JOE Sandbox Cloud BASIC

ID: 511809
Sample Name: SEMqjw.exe
Cookbook: default.jbs
Time: 17:20:46
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report SEMqjw.exe

Overview

General Information

Sample Name:	SEMqjw.exe
Analysis ID:	511809
MD5:	1eeced28416a15..
SHA1:	eb423477cacd23..
SHA256:	b5070e72b3a0b2..
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

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

Signatures

Antivirus / Scanner detection for sub…

Multi AV Scanner detection for subm…

Detected potential unwanted applica…

Machine Learning detection for samp…

Tries to harvest and steal browser in…

Uses 32bit PE files

Queries the volume information (nam…

Sample file is different than original …

PE file contains strange resources

Allocates memory with a write watch…

Tries to load missing DLLs

Uses a known web browser user age…

Checks if the current process is bein

Classification
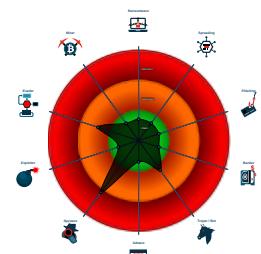
Process Tree

- **System is w10x64**
- SEMqjw.exe (PID: 6564 cmdline: 'C:\Users\user\Desktop\SEMqjw.exe' MD5: 1EECED28416A157BB6C1915C75F01BD3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

💡 Click to jump to signature section

AV Detection:

| Antivirus / Scanner detection for submitted sample |
| Multi AV Scanner detection for submitted file |
| Machine Learning detection for sample |

System Summary:

| Detected potential unwanted application |

Stealing of Sensitive Information:

| Tries to harvest and steal browser information (history, passwords, etc) |

Mitre Att&ck Matrix

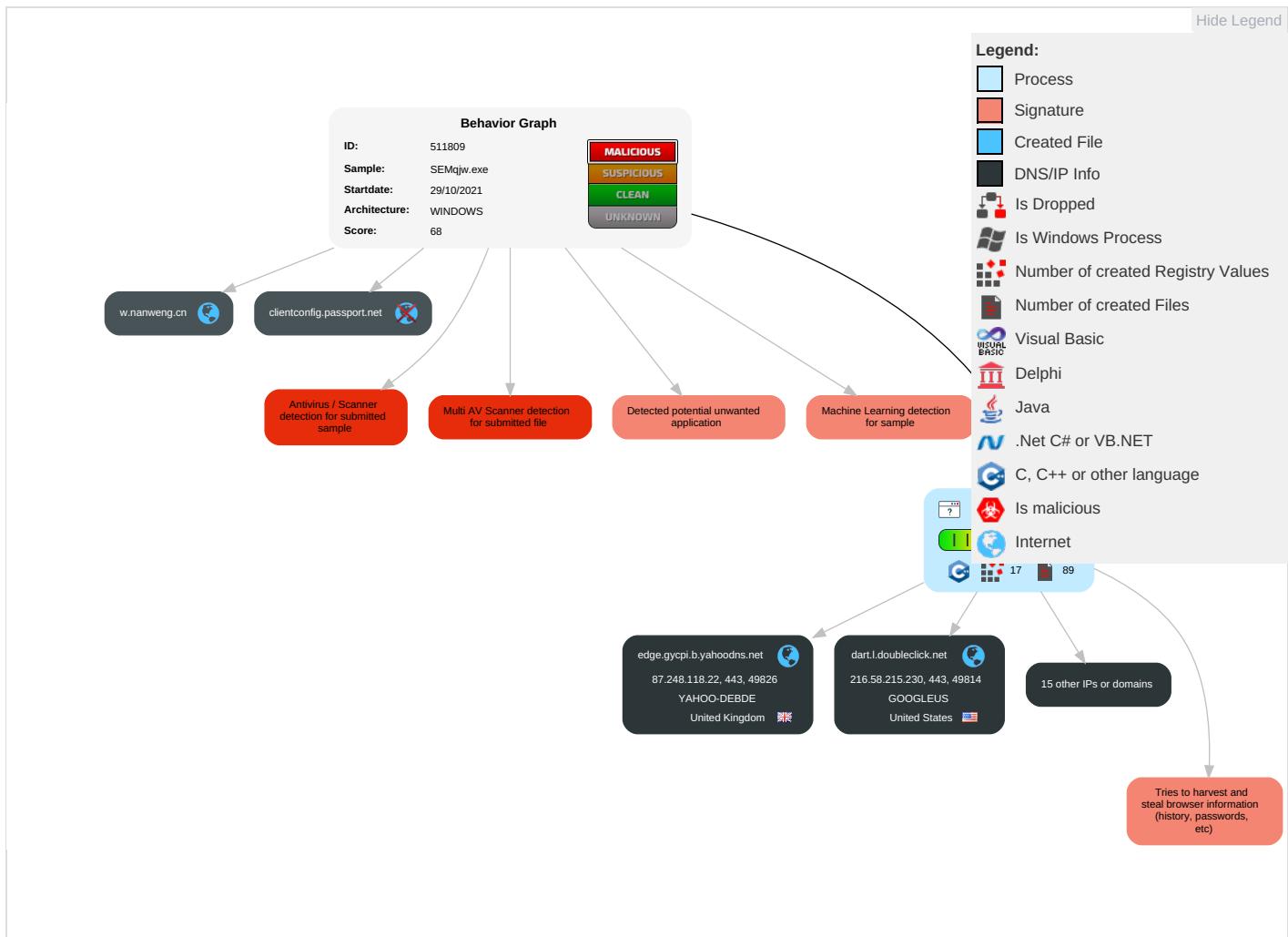| Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	DLL Side-Loading 1	Masquerading 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Data from Local System 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph

