
Oct 26, 2021 22:16:59.087426901 CEST	8.8.8.8	192.168.2.3	0x1163	No error (0)	lh4.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:16:59.087426901 CEST	8.8.8.8	192.168.2.3	0x1163	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:00.575644970 CEST	8.8.8.8	192.168.2.3	0xb20b	No error (0)	lh4.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:17:00.575644970 CEST	8.8.8.8	192.168.2.3	0xb20b	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:00.576242924 CEST	8.8.8.8	192.168.2.3	0xf79f	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:17:00.614655972 CEST	8.8.8.8	192.168.2.3	0x8157	No error (0)	fc6y67oygyo8.wpeprox.com		141.193.213.20	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:00.614655972 CEST	8.8.8.8	192.168.2.3	0x8157	No error (0)	fc6y67oygyo8.wpeprox.com		141.193.213.21	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:47.890844107 CEST	8.8.8.8	192.168.2.3	0x56fc	No error (0)	play.google.com		172.217.168.14	A (IP address)	IN (0x0001)
Oct 26, 2021 22:17:47.897042036 CEST	8.8.8.8	192.168.2.3	0x8450	No error (0)	docs.google.com		172.217.168.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 22:18:40.949260950 CEST	8.8.8.8	192.168.2.3	0x4ac3	No error (0)	0.docs.google.com	browserchannel-sites.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 26, 2021 22:18:40.949260950 CEST	8.8.8.8	192.168.2.3	0x4ac3	No error (0)	browserchannel-sites.l.google.com		74.125.143.189	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- docs.google.com
- clients2.google.com
- accounts.google.com
- https:
 - fonts.gstatic.com
 - lh3.googleusercontent.com
 - apis.google.com
 - contacts.google.com
 - edadfed.ed.ac.uk
- lh5.googleusercontent.com
- bit.ly
- marketingandsoftwaretools.com
- lh4.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	172.217.168.78	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	0	OUT	<pre>GET /document/d/1hHFEB09XYOGm1F87Tdc5etNXb38nGMo/edit?usp=sharing_eip_m&rtpof=true&sd=true&invite=C KvaqcMD&ts=6178419e HTTP/1.1 Host: docs.google.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-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</pre>

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	5	IN	<p>HTTP/1.1 200 OK</p> <p>Content-Type: text/html; charset=utf-8</p> <p>X-Robots-Tag: noindex, nofollow, nosnippet</p> <p>Cache-Control: no-cache, no-store, max-age=0, must-revalidate</p> <p>Pragma: no-cache</p> <p>Expires: Mon, 01 Jan 1990 00:00:00 GMT</p> <p>Date: Tue, 26 Oct 2021 20:16:45 GMT</p> <p>P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."</p> <p>Strict-Transport-Security: max-age=31536000; includeSubDomains</p> <p>Referrer-Policy: strict-origin-when-cross-origin</p> <p>Content-Security-Policy: base-uri 'self';object-src 'none';report-uri https://docs.google.com/document/cspreport;script-src 'report-sample' 'nonce-5uh96NCZrVMPInKS62mGzQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';worker-src 'self' blob;</p> <p>X-Content-Type-Options: nosniff</p> <p>X-XSS-Protection: 1; mode=block</p> <p>Server: GSE</p> <p>Set-Cookie: S=documents=L1867nq6ul72cGaWwyzODuP56_5MPD20-ARVaxlQlwo; Domain=.docs.google.com; Expires= Tue, 26-Oct-2021 21:16:45 GMT; Path=/document/d/1hHFEB09XOgM1F87Todc5etNXb38nGmO; Secure; HttpOnly; Priority=LOW; SameSite=none</p> <p>Set-Cookie: COMPASS=documents=CjIACWuJVvWQU6ufUF3A6o-A74GL60k1qoHskujJKbAr6hXqE2077iEYXO-k eiAbRV3vMRC94OGLBho0AAlriVe4fZZDEzrhTneDxhl_jHuOFofUjo5mfq8pnYrEocXvyNqX_bM2k8vX38qSxrfuw==; Domain=.docs.google.com; Expires=Tue, 26-Oct-2021 21:16:45 GMT; Path=/document/d/1hHFEB09XOgM1F87Todc5etNXb38nGmO; Secure; HttpOnly; Priority=LOW; SameSite=none</p> <p>Set-Cookie: NID=511=Y92BNZ9vutvPx5gYeR8PaBR1g_mjrmCbnEFTAUIP5QU_3dlISckilHC1ufW60kTsfthHGW jfh8tX89A0mP3NPzrSONW4oQZwqfZSyaVggZ0e0Vz6RdOINyVMWlqXMN_dQU9K8Lua7RTR5hqBAFF4A 5J7LsZ4WTk3rzAAALtqY; expires=Wed, 27-Apr-2022 20:16:45 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none</p> <p>Set-Cookie: GFE_RTT=618; Domain=.docs.google.com; Expires=Tue, 26-Oct-2021 20:21:45 GMT; Path=/; Secure; Priority=LOW; SameSite=strict</p> <p>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</p> <p>Accept-Ranges: none</p> <p>Vary: Accept-Encoding</p> <p>Connection: close</p> <p>Transfer-Encoding: chunked</p>
2021-10-26 20:16:45 UTC	7	IN	<p>Data Raw: 31 35 64 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 47 42 22 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 35 75 68 39 36 4e 43 5a 72 56 4d 50 49 6e 4b 53 36 32 6d 47 7a 51 22 3e 76 61 72 20 44 4f 43 53 5f 74 69 6d 69 6e 67 3d 7b 7d 3b 20 44 4f 43 53 5f 74 69 6d 69 6e 67 5b 27 70 6c 73 27 5d 3d 6e 65 77 20 44 61 74 65 28 29 2e 67 65 74 54 69 6d 65 28 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 6d 65 74 61 20 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 41 64 6a 75 6e 63 74 20 45 76 61 6c 75 61 74 69 6f 6e 20 28 32 29 2e 64 6f 63 78 22 3e 3c 6d 65 74 61 20 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 61 72 74</p> <p>Data Ascii: 15d5<!DOCTYPE html><html lang="en-GB"><head><script nonce="5uh96NCZrVMPInKS62mGzQ">var D OCS_timing={}; DOCS_timing[pls]=new Date().getTime();</script><meta property="og:title" content="Adjunct Evaluation (2).docx"><meta property="og:type" content="art</p>
2021-10-26 20:16:45 UTC	9	IN	<p>Data Raw: 22 73 75 62 73 65 74 22 3a 22 2a 22 7d 2c 22 43 61 6c 69 62 72 69 2d 34 30 30 2d 69 74 61 6c 69 63 22 3a 7b 22 66 6f 6e 74 46 61 6d 69 6c 79 22 3a 22 64 6f 63 73 2d 43 61 6c 69 62 72 69 2d 2c 22 73 6f 75 72 63 65 53 74 72 69 6e 67 22 3a 22 6c 6f 63 61 6c 28 5c 75 30 30 32 37 43 61 6c 69 62 72 69 2d 49 74 61 6c 69 63 5c 75 30 30 32 37 29 2c 20 75 72 6c 28 66 69 6c 65 73 79 73 74 65 6d 3a 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 70 65 72 73 69 73 74 65 6e 74 2f 64 6f 63 73 2f 66 6f 6e 74 73 2f 4a 37 61 64 6e 70 56 2d 42 47 6c 61 46 66 64 41 68 4c 51 59 36 77 2e 77 6f 66 66 32 29 2c 20 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67</p> <p>Data Ascii: "subset":{},"Calibri-400-italic":{"fontFamily":"docs-Calibri","sourceString":"local(\u0027Calibri Italic\u0027), local(\u0027Calibri-Italic\u0027), url(filesystem:https://docs.google.com/persistent/docs/fonts/J7adnpV-BGlaFfdAHLQY6w.woff 2), url(/fonts.g</p>
2021-10-26 20:16:45 UTC	11	IN	<p>Data Raw: 6f 20 53 61 6e 73 2d 37 30 30 2d 6e 6f 72 6d 61 6c 22 3a 7b 22 66 6f 6e 74 46 61 6d 69 6c 79 22 3a 22 64 6f 63 73 2d 51 75 61 74 74 72 6f 63 65 6e 74 6f 20 53 61 6e 73 22 2c 22 73 6f 75 72 63 65 53 74 72 69 6e 67 22 3a 22 6c 6f 63 61 6c 28 5c 75 30 30 32 37 51 75 61 74 74 72 6f 63 65 6e 74 6f 20 53 61 6e 73 20 42 6f 6c 64 5c 75 30 30 32 37 29 2c 20 6c 6f 63 61 6c 28 5c 75 30 30 32 37 51 75 61 74 74 72 6f 63 65 6e 74 6f 53 61 6e 73 2d 42 6f 6c 64 5c 75 30 30 32 37 29 2c 20 75 72 6c 28 66 69 6c 65 73 79 73 74 65 6d 3a 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 70 65 72 73 69 73 74 65 6e 74 2f 64 6f 63 73 2f 66 6f 6e 74 73 2f 7f 61 39 5a 34 6c 6a 61 32 4e 56 49 44 64 49 41 41 6f 4d 52 35 4d 66 75 45 6c 61 52 42 30 52 79 6b 6d 72</p> <p>Data Ascii: o Sans-700-normal":{"fontFamily":"docs-Quattrocento Sans","sourceString":"local(\u0027Quattrocento Sans Bold\u0027), local(\u0027QuattrocentoSans-Bold\u0027), url(filesystem:https://docs.google.com/persistent/docs/font s/va9Z4ja2NVIDIAA0MR5MfuElARBORykmr</p>
2021-10-26 20:16:45 UTC	12	IN	<p>Data Raw: 31 33 39 64 0d 0a 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 35 75 68 39 36 4e 43 5a 72 56 4d 50 49 6e 4b 53 36 32 6d 47 7a 51 22 3e 5f 64 6f 63 73 5f 66 6c 61 67 5f 69 6e 69 74 69 61 6c 44 61 74 61 3d 7b 22 64 6f 63 73 2d 61 69 6c 73 22 3a 22 64 6f 63 73 5f 63 6f 6c 64 22 2c 22 64 6f 63 73 2d 66 77 64 73 22 3a 22 64 6f 63 73 5f 6e 66 22 2c 22 64 6f 63 73 2d 63 72 73 22 3a 22 64 6f 63 73 5f 63 72 73 5f 6e 6c 6f 22 2c 22 64 6f 63 73 2d 64 65 63 73 22 3a 31 2c 22 64 6f 63 73 2d 73 68 64 6e 22 3a 31 30 35 2c 22 64 6f 63 73 2d 74 66 68 22 3a 22 2c 22 2c 22 69 6e 66 6f 5f 70 61 72 61 6d 73 22 3a 7b 22 69 6e 76 69 74 65 22 3a 22 43 4b 76 61 71 63 4d 44 22 2c 22 69 6e 63 6c 75 64 65 73 5f 69 6e 66 6f 5f 70 61 72 61 6d 73 22 3a 74 72 75 65 7d 2c 22 64 6f 63 73 2d</p> <p>Data Ascii: 139d<script nonce="5uh96NCZrVMPInKS62mGzQ">_docs_flag_initialData={"docs-ails":"docs_cold","docs-f wds":"docs_nf","docs-crs":"docs_crs_nlo","docs-decs":"1","docs-shdn":"105","docs-tfh":"","info_params":{"invite":"CKvaqcMD", "includes_info_params":true},"docs-</p>
2021-10-26 20:16:45 UTC	14	IN	<p>Data Raw: 6f 74 6f 20 53 6c 61 62 22 2c 22 52 61 6c 65 77 61 79 22 2c 22 4f 70 65 6e 20 53 61 6e 73 22 2c 22 4f 73 77 61 6c 64 22 2c 22 41 6d 61 74 69 63 20 53 43 22 2c 22 53 6f 75 72 63 65 20 53 61 6e 73 20 50 72 6f 22 2c 22 52 6f 62 6f 74 6f 22 2c 22 45 63 6f 6e 6f 6d 69 63 61 22 2c 22 52 65 65 6e 69 65 20 42 65 65 6e 69 65 22 2c 22 53 74 69 6e 74 20 55 6c 74 72 61 20 45 78 70 61 6e 64 65 64 22 2c 22 41 6c 65 67 72 65 79 61 22 2c 22 4d 65 72 72 69 77 65 61 74 68 65 72 22 5d 2c 22 64 66 66 64 22 3a 5b 22 43 61 6c 69 62 72 69 22 2c 22 43 61 6d 62 72 69 61 22 2c 22 53 79 6e 63 6f 70 61 74 65 22 2c 22 4c 6f 62 73 74 65 72 22 2c 22 43 6f 72 73 69 76 61 22 2c 22 43 6f 6d 69 6e 67 20 53 6f 6f 6e 22 2c 22 53 68 61 64 6f 77 73 20 49 6e 74 6f 20 4c 69 67 68 74 22 2c 22 49</p> <p>Data Ascii: oto Slab","Raleway","Open Sans","Oswald","Amatic SC","Source Sans Pro","Roboto","Economica","Reenie Beenie","Stint Ultra Expanded","Alegreya","Merriweather"],"dfid":{"Calibri","Cambria","Syncopate"},"Lobster","Corsiva", "Coming Soon","Shadows Into Light","I</p>

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	25	IN	Data Raw: 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 74 61 66 6c 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 65 73 61 72 75 22 3a 22 68 74 74 70 73 3a 2f 2f 65 6e 74 65 72 70 72 69 73 65 73 65 61 72 63 68 2d 70 61 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 65 78 70 6c 6f 72 65 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 65 66 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 6d 6f 64 6f 22 3a 30 2c 22 64 6f 63 73 2d 65 65 65 73 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 65 72 69 73 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 65 72 69 73 66 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 64 65 6e 73 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 65 72 69 73 64 64 22 3a 66 61 6c 73 65 2c 22 64 6f Data Ascii: ".false","docs-taff":true,"docs-eesaru":"https://enterprisesearch-pa.googleapis.com","docs-explore":true,"docs-eeef":false,"docs-emodo":0,"docs-eees":false,"docs-eeris":false,"docs-eerisf":false,"docs-dens":false,"docs-erispe":false,"docs-eerisdd":false,"do
2021-10-26 20:16:45 UTC	26	IN	Data Raw: 2c 22 64 6f 63 73 2d 68 77 67 22 3a 22 22 2c 22 64 6f 63 73 2d 68 77 73 74 22 3a 22 4e 35 75 34 56 65 57 68 78 30 69 53 46 54 43 62 69 45 42 30 56 55 54 4e 64 58 36 67 22 2c 22 64 6f 63 73 2d 6e 64 74 22 3a 22 55 6e 74 69 74 6c 65 64 20 64 6f 63 75 6d 65 6e 74 22 2c 22 64 6f 63 73 2d 70 6c 75 22 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 64 6f 63 73 2f 63 6f 6d 6f 6e 2f 70 72 6f 64 75 63 74 2f 64 6f 63 73 5f 6c 6f 63 6b 75 70 32 2e 70 6e 67 22 2c 22 64 6f 63 73 2d 70 6c 77 74 75 22 3a 22 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 64 6f 63 73 2f 63 6f 6d 6f 6e 2f 70 72 6f 64 75 63 74 2f 64 6f 63 73 5f 61 70 70 5f 69 63 6f 6e 31 2e 70 6e 67 22 2c 22 64 6f 63 73 2d 70 72 6e 22 3a 22 47 6f 6f 67 6c 65 20 44 6f 63 73 22 2c 22 Data Ascii: ", "docs-hwg":"", "docs-hwst":"N5u4VeWhx0iSFTCbIEB0VUTNdX6g", "docs-ndt":"Untitled document", "docs-plu":"//ssl.gstatic.com/docs/common/product/docs_lockup2.png", "docs-plwtu":"//ssl.gstatic.com/docs/common/product/docs_app_icon1.png", "docs-prn":"Google Docs", "
2021-10-26 20:16:45 UTC	28	IN	Data Raw: 6f 63 73 2d 65 63 75 72 66 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 66 73 69 69 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 74 65 78 74 2d 65 6c 6e 6d 61 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 6c 63 66 64 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 64 6d 69 74 6d 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 69 72 22 3a 74 72 75 65 2c 22 73 65 72 76 65 72 5f 74 69 6d 65 5f 6d 73 22 3a 31 36 33 35 32 37 39 34 30 35 36 34 37 2c 22 67 61 69 61 5f 73 65 73 73 69 6f 6e 5f 69 64 22 3a 22 22 2c 22 61 70 70 2d 62 63 22 3a 22 23 34 32 38 35 66 34 22 2c 22 65 6e 61 62 6c 65 5f 69 66 72 61 6d 65 64 5f 65 6d 62 65 64 5f 61 70 69 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 66 75 74 22 Data Ascii: ocs-ecurf":true,"docs-efsii":true,"docs-text-elnma":true,"docs-elcfd":false,"docs-edmitm":false,"docs-enjec":true,"ecid":true,"docs-eir":true,"server_time_ms":1635279405647,"gaia_session_id":"","app-bc":"#4285f4","enable_iframed_embed_api":true,"docs-fue"
2021-10-26 20:16:45 UTC	29	IN	Data Raw: 6e 2f 6d 73 77 6f 72 64 22 5d 2c 22 64 6f 63 73 2d 70 6f 22 3a 22 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 74 6f 22 3a 22 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 65 61 73 74 64 22 3a 74 72 75 65 2c 22 6f 70 65 6e 64 76 22 3a 74 72 75 65 2c 22 6f 6e 65 50 69 63 6b 49 6d 70 6f 72 74 44 6f 63 75 6d 65 6e 74 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 70 69 63 6b 65 72 3f 70 72 6f 74 6f 63 6f 6c 5c 75 30 33 64 67 61 64 67 63 74 73 5c 75 30 32 36 70 61 72 65 6e 74 5c 75 30 33 64 68 74 74 70 73 3a 2f 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 72 65 6c 61 79 2e 68 74 6d 6c 5c 75 30 30 32 36 68 6f Data Ascii: n/msword"], "docs-po":"https://docs.google.com", "docs-to":"https://docs.google.com", "docs-eastd":true, "opendv":true, "onePickImportDocumentUrl":"https://docs.google.com/picker?protocolu003dgadgetsu0026parentu003dhttps://docs.google.com/relay.htmlu0026ho
2021-10-26 20:16:45 UTC	30	IN	Data Raw: 31 61 34 34 0d 0a 3f 6d 69 64 5c 75 30 30 33 64 41 43 6a 50 4a 76 45 47 51 4b 51 41 33 39 47 4f 53 74 6c 2d 5a 69 32 74 6e 76 78 75 30 6c 6b 77 54 5f 76 54 53 4b 6c 74 4f 64 32 77 6a 78 63 5a 56 77 74 43 63 70 71 34 30 67 75 63 39 75 65 75 45 6d 41 76 51 73 78 70 41 4f 34 67 43 37 55 33 31 6d 4a 48 53 57 49 6a 31 6a 36 41 77 7a 6e 48 4a 48 56 67 4c 47 39 50 59 46 55 64 37 41 63 75 35 51 5c 75 30 30 32 36 75 69 76 5c 75 30 33 64 32 22 2c 22 6d 61 65 73 74 72 6f 5f 6e 65 77 5f 70 72 6f 6a 65 63 74 5f 75 72 69 22 3a 22 68 74 74 70 73 3a 2f 2f 73 63 72 69 70 74 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 6d 61 63 72 6f 73 2f 63 72 65 61 74 65 3f 6d 69 64 5c 75 30 30 33 64 41 43 6a 50 4a 76 45 47 51 4b 51 41 33 39 47 4f 53 74 6c 2d 5a 69 32 74 6e 76 78 75 30 6c 6b Data Ascii: 1a44?midu003dACjPJvEGQKQA39GOSit-Zi2tnvxu0lkWt_vtSKltOd2wjxcZVwtCcpq40guc9ueuEmAvQsxpAO4gC7U31mJHSWj1j6AwznHJHVgLG9PYfUd7Acu5Qlu0026uivv003d2","maestro_new_project_uri":"https://script.google.com/macros/create?midu003dACjPJvEGQKQA39GOSit-Zi2tnvxu0lk
2021-10-26 20:16:45 UTC	31	IN	Data Raw: 64 22 3a 22 64 6f 63 73 2e 67 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 65 64 74 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 68 64 63 6b 22 3a 22 22 2c 22 64 6f 63 73 2d 68 75 63 73 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 68 75 66 63 6d 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 68 75 6e 63 61 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 63 62 72 73 22 3a 35 30 2c 22 64 6f 63 73 2d 63 61 72 75 22 3a 22 68 74 74 70 73 3a 2f 2f 63 6c 69 65 6e 74 73 36 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 63 62 61 75 22 3a 22 68 74 74 70 73 3a 2f 2f 64 72 69 76 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 63 66 72 75 22 3a 22 68 74 74 70 73 3a 2f 2f 6c 68 33 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 64 6f 63 73 2d 63 74 61 6b 22 3a 22 41 49 7a Data Ascii: d":"docs.google.com", "docs-edt":true, "docs-hdck":"","docs-hucs":true, "docs-hufcm":false, "docs-hunca":true, "docs-cbrs":50, "docs-caru":"https://clients6.google.com", "docs-cbau":"https://drive.google.com", "docs-cfru":"https://lh3.google.com", "docs-ctak":"Alz
2021-10-26 20:16:45 UTC	32	IN	Data Raw: 6c 73 65 2c 22 64 6f 63 73 2d 62 68 75 69 74 6d 22 3a 31 32 30 30 30 30 2e 30 2c 22 64 6f 63 73 2d 65 68 73 72 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 68 70 6d 22 3a 31 38 30 30 30 30 2e 30 2c 22 64 6f 63 73 2d 62 68 62 63 69 74 6d 22 3a 31 32 30 30 30 30 2e 30 2c 22 64 6f 63 73 2d 65 68 62 63 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 61 69 69 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 61 66 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 61 63 74 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 61 63 22 3a 22 5b 5c 22 64 6f 63 73 5f 61 6e 61 6c 79 74 69 63 73 5f 63 61 70 61 62 69 6c 69 74 69 65 73 5c 22 5d 22 2c 22 64 6f 63 73 2d 65 6f 64 72 73 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 61 6f 70 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 61 73 68 74 22 3a 22 22 2c Data Ascii: lse,"docs-bhuitm":1200000.0,"docs-ehsr":true,"docs-hpm":1800000.0,"docs-bhbcitm":1200000.0,"docs-ehbc":true,"docs-aii":true,"docs-af":false,"docs-act":false,"docs-ac":["docs_analytics_capabilities"],"docs-eodrs":false,"docs-eaop":false,"docs-asht":"","
2021-10-26 20:16:45 UTC	34	IN	Data Raw: 61 6f 61 6b 22 3a 22 22 2c 22 67 73 61 6f 69 75 22 3a 22 68 74 74 70 73 3a 2f 2f 61 64 64 6f 6e 73 2e 67 73 75 69 74 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 63 6c 69 65 6e 74 22 2c 22 65 67 61 73 6f 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 61 69 66 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 61 69 66 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 63 6f 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 63 6f 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 63 6f 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 65 67 73 61 6f 63 61 22 3a 74 72 75 65 2c 22 64 6f 63 73 2d 67 61 61 6f 69 22 3a 5b 5d 2c 22 64 6f 63 73 2d 65 67 66 22 3a 66 61 6c 73 65 2c 22 64 6f 63 73 2d 63 73 65 2d 61 73 69 22 3a 33 30 30 2c 22 64 6f 63 73 2d 63 73 65 2d 61 73 69 74 22 3a 33 30 2c 22 64 6f 63 73 2d 63 73 65 2d Data Ascii: aoak":"","gsauiu":"https://addons.gsuite.google.com/client", "egaso":true, "docs-egsaoaif":true, "docs-egsaoac":true, "docs-egsaooco":true, "docs-egsaoos":false, "docs-egsaoasa":true, "docs-gaai":[], "docs-egf":false, "docs-cse-asi":300, "docs-cse-asit":30, "docs-cse-

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	54	IN	Data Raw: 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 31 30 30 2d 30 32 34 46 2c 55 2b 30 32 35 39 2c 55 2b 31 45 30 30 2d 31 45 46 46 2c 55 2b 32 30 32 30 2c 55 2b 32 30 41 30 2d 32 30 41 42 2c 55 2b 32 30 41 44 2d 32 30 43 46 2c 55 2b 32 31 31 33 2c 55 2b 32 43 36 30 2d 32 43 37 46 2c 55 2b 41 37 32 30 2d 41 37 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 47 6f 6f 67 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 69 74 61 6c 69 63 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 67 6f 6f 67 6c 65 73 61 6e 73 2f 76 31 34 2f 34 55 61 5a 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 33 4c 2d 69 64 78 4f 77 52 6d Data Ascii: nicode-range:U+0100-024F,U+0259,U+1E00-1EFF,U+2020,U+20A0-20AB,U+20AD-20CF,U+2113,U+2C60-2C7F,U+A720-A7FF;@font-face{font-family:'Google Sans';font-style:italic;font-weight:700;src:url(//fonts.gstatic.com/s/googlesans/v14/UaZrENHsxJIGDuGo1OILL3L-idxOwRm
2021-10-26 20:16:45 UTC	56	IN	Data Raw: 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 31 30 30 2d 30 32 34 46 2c 55 2b 30 32 35 39 2c 55 2b 31 45 30 30 2d 31 45 46 46 2c 55 2b 32 30 32 30 2c 55 2b 32 30 41 30 2d 32 30 41 42 2c 55 2b 32 30 41 44 2d 32 30 43 46 2c 55 2b 32 31 31 33 2c 55 2b 32 43 36 30 2d 32 43 37 46 2c 55 2b 41 37 32 30 2d 41 37 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 47 6f 6f 67 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 67 6f 6f 67 6c 65 73 61 6e 73 2f 76 31 34 2f 34 55 61 47 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 33 4f 77 70 34 2e 77 6f 66 66 32 29 Data Ascii: code-range:U+0100-024F,U+0259,U+1E00-1EFF,U+2020,U+20A0-20AB,U+20AD-20CF,U+2113,U+2C60-2C7F,U+A720-A7FF;@font-face{font-family:'Google Sans';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/googlesans/v14/UaGrENHsxJIGDuGo1OILL3Owp4.woff2)
2021-10-26 20:16:45 UTC	57	IN	Data Raw: 33 36 38 61 0d 0a 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 55 39 34 59 74 38 43 77 5a 2d 50 77 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 7f 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 31 30 32 2d 30 31 30 33 2c 55 2b 30 31 31 30 2d 30 31 31 31 2c 55 2b 30 31 32 38 2d 30 31 32 39 2c 55 2b 30 31 41 30 2d 30 31 41 31 2c 55 2b 30 31 41 46 2d 30 31 42 30 2c 55 2b 31 45 41 30 2d 31 45 46 39 2c 55 2b 32 30 41 42 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 47 6f 6f 67 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 Data Ascii: 368arENHsxJIGDuGo1OILLU94Yt8CwZ-Pw.woff2)format(woff2);unicode-range:U+0102-0103,U+0110-0111,U+0128-0129,U+0168-0169,U+01A0-01A1,U+01AF-01B0,U+1EA0-1EF9,U+20AB;@font-face{font-family:'Google Sans';font-style:normal;font-weight:500;src:url(//fonts.gst
2021-10-26 20:16:45 UTC	58	IN	Data Raw: 6f 67 6c 65 73 61 6e 73 2f 76 31 34 2f 34 55 61 62 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 56 31 35 34 74 38 43 77 5a 2d 50 77 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 7f 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 31 30 32 2d 30 31 30 33 2c 55 2b 30 31 31 30 2d 30 31 31 31 2c 55 2b 30 31 32 38 2d 30 31 32 39 2c 55 2b 30 31 36 38 2d 30 31 41 30 2d 30 31 41 31 2c 55 2b 30 31 41 46 2d 30 31 42 30 2c 55 2b 31 45 41 30 2d 31 45 46 39 2c 55 2b 32 30 41 42 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 47 6f 6f 67 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 3b 73 72 63 3a 75 72 6c 28 Data Ascii: oglesans/v14/UabrENHsxJIGDuGo1OILLV154t8CwZ-Pw.woff2)format(woff2);unicode-range:U+0102-0103,U+0110-0111,U+0128-0129,U+0168-0169,U+01A0-01A1,U+01AF-01B0,U+1EA0-1EF9,U+20AB;@font-face{font-family:'Google Sans';font-style:normal;font-weight:700;src:url(
2021-10-26 20:16:45 UTC	59	IN	Data Raw: 65 6e 67 74 68 26 26 28 64 3d 62 2e 73 68 69 66 74 28 29 29 3b 29 62 2e 6c 65 6e 67 74 68 7c 7c 7e 6f 69 64 20 30 3d 3d 3d 61 3f 63 5b 64 5d 26 26 63 5b 64 5d 21 3d 3d 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 5b 64 5d 3f 63 3d 63 5b 64 5d 3a 63 3d 63 5b 64 5d 3d 7b 7d 3a 63 5b 64 5d 3d 61 3b 7d 29 2e 63 61 6c 6c 28 74 68 69 73 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 35 75 68 39 36 4e 43 5a 72 56 4d 50 49 6e 4b 53 36 32 6d 47 7a 51 22 3e 44 4f 43 53 5f 61 74 74 61 63 68 49 6e 69 74 69 61 6c 4d 61 74 65 72 69 61 6c 46 6f 6e 74 4c 6f 61 64 4c 69 73 74 65 6e 65 72 28 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 74 79 6c 65 3e 2f 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 32 31 20 47 6f 6f 67 6c 65 20 49 6e 63 2e 20 41 Data Ascii: ength&&(d=b.shift());b.length void 0===a?c[d]&&c[d]===Object.prototype[d]?c=c[d]:c=c[d]={}:c[d]=a;).call(this);</script><script nonce="5uh96NCZrVMPInKS62mGzQ">DOCS_attachInitialMaterialFontLoadListener();</script><style>/* Copyright 2021 Google Inc. A
2021-10-26 20:16:45 UTC	60	IN	Data Raw: 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 76 61 72 20 69 66 72 61 6d 65 20 3d 20 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 6b 69 78 2d 68 69 64 64 65 6e 2d 69 66 72 61 6d 65 27 29 3b 20 76 61 72 20 69 66 72 61 6d 65 44 6f 63 75 6d 65 6e 74 20 3d 20 69 66 72 61 6d 65 20 3f 20 69 66 72 61 6d 65 2e 63 6f 6e 74 65 6e 74 44 6f 63 75 6d 65 6e 74 20 7c 7c 20 69 66 72 61 6d 65 2e 63 6f 6e 74 65 6e 74 57 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 20 3a 20 6e 75 6c 6c 3b 20 5f 64 6f 63 73 5f 77 65 62 66 6f 6e 74 73 5f 69 66 72 61 6d 65 5f 66 6f 6e 74 46 61 63 65 73 20 3d 20 5f 64 6f 63 73 5f 77 65 62 66 6f 6e 74 73 5f 63 72 65 61 74 65 46 6f 6e 74 46 61 63 65 73 28 69 66 72 61 6d 65 44 6f 63 75 6d 65 6e 74 29 3b 7d Data Ascii: (function() {var iframe = window.document.getElementById('kix-hidden-iframe'); var iframeDocument = iframe ? iframe.contentDocument iframe.contentWindow.document : null; _docs_webfonts_iframe_fontFaces = _docs_webfontnts_createFontFaces(iframeDocument);}
2021-10-26 20:16:45 UTC	62	IN	Data Raw: 76 61 72 20 63 6f 6e 74 65 6e 74 73 53 74 72 69 6e 67 20 3d 20 22 5c 78 33 63 6c 69 6e 6b 20 72 65 6c 5c 78 33 64 5c 78 32 32 73 74 79 6c 65 73 68 65 65 74 5c 78 32 32 20 68 72 65 66 5c 78 33 64 5c 78 32 32 68 74 70 73 3a 5c 2f 5c 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 5c 2f 63 73 73 3f 66 61 6d 69 6c 79 5c 78 33 64 47 6f 6f 67 6c 65 2b 53 61 6e 73 3a 62 6f 6c 64 2c 6e 6f 72 6d 61 6c 5c 78 32 36 6c 61 6e 67 5c 78 33 64 65 6e 5c 78 32 32 20 6e 6f 6e 63 65 5c 78 33 64 5c 78 32 32 64 67 62 78 72 41 65 34 48 64 48 38 46 4e 43 70 72 51 6b 4d 77 67 5c 78 32 32 5c 78 33 65 5c 78 33 63 6c 69 6e 6b 20 72 65 6c 5c 78 33 64 5c 78 32 32 73 74 79 6c 65 73 68 65 65 74 5c 78 32 32 20 68 72 65 66 5c 78 33 64 5c 78 32 32 68 74 74 70 73 3a 5c 2f Data Ascii: var contentsString = "\x3cclink rel\x3dx3d\x22stylesheet\x22 href\x3dx3d\x22https://fonts.googleapis.com/vcss?famiily\x3dGoogle+Sans:bold,normal\x26lang\x3den\x22 nonce\x3dx3d\x22dgbxrAe4HdH8FNCPrQkMwglx22\x3elx3cclink rel\x3dx3d\x22stylesheet\x22 href\x3dx3d\x22https://
2021-10-26 20:16:45 UTC	63	IN	Data Raw: 3b 66 6c 6f 61 74 3a 72 69 67 68 74 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 68 65 69 67 68 74 3a 32 34 70 78 5c 78 37 64 70 23 63 68 72 6f 6d 65 2d 75 72 6c 2d 62 6f 78 20 63 6f 64 65 5c 78 37 62 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 66 6c 6f 61 74 3a 6c 65 66 74 3b 68 65 69 67 68 74 3a 32 34 70 78 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 5c 78 37 37 20 63 62 75 74 74 6f 6e 73 2d 72 6f 77 5c 78 37 62 74 65 78 74 2d 61 6c 69 67 6e 3a 72 69 67 68 74 5c 78 37 64 70 23 62 75 74 74 6f 6e 73 2d 72 6f 77 20 62 75 74 74 6f 6e 5c 78 37 62 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 36 70 78 5c 78 37 64 62 75 74 74 6f 6e 2e 74 65 78 74 2d 62 75 74 74 6f 6e 5c 78 37 62 66 Data Ascii: ;float:right;background:none;height:24px!x7dp#chrome-url-box code!x7bfont-family:inherit;display:block;float:left;height:24px;vertical-align:middle!x7dp#buttons-row!x7btext-align:right!x7dp#buttons-row button!x7bmargin-left:16px!x7dbutton.text-button!x7bf