Behavior Graph

Behavior Graph

ID:	511809
Sample:	SEMqjw.exe
Startdate:	29/10/2021
Architecture:	WINDOWS
Score:	68

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

w.nanweng.cn

clientconfig.passport.net

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Detected potential unwanted application

Machine Learning detection for sample

17   89

edge.gycpi.b.yahoodns.net
87.248.118.22, 443, 49826
YAHOO-DEBDE
United Kingdom

dart.l.doubleclick.net
216.58.215.230, 443, 49814
GOOGLEUS
United States

15 other IPs or domains

Tries to harvest and steal browser information (history, passwords, etc)

Legend:

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

Hide Legend

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
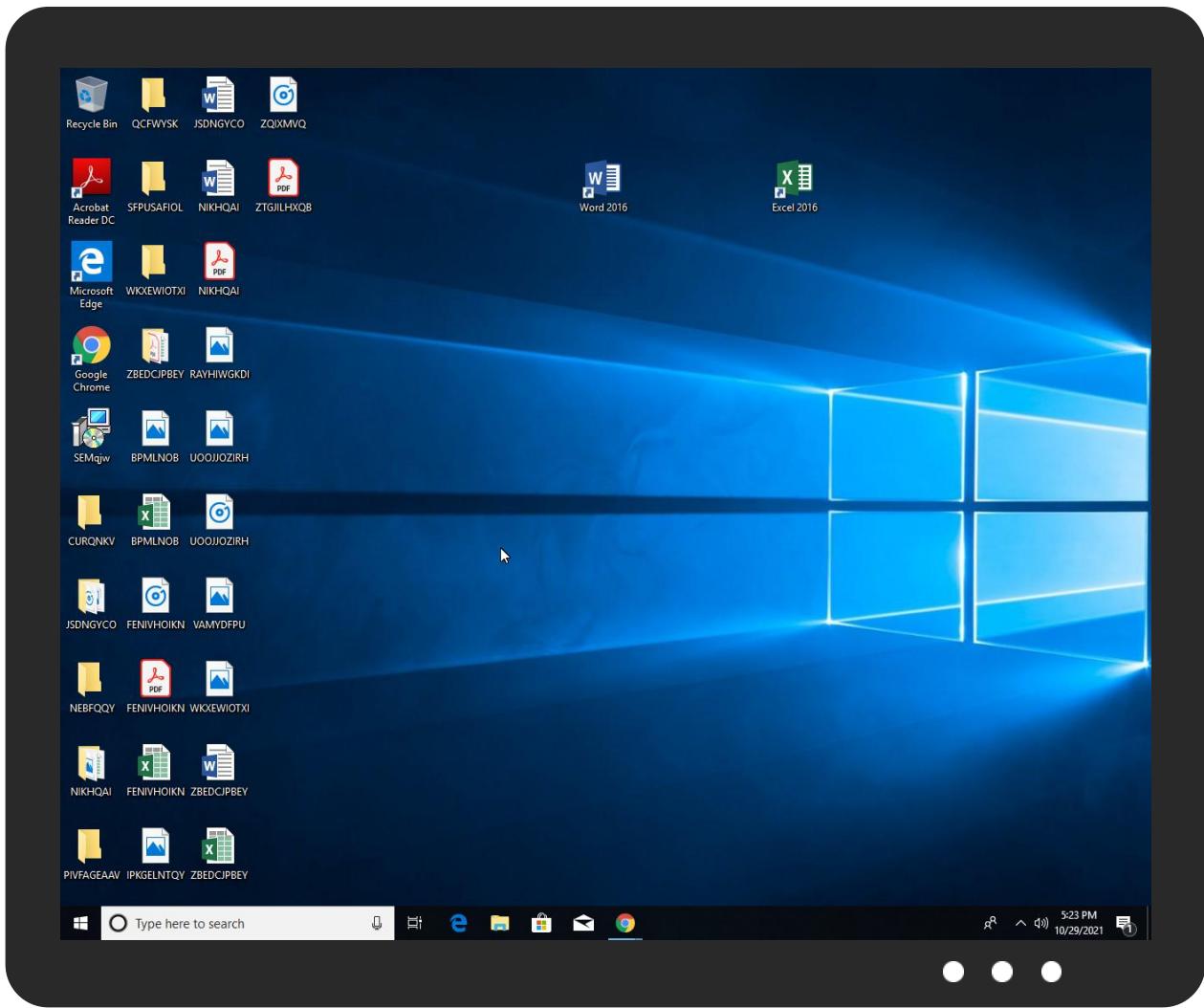
Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SEMqjw.exe	29%	Metadefender		Browse
SEMqjw.exe	82%	ReversingLabs	Win32.Adware.Qjwmonkey	
SEMqjw.exe	100%	Avira	ADWARE/Qjwmonkey.Gen	
SEMqjw.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.SEMqjw.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comout	0%	Avira URL Cloud	safe	
http:// https://contextual.media.netlogid=kfk&evtid=agptslogt.mnjs.stu.checkItemExistst.mnjs.stu.isObjectEmp	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comBibl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/6	0%	URL Reputation	safe	
http:// https://contextual.media.netlogid=kfk&evtid=agptslogFORCED_HIDE_BLOCKbidStreamUrlGcpEulogid=kfk&evti	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://www.sajatypeworks.comta	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0C	0%	Avira URL Cloud	safe	
http:// https://lg3.media.netSTOP_SENDING_PIIbidStreamUrlGcpApaclogid=kfk&evtid=alsspServerScriptUrllogid=kf	0%	Avira URL Cloud	safe	
http://https://c21lg-a.media.netbidNonStreamUrlWestOriginAPPLY_GOOGLE_RESTRICTIONhttps://contextual.media.n	0%	Avira URL Cloud	safe	
http:// https://contextual.media.net&https=1&act=headerBid&prvReqId=237211076658808661635553328200&erTr=0&hl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp/datenschutz-ssp.html	0%	URL Reputation	safe	
http://https://hotmailproxy.betaplace.com/pm/v1.0/getheaders.aspx	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
hblg.media.net	23.211.6.95	true	false		high
w.nanweng.cn	47.102.38.15	true	false		unknown
lg3.media.net	23.211.6.95	true	false		high
btloader.com	104.26.7.139	true	false		unknown
geolocation.onetrust.com	104.20.184.68	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
ad-delivery.net	172.67.69.19	true	false		unknown
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
s.yimg.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
clientconfig.passport.net	unknown	unknown	false		unknown
cvision.media.net	unknown	unknown	false		high
dcdn.adnxs.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/z3nJ.i0wJLUKE.PUO3hx1w--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1634277746662-1414.jpg	false		high