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	73	IN	Data Raw: 65 72 73 69 6f 6e 3d 22 31 2e 31 22 20 63 6c 61 73 73 3d 22 6b 69 78 2d 73 70 65 6c 6c 69 6e 67 2d 65 72 72 6f 72 2d 70 61 74 74 65 72 6e 20 64 6f 63 73 2d 6f 66 66 73 63 72 65 65 6e 2d 7a 2d 69 6e 64 65 78 22 3e 3c 64 65 66 73 3e 3c 70 61 74 74 65 72 6e 20 69 64 3d 22 6b 69 78 2d 73 70 65 6c 6c 69 6e 67 2d 7a 69 67 7a 61 67 22 20 77 69 64 74 68 3d 22 34 22 20 68 65 69 67 68 74 3d 22 35 22 20 70 61 74 74 65 72 6e 55 6e 69 74 73 3d 22 75 73 65 72 53 70 61 63 65 4f 6e 55 73 65 22 3e 3c 70 61 74 68 20 64 3d 22 4d 20 30 20 33 20 4c 20 32 20 31 20 4c 20 34 20 33 22 20 73 74 72 6f 6b 65 3d 22 72 67 62 61 28 32 35 35 2c 32 35 35 2c 32 35 35 2c 3e 38 35 29 22 20 73 74 72 6f 6b 65 2d 77 69 64 74 6 8 3d 22 31 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 20 73 74 72 6f Data Ascii: erision="1.1" class="kix-spelling-error-pattern docs-offscreen-z-index"><defs><pattern id="kix-spelling-zigzag" width="4" height="5" patternUnits="userSpaceOnUse"><path d="M 0 3 L 2 1 L 4 3" stroke="rgba(255,255,255,0.85)" stroke-width="1" fill="none" stro
2021-10-26 20:16:45 UTC	74	IN	Data Raw: 2d 75 6e 70 72 69 6e 74 61 62 6c 65 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 22 64 6f 63 73 2d 73 70 65 6c 63 68 65 63 6b 73 6c 69 64 69 6e 67 64 69 61 6c 6f 67 2d 69 64 22 20 63 6c 61 73 73 3d 22 64 6f 63 73 2d 75 69 2d 75 6e 70 72 69 6e 74 61 62 6c 65 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 22 64 6f 63 73 2d 63 68 65 63 6b 75 70 64 69 61 6c 6f 67 2d 69 64 22 20 63 6c 61 73 73 3d 22 64 6f 63 73 2d 75 69 2d 75 6e 70 72 69 6e 74 61 62 6c 65 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 69 64 3d 22 6b 69 78 2d 68 6f 72 69 7a 6f 6e 74 61 6c 2d Data Ascii: -unprintable"></div><div id="docs-spellcheckslidingdialog-id" class="docs-ui-unprintable"></div><div id="docs-checkupdialog-id" class="docs-ui-unprintable"></div><div id="docs-suggestioindialog-id" class="docs-ui-unprintable"></div><div id="kix-horizontal-
2021-10-26 20:16:45 UTC	75	IN	Data Raw: 72 44 69 61 6c 6f 67 28 29 20 3a 20 28 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 27 68 74 74 70 73 3a 5c 2f 5c 2f 73 75 70 70 6f 72 74 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 5c 2f 61 63 63 6f 75 6e 74 73 5c 2f 61 6e 73 77 65 72 5c 2f 33 32 30 35 30 27 29 29 7d 44 4f 43 53 5f 69 6e 69 74 69 61 6c 6f 64 75 6c 65 73 28 7b 22 6b 69 78 5f 63 6f 72 65 22 3a 5b 5d 2c 22 6b 69 78 5f 61 70 70 22 3a 5b 22 6b 69 78 5f 63 6f 72 65 22 5d 2c 22 6b 69 78 5f 63 61 6e 76 61 73 22 3a 5b 22 6b 69 78 5f 63 6f 72 65 22 5d 2c 22 6b 69 78 5f 61 70 70 22 5d 2c 22 6b 69 78 5f 74 65 72 74 69 61 72 79 22 3a 5b 22 6b 69 78 5f 61 70 70 22 5d 2c 22 61 64 64 5f 6f 6e 73 5f 61 70 70 5f 66 69 6e 64 65 72 5f 70 6f 70 Data Ascii: rDialog() : (window.location.href = 'https://Vsupport.google.com/Vaccounts/Vanswer/32050'))DOCS_initializeModules({"kix_core":"","kix_app":{"kix_core":"","kix_canvas":{"kix_core":"","kix_jstex":{"kix_app"},"kix_tertiary":{"kix_app"},"add_ons_app_finder_pop
2021-10-26 20:16:45 UTC	77	IN	Data Raw: 78 5f 74 65 72 74 69 61 72 79 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 31 32 32 32 32 36 30 34 39 34 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 79 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 61 64 64 5f 6f 6e 73 5f 61 70 70 5f 66 69 6e 64 65 72 5f 70 6f 70 75 6c 61 74 6f 72 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 31 31 34 32 34 37 37 37 33 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 61 64 64 5f 6f 6e 73 5f 61 70 70 5f 66 69 6e 64 65 72 5f 70 6f 70 75 6c 61 74 6f 72 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 61 64 64 5f 6f 6e 73 5f 68 6f 73 74 5f 63 6f 6e 74 65 6e 74 5f 6f 61 63 74 6f 72 79 22 3a 5b 22 2f 73 74 61 Data Ascii: x_tertiary":["/static/document/client/js/1222260494-client_js_prod_kix_tertiary__en_gb.js"],"add_ons_app_finder_populator":["/static/document/client/js/114247773-client_js_prod_add_ons_app_finder_populator__en_gb.js"],"add_ons_host_content_factory":["/sta
2021-10-26 20:16:45 UTC	78	IN	Data Raw: 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6d 65 65 74 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2f 63 6c 69 65 6e 74 2f 6a 73 2f 33 37 31 34 38 38 31 34 39 2d 63 6c 69 65 6e 74 5f 6a 73 5f 70 72 6f 64 5f 6b 69 78 5f 74 65 72 74 69 61 72 6f 64 5f 6b 69 78 5f 77 65 62 5f 77 6f 72 6b 65 72 5f 5f 65 6e 5f 67 62 2e 6a 73 22 5d 2c 22 6f 66 66 69 63 65 65 64 69 74 69 6e 67 66 69 6c 65 65 78 74 65 6e 73 69 6f 6e 22 3a 5b 22 2f 73 74 61 74 69 63 2f 64 6f 63 75 6d 65 6e 74 2

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	83	IN	Data Raw: 64 22 3a 66 61 6c 73 65 2c 22 70 73 5f 70 62 62 22 3a 66 61 6c 73 65 2c 22 70 73 5f 62 72 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6b 6c 74 22 3a 74 72 75 65 2c 22 70 73 5f 62 74 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 68 64 22 3a 30 2c 22 70 73 5f 6b 77 6e 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 69 66 6c 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 74 73 22 3a 7b 22 63 76 22 3a 7b 22 6f 70 22 3a 22 73 65 74 22 2c 22 6f 70 56 61 6c 75 65 2c 22 3a 5b 5d 7d 7d 2c 22 70 73 5f 62 62 74 77 22 3a 6e 75 6c 6c 2c 22 70 73 5f 6c 73 6c 6d 22 3a 30 2c 22 70 73 5f 62 62 22 3a 6e 75 6c 6c 2c 22 70 73 5f 6c 73 22 3a 31 2e 31 35 2c 22 70 73 5f 62 6c 22 3a 6e 75 6c 6c 2c 22 70 73 5f 6b 77 6e 22 3a 74 72 75 65 2c 22 70 73 5f 73 6d 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 69 6c 5f 69 Data Ascii: d:"false","ps_pbb":false,"ps_br_i":true,"ps_klt":true,"ps_bt_i":true,"ps_hd":0,"ps_kwn_i":false,"ps_ifl_i":true,"ps_ts":{"cv":{"op":"set"},"opValue":{}},"ps_bbtw":null,"ps_lslm":0,"ps_bb":null,"ps_ls":1.15,"ps_bl":null,"ps_kwn":true,"ps_sm_i":true,"ps_il_i
2021-10-26 20:16:45 UTC	84	IN	Data Raw: 22 3a 74 72 75 65 2c 22 70 73 5f 73 64 22 3a 6e 75 6c 6c 2c 22 70 73 5f 62 74 22 3a 6e 75 6c 6c 2c 22 70 73 5f 68 64 69 64 22 3a 22 22 2c 22 70 73 5f 6c 73 6c 6d 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 6d 22 3a 30 2c 22 70 73 5f 62 62 74 77 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 61 6c 22 3a 30 2c 22 70 73 5f 62 62 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 61 6c 22 3a 66 61 6c 73 65 2c 22 70 73 5f 69 6c 22 3a 30 2e 30 7d 2c 22 73 64 65 66 5f 74 73 22 3a 7b 22 74 73 5f 75 6e 22 3a 66 61 6c 73 65 2c 22 74 73 5f 75 6e 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 73 63 22 3a 66 61 6c 73 65 2c 22 74 73 5f 73 74 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 62 67 63 22 3a 6e 75 6c 6c 2c 22 74 73 5f 66 73 5f 69 22 3a 66 Data Ascii: "true","ps_sd":null,"ps_bt":null,"ps_hdid":"","ps_lslm_i":true,"ps_sm":0,"ps_bbtw_i":true,"ps_al":0,"ps_bb_i":true,"ps_pbb_i":false,"ps_awao":false,"ps_il":0.0},"sdef_ts":{"ts_un":false,"ts_un_i":true,"ts_sc":false,"ts_st_i":true,"ts_bgc":null,"ts_fs_i":f
2021-10-26 20:16:45 UTC	86	IN	Data Raw: 22 74 73 5f 62 64 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 76 61 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 73 22 3a 31 2e 30 2c 22 74 73 5f 66 66 22 3a 22 41 72 69 61 6c 22 2c 22 74 73 5f 62 64 5f 62 64 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 67 63 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 67 63 22 3a 66 61 6c 73 65 2c 22 74 73 5f 76 61 22 3a 22 6e 6f 72 22 2c 22 74 73 5f 73 74 22 3a 66 61 6c 73 65 2c 22 74 73 5f 73 63 5f 69 22 3a 66 61 6c 73 65 7d 7d 2c 22 68 73 5f 73 74 22 3a 7b 22 73 64 65 66 5f 70 73 22 3a 7b 22 70 73 5f 61 77 61 6f 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6b 6c 74 5f 69 22 3a 66 61 6c 73 65 2c 22 70 Data Ascii: "ts_bd_i":false,"ts_va_i":false,"ts_fs":11.0,"ts_ff":"Arial","ts_bd":false,"ts_tw":400,"ts_it_i":false,"ts_fgc":"#000000","ts_fgc_i":false,"ts_it":false,"ts_va":"nor","ts_st":false,"ts_sc_i":false},"ts_st":{"sdef_ps":{"ps_awao_i":true,"ps_klt_i":false,"p
2021-10-26 20:16:45 UTC	87	IN	Data Raw: 75 65 2c 22 70 73 5f 72 64 22 3a 22 22 2c 22 70 73 5f 62 6c 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 64 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 62 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 69 66 6c 22 3a 30 2e 30 2c 22 70 73 5f 73 61 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 73 68 64 22 3a 66 61 6c 73 65 2c 22 70 73 5f 70 62 62 22 3a 66 61 6c 73 65 2c 22 70 73 5f 62 72 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6b 6c 74 22 3a 74 72 75 65 2c 22 70 73 5f 62 74 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6b 77 6e 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 69 66 6c 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 74 73 22 3a 7b 22 63 76 22 3a 7b 22 6f 70 22 3a 22 73 65 74 22 2c 22 6f 70 56 61 6c 75 65 22 3a 5b 5d 7d 7d 2c 22 70 73 5f 62 62 74 77 Data Ascii: ue,"ps_rd":"","ps_bl_i":true,"ps_sd_i":true,"ps_sb_i":false,"ps_ifl":0.0,"ps_sa_i":false,"ps_shd":false,"ps_pbb":false,"ps_br_i":true,"ps_klt":true,"ps_bt_i":true,"ps_hd":0,"ps_kwn_i":false,"ps_ifl_i":true,"ps_ts":{"cv":{"op":"set"},"opValue":{}},"ps_bbtw
2021-10-26 20:16:45 UTC	88	IN	Data Raw: 6e 75 6c 6c 2c 22 70 73 5f 6b 77 6e 22 3a 74 72 75 65 2c 22 70 73 5f 73 6d 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 69 6c 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 61 22 3a 34 2e 30 2c 22 70 73 5f 73 62 22 3a 31 32 2e 30 2c 22 70 73 5f 62 72 22 3a 6e 75 6c 6c 2c 22 70 73 5f 69 72 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 64 22 3a 6e 75 6c 6c 2c 22 70 73 5f 62 74 22 3a 6e 75 6c 6c 2c 22 70 73 5f 68 64 69 64 22 3a 22 2c 22 70 73 5f 6c 73 6c 6d 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 6d 22 3a 30 2c 22 70 73 5f 62 62 74 77 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 61 6c 22 3a 30 2c 22 70 73 5f 62 62 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 70 62 62 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 61 77 61 6f 22 3a 66 61 6c 73 65 2c 22 70 73 5f 69 6c 22 3a 30 2e 30 7d Data Ascii: null,"ps_kwn":true,"ps_sm_i":true,"ps_il_i":true,"ps_sa":4.0,"ps_sb":12.0,"ps_br":null,"ps_ir_i":true,"ps_sd":null,"ps_bt":null,"ps_hdid":"","ps_lslm_i":true,"ps_sm":0,"ps_bbtw_i":true,"ps_al":0,"ps_bb_i":true,"ps_pbb_i":false,"ps_awao":false,"ps_il":0.0}
2021-10-26 20:16:45 UTC	89	IN	Data Raw: 65 2c 22 74 73 5f 73 74 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 62 67 63 22 3a 6e 75 6c 6c 2c 22 74 73 5f 66 73 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 62 67 63 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 66 66 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 62 64 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 76 61 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 66 73 22 3a 31 32 2e 30 2c 22 74 73 5f 66 66 22 3a 22 41 72 69 61 6c 22 2c 22 74 73 5f 62 64 22 3a 66 61 6c 73 65 2c 22 74 73 5f 74 77 22 3a 34 30 30 2c 22 74 73 5f 69 74 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 66 67 63 22 3a 22 36 36 36 36 22 2c 22 74 73 5f 66 67 63 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 69 74 22 3a 66 61 6c 73 65 2c 22 74 73 5f 76 61 22 3a 22 6e 6f 72 22 2c 22 74 73 5f 73 74 22 3a 66 61 6c 73 65 Data Ascii: e,"ts_st_i":true,"ts_bgc":null,"ts_fs_i":false,"ts_bgc_i":true,"ts_ff_i":true,"ts_bd_i":true,"ts_va_i":true,"ts_fs":12.0,"ts_ff":"Arial","ts_bd":false,"ts_tw":400,"ts_it_i":true,"ts_fgc":"#666666","ts_fgc_i":false,"ts_it":false,"ts_va":"nor","ts_st":false
2021-10-26 20:16:45 UTC	91	IN	Data Raw: 72 69 20 49 74 61 6c 69 63 22 7d 2c 7b 22 66 6f 72 6d 61 74 22 3a 22 77 6f 66 66 32 22 2c 22 69 73 4c 6f 63 61 6c 69 63 22 7d 2c 7b 22 66 6f 72 6d 61 6c 22 3a 74 72 75 65 2c 22 75 72 6c 22 3a 22 43 61 6c 69 62 72 69 2d 49 74 61 6c 69 63 22 7d 2c 7b 22 66 6f 72 6d 61 6c 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 2f 66 6f 6e 74 3f 6b 69 74 5c 75 30 30 33 64 4a 37 61 64 6e 70 56 2d 42 47 6c 61 46 66 64 41 68 4c 51 59 36 77 5c 75 30 30 32 36 73 6b 65 79 5c 75 30 30 33 64 33 61 33 64 35 37 35 38 65 30 65 32 66 35 38 5c 75 30 30 32 36 76 5c 75 30 30 33 64 76 31 31 22 7d 5d 2c 22 73 74 79 6c 65 22 3a 22 69 74 61 6c 69 63 22 2c 22 73 75 62 73 65 74 22 3a 22 41 4c 4c 22 2c 22 73 75 Data Ascii: ri Italic},{format:"woff2","isLocal":true,"url":"Calibri-Italic},{format:"woff2","isLocal":false,"url":"fonts.gstatic.com/font?kitu003dJ7adnpV-BGlaFfdAhLQY6wlu0026skeyu003d36a3d5758e02f58u0026vlu003d3v11"},"style":"italic","subset":"ALL","su
2021-10-26 20:16:45 UTC	92	IN	Data Raw: 5b 7b 22 66 6f 72 6d 61 74 22 3a 22 77 6f 66 66 32 22 2c 22 69 73 4c 6f 63 61 6c 22 3a 74 72 75 65 2c 22 75 72 6c 22 3a 22 43 61 6c 69 62 72 69 20 42 6f 6c 64 20 49 74 61 6c 69 63 22 7d 2c 7b 22 66 6f 72 6d 61 74 22 3a 22 77 6f 66 66 32 22 2c 22 69 73 4c 6f 63 61 6c 22 3a 74 72 75 65 2c 22 75 72 6c 22 3a 22 43 61 6c 69 62 72 69 2d 42 6f 6c 64 49 74 61 6c 69 63 22 7d 2c 7b 22 66 6f 72 6d 61 74 22 3a 22 77 6f 66 66 32 22 2c 22 69 73 4c 6f 63 61 6c 22 3a 66 61 6c 73 65 2c 22 75 72 6c 22 3a 22 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 2f 66 6f 6e 74 3f 6b 69 74 3f 6b 69 74 5c 75 30 30 33 64 4a 37 61 59 6e 70 56 2d 42 47 6c 61 46 66 64 41 68 4c 51 67 55 70 35 71 48 77 5c 75 30 30 32 36 73 6b 65 79 5c 75 30 30 33 64 38 62 30 30 31 38 33 65 35 66 36 37 Data Ascii: [{"format":"woff2","isLocal":true,"url":"Calibri Bold Italic},{format:"woff2","isLocal":true,"url":"Calibri-BoldItalic},{format:"woff2","isLocal":false,"url":"fonts.gstatic.com/font?kitu003dJ7aYnpV-BGlaFfdAhLQgUp5qHwlu0026skeyu003d8b00183e5f67

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	103	IN	Data Raw: 37 38 2c 22 73 6d 22 3a 7b 22 70 73 5f 6b 6c 74 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 61 77 61 6f 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 6d 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6c 73 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 62 6c 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 63 64 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 73 61 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 62 72 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 62 62 74 77 5f 69 22 3a 74 72 75 65 2c 22 70 73 5f 6b 77 6e 5f 69 22 3a 74 72 75 Data Ascii: 78,"sm":{"ps_klt_i":true,"ps_await_i":true,"ps_sm_i":true,"ps_ls_i":true,"ps_il_i":true,"ps_ir_i":true,"ps_al_i":true,"ps_bl_i":true,"ps_sd_i":true,"ps_sb_i":true,"ps_sa_i":true,"ps_slm_i":true,"ps_br_i":true,"ps_bbtw_i":true,"ps_kwn_i":true,"ps_bt_i":true
2021-10-26 20:16:45 UTC	105	IN	Data Raw: 5f 6f 66 22 3a 32 33 34 2e 30 7d 2c 7b 22 74 62 73 5f 61 6c 22 3a 32 2c 22 74 62 73 5f 6f 66 22 3a 34 36 38 2e 30 7d 5d 7d 7d 7d 2c 7b 22 74 79 22 3a 22 61 73 22 2c 22 73 74 22 3a 22 70 61 72 61 67 72 61 70 68 22 2c 22 73 69 22 3a 38 37 2c 22 65 69 22 3a 38 37 2c 22 73 6d 22 3a 7b 22 70 73 5f 6c 73 6c 6d 22 3a 31 2c 22 70 73 5f 6c 73 22 3a 31 2e 30 2c 22 70 73 5f 6c 73 6c 6d 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 73 6d 22 3a 31 2c 22 70 73 5f 73 6d 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 6c 73 5f 69 22 3a 66 61 6c 73 65 2c 22 70 73 5f 73 6d 22 3a 7b 22 6f 70 22 3a 22 73 65 74 22 2c 22 6f 70 56 61 6c 75 65 22 3a 5b 7b 22 74 62 73 5f 61 6c 22 3a 31 2c 22 74 62 73 5f 6f 66 22 3a 32 33 34 2e 30 7d 2c 7b 22 74 62 73 5f 61 6c 22 3a 32 Data Ascii: _of":234.0},{tbs_al":2,"tbs_of":468.0}}},{ty":"as","st":"paragraph","si":87,"ei":87,"sm":{"ps_slm":1,"ps_ls":1.0},"ps_slm_i":false,"ps_sm":1,"ps_sm_i":false,"ps_ls_i":false,"ps_ts":{"cv":{"op":"set"},"opValue":{"tbs_al":1,"tbs_of":234.0},"tbs_al":2
2021-10-26 20:16:45 UTC	106	IN	Data Raw: 66 61 6c 73 65 2c 22 74 73 5f 62 67 63 22 3a 6e 75 6c 6c 2c 22 74 73 5f 66 73 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 62 67 63 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 66 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 62 64 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 61 6c 73 65 2c 22 74 73 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 67 63 22 3a 22 23 30 30 30 30 22 2c 22 74 73 5f 66 67 63 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 62 61 6c 73 65 2c 22 74 73 5f 7d 7d Data Ascii: false,"ts_bgc":null,"ts_fs_i":false,"ts_bgc_i":false,"ts_ff_i":false,"ts_bd_i":false,"ts_va_i":false,"ts_fs":11.0,"ts_ff":"Arial","ts_bd":false,"ts_it_i":false,"ts_fg": "#000000","ts_fg_i":false,"ts_it":false,"ts_va": "nor","ts_st":false,"ts_sc_i":false}}
2021-10-26 20:16:45 UTC	107	IN	Data Raw: 74 73 5f 62 64 22 3a 74 72 75 65 2c 22 74 73 5f 66 73 5f 69 22 3a 74 72 75 65 7d 7d 2c 7b 22 74 79 22 3a 22 61 73 22 2c 22 73 74 22 3a 22 74 65 78 74 22 2c 22 73 69 22 3a 37 38 2c 22 65 69 22 3a 37 38 2c 22 73 6d 22 3a 7b 22 74 73 5f 66 66 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 75 6e 22 3a 74 72 75 65 2c 22 74 73 5f 66 67 63 22 3a 22 23 30 30 30 66 66 22 2c 22 74 73 5f 75 6e 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 66 67 63 5f 69 22 3a 74 72 75 65 2c 22 74 73 5f 62 64 5f 69 22 3a 66 61 6c 73 65 2c 22 74 73 5f 66 73 22 3a 31 38 2e 30 2c 22 74 73 5f 66 66 22 3a 22 51 75 61 74 74 72 6f 63 65 6e 74 6f 20 53 61 6e 73 22 2c 22 74 73 5f 62 64 22 3a 74 72 75 65 2c 22 74 73 5f 66 73 5f 69 22 3a 66 61 6c 73 65 7d 7d 2c 7b 22 74 79 22 3a 22 61 73 22 2c 22 73 74 Data Ascii: ts_bd":true,"ts_fs_i":true},{ty":"as","st":"text","si":78,"ei":78,"sm":{"ts_ff_i":false,"ts_un":true,"ts_fg": "#0000 ff"},"ts_un_i":true,"ts_fg_i":true,"ts_bd_i":false,"ts_fs":18.0,"ts_ff": "Quattrocento Sans","ts_bd":true,"ts_fs_i":false},{ty":"as","st
2021-10-26 20:16:45 UTC	108	IN	Data Raw: 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 6e 6f 6e 63 65 3d 22 35 75 68 39 36 4e 43 5a 72 56 4d 50 49 6e 4b 53 36 32 6d 47 7a 51 22 3e 69 66 20 28 77 69 6e 64 6f 77 5b 27 5f 67 65 74 54 69 6d 69 6e 67 49 6e 73 74 61 6e 63 65 28 29 2e 73 65 74 53 65 72 76 65 72 56 61 6c 75 65 73 28 7b 22 73 6c 62 63 22 3a 34 37 34 2c 22 73 6c 63 65 22 3a 35 35 30 2c 22 73 6d 62 72 22 3a 35 34 36 2c 22 73 6d 66 22 3a 30 2c 22 73 70 62 72 22 3a 34 38 34 7d 29 3b 69 66 20 28 77 69 6e 64 6f 77 5b 27 5f 67 65 74 53 65 72 76 65 72 50 65 72 66 44 65 74 61 69 6c 52 65 63 6f 72 64 65 72 28 29 2e 73 65 74 50 65 72 66 44 Data Ascii: script<script nonce="5uh96NCZrVMPInkS62mGzQ">if (window['_getTimingInstance']) _getTimingInstance().setServerValues({"slbc":474,"slce":550,"smbr":546,"smf":0,"spbr":484});if (window['_getServerPerfDetailRecorder']) _getServerPerfDetailRecorder().setPerfD
2021-10-26 20:16:45 UTC	109	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49747	142.250.185.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdfgpdelpbcmbmeomcjbeemfm%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: nmmhkkegccagdldgiimedpiccgmieda,pkedcjkdfgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 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/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:50 UTC	246	IN	Data Raw: 79 79 59 46 67 4a 4d 53 39 71 79 5a 46 72 46 59 31 33 41 22 3e 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 33 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 6d 53 55 35 66 42 42 63 3a 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 34 36 30 2d 30 35 32 46 2c 55 2b 31 43 38 30 2d 31 43 38 38 2c 55 2b 32 30 42 34 2c 55 2b 32 44 45 30 2d 32 44 46 46 2c 55 2b 41 36 34 30 2d 41 36 39 46 2c 55 2b 46 45 32 45 2d 46 Data Ascii: yyYFgJMS9qyZrFY13A">@font-face{font-family:'Roboto';font-style:normal;font-weight:300;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fCRc4EsA.woff2)format('woff2');unicode-range:U+0460-052F,U+1C80-1C88,U+20B4,U+2DE0-2DFF,U+A640-A69F,U+FE2E-F
2021-10-26 20:16:50 UTC	247	IN	Data Raw: 32 30 41 42 2c 55 2b 32 30 41 44 2d 32 30 43 46 2c 55 2b 32 31 33 2c 55 2b 32 43 36 30 2d 32 43 37 46 2c 55 2b 41 37 32 30 2d 41 37 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 33 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 6d 53 55 35 66 42 42 63 3a 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 30 30 2d 30 30 46 46 2c 55 2b 30 31 33 31 2c 55 2b 30 31 35 32 2d 30 31 35 33 2c 55 2b 30 32 42 42 2d Data Ascii: 20AB,U+20AD-20CF,U+2113,U+2C60-2C7F,U+A720-A7FF;}@font-face{font-family:'Roboto';font-style:normal;font-weight:300;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5fBbc4.woff2)format('woff2');unicode-range:U+0000-00FF,U+0131,U+0152-0153,U+02BB-
2021-10-26 20:16:50 UTC	249	IN	Data Raw: 65 2d 72 61 6e 67 65 3a 55 2b 30 31 30 32 2d 30 31 30 33 2c 55 2b 30 31 31 30 2d 30 31 31 31 2c 55 2b 30 31 32 38 2d 30 31 32 39 2c 55 2b 30 31 36 38 2d 30 31 36 39 2c 55 2b 30 31 41 30 2d 30 31 41 31 2c 55 2b 30 31 41 46 2d 30 31 42 30 2c 55 2b 31 45 41 30 2d 31 45 46 39 2c 55 2b 32 30 41 42 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 33 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 75 37 47 78 4b 4f 7a 59 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e Data Ascii: e-range:U+0102-0103,U+0110-0111,U+0128-0129,U+0168-0169,U+01A0-01A1,U+01AF-01B0,U+1EA0-1EF9,U+20AB;}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu7GxKOzY.woff2)format('woff2');un
2021-10-26 20:16:50 UTC	250	IN	Data Raw: 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 6d 45 55 39 66 42 78 63 34 45 73 41 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 33 37 30 2d 30 33 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e Data Ascii: ily:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBxc4EsA.woff2)format('woff2');unicode-range:U+0370-03FF;}@font-face{font-family:'Roboto';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUfABc4EsA.woff2)format('woff2');unicode-range:U+0400-045F,U+0490-0491,U+04B0-04B1,U+2116;}@font-face{font-family:'Roboto';font-style:normal;font-weight:700;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1M
2021-10-26 20:16:50 UTC	251	IN	Data Raw: 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 6d 57 55 6c 66 41 42 63 34 45 73 41 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 34 30 30 2d 30 34 35 46 2c 55 2b 30 34 39 30 2d 30 34 39 31 2c 55 2b 30 34 42 30 2d 30 34 42 31 2c 55 2b 32 31 31 36 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 52 6f 62 6f 74 6f 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 37 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 31 38 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d Data Ascii: gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUfABc4EsA.woff2)format('woff2');unicode-range:U+0400-045F,U+0490-0491,U+04B0-04B1,U+2116;}@font-face{font-family:'Roboto';font-style:normal;font-weight:700;src:url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1M
2021-10-26 20:16:50 UTC	253	IN	Data Raw: 55 2b 46 45 46 46 2c 55 2b 46 46 44 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4d 61 74 65 72 69 61 6c 20 49 63 6f 6e 73 20 45 78 74 65 6e 64 65 64 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 6d 61 74 65 72 69 61 6c 69 63 6f 6e 73 65 78 74 65 6e 64 65 64 2f 76 31 30 39 2f 6b 4a 45 6a 42 76 67 58 37 42 67 6e 6b 53 72 55 77 54 38 55 6e 4c 56 63 33 38 59 79 64 65 6a 59 59 2d 6f 45 5f 4c 76 4a 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 7d 2e 6d 61 74 65 72 69 61 6c 2d 69 63 6f 6e 73 2d 65 78 74 65 6e 64 65 64 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 Data Ascii: U+FEFF,U+FFFD;}@font-face{font-family:'Material Icons Extended';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/materialiconsextended/v109/kJfEjBvgX7BgnkSrUwT8UlnVc38YydeYY-oE_LvJ.woff2)format('woff2');font-family:}material-icons-extended{font-family
2021-10-26 20:16:50 UTC	254	IN	Data Raw: 30 30 2d 30 34 35 46 2c 55 2b 30 34 39 30 2d 30 34 39 31 2c 55 2b 30 34 42 30 34 42 31 2c 55 2b 32 31 31 36 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4f 6f 6f 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 67 6f 6f 67 6c 65 73 61 6e 73 2f 76 31 34 2f 34 55 61 47 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 33 4e 77 70 35 4d 4b 67 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 33 37 30 2d 30 33 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d Data Ascii: 00-045F,U+0490-0491,U+04B0-04B1,U+2116;}@font-face{font-family:'Google Sans';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJIGDuGo1OIL3Nwp5MKg.woff2)format('woff2');unicode-range:U+0370-03FF;}@font-face{font-fam
2021-10-26 20:16:50 UTC	255	IN	Data Raw: 34 42 30 2d 30 34 42 31 2c 55 2b 32 31 31 36 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4f 6f 6f 6c 65 20 53 61 6e 73 27 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 73 72 63 3a 75 72 6c 28 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 67 6f 6f 67 6c 65 73 61 6e 73 2f 76 31 34 2f 34 55 61 47 72 45 4e 48 73 78 4a 6c 47 44 75 47 6f 31 4f 49 6c 4c 33 4e 77 70 35 4d 4b 67 2e 77 6f 66 66 32 29 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 55 2b 30 33 37 30 2d 30 33 46 46 3b 7d 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4f 6f 6f 6c 65 20 53 61 6e 73 27 3b 66 Data Ascii: 4B0-04B1,U+2116;}@font-face{font-family:'Google Sans';font-style:normal;font-weight:500;src:url(//fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJIGDuGo1OILU94YtwCwZ-Pw.woff2)format('woff2');unicode-range:U+0370-03FF;}@font-face{font-family:'Google Sans';f

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:50 UTC	267	IN	Data Raw: 61 67 4e 61 6d 65 28 22 69 6d 67 22 29 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 74 72 79 7b 5f 72 65 63 6f 72 64 49 73 41 62 6f 76 65 46 6f 6c 64 28 61 29 7d 63 61 74 63 68 28 62 29 7b 74 68 72 6f 77 20 62 2e 6d 65 73 73 61 67 65 3d 61 2e 68 61 73 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 69 69 64 22 29 3f 62 2e 6d 65 73 73 61 67 65 2b 22 5c 6e 72 65 63 6f 72 64 49 73 41 62 6f 76 65 46 6f 6c 64 20 65 72 72 6f 72 20 66 6f 72 20 64 65 66 65 72 20 69 6e 6c 69 6e 65 64 20 69 6d 61 67 65 22 3a 62 2e 6d 65 73 73 61 67 65 2b 28 22 5c 6e 72 65 63 6f 72 64 49 73 41 62 6f 76 65 46 6f 6c 64 20 65 72 72 6f 72 20 66 6f 72 20 69 6d 67 20 65 6c 65 6d 65 6e 74 20 77 69 74 68 20 3c 73 72 63 3a 20 22 2b 61 2e 73 72 63 2b 22 3e 22 29 2c 62 3b 7d 7d 29 3b 69 66 28 30 3d Data Ascii: agName("img"),function(a){try{recordsAboveFold(a)}catch(b){throw b.message=a.hasAttribute("data-iiid"? b.message+"\nrecordsAboveFold error for defer inlined image":b.message+("\nrecordsAboveFold error for img element with <src: "+a.src+">"),b}};if(0=
2021-10-26 20:16:50 UTC	268	IN	Data Raw: 4c 54 63 43 4f 6d 67 74 6f 64 39 68 79 4a 56 6c 79 38 46 74 4c 36 64 48 73 75 45 54 4a 32 41 51 5c 2f 6d 25 32 35 33 44 5f 5f 66 65 61 74 75 72 65 73 5f 5f 27 2c 27 68 74 74 70 73 3a 5c 2f 5c 2f 61 63 63 6f 75 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 5c 2f 53 69 67 6e 4f 75 74 4f 70 74 69 6f 6e 73 3f 63 6f 6e 74 69 6e 75 65 5c 78 33 64 68 74 74 70 73 3a 5c 2f 5c 2f 63 6f 6e 74 61 63 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 5c 2f 77 69 64 67 65 74 5c 2f 68 6f 76 65 72 63 61 72 64 5c 2f 76 5c 2f 32 3f 61 75 74 68 75 73 65 72 25 32 36 6f 72 69 67 69 6e 25 33 44 68 74 74 70 73 3a 5c 2f 5c 2f 64 6f 63 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 25 32 36 75 73 65 67 61 70 69 25 33 44 31 25 32 36 6a 73 68 25 33 44 6d 3b 5c 2f 5f 5c 2f 73 63 73 5c 2f 61 70 70 73 2d 73 74 Data Ascii: LTCComgtod9hyJVly8FiL6dHsuETJ2AQVm%253D__features_',https://accounts.google.com/VSignOutOptions?continue&3dhttps://contacts.google.com/Vwidget/hovercard/VV2?authuser%26origin%3Dhttps://docs.google.com%26usegapi%3D1%26jsh%3Dm;V_vscsvapps-st
2021-10-26 20:16:50 UTC	269	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49778	142.250.203.97	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:50 UTC	269	OUT	GET /a/AATXAJyEMzwYioPomGpTeso8L_wKY3bPrTht3se5MVA=s50-c-k-no 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: lh3.googleusercontent.com
2021-10-26 20:16:50 UTC	269	IN	HTTP/1.1 200 OK Access-Control-Expose-Headers: Content-Length Expires: Wed, 27 Oct 2021 20:16:46 GMT Content-Disposition: inline;filename="unnamed.png" Content-Type: image/png Vary: Origin Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-Content-Type-Options: nosniff Date: Tue, 26 Oct 2021 20:16:46 GMT Server: fife Content-Length: 476 X-XSS-Protection: 0 Cache-Control: public, max-age=86400, no-transform Age: 4 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 Connection: close
2021-10-26 20:16:50 UTC	270	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 32 00 00 00 32 08 02 00 00 00 91 5d 1f e6 00 00 00 03 73 42 49 54 08 08 08 db e1 4f e0 00 00 00 06 62 4b 47 44 00 5c 00 6b 00 c0 db 46 7f c4 00 00 01 82 49 44 41 54 58 85 63 8c c9 3e c0 30 f8 00 d3 40 3b 00 3b 18 75 16 29 60 d4 59 a4 80 51 67 91 02 46 9d 45 0a 18 75 16 29 60 d4 59 a4 80 41 ea 2c 16 f2 b4 b9 da 4b 73 73 b2 fc fc f5 77 fb be 27 d4 75 10 04 90 e9 2c 6f 67 59 61 21 f6 6f df ff 0c 2e 67 61 05 12 62 9c 25 99 ba 0c 0c 0f 1e 7f 99 32 ef 1a 25 46 51 d3 59 1c ec cc e2 a2 9c 0c 0c 0c 9f be fc a6 d0 a8 e1 95 e4 d1 80 91 ae b0 86 aa 00 33 13 23 84 cb cd c5 12 15 a4 cc c0 c0 70 ed e6 fb 0b 57 df 0d 98 b3 74 34 85 5c ed a4 e0 5c 29 71 2e 29 71 2e 08 7b 20 9d f5 fe c3 cf 27 cf bf 31 32 30 48 4b Data Ascii: PNGIHDR22]sBITObKGDkFIDATXc>0@;:u)YQgFEu)YA,Kssw'u,ogYalo.gab%2%FQY3#pWt4\l)q.)q.{ '1 20HK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49779	142.250.203.97	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:50 UTC	270	OUT	GET /pwYVsXf9mnduU19ekvkzpxBcGkRyYKUMGZ_V8GMA2zfiJjenvGHc7JSfltkCbvWz8maNXS86sFO_7LkM_SSG oIAKJvipGHjICB3qQHkQBly7B4CT09UXIUvc5r2w 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: lh5.googleusercontent.com

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:55 UTC	283	OUT	GET /wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html HTTP/1.1 Host: marketingandsoftwaretools.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 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
2021-10-26 20:16:55 UTC	284	IN	HTTP/1.1 200 OK Date: Tue, 26 Oct 2021 20:16:55 GMT Last-Modified: Tue, 26 Oct 2021 17:46:15 GMT Content-Type: text/html ETag: W/"327618a-439d-5cf450ddef95e" Vary: Accept-Encoding X-Varnish: 37475934 Age: 0 X-Cache: MISS Accept-Ranges: bytes Transfer-Encoding: chunked Connection: close
2021-10-26 20:16:55 UTC	284	IN	Data Raw: 30 30 34 33 39 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 31 30 2e 30 30 30 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 2f 3e 0d 0a 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 6 4 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 2f 3e 0d 0a 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 Data Ascii: 00439d<!DOCTYPE html><html lang="en-US"> <head> <meta content="IE=10.000" http-equiv="X-UA-Com patible" /> <meta content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" name="viewport "/> <meta content="te
2021-10-26 20:16:55 UTC	300	IN	Data Raw: 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 62 72 61 6e 64 69 6e 67 57 72 61 70 70 65 72 22 29 2c 20 22 64 69 73 70 6c 61 79 22 29 3b 0d 0a 0d 0a 20 20 20 20 69 66 20 28 62 72 61 6e 64 69 6e 67 44 69 73 70 6c 61 79 20 26 26 20 62 72 61 6e 64 69 6e 67 44 69 73 70 6c 61 79 20 21 3d 3d 20 22 6e 6f 6e 65 22 20 26 26 0d 0a 20 20 20 20 20 20 20 62 72 61 6e 64 69 6e 67 57 72 61 70 70 65 72 44 69 73 70 6c 61 79 20 26 26 20 62 72 61 6e 64 69 6e 67 57 72 61 70 70 65 72 44 69 73 70 6c 61 79 20 21 3d 3d 20 22 6e 6f 6e 65 22 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 76 61 72 20 6e 65 77 43 6c 61 73 73 20 3d 20 22 69 6c 6c 75 73 74 72 61 74 69 6f 6e 43 6c 61 73 73 22 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 69 66 20 28 62 72 61 6e 64 69 6e 67 2e 63 6c 61 73 73 4c 69 Data Ascii: getElementById("brandingWrapper"), "display"); if (brandingDisplay && brandingDisplay !== "none" && brandingWrapperDisplay && brandingWrapperDisplay !== "none"){ var newClass = "illustrationClass"; if (b randing.classLi
2021-10-26 20:16:55 UTC	301	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49794	129.215.55.224	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:56 UTC	301	OUT	GET /adfs/portal/css/style.css HTTP/1.1 Host: edadfed.ed.ac.uk Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://marketingandsoftwaretools.com/wp-content/plugins/autoptimize/ANGEL/MicrosoftAccount.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-10-26 20:16:56 UTC	302	IN	HTTP/1.1 200 OK Content-Length: 7829 Content-Type: text/css Expires: Thu, 25 Nov 2021 21:16:56 GMT ETag: DBC0B4741D4217A138377E7BCC747D0D30B93B979DC99146E4C4016785BA8C42 Server: Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0 Strict-Transport-Security: max-age = 31536000 X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;; Date: Tue, 26 Oct 2021 20:16:56 GMT Set-Cookie: NSC_febegfe.fe.bd.vl-fyufsobm=ffffff82df78445525d5f4f58455e445a4a42378b;path=/;secure

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:56 UTC	333	IN	Data Raw: f1 b0 0d 41 ec e1 cb 9c 05 54 18 8e d1 9c d0 e9 db e6 d9 de 5b e0 d4 50 da be 87 10 d6 5f f4 7d 74 99 f5 a1 c3 ba 49 58 23 e3 8a e4 c3 b0 c0 3b 2e a6 57 f2 c2 b6 b4 67 5a 30 c9 93 49 20 8e f9 4d 8f 8d 49 e0 f5 f4 00 df a6 52 d8 ee 99 c5 bd a5 c3 a8 d8 27 43 73 b6 71 5f 57 db 2e 1c 69 d8 18 9f a0 49 93 1c 2e dc f2 bd d3 d4 b3 dc 7d 3a b4 a8 56 35 0b 43 5f d6 ec 99 f7 10 ad ef 49 00 8c 72 ca 68 ec bc 3b 4b ed c4 9a 7d 14 fb 65 05 fc c5 b8 be f2 92 57 d1 84 27 5a 2f 62 b6 7f 2e f7 22 c8 07 ec ab 19 d3 6d 2c a3 6e 36 96 1b 33 b3 50 d4 34 20 62 df 59 9c b2 92 2c 13 f7 ee 9a 7a 10 2f d6 67 5f b3 b5 a3 ab de 63 ee 5a 4b 4b d8 a8 ab 5f a6 05 d9 5b e6 1f 1d eb 6a 0f 89 52 a0 73 2c 69 39 ad e9 02 dd e2 32 0f 87 3f 0d 33 f5 4e 8b ab 3e ad e3 9f ba 2d 80 79 35 3f eb Data Ascii: AT[P_]tIX#;.WgZ0I MIR^Csq_W.il.;V5C_Irh;KjEwZ/b."m,n63P4 bY,z/g_cZKK_jjRs,i92?3N>:y5?
2021-10-26 20:16:57 UTC	341	IN	Data Raw: c5 4f 61 97 36 9b 9d 56 5e db 66 06 10 35 a2 81 ad d8 4f bc 58 c3 74 c0 f6 ef 5d 05 f4 d9 b6 a5 dd 7e f6 ac 05 3b ce 72 35 0b 7a c2 9f 76 d9 3e 92 20 ae b1 b5 7d ae 27 ba 4a d3 9a d2 84 42 9b 4d cd 4f 6f 1f 4c 05 dd ba 6e 53 cb 7c b5 2d 08 cf 3c 47 a4 42 2b 07 a3 aa b0 04 18 4b 43 f3 00 a5 7c 42 bd c3 1f b2 01 4b 77 41 72 80 50 57 00 38 0c 69 27 61 83 a8 07 3b 6c a2 bd 84 c1 6e 4d 6f 35 3b bd 54 10 7e 7f c3 8d 63 11 8b 05 fc c5 b8 be f2 92 57 d1 84 27 5a 2f 62 b6 69 99 a6 b7 5c 6d 3d 32 f8 e2 c1 53 f9 cc 26 67 ca c8 c2 cd db ab 52 af 70 5b 34 cb 4a a6 a0 de b3 2f 7c 2c fa 76 01 78 b5 db 63 d5 56 fb 22 3e f3 e8 e5 6e 36 a7 be 06 67 48 03 b8 93 0f b3 15 b8 8d 4f 68 36 1d d2 9e af 13 9e 21 85 7f 9b fb b3 47 a6 2a d4 16 ad 2d db 2d 81 a6 7d d1 76 3e ea 0d Data Ascii: Oa6V^f5OXtj-;r5zv }JBMOoLnSj-<GB+KC BKwArPW8i'a;InMo5;T~c41SV?l\m=2S&gRp[4J]/vxc">n6g HOH6IG*~jv>
2021-10-26 20:16:57 UTC	349	IN	Data Raw: 30 15 99 c5 6e b5 18 b9 54 39 61 89 93 7d e6 dd 36 ca aa 9e 32 c7 41 63 a8 35 38 b0 ca 72 fb 6b b3 31 9b be f3 2e 5e 6d d6 e8 02 f7 0d 51 41 c3 f5 55 47 21 25 b1 dc 31 6a 5c 35 50 6a 47 63 8d 2d f6 4a d7 8d fd cd ca d1 9a e9 35 2c 7b 24 fc b6 54 a9 c6 e3 0a 31 1c c7 3f 44 db 1f 97 17 ab 0f e6 cc 9c 2c df 3a 45 57 d8 34 35 e4 e9 c6 56 bd 73 ce 02 b8 11 97 2e d1 dd 20 9b 9c 0a b8 a8 ff 00 2f a6 0e e3 5a 00 e8 26 b9 c2 6a 2d cf 39 0e eb 91 6c d4 d7 11 94 8f 88 28 62 0d 0e 46 42 eb 82 81 40 a5 4e 33 4f a7 d0 59 0e c2 a5 4d 13 d1 c6 5d e3 59 71 dd 7e 0d 36 f2 79 2e 9a dc 7e 5c e5 47 e1 37 77 3c 4b 61 e9 dd 4f ae 5f b1 66 fa da 02 e5 b6 52 30 c4 4b a2 e9 27 33 26 2e 91 c6 45 df 33 18 77 6b fb 29 ae d7 6f 7d b6 a9 e5 9e 1d f1 4b c2 ed 73 c6 31 4b 2f 9a 80 79 8c Data Ascii: OnT9a]62Ac58rk1.^mQAUG!%1]5PjGc-J5,{ \$T1?D;.:EW45Vs. /Z&j-9(fB@N3OYM)Yq~6y.-iG7w<KaO_fr OK'3&.E3wk)o}Ks1K/y
2021-10-26 20:16:57 UTC	357	IN	Data Raw: 68 15 d6 c1 7b 0c b1 b5 71 e4 69 f7 c1 24 fe 00 b4 5a 76 7d b0 76 69 a9 c9 e0 86 27 06 da 5a 71 f7 49 7e d5 26 06 d2 db 8d 57 50 1e 2c b5 ee 06 b2 b5 c6 ad e2 c3 99 96 36 ae 3c c4 60 6b 81 60 7b 02 d6 52 53 57 03 8b 06 6f 59 31 77 36 bf cb af af ae 32 1a 7e 5d 92 53 b7 05 07 eb 97 3a fd cd 3b 8e eb 40 7f 38 99 c9 db de 5f da f5 9f 3b 6f fb d4 ba 3c b0 70 0c 68 14 a1 3c 98 61 3a 2e bf 70 b6 f2 e8 a5 28 14 11 ca 8b 5a 7a cc 54 4e d5 9d 6e 8c 96 c1 e2 a7 d7 ce 13 7a df e2 dc f1 5b 60 7a 64 7e eb 57 b4 9f 87 e9 20 46 dd d4 ef 2f 83 9d 14 7a cc 3b 3c ec df b0 c6 67 e5 b5 61 5d 57 67 f8 ee 52 64 ee 90 1b 97 2d 9c bc 28 69 85 34 d0 61 e9 9b db 64 d5 d1 fe 76 88 c0 80 48 ec ab 19 80 7f cc bc e5 56 04 e5 c9 54 d2 2c f3 f4 1e bf 34 ed 10 db b6 e2 03 0c f3 aa ae Data Ascii: h{q[\$Zv]viZql~&WP,6<k' {RSWoY1w62~}S;.;@8_ ;o<ph<a.:p(ZzTNnz[zdwV F/z;ga]WXRd-(i4advHFT,4
2021-10-26 20:16:57 UTC	364	IN	Data Raw: 37 08 5c 71 14 5e 71 fe b6 de 90 bf 43 5f 5a 8f 9f 67 ef 7d 06 3f 9f 6b ef 7d 06 1e ee d5 74 6a 41 c4 f1 e0 3b 24 53 66 4b b2 54 d2 95 53 cf e8 87 eb 5f 48 3f 43 5f 5a d0 e8 57 6d b7 54 b0 aa d5 3e 3c 31 fb 8d 3a 4d c7 ef 9b d1 f5 09 cc fc bf 68 8e a7 65 e8 69 e3 c7 87 b0 d3 a6 dc 7e fd bd 1f 54 c3 cd b7 bb 16 b7 f0 69 35 b6 40 a4 81 91 8e 26 2e a4 c9 a2 3f e1 6f aa 79 bf 58 3f e3 6d ff 00 b3 5f ac cf 46 6f dd bf e1 3f 54 f3 9e b1 fe fa 9f ec d7 eb 31 4f ba 7c a9 7f 2d f9 c1 3a 6d c5 b5 d4 ad 5c 73 45 0c d5 fe 69 9a 9b cd c5 9b 8a 74 30 af 2c 66 1d 93 4d d0 ef 32 f5 4b 29 65 52 51 7d a6 02 aa 2b cc e5 3a 74 99 d2 cf 8b 9f 7b 8d f2 03 5c 15 e0 3d 72 0d 75 40 20 b0 15 c3 22 63 5d ee 94 ee 31 ac 9b a4 87 ef ab 8d b8 53 6d 6d 9b 98 26 54 59 0f 3a d7 32 7d 12 Data Ascii: 7lq^qC_Zg)?k]tjA;\$SfKTS_H?C_ZWmT><1:Mhei~Ti5@&.&?oyX?m_Fo?T1Oj~:mS Eit0,fM2K)eRQ]+:t{!~ru@ "cj1Smm&TY:2}
2021-10-26 20:16:57 UTC	372	IN	Data Raw: 35 61 c1 84 24 c8 b5 9b d6 fa ae ef a6 a2 3d ab 01 ad 5c 3a 4e e1 8d 56 db f0 0c bc 2b ce 73 37 b7 bb bd d5 c2 37 57 9a e6 af 0a 68 21 6d 97 6e 1a 9b c2 29 dd 8c ef 1e da 5d 46 b5 71 43 db b8 0a ba 30 aa b2 9e 06 71 5d 53 a4 b7 4e d6 6c 68 bd d3 ee 51 45 db 95 ba db 45 63 ec 90 38 72 69 a4 98 e8 8b 7d 54 15 0e 95 54 f0 de 04 f9 77 53 d8 72 07 e6 3f 98 fc b8 a8 f4 48 0b ab a8 9b 4b aa f0 f0 85 4a b2 b8 ae 25 ae 36 26 bc 39 42 ba 5a 43 fe 27 56 e5 1c 05 db 6e 1d bc bb 01 97 02 da 69 52 04 bd 66 dd ab b6 8d b1 f9 37 d5 49 43 4a 25 c0 32 b8 80 e2 47 64 70 25 d2 fa b5 fd a5 6d 5b 94 f2 ab a4 ed 81 2f 74 1f bd fc b3 ae b3 7a d6 e2 d8 bb 65 83 23 71 1f 51 9c 0d cb 1b 8b a7 cd b8 e8 97 02 e9 44 4c 15 fb 1b 8d 25 be 99 d4 f7 1b 2b ce ce c8 b6 c0 f1 6d c0 a2 81 c0 Data Ascii: 5a\$=:NV+s77Whlmm)]FqC0qjSNlhQEec8rj)TTwSr?HKJ%6&9BZCVniRf7ICJ%2Gdp%[/tze#qQDL%+m
2021-10-26 20:16:57 UTC	380	IN	Data Raw: 68 69 fb 31 75 7d 99 ea 1b 6d 56 80 1b 9b 5e 2b 47 ef 7d e4 f4 c9 74 ef dc ed bf 02 7f 56 5d 54 36 c9 5e 03 2e e9 b7 67 3e d7 1b 65 c3 5b 17 5d 1a e7 94 fa 6d e0 ec 14 90 a7 91 8d 6f 70 3f b3 6f 44 ea ae 75 24 da ee 9f 6f 71 28 95 d5 ad 7f 5b 13 a8 48 df e9 bd 27 a8 a9 ba 02 ab e6 6e db f0 b0 fc 43 f4 c8 bd 5a cb c6 6c 73 b6 f7 aa 48 0e 31 e6 25 c1 79 1c 6a 2d aa 82 98 52 a6 73 dd 48 8d 9e f5 f6 c8 de 62 25 29 70 8d 25 83 76 4b 1b 5b f5 a0 27 18 60 fd d3 38 6d e9 0d 8a 98 c3 5a 1a 82 41 e6 30 80 b6 c6 98 43 0b 84 76 88 05 cb 3d 46 fd a0 35 f8 d7 b7 39 9b f3 2f 5f b8 36 c3 67 b5 aa 3d d1 5b cd ef 04 3e e8 ef 85 67 51 aa e3 e0 88 35 37 70 e1 39 7d d5 d6 bf 79 ee 3e 6e 49 3d 9c 84 ad 75 e3 28 da c9 63 6f e5 8e a8 9b 8b 7f c2 37 86 a4 63 b5 73 9d 38 a7 e8 96 Data Ascii: hi1u]mV^+Gj]V]T6^,g>e]mop?oDu\$0q([H'nCZlsH1%yj-RsHb%)p%vK[' 8mZA0Cv=F59/_6g=>gQ57p9]y> nl=u(co7cs8
2021-10-26 20:16:57 UTC	388	IN	Data Raw: 40 a6 db 70 69 5a 1f 2c 7d 38 c4 77 37 80 1a 76 db 81 5a d6 b6 bf 96 13 77 be d9 ed 98 db 2b 71 ef 8c 74 21 ae 9f c5 ca 42 d7 51 d9 df 62 b6 85 c0 e3 3b 6e 68 e3 b7 b6 04 a9 bf dc dd 7d a5 d5 6b 57 bc b2 b4 62 d6 f4 2a e3 c5 a2 e9 f7 ef 0d a5 a6 4d ab bd b5 14 0e 1d 54 13 96 47 b6 5b bb 7a cd e4 7b 04 96 4b 8a 54 a9 6c 0f f9 19 4b a3 5c bc fb 13 64 5b 17 15 1d 85 69 ef 67 18 5d d7 76 95 6d a7 78 f3 ad 83 08 75 e9 14 da e9 24 62 0e e1 3e aa 4b 22 c2 90 01 b2 31 18 e0 d9 c9 2d 95 d0 a7 e1 ea 6a 6b ed 0c b2 e3 16 4d 48 79 ca 70 da 8c 73 fc f4 32 41 ef e0 3e 1a a4 60 07 9f 6f 8c bc 2d 28 52 a2 c6 04 83 9b 40 dd 55 b7 81 b3 e1 61 5f 78 c3 21 58 df bc 1b 0d bb 83 90 61 72 d1 1f 64 75 dd 6f ec 12 fe f6 da 85 c0 03 6a f2 ae fb 15 ca a6 49 9d 2e 5b aa 2b 0a 54 55 Data Ascii: @piZ,}8w7vZw+qt BQb;nh}kWb*MTG[z{KTIKd[ig]vmxub\$>K"~1-jkMHyts2A>~>-(R@Ua_x!Xarduoji.[+TU
2021-10-26 20:16:57 UTC	395	IN	Data Raw: 5e 9c eb 5c 06 1d b2 f2 df b5 71 03 5a 75 71 cd 4d 60 0f ba e9 9b 1d cd 59 ed e8 b8 73 b9 6a 88 c4 f6 8f 64 fa a7 3f bc e8 5b 9b 20 bd aa 6e 2d 8c 49 41 4b 8a 3b 53 f4 56 74 5e 69 29 4a f2 1e 88 4b 6d ab c4 01 05 72 ef ec 81 61 c2 51 ed d1 ed b1 0c 32 61 81 07 b2 6e 6c 7a f9 a1 4d e8 ad c0 29 6a e8 00 2e a1 80 0e 3e df 5c d4 ea 3d 2f 6d bd 53 77 0b 3b 91 4f ce 02 ab 73 b2 e2 8c cf 68 c6 72 fb cd 95 ed ad d3 6a fa 69 7a 54 53 14 75 fb cd 44 0b a3 a6 b4 b7 02 0d c3 fb 6f e2 b6 0f 23 ef 1e fe 10 d7 1d ed ae ab 8c 43 e7 43 ee 0e 67 b6 73 7d 3b ab 3e d2 b6 2e f8 ed 9f dd 96 26 96 9f 9d 39 7f d3 37 56 f2 db d3 72 e1 17 2f 90 19 45 75 ad bd 58 d4 fd e6 fa a2 b9 54 c1 cb 5d 50 da ae 30 26 9a 2d d7 15 53 8e a6 e4 4f 29 99 76 eb 5a ea b6 2f 69 17 35 db d2 03 0d Data Ascii: ^\qZuqM^Ysjd?[n-IAK;SVT^i)JKmraQ2anlzM]j.> =mSw;OshrijzTSuDo#CCGs];>.&97Vr/EuXTjP0&-SO)vZf5

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:57 UTC	403	IN	Data Raw: ad 37 0d 34 e1 35 9b 71 19 59 cd f9 10 28 36 57 89 34 0b 76 c9 af e2 17 16 57 37 15 b5 05 f1 68 01 8d 3b e5 8d b6 f3 70 1d dd 4a 6a 46 db 90 7c bb 74 a3 5c 65 38 69 a4 09 dc bd d0 51 88 21 54 91 44 44 e2 3e e8 10 f7 67 3f 11 8e 8d 0d a9 5d 6c 2a 34 86 ba 03 66 3c 41 1a 69 6b b4 a8 0b 9a 14 01 6a 46 7d a2 65 6c d3 45 c7 b6 e7 2b a4 12 30 c1 ed ab 61 35 07 92 a5 7c 3a 9c e0 a4 f0 c2 b3 2a d2 25 e6 da 43 a4 83 5d 21 8d 06 22 bc 21 96 e5 bd 34 38 01 80 3c c7 39 5d ed da b8 54 ba 9f 67 48 01 b3 15 e3 eb 92 53 67 c0 8c 86 8c 28 1b 57 15 15 a1 f5 40 0a b7 2d d1 bc 46 8a 42 93 4e 2c 2a 24 5d 93 c4 35 d7 5a d3 23 84 08 6b 0a af 75 15 a8 42 92 a5 ea 33 34 81 7b e8 09 3a 4e 43 0d 5c fd 10 05 68 db b6 cd a7 f3 43 0a b6 5a 56 86 5c e9 f7 2c 9b ee e8 58 84 5a 95 38 Data Ascii: 745qY(6W4vW7h;pJfJf{t8iQ!TDD>g?}*4f<AikjF}eE+0a5]*%C!*"!48<9]TgHsG(W@-FBN,*\$]Z#kuB3 4:[NChCjV\,XZ8
2021-10-26 20:16:57 UTC	411	IN	Data Raw: 59 ad 2b ae 74 91 e5 7e ac f4 fc 4b 9f 55 15 e9 5a 50 29 bb 52 33 3a 73 fa 64 2f 74 8f 35 02 0b da 28 6a 4e 9a ff 00 9d 34 63 c3 df 3f a7 f1 19 be ac 5f 9f 7d e8 07 c5 1c 2b 4f 07 3f db 84 4e 88 ea 46 ad ce a1 42 0f 83 3a fe d4 d6 8a 3f 7f c3 f1 19 be ac 9b 7d 0c a3 2b 1b f5 20 d7 d8 ff 00 ad 32 13 e4 8d 3b 91 b8 3b ea 9d 45 ca f9 34 1e 23 5f f5 93 ea 8a 3f 7f c0 b9 72 97 fe 4a 4b bb 81 b8 1b c2 ad a8 33 03 6f 50 3a 48 cb c6 29 94 d5 6e 88 cd ac fc 46 2c 6b 52 95 a7 f4 a6 b4 50 f7 67 b1 cb 67 46 22 f4 0b a2 83 e2 fc 22 b8 0b 78 e3 db ae 38 f9 7c d4 eb dd 31 07 2a 2d 0f af 51 9b 51 43 8f 4f c4 7b b6 f5 61 ee be 5d 6d c6 cd b6 67 74 56 db 36 aa 94 d4 d4 e4 49 6c 66 71 f9 28 95 61 f1 d8 b0 41 5f 25 73 b5 91 f6 e7 5b 14 73 6c 76 2b 9b d5 ca 7f c9 64 65 be fe Data Ascii: Y+t-KUZP)R3:sd/t5{N4c?}_+O?NFB:~?+ 2;;E4#_?rJK3oP:H)nf,kRPggF""x8]1*-QQCO{a]mgtV6llft(a A_%s[slv+de
2021-10-26 20:16:57 UTC	419	IN	Data Raw: 03 0c 2d c9 79 54 8a d2 24 18 42 56 40 02 24 b8 4c c3 33 a4 22 3f 54 d9 a3 80 c8 6f a0 65 38 82 35 71 13 d7 52 cd 9b 7f bb 45 4f c2 00 fa a7 91 f4 86 54 ea db 36 72 15 56 fa 55 89 a0 00 36 64 99 e9 7d 7a ef 46 b5 83 ef 6c 92 38 2b 8b 8d ea 4a 99 dd 7a b4 8b e7 8d 72 83 2d f4 cc 7b df 33 6c 15 b4 d9 b5 b8 be 5c 78 34 5a 65 0d dc 6e 69 8f b1 ea 9b dd ee e5 51 b6 0f b6 db 1f ed ae ba ea ad 2a a1 50 67 59 15 51 91 f3 be 09 b1 1c 35 5c fa 96 72 83 29 d5 7c 0f 08 5d 88 fd 6b 9f 52 ce 54 56 91 19 38 c3 09 00 c7 23 24 c4 89 12 2a 2a 33 8c 27 90 af 01 0a b4 a1 d8 b8 58 03 1a 69 ec 95 cb 82 c9 52 a2 95 c2 67 bb 05 24 7a e3 85 52 be d5 2b ca 90 3a 84 4c d5 8d 58 d2 b2 8d e0 1d 90 c6 e8 f2 e9 8e 22 51 56 a1 cf 09 23 76 a2 2c 1e 44 0c 4d 00 ca 44 8e 6d 20 18 e4 22 00 Data Ascii: -yT\$BV@L3"?Toe85qREOT6rVU6dzFI8+Jzr-{3lx4ZeniQ*PgYQ5V})]kRTV8*\$**Xi,Rg\$zR+:LX"QV#v,DMDm "
2021-10-26 20:16:57 UTC	426	IN	Data Raw: 5b 00 61 23 6d b0 9b 55 98 35 32 95 99 88 33 55 ac d4 4a 17 ed 50 c9 d3 6e 4a 50 d1 8c 3a 99 5d 05 21 d4 cd 54 9c 90 40 73 83 d5 24 b7 31 93 42 42 de 35 e1 0c b4 18 46 5a b4 67 05 66 68 a2 0a 13 2c 81 84 a2 84 d6 68 d8 b6 ec 24 d8 40 b2 71 12 60 1e 30 cd 65 84 18 56 ad 22 80 81 22 0d c5 4e 12 da d9 34 c6 0a e5 bd 06 b1 9c aa e2 d9 32 c2 fb c2 0c 30 06 18 5d 14 8c 0a e0 08 12 46 70 97 1e b2 b9 34 31 64 86 4b cd 95 65 ab 46 b8 99 4e d8 04 cb 89 80 88 f2 29 ca 42 80 e0 62 66 23 08 3f 33 c5 4a 46 47 29 a4 d4 46 f3 1b 9c 67 b9 4c e4 55 95 8e 10 ce 4d 16 d4 d1 ac 50 f8 e7 0f a3 94 45 48 35 a6 50 c1 34 b6 c5 40 12 e8 20 e5 31 ed 5d d3 8d 25 bb 77 f8 d6 29 0f 2b d1 9a 04 5e a8 92 d6 0e 51 50 45 4 5 0c 0b 24 28 ac 47 18 60 d4 f4 b0 6a 49 e8 6a 43 84 ac 20 4c 20 Data Ascii: [a#mU523UJPNP:]!T@s\$1BB5Fzgh,h\$@q?0eV""N420]Fp41dKeFN)Bf#?3JFG)FgLUMPEH5P4@ 1]9#w)+^QPEES(G]j]C L
2021-10-26 20:16:57 UTC	434	IN	Data Raw: 00 cd dd ab 05 f9 2d 58 e2 28 7f fa 83 39 47 d6 cd 51 33 f2 4f cd 3f c5 8e d3 91 ee ee 89 6a 09 5f c4 ed a8 9c 04 2d ab 35 c5 b1 97 6d 6c 4b da 37 48 fc b0 69 5e d9 32 ce 90 48 06 de e2 86 a1 cb b6 5d 37 81 c0 4a 2d 6b ca b9 87 88 49 fc 4e 23 c3 26 cc 96 30 9d e7 a6 22 00 62 71 8a e5 cd 4e 69 97 0a c1 d4 a9 c7 19 3a e9 cf 21 67 58 02 9c e5 5b 98 9c 24 f5 13 20 d3 5b 01 58 42 ef 4a d2 6a a6 d6 db 21 56 7d 37 38 72 99 76 d8 ad 08 9e de 56 6a 06 c2 12 fc 0d 13 6d d5 88 39 88 27 24 42 df dc 26 b3 a4 d4 0c 09 e6 65 4b 97 81 30 c1 61 61 31 12 17 30 80 17 e9 17 9e 1a 56 29 e0 8a 93 04 45 0c 3e a1 48 17 60 4c 73 aa a1 08 a9 12 c9 4b 52 24 13 12 db ac 22 ad 61 42 d2 04 82 25 22 7c 04 30 a5 24 5c 02 24 9a ad 69 1c 19 26 59 1a 40 97 36 3e dd 66 f5 bf 64 4e 7f 6a 68 Data Ascii: -X(9GQ3O?]-5mlK7Hi*2H]7J-kIn#&0"bqNi:gx[\$ [XBj]V]78rVjm9\$B&eK0aa10V)E>H"LsKR\$"aB%"] O\$!\$&Y@>6>fdNjh
2021-10-26 20:16:57 UTC	438	IN	Data Raw: 03 1a fd 72 b1 e9 2a b7 30 e2 68 16 6d ed 36 03 6a 96 c5 2a ec 6a c7 bb 08 7b 67 65 e6 f7 63 ef b7 07 6e c4 11 80 cc c7 db 6e 12 e8 04 37 a6 b3 47 a8 6c 2d dc 56 2c 38 e0 44 c6 5e 94 a0 9c e8 78 43 10 66 ae fc 50 2f a6 c9 d6 a3 da 23 2e ea cd 5d bd c2 6d 8b cb 83 a1 a1 1d 93 3b 6f b5 b7 68 0d 22 92 e5 a7 16 9c ea f6 58 78 be c9 27 8b 63 4d d5 6e da d4 99 1c 47 63 71 13 27 70 94 a8 a6 18 30 97 b6 d7 0d bb a6 c9 3e 07 c5 4f 6e 62 07 a8 2e 95 2e 38 d3 e9 8d 9a ba 0a 23 29 c9 ab 4f 44 b9 b5 7a db a1 cc 11 29 dd 6a 05 c7 12 3e 93 8c 25 8b 84 77 18 93 bc e1 78 b0 a4 0b dd 0a 09 26 80 66 60 5e ef 01 29 ee 2f 6a f0 8c 54 7b 5d a6 1e 3f 1d f2 6d 8e dd eb 9f 28 ef 37 8d 77 c0 86 96 86 7c da 66 b9 3d f0 c6 e9 a3 31 04 80 48 20 0a fa a0 8b eb 05 b4 95 23 dc 71 42 67 Data Ascii: r*0hm6*j]{gecn7G1-V,8D^xCfP#;.jm;oh"Xx'cMnGcq'p0>Onb..8#)ODz}>)%wx&f^)}JT]?m(7w{f=1H #qBg
2021-10-26 20:16:57 UTC	446	IN	Data Raw: a0 d3 51 79 4e 23 95 38 c0 02 2e 5f b3 69 6f ec 48 64 20 8e ca 40 5c bc 5e a4 81 a8 e2 c4 73 e7 2d b2 96 25 ae ea 40 0f da 38 19 5a ef 96 14 83 ed f0 22 3c 8c 02 cc af 8b 60 44 80 24 65 26 b6 6e bf b2 a4 cb 27 a7 5e 54 d4 d8 37 15 22 2c c1 8b e8 a5 24 aa 4e 58 c6 f6 5a 87 86 71 cb 0e 51 92 60 84 f6 94 13 c2 22 92 e5 a7 16 9c ea f6 58 78 be c9 27 8b 63 4d d5 6e e6 f2 f8 b4 87 48 cd d8 e4 ab c4 c2 dc 1c 96 dc 4e e0 80 0f 1c 79 cb 8a a1 ed f8 5f c6 bc 7d d9 d0 af 49 e9 29 63 c3 64 df 03 da b9 aa 84 f7 09 93 d5 ba 55 9d b5 a4 de 6c 9c be d2 e1 d2 c8 de dd ab 83 dd 32 75 f2 6b 6e 17 bf 87 6d 66 7a fc 9d 66 cf 53 7c 98 9a 8e a6 c6 a7 ff 00 dc 99 ca ee 10 63 85 0c ea ba 73 03 f2 5d b6 a5 07 8b 0f ff 00 70 67 35 7c a9 ac cf c9 f7 4f 93 2a ad b6 18 cd ad b3 10 04 cc da db c6 6d Data Ascii: QyN#8..iHd @l^s-%p8Z"<D\$e&n^T7",,\$NXZqQ""P'eHNY_)clUd1uknmfzS[cs]pg5]O*m
2021-10-26 20:16:57 UTC	454	IN	Data Raw: 79 85 36 be 64 70 bd 42 d8 cb f2 54 b3 76 6b 79 53 ed db e8 8d be ed 7e a8 5a ba 96 57 53 1a 93 2c 2d d1 73 c4 f8 53 87 2e ce f9 8d 6d d9 d8 5c 6c 10 7e ed 4f f5 8c b2 2f 50 54 1a 72 fd 31 06 8b b0 39 1a 0e 27 97 60 82 ba a9 6c 06 7e 3e ca 7b c6 57 17 fc 90 a4 8d 57 5f f7 56 bf ce 32 cd 8b 6c ce 6e 5e 3a ef 1e 5c 3b 16 00 1d 05 49 72 68 c7 dd 1c 04 38 b6 b7 97 55 28 cb 9f 22 24 d5 6d eb a1 fc c6 ae 2a b9 0e f3 2d ad 90 06 54 af 09 44 cc 43 b8 d9 dd f8 8d a8 d5 4f 6e d8 c9 d7 88 9d 26 de fd bd cd 84 bf 6f d9 71 5a 1c c1 e4 66 6b ed 81 f1 29 d2 dc c4 b1 d3 5a fe 9b 9e ae 53 c0 6a 30 a0 35 9a 78 ef 38 67 e4 d7 8c af 46 8a b5 8a 6c c4 a3 47 8d 00 68 f4 d4 ca a7 10 41 11 47 5c e3 0f 38 ea bb 11 67 75 58 12 28 4d b3 cd 6b 88 f4 4c 0b 80 d6 a6 9d c3 84 f4 7e Data Ascii: y6dpBTvkyS-ZWS,-sS.ml-/O/PTR19"l->{WW_V2ln^.;l;rh8U{"\$m*-TDCOn&ozqfZ]Sj05x8gFIgHAG]8gu uX(MkL~
2021-10-26 20:16:57 UTC	462	IN	Data Raw: 07 b6 f9 4b d6 4d 46 72 85 ba 13 a5 07 a6 59 2e 17 05 cb 8f 7c 2d 0b 27 30 dc 1b 28 55 7f 2c 33 9f 74 13 ea 99 5d 4f 7e bb 43 6a dd 0b 31 d0 58 0f 76 d9 3a 6a 7b ce 5d d2 f8 71 7f 68 58 fb e9 53 de 33 fa 44 9e 71 2f 6b d0 4b 9f a2 b6 c7 65 6b 6f d3 ae 6c ed 7f 68 97 35 31 f6 9e e5 c5 38 b7 d5 38 6b 15 04 83 9e 47 bc 4f 43 db b6 9d 27 b8 ce 1b 77 b7 f8 7d fe e6 cb 0a 69 ba c4 0f d4 63 a9 48 f4 18 b6 e8 bd 7a 98 19 2a c1 d0 c9 0d 53 26 83 58 51 73 71 65 0e 4d 71 01 f4 b8 12 b7 cd 17 05 ce bb bb 22 be 16 0b e2 fd 50 06 1d 92 ef 4e 1a ba 86 d4 37 b2 2e ab 1a 72 43 ac d3 d5 31 3a 96 e5 77 7b fd c6 e9 2b a6 f5 c6 75 d5 9d 18 e1 94 d7 c7 d2 b2 f2 75 80 d9 18 b1 e4 ac 7e 8a 4d 5e 9f 4d 0a 3b 26 55 a0 68 f4 e2 87 eb 15 9a 3b 4a db f6 43 16 a6 1a 8f 86 3d fa 31 d9 Data Ascii: KMFRy.-]0(U,3t]O-Cj1Xv:j[qlhXS3Dq/kKekolh5188kGOC'w]jchZ*sX&QsqeMq"PN7.rC1:w+uu-M^M;&U h;JC=1