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.69.19	ad-delivery.net	United States	🇺🇸	13335	CLOUDFLARENETUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom	🇬🇧	203220	YAHOO-DEBDE	false
216.58.215.230	dart.l.doubleclick.net	United States	🇺🇸	15169	GOOGLEUS	false
104.26.7.139	btloader.com	United States	🇺🇸	13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States	🇺🇸	13335	CLOUDFLARENETUS	false
47.102.38.15	w.nanweng.cn	China	🇨🇳	37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511809
Start date:	29.10.2021
Start time:	17:20:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SEMqjw.exe
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:	22
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:	mal68.spyw.winEXE@1/62@32/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:21:38	API Interceptor	5x Sleep call for process: SEMqjw.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.69.19	0001.dll	Get hash	malicious	Browse	
	invoice_32.dll	Get hash	malicious	Browse	
	0001.dll	Get hash	malicious	Browse	
	Qxioyfdvub.dll	Get hash	malicious	Browse	
	sgRkrN.dll	Get hash	malicious	Browse	
	0x00020000000155fc-286.dll	Get hash	malicious	Browse	
	ytr.dll	Get hash	malicious	Browse	
	Documents.dll	Get hash	malicious	Browse	
	Documents.dll	Get hash	malicious	Browse	
	zes2.dll	Get hash	malicious	Browse	
	KKeBnxkGGg.dll	Get hash	malicious	Browse	
	vdbb9MZTVz.dll	Get hash	malicious	Browse	
	zq8o6y1z60.dll	Get hash	malicious	Browse	
	New PO_NO20211010-7353 Bisco Industries.dll	Get hash	malicious	Browse	
	a04.dll	Get hash	malicious	Browse	
	3JWv5bYojD.dll	Get hash	malicious	Browse	
	3JWv5bYojD.dll	Get hash	malicious	Browse	
	jLluep47xI.dll	Get hash	malicious	Browse	
	jqzMAYCER2.dll	Get hash	malicious	Browse	
	TooltabExtension.dll	Get hash	malicious	Browse	
87.248.118.22	http://us.i1.yimg.com	Get hash	malicious	Browse	• us.i1.yimg.com/favicon.ico
	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif
	http://t.eservices-laposte.fr/TrackActions/NzA0YmE3MTRiOTg4NGEyM2E4Njc4ZDlyNGVjNmJmMTYzMDQxMzhmZTVjNzEyMDU2OTMxM2JkODcxMDUzMmYxY2ZlZWFjODU5ZDUyYzM3MGQxNzM2YTU1NjRlOTA0YWUzZmY4Mjc4MDQ2YWFzY2ZkZDA5MWWQ0MWE0OWJmODc4NWM2ZDA2YWI4MmJmYmRkNGNjZTQyNmRlZjRkNjMyM2NmNTUyM2FlZDI5NmVjM2UzMmUyZThhMjEwMzk0MzYxMzI1MmExeZjBiMmU5ZWNjMDg0OTY3YTZhYWZkOTMzMGQxZWI0YjBkZmM1MjBkNzQyM2QzMTY4MjjgyOTJjM2QwZGUxZmVkZTU1MjhiZTE5YjdhY2MwNTQ0ZjdkMGJmODNjNzYwODY2ODY5M2RhZjjgwMjAzMzcxNzM5MjjBjM2QxOTI0MzQ5OONDhhMGNlNWYwNjlmZGY5YjcjwNDQ0ZGQ4MjM3ZGM0Njk4MzU0MWWRjYjE0ZTRiNDk3NWM1MDAyYjYxZGIzMGI2NzllMjg4ZTTYxNjhlZWViYzM1ZDcwNDJhYjjg4NjhlNTA5NjAyZTc3M2TJkODExM2NhZGRiYTYwM2Y3NDRmNmY5MDY5MTU0N2l3NGE1MzhiMzA5OGFhYmVZjZjZjkkN2VhNDQzMjljNzM5MWWU1ODM1ZDg1YzViYjVmODMzZGNmYWRmODc3MGM3MTZkZGU2ZjFkYWU4NTNlNGQ0OTFkYTM5ZmQzOA	Get hash	malicious	Browse	• yui.yahooapis.com/3.4.1/build/yui/yui-min.js
	http://www.knappassociatesinc.com	Get hash	malicious	Browse	• www.flickr.com/photos/knappassociatesinc/
	http://https://skphysiotherapy.ca/FEDWIRE/	Get hash	malicious	Browse	• cookiex.ngd.yahoo.com/ack?xid=E0&eid=XjSTxQAAAemDVVL0
	Doc.htm	Get hash	malicious	Browse	• l.yimg.com/a/i/ww/met/yahoo_logo_us_061509.png

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hblg.media.net	0001.dll	Get hash	malicious	Browse	• 23.211.6.95
	0001.dll	Get hash	malicious	Browse	• 23.211.6.95
	invoice_32.dll	Get hash	malicious	Browse	• 23.211.6.95
	Project update-xl32.dll	Get hash	malicious	Browse	• 23.211.6.95
	0001.dll	Get hash	malicious	Browse	• 2.18.160.23
	8IOETICF6d.dll	Get hash	malicious	Browse	• 23.211.6.95
	cob.dll	Get hash	malicious	Browse	• 23.211.6.95
	PO # RSLDH102115239.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qxioyfdvub.dll	Get hash	malicious	Browse	• 23.211.6.95
	Xnzm5rS5hN.dll	Get hash	malicious	Browse	• 23.211.6.95
	peju3.dll	Get hash	malicious	Browse	• 23.211.6.95
	sgRkrN.dll	Get hash	malicious	Browse	• 23.211.6.95
	e3w4F49JTz.dll	Get hash	malicious	Browse	• 23.211.6.95
	Ru7XGPeyjm.dll	Get hash	malicious	Browse	• 2.18.160.23
	KMgtzcYR.dll	Get hash	malicious	Browse	• 23.211.6.95
	CyLZnU.dll	Get hash	malicious	Browse	• 23.211.6.95
	16hVsNu6JV.dll	Get hash	malicious	Browse	• 23.211.6.95
	21d0000.dll	Get hash	malicious	Browse	• 23.211.6.95
	21d0000.dll	Get hash	malicious	Browse	• 23.211.6.95
	0x00020000000155fc-286.dll	Get hash	malicious	Browse	• 23.211.6.95
contextual.media.net	0001.dll	Get hash	malicious	Browse	• 23.211.6.95
	0001.dll	Get hash	malicious	Browse	• 23.211.6.95
	invoice_32.dll	Get hash	malicious	Browse	• 23.211.6.95
	Project update-xl32.dll	Get hash	malicious	Browse	• 23.211.6.95
	0001.dll	Get hash	malicious	Browse	• 2.18.160.23
	8IOETICF6d.dll	Get hash	malicious	Browse	• 23.211.6.95
	cob.dll	Get hash	malicious	Browse	• 23.211.6.95
	PO # RSLDH102115239.dll	Get hash	malicious	Browse	• 23.211.6.95
	Qxioyfdvub.dll	Get hash	malicious	Browse	• 23.211.6.95
	Xnzm5rS5hN.dll	Get hash	malicious	Browse	• 23.211.6.95
	peju3.dll	Get hash	malicious	Browse	• 23.211.6.95
	sgRkrN.dll	Get hash	malicious	Browse	• 23.211.6.95
	e3w4F49JTz.dll	Get hash	malicious	Browse	• 23.211.6.95
	Ru7XGPeyjm.dll	Get hash	malicious	Browse	• 2.18.160.23
	KMgtzcYR.dll	Get hash	malicious	Browse	• 23.211.6.95
	CyLZnU.dll	Get hash	malicious	Browse	• 23.211.6.95
	16hVsNu6JV.dll	Get hash	malicious	Browse	• 23.211.6.95
	21d0000.dll	Get hash	malicious	Browse	• 23.211.6.95
	21d0000.dll	Get hash	malicious	Browse	• 23.211.6.95
	0x00020000000155fc-286.dll	Get hash	malicious	Browse	• 23.211.6.95