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:57 UTC	469	IN	Data Raw: 56 35 63 42 d3 4e b1 56 42 3c 59 07 8e 24 6b 14 61 38 ab 23 58 ab 0c 84 eb 14 85 62 ac 32 12 8a b2 35 8a b0 09 56 3d 64 2b 1e b0 09 d6 2a c8 83 15 65 04 ab 15 64 62 80 79 36 ab 77 3a 86 bb 40 8b 6d 73 52 83 9e 26 1f aa d4 ee 2d d7 97 db 2b 6c 14 36 f2 ca b6 20 b0 ca 6a ee b6 47 71 ba 5c 4a 5a 4f 69 88 3e ae 33 ae 98 1b 9c 36 cf da 25 11 fe e8 df 8a 6a 75 0b 4a bb 62 2d 9d 44 e1 4e 39 ca 97 b6 87 6d b2 ad d7 1a dc 8a 20 a1 c6 20 a1 48 65 18 52 0d 71 ef 86 51 26 aa 0d b3 07 e5 26 c4 0d 4c 2e 29 0b cc 86 13 a1 b3 be de 1b 97 05 d2 95 d4 ca ea 13 c0 43 67 db 39 fd a5 cf 2b 73 6a e5 0d 50 96 5f c5 43 49 ab b3 b8 2e 31 61 52 f7 15 9f 1f be 33 12 76 b6 4e 1a e9 ac b7 99 95 1d f5 8b 16 77 8c b6 54 d2 80 8a 80 07 88 57 00 32 10 04 b3 2e 96 20 a6 7a 09 a0 d5 dd ce Data Ascii: V5cBNVB<Y\$ka8#Xb25V=d+*edby6w:@msR&-+l6 jGqJZOi>36%juJb-DN9m HeRqQ&6L.)Cg9+sJP_Cl.1aR3 vNwTW2. z
2021-10-26 20:16:57 UTC	477	IN	Data Raw: 27 c0 82 8b e9 94 af 39 63 36 d2 63 54 d0 5d aa 64 40 c6 39 42 22 a7 09 40 f0 4e 61 20 5f 38 04 2b 8c 44 e0 63 46 26 20 aa 31 62 64 6e 67 4f 5c 67 25 58 89 19 26 63 35 b6 36 3d 94 6c 87 8e e9 fe aa cc db 09 e6 5e 55 a5 46 64 77 4e 92 cd 8d 16 c2 b7 1f 13 9e 6c 63 d6 0a 6a 35 d7 ae 4a 32 12 67 45 bc 2b 56 e4 21 0a e1 41 e1 5e cc cc 13 69 40 74 8a 1e 66 5a 41 bc e6 92 ab 34 9d c7 04 c0 13 58 a9 98 99 02 62 31 89 e1 24 27 ca 55 be c7 cc 3 84 b0 c6 9e 81 29 dd 35 68 53 4d 1b c2 69 91 cf b6 09 8d 4d 64 a9 45 90 32 4c 42 70 f4 c7 39 82 30 32 15 f0 c9 56 32 4f 55 70 6c 3b 64 81 c0 77 41 f3 88 12 bd a3 94 00 c0 c9 ab 41 0c 45 44 90 31 81 81 f1 03 35 13 aa 69 e8 3b de 99 70 f8 a8 1b 6c 7f 54 ba 97 4f 46 62 64 03 94 25 03 0a 1e 31 92 86 96 63 80 a1 c8 56 16 de dd Data Ascii: '9c6cTjd@9B'@Na_8+DcF& 1bdngOlg%X&c56='^UFdwNlCj5J2gE+VIA^i@fZA4Xb1\$U)5hSMiMEdELBp902 V2OUpl;dwAAED15i;plTOFbd%1cV
2021-10-26 20:16:57 UTC	485	IN	Data Raw: 6c b6 6b a7 6f 64 2f eb 52 ac 7d 31 e0 65 c9 6d fa 37 54 dc d0 8b 5e 5a 9f 7a e1 a7 d1 34 ec fc ac 30 3b ad c1 3c d5 05 3e 99 d1 93 5e 31 a8 63 c4 2c d5 0b 1d 17 a5 d8 a6 9b 21 d8 7b cf e2 32 f2 84 41 4b 6a 10 72 02 91 63 14 64 7a 93 15 4f 38 a2 ef 80 3d 4f 38 e1 8c 60 39 49 50 01 52 68 20 08 34 90 35 94 77 1d 57 61 b6 a8 7b a0 b0 f7 57 c4 7e 89 9c ff 00 30 97 af 91 6e 83 9b fe 89 37 7d 67 5a a9 a6 d7 a4 6e 3d ab 4e 28 e8 ac 3b 40 94 6e 74 fe 92 ef a1 92 d8 b8 78 03 42 66 15 ed f6 fa fd 75 5d 2a bc 97 c2 25 03 bb 1b 76 25 ed 9b a1 b3 70 4f 98 9d ab 22 f9 25 b8 c6 7e 6d 27 8e c9 9c ff 00 07 61 6f 69 b2 b1 85 bb 00 11 cc 54 fd 30 de 75 32 5a 4e 73 a7 fc ca 8b 4b 5b b3 ae d6 49 7b df 1f 8c 4e 85 4d ab ca 2e 5a 60 e8 72 61 34 96 63 86 7b 4b dc e6 f3 c8 eb 73 Data Ascii: lkod/R}1em7T^Zz40;<>^1c,{2AKjrcdzO8=O8`9IPRh 45wWq{W-0n7}gZn=N{;@ntxBfu}%v%pO%-m'aoiT Ou2ZnsK{[NM.Z'ra4c{Ks
2021-10-26 20:16:57 UTC	493	IN	Data Raw: 0e 1d e4 9c 62 d4 57 11 81 ec 13 56 49 6b c9 59 aa 09 c0 0c 3e b8 cd a8 62 14 9a f7 48 6a 27 06 2c 4f 31 e1 8d a8 81 4d 35 1d a4 56 03 29 8a 8f 12 69 46 39 8f f2 ac 8e 0e 74 bb 78 cf dd c8 9f 4c 88 24 e2 08 1f a2 3b 38 39 6a f4 c0 64 cc 85 45 0a 96 83 36 ca f8 94 a0 27 9e 38 42 02 46 05 6a 0f 16 31 aa 41 f0 10 0f 64 58 3c 86 46 34 57 a1 3c 14 52 25 43 5a 35 49 3e f1 f0 c2 07 27 32 49 ec c2 3e aa 0a 15 d4 79 93 0c 0c 84 51 94 0f 79 91 d3 5c 88 af 60 85 a8 ad 41 00 fa e3 92 0e 67 13 c8 43 03 20 30 39 1d 44 f6 0c 24 a4 38 cd 6a 39 9f e4 96 30 19 8a c4 00 15 2b 4e e3 16 0f 2a ba 6e 27 b0 c3 f6 7f 96 30 17 4e 15 3a bd 12 cd 07 13 43 d8 22 2b 87 88 13 db 0f 6c 19 56 26 e0 cd 7d 35 92 0f 70 0a 51 48 f5 c2 84 a6 22 87 b0 e3 16 91 cf 49 3c 86 10 f6 c1 94 3c c3 Data Ascii: bWVIKY>bHj',O1M5V)jF9tXL\$;89jdE6'8BFj1AdX<F4W<R% CZ5I>'2I>yQdy'\ AgC 09D\$J8j90+N*n'0N:C"+H V&}5pQH"l<<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49806	142.250.203.97	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:17:00 UTC	496	OUT	GET /-6DRE7a5AcB4/AAAAAAAAAAI/AAAAAAAAAKM/5K1J4UolszQ/s0-c-k-no-ns/photo.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: lh4.googleusercontent.com
2021-10-26 20:17:00 UTC	496	IN	HTTP/1.1 200 OK Access-Control-Expose-Headers: Content-Length ETag: "v457" Expires: Wed, 27 Oct 2021 20:16:59 GMT Content-Disposition: inline;filename="" Content-Type: image/png Vary: Origin Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-Content-Type-Options: nosniff Date: Tue, 26 Oct 2021 20:16:59 GMT Server: fife Content-Length: 21418 X-XSS-Protection: 0 Cache-Control: public, max-age=86400, no-transform Age: 1 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 Connection: close
2021-10-26 20:17:00 UTC	497	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 0d 49 48 44 52 00 00 03 84 00 00 03 84 08 06 00 00 0f 94 e4 ff 3b 00 00 00 04 73 42 49 54 08 08 08 7c 08 64 88 00 00 00 5f 7a 54 58 74 52 61 77 20 70 72 6f 66 69 6c 65 20 74 79 70 65 20 41 50 50 31 00 00 08 99 e3 4a 4f cd 4b 2d ca 4c 56 28 28 ca 4f cb cc 49 e5 52 00 03 63 13 2e 13 4b 13 4b a3 44 03 03 0b 03 08 30 34 30 30 36 04 92 46 a0 b6 39 54 28 d1 00 05 98 98 9b a5 01 a1 b9 59 b2 99 29 88 cf 05 00 4f ba 15 68 1b 2d d8 8c 00 00 20 00 49 44 41 54 78 9c ed dd 7f a8 dd e7 9d 1f 8f cf e7 ea da 96 13 a5 51 27 6a 47 d3 8a 1d 75 2b a8 97 f5 52 b1 78 a9 a1 82 15 b4 a5 29 cd 82 4b 5d 70 a9 97 f1 d0 94 99 a5 29 f5 30 59 66 4a 5a a6 c5 bb 98 92 2d 9e 92 2e e9 92 2d 99 c5 2d 2e 24 c3 14 26 25 29 33 90 94 b8 4c ba 93 32 2e e3 Data Ascii: PNGIHDRN;sBITj_d_zTtRaw profile type APP1JOK-LV((OIRc.KK0D0006F@9T(Y)OH- IDatXqJGu+Rx)K Jp)0YfJZ-...&%)3L2.
2021-10-26 20:17:00 UTC	498	IN	Data Raw: fd 95 c1 b1 00 38 00 85 10 60 45 25 39 55 d3 a4 ef 96 e5 9e 0f bb bf 8f 55 36 dd a7 f8 ae 92 58 7b cb 4e dd 9f 08 b0 82 14 42 80 15 30 9d d9 f7 48 55 5d 48 f2 47 ab ea 82 e5 9e 6c 92 24 af 57 d5 8b dd fd 2f aa ea c5 da 2b 89 57 07 c7 02 d8 7a 0a 21 c0 00 d3 2e 9f 37 cb df a3 55 f5 a8 c9 1f db 64 9a 24 7e a3 aa be 71 b3 24 76 f7 1b 83 63 01 6c 1d 85 10 60 09 92 9c ad 5b 0a 60 77 9f 1f 1c 09 56 4e 92 97 6b af 18 fe cb aa fa 5a 77 5f 1a 1c 09 60 e3 29 84 00 73 36 2d ff 7c b8 aa 2e 26 f9 23 b5 b7 fc f3 cc e0 58 b0 76 92 bc 56 ef 5d 66 7a 7d 70 2c 80 8d a2 10 02 1c d1 74 e4 c3 a3 b5 37 01 bc 59 00 4f 0c 8e 05 1b 67 3a 27 f1 9b dd fd cf 6b 6f b9 e9 8b 8e be 00 38 1a 85 10 e0 80 a6 09 e0 a3 49 fe 64 55 7d b4 aa ce 77 f7 ee 0e 58 b0 95 92 bc 54 55 5f e9 ee 7f 56 Data Ascii: 8'E%9UU6X{NB0HU}HGISW/+Wz!.7Ud\$-q\$vc\['wVnKzW_)s6- .&#XvV[fz,t7YOg:'ko8IdU}jwXTU_V

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:17:00 UTC	499	IN	Data Raw: 58 5f 0a 21 ac 91 24 e7 a7 89 e0 63 a3 b3 00 c0 ed 92 7c 69 da 7c e6 a5 d1 59 80 fd 51 08 61 0d 24 39 37 1d 1f f1 f8 e8 2c 00 f0 7e 92 7c b1 bb ff 5a 77 bf 3a 3a 0b 70 6f 0a 21 ac b0 24 27 93 fc 54 55 3d dd dd c7 47 e7 01 80 fd 4a 72 b5 aa 7e b6 bb ff 76 77 bf 31 3a 0f 70 67 0a 21 ac a0 24 bb 55 f5 d4 74 9f e0 e9 d1 79 00 e0 b0 92 bc d6 dd 7f a3 aa 7e ce e1 f6 b0 7a 14 42 58 31 d3 86 31 cf 75 f7 23 a3 b3 00 c0 bc 4c 47 55 fc 84 8d 67 60 b5 ec 8c 0e 00 ec 49 72 76 36 9b bd 50 55 5f 57 06 01 d8 34 dd 7d be aa be 3a 9b cd be 90 e4 dc e8 3c c0 1e 13 42 18 2c c9 89 e9 3e c1 4f ba 4f 10 80 6d e0 fe 42 58 1d 0a 21 0c 94 e4 c9 24 9f 76 9f 20 00 db c8 fd 85 30 9e 42 08 03 24 79 74 ba 4f f0 d1 d1 59 00 60 b4 e9 fe c2 bf d2 dd 2f 8e ce 02 db c6 3d 84 b0 44 49 ce cc Data Ascii: X_!\$c jYQa\$97,- Zw:po!\$TU=GJr-vw1:pg!\$Uty-zBX11u#LGuGj Irv6PU_W4]:OoMBX!\$v 0B\$yOY'=/DI
2021-10-26 20:17:00 UTC	500	IN	Data Raw: 92 92 7c 3c c9 af 28 83 00 c0 3a eb ee 33 49 7e 25 c9 c7 47 67 81 3b 31 21 64 a5 24 39 9e e4 b3 dd fd d4 e8 2c 00 00 f3 94 e4 e7 ba fb bf eb ee ab a3 b3 c0 4d 0a 21 2b 23 c9 d9 69 89 e8 f9 d1 59 00 00 16 21 c9 4b d3 12 d2 4b a3 b3 40 95 42 c8 8a 98 ee 17 fc c5 ee 3e 3d 3a 0b 00 c0 22 25 79 ad bb ff 1b f7 15 b2 0a dc 43 c8 70 49 1e 4b f2 55 65 10 00 d8 06 dd 7d 3a c9 57 93 c3 36 3a 0b 28 84 0c 95 e4 13 49 9c 2f 08 00 6c 95 ee 3e 91 e4 0b 49 3e 31 3a 0b db 4d 21 64 88 e9 b0 f9 4f 57 d5 67 ba db a1 ad 00 c0 d6 99 ae 81 3e 33 9b cd 3e ed 10 7b 46 71 0f 21 4b 97 e4 44 92 cf 77 f7 e3 a3 b3 00 00 ac 82 24 5f ec ee 1f ed ee 2b a3 b3 b0 5d 14 42 96 2a c9 e9 69 89 e8 85 d1 59 00 00 56 49 92 17 bb fb cf 75 f7 6b a3 b3 b0 3d 14 42 96 26 c9 43 d3 4e a2 e7 46 67 01 00 Data Ascii: <(-3!-%Gg;1d\$9,M!+#!YIKK@B>=":%yCpIKUe):W<6:(/!>1:MidOWg>3>{Fq KdW\$+_jB'iYIvuk=B&CNFg
2021-10-26 20:17:00 UTC	501	IN	Data Raw: 1f 1d 12 90 a1 14 c2 2d 34 9b cd 9e eb ee a7 ef f6 f7 5d 55 b3 d9 8d 9a 7d ef bb b5 f3 9d df ac e3 df fe f7 b5 73 e3 5a e5 d8 6e f9 bc 1b 58 1d a9 ae d4 f5 9d 63 75 ed ea 77 6b f6 fb cf 55 7d ff 6a 65 b6 bc cd b0 32 2d 19 fd ce d5 ff b7 be fd e6 f4 dc ec d8 f6 57 1f bb 51 95 1d 1f 9e 01 e3 4d ab ba 76 1e b8 5e b3 1b a9 df fa de 95 fa de b5 6f df f1 5b bb fb a9 d9 6c f6 c6 ce ce 4c 2c 37 24 a3 29 84 5b 66 36 9b 3d 73 af 32 78 53 57 55 66 37 20 a7 1e ae 5e ee 8d 6b 85 c0 3a 6a 76 bd 6c a0 07 ac 82 7e fb 3f aa 72 ed 7a d5 fd 6f 55 5d bf 56 99 dd 58 6a 8e 24 95 9a d5 2c d7 ea fa ec 6a 65 e7 fb b5 bb 53 35 bb 51 0a 21 30 de f4 3e b9 bb bb b7 df d6 d5 37 af ee 2d 6b bf db b7 77 3f 3d 9b cd 4a 29 dc 2e 0a e1 16 49 f2 74 55 fd f5 7d 7d 73 77 f5 b1 fb ea fa b1 dd Data Ascii: -4 U)sZnXcuwkU je2-ooWQMv^o[O,7\$] f6=s2xSWUf7*kjvl~?rzoU VX{j,\$jeS5Q!0>7-kw?=>J)lTu }sw
2021-10-26 20:17:00 UTC	503	IN	Data Raw: 92 4c 87 cf 7f a1 bb 4f 8f ce 02 00 00 ab a8 bb 4f 26 f9 42 12 1b 2f 2e 89 42 b8 24 49 9e eb ee 47 47 e7 00 00 80 55 d6 dd e7 93 7c 76 74 8e 6d a1 10 2e 41 92 a7 ba fb 13 a3 73 00 00 c0 3a e8 ee 27 93 b8 7e 5e 02 85 70 c1 92 9c 4b f2 99 d1 39 00 00 60 9d 24 f9 74 92 f3 a3 73 6c 3a 85 70 81 a6 fb 06 5f 70 f8 3c 00 00 15 4c 77 1f 4f f2 7c 92 e3 a3 b3 6c 32 85 70 81 92 fc 4c 77 3f 32 3a 07 00 00 ac a3 ee 7e d8 91 6d 8b a5 10 2e 48 67 20 01 00 80 55 f5 d3 a3 73 00 00 c0 3a 6a ee a7 9d 4f b8 38 0a e1 02 24 39 99 e4 79 e7 0d 02 00 c0 d1 25 f9 7c 92 53 a3 73 6c 22 85 70 01 92 7c b6 bb cf 8e ce 01 00 00 9b a0 bb 4f 27 f9 dc e8 1c 9b 48 21 9c b3 24 74 f7 13 a3 73 00 00 c0 26 e9 ee c7 92 fc f8 e8 1c 9b 46 21 9c a3 24 67 1d a2 09 00 00 8b 31 1d 45 71 6e 74 8e 4d a2 10 ce Data Ascii: LOO&B.B\$IGGUjtm.As:~"pK9*\$ts!p.p<LwO l2pLw?2:~m.HUs:O8\$9y% Ss 'p O'H O\$ts&F!\$g1EqntM
2021-10-26 20:17:00 UTC	504	IN	Data Raw: 00 cc dd 26 76 8d 8d 2a 84 49 2e 76 f7 c5 d1 39 00 00 80 cd d3 dd 17 93 5c 1c 9d 63 9e 36 ad 10 6e e4 ba 5e 00 00 60 35 6c 5a e7 d8 98 42 68 3a 08 00 00 2c da a6 4d 09 37 a9 10 6e 54 53 07 00 00 56 d3 26 75 8f 8d 28 84 49 1e 33 1d 04 00 00 96 61 9a 12 6e c4 c9 06 9b 52 08 37 a6 a1 03 00 00 ab 6f 53 3a c8 da 17 c2 69 3a 78 7e 74 0e 00 00 60 7b 74 f7 f9 4d 98 12 6e 42 21 dc 88 66 0e 00 00 ac 97 4d e8 22 6b 5d 08 4d 07 01 00 80 55 66 31 4a b8 b6 85 c0 c9 6e 92 67 47 e7 00 00 00 b6 57 92 67 93 ec 8e ce 71 58 6b 5b 08 ab ea c9 ee 7e 68 74 08 00 00 60 7b 4d 9d e4 c9 d1 39 0e 6b 2 d 0b e1 34 1d fc d4 e8 1c 00 00 00 49 3e b5 ae 53 c2 b5 2c 84 b5 37 1d 3c 37 3a 04 00 00 c0 d4 4d d6 72 4a b8 76 85 d0 74 10 00 00 58 35 eb 3a 25 5c bb 42 58 a6 83 00 00 c0 8a 59 d7 29 Data Ascii: &v*1.v9!c6n^5lZBh;.M7nTsv&u(l3anR7oS:i:x-t'!tMnBfM"kJMQ6aJ0ngWGqXk[-ht'!M9k-4!>S,7<7:MrJvtX5:%BXY)
2021-10-26 20:17:00 UTC	505	IN	Data Raw: b0 4d ba fb 5c 92 b9 df 96 b7 88 42 68 33 19 00 00 80 39 5b 44 d7 5a c4 92 d1 c7 17 f0 9c 00 00 00 db 6e ee 5d 6b ae 85 30 c9 d9 ee 7e 68 9e cf 09 00 00 40 55 77 3f 94 e4 ec 3c 9f 73 de 13 c2 8f ce f9 f9 00 00 00 78 c7 5c 3b d7 bc 27 84 7f 7a 9e cf 07 00 00 c0 3b e6 dd b9 e6 56 08 93 ec 56 d5 c5 79 3d 1f 00 00 00 ef 71 71 ea 5e 73 31 cf 09 e1 85 ee 3e 31 c7 e7 03 00 00 e0 16 53 e7 ba 30 af e7 9b e7 84 f0 4f ce eb b9 00 00 00 b8 b3 79 76 af 79 4e 08 3f 36 c7 e7 02 00 00 e0 ce e6 d6 bd e6 52 08 93 9c e9 ee 87 e7 f1 5c 00 00 00 dc 5d 77 3f 9c e4 cc 3c 9e 6b 5e 13 42 c7 4d 00 00 00 2c cf 5c 3a d8 bc 26 84 ee 1f 04 00 00 58 92 79 75 b0 23 17 c2 69 cb 53 13 42 00 00 80 e5 f9 e8 3c 8e 9f 98 c7 84 d0 71 13 00 00 00 00 4b 34 af e3 27 e6 31 21 fc 63 47 7d 0e 00 00 00 Data Ascii: MBh39[DZn]k0-h@Uw?<sl';z;Vvy=qq^s1>1S0OyvyN?6R w?<k^BM,;Xy#u#SB<qk4!1cG}
2021-10-26 20:17:00 UTC	507	IN	Data Raw: 76 f9 71 00 00 00 58 b2 b3 37 ff a0 10 02 00 00 6c 97 b3 37 ff 70 6b 21 b4 c3 28 00 00 c0 e6 7b bb fb dd 7a 0f a1 33 08 01 00 00 36 dc ad dd cf 92 51 00 00 80 ed 72 f6 e6 1f 6e 2d 84 27 96 9f 03 00 00 80 25 7b bb fb dd 5a 08 4f 0d 08 02 00 00 c0 72 bd dd fd 6e 2d 84 a7 07 04 01 00 00 60 b9 de ee 7e 3b 55 55 49 76 bb fb f8 b8 3c 00 00 00 2c 43 77 1f 4f b2 5b f5 ce 84 f0 cc 3d be 1f 00 00 80 cd 72 a6 ea 9d 42 78 72 60 10 00 00 00 96 eb 64 95 42 08 00 00 b0 8d de 55 08 2d 19 05 00 00 d8 1e ef 5a 32 ea 0c 42 00 00 80 ed 71 a2 ea 9d 42 e8 c8 09 00 00 80 ed 71 ba ea 9d 63 27 3e 32 36 0b 00 00 00 cb 92 e4 c3 55 96 8c 02 00 00 6c 23 9b ca 00 00 00 6c 29 9b ca 00 00 00 6c 29 9b ca 00 00 00 6c a9 77 36 95 a9 aa 53 03 83 00 00 00 b0 5c a7 aa a6 42 d8 dd 96 8c 02 00 Data Ascii: vqX7l7pk!({z36Qm-%{ZOrn-';UUlv<CwO[=rBxr'dBU-Z2BqBqc>26U# !)}lw6SIB
2021-10-26 20:17:00 UTC	508	IN	Data Raw: 9d aa 07 8f ed d4 e9 e3 5d bf ff c1 ae 53 c7 bb 8e 2d eb 6d 2a b3 aa 6b ff b1 ea ea ff 57 75 ed f5 aa d9 d5 bd c7 aa 5c 6c 01 ab 63 76 7d fa f4 ec c1 aa 0f fd 17 55 0f fe a7 a3 13 b1 42 76 bb fb 5b a3 43 b0 5a 66 a9 7a f3 46 ea df 7d 77 56 5f ff 0f d7 eb 97 ff fd b5 fa fe ac 6b b7 6b ba c8 f2 e9 37 30 56 ea 9d 77 a2 07 01 00 80 55 66 31 4a b8 b6 85 c0 c9 6e 92 d1 df b3 5b 1f be bf eb d8 b2 1a 61 6e 54 bd f9 1b 55 bf fd 8d aa df f9 f5 aa 6b df ae ca b5 aa da 51 08 81 d5 71 fd 7b 7b ef 49 0f fc 9e aa 7e aa ea c1 3f 50 b5 c4 b5 14 ac ae ee fe 96 09 21 ef 91 a4 ae cd aa 7e fb ad d4 a5 2b 37 ea 07 be 7d a3 de bc 5e 75 df e4 d5 ee 34 25 8c 25 51 c0 40 a9 aa a4 2b 95 7a 70 b7 eb 07 1f 3c 56 a7 8f 77 7d e7 5a 6a b6 cc b7 a7 cc f6 4a e0 9b ff f7 5e 21 7c eb 3f 54 e5 ad Data Ascii:]S-m*kWu!cv UBv{CZfzF}wV_kk70Vwu;_N[anTukQq{!-?P!-+?^uN4%Q@+zpcVw}Zj'! ?T
2021-10-26 20:17:00 UTC	509	IN	Data Raw: 00 00 5b ea 50 4b 46 af 24 79 75 31 79 00 00 00 58 b4 24 af 76 f7 95 bb fd fd bd 26 84 55 ae 84 00 00 00 eb ec 9e 9d 4e 21 04 00 00 d8 5c 87 2f 84 dd fd af e7 9b 05 00 00 80 65 79 bf 4e f7 7e 13 c2 5f e6 98 05 00 00 80 e5 3a d2 84 f0 e5 24 57 e7 9b 07 00 00 80 45 4b 72 b5 bb ef 39 e4 7b bf 09 61 95 fb 08 01 00 00 d6 d1 fd 76 39 85 10 00 00 60 33 1d bd 10 da 58 06 00 00 60 fd ec a7 cb 99 10 02 00 00 6c a6 b9 2c 19 7d 69 0e 41 00 00 00 58 ae f7 ed 72 fb 59 32 fa 7a 92 d7 e7 93 07 00 00 80 45 4b f2 7a 77 bf 6f 8f db cf 84 b0 aa ea c5 23 e6 01 00 00 60 79 f6 d5 e1 f6 55 08 bb fb 5f 1c 2d 0b 00 00 00 cb b2 df 0e 67 42 08 00 00 b0 79 e6 37 21 ac aa 97 92 5c 3d 42 18 00 00 00 96 60 ea 6e fb da 1c 74 bf 4b 46 af 56 d5 37 8e 12 0a 00 00 80 a5 f8 c6 d4 e1 de d7 7e Data Ascii: [PKF\$y1uX\$V&UN!VeyN-W:\$WEKtr9{av'9'3X'1,}iAXrY2zEKzwo#yU_gBy7!=-B'ntKFV7~
2021-10-26 20:17:00 UTC	510	IN	Data Raw: ce 39 cf ff 7d df df 2f 08 4b 76 9c 73 25 38 af cf e5 fb 79 9e 1b 00 80 4f b0 bd 9d 69 57 0b 61 55 1d e9 ee 8b bb fc 35 01 00 00 66 6f ea 4a 47 76 f3 6b ee fe 84 70 d7 ff 0b 02 00 00 2c 89 23 53 67 da 35 bb 3d 21 ac 24 3f d8 ed af 09 00 00 77 23 ba d2 88 42 f8 4e 77 9f dc ed af 0b 00 00 30 57 dd 7d 32 c9 3b bb fd 75 77 bd 10 56 99 12 02 00 00 5c 6d 54 47 1a 52 08 6b f3 71 99 4b 83 be 36 00 00 c0 6c 4c dd 68 c8 5b 2b a3 26 84 17 aa ea f5 11 5f 1b 00 00 60 66 5e 9f 3a d2 ae 1b 35 21 74 6c 14 00 00 a0 c6 76 a3 91 85 f0 78 77 9f 1e f5 f5 01 00 00 46 eb ee d3 49 8e 8f fa ca 3 0a 61 95 29 21 00 00 b0 de 46 77 a2 a1 85 b0 aa 0e 7b 5c 06 00 00 58 47 53 17 3a 3c 32 c3 e8 09 e1 bb 55 f5 e6 c8 0c 00 00 00 83 bc 39 75 a2 61 46 4f 08 87 8f 48 01 00 00 46 98 43 17 Data Ascii: 9 /Kvs%8yO!Wau5fJGvkv,;#Sg5=!\$?0w#BNw0W}2;uvmVtGRkqK6LHf+&_!^:5!tlvxwFla)!Fw{XGS:<2U9uaFOHFC

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:17:00 UTC	512	IN	Data Raw: 35 ad 99 38 36 3a c7 e6 58 8b 42 58 65 0d 05 00 00 70 73 ab be 66 e2 5a eb 54 08 ad a1 00 00 00 6e 66 a5 d7 4c 5c 6b 6d 0a 61 95 35 14 00 00 c0 8d ad c3 9a 89 6b ad 5b 21 b4 86 02 00 00 b8 ae 75 58 33 71 ad b5 2a 84 13 6b 28 00 00 80 8f 58 97 35 13 d7 5a bb 42 38 ad a1 38 30 3a 07 00 00 30 1f 49 0e ac c3 9a 89 6b ad 5d 21 ac aa 4a 72 bc bb 5f 1f 9d 03 00 00 18 af bb 5f 4f 72 7c 74 8e 11 d6 b2 10 56 59 43 01 00 00 ac df 9a 89 6b ad 73 21 3c 5b 55 2f 8f ce 01 00 00 0c f5 f2 d4 0d d6 d2 da 16 c2 2a 6b 28 00 00 60 9d ad e3 9a 89 6b ad 7b 21 bc b8 ce e3 61 00 00 58 67 49 9e 4b 72 71 74 8e 91 d6 ba 10 56 55 25 39 dc dd 27 46 e7 00 00 00 76 4f 77 9f 48 72 78 74 8e d1 d6 be 10 56 55 25 d9 df dd 6b f7 c4 2c 00 00 ac a3 ee de 48 b2 7f 74 8e 39 50 08 ab 2a c9 a9 24 Data Ascii: 586:nXBxepsfZTnflkma5k!uX3qk(X5ZB880:0lk)Jr__Or!tVYCKs<[U* k!aXgIKrqtVU%9FvOwH rxtVU%k,Ht9P*\$
2021-10-26 20:17:00 UTC	513	IN	Data Raw: 9b 14 c2 19 49 f2 4e 92 67 46 e7 00 00 80 9d 90 e4 40 92 13 a3 73 f0 21 85 70 66 92 bc d6 dd 87 47 e7 00 00 80 ed d4 dd 87 93 bc 3a 3a 07 1f a5 10 ce 50 92 67 ba fb e4 e8 1c 00 00 b0 1d ba fb a4 93 70 f3 a4 10 ce 50 92 4b d3 7d 42 67 ab 01 00 58 6a d3 23 32 5f 4f 72 69 74 16 3e 4e 21 9c a9 24 67 93 3c d1 dd 17 47 01 00 80 db d1 dd 17 a7 32 78 76 74 16 ae 4f 21 9c b1 e9 91 99 bd 5e 1e 05 00 60 d9 4c 2f 8a ee f5 88 cc bc 29 84 33 97 e4 cd 24 07 47 e7 00 00 80 ad 48 f2 6c 92 37 47 e7 e0 93 29 84 4b 20 c9 a1 ee 7e 79 74 0e 00 00 b8 15 dd 7d 28 c9 2b a3 73 70 73 0a e1 92 48 f2 5c 77 bf 31 3a 07 00 00 7c 92 ee 76 c2 6d 89 36 a7 3b d4 00 00 12 de 49 44 41 54 28 84 4b 22 c9 46 92 7d dd 7d 7c 74 16 00 00 b8 9e ee 7e 67 ba 37 e8 0d 8c 25 a1 10 2e 91 24 17 93 3c Data Ascii: !NgF@slpfG::PgPpKjBgXj#2__Orit>N!\$g<Gg2xvtO!^L)3\$GHI7G)K ~yt}+spsHw1: vm6; DAT(K"F)}}[t-g7%.\$<
2021-10-26 20:17:00 UTC	514	IN	Data Raw: ab ae 9c 63 d8 f1 bf c1 5d 79 ad cf 0b cc c0 12 98 1e 90 79 e2 ca 64 b0 a7 7f ce 1f c7 bf d6 9e 33 2d 7c 4c 92 8b 49 1e df f2 9e 42 80 19 d8 b5 c7 46 a7 7b 8c 00 73 37 ad 96 78 fc ea 63 a2 49 b5 32 48 95 09 21 9f a0 bb f7 74 f7 1f 27 f9 c6 e8 2c 00 00 6c 9d 3d 83 dc 8c 09 21 37 74 d5 f2 fa c3 a3 b3 00 00 b0 35 dd 7d 58 19 e4 66 14 42 3e 51 92 8d c5 62 b1 af bb 5f 19 9d 05 00 80 5b d3 dd af 2c 16 8b 7d ca 20 37 e3 c8 28 b7 ec f2 e5 cb bf 99 e4 db a3 73 00 00 70 63 53 19 3c 38 3a 07 cb c1 84 90 5b 36 7d b0 3c 3f 3a 07 00 00 37 f4 bc 32 c8 56 98 10 b2 65 dd fd ed aa fa cd d1 39 00 00 f8 88 83 49 5c f3 61 4b 14 42 6e 8b 52 08 00 30 2b ca 20 b7 45 21 e4 b6 75 f7 37 a6 b5 14 7b 46 67 01 00 58 47 dd bd 31 bd 24 6a 7f 34 b7 45 21 e4 8e 28 85 00 00 63 28 83 6c 07 Data Ascii: c jy3d3- LlBF{s7xcl2Ht!r, =I75)XfB>Qb_[] 7(spS<8:[6]<?:72Ve9!aKBNr0+ Elu7{FgXG1\$4E!(c(l
2021-10-26 20:17:00 UTC	515	IN	Data Raw: 0c b2 ce 4c 08 a1 aa ba fb 9b dd fd 3b 49 ee 19 9d 05 00 d8 59 dd 7d 31 c9 81 24 87 47 67 81 d1 14 42 98 74 f7 7d d3 11 d2 c7 46 67 01 00 76 46 77 9f 98 1e 8e 39 3b 3a 0b cc 81 23 a3 30 49 72 2e c9 e3 55 f5 ac 07 67 00 60 b5 74 f7 46 77 bf 98 e4 a7 95 41 f8 90 09 21 5c 4f 77 3f 3c 2d b3 b7 9e 02 00 96 5c 77 9f 4a b2 3f c9 89 d1 59 60 6e 4c 08 e1 3a 92 9c 4c f2 95 da 9c 16 5e 1a 9d 07 00 d8 ba e9 ef e1 2f 24 f9 a2 32 08 d7 67 42 08 37 d1 dd f7 77 f7 ef bb 5b 08 00 cb 63 ba 2b b8 cf 5e 41 f8 64 26 84 70 13 49 ce 2e 16 8b 9f a9 aa 7d dd 7d 61 74 1e 00 e0 c6 ba fb 62 55 1d 58 2c 16 5f 51 06 e1 e6 4c 08 61 0b ba fb de ee fe ad 24 df 18 9d 05 00 f8 a8 ee 3e 3a ad 93 38 3b 3a 0b 2c 0b 85 10 6e 43 77 3f 39 15 c3 fb 46 67 01 80 75 d7 dd ef 26 39 98 e4 c8 e8 2c b0 Data Ascii: L; Y}1\$GgB}FgvFw9;#0lr.Ug'tFwA!Gw?<-lwJ?Y'nL:~\$g2B7w[c+^Ad&pl.}]atbUX,_QLa\$>8;:,nCw?9Fgu&9,
2021-10-26 20:17:00 UTC	517	IN	Data Raw: 7e 90 e4 ed d1 79 80 d5 a5 10 02 bb 62 ba 6b f8 ad 69 d9 fd 43 a3 f3 00 cc 51 77 9f 4e f2 83 da 9c 06 be 3b 3a 0f b0 fa 14 42 60 d7 75 f7 97 ba fb 17 ab ea 5b 49 ee 1e 9d 07 60 a4 69 1a f8 fa 34 0d 3c 3e 3a 0f b0 5e 14 42 60 98 ee be bb 36 a7 86 bf 98 e4 4b a3 f3 00 ec a6 ee 3e 39 4d 03 8f 78 29 14 18 45 21 04 66 a1 bb 1f ea ee 5f ae cd a9 a1 bd 08 c0 4a ea ee 8b b5 59 00 7f 90 e4 9d d1 79 00 14 42 60 56 ba fb ae aa fa e6 34 35 7c 74 74 1e 80 ed d0 dd c7 93 fc 51 6d 96 c1 8b a3 f3 00 5c a1 10 02 b3 d5 dd f7 55 d5 37 ba fb e7 94 43 60 d9 4c 25 f0 4f aa ea 8d 24 e7 46 e7 01 b8 1e 85 10 58 0a ca 21 b0 0c a6 7b 81 7f 54 9b 8f c4 28 81 c0 ec 29 84 c0 d2 99 ca e1 37 bb fb 9f 26 79 78 74 1e 60 bd 4d 25 f0 4f 6a b3 04 9e 19 9d 07 60 2b 14 42 60 a9 75 f7 03 b5 59 Data Ascii: ~ybkiCQwN;:B`u 'i4<>:^B`6K>9Mx)E!f_JYyB`V45!tQmU7C`L%O\$FX!{T(0)yxT`M%Oj`+B`uY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49750	172.217.168.13	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:45 UTC	1	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/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-10-26 20:16:45 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	110	IN	Data Raw: de 04 22 58 80 63 a5 5b a3 80 25 6b 3b 0b d4 ca a7 ff 8f 7b b6 e7 be 3f 93 6a a2 11 25 90 36 bd db eb 30 0f b9 4c 6d 6e af ae 31 17 4c 3e fe 10 7d 0e 24 ed fc b7 b5 a2 66 91 87 c8 14 7c 99 51 22 db aa 3a 1f 57 c5 9c 91 4a b6 92 eb d2 8c 08 1f 9f 3b 7c a7 fe c9 4e 1e dc d9 45 1e 21 4b 3a a7 4e aa 75 ce e6 6d 7e 0c 9c 6f fd bd 66 88 10 ab 99 83 1f bf b2 15 4c 81 39 0c b7 45 6d da c1 3a e4 0e 0c 5d 23 7c cf bf 6a 7a 66 6e 79 0f 20 21 6e 93 4b 93 a0 75 93 6d 39 45 c1 92 29 f5 37 43 73 69 6e e3 64 e3 87 82 24 92 23 10 66 aa 84 6a 24 59 f6 75 ed 63 09 83 7c 81 96 03 2d 07 20 64 b4 aa 0a c4 80 96 59 b5 3e 7f 57 8e dc fc 7e 66 03 c9 22 81 15 64 31 8d 41 c4 9e f8 17 f3 aa bc fa da ea 53 0c ef 34 81 a2 d1 48 e4 ed d1 9f d3 61 13 4b 87 0b 0f b1 ff 11 2b 10 2c ad 4f Data Ascii: "Xc%k;{?}%60Lmn1L>}\$fQ":WJ; NEIK:Num-ofL9Em: #jzfnY InKum9E)7C\$ind#\$f\$Yucf- dY>W~f'd 1AS4HaK+,O
2021-10-26 20:16:46 UTC	112	IN	Data Raw: 85 22 11 0f 7a 95 a8 90 ac 86 18 54 92 83 d1 16 f9 f5 e2 64 0d a4 d0 a7 43 24 64 4f 6f 6e 57 5e 14 2b c2 4b 59 5d fa d6 27 8a 9b 7b 46 5a 9c 82 5a 27 31 82 3e 6d 49 86 22 70 04 e3 c6 69 2c 3e 26 47 b7 48 f5 89 36 fd 81 85 f1 8e 78 f3 31 1c c2 c6 5e 38 9a b3 d8 af 65 47 85 72 9a 6a 59 ea f8 34 30 74 f6 29 c2 8b ad c4 0d e9 e2 65 90 1b 41 12 83 c2 6c 55 5e 1d 16 c5 63 ac 5c a4 ea 62 98 90 81 0b 88 78 18 08 d4 19 0d 95 47 a9 6e 41 91 e9 2b 2f a8 39 c1 13 6d 9c ca a5 89 48 85 57 cc f5 8b 61 48 39 ff 8b b8 29 d7 0d 79 d9 8d 58 00 2f 63 25 e8 0c b1 3d bd 40 d8 f0 ed ae 10 5f 24 a2 bd 51 ce 51 46 a0 cf 55 fb 54 45 67 c8 cc 14 4b 27 7b 59 81 33 ba e1 48 c8 75 36 fd ba cc 74 05 01 30 50 4b da 7c ba 22 9a e8 4a 07 a4 89 57 bc cc a2 a5 6a 44 f3 e3 9b 9d 60 b9 78 be Data Ascii: "zTdC\$dOoW^+KY]{FZZ'1>ml"pi,>.&GH6x1^8eGrjY40t),eAIU^c bXGnA+9mHwHa9jYx c%=@_\$\$QQFUTEgK' {Y3Hu6t0PK"}JWjD'x
2021-10-26 20:16:46 UTC	113	IN	Data Raw: b9 c4 a8 ff 5d 55 0e a2 be 5e 7b 2d b6 6f 8c 1a 86 90 a1 64 a2 59 9e 16 0e e4 ae 5a 6a c5 7a 57 53 ff 0c 3a c6 4e f5 04 12 94 74 a8 a2 4f 34 81 60 1e 3c 71 9c ed a5 ae 18 d0 b0 67 e3 1c dc 39 66 44 36 84 c3 12 ed 06 4b f7 7b 2f e2 f7 e6 52 be 0e c5 ee fd 4d 24 ce bf 6a b5 2c 09 fc de f1 10 94 c2 a3 e9 c9 37 61 d0 ab 1d 03 1f 62 bd 16 8c 40 6a 35 d6 cc aa 37 c0 98 55 72 8e d7 e9 d7 38 9b 2a 6d 16 d9 45 86 b0 a9 bd af 91 91 d8 30 a4 8c 15 40 26 bf 49 28 a2 16 8d ab 93 8f 0e c8 a2 7d c1 f3 b5 21 40 71 33 cd ac e5 08 40 cc f5 e5 84 da 28 6d a1 a6 a7 25 e1 c3 80 4f c7 78 ef 98 01 3a ed e4 70 03 c2 0b 75 24 05 6d 42 59 73 18 0b 16 68 4a d1 a6 e5 39 94 84 91 51 47 0f 0a 04 f7 4f 78 fe 5b 05 2a 8a 35 7c 78 01 46 e8 21 19 99 e9 80 40 46 36 c9 4c 52 a5 4a e0 e0 60 Data Ascii:]U^{\-odYzjzWS:NtO4' <qg9fD6K{/RM\$},7ab@]57Ur8*mE0D&l(!@!q3@!(m%Qx:pu\$mBYshJ9QGOx*5 xF!@F6 LRJ'
2021-10-26 20:16:46 UTC	114	IN	Data Raw: 83 d3 7c f5 0a bc 3d ef bb 7d f9 94 99 e2 80 cb 18 a1 00 ee e3 fc be d4 fc 9f c2 08 e9 7d 74 e1 9b c3 45 4a 08 7a cd 5c cd 35 09 7e ac 29 82 f6 7d f5 46 ee 2a 02 ce 82 e5 74 c9 c0 c3 91 53 3e 3a ce b8 3b 06 6b 18 2c 83 5f 45 63 26 ab 01 d1 00 49 ea 13 53 2f d4 af 5b b4 2b 40 25 4f 1b 12 d2 78 6a 0a 06 f5 9e 85 3e 6f 21 85 7b fc 5a db 00 27 c2 72 bd ec 6a 1d 59 af 13 b1 a4 da 14 44 8c 80 06 bb 08 d1 33 09 56 95 37 df e1 0c 33 14 98 d9 45 40 12 b1 3c 05 b2 51 c9 0a 33 bc b9 cd 4b 32 91 8a 4a 8d 16 f6 7a d2 7b fc 9b c2 e9 4a 0b b1 5c 4d 45 9a 5a b4 f7 27 f5 34 d8 a2 8c 05 81 ef 7a 5d da 29 83 19 96 3a 51 f7 c6 c1 7a 8c d6 32 d8 82 14 19 ea f4 e2 26 e0 76 c6 f2 67 35 ad d9 27 ff c1 3f ab 54 ad fa 82 06 a8 6b 69 af 89 dc 2e 56 46 4d 88 b9 09 29 bb ed d1 09 cc Data Ascii: =} EJz5-)}F*!S>:,k,_Ec&lS /+@%Oxj>o!{Z'rjYD3V73E@<Q3K2Jz{JWMEZ'4z};Qz2&vg5?Tki.VFM)
2021-10-26 20:16:46 UTC	116	IN	Data Raw: 5a a3 39 92 86 31 31 88 26 3e 8b 7b df 7e 54 ec d0 9f e3 54 20 ac c8 cd 96 32 7a 55 f6 b6 41 69 f6 df f1 4c 77 34 0e 82 98 ba d2 10 75 15 36 49 c9 98 4b 8b 34 26 4e ea 6c a4 92 82 d5 4f ab 99 c5 9f 4b 6a 4b c2 8a 1c ba 65 1b 6b c5 22 55 5c 46 55 5b 0d 5d 41 ca 4d 7b c5 87 f2 b1 67 bc 51 6f ea 9b 38 c4 b8 49 8e 13 cd 3b e9 82 23 64 e1 6a 6e 3e 27 ad f0 4d e8 af 48 48 c3 1d 69 f3 01 b1 1c d3 73 f1 05 d9 4d 7a 80 3d 08 68 d1 36 6d ee 0b a3 07 ba d8 30 68 d4 bb fb b1 89 f6 f9 44 39 1d ba 37 02 ca 17 f2 08 42 b4 b0 2e fe fd d7 92 42 ba be 01 02 f3 5d 9b 12 68 3b ea 5e a2 c5 36 6d cd 64 4e a1 bf db c8 ff 4c 65 54 88 ff c7 c2 36 65 d2 30 b8 23 b7 fc c6 ae 94 8a 8b fc 13 6e d7 9b e2 1c 3a 79 dd f5 ed c0 6e 3c b3 1e 37 2c ad 2c e1 3a c3 09 37 30 b5 0f 7b d8 6e 9d Data Ascii: Z911&{-TT 2zUAIw4u6IK4&NIOkKek"UUFU][AM{gQo8!;#djm>"MHHisMz=h6m0hD97B.B}h;^6mdNLt6e0 #n:yn<7,..:70{n
2021-10-26 20:16:46 UTC	117	IN	Data Raw: 0c a7 19 fc 75 35 a3 5b 9f 79 98 54 74 5a d3 52 c3 6a f7 27 c3 e5 70 3e be 37 38 13 9f 3f 50 76 9c c4 d5 af 68 9f ad 83 d2 fe f4 59 34 83 c6 47 c1 f9 f4 c0 72 5e e9 bb 37 c7 bb 65 47 76 6d bd 05 a8 f8 c2 0a 12 01 5a e8 fb 2e 38 d2 bb 8c bf d2 b4 46 f7 ab a8 55 dc 34 36 f4 f6 36 a9 52 ce f5 ee c1 1a c0 5b a9 1e cf 07 d2 3b c7 a7 9e 82 e9 ef b3 41 47 6d 72 a9 00 01 85 23 42 b2 08 6d 2f 7c 77 ff 14 4c 70 82 90 7c 3d 31 fd 4b f5 bb 92 0e a8 6e bd 25 57 c6 f0 5b 8c 17 45 3f 1c b1 d9 a2 2e f9 b7 98 b1 a9 d9 b2 c4 eb d3 4b 2c 73 b0 4d 98 00 ae 8d 63 48 59 c8 1e d6 c6 72 3a 6d 4f fb 19 a3 ef 95 c0 69 33 f6 25 37 27 14 5b 6e 39 ff d6 04 cf ec e4 fb 09 c3 48 b4 0a 72 30 26 18 cc db 4e 69 ba 55 58 c7 74 58 03 61 70 53 6f 81 ce 47 b0 d2 7a dd 81 1e d3 09 6b 47 33 Data Ascii: u5jyTtZr]p>78?PvhY4G^7eGvmZ.8FU466R[;AGmr#Bm wLp =1KnUb[E?.K,sMchYlr:mOi3%7[n9Hr0&Ni UxIXapSoGzkG3
2021-10-26 20:16:46 UTC	118	IN	Data Raw: 67 c8 4c 4a d1 31 ef a8 60 d1 b1 50 7e ba f3 4c 05 01 c9 22 98 9b 58 3e 3d 73 7d 05 d0 64 13 70 b5 67 b6 7e 39 ef 3a 3c 2f ab 5b 95 1d 7b fe a0 19 8b f7 ef 3e b5 29 76 88 6b cc e0 ce 70 b0 e6 d4 de 9d 41 4b 37 ac 15 6f 3b b9 86 31 d1 ab d7 1f 7f 8f ea 3f 12 ab c9 21 33 98 eb 43 c8 0b 09 e4 0a f8 8c cc 92 3b dc ec 3b 08 ae 89 43 98 89 89 ed c1 fd d7 06 5b bf 7b ac f9 8e b3 b8 c3 05 be 19 ea 05 7b bf fb 24 dd e1 ad e0 7a 79 48 1f cf 82 79 e9 9c ed 65 00 32 14 e6 8f ee b7 3f 29 da 39 3c a0 ce c5 49 77 55 c5 4d dd 2e 51 32 d5 fc 52 78 6b b5 37 90 6d 08 c4 0c 24 6a 1a 02 d1 b2 1c d9 2a e1 24 7c 4e af 3f da db 5e 3d fb b4 5d 1d 18 8a 04 e4 00 6b 7a 82 5a 1d ca 7d 47 45 45 3e 27 4e 42 39 a5 cf 24 7f 09 8a fa db f6 02 1f 4f 9f 64 f4 6c 14 7a 23 1a 3b 1d 8d 3e e7 85 Data Ascii: gLJ1'P~L"X>=s)dpqg-9:<[<]vkv'AK7o;1?!3C;:iG;g[{\$zyHye2?}>lwUM.Q2Rxxk7m\$}*N ^= kzZ}GEE >NB9\$Odiz#;>
2021-10-26 20:16:46 UTC	119	IN	Data Raw: b0 22 9b 12 1f da 27 9b 0d 76 82 89 87 42 ba 69 10 fa aa e0 94 04 23 48 79 4b 1b bf 6f 9d b7 b6 a8 30 23 a3 b8 b0 b6 13 dc 25 23 67 dc 2d 64 ea c1 12 e6 21 42 86 6c 57 d2 bc 3f c6 0d b7 78 08 ae 89 43 98 89 89 ed c1 fd d7 06 5b b3 b3 a1 c7 26 11 ee 03 3f 2c e6 f5 7f 87 bc 03 ec c0 f3 cd f9 48 f8 75 64 fe d0 3d d6 a5 c1 3a 8a 3d 44 fa 5e 7a 31 a4 23 f3 8e f2 b0 32 f3 8c fc b4 3c ed 65 47 71 87 8e 74 93 94 05 cb f8 1a 9f 3b 14 38 14 98 f5 cd 08 4b cb ed 0d ec c8 3d af ed d7 66 ff 99 14 96 14 f4 d7 2d 4b 54 fa ad e6 eb 06 6b 03 9b 08 8e 0c c5 bf d0 70 e6 b0 94 46 a8 84 7f bd 97 c1 7a 78 29 b8 6b f3 fb 6b 4e c8 69 73 24 d5 58 59 fa f9 e9 92 d3 67 4f 23 dc 01 dd 36 22 60 0e c9 68 b0 c7 68 34 a6 74 7a 41 00 33 32 98 63 8d 0b 1c 46 13 7c b9 f0 d3 c8 29 64 1b 82 Data Ascii: "vBi#HyKo0%#g-d BIW?xC[&?;Hud:=D^z1#2<eGqt;8K=f-KTkpFzx)kkNis\$XYgO#6""hh4tzA32cF)d
2021-10-26 20:16:46 UTC	121	IN	Data Raw: 8c 90 ab 34 a6 72 55 a6 4c cd 80 1b 7c 1c 0d 77 40 9b f3 d5 6d d2 02 45 f7 47 44 86 4e c5 ac 71 a0 2d 02 da bd 8f 3a 2f 7d 7f 6d d0 a3 d2 c0 a5 41 b6 a5 41 81 41 e7 f3 82 ce 07 2c 0b 2d 0b 0a 28 0d 7a f4 f2 3c 18 78 3e 60 69 70 e2 d2 e0 c0 6f c5 a6 df 22 cc c3 f9 81 0d 08 3a ef b5 6d 9d 1f 17 67 91 62 9f dd 7d 40 a5 5d 3c 77 1d 1b f1 ed dd 11 d2 21 0e 8f 46 d3 72 b8 04 0a cd 3e d9 e3 35 e4 9b e6 42 4c 59 ff d2 5f b9 52 d9 bb 07 b5 01 8d 94 7c 38 24 ba d7 81 da 98 d8 ff 08 05 ce c9 11 c2 c5 db 92 51 43 68 fb 64 10 83 bc 25 34 91 93 69 06 a9 98 6c d4 9a 71 e9 59 da cc 55 e5 14 33 3a 41 9d cc b8 00 59 61 a4 be 9c c6 e5 6d 80 1b 30 ae 6c 6d 7d 12 81 fb 76 54 ce cb dd 6a 5a 5c 1b 7a 68 d1 84 bd 27 59 b3 6f 74 82 67 40 07 f1 e6 5c 33 7d 20 07 65 19 79 4e 10 71 Data Ascii: 4rUL w@mE_GDNq;-}mAAA,-(z<x>`ip0@]@]<w Fr>5BLY_R]8\$QChd#4ilqYU3:Ayam0lm vT]zhYotg@ 3} eyNq

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	122	IN	Data Raw: ca e1 cc 92 87 85 fe 0c 3f 75 b0 b5 a3 0d 3f aa bd 73 bc f8 8e 7e b6 18 f7 e4 d2 dc 39 f2 6f b8 d1 1d 63 84 e7 f4 04 c6 f9 e8 43 db c6 c5 23 33 ce 5b 85 bb 19 97 cd 53 9b 09 39 32 19 21 2b 5a 9f c5 8e 8d cb e1 6a 8c c4 6c 99 8c 98 ad 36 66 73 e2 b6 f2 36 b9 10 46 36 07 69 69 3e 27 e0 af 70 5c 1b 55 9c 9b 32 a4 23 44 8c 36 16 e8 06 53 b1 24 8d 8d ed e2 76 41 4f e4 78 2f ba b5 91 08 7b 22 c5 96 79 79 ff dc 98 65 86 64 76 45 1f 5c 51 14 6d a3 34 52 b1 89 c5 31 5b ce 55 c4 98 a3 32 db 5b e7 a3 0e 5e 63 26 ab 7f 9c 90 31 db e5 78 11 de 4c 0a 2d 8e c4 58 0e d7 49 3c 86 b3 03 86 ec 75 82 28 ca cc fe d1 86 08 9f 06 3d f4 ea 11 26 77 2c 93 c1 47 8f c2 10 e1 8c 79 4c 42 01 a1 23 f6 37 09 b7 0f 67 21 1e 9c 4f 8b 68 08 96 c2 22 20 b5 6d 38 5c fa cf 23 f3 19 d1 6a 0c Data Ascii: ?u?s-9ocC#3[S92!+Z]j6fs6F6ii> pU2#D6S\$VAOx/{"yyedvEIQm4R1[U2{^c&1xL-Xl<u(=&w.GyLB#7g!Oh" m8#Hj
2021-10-26 20:16:46 UTC	123	IN	Data Raw: 02 7c cf 65 54 bc 55 f3 9d 03 fc bf 17 10 39 f4 d9 1d 59 c3 90 91 8b 13 f9 4d 5a 87 21 e5 56 a5 b0 cb 1f 95 86 12 ca 72 cf 0f da b7 4d 9f 16 b0 79 5a 8a c7 54 4d ac 2a 5e 3f 98 38 77 ea e3 a5 4b 9c 32 75 c9 54 6b 87 2f 69 de e6 cc 03 77 4f be ce 5c be 6f e9 be cc 13 2f f7 df cf ec e5 42 de f1 b3 34 c9 c9 51 32 ff 06 43 b0 81 36 22 10 cd 0d e2 a9 8b eb 9f 1c 48 df 35 6e f5 b8 d4 ed c7 b9 41 3a 37 f9 3c d4 9a 79 03 bf 77 9a 2b 98 0b 73 06 0d f5 4f f0 fa f9 ca fa e6 63 c2 bb 0f 13 1f 17 36 2a 3b 9b c3 37 2a 37 0e 26 0d 6e 57 cd 2b ef fa 98 f1 22 36 26 e6 73 96 37 36 65 e1 a9 0d b7 d2 6b 1f 97 1c f1 ff cc 4b f4 2e 95 a9 80 d1 6a 32 32 db cc 45 15 6a a3 a1 44 a5 cb a7 b5 98 ac cc 31 a6 02 97 4a e3 92 59 f9 91 36 8c 4b 13 87 2d 13 5b 2d 5c 89 d4 cc 11 80 a8 d2 d8 Data Ascii: eTU9YMZ!VrMZYTM^*8wK2uTk/IwOlo/B4Q2C6"H5nA:7<yw+sOc6*;7*7nW+*6s76ekJ.k2E2JD1Y6K{-\
2021-10-26 20:16:46 UTC	124	IN	Data Raw: 5e 7a bc 86 59 f7 76 93 2d 38 c9 9d 9f ec 04 40 5c a8 5d 5c 6a 8e d2 d0 c0 60 8d da 45 01 a1 90 cb 5d 11 ed 60 b8 b1 00 9e 0e 42 99 9b c4 a7 0f 59 63 8e 5a 3b ad be 36 30 16 61 15 c7 17 af c4 c3 3e 6c ba d9 1d 93 1a 3d 1d 7b ec fe cc 09 4d 8f b7 8a ed 71 c7 92 fd 19 1c ab 0c 22 ff 79 28 42 0e 3e 7f c5 7b 75 99 c6 81 c7 9c 40 ae c7 a4 4d e3 a2 f3 3b 44 46 31 af d2 48 7c 9d d1 d5 11 30 02 d2 a3 6e a7 dd 0a 98 ac c6 5c a6 6a b0 c4 c5 b8 aa f8 04 08 de 05 5e 27 7a 5d e5 bd e3 20 0c 81 f3 cf e1 72 d1 64 49 a4 e0 33 3e bb e4 d4 ac 7e 7c 33 ed 18 23 ee 45 cb 7b 2b e3 d3 51 58 f2 1c dd 12 ce cf 08 a2 19 44 a5 42 a8 e1 81 6f 77 5f 86 22 9c 31 88 0a 5d 26 57 6c e2 8d 22 aa a4 2f b4 37 eb 57 64 09 46 3e 86 1c ce 34 4d e4 d8 9f 8b 0f 01 bc e1 f7 6f 87 d5 72 d1 cf ff Data Ascii: ^zYv-8@ j E" BYCz:60a> = Mq'y(B-{u@M;DF1H 0nj^z} rdl3>- 3#E{+QXDBow_"1 &W! 7WdF>4Mor
2021-10-26 20:16:46 UTC	126	IN	Data Raw: a7 d3 d7 83 64 8f c3 3a ed b2 2e f4 8d aa e8 37 1e ce a7 83 fc dc 36 8e 54 c7 d7 77 04 c7 be c0 7c 8f 7c 47 44 90 5b a5 d9 61 4c a3 7b a4 35 d5 48 1b c4 c4 a7 50 d6 89 6f 3b ae ad 68 2c 7a 76 db b0 e4 dd cd f6 65 f7 d2 35 f1 98 8c a1 2f 98 33 63 ad bf 6d 4b ed e9 b4 37 7a 07 f6 03 86 48 a1 d7 59 f0 40 fd 62 19 3d 22 97 55 49 fa 38 81 0f 32 ff 6a 96 cd d8 42 77 96 07 05 77 77 88 57 22 36 79 bc 21 59 21 a1 55 85 24 4a 5b f3 16 ed 5e 8b 88 7a 1e 2c d4 4d 66 c7 10 07 38 2e c3 ef 0d 89 dd ef 52 75 8c 70 28 5a d2 1f 6e 83 f2 e5 97 cd e3 f0 58 57 55 99 44 26 60 cc c2 b3 fc 18 09 ac 8f a8 1e a2 d7 5b d1 fc 56 cc b1 53 4a 55 1e a4 95 61 08 8d 27 0f e6 84 f4 e6 0b ac 34 19 83 38 3d 42 02 51 1b 26 fb c7 af 47 c8 f6 57 a9 1b a4 79 61 d5 4f 9a 76 de 93 8c be 49 85 Data Ascii: d.:76Twl GD aL{5HP;h.zve5/3cmK7zHY@b="U182 BwwwwW"6y!YU\$J{z,0xYM.Rup(ZnXWUD& [VJSJua48= BQ&GWyaOvl
2021-10-26 20:16:46 UTC	127	IN	Data Raw: 67 1e 50 a2 6b 64 2a e9 81 80 c0 cd 34 94 ec 68 8a 63 f6 dd 59 3c ec ad 09 be fc b2 7f 3c 3c 5a 7f c7 df 2f 8b a6 4a 22 c9 e7 b6 d4 28 67 38 f1 6d 45 fe 60 29 42 bc 7e 10 cb 57 01 f1 66 ca 45 99 37 98 6d 0f 6f 8a d7 a0 41 e1 2b 5d df 00 e8 d8 26 ca ab 85 f1 2c 4a 7f 8a 67 8c 52 45 97 3e 3c da 34 ad d1 0f 35 86 ec 63 8d ae 1e d3 4a 4d 66 c7 10 07 38 ba df 6f fe 7b 97 7f 53 a0 de 7e fa f9 49 a9 0f ab ec f3 fc 73 fc 51 3d 5e cf fb ed b2 2f f3 38 f2 90 b5 89 72 07 5a 7c d7 c1 9a 7f 96 1c ff 41 3b 51 29 ee 73 5a 4f b9 ae d6 6c b2 4f 85 ca 23 74 be 70 83 dc 61 8c 99 98 f3 6e 36 cb b2 60 65 5d 07 f5 a0 03 51 b6 45 ae 36 99 7a 0e 19 e1 de 11 b4 76 46 4a 7e e9 6b ad 4b 49 ae ac ac 14 39 d5 23 0d 56 aa 41 4d e5 4c 20 ab 37 1b a6 8c 70 b2 1c 20 62 7f e9 3b 55 79 9f Data Ascii: gPkd*4hcY<<<Z J"K(g8mE)B~WfE7moA+&.&.]gRE>>45cJmff8o{S-IsQ=~/8rZ A;Q}szOIO#ipan6' e QE6z vFJ-kkI9#VAML 7p;b;Uy
2021-10-26 20:16:46 UTC	128	IN	Data Raw: 24 c3 a3 4c 21 02 f4 eb a2 a9 64 5e ef 94 62 5d af e4 be 60 22 7d 84 ac b4 59 99 3f 71 f6 49 2a 76 6d 2a dc 75 9a 23 83 6d e3 6d 6f b4 3f 2d a8 97 2e 9e 21 d0 a1 b9 84 cb 13 40 75 1b 30 f1 49 37 90 b0 8d 8e 21 0a ff df f3 de 36 b5 e8 a5 59 8a 60 74 8a 11 fb ee 68 4a d8 21 c8 1a fc 3f c9 d6 6a 09 f8 5e 07 e9 90 c9 dd f9 38 ac 8b cc 5b f8 0b 2a ba d2 21 3e ea f4 d3 51 6d 7c fa 4c 22 af 92 15 7b 83 12 ad a4 a0 89 76 ac e5 93 90 78 ad 15 ec 40 82 a0 34 d0 da 53 8c b7 fe 76 36 82 7f 82 b5 ef b6 43 73 6d af 79 6a 8f 9a bf ce 06 a1 36 e7 67 ba 78 f8 f1 9e 10 b1 9f dc ea 64 3e aa 48 69 7c a7 19 6e 47 35 bf fc ee 31 27 45 fd 31 c7 69 81 1f 8e a3 b9 25 c9 e5 91 8a 1a 25 9c 22 92 04 01 9b eb 04 ff 2b 04 77 a8 88 9a 02 89 08 41 0e 45 41 0d 76 b1 c9 c2 1e 18 80 43 de Data Ascii: \$L d"b")jY?ql*vm*#momo?-.!@u0I7!6Y!thJ!?!>Qm L"v{x@4Sv6Csmjg6xd>H jG5!E1i%#%"wAEAVC
2021-10-26 20:16:46 UTC	130	IN	Data Raw: b0 a9 3c b4 9d b6 d5 b9 41 9e b5 dd f7 3e aa 93 7a f4 70 b2 cb cd a1 45 15 b3 68 3c db 5a 49 b1 d7 d6 15 1a 36 18 4b 44 6e ad 19 d2 59 57 05 82 0e 35 58 01 73 b3 a2 eb 82 38 1f b4 e8 6e 1d f7 00 41 cd 45 b3 8a 25 0f 2f 85 dd c6 ab f0 1b d9 41 fe ba c8 5f 8e eb ea e6 ea f8 e9 e4 69 6b a3 3a aa 8f ac 5d 1e 0b 6e cf 65 9c 0e 77 c9 f5 59 c7 e2 fb 88 46 fd fd 2f 52 71 27 35 75 f5 23 1d 8d c2 46 a1 6a c5 51 ba 28 d4 54 65 8e 7f 7f c0 9c 8f d2 7d 6f 95 7e 53 67 55 18 73 a0 66 1d 42 4b 00 15 5a 22 41 7c 69 e2 92 8c 21 56 33 5e 9e da 89 94 42 c7 8a ae 94 38 92 1b 45 ec 22 7d 2f 2e 4d 3f 65 c7 9b 5f bb 26 4f a9 1e e1 06 84 0a 2d 1f 45 cc ed 14 35 0e 06 bb 2e 3b bd d7 c2 0e d3 95 63 0e 74 30 e7 03 5d f8 1a 04 8c 9c ba c6 b4 5a d2 96 b4 34 41 ca 5a 7f 05 72 b6 Data Ascii: <A>zpEh<Zl6KdnYW5xS81NAE%/_ik: newYF/Rq'5u#FAJQ(Te)-SgUsfBKZ"A ! v3*B8E"J/.M?e_&O-E5.; ct0 ZAZr
2021-10-26 20:16:46 UTC	131	IN	Data Raw: ca d9 a2 14 59 f7 8e d3 4a 31 7c 3a 2f e3 0b db 69 97 87 38 a7 9b bf 5a f7 4e 03 d1 77 3a f6 13 91 6e ac 60 10 71 4e b4 28 28 72 7d 3f 8a a5 4b 16 1e 9a 7e 2b b5 01 e5 77 53 6e 56 9b 27 ea b8 45 97 25 a3 bb 23 2f e5 e7 0a 27 09 56 d8 c7 97 6d c3 04 16 b2 1c 87 5c 9a f1 6c c9 86 c3 a2 95 c6 b9 0d 8a 99 56 e5 61 29 1b 45 e9 26 9d 28 c8 0d 89 ed a1 69 29 81 4d d2 0a 22 4c db f8 a9 da c1 1f df 61 2b b7 7a b4 49 0e 8b 20 66 1d ee 45 89 a6 90 73 d7 f0 84 f4 2e 21 d6 f0 e8 44 da 89 b4 33 68 e7 d3 2d 13 08 1f 27 1f 5e cf 70 32 87 e0 ff 12 f5 21 d2 2a d3 1c de 8c 7e 43 ba 1b 41 36 e7 6a 4f cd ef 6a 38 0b 8d 00 2a f0 2a 50 d8 03 97 b4 68 b0 14 a8 4a 20 de 97 43 35 c0 03 0f a3 60 7d ce 9a 01 8c ef bb 1d 24 48 e4 fd 7c e2 a3 f3 91 3d 1a 3d cb 6a 52 9e de 74 ef 3b 47 Data Ascii: YJ1 ;/i8ZNw:n'qN((?K~+wSnV'E%#/'Vm V)a)E&(i)M"La+z fE5.!D3h-'^p2!*-CA6 Oj8*PpH C5'}\$H = rj;G
2021-10-26 20:16:46 UTC	132	IN	Data Raw: 12 d4 47 a4 67 57 23 51 24 a9 f8 18 f8 a3 0b de 2b 55 87 b7 c3 a2 9b 6c 09 f6 64 5f e7 0c d6 ef 48 23 61 f5 2f 12 e3 3e 55 9c 88 46 5a 55 9b 98 d4 a2 64 66 53 fc d9 01 cc c8 2a 83 d5 9d 6b c7 22 ea 8a 98 3c 61 78 ec 4f 9c 1d c5 f4 54 f7 24 51 3d ac 86 72 91 59 2f 5c 8b 50 db ae c1 89 a3 c6 5e 24 81 79 17 62 d1 e7 88 63 15 f6 d0 99 f4 f1 9a d0 c9 78 bd 11 e7 50 72 7a 48 d6 d5 9a b8 75 b2 17 57 84 b5 3c 3a 52 4f e5 d0 ae 8f 84 7b 16 32 c2 81 fd 29 79 c0 6b a7 ec e0 a3 ef 9a 33 f0 d3 25 04 0f f6 59 b0 eb 52 0a 8b 34 ee 1b eb a9 10 e5 e1 25 5c a9 d5 a0 d4 9e 33 79 9d 46 25 3b 24 b1 98 7b b5 6e 3a b4 f3 ab 1a 14 62 3e a2 04 1d 59 b9 08 1c ba 36 35 f1 d9 21 18 b1 67 8e a4 59 f1 17 f2 c8 fb fa 39 1f b3 fe dc d6 55 51 9b 3a cb 93 ad 31 a8 e8 16 f1 3a 29 f2 73 Data Ascii: GgW#Q\$+Uld_H#a/>UFZUdfS*k"<axOT\$Q=rY/AP^\$ybcxPrzHuW<:RO{2}yk3%YR4%3yF%;\$(n:b>Y65lgY9UQ: 1:}s