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	bcsaQLr77Z.exe	Get hash	malicious	Browse	• 172.67.160.46
	6JBO8gxFVk.exe	Get hash	malicious	Browse	• 104.21.9.146
	iKTIZaTyFl.exe	Get hash	malicious	Browse	• 172.67.160.46
	SYzU0M7gx6.exe	Get hash	malicious	Browse	• 162.159.134.233
	Message.html	Get hash	malicious	Browse	• 104.16.19.94
	New Fax Message from 120283803.html	Get hash	malicious	Browse	• 104.16.19.94
	Z6hcy6XH34.exe	Get hash	malicious	Browse	• 104.21.9.146
	19292021 PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	AutoInstallYouTube.exe	Get hash	malicious	Browse	• 162.159.129.233
	vO8uY19zBO.exe	Get hash	malicious	Browse	• 104.21.9.146
	Mu9ZCqJHeC.exe	Get hash	malicious	Browse	• 104.21.9.146
	gvMlh3X76V.exe	Get hash	malicious	Browse	• 104.21.9.146
	SkB6zJ6H3N.exe	Get hash	malicious	Browse	• 162.159.133.233
	fax45367876545678.exe	Get hash	malicious	Browse	• 162.159.133.233
	TJL22phPvo.exe	Get hash	malicious	Browse	• 104.21.9.146
	Sa3qSXcAEN.exe	Get hash	malicious	Browse	• 104.21.9.146
	Md0q201V1D.exe	Get hash	malicious	Browse	• 172.67.160.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bds3fEtN0j.exe	Get hash	malicious	Browse	• 104.21.9.146
	gemfs.co.uk (1).html	Get hash	malicious	Browse	• 104.16.19.94
	QM5qEGS2aT.exe	Get hash	malicious	Browse	• 162.159.134.233
YAHOO-DEBDE	8IOETICF6d.dll	Get hash	malicious	Browse	• 87.248.118.23
	cob.dll	Get hash	malicious	Browse	• 87.248.118.23
	glovo-comida-a-domicilio-y-mucho-mas.apk	Get hash	malicious	Browse	• 87.248.118.23
	santander-empresas.apk	Get hash	malicious	Browse	• 87.248.118.22
	glovo-comida-a-domicilio-y-mucho-mas.apk	Get hash	malicious	Browse	• 87.248.118.23
	santander-empresas.apk	Get hash	malicious	Browse	• 87.248.118.22
	sgRkrN.dll	Get hash	malicious	Browse	• 87.248.118.23
	e3w4F49JTz.dll	Get hash	malicious	Browse	• 87.248.118.22
	KMgtzcYR.dll	Get hash	malicious	Browse	• 87.248.118.22
	ytr.dll	Get hash	malicious	Browse	• 87.248.118.23
	Documents.dll	Get hash	malicious	Browse	• 87.248.118.22
	zes2.dll	Get hash	malicious	Browse	• 87.248.118.23
	1510.dll	Get hash	malicious	Browse	• 87.248.118.23
	reg.dll	Get hash	malicious	Browse	• 87.248.118.23
	tvnserver.dll	Get hash	malicious	Browse	• 87.248.118.23
	artifactx64.dll	Get hash	malicious	Browse	• 87.248.118.22
	vdbb9MZTVz.dll	Get hash	malicious	Browse	• 87.248.118.22
	lpa-park.apk	Get hash	malicious	Browse	• 87.248.118.22
	New PO_NO20211010-7353 Bisco Industries.dll	Get hash	malicious	Browse	• 87.248.118.22
	aVFOmbW2t7.dll	Get hash	malicious	Browse	• 87.248.118.22

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	New Fax Message from 120283803.html	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	fax45367876545678.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	gemfs.co.uk (1).html	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	instruction.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	stash-9131480.xls	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	oCN3rc0FzJ.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	cjzu7hTifh.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	e0PXyEbkUg.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	#Ud83d#Udd0a VM 9193407174.wav.html	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PL5m30TFgh.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	stash-1675061873.xls	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	stash-1822309505.xls	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	stash-1817904387.xls	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	stash-1675061873.xls	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	Casting Invite.-06503_20211027.xlsb	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	0x000500000001abb1-152.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	KpDtm40Lne.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19
	Cardinaltek Payment copy.html	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.22 • 104.20.184.68 • 216.58.215.230 • 172.67.69.19

Dropped Files

No context

Created / dropped Files

C:\ProgramData\roundinfo.ini	
Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.32453476270788
Encrypted:	false
SSDEEP:	3:VihK0oSD4Vy:AoSD4Vy
MD5:	47C232714DB9EDEA9A53A01359816577
SHA1:	99A521E5180B88AF894672FD496F6F19A7A5F6CD
SHA-256:	69716C01458C78989C24783B67A70704759A07C85A3DF429706C71FC42AFC713

C:\ProgramData\roundinfo.ini

SHA-512:	D6D29E3CCACCC872A3FD996C7B44A50D3B6D4B626BE4EF8EF30E90751BE1D89B1255749DED36E7A3D6C66865D1F5BCF1B4CEA04AA9B232BCF6F50041F7A34 9AA
Malicious:	false
Reputation:	low
Preview:	
	[info]..time=2021-10-29..round=1..install=0..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\contextual.media[1].xml

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	
	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.msn[1].xml

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	5.196269394173945
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAeudFFDM9qSmXWLKb:JUFkduqswEkIXH40AAeudFalmpb
MD5:	0B7E6FCF20CECE3F5899DD79D4F69EFC
SHA1:	D67ACF94B60C68B33B3C290FE2CD22A9EFFB8AF0
SHA-256:	1E16603AD04CAA549B719585BB3F213A77B3E0E058771A7896D38777798A7A80
SHA-512:	85F479948F2309377E38B8469F3750F449BF09CE7A0CD0F906A77FD2A17296C4FC1E52B00B389D3DD32B5B414ECD4EF47D22960C40E2D66466DCF4D6926A6319
Malicious:	false
Reputation:	low
Preview:	
	<root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="1214814288" htime="30919972" /></root>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\52-478955-68ddb2ab[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	396910
Entropy (8bit):	5.32436826291309
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/Ms1JuKb4K7hmnidfWPqIjHSjaiCr1UgxO0DkV4FcjtIuNK:CW/ycnidfWPqIjHdT1btbcjut
MD5:	60F0A61A7D41A83C882D8013072D46CC
SHA1:	8ECE4A278B5074FE9DDDC01798740D8C9E895E83
SHA-256:	9F453B838BFF02D3B98E6F0BE4FEA285CE93D41D0829A18490A6F60974A2CAE5
SHA-512:	1FF49B6082FEF3BD54782F4F5DF6C6AB27FBCE5F5A44ACBCCF87F970BB49664F14C584B2A659E5FBBDB990D249DB7CCB459C00E5B8FD4396D138DA6FF059EA EC
Malicious:	false
Reputation:	low
Preview:	
	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMa rker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or nu ll";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAPYODK[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAPYODK[1].jpg

Category:	dropped
Size (bytes):	49213
Entropy (8bit):	7.96318952741593
Encrypted:	false
SSDEEP:	1536:IkWT3+OFEbnXAkgDrz7zaNkdlrxPWINTHHx1QqP60:EO5bX+77OaPNZHxTS0
MD5:	713ED3463C87A7CA6E3FD4511574D8F9
SHA1:	28E32E41D28360A6150BDE52863DA78F29C6ED59
SHA-256:	EE01FF6DFDFCB4C66640BA7686893BE3A1FE4366ACE67D5BBFA1AF8F794229D6B
SHA-512:	826F08EE5DB763A761587A14DFC4D45404F78B5C80CDC022CFC24505D4661ED1986D62DFFA784300DFDC0C418D4BE88C55CCFB160755DEB7E4A320F32B70A5 2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.................... ......'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}.......!1A..Qa."q.2....#B...R..$3br.......%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..3.TH...'. ...z.....O$P!7...).c.'....Bh...>...~....%vL.1.m.DN..*.5....@.%.F.I..3..3...".h$i.W.g.T..Vb..I.J.>.....+Hc..V..Q.$.*+(. .N\.h....)F.... .9].......U...y.4.PX.$.v1.....2...c...'.Rb-.....1.....p.Q@..b.$.i...S...P. .=(...Lc.T......(.(....`.h.g..J.Bp:..F\.j.qX....1\E...I..4.Q..P.z.E!...B....q....Z.%.2S.$..;.P.m.<y....>G... .C.....1E........7.J..%*.Y...hH....@.".o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1aXBV1[1].png

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...............U....pHYs..........+.....;IDATx...}..c.....j...2..Y.l....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7......0.[... ..5.)p...x...d\...g.........WmE1.sl......u....3K.[.....;.........f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1......7.@.Tn.r......C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c.::..#//...iES....E.w..op.... .9.W........).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|....e.(..."9.z\.~-.....G.h...\.'.;.... G........J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F ..*.a..lj..t\.W.....&.l|?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..|].c..\.'...I.....u8......Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f........S......S..)N..D;.....<.....7#..X2.ws.....H.vF '...,$l..R4.O/.~..j.'&..6.........!.D.m..].G........W#.Uir..sT..m...h...UN._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cEP3G[1].png

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...............U....pHYs..........+......IDATx...]..U.....d..6YwW(.UV\.v.>..>..`.K}X).i..Tj...C..RD. ..AEXP.............]).vQ../$.%.l2.....dH&.YiOr93.....~..uS...5........J. &..;.JN..z...2..;.q4..I .....c!....2;*J.........l(......?.m+......V...g3.0.............C..GB.$..M.....jl.M..~6?...........a%...;....E.by.J..1.$..".&.DX..W..jh.....=...aK...[.#....].. ....:Q....X.........uk.6 .0...e7..RZ..@@H..k.........#......[..C.-.AbC.fK.(a.<.^p.j`...._>{<...`.........%.L...q.G...).2oc{...vQ...N5..%m-ky19..F.S....&..../..F.......y.(.8.1..>?Zr......Q.`.e.|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=.......i.^...s&..Hr.z.....M....:.......EF.....0.. .N.x...........N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg.....]){.,.v.F.e.ZF.z..Ur+..^..].#.]....~..}..{.g.W0? ....&....6n....p\.=.].X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t......!..g......0t.h..8..4cB....px..............1.!...}=...Qb$W.*..."............V....!.y......<H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cG73h[1].png

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cG73h[1].png

SSDEEP:	24:IGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AAC6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG........IHDR................U....pHYs..........+......IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E.....PEJ.......B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G......7o..9....vQ.+...Q......."!#I......x\|...\...& .T6..~......Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z......^K...z........y...._..E.S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..\]t.Y.`...o....[.~~..u.sX.L..tN..m1...u ..........Ic...,7..(..&..t.Ka.].,.T.g.."...W.....q....:+t.?6....A.}...3h.BM/.....*..<.~..A.`m..:....H...7....{....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%"......[.=a......X..j.. <725.C..@.\. ..`.._....'...=....+.Sz.{......JK.A...C\|{.\|r.$.=Y.#5.K6.!........d.G....{......$.-D*.z..{...@.!d.e...&..o..$Y...v.1.....w..(U...iyWg.$...\>..\].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.......(.A&..#.jM~4.1.sH.%...h...Z2"........RP....&.3..............a..&.I...y.m...XJK..'...a.....!.d.......Tf.yLo8.+..+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1gPsLO[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.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):	18506
Entropy (8bit):	7.7264499951137156
Encrypted:	false
SSDEEP:	384:IjBDbOm9Eq8JuH53JG+rUIoMS5R2S3zx4rU5PmSIsXGPfVHpWINbSBkX:IjMCH53F5oMg3zxMU5e4GPfVH1M6X
MD5:	8125B95E3CA1DA5EB73C026BBA80FF27
SHA1:	7A866909003E41E63BE5E99D982F16F3F3EABF01
SHA-256:	A4E95EBA47223149AD3B055114DE432C9231002D766AC1AAD437B59D9CA7829A
SHA-512:	1DE8B7F85F56BA6BD2BFE9F7D4856E6F67E42773B06154DB71B1EF875DC7DFB48B9E44793ED5F327330F93E12E66D9A9B0062422CCCB6DAEE52486C2DD84031
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}.......!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.....!1..AQ.aq."2...B....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?......FI.W.. .+X...bBV%. ...P.b..1@....h&h.:.....,..w(m..a.V..:....!.Z.!..J@%...P.@.C..~...Gu.H...j.4<..."...w.c....C........D.~...] {..mth.3pM0.fc@.......94..M.&.@.(.BS.vP .@.e0...&..F.@.4b...*..E.6Ar~Z....n.....A@..c2T....>AX.T<. "t.".&.......t...........RH..-.:.52.Jl........5..^.i.Z..a..(....R...*S..H.Q`. ....(.\\... .@\..q.i......A.MD..f.b.H..C.h.(.qL....p....l... .Lc_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBih5H[1].png