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	140	IN	Data Raw: 41 86 9a 09 35 34 0a 60 8b ac 94 9d e4 44 ad 51 5d 54 7d 70 e7 f7 44 17 f5 b7 63 c3 a5 24 7d ab eb b8 7a a7 2b b6 42 99 71 0e 2b 2e 22 94 60 74 ee e0 b9 0b 5e b8 41 93 29 4d 19 96 4f 36 f5 b4 3c d5 76 4f c7 35 f3 54 e9 ab 27 08 4e 8f eb ba b8 cc 0f cc f3 7c 73 27 7a 17 16 1e 99 4b de 7d ac 92 a3 c6 1b 1d 32 66 de 84 86 36 34 c9 bd c7 08 e2 c4 87 7b 7f a1 28 92 5e bc d1 a6 18 1a 67 09 df 80 16 06 cc 06 02 19 10 40 6a fb 2a 42 31 b3 ae 62 87 e1 09 4c 98 16 31 35 0a 11 01 97 4a dd 73 ee e9 0e a5 45 1b cb 6e db 03 a3 32 62 e9 10 a4 04 95 42 20 52 50 00 30 41 80 88 21 36 63 7e a2 99 7e e1 a9 3b c9 a9 28 70 90 13 55 ad 31 16 30 f1 8b 8b 31 2f 57 5f 04 dc 24 43 3b bd b2 4b 46 d0 f8 cc b9 2c ce 97 a7 b4 d8 78 1f f4 c2 1b 6a 1e 1a 98 41 6f 31 15 53 a3 a1 52 4e Data Ascii: A54'DQJ]pDc\$}z+Bq+."t^A)MO6<vO5_4N; s'zK}2f64{(^g@j*B1bL15JsEn2bB RP0A!6c---;(pU101W_ \$C;KF,xjAo1SRN
2021-10-26 20:16:46 UTC	141	IN	Data Raw: 3d 61 4a 14 95 9a e6 90 d3 26 b3 c1 c3 6b cc cb 58 14 26 15 ce 60 53 97 c0 39 1c f3 b0 56 f2 05 3d 59 c5 a0 02 6c 15 64 7e 55 61 40 34 cb c6 7c 21 0d 78 ce 36 b6 96 8d ca 2a 08 35 6b 1f 1a e8 3e 27 a6 cc aa 84 81 50 45 0d e2 16 99 cf df 68 40 24 f8 eb c8 59 d6 37 80 ca 73 32 b1 e1 ef f5 1e a4 61 36 7b 31 d0 6f ff 5b 4a e4 7f 8e 6a ff bb 6c bd 1b a1 65 cf d8 08 f8 0a 1e 32 f0 03 ff a0 b9 44 46 c1 8b fd e5 7f 80 03 e9 69 64 70 23 84 4d 3f 8e d4 b6 9a c2 3c 37 58 8b c8 bb 8d cc f7 81 86 9b a9 b4 cb b6 16 5e a5 77 7d 7e 7c 40 13 ee ea 6b 3b d8 79 23 e6 f6 02 b4 dd 74 e8 c1 ce 2c b6 75 29 fd bd c2 b8 dc a7 62 bb 20 56 fd 9e ff 49 a6 ba 77 0d 9a 26 a9 f5 bb 40 0e c7 aa 76 f5 e5 2a cb eb 9c 0f b7 78 9b 78 17 23 16 17 78 7a ae 2b 7b 5f 1f 78 e3 99 d7 bb 2a 4d b6 Data Ascii: =aJ&kX&'S9V=Yld-Ua@4! x6*5k>PEh@\$Y7s2a6{1oJ]je2DFidp#M?<7X^w)- @;k,y,t,u,b) Vlw&^v*xx#xz+ {_x*M
2021-10-26 20:16:46 UTC	142	IN	Data Raw: 99 d4 1b 6e fc 8e 57 94 75 d3 85 42 62 5e 5c aa 1f 87 87 ce f6 b6 2f 14 88 76 bd 1b 58 97 2b bd 3b 39 4e c9 ae 9c 5c 3f 9f 97 e3 1e 2d 72 55 f5 a3 b2 26 9f bb aa a4 68 b3 d5 fe 4c fb 48 fb 9f 84 4f 65 3f f0 17 92 ba 0b 86 43 19 a5 6a 28 ff b3 42 80 9f 48 af 82 9e c6 2f 28 cf f3 4b 35 60 9a 3a e8 29 90 cb 16 94 ac fd 7e 54 cb f3 a9 b8 08 78 a8 d7 53 eb 69 82 f7 f4 fb e7 9f ea d6 63 78 16 bd a8 c3 b7 c5 67 e4 6c 35 a6 b3 dd 0c d8 c2 d5 71 e6 96 37 c6 b0 b4 9d bd d6 9a 4a 93 42 2d c4 88 3e 3c 95 b0 f5 86 03 db 50 b6 e0 29 fa f3 a2 3a ea 06 b5 00 7d 08 2f 0a c5 1d 4a 87 b6 05 da a4 ed 23 ea d6 fb a8 94 07 21 a3 93 75 42 61 16 89 ec f4 f0 fd 08 d4 a6 e3 45 1e 95 ac 15 5b 9b 5b 20 22 84 16 d2 f5 db 68 c1 9e 58 a6 5a d0 14 eb e8 4f d1 e4 38 1b fc 74 a5 98 a9 a9 cc 56 Data Ascii: nWuBb^VvX+;9N!-rU&LHOe?Cj(BH/(K5')-TxSicxgl5q7JB-><P):Uj)#!uBaE[["hXZO8tV
2021-10-26 20:16:46 UTC	145	IN	Data Raw: cb 13 57 b0 bf 78 7b 36 50 b0 b2 51 88 db 62 40 79 1a 97 01 f5 7a 59 91 ee 9c fa 5e ba f5 99 bd 04 b4 e0 b2 5c 19 9c 9b 65 ac 10 37 1f d6 55 fc 5c 4d 4e 3f c9 f6 ab f1 e6 5d fe 4f fc f6 b1 52 e9 d1 b1 e6 5d ea 77 9f 48 9b b5 66 72 af cd 62 98 78 96 93 67 10 f0 d3 41 2b e5 9b 56 d8 a3 29 05 84 4b 20 dc d0 bc 81 37 62 8a 83 ea 40 3b fd dc 9c b8 25 10 31 e0 b3 86 f5 23 ce 4f 0d c1 67 1d de 31 05 b6 bf 23 1d e8 b2 a0 06 22 d9 1c b1 59 ea 87 12 66 17 d4 8a 77 24 9d ab e4 7d a5 c5 dc 32 23 f2 58 8c 1e d1 67 a4 a8 28 4c 7d ab bb a1 58 d7 90 8a 54 02 43 02 b1 52 e9 d1 a2 72 0a c5 1d 4a 87 b6 05 da a4 ed 23 ea d6 fb a8 35 36 09 a2 26 48 92 40 96 5a 6a 4b 16 d4 d8 ec c4 c1 44 95 02 43 40 5e 43 be d1 7f 5f e1 5b 6f 48 05 0c 70 e3 b9 59 db b5 8f 54 8e 68 d0 4f e2 7a 46 97 4b c1 f5 59 1f d1 ae Data Ascii: Wx{6PQb@yzY^le7UUMN?}OR]wHfxbgA+V)K 7b@;:%!#Og1#^Yfw\$}2#Xg(L)XTru56&H@ZjKDC@^C _[oHpyTthOzFKY
2021-10-26 20:16:46 UTC	147	IN	Data Raw: c1 a6 11 d0 dc 39 8f 95 ac 26 a2 52 78 b3 d1 b9 36 85 75 9f 3f 02 1d 50 03 f5 05 85 06 98 b1 4e ee 5c ce 23 2c d0 29 10 b1 30 98 a7 f2 fa 23 00 79 53 7b 04 11 0f f2 ad d2 ba d9 36 b8 8c 4e 9d 27 d6 c4 d6 16 d6 d4 41 7b 0c 6e 4e 1e 70 ef 9d c8 d9 81 53 d9 fb 65 26 3e 66 8e 38 1b 44 68 bd 39 53 ea ff 14 ea 18 31 ef a0 ff b7 b3 85 9a 16 0a bc 78 d8 45 75 7c 00 3b 58 10 20 44 64 3b af 5e c1 be 11 94 1a 5b db 93 2d e1 ab bd e1 34 7a 2a f8 ea b2 1d 6c 35 73 c4 38 6a d2 6f af 01 8e 5d de b1 98 e1 33 0c 26 5c 88 99 19 7a eb b1 f4 ca ee b5 21 05 dc 16 9a 9b c9 ea b8 01 5b c0 a4 f0 30 30 bf 1d 81 55 6a 01 26 60 eb 5b 4a 03 25 da 56 e8 d7 7a 9e b5 9f b4 37 2c dd 51 30 57 30 02 b7 93 1c a2 36 be ff c4 9a db 17 c6 41 6f b6 6d f5 e4 da 55 07 12 5c d5 0b 89 03 03 13 17 ff Data Ascii: 9&Rx6u?PN#;0#yS{6N^A{nNpSe&>f8Dh9S1xEu};X Dd;^[-4z*!5s8jo]3&zl![]00Uj; [J%Vz7,Q0W06AomU\
2021-10-26 20:16:46 UTC	155	IN	Data Raw: 9a 4d 3f f2 1b 97 e6 f3 14 e5 a7 67 f0 cd 52 ed 3c 5f 76 b1 08 3a 4b 97 e6 6d 6b ac e5 3b 0b 4a a2 62 50 ef 3c 37 5e 9e c0 ab 82 07 9b 65 60 c2 47 6d d4 a8 49 5c 55 2c 4d 83 12 81 5f c2 99 aa 61 28 0c b3 3c ea 8e 48 1c 59 da 8d 78 b4 15 9a 88 eb 78 55 1d 53 f9 32 25 a3 99 35 53 00 1e 5a e5 6d ae 4b 1f 2c ea 11 93 87 58 47 c5 3b b5 bf e2 59 c9 fe da dd 9f f3 fc 0a b6 9b c7 68 0d 01 bc 72 cb df d5 a2 8d ad 01 1a e7 95 99 03 a9 e4 93 4a 2f c7 4a 73 5e d2 62 2a b9 f2 e0 83 8d a7 60 05 1a bc 09 c6 f8 ce 5d 4e 24 bb 35 3c b6 fd cd 99 ed a1 be 4e 30 42 1f 99 9c 0a 88 04 f0 30 30 bf 1d ce ce 3b 3c ef 68 36 aa 7b ca 99 fd f7 ab 1d 49 df 22 9b 83 38 0f f0 21 58 2d 94 db be 2c 65 f7 b8 4d c6 3d 76 4f 5d 20 e0 80 1d 1a 04 31 ae 53 84 86 46 64 41 c6 b9 28 fc 70 e4 Data Ascii: M?gR<_v:Kmk;JbP<7^e'GmlU,M_a(<HYxxUS2%5SZmK,XG;YhrJ/Js^b*)N\$5<N0B;<h6!["!X;-eM=VO] 1S FdA(p
2021-10-26 20:16:46 UTC	159	IN	Data Raw: 02 a7 e0 cd 9b d2 d2 95 e0 0f eb 46 af 43 82 17 60 d3 18 c3 ab 35 1b 79 c8 84 83 24 8c 43 c1 40 65 9d ac 96 9a 96 c2 bb cb fe 82 7d 11 8d 02 5c 79 06 0f ee 69 dd db ff e5 49 db 8f 7e 84 db 17 67 9d 0f 41 6f 7b 47 22 e1 fb 24 5c b5 5b 5b 60 f1 21 b3 72 6c fa 74 01 16 e6 58 a3 8a f4 34 48 a2 9b 39 08 e7 2e fb 35 4c 61 0e 1a ce 5b c8 4d 65 30 07 33 9c cd 7f cc 93 9b 0a c7 fe 6c 94 f2 85 ff 85 c2 af bb cc bd 4e 1b a4 59 27 98 06 19 52 d5 7b 9d f5 0d 62 49 03 ff 23 65 1b 4d 55 f2 e2 8d f3 c2 06 41 b2 94 2b 9f e8 0c 57 f9 42 73 e2 a2 d8 56 2d ad d2 b2 c3 e7 e6 72 5d 87 1d 2e 8b 5c bc 18 98 72 45 c9 d3 b5 f8 bf 23 c9 b9 a7 8d e2 f3 ca 87 80 9e e7 d0 07 a3 1e 44 63 3e 61 a3 df b4 de 83 e2 fe 0d c9 cc 96 3c e0 4c 7f 90 d6 dd 5d f8 b6 f1 ad 86 70 7c 85 2d e6 c1 a9 Data Ascii: FC'5y\$C@e]yil-gAo{G"\$[! rtX4H9.5La[Me03INY'R b#eMUA+WBSV-r].rE#Dc>a<L]p-
2021-10-26 20:16:46 UTC	169	IN	Data Raw: b3 df de 9d 24 fe 50 3e db db 1d e8 67 f7 67 94 d4 e6 a4 8b 19 f9 a0 b1 8a 67 14 eb e5 df ad b8 1c d4 14 6a 02 46 1a 53 54 e4 ce 88 5d be f6 da f2 59 be 0f 2d 8a f9 e5 9e 45 96 82 00 c4 9d 57 5a 24 9b 03 87 c6 8f 82 f1 2d 04 03 55 4b a0 61 cd 30 a5 e6 b3 0e f1 c8 9b 25 54 5a 68 83 84 54 87 ca be be e2 1b 54 5a ef b4 32 31 e0 37 b3 e0 f5 31 7a f1 21 9c 50 9a 48 5c c8 cf 61 d9 17 18 0f 53 50 90 9b c2 5d ff f1 d0 13 24 81 9d a5 1e dc 72 76 0f 5b 2d ce 72 28 2a b1 0a 5d 35 45 c9 4c f9 19 bc 20 9e a1 48 41 fc ed c0 13 97 ad 91 cf 14 cc 6d 29 a1 c8 39 56 a3 b8 10 2d 57 96 a2 de 33 6d 57 dc 87 6e 20 2d d9 71 de e6 f3 f9 ee 90 8e f6 7c 4b fc 36 1d a0 ec 70 1f 7d 8a f5 b8 eb 46 fb f5 09 76 eb 84 f5 97 2f 04 fc b8 e4 21 52 3c 25 aa a4 2a dd 21 24 67 e9 f5 d5 5c 2b Data Ascii: \$P>gggjFSTJY-EWZ\$-UKa0%tZHTT2171z PHlaSP}rV[-r{^]5EL HAM)9V-W3mWn -q K6p Fv /R%*!\$gl+
2021-10-26 20:16:46 UTC	174	IN	Data Raw: 8e 54 8b 75 72 29 5f c2 30 0c 6e 21 0d a7 fb 58 45 51 89 41 d2 0d 14 c8 51 32 6a 2c 19 8d 32 ab 38 07 d5 dc f7 94 9a e7 46 05 6e a0 68 23 11 c1 f5 e5 91 71 a2 81 32 b2 ee cb 54 58 08 39 d2 1a 3e 08 1d d2 c7 8e dd c6 d3 dd ef 81 eb 58 13 98 7d 20 6b 57 5a 66 13 02 57 01 3d 2b f0 ae 2f d0 db e8 ed 8c 68 32 0d 8f d0 e1 89 67 2f 62 72 cb 0f b9 8d 08 cd e0 af 0d cc 94 1c 79 2a f9 ac ae c7 49 38 83 9f a4 c6 4d 5c ff 6e 8a 86 29 a6 14 eb ac 6e 89 21 90 d0 a9 46 4c 93 4b 1c 96 94 ec 33 7a f6 26 a4 3e 3d 54 1f fe 39 d4 a2 e8 18 98 19 16 b1 fe 57 4a 38 0c 74 76 a2 68 68 58 0e 0c 5d 8a 82 29 da 82 ec ca 14 1c 3c df 89 ae ce b3 99 0e cf 53 15 b0 b5 7a 46 81 3c 25 79 72 75 d9 4c 95 45 91 c7 4e 36 d0 0b e5 26 cd e4 ea d2 69 71 2f 35 cd e2 bc 4c 79 83 46 44 74 e4 a5 52 Data Ascii: Tur)_On!XEQAQ2;28Fnh#q2TX9>X} kWZfW=+/h2g/bry*!8Mn)INFLK3z&=>T9WJ8thvhX)}<Zf<%yruLEN6 &iq/5LYfDIR

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	177	IN	Data Raw: 06 9a cf 24 3f ea 0c 69 7c 5b d3 9f 56 d2 1f b8 ad df b9 b7 bf 37 b0 a5 26 ba 3f d5 ee 7c 59 cd 6f 0d e1 67 0d b7 5a cd 19 d5 09 f6 04 e0 ca 59 39 da 58 29 82 bb 88 81 4b fe bd 7a 48 c3 36 05 0f 1b 95 5f 9e 60 20 bc c1 c5 53 30 85 fa b8 0b 2b 42 bd 19 5e 81 79 d9 10 69 4f e4 06 a0 06 81 d7 c2 b0 cd 18 78 52 32 07 27 c0 bf d6 05 fb b2 3f 13 a4 c6 f4 bf 7a f3 dc e8 f5 a1 7b 62 7f a5 5c d1 7b bf 97 56 68 6b ce 60 42 27 ea b2 0f 9f ae dc 59 db 53 81 f6 76 73 ee ee fa ea 3c ff f5 ec 22 39 a8 e3 b2 43 fa 61 f1 19 50 fa 97 6f 01 b0 c1 75 c5 24 e9 c1 64 63 e1 e3 c8 58 60 6f 14 af 93 97 d6 f8 2d d3 c8 da 43 81 73 c5 e0 e7 53 69 7b 4a ff 7d 29 8a 66 bf dd d2 e9 fb 9c 0b 04 4f 3a 1e b6 87 c4 67 c5 fe ab 60 6e db e6 95 66 68 63 a5 70 de 2e 86 ac 44 73 57 c3 36 b9 2e Data Ascii: \$? [V7&? YogZY9X)KzH6_ S0+B*yiOx2'?z{b{Vhk'BYsvs<"9CaPou\$dcx'c-OcsSI(J)IO;g nfhcp.DsW6.
2021-10-26 20:16:46 UTC	178	IN	Data Raw: c6 26 ab c6 7f 0c 3a 0d 0c 77 c3 b1 6c 78 7d 3c 81 06 33 9f 31 e8 d7 19 13 16 40 e8 bf e6 39 09 62 45 06 d9 4d d1 9e 48 23 31 08 57 bf c3 10 d1 d9 d8 02 0c 11 24 d1 ef 58 52 d0 02 44 df 38 cd 85 1f c0 a8 b7 0d 42 cd 77 07 e9 a3 81 e5 1b ea 44 5e fb f1 ce 7c 38 71 93 0f 89 9d 51 b9 a7 66 01 05 fd 66 19 3d 51 8d 14 30 74 05 ff 11 49 1b 62 d9 fa eb 37 71 30 fc 46 28 0a 3b 33 21 f1 54 32 2c 1f 07 86 12 2a 64 68 ad f9 dd 08 21 8a 88 c9 10 87 1d 41 da c7 19 a5 29 9a 52 b7 a0 9d dc 51 fd 65 f4 bc 4c 47 62 99 d8 59 c2 52 4d b9 bd 22 a3 24 33 c7 ad 87 80 4b 20 e0 c9 a9 f3 1b 57 a5 2d d9 df 36 72 99 99 ef 26 89 2b 66 70 4f 9a 58 1d 69 09 c2 1a fb 65 95 ca 4c 69 82 83 56 1a 34 13 d5 37 a1 8c 18 63 a8 93 bf f0 cc 51 b1 5e 5f c3 1a 4e 1d b0 ee fb 62 15 4d 93 3e ba 7c Data Ascii: &.wix}<31@9bEMH#1W\$XRD8BwD^ 8qQff=Q0tlb7q0F(;3!T2,*dh!A)RQeLGBYVRM"\$3K W-6r&+fpOXieLiV47c Q^_NbM>
2021-10-26 20:16:46 UTC	187	IN	Data Raw: 70 ad cc b5 24 a7 4f 4b 12 18 f9 ed 29 f2 ac 06 ad 32 e1 98 02 8d cc 00 e3 d5 1d c9 18 00 63 18 13 11 39 a4 ae 0d 0b a2 60 e5 33 91 1f 3d e4 76 9f b4 47 e0 15 a9 c2 c4 04 05 e2 fc f8 35 7b 56 97 fb 8c fe 2d e7 41 31 cf 7c fa 38 0f b2 cb 4d 3a af 11 3f dc 9a 64 9e a1 93 e5 a8 48 0f 75 5c 9f 4f 55 64 24 2c 82 42 50 2b 8b 4d 48 8d fa a6 f8 a5 18 15 f8 b7 bf 53 41 12 41 4d 3e e1 57 4c 07 2d 2b 3a 9e 1e 44 fa 3e b6 40 94 2a 2e 85 e2 75 78 1e 3e 9a c9 32 ad a7 34 34 f6 6f 06 a7 a2 6e c9 3c 6e 52 02 85 24 9f b0 16 11 f8 4b fe 2c 5a 16 64 fe b3 42 a2 bc 3d cc d6 5a 66 69 bc af bb 63 c2 33 d7 6f 98 a0 a6 3a aa 45 03 21 77 0b 64 4a 46 21 cd be 6f 42 67 47 ee 84 6a 21 0f 99 db e2 15 d7 06 5d a7 70 4c f5 ea 7c 0a 35 a9 7f 4a 6c 31 a9 70 88 fc c5 b9 88 ed 73 17 f4 a1 Data Ascii: p\$OK)2c9'3=VG5{V-A1}8M:~dHu OUd\$,BP+MHSAAW>L-+:D>@.ux>2440n<nR\$K,ZdB=Zfic3o:ElWdJFloBg Gij pL 5Jl1ps
2021-10-26 20:16:46 UTC	188	IN	Data Raw: aa 42 91 e1 19 c4 6b ea f0 3e 5d 94 53 42 de 82 47 08 4e da 2d df ca 3f e6 84 50 04 f0 69 9a 29 d3 84 19 3d af 95 93 e4 8c ca f9 a4 5e c4 7d 90 3c 29 dd d7 1b fa 58 8a 2a 75 cd 9c e9 fb d9 e9 50 2a b7 99 28 09 5e 81 cc 2d 8d 57 09 b2 f2 ee c9 29 f8 76 2b a0 94 aa dc c9 7c 4f 40 41 22 01 28 46 e5 0d 7d 2f 78 ac 82 10 66 1c 26 10 27 c8 83 16 fb 89 91 87 8f 5e 75 d7 07 89 c7 c5 97 d5 75 7c 50 76 b3 d0 93 39 be 40 5e a5 05 04 08 a9 e4 2c d9 14 4d 19 88 db 1a dd 10 2b 33 a9 03 b6 a0 71 50 93 79 18 1e 4e 4c f1 91 45 c3 12 5a 09 a5 93 66 62 66 dd c1 1c 22 35 88 d1 6e 24 af 15 b5 3a f5 fd a2 23 1c cc f0 b7 ae ab 61 c6 2d 9e 61 93 96 df c9 07 07 6d 20 19 40 20 a1 3b 5b 0c fe 4c 7c 93 25 16 05 e6 6f 3b 41 85 87 c2 a7 c4 8b aa a7 e2 68 5f 9c ba 2f 25 2f 82 6b e5 Data Ascii: Bk>]SBGN-?Pi)=^<)X*uP*(^~W)v O@A'(F)/xf&^uu Pv9@,^M+3qPyNLEZfbfq"5n\$:#a-am I ; :%;Ah _%/k
2021-10-26 20:16:46 UTC	192	IN	Data Raw: e2 b6 f4 8d b6 2a 13 69 94 76 9b 93 27 81 0c 09 62 8e 8b 91 77 90 07 0a b5 29 e5 38 05 d3 64 1e d7 ed b4 e4 29 8d 4a 82 45 2c 54 6e 94 33 6a 91 89 90 1b 50 09 0b 52 de 6a 08 f3 62 7d 83 1f f0 c8 3d 91 15 6f 67 9b 11 74 27 58 e2 01 0b 84 25 16 54 a9 40 ae 26 95 de c7 e2 e4 b0 2f f4 6c 6f 54 c6 93 38 2f 25 6e cb 32 ac 9f eb 68 e2 71 95 c3 d2 64 ef fc 5e 51 93 8f df b0 50 dd 16 bd ae e7 63 6b 2b 23 44 27 67 9c 8b 55 39 50 af 99 cd 62 4d f7 93 ab 99 05 bc 1a 49 c6 b9 f0 9b 40 d5 36 61 ed b0 3c b0 59 4f 8a e0 8b 07 14 9a 87 0b 40 6c bc e3 b1 33 52 23 af 32 b4 32 31 85 ab 80 dc ab 81 d6 69 ed a5 e6 fc 6e cb a6 f1 d4 6d 5b df 9b 66 d1 b7 71 b6 b9 59 fa 09 ca 30 cb 49 b3 63 82 30 46 86 7e 0c 0d 46 b8 e8 a7 9c 36 15 57 3b a2 42 68 ba e3 60 35 06 aa b2 de 3e 9b Data Ascii: *ivbw)8d)JE,Tn3 PRj =ogt%X%T @&/l0T8/%n2hqd^QPck+D#gU9PbMl@6a<YO@l3R#221in[mqY0lc0F--F6W;Bh 5>
2021-10-26 20:16:46 UTC	193	IN	Data Raw: 19 18 3a 81 dd ec 7d 73 a4 72 2a 7f 08 ce a4 56 54 64 2d d6 87 32 96 2f be 56 bf e3 46 75 ac 3f ae 85 a9 3b c0 14 51 65 13 40 ba 4c 5a 6b 94 e9 1b e1 6b 52 75 e4 3b a5 9b 44 f2 51 e5 86 33 ec 01 97 3b 17 35 b0 5e a6 db f4 09 dd 3b 4b 82 85 1a 23 f8 0b a8 5e f5 19 34 07 bf c3 a0 a4 2a c1 51 48 5c 15 d4 ac 60 ae 44 37 64 8c 0a 7c 4a 32 f7 9a cd 4e 19 36 36 d3 4b 50 e7 41 81 ec 81 69 2b 1a 83 c6 09 5a 8a be 7e f8 ff cf 97 e7 fb bb d5 fb d3 6d 38 db 3a 4b 83 1e 2a a9 e0 f7 eb bb eb 01 8b 3f cb 7e fa fc 05 0a 5f 09 ba 8e de a1 1e 0d d8 1c 1e a8 94 b0 2f 2d 3d 5b 60 a1 41 13 78 c0 ce a7 c2 29 a7 14 0b e3 93 b9 ee 6c 10 29 5a 71 b4 ea c5 bf 7f ee ba 2a f5 fa 58 bf fb df e1 32 e2 d0 89 7a 55 1a 5d dc 37 bb 0d 3e 06 cb dd 75 47 0e 6e 24 56 f7 96 1a a9 eb 08 01 48 cd Data Ascii: : sr~VTd-2VFu?;Qe@LZkkRu;DQ3;5^;K#^4^QH\`D7d J2N66KPAi+Z--m8:K?~_K'=[Ax])Zq^X2zUj]>uGn\$VH
2021-10-26 20:16:46 UTC	197	IN	Data Raw: df 41 19 ef 74 63 3f 2a 11 ef d1 9c c8 53 e1 58 b5 79 3a 6a c0 18 3b 16 60 b1 93 9d 0e 68 3b 90 06 8f 62 c0 36 89 16 3b 6b 95 10 03 81 04 f5 62 91 23 6c b5 64 a3 5b f7 46 b4 16 ca ed 93 7d 6f 2f ed 45 e4 81 7f fc 91 3c 54 38 5c 6f 32 42 c9 1f 16 8e ca 21 a8 d0 ad 1f e5 d7 31 40 40 84 82 7a 4d 93 6f 3b 3f 00 ec 37 7a 69 02 ba c8 60 1e a1 4f e6 ff b6 d0 f8 9e 0a 35 0c fb e1 cb d7 a3 a7 ab 35 38 bd f1 e5 fd b6 4e e3 26 7a 74 8d ea d9 f5 d1 96 b1 58 52 89 a4 41 ab 65 0e f2 30 87 eb 56 2d d8 84 56 3d ba 4c 66 f3 4e 7e 1e 7e bc 3d df 97 c9 d5 46 0d e8 8f 98 17 9e 56 19 a3 8b 85 24 95 c0 03 b4 42 b9 5e 83 c5 9a 06 b3 8b 94 b3 93 44 17 44 f4 84 01 95 c5 22 a7 40 cc 7d 33 a8 f9 d2 0d 31 c8 f4 9d be 26 aa ef b1 10 d7 70 68 28 2b 2a c1 fc e6 e1 97 4b 7a 1d 1d 4b 24 Data Ascii: Atc?*SXy;j;h;b6;kb#d[F]o/E<T8\o2BI!1@>zMo;?7zi'0558N&ztXRAe0V-V=Lfn---=FV\$B^DD"@}31&ph(+*KzK\$
2021-10-26 20:16:46 UTC	198	IN	Data Raw: b9 f7 4c a1 ee fd 30 57 d8 aa 2b 67 a9 1a 79 d0 c6 f3 11 00 24 52 c6 76 d3 ce 00 c8 9b 31 26 e0 0c 8a 95 27 04 e2 c3 ee 1d 6c 23 8b 09 11 4f 3f ac a3 56 13 ad 14 c8 e6 bf 12 10 d3 7e 37 ec 10 05 8a c6 98 90 9d 7e ef 48 33 a4 d3 e5 14 9b 38 71 63 50 5e d3 c8 21 2c 21 cd 2e 98 e4 2c 07 ee 2d f7 6e 2c 99 71 8e a4 84 29 39 3a 26 7b 9f d0 ac fe 6c 04 d6 b1 99 45 4e a6 eb 2b 2d f2 e2 4a 5c d9 04 51 2b a4 01 9c 99 05 22 e3 52 28 00 47 bc de 88 e4 60 36 6e 87 e9 63 e9 f8 9f e5 11 4c 51 25 9d 86 c5 cc 02 b8 2c 1f 39 59 29 14 34 88 d0 33 4d 51 96 53 80 52 4b ea 38 ca 7c a8 25 11 e3 01 c7 ba 05 0b 42 7d 1f 3f fe 30 04 bf c4 34 a3 a3 73 77 e0 b7 a0 72 c0 1f 3b f8 d1 75 1b cd 42 32 c8 83 4c d0 32 db a8 c0 43 c5 7b 39 41 12 fb 19 af 34 c9 d8 13 d0 03 c6 58 dc 14 4f 46 Data Ascii: LOW+gy\$Rv1&#fO?V~7-H38qcP^!,.,!.,q)9:&{IEN+-JlQ+R(G'6cLQ%,9Y)43MQSRK8 B%}04swr;uB2L2 C{9A4XOF
2021-10-26 20:16:46 UTC	202	IN	Data Raw: 21 05 a4 90 6b 6e 0c 51 60 29 42 77 e0 40 b3 d2 aa 61 c9 1f 18 61 dc bc ed 45 5a 73 af 90 fb 75 62 39 21 53 46 c0 f4 56 05 47 58 40 33 01 dc 7b 1e 94 f7 2e c6 2c 19 b2 27 59 f2 b0 f9 aa 9b 56 1b b6 59 a3 80 1f ca a6 06 94 55 46 82 d5 1a 54 35 ba 53 aa e6 bc 8c 7b 56 63 b7 40 76 10 4c 39 05 eb 71 10 07 24 cc 8f f4 28 31 35 17 44 62 b8 fc 10 37 45 76 be d5 f1 85 38 c9 53 bc af 58 84 43 e2 03 d6 96 80 40 9f 92 4d 3d a0 37 83 88 47 85 42 42 9c 73 d0 02 25 15 97 a7 4d d0 76 04 24 fc 71 07 1f 8e a4 42 86 79 c8 b9 9b 6a 53 79 28 4b ef 3a de 36 7a 34 96 0e 30 9f 65 45 a4 bf 1b fd f3 2b 21 12 0f 9e c9 9c f0 2e d4 75 86 c2 40 46 33 62 28 34 a7 c5 30 8b 1e 7a 96 e7 10 db 2f 77 d7 7e af 64 db 29 59 c3 fa 19 9e 10 47 f9 69 38 96 45 b4 0d d4 dd e8 33 3e cb 70 f9 74 d6 Data Ascii: !knQ)Bw@aaEZsub9!SFVGX@3{, 'YVYUFT5S{Vc@vL9q\$(15Db7Ev8SXC@M=7GBBs^Mv\$BjSj(K :6z40eE+.u@F3b(40z/w~d)YGiE3>pt

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	203	IN	Data Raw: 04 c5 4f c8 12 1e f0 70 fd 5f 1f 0b 2b 22 69 60 18 13 85 11 cb 80 2d 8a da da 02 27 c7 1f 46 3c 9f b4 9c da 63 6c c1 54 49 db 92 62 7e 9b 42 61 bb ca 81 00 84 87 84 06 89 1d cb 5f 28 90 02 3b 62 34 8c 50 bc 05 52 b8 ae c4 a0 14 2b 63 32 44 57 84 f1 d4 6c 62 51 52 45 a5 33 21 9f c2 64 56 ea 7c 2b e9 24 e7 95 09 f5 88 0c 43 31 64 ef 52 1c 2f ab 64 ed e9 bb a6 1a c4 90 3c bc 71 1e 18 95 35 86 52 f3 21 5b fa f4 b7 fc 36 2e 4c f3 d8 53 b9 41 66 80 21 3e 6b 43 64 a0 42 39 70 5c 96 ce 99 3d 77 92 8e c0 73 84 43 c2 23 55 86 e7 c3 41 12 13 26 b2 e4 d1 9a 3b 40 b6 e8 c3 b8 72 63 0a bb 32 11 07 43 a8 33 a3 27 5a 85 63 d9 b3 98 73 0b 87 0b 6c 9f a4 67 12 29 ed ec 92 2c 11 ed 41 bc ba ea 00 ec 6d a0 67 7a 4e 88 5a 0a 8d 96 50 8c a8 a0 b0 a7 30 21 59 f1 21 ab e2 33 85 Data Ascii: Op_+`i`-F<clTib-Ba_(;b4PR+c2DWibQRE3!dV!+\$C1dR/d<q5R![(6.LSAf!>kCdB9p!>wSc#UA&;@rc2C3Zc slg),AmgzNZP0!Y!3
2021-10-26 20:16:46 UTC	207	IN	Data Raw: 96 fd 49 62 82 d2 19 67 74 af 20 5e e1 79 71 bd 4b fc 8a 8f ed ba 81 fe 9f 6d 3b eb 61 73 35 0e 74 7d 98 a0 e1 67 1e 14 18 9f c8 51 57 3e 3f 4e 47 c9 f1 b2 df 26 e5 3f d5 3f c1 7a 7c 3f bd 2b d7 05 49 52 9b 82 7d a3 2b 90 23 ef 23 cd 44 bd 88 36 60 38 ad 71 28 3c 2c e9 e8 b4 27 35 d1 87 58 a2 ba 69 c1 2b 72 63 31 14 28 a7 db 83 a1 91 8f e8 56 64 e4 87 07 e4 a0 8a 74 5e 85 92 5f 44 76 96 4e 16 71 11 9b 4d 06 8f b5 1a 9f f1 31 26 b9 82 51 9e 03 b8 35 9d fc ff 72 78 10 9b bf ae ff ff f2 f2 fb f5 f7 f5 e5 c1 f3 e1 73 cc 26 d7 b1 c9 91 cb e0 8d e6 a6 2f 29 cc 62 d3 5d 29 79 ab db a5 03 d6 e9 99 30 11 63 79 7d 04 49 23 45 b4 22 3b 9f 9c 20 07 3b d2 89 97 39 28 de f3 53 aa 1c 03 47 7c 02 d3 7b af ce d2 48 00 e2 a5 f1 fd 2a aa 3f b0 3b 14 4e 16 cb ba 15 2f 66 0e Data Ascii: lbgt ^yqKm;as5!jgQW>?NG&??z!+IR}+##D6`8q(<,'5Xi+rc1(Vdtr_ DvNmQ1M&Q5rxs&/b!)y0cy}!#E"; ;9(cSG){H*? ;N/f
2021-10-26 20:16:46 UTC	208	IN	Data Raw: 54 c9 a3 21 30 95 bf 37 68 d5 f0 78 58 fd e6 c2 07 27 e8 1b 2a 53 05 57 6b e6 d0 5a a3 b9 17 86 ee d3 6f ae 44 bc 38 aa 48 08 6d a1 b1 56 d5 a8 32 54 6a 09 43 18 bd f6 2b 50 99 34 6a 08 46 72 70 19 60 9b 57 a2 4a 37 8a 2b ed 9f e6 d1 a8 1c 31 30 6a 20 f3 b5 6d d0 22 c6 cd 59 08 83 9d ab 89 d2 9d 97 6d 02 c2 c8 17 37 4d c2 48 70 6f da 4f 08 60 33 d5 ff 40 42 f4 36 96 d6 ca 89 ae 6a 8b 9a 88 42 3e d5 18 e2 1f 55 5c 32 fa 8a ac 6a cc fd 4d 12 c4 52 b5 45 79 48 ab 4d 5a a3 d3 6e b9 6f b9 46 f8 33 5a 25 96 93 89 8d 3f 00 52 72 cc 0f ff 7c 6b 98 60 21 4b d3 56 3b 7c b5 93 0f 5b 05 0e ae 4a 66 e5 bc 8b 2e 79 95 bf 49 f8 04 84 2e bb e2 7f ae fe 95 86 e4 46 38 ab ff 2f 9e 02 aa be 73 8b fc 41 46 4e a1 e9 29 95 b7 e2 dc 70 53 b5 5b e2 ff 8a 41 ba df 38 5c 7d ce 98 Data Ascii: T!07hxX*SWkZoD8HmV2TjC+P4jFrp`WJ7+10j m"Ym7MHpoO`3@B6jB>U!2jMREyHMZnoF3Z%?Rr!k!KV;[Jf .yl.FB/sAFNA)pS[A8]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49755	172.217.168.35	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	136	OUT	GET /s/quattrocentosans/v13/va9Z4lja2NVIDdIAAoMR5MfuElaRB0RykmrT.woff2 HTTP/1.1 Host: fonts.gstatic.com Connection: keep-alive Origin: https://docs.google.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: /* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://docs.google.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-10-26 20:16:46 UTC	143	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Content-Type: font/woff2 Access-Control-Allow-Origin: * Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/apps-themes Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="apps-themes" Report-To: {"group":"apps-themes","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/apps-themes"}]}\nTiming-Allow-Origin: *\nContent-Length: 26052\nDate: Thu, 21 Oct 2021 06:41:32 GMT\nExpires: Fri, 21 Oct 2022 06:41:32 GMT\nLast-Modified: Tue, 01 Sep 2020 05:20:51 GMT\nX-Content-Type-Options: nosniff\nServer: sffe\nX-XSS-Protection: 0\nAge: 480914\nCache-Control: public, max-age=31536000\nAlt-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\nConnection: close
2021-10-26 20:16:46 UTC	144	IN	Data Raw: 77 4f 46 32 00 01 00 00 00 00 65 c4 00 10 00 00 00 01 62 4c 00 00 65 64 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 b3 d3 08 1c 81 40 06 60 00 85 62 08 30 09 8e 49 11 08 0a 84 be 44 84 95 0b 0b 83 66 00 01 36 02 24 03 87 48 04 20 05 87 30 07 85 35 0c 56 5b 92 4a 71 80 6d 4b a3 81 dd 0e 20 53 5c 92 fa c8 40 b0 71 30 b0 65 36 76 56 04 1b 07 02 01 af b3 24 ff ff e7 25 93 31 d6 dd 66 37 07 40 2a 61 f5 bd 43 42 88 fe cc 92 a8 94 99 d9 3a 25 72 a0 34 24 c5 78 c6 91 38 2f d4 bd 56 e4 a5 a9 91 af ce 13 89 d5 50 0a 72 83 d3 12 64 ca ba 31 f8 c9 59 4d 39 1a 15 0e cf db 10 35 43 8e 66 1f 9f 6f 0f 5f b0 58 2c d1 52 70 8b 2d 4e f3 6f d9 32 df 7a b8 1b 43 93 c5 b7 21 7f 0e 49 86 48 1b f5 be c4 53 66 97 39 e5 fe c9 b9 98 61 dd 98 a7 21 ac 66 Data Ascii: wOF2ebLed@`b0Idf6\$H 05V[JqmK S!@q0e6vV\$%1f7@*aCB:%r4\$8VPrd1YM95Cfo_X,Rp-No2zCIIHSf9alf

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	146	IN	Data Raw: 03 23 72 f0 5f 4d 75 4c 55 aa 4b 3b a7 f6 8f 52 1f 0d 3e 40 6f 42 98 10 58 40 c5 60 10 30 5c 51 05 b7 d9 fb 40 24 f4 5c 02 11 37 67 64 5b 5e b8 96 c1 df 50 4f 38 30 ce 41 b4 b9 7b 4b 8b 66 19 32 fa 6a dc fe 5f 34 77 a5 a4 b0 6b 17 0d 47 14 3e 00 2a f1 03 db 6a a2 e4 9c ab da 61 74 7e a3 df 20 1a f0 28 04 c7 e8 cb 53 d2 7f 8e a5 a1 5c 05 ea 59 ab 6b 03 79 03 54 88 a1 2c 3c 22 40 f2 ee a9 8e f5 c9 68 d7 c2 f7 54 6a e5 8b f8 26 b3 aa 50 a0 6b ce f8 2e c1 36 7e 76 67 b9 68 50 ce dc 74 d3 5d 47 d1 f3 ec bc 1f 06 d9 68 01 f3 80 70 8f 87 72 da bb 6f 55 2d db 69 4d e9 07 ff 04 b0 20 72 c3 af fb 0a b1 5e bb e8 14 2f 2d c4 2f ee 00 7e e0 dc d0 9a 23 6f 99 68 c9 3d 52 a1 7a 2b 7c 85 3a 51 7b 11 99 9f 4c cd 95 bb 1b c0 23 2e f2 16 17 1e 54 31 29 b1 30 a7 0a 9c d9 93 Data Ascii: #r_MuLUK;R>@oBX@'0lQ@\$!7gd[["PO80A{Kf2j4wkG>*jat- (S\YkyT,<"@hTj}Pk&6-vghPtj}GhproU-iM rY/-/#oh=Rz+]:Q{L#.T1)0
2021-10-26 20:16:46 UTC	149	IN	Data Raw: a3 29 98 10 78 f7 fa b2 8c 04 29 50 15 e1 32 1a d4 0c 51 40 d9 39 3d ac 66 44 cd c4 5e 81 7f c8 92 1a 3a 88 31 f0 7c da 83 0d 8a 18 66 73 cf a7 d5 dd 17 a0 5b de 02 8d 52 69 96 25 e0 fe d9 15 41 72 d1 42 bc 85 8f 9c 2c cc 91 b6 27 3c d3 c7 00 79 65 1b ff 78 1b 0c 42 21 9a 8f b7 3d 8e c8 a3 34 5c 5e 5f 92 43 31 c2 32 6a b5 24 41 82 fb 64 9c cd 43 d5 b0 65 2e fd 95 bb 30 75 5c ff d4 45 c7 ad 77 4a d3 19 cd 60 e3 f1 07 f8 d6 7a a6 68 e6 6d 0b 0a 5c 84 9c 26 6b 79 6b 91 11 9f d9 95 40 60 63 23 e6 78 81 be 19 8f d1 e4 2c cb 09 11 85 16 03 15 f1 7d ac 70 c2 8e d7 10 6b cd c4 2c 44 44 25 e2 2a 49 1c d2 ad f1 31 08 72 18 10 47 ce 02 15 e4 28 d0 e1 ce ed 0a 20 79 68 31 de 97 e3 21 22 20 8d 53 44 0d 8f ba 87 f2 6d 44 fe d5 c9 6a f4 df 32 55 27 23 ae 94 b9 53 cd cb Data Ascii: :x)P2Q@9=fd^41fj[Ri%ArB,<yexBl=4^_C12j\$AdCe.0uEwJ'zhml&kyk@'c*x,)pk,DD%*1rG(yh1!"SDmDj2U#S
2021-10-26 20:16:46 UTC	150	IN	Data Raw: 69 5b d5 82 64 32 c7 42 03 be 4a 09 e5 05 d4 be 57 1a d2 2d 48 9c ce 8e 3c 3b a9 ef 1e d1 69 58 91 b6 c2 84 61 95 49 7f 67 89 ae 07 5c b2 65 bf 2a 7f e7 9a ee 37 95 d1 8a 66 df de 6e 73 2a 87 6f 3e 4f 45 de 8e 91 08 77 d0 3c b5 c6 d9 3b bd b1 a5 a8 7a 81 54 c0 eb ef da 6e e2 7f 32 b0 92 5c 6c b7 41 8b 44 71 20 42 e9 6a a2 37 eb 17 f4 c1 d1 3b b6 cc 5e 9a fd 9d cd 31 4f db 76 8d 5a 3b 79 4a cb 98 e0 44 c4 9b cf d5 9f 05 95 38 90 c9 92 b9 e3 42 ce e1 c9 d1 bb 7e 84 74 0f 3c 65 d2 8e ef de ac 14 25 e7 a6 c0 a9 89 05 4d e8 89 0e c8 39 e7 af df 13 e6 e6 7c 3d af 17 52 65 c6 d4 a0 fa 9d 5d b1 fd e2 90 a2 db ec ec dc 9d 11 dd c8 4d fc 6c 85 9a 38 9a 66 cb 08 33 4a 70 14 02 e2 f7 6a 82 74 ab 44 e3 91 55 c5 91 50 bd 06 12 29 e6 a6 9f 15 3b f3 8c f2 49 44 11 Data Ascii: i[d2BJW-H<i;XalgQ*7fns*o>OEW<z;Tn2lADq Bj7;^1OvZ;YJD8B-t<e%M9]=Rej}M8f3pjDUP);lD
2021-10-26 20:16:46 UTC	151	IN	Data Raw: a6 38 0e d5 63 22 f2 37 46 2b e5 af 8c 13 f7 6c ea 6a 16 93 de 48 1b b2 e9 4a 51 86 1d 10 d6 54 f9 49 de 43 10 39 17 30 87 04 ef 1d 63 f8 6d 43 8e 1f 76 80 c0 29 d0 fd dc d6 12 79 2a 60 0d 84 88 73 30 ce 4a 52 bf 1f 51 bb 41 b0 62 94 4f b5 99 5d a6 90 52 be 01 23 19 13 98 38 eb 67 a5 f6 23 bd 2a db b7 ef a9 a9 68 1d c1 ac 1e 36 04 c2 a8 28 f0 94 30 79 eb 72 41 ad 16 53 e0 0e 8a 89 41 92 1b 07 8c f0 41 b6 e1 52 10 fe 04 c5 c4 1f 34 75 ad 4b fa 85 12 11 f5 2e f2 97 fd 72 19 66 ed 0d cc 6e f3 0e 22 79 28 69 db 47 0a 3c a2 08 87 24 76 6f 55 db ad 00 84 ac 0f ea df 33 38 e9 91 51 a3 a8 c8 53 01 1d 3f 34 1b bb bc 3b 66 eb 52 09 e1 22 fb 1f b9 39 11 dc cd 58 51 20 74 20 ea 2f d2 db 84 52 aa 9e 81 a9 28 49 da fc b6 31 1d b4 f6 30 9a 9f db ce fb d1 9f 52 89 28 06 8a Data Ascii: 8c"7F+lJHJQTC90cmCv)y* sORQAbO}R#8g#*h6(0yrASAAR4uK.rfn'y(iG<\$vUo38SS?4;fr"9XQ t .R(110R(
2021-10-26 20:16:46 UTC	152	IN	Data Raw: 0c fc 2c 4c 57 38 31 b0 f7 26 04 e0 c1 93 e7 95 d1 ee d2 76 7a c2 22 13 1a 3d ed 06 a8 fe 73 31 b2 8a 34 57 7c 10 6d 90 f5 b0 f4 7b 1a e5 31 60 f1 09 80 0a b3 46 4e b2 26 a4 19 c1 c9 b0 dd 84 88 73 30 ce 4a 52 bf 1f 51 bb 41 b0 62 94 4f b5 99 5d a6 90 52 be 01 23 19 13 98 38 eb 67 a5 f6 23 bd 2a db b7 ef a9 a9 68 1d c1 ac 1e 36 04 c2 a8 28 f0 94 30 79 eb 72 41 ad 16 53 e0 0e 8a 89 41 92 1b 07 8c f0 41 b6 e1 52 10 fe 04 c5 c4 1f 34 75 ad 4b fa 85 12 11 f5 2e f2 97 fd 72 19 66 ed 0d cc 6e f3 0e 22 79 28 69 db 47 0a 3c a2 08 87 24 76 6f 55 db ad 00 84 ac 0f ea df 33 38 e9 91 51 a3 a8 c8 53 01 1d 3f 34 1b bb bc 3b 66 eb 52 09 e1 22 fb 1f b9 39 11 dc cd 58 51 20 74 20 ea 2f d2 db 84 52 aa 9e 81 a9 28 49 da fc b6 31 1d b4 f6 30 9a 9f db ce fb d1 9f 52 89 28 06 8a Data Ascii: ,LW81&vzb"=s14W m{1`FN&-J:R_Z30xaUnTzj #scthlDgLN'NBFLBvGMt-zX?6AB*S>Zd6Lak2_ofs)O3lJiei g))0,-&9G-.l3
2021-10-26 20:16:46 UTC	154	IN	Data Raw: 61 73 e7 a3 af 8f 6f eb fc aa 9a 53 e2 52 2d c5 c5 0e c1 3b e7 9d 06 fb 9e 6d 16 e1 e1 0c ff 87 46 38 24 8c b0 c5 0a 93 a5 6f 34 cc 39 81 45 f8 56 13 1e ee 0f 66 06 e3 6c db 0f 9a 2a 1d 47 1f 03 19 64 59 5e 20 91 98 e7 29 be 99 fc e0 7d 6a 65 a7 c6 b8 f4 4c 01 c9 a5 c7 49 b0 d3 09 5d fa f7 d4 a8 4b bc 18 c5 d5 d0 a6 1e c6 5d f2 63 31 cb 44 9c 23 07 42 30 44 09 08 3d e8 b0 c1 84 c2 49 f9 16 42 cd 30 a8 a7 d1 a4 40 99 fa 27 8a 15 b9 29 a7 7c 73 60 30 2a be fd 18 7d 0d 42 2d 93 63 ee 5c ae 0f 77 8e 82 ee 9d 43 f2 85 99 0a 5c 2b 8f f6 2b 4b 4b 44 4a 65 a9 dc 21 71 85 6c 6a 4a 5a 10 12 7e ee 32 6e 90 c7 d4 18 eb 7c 9b 06 8b 59 30 a4 dc 6a 4a 47 dc 52 ad 53 22 3f 1f 99 bf 35 9f 6f 23 34 60 da e4 bd 9f 77 ae 95 6e 80 7a a5 b5 24 85 9a 85 7c fa c4 51 c5 12 04 69 85 24 Data Ascii: asoSR";mF8\$049EVfl*GdY^)jleLlKjC1D#B0D=IB0@'j's 0*)P-cwlcw+!Kd)qjJr2nY0jJGRS"?#0#a'wnz\$QlQ\$
2021-10-26 20:16:46 UTC	164	IN	Data Raw: 13 36 f0 3d f0 e9 e9 15 08 f8 6f e1 7f 40 b0 bf 05 7f 03 29 bf bd a6 b7 c6 0c 7f 53 0d 37 3a bb f3 e6 34 1d ca 7c 3f 7c 31 76 68 7f fe 60 73 56 77 51 e1 f9 b5 73 0b e7 9e fe 2f a6 ff 79 cb 33 27 93 f8 67 36 6d df 43 7a 5f be c1 dd ff 3d 08 90 95 73 5c fd 08 6b 77 ff 88 8a 5c fa cf dc 0c 66 e9 cf fd 49 af 7d 3f 1d b6 b7 4f 41 40 10 08 d1 4e 02 f7 07 cd 85 df 41 6c cf e9 dd e6 42 c1 9b bd eb b8 3a 27 0b 00 7a ef ef 6e e8 cb a7 3f 7c 04 b1 23 b9 62 0a dc e0 03 6f 9e 19 73 ce 0f 75 6e da cf 66 76 2a 9c a2 62 7e c8 7a 3e 5d 18 10 12 00 d4 02 41 c1 01 a0 62 a7 7b 9e 7f a5 cd 54 c1 48 f4 3d b8 ef 43 b1 01 84 4a 8 fb 7f 4c f2 88 e5 37 0a a7 f6 c3 80 d3 64 ce f5 d7 5f 32 89 72 7a 9f ca a8 64 e3 a2 6f a5 13 65 21 45 9e 54 47 6f f5 d5 2b e0 d2 6a d3 90 0f 24 c9 e5 af Data Ascii: 6=@)S7:4? 1vh'sVwQs/y3'g6mCz _=slkwf }?OA@NAIB:'zn? #busonfivb-z> Ab{TH=CHL7d_2rzdoo!ETGo+j\$
2021-10-26 20:16:46 UTC	166	IN	Data Raw: 3d 05 70 29 d5 ef d4 16 1f b7 00 89 b5 a2 3c 6a f3 7b ce 89 7c dd 05 69 fe e1 4b 3b e6 25 7e 23 7a d1 3e 1d 21 78 1b 3e 9a d1 e6 be c1 c6 14 4e e9 f4 11 2c b2 5c c1 4d 47 48 39 01 8c 99 cb 42 62 3a a1 06 25 3d 2b 3f b4 f6 05 5b 7a 2f 8e f8 9b 95 0e 31 c4 b0 f8 11 4e 3d 1b c0 3e a7 4e 35 3b 4f c2 00 99 29 d7 76 9c 13 fe 08 60 95 59 21 0a 09 37 aa d5 f0 6f ad ec ae 25 cb 92 0c 60 ea 72 c5 14 1c 14 ee 49 a2 19 30 a7 40 c9 67 0d ce 52 bc 2c 8d 7f 66 7d 25 2d 82 22 82 00 b1 52 b1 3a 9e 6a 02 10 d9 53 31 3f 9f 9d 3d 83 e0 2a 40 bf a1 06 1d 3d 07 fe e8 52 e3 83 7f 53 c9 c1 8b 71 0a 6c 78 86 17 ee 90 db 23 12 da a7 23 84 d7 7e 64 d8 dd db 83 3a f9 7b 9b dc c0 ca d3 ce 67 9d eb 1c 5d 7d 2c 7e a9 cf 97 a8 c0 c8 b9 0b a7 c9 e4 e4 02 9e 32 d4 88 77 60 55 54 8c b7 1b Data Ascii: =p)<j lK;#-#z> >F,IMGH9Bb:%=+? z 1N=>N5;O)v'Y!70%'r!0@gR,f}%-"RjS1?*=@=RSqX##-d: g ,-2w'UT
2021-10-26 20:16:46 UTC	170	IN	Data Raw: e0 05 08 4e db b0 c6 0f 73 52 2f a4 22 21 ac b8 6d ff ad d8 5f 02 a0 94 87 4c 7e 5a 59 67 25 bf 0f 6f 92 35 b2 0c 15 1b a5 2f 48 c1 4b 23 52 88 12 84 8e ae 8c 4a 9f e1 ce 0d d6 85 e8 73 cc 69 96 bc 54 bd 38 48 9f e8 71 10 31 d8 3d 07 8b ab 77 0c c2 25 db 84 c2 6d b8 62 46 39 9d d6 cc 64 af a7 50 d6 f7 1d 68 b1 70 33 36 92 18 bc 5f a6 fd 04 c2 d0 6e e0 fc e7 5e 39 9c 3f 2f 18 c4 3b 79 85 e1 d0 c8 c6 32 b3 91 5d db 46 ba 81 cc cf cd 44 a8 aa 04 ed cf 5c 65 8d 84 97 8b 0d 56 a1 5a 6e 61 85 a8 51 66 5e 20 c6 1c a2 4c a6 8b 45 2a 32 8e a8 24 1a e6 d4 45 f5 1a 14 86 e3 df e8 c2 fa 1d 11 97 dd db 2c 57 2a 04 e5 71 28 9e 24 9e 26 52 20 cd 81 42 84 25 48 15 cf d4 a5 e0 07 2e 9e c7 13 9f 3c 7b 42 42 3f b9 7a 72 cf 17 62 a8 73 0b a5 e9 a0 01 cf a3 dd 3a 37 9f cc a3 eb f8 31 8c 34 79 b1 9a 96 c5 d5 67 52 98 4e 3c f1 6f 98 e8 bf 31 ff 06 db 5b b5 83 66 ef 26 ad 1b f4 56 13 e2 56 f2 13 57 eb fa a3 Data Ascii: NsR!"mZL-ZYg%5/HK#RjSiT8Hq1=w%mbF9dPhp36_n'9?;y2 FD eVZnaQf' LE*2\$wpe;:%;xdZ {#;co(lK'? 7KpG
2021-10-26 20:16:46 UTC	171	IN	Data Raw: b2 e7 e4 c4 03 34 e9 c9 d3 c7 44 fc f9 8b 03 ce 2d 5f be c0 f8 3a 22 02 15 cd 0e 26 25 3c b2 a0 25 34 32 d7 77 cf 8d 4b b9 4b d3 96 4a 9e d9 42 6c 94 02 60 8d 92 e1 9d 85 2b 93 da 7d 94 c8 2c 63 c9 a3 19 33 4a 1e 66 99 bd 3c 54 6e 59 e6 92 87 1d fa e8 85 bc 52 1f 0d d1 e5 78 67 31 94 16 62 23 d6 6e de 83 db bc 9a fb df d2 99 22 17 36 7f 85 13 11 3d 86 9e b5 b6 b5 2b 0c 2b ba 6d 15 ba 8a 3a ab cd 5a 65 a8 2a b0 15 d4 45 f5 1a 14 86 e3 df e8 c2 fa 1d 11 97 dd db 2c 57 2a 04 e5 71 28 9e 24 9e 26 52 20 cd 81 42 84 25 48 15 cf d4 a5 e0 07 2e 9e c7 13 9f 3c 7b 42 42 3f b9 7a 72 cf 17 62 a8 73 0b a5 e9 a0 01 cf a3 dd 3a 37 9f cc a3 eb f8 31 8c 34 79 b1 9a 96 c5 d5 67 52 98 4e 3c f1 6f 98 e8 bf 31 ff 06 db 5b b5 83 66 ef 26 ad 1b f4 56 13 e2 56 f2 13 57 eb fa a3 Data Ascii: 4D-_-;"&%<%2wkkJBl'+),c3Jf<TnYRxl1b#n""6=++m:Ze"E,W*q{&R B%H.<{BB?zrbs:714ygRN<01f VVW