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	835
Entropy (8bit):	7.675892111492914
Encrypted:	false
SSDEEP:	12:6v/7eorYebkI7N8EWhref+IdamL6pZvzKOH3X+tLNUAV6W9ONhTKnLw2x2lZgmAu:iYekvatqlKOXXS9V6W9uzRcQ9bL
MD5:	F79F56222F8B1B951A00A306C8AFA5C4
SHA1:	9FE78220A6811338E68FE7A2D65DC3B7FB5302BD
SHA-256:	2EF60D23400424838CD3B53021CFD903AA330168BDCC0A2AACFC7185832C00A9
SHA-512:	2172E9FCAB0547423F941BDB338D25528081F454857CA20A2D984C246CBF403341AC3689A748CECC1401B125E2138CFB61A9BF95F05D70329FB0BF504AFF9028
Malicious:	false
Preview:	.PNG........IHDR.............;0......pHYs..........+......IDATx..MHTQ....,...#..i...-.. J.6...iQd...p........D.6.e...>6AE.FJa.IA.b5ji..;>....|..-<.s.}......&90I6%..6.........o.-!'..!...Z<+^D...7..q:.. ....Gx..5.......&..6.{.4NBh.._Av....<..;`=<..D..5.[.g.4..Y+|.......X...M....=..4.0.4....6.......x....3......e0b....k.Fa..@-.....=...c|.8....4?../.o.g@=....ho.&...3$6.V....Ds .f.T.-...G\.7.z ....h.&..^....bE...c...].0..!.Y.i.EU9t.$L...%ra.....I.......*L.l..uUyO. .%..F..s...kmW#~-...2v.L~...N{3...i.U.......E.g}.l...b]..%g.^7r.9.t...)...N.....a.4.....^'.....-.f.A-..(LV...:} .~.O@.....g... ...|`....".#..I.......@..*.u.>.{xD|....`:.0.U...v9.u.......c2C4)..,.u.*a5....d.i.*...q....4.9.-.ip...C..:..g..h.N.B..+.U.w.......a.g...[.G.8.xZ<....:2nw:3ne.|.oa...G.J1...c.&.N.Ox..6......... ....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\a8a064[2].gif

Process:	C:\Users\user\Desktop\SEMqjw.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:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\a8a064[2].gif

Malicious:	false
Preview:	GIF89a.......dbd...........lnl.........trt..................!..NETSCAPE2.0.....!......,.........+..I..8...`(.di.h..l.p,..(.........5H.....!......,.........dbd...........lnl.......dfd...................../..I..8...`(.di.h..l..e....Q.. ..-.3...r...!.....,.........dbd.............tvt..........................*P.I..8...`(.di.h.v....A<.. ......pH,.A..!.....,.........dbd........|~|.....trt...ljl........dfd.............................................B`%.di.h..l.p,.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\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\background_gradient[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.......P......Adobe.d... ....W...Qa................................?......%.....x.....s...Z.......j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.........p.....A.........BP..qD.(.........ntH.@......h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[1].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305279142191786
Encrypted:	false
SSDEEP:	384:veAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOVQWwY4RXrqt:Q86qhbS2RpF3OsVQWwY4RXrqt
MD5:	5015CB2F36436FBD31DA601C411B75A3
SHA1:	556D4BFEA0AFDE9123575B8BF41BB9A96FFFB549
SHA-256:	C2561AD28587CE88C5A351E2BEFF8811052FC38F05512D580DFA71BBE430B2B1
SHA-512:	695CC9D1A93DBBDB2A28AAB813AAF99DCB52667D9EBF21CEA60A8750740B672213BC2CA6903C5EF828D462559CC0DD2F401C3307B3AD5291F3ACC3C89EDB8B0
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"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\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[2].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305279142191786
Encrypted:	false
SSDEEP:	384:veAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOVQWwY4RXrqt:Q86qhbS2RpF3OsVQWwY4RXrqt
MD5:	5015CB2F36436FBD31DA601C411B75A3
SHA1:	556D4BFEA0AFDE9123575B8BF41BB9A96FFFB549
SHA-256:	C2561AD28587CE88C5A351E2BEFF8811052FC38F05512D580DFA71BBE430B2B1
SHA-512:	695CC9D1A93DBBDB2A28AAB813AAF99DCB52667D9EBF21CEA60A8750740B672213BC2CA6903C5EF828D462559CC0DD2F401C3307B3AD5291F3ACC3C89EDB8B0
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"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\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\e151e5[1].gif

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7IU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Preview:	GIF89a.............!......,...........D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\errorPageStrings[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fcmain[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	39357
Entropy (8bit):	5.054829698830934
Encrypted:	false
SSDEEP:	768:l1avJ4u3uPPbW944hl4wi0d4rrUk5WYXf9wOBEZn3SQN3GFl295odVl41sVv:PQJ4ueLWm+iwBd4roqWYXf9wOBEZn3SH
MD5:	394BE310FB9F5C45D10C1A4960C4B388
SHA1:	A0A159DEFE0FEB6AD8DEC3DD347BDA19946E4B1B
SHA-256:	FD35DC37ED407C513C6D6EB4C6985CB8C3B577D2589A744A5DCCA878DC26F009
SHA-512:	9E0A6EAD684A9A8287300F9F15031068A3E0F75E4F91A25F68E186D8D7B0D14E329920B8C25F37F89C5B253CA3A0B80BE06F433806F26EEA058FD9A8B71FE9B9
Malicious:	false
Preview:	;window._mNDetails.initAd({"vi":"1635520908789364092","s":{"_mNL2":{"size":"306x271","viComp":"1635520019288543597","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"170721335","l2ac":"","sethcsd":"set!N9|7094"},"_mNe":{"pid":"8PO8WH2OT","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=858412214#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html 4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><link rel=\"dns-prefetch\" href=\"https:\/\/contextualtag.media.net\"><style type=\"text\/css\">body{background-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{window.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"858412214\"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\nrrV8478[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	91171
Entropy (8bit):	5.423314806997941
Encrypted:	false
SSDEEP:	1536:uEuukXGs7ui/gn7qeOdill5x5Q3YzuZp9oNuvby3TdXPH6viqQDnjs2i:aKio0di3m8ufMfHgjV
MD5:	AFB146A2E4995375C3D1DC735A2209E6
SHA1:	BF75C7724ADB65ADA84E9E8D0CF6B71F92E67EB1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\nrrV8478[1].js

SHA-256:	599B44D7016054B6EEC525539E2C20E18B14824CDD5A01970A99A375C123AAAF
SHA-512:	2C32092D5F865185EF742B2C0824B61A6103F7C0A1EE66DD8725351807807161EED84D2D2572EE88F8698ABA20A251ACC270DA2DD0E278370AFAC8530017183D
Malicious:	false
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\tag[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10157
Entropy (8bit):	5.433955043303664
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqH3wgiKGWdrBpOIztlomlRokr:4EamR7OrxYSLQdiMoH3wgxGWdrz4+
MD5:	DDFF3756F9EFD3A46CF3325875D813A1
SHA1:	05D238659959B28B786CCE43E9E55A728E69428E
SHA-256:	E80C669818773959643790269ED9448F71BD45D27D61FAFD73BC44C0F40BAACD
SHA-512:	7E6D325A705718D0B4060BB4A2FACC538B3812B5767CBEF9F15F787C20EFB492F9E72F8F4B215A3C4D4F684236F49D80C37597E2C13F9B482C3CB441B6CA574I
Malicious:	false
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1634277746662-1414[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 150x150, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	217987
Entropy (8bit):	7.970658247536232
Encrypted:	false
SSDEEP:	6144:uIwZnQ8iCq3Lje2m7H/KVMgfkP9nZzGg0ZRBCR:4ZQfTn87H/oMgcPxZzGgoRA
MD5:	019C4E8E1E43845ADF8A3E821C73B996
SHA1:	B8F78A37EBA1B8C1F95691FBFCDAB19AA6FB65A4
SHA-256:	AA980948110DC4A94945FA33A6D17BBD932FBBD225693E8FB3D1A93E355C2472
SHA-512:	F46E6BEE310BA72403B2968EA697EA0BD3BABE58B03854897C51DB54082066404854F57C82682DF5D313B3A37332E9A0076683A56246788D43FAA325425EF4FB
Malicious:	false
Preview:	......JFIF.............(ICC_PROFILE..............mntrRGB XYZ ....acsp...................................-..desc.......trXYZ...d...gXYZ...x....bXYZ........rTRC......(gTRC......(bTRC......(wtpt........cprt......<mluc............enUS...X.....s.R.G.B...XYZ ......o...8.....XYZ ......b.........XYZ ......$.........para..........ff......Y.......[.......XYZ ....-mluc...........enUS... .....G.o.o.g.l.e. .I.n.c.. .2.0.1.6...C...C..p.n.....................W.........................!.1.."A.Qa..2q..#B......$3R...%b.&4C'5Dr...6STUe.7FVWstv...............................U....................!.1A.Qaq.."....2....#B.R..3br.$4C...Scs...%Dd.5T......U...............?...d...<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2d-0e97d4-185735b[1].css

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	240569
Entropy (8bit):	5.307603888190693
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvzZkrqq7pjD4tQH:Fa0ULTAHLOUdvoZkrqq7pjD4tQH
MD5:	761B3F378259A12BDCDB434564758254
SHA1:	E44E177CE1D4B1514A124200C8589129