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	165	IN	Data Raw: 49 ec 95 54 4d e5 99 b2 45 f5 fe 2b 19 e2 3a fd 0c d3 20 a8 79 22 ab 88 f4 bd c7 94 6f 6f 82 d8 0c 76 4d 32 89 ce b8 a9 bc f0 37 5f ce 40 ab c8 93 a5 61 51 11 42 93 84 a1 d3 f5 58 24 44 d5 7c 74 29 4b aa 88 75 59 46 ec 04 ee 9f 34 1e ab 82 e6 41 52 c2 66 b0 94 45 b9 a2 3c 8a 00 37 61 ef 4f 50 4d 56 0b 8f 95 6b 2c 00 0f 36 93 75 ab 18 76 bc 21 08 12 a4 ff 5b b7 f4 f3 de 0d f0 ee 84 18 b3 c7 75 f4 52 0b 3d 00 b0 38 06 2f ca bc c3 43 09 ad 01 53 47 5e 0d 75 f3 2a 28 1f 84 07 65 3e 93 27 d4 dc 44 9d f9 e5 50 94 4f 95 b4 39 62 d7 8a 81 18 bb 65 92 a0 dd 83 bc 7a 23 01 b7 72 5c 4e 08 50 8a 86 3a e0 2f 65 1a 9a 97 67 0e 72 91 5f e3 b9 c8 d0 ca ea 25 2a 87 3e 25 61 9b 18 72 e5 18 c2 6b 3b e8 66 b9 d5 5c ff ec 34 eb 67 83 3b 4d 62 13 be d9 7c 2b 4f 7b 87 4b 27 Data Ascii: ITME+: y"oovM27_@aQBX\$D)KuYF4ARTE<7aOPMVk,6u!uR=8/CSG*u*(e>DPO9bez#rNp:/egr_%*>%ark ;f4g;Mb +O{K'
2021-10-26 20:16:46 UTC	168	IN	Data Raw: 3b 4c 74 ca 3e 10 3a d2 55 e9 64 ef 7a 75 e0 ac 10 87 f6 d5 67 23 96 d5 27 64 71 e2 c9 23 3e 9b 63 90 c8 fa e2 d2 65 ec 8c a2 46 80 29 10 82 d8 09 c1 18 a2 8b cd b5 55 aa 7b a8 8d fb 31 03 e8 e7 69 1a 81 15 1a 09 06 e5 f6 79 c4 6d 07 bf e3 32 98 c2 2b 13 6e df cb 88 ee ee fb 85 65 62 7a 4b f7 87 c3 8d 65 d3 20 84 37 5e 15 83 69 21 ca ce 78 80 c3 db c0 d5 fa 09 98 25 19 2e ac 75 c8 d3 3a 68 01 35 2e 65 87 da 29 4f 83 6a a2 3c 32 66 5e 1f 19 f7 88 c2 4f 16 c1 51 c1 b7 de 3f 73 99 0e 54 8f 78 02 5e ca 43 aa 51 3f 5e ed 83 8d 63 60 bf 0c 35 4d da e0 69 37 c2 f6 70 c9 79 97 19 1e 92 95 68 46 17 88 d8 89 b2 1d dc 9a 76 56 0e ab 58 a9 59 dc ed 26 01 25 f1 ec 78 e1 e0 1f 36 a3 50 18 c7 f5 b3 9b 73 6f cf f8 29 cb 7a 48 f6 7a 4c d2 33 c2 60 bf 7d c6 81 e8 74 b1 28 Data Ascii: ;Lt>:Udzug#dq#>ceFU{liym2+nebzKe 7!~!x%u:h5.e)Oj<2f*OQ?zTx^CQ?c* 5Mi7pyhFVvXY&%x6Pso) zHzL3'}{
2021-10-26 20:16:46 UTC	173	IN	Data Raw: cd a8 55 0d 90 c6 bb 31 fc 9e fb e8 77 36 03 a8 55 1c e1 a0 8a af f2 7f 21 4c aa e1 5d 45 cc 0f 4a d9 91 f5 9d e9 67 db 28 ab b2 df ab c7 36 f2 2a 56 53 9b 5a 86 6a 72 f5 24 ca 36 10 d3 b2 4d 6e 12 f6 6b 6c f1 46 fa fa a9 45 a1 32 b0 89 0c 7a 2c 14 32 be 20 ff ef 99 91 77 6c 5b cc 8d ba 8c eb 72 a5 80 88 d2 28 64 cd 92 4c 54 c9 7f 1d 2c ea bc a9 8a 4f 66 38 37 03 47 66 ec af 83 82 4e 2a 90 c4 1c 12 12 71 25 15 41 d6 7a 1b e6 d2 cf fd 55 7d ae 75 c9 90 fd 61 db 1f de cf e7 d6 24 b1 cf 1c 5e 7a a6 fd f3 50 39 b2 74 9a 3a dc 87 2c ed e7 4e 7d c7 18 15 fa 7f 47 b7 f0 14 d0 d4 35 2f d0 67 c7 42 7e 0e 3f 64 97 5d 2d 31 81 20 6b 03 02 76 d0 5e d5 cc e6 3e bb 46 b9 c5 06 ce b3 65 71 4a 39 b6 61 5d a7 ed a7 6f ce 4a dc 9f d0 6f 25 1b a0 c8 b3 48 e8 25 e5 7a Data Ascii: U1w6U! EJg(6*VSZjr\$6MnkIFEz,2 w!r(dLT,Of87Gfn*q%AzU uaq\$z*P9t;N)8qG5mB~?d]-1 kv^>Fe qJ9aJoJoH%z
2021-10-26 20:16:46 UTC	175	IN	Data Raw: 59 85 67 a2 b5 81 32 a0 fe 37 2d 72 72 5b 06 3f 42 8b cb 91 f2 97 d9 f9 8d ef 5b 8a fe 07 07 c1 4c a0 e0 7f 0e fa e3 8a e5 0a 48 5d 43 6a 12 0d a1 68 55 08 ae 1f e1 f4 d4 47 fa a0 27 d8 67 e2 54 5a 6d 04 4d fc ea f9 7b f8 5f 17 ea 5a af 2d bd 72 82 a3 10 5b d2 64 a5 98 70 55 35 45 16 56 fd 6f 26 53 9e a8 8e e0 61 ed 58 e7 db b5 fa a9 63 9c 28 76 ba 26 34 0f 1d 16 61 43 fd 20 ae 7c 67 c1 71 a4 0f b7 61 2b 0c 1c b0 55 c9 0d a5 e8 5c b3 c8 d5 3c cd 19 69 ff 69 95 17 93 af c1 1e b4 70 da 4b 42 4f 88 b2 dd d0 25 a1 be 64 e6 ce 3b e7 8e e7 43 e5 6a 69 5c 52 49 6a 90 35 6b c8 61 dd 3b 12 6a 36 aa ea 58 09 f2 4c 42 21 46 c9 a2 6e 73 e1 5a 8e 32 74 26 c7 e5 8c d5 71 96 64 c8 0b c7 cc 0d 19 15 5d b6 9b 89 45 1d 5c d5 07 0a fc 65 4f d5 71 9b c9 94 3f 30 f7 6a 3a 1d Data Ascii: Yg27-rr[?B[LH]CjhUG'gTzmm[_Z-r[dpU5EVo&SaXc(v&4aC gqa+u!<iipKBO%&C;]lRlj5ka;j6XLB!FnsZ 2t&qd EveOq?0j;
2021-10-26 20:16:46 UTC	182	IN	Data Raw: 88 b0 b2 14 2a 86 35 2c 21 7e 7e 45 51 7f 84 21 dc c2 8a 57 d3 73 c3 74 71 78 6d 16 f6 44 b6 7d 3f be 0c 4f ea d9 7a 35 88 4a 66 12 ef e7 7b ea 6a 74 28 16 1d f4 eb 4b 02 0b 6b 08 49 61 84 d3 5e f8 5b cb 62 6a 04 19 69 a1 15 72 1e de 00 d6 92 43 e4 8e b4 b0 52 1e 72 75 a2 75 e4 fd d9 ce e5 4b 50 74 9c ee 6c 8c 5e 25 8b d2 31 8e 50 95 97 cc ba 63 d9 09 1c 1e 1d af 5b 1a a5 57 cb a2 75 ef e3 28 aa 51 b3 6e 75 94 8a 2b c3 38 4d 74 36 74 59 a6 27 bb a9 c2 cd af 26 20 36 0f 34 5d 34 da da e1 d7 0e 91 1e 65 0a 60 a7 8f de 53 a3 7e 18 94 ef 37 08 41 95 0d 40 fc 82 26 3b e3 27 7d bf a2 7d 8f 82 30 0f 27 bf df ba a2 a6 97 1e 03 04 88 53 0f b5 f7 13 3c 42 56 fb aa fc f0 d2 ed 9b d7 0d c1 2b 62 6a 04 24 dd fa 8f 3c f2 c1 bd 47 51 94 8a 53 8f 81 17 51 5f 65 03 81 Data Ascii: *5,!~EQ!WstqxmD)?Oz5Jffj(Kkkl^!bjirCRruuKPt!^%1Pc[Wu(Qnu8M6tY & 64)e!S~7A@&.);}0S<BV +bj\$<GQSQ_e
2021-10-26 20:16:46 UTC	183	IN	Data Raw: 1e d3 d3 c5 2c f0 23 05 90 18 1a 51 b5 9c ee 2c 9a ce 76 82 7e 9f 73 e8 12 2a e4 69 c4 4a 86 a4 64 26 5f b8 70 29 74 7e a3 2a d2 1d 7d eb 64 7f 5d 97 2f b4 38 5f 17 2e aa ef 12 73 1a ee 7a c7 e9 7d 0e 11 91 f0 25 bd ca 8a eb 7b 5c cc 91 12 21 d1 89 14 b4 35 eb db 35 c0 7c 85 2b 95 26 16 9c 15 3e 22 70 c8 16 85 c1 2e d2 08 95 a0 d5 88 64 21 cb df 46 2e 97 d8 93 52 4b 45 2a c4 e8 86 8c b3 3c f3 b8 26 88 28 52 f1 f9 1a 7c 46 b3 e2 5f f2 ec ac 0f 91 fc 9e 43 f9 03 13 44 62 3b ae fe 15 bd 4e 5c fb bc b1 5d 62 1c fd ff 47 fc ae 97 52 8d e5 4c 4b 0d dd 54 63 be 59 11 99 ec 13 5d 9c d2 c5 07 41 65 54 63 85 71 a2 00 d9 5a 15 9e d5 4c 4b fe c9 76 d7 c7 3e 91 e8 c8 33 48 0d 3b 32 b8 52 6f aa 0e 4d 90 e8 49 f7 50 6e 69 11 cc aa 84 8c 1a 89 ff 90 5f 2a 70 0d 06 cf 5e Data Ascii: .#Q.v~s!Jd&_p)~*}d 8_~sz}%{l55!+&~"p.d!F.RKE*<&(R F_CDB;N!)bGRlKtCY AeTcqZkV>3H;2RoMlPni_*p^
2021-10-26 20:16:46 UTC	184	IN	Data Raw: b8 ef b6 44 11 2a 64 65 1b 54 b5 6c dd 1c a5 5a 68 bd 9e 4a 0b 4d 49 4d 56 b2 89 d1 04 78 36 85 b0 f5 f6 5f 58 ea 22 72 d0 ce 65 aa 27 4f 26 fa 82 64 eb d7 28 57 1c 76 29 ec 68 66 0e a2 e8 a3 1a 39 c1 4a b8 52 75 26 67 c9 af a1 6f 2b d8 a6 ac 7b 9a 28 7c aa 11 f2 4d f2 dd 23 df b6 12 83 6a 5e 0b 3c 9c 68 65 92 f5 61 7a ad 2e 45 97 a6 57 41 90 f6 55 48 7b b8 29 c1 a8 4d 52 47 2b 85 14 fa bf 2c 5e 0e 9e b6 f2 7e 9c a5 ad 16 56 c7 32 9c c5 aa f9 0d 3f 40 11 3f 71 a2 c8 e8 3c 55 a4 db bf c4 02 44 42 bc f0 53 d4 9d c2 9c c4 5f c6 cd dc dd 41 00 b8 04 4a e1 f7 99 05 1c 87 7b 05 37 45 10 12 34 26 8c ba a5 cb 7e 4f 45 b4 5f 05 ce da bd 91 5f 25 98 6e 82 00 6b 61 19 cc 78 38 f2 bc 41 8c 98 d2 cb 6f 29 7c 7a b2 a6 5d f2 ba 17 75 35 6b b6 c4 ef 88 ef d1 4c bb f8 Data Ascii: D*deTlZhJmIMVx6_X"re'O&d(Wv)hf9JRw%go+{((M#j^>leaz.EWAUH)MRG+^~V2?@?>q<UDBS_A J{7E4&~OE_~%nkax8Ao)}z u5kL
2021-10-26 20:16:46 UTC	185	IN	Data Raw: 00 c7 63 63 74 a6 ea 28 a6 72 53 83 03 77 1d fe c5 39 3e 94 6c ec 5c ce 63 50 6a 70 f5 7a 4e 3c 26 15 88 22 83 5b 44 58 5a 04 29 3d 32 6c 6c 4b 01 31 2c 35 39 7c 5e 81 ec b1 77 11 20 d8 1c 96 e8 6c 7c f7 ed 07 75 15 78 44 af 9f 56 fb 7a 9f 46 5e 19 94 62 72 51 de 8c 03 9d ef 75 d8 61 e6 bd 5c 1f 8b 3b 84 e6 46 0d 39 ca 22 1b c5 59 e2 e1 f4 6a 83 08 48 77 c0 e9 7b db 7a d8 7d 9d 0f 2a b5 43 14 ef 35 88 16 38 b1 41 e7 cd d2 5f d6 a3 b8 75 d5 54 96 52 24 3f 0e 50 11 75 e3 87 ab 66 57 f1 69 90 f8 d2 32 e4 9d ce 0e ff 90 29 4a ef 10 71 90 15 1b d8 d0 e7 bc da 40 f2 97 dd f6 eb 2d 49 e4 4a d7 85 94 51 07 11 8e f1 56 1c 46 a9 39 01 18 08 78 a5 6c 11 6b bc d7 66 eb a0 1f f6 f5 38 1d b6 eb d0 15 59 e8 cb bb 93 8c 04 7a bf 70 bb 1d 8c f8 fe 86 64 fe 20 55 bf ac e6 Data Ascii: cct(rSw9> cPjpnZ<&[DXZ]=2lIk1,59!^w luxDVzF^brQua;F9^YjHw{z}*C58A_uTR\$?PuWf2)Jq@IJQ VF9xklf8Yzpd U
2021-10-26 20:16:46 UTC	209	IN	Data Raw: d1 dd 44 46 7f 20 51 58 39 db 43 e3 59 be 93 24 03 a3 62 d3 36 54 c2 65 0e 47 c3 a3 5f cf 32 db 2e ac 60 4a b8 57 f6 8e 9e 18 95 43 04 35 3c d6 3b 79 7f 6d 73 eb b1 ed 90 a0 72 ae c3 22 3f 2d 9a aa 5f 5f ce f0 d0 2b ad 1b 14 c5 1e fe 3b b4 0e e2 d0 ac ad ba 09 75 5b c2 20 ec 1f 2f 79 b5 0d 26 2d 79 5d ab 33 3c 80 eb d8 40 c3 02 32 32 60 77 dc c2 1f 4d 7c 2f c8 f1 d7 d2 63 f0 a1 40 18 64 49 d0 84 8d 4f df 42 10 93 50 17 9b 35 b4 f6 d3 62 c0 bd 15 57 f0 f6 8f 95 31 69 f5 9a 4d 9c ee 19 4b ba 0c 01 c3 38 7b 44 a0 c2 ea d5 af 9d 39 89 a1 c1 aa 43 01 43 05 cf c7 99 43 83 9b a4 c9 e6 48 96 c5 6b 02 1b e8 40 11 23 17 8f ba 55 11 36 10 bd a6 d3 03 10 a3 9c 4f ab 70 9d 38 18 53 a7 8b 35 67 46 da d5 ac d2 8b c4 91 4c 18 c4 64 29 41 99 12 82 bf 1a 32 00 f3 eb 4c 15 Data Ascii: DF QX9CY\$b6TeG_2_.JWC5<;ymrsr"-__+;u[/y&-y]3<@22'wM /c@diOBP5wB1iMK8{D9CCHk@# U6Op8S5gFLd)A2L

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	210	IN	Data Raw: 8a e3 95 92 35 81 68 97 b5 6a da ec 23 68 1c 8e 34 18 42 0a 75 4d ec 41 04 24 55 d7 44 31 0c 95 66 66 15 1d 4d 57 84 c4 eb 7e c6 4a db 54 65 9e 25 91 6b ab 37 9d a3 0e ba be 2b 48 a5 c2 3d 6e cf 90 3a 8c cc f3 95 ee 4b 3b 69 10 65 3e dd 09 3a ac 4f a6 9b 41 61 66 a0 69 61 75 ca 2e ea ec 7a 8f 28 62 b5 0b 84 32 01 42 9c 0e 6a 7e 56 ef 64 11 c6 f1 2a 99 2f a5 6f 1c 81 dd 00 24 99 1f 15 7a 71 cc c1 e4 51 96 62 c0 19 c2 c2 ad 03 40 16 00 3f 2d b6 4f c8 f9 ad 54 80 b3 43 43 d7 ee ce 27 d6 ac 45 45 07 6c d2 c1 64 0c 2d 33 13 17 35 93 29 9c ee 17 11 b1 9e f0 b4 3a 70 6c bb 22 82 1d fd 84 24 74 27 f3 20 f7 41 00 f5 80 e7 b7 5e 4f 7b 78 83 62 c1 88 be 11 63 6b 2b 0c 1a 61 8c 35 0a ff c7 37 45 f0 2e 1a 2b 55 ec 7a 53 10 78 ce 7d e3 61 13 e8 3e 4c 42 49 18 27 a4 d8 Data Ascii: 5hj#h4BuM\$UD1ffMW~JTe%k7+H=n:K;ie>:OAafiau.z(b2Bj~Vd*/o\$zqQb@?-?OTCC'EElD-35):pl'\$t' A^O {xbck+a57E.+UzSx)a>LBI'
2021-10-26 20:16:46 UTC	211	IN	Data Raw: 10 fe 38 63 6f 33 dc 81 f5 06 73 65 ed 93 eb d1 2f a8 de 21 e6 49 95 4e 9b ba 9b 0e 9e 8b c7 75 11 be 23 7f 8e b6 36 e6 d3 f8 76 d8 d8 7d 9e 3a 96 38 43 94 02 37 eb 4f bf 20 de 49 e8 7f 22 e4 b4 c6 8d ad 63 3a 6d f6 b6 0e 19 a8 94 8b be ea 8b dd dc 1b 1a 4e 60 fc d5 68 37 c0 9f b3 4a a9 30 4c ae 55 4a b1 ca f0 8a 1b 98 99 ea 0e ad ee 75 42 2a 97 ac 85 e6 b1 62 e5 39 99 e1 0f 02 f7 bb 20 78 dc 76 9f ad cf 60 1b 18 51 2c 18 8a 2c 89 a3 d0 2b 32 ea ea c9 58 1b e1 ef a4 5c 34 58 64 9f 62 3b 47 7b ac a3 76 0b 40 19 2d 62 87 06 4a da 0e 4d 7a e4 a5 80 3a 24 e1 fb 35 30 be eb e5 17 c2 77 82 8c fb 4e 9a ea 2a 2a 27 b6 78 3e 07 ec 40 ff aa 6e 7f c8 ba 41 b0 64 e4 3c 99 e6 5a 87 2a 96 30 67 96 ba b0 83 3a 60 37 54 c3 51 7c fe de 57 98 98 6d ea 7a d8 1c 84 ab 78 ba Data Ascii: 8co3se!!!Nu#6v};8C7O !":mN'h7J0LUJuB*b9 xv' Q,,+2Xl4Xdb;G{v~-bJmZ:\$50wN**x>@nAd<Z*0g:~7 TQ Wmzx
2021-10-26 20:16:46 UTC	212	IN	Data Raw: c3 f3 ee f7 39 a8 a9 93 83 ef 22 51 57 a8 f1 b8 9a eb 39 f4 4d 5d 98 3c ca af c6 6c 81 61 a3 e9 41 3c 01 24 f9 19 0d 54 68 c0 d9 39 0f 3d c6 ac 00 45 23 d9 e1 50 f5 94 19 44 6e 12 50 ce b4 e8 43 8b 32 20 1b 8f a6 6a e0 05 ac f8 f9 dd 5a 4b b0 1b c2 15 55 98 ab 71 19 fb d1 fd 6a db 5c 4b 1f 01 91 26 ec 35 4d 39 76 51 00 d0 97 ff 8a 04 b4 4c 61 de 9e 82 48 7e 7b 68 a8 fe da fe 76 ad fa db 7c 7a b7 5e b7 d7 6a 09 be 50 b7 70 72 dc 78 ea 89 cc 87 66 6d cb e5 9d e0 f3 35 a9 da ca f0 07 b3 8e c0 0e 2a 51 1c a0 ef 70 67 c0 ca b6 a6 97 b4 82 33 aa 6d 23 b0 f1 a1 d5 2d 4f 6f c6 df cb 93 51 72 2f 55 da 0c 52 f2 32 fb 8e 92 d1 94 c1 97 42 81 65 4b 97 7a ef c4 43 a4 a5 34 d6 74 d8 28 f8 8b f4 24 59 06 de 9e 88 02 19 16 19 8c 3c 6f 1c 95 31 31 d9 4d 62 c8 a3 30 b7 6e Data Ascii: 9"QW9M]<laA<\$Th9=E#PDnPC2 jZKUq K&5M9vQLaH~{hv z'jPprxfm5*Qpg3m#~OoQr UR2BeKzC4t(\$Y<o11 Mb0n
2021-10-26 20:16:46 UTC	214	IN	Data Raw: 42 c2 34 8a c0 6f 3a 4d 15 a9 a6 71 c1 09 ae 1e 35 ec b2 ac 20 94 b7 c0 93 b8 f1 87 90 bd b1 62 ef 44 17 66 96 82 b2 41 1d 8a 0b c5 97 34 69 92 64 71 55 19 b9 d8 9a 9a a1 b3 39 1f 88 02 e0 78 c6 7a f3 d1 05 c8 93 a9 7e 72 88 8a 6f 91 e4 eb f1 e3 93 a6 c8 03 6a 9b ba 96 e5 58 27 d7 34 57 71 d1 fd c3 8b 64 54 b6 31 69 37 34 f4 ea 16 8e 76 e7 ec a8 db 41 69 06 ba 05 12 62 69 b6 86 cc 07 0f bc 18 06 6d 95 61 cd c8 21 e9 e2 b9 20 fb c1 eb b8 de 50 a4 a3 56 bf d1 5d 27 83 59 d2 61 98 97 4c 0a 2f 21 ba 42 14 99 6c e6 52 54 7c 38 6b 12 34 76 74 3b bd 54 a2 3f 00 c0 23 9f 1f 5b 0a 97 15 75 14 b8 13 13 47 2e 63 9f 21 67 33 1a 9f 2b 7d f3 dc 7d 7f 55 66 44 71 74 e3 af 36 bd 35 1f 06 09 8f 6b 7b bd 1a 99 af 55 ec 16 1e 9d 66 51 b7 af ff e8 48 71 5c 68 90 45 7b dc 66 31 Data Ascii: B4o:Mq5 bDfA4idqU9xz~rojX'4WqQdT1i74vAibima! PVj'YaL BIRT 8k4vt;T?# uG.clg3+} UfdQ65k UfQHq e{f1
2021-10-26 20:16:46 UTC	215	IN	Data Raw: f9 4f 5b 26 a6 7a 51 ca 26 74 13 27 c2 8f 7c ab 17 77 74 f0 07 ad f8 8b 2f e5 5d 1b b0 64 63 5d a4 f1 c4 31 be 2b c1 c7 ce 67 0c 3f ce 06 f6 cb e2 12 99 60 a9 20 76 af 47 25 27 85 d6 1b 9b 05 86 a6 95 f1 c7 6f 7a 4d f2 1d 34 ed f0 dc 3a b4 eb 64 80 86 2f e1 b0 10 78 cf 6e e8 79 ca b9 ef a2 bd a1 5d ab f1 da a5 d2 92 aa e1 37 4d 79 7a e8 fd e3 bf 09 cc 71 5b 3e 04 ef 12 80 70 a8 64 ae 04 68 06 29 bb c2 91 0e 05 49 e3 73 d7 5a 13 97 b9 03 6d 64 06 47 c3 a4 64 0e 23 9d 54 28 9f 32 27 7f d1 16 b4 e6 b3 50 c0 bf bb 55 15 1d 7b cb a9 2e 53 f2 ce ae 14 5b 66 91 d0 96 0c 19 66 1b 98 77 2b 12 55 8e d8 e5 c5 93 57 34 0c c9 3a 74 4f cb ee 2e e9 33 5c e8 38 8c 1c 7b 9d 1f 0a b8 22 51 0d bd d9 41 19 dd 47 57 ee 87 c5 2a ac cc 3b 12 24 a4 6d 09 98 c3 20 b3 36 c0 01 ce Data Ascii: O[&zQ&t', w dc]1+g?' vG%oZM4:d xny 7Myzq[>pdh]lsZdGd#T(2'PU{.S ffw+UW4:tO.3l8'QAGW*;\$m 6
2021-10-26 20:16:46 UTC	216	IN	Data Raw: 74 6b 9b aa b9 a5 7b bb 14 7d 2d 66 ed b5 b4 b4 0a 7e 32 1c 98 37 f8 94 4f 4f 6c 1d 89 c9 d9 f3 36 54 c5 f4 9b 98 b4 a5 c3 18 4c 8e bd 65 08 49 63 b2 aa d0 72 25 37 55 18 2f ad d5 c7 36 04 00 fa 13 d0 cd ed 25 f4 96 dd 27 a5 0c 4b 09 dd b8 78 4a 24 6e fb 88 3e 82 fb ef 0c 99 24 c0 c3 93 a4 cb f6 c2 f2 ba 94 a6 cc 98 35 6a 4e a5 9d b7 70 d2 a2 81 2e 8f 88 64 f5 1a 51 d6 18 50 d4 53 7a 73 0b 11 3e 45 05 c9 5b b3 52 60 46 8e 8a 94 09 00 58 18 5d a1 cc ab 84 c2 c9 52 4d cf 99 0e a5 fd c6 be f8 57 9b 78 37 40 ad 9a 18 f2 4c 6d 35 c1 a2 6d 1f 1d 3c 93 4d 6e 66 84 f5 65 c8 6f 64 e0 74 79 2f 98 24 cf 14 44 a8 f6 fc e8 a3 27 cf 4c e3 99 82 72 a5 8f de 4b 67 9d ea a6 67 8a fe 70 a0 06 6d 6f c0 87 01 1f 1e 93 c3 63 66 78 4c 0e 7f 6b cd cc a7 4a 7c 4d 6a 00 4d d6 59 Data Ascii: tk{}-f-27OO6TLelcr%7U/6%'KxJ\$N>\$5jNp.dQPSzs>E[R'FX]RMWx7@Lm5m<Mnfeodyt \$D'LrKggpmocfLk J MjMY
2021-10-26 20:16:46 UTC	218	IN	Data Raw: 19 b0 21 ee d9 fb bb b3 9d 7b f4 5a 29 8e f6 b0 76 68 26 61 b5 ea 49 43 0c f0 57 bf 88 f2 be f0 ed ba cc d3 d8 50 6b 0b b4 de c5 65 e7 b0 df b1 aa 8d ae dd c2 51 f6 7c 88 a6 a6 f7 25 c6 b8 bb 36 dd 54 15 44 60 16 9d 92 f9 8a 7f 88 7f 5d ab f4 f5 f3 00 6d d5 86 a4 19 cc 0c e8 65 ab cf b9 ff ac ac 99 7b 74 cc f0 e9 e1 b7 75 d1 d9 c9 79 24 25 c7 d7 6a d2 d1 9f 10 b9 25 6f dd 34 a0 98 65 1e eb e3 ac 39 0a 3d 3d e6 88 17 4a b1 64 89 67 54 93 87 e2 b7 5b 28 0b 51 88 e5 98 62 de 2f ee f9 81 9e ae f9 41 87 e3 33 8e f6 50 f3 20 26 4c c8 e2 27 0d 51 60 d7 75 aa 9f 92 43 ec 35 59 b6 65 99 46 89 73 2c 2a 95 3e 1e 37 e7 fb 74 98 bf 7b 2a f1 6d 69 d1 7a 69 89 eb d7 ce d0 2a 1c 3e f8 a3 98 fe 2b a2 bf 96 b5 fe 46 e6 72 7b 2a 3c f4 46 8e 7c 76 74 92 57 59 98 bc b3 c9 1b Data Ascii: !{Z)vh&a CWPkQ !%6TD} me{tuy\$%i%o4e9==JdgT[(Qb/A3P &L'Q' uC5YeFs,*>7{*(mizi>+Fr{*<F vWVY
2021-10-26 20:16:46 UTC	219	IN	Data Raw: 86 7b 8b 5f 6b 5a 5f 58 ad a5 dd d7 da 9c d5 e7 f3 ae f2 56 5e 1c 35 a7 3a 6d 1a 5a 2a 57 a1 11 15 87 1d 17 95 84 58 e8 50 3e 82 e9 8a d9 d4 70 5e dd a0 56 9d 62 35 6a 14 cf 12 bc 69 49 a7 16 aa 9c 88 85 ec 9c ed 64 73 3e 3b 85 f2 4e 71 7f 0d e6 cc 70 f1 41 59 35 37 28 57 c9 61 53 32 f6 38 08 77 62 74 ae 6a a5 1a 38 98 74 51 76 2b 56 d7 fc 63 b5 ed c1 73 51 d5 a0 d4 95 28 36 ab 2f b4 d7 99 72 38 6a 9b ba b4 a1 a2 44 8a 10 e0 6e 37 aa d4 a8 02 95 49 29 17 7f 6d 5e ab 4b 50 e9 38 39 38 b8 54 c5 74 b0 14 95 51 93 e2 ac 56 36 70 b2 cb a4 c8 42 c6 e9 3a b8 08 bb 54 c5 a9 26 bf 1 a 4c d8 6b a5 49 25 fd 65 ad c2 d7 40 6c 63 7c 29 fc 6d eb d1 3c 3d 2a 0b 35 5a e0 e8 73 e4 ec ed 6c e9 ea 2e 95 a2 19 d 9 ea 42 e2 43 a8 8e 9a 82 40 6c ed 0a f4 7a 75 a2 89 88 b8 d8 4b Data Ascii: {_kZXV^5:mT*WXP>p^Vb5jilds>;NqpAY57(WaS28wbjtQv+VcsQ(6/rfDn7l)m^KP898TlQV6pB:T&Lk!%e@ c)m<=5Zsl.BC@ zuK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49759	142.250.203.97	443	C:\Program Files\Google\Chrome\Application\chrome.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:46 UTC	220	OUT	GET /a/AATXAJyEMzwYioPomGpTeso8L__wKY3bPrTHt3se5MVa=s50-c-k-no HTTP/1.1 Host: lh3.googleusercontent.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://docs.google.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-10-26 20:16:46 UTC	220	IN	HTTP/1.1 200 OK Access-Control-Expose-Headers: Content-Length Expires: Wed, 27 Oct 2021 20:16:46 GMT Cache-Control: public, max-age=86400, no-transform Content-Disposition: inline;filename="unnamed.png" Content-Type: image/png Vary: Origin Access-Control-Allow-Origin: * Timing-Allow-Origin: * X-Content-Type-Options: nosniff Date: Tue, 26 Oct 2021 20:16:46 GMT Server: fife Content-Length: 476 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 Connection: close
2021-10-26 20:16:46 UTC	221	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 32 00 00 00 32 08 02 00 00 00 91 5d 1f e6 00 00 00 03 73 42 49 54 08 08 08 db e1 4f e0 00 00 00 06 62 4b 47 44 00 5c 00 6b 00 c0 db 46 7f c4 00 00 01 82 49 44 41 54 58 85 63 8c c9 3e c0 30 f8 00 d3 40 3b 00 3b 18 75 16 29 60 d4 59 a4 80 51 67 91 02 46 9d 45 0a 18 75 16 29 60 d4 59 a4 80 41 ea 2c 16 f2 b4 b9 da 4b 73 73 b2 fc fc f5 77 fb be 27 d4 75 10 04 90 e9 2c 6f 67 59 61 21 f6 6f df ff 0c 2e 67 61 05 12 62 9c 25 99 ba 0c 0c 0f 1e 7f 99 32 ef 1a 25 46 51 d3 59 1c ec cc e2 a2 9c 0c 0c 0c 9f be fc a6 d0 a8 e1 95 e4 d1 80 91 ae b0 86 aa 00 33 13 23 84 cb cd c5 12 15 a4 cc c0 c0 70 ed e6 fb 0b 57 df 0d 98 b3 74 34 85 5c ed a4 e0 5c 29 71 2e 29 71 2e 08 7b 20 9d f5 fe c3 cf 27 cf bf 31 32 30 48 4b Data Ascii: PNGIHDR22]sBITObKGD{kFIDATXc>0@::;u`YQgFEu)`YA,Kssw'u,ogYato.gab%2%FQY3#pWt4\)\q.}\ '1 20HK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49767	74.125.143.189	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:48 UTC	221	OUT	OPTIONS /document/d/1hHFEB09XYOGm1F87Tdc5etNXb38nGMO/test?id=1hHFEB09XYOGm1F87Tdc5etNXb38nGMO&sid=71e310a68d1bf3d9&invite=CKvaqcMD&includes_info_params=true&usp=sharing_eip_m&VER=8&lsq=-1&u=ANONYMOUS_06287517911256457317&flr=0&gsi&ssfi=1&ar=1&arat=PbWXfj9XdnHm1A&smv=20&cimpl=0&TYPE=xmlhttp&zx=jzga9o2idvj&t=1 HTTP/1.1 Host: 0.docs.google.com Connection: keep-alive Accept: /*/* Access-Control-Request-Method: GET Access-Control-Request-Headers: x-same-domain Origin: https://docs.google.com Sec-Fetch-Mode: cors Sec-Fetch-Site: same-site Sec-Fetch-Dest: empty Referer: https://docs.google.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:48 UTC	222	IN	HTTP/1.1 200 OK Content-Type: text/plain; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Tue, 26 Oct 2021 20:16:48 GMT Access-Control-Allow-Origin: https://docs.google.com Access-Control-Allow-Credentials: true Access-Control-Allow-Methods: GET,OPTIONS Access-Control-Allow-Headers: x-same-domain X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: S=documents=imCJ5EuNOibRJwjJKmh_dqsb3ZOXHA7nuJhBLPIUFTA; Domain=.docs.google.com; Expires=Tue, 26-Oct-2021 21:16:48 GMT; Path=/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo; Secure; HttpOnly; Priority=LOW; SameSite=none Set-Cookie: COMPASS=documents=CjIACWuJV68QgJbpGqoMnUqB7-WN3AYzLgMBxZ8n3cJa0UHKlyJhbmJfM56buCPnse-sihDA4OGLBho0AAIriVc07sGPF-siLqmfWNF_nlKdDZjM-hjAaRH5m8wNKljrDF7uOgX_5CRGHITcrZkw=; Domain=.docs.google.com; Expires=Tue, 26-Oct-2021 21:16:48 GMT; Path=/document/d/1hHFEB09XYOGm1F87Todc5etNXb38nGMo; Secure; HttpOnly; Priority=LOW; SameSite=none 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 Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-10-26 20:16:48 UTC	223	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49770	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:49 UTC	223	OUT	GET /js/api.js HTTP/1.1 Host: apis.google.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: same-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://docs.google.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: NID=511=Y92BNZ9vutvPx5gYeR8PaBR1g_mjrmCbnEFTAUIP5QU_3dlISckIihC1ufW60kTsttHGwJfh8tX89A0mP3NPzrSONW4oQZwqfZSyaVggZ0e0Vz6RdOINyVMWlqXMM_nDQQU9k8Lua7RTR5hqBAFF4A5J7LsZ4WTk3rzAAoLqY; CONSENT=PENDING+043
2021-10-26 20:16:49 UTC	224	IN	HTTP/1.1 200 OK Content-Type: application/javascript; charset=utf-8 x-ua-compatible: IE=edge, chrome=1 Timing-Allow-Origin: * Access-Control-Allow-Origin: * Expires: Tue, 26 Oct 2021 20:16:49 GMT Date: Tue, 26 Oct 2021 20:16:49 GMT Cache-Control: private, max-age=1800, stale-while-revalidate=1800 Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="AZM8iraZH88pL4jQdjcWpuaSZEaZk6SzMEy_nltKJ7e9QFt" Report-To: {"group":"AZM8iraZH88pL4jQdjcWpuaSZEaZk6SzMEy_nltKJ7e9QFt","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/encsid_AZM8iraZH88pL4jQdjcWpuaSZEaZk6SzMEy_nltKJ7e9QFt"}]} Content-Security-Policy: script-src 'report-sample' 'nonce-AV5KFtyq7/afnF7Pw+laPQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri /_cspreport Strict-Transport-Security: max-age=31536000 Server: ESF X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff 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 Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-10-26 20:16:49 UTC	225	IN	Data Raw: 33 32 31 62 0d 0a 76 61 72 20 67 61 70 69 3d 77 69 6e 64 6f 77 2e 67 61 70 69 3d 77 69 6e 64 6f 77 2e 67 61 70 69 7c 7c 7b 7d 3b 67 61 70 69 2e 5f 62 73 3d 6e Data Ascii: 321bvar gapi=window.gapi {};gapi_bs=n

Timestamp	kBytes transferred	Direction	Data
2021-10-26 20:16:49 UTC	235	IN	Data Raw: 69 6d 5f 73 6f 63 69 61 6c 68 6f 73 74 3a 22 3a 22 68 74 74 70 73 3a 2f 2f 70 6c 75 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 2c 22 62 61 63 6b 64 72 6f 70 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 63 6c 69 65 6e 74 73 33 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 63 61 73 74 2f 63 68 72 6f 6d 65 63 61 73 74 2f 68 6f 6d 65 2f 77 69 64 67 65 74 2f 62 61 63 6b 64 72 6f 70 3f 75 73 65 67 61 70 69 5c 75 30 30 33 64 31 22 7d 2c 22 76 69 73 69 62 69 6c 69 74 79 22 3a 7b 22 70 61 72 61 6d 73 22 3a 7b 22 75 72 6c 22 3a 22 22 7d 2c 22 75 72 6c 22 3a 22 3a 73 6f 63 69 61 6c 68 6f 73 74 3a 2f 3a 73 65 73 73 69 6f 6e 5f 70 72 65 66 69 78 3a 5f 2f 77 69 64 67 65 74 2f 62 65 6e 64 65 72 2f 76 69 73 69 62 69 6c 69 74 79 3f 75 73 65 67 61 70 69 5c 75 30 30 Data Ascii: im_socialhost:":"https://plus.googleapis.com","backdrop":{"url":"https://clients3.google.com/cast/chromecast/home/widget/backdrop?usegapiu003d1"},"visibility":{"params":{"url":"","url":"socialhost:/session_prefix:/widget/render/visibility?usegapiu00
2021-10-26 20:16:49 UTC	236	IN	Data Raw: 22 3a 73 6f 63 69 61 6c 68 6f 73 74 3a 2f 3a 73 65 73 73 69 6f 6e 5f 70 72 65 66 69 78 3a 5f 2f 77 69 64 67 65 74 2f 72 65 6e 64 65 72 2f 63 6f 6d 6d 65 6e 74 63 6f 75 6e 74 3f 75 73 65 67 61 70 69 5c 75 30 30 33 64 31 22 7d 2c 22 63 6f 6e 66 69 67 75 72 61 74 6f 72 22 3a 7b 22 75 72 6c 22 3a 22 3a 73 6f 63 69 61 6c 68 6f 73 74 3a 2f 3a 73 65 73 73 69 6f 6e 5f 70 72 65 66 69 78 3a 5f 2f 70 6c 75 73 62 75 74 74 6f 6e 63 6f 6e 66 69 67 75 72 61 74 6f 72 3f 75 73 65 67 61 70 69 5c 75 30 30 33 64 31 22 7d 2c 22 7a 6f 6f 6d 61 62 6c 65 69 6d 61 67 65 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 73 73 6c 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 6d 69 63 72 6f 73 63 6f 70 65 2f 65 6d 62 65 64 2f 22 7d 2c 22 61 70 70 66 69 6e 64 65 72 22 3a 7b 22 75 72 6c Data Ascii: "socialhost:/session_prefix:/widget/render/commentcount?usegapiu003d1","configurator":{"url":"socialhost:/session_prefix:/plusbuttonconfigurator?usegapiu003d1"},"zoomableimage":{"url":"https://ssl.gstatic.com/microscope/embed/"},"appfinder":{"url
2021-10-26 20:16:49 UTC	237	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6564 Parent PID: 476

General

Start time:	22:16:41
Start date:	26/10/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://docs.google.com/document/d/1hHFEB09XyOGm1F87T0dc5etNXb38nGMO/edit?usp=sharing_eip_m&rtopf=true&sd=true&invite=CKvaqcMD&ts=6178419e'
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 6752 Parent PID: 6564

General

Start time:	22:16:43
Start date:	26/10/2021
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 --field-trial-handle=1560,8177781781073637063,12308943224005517833,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1912 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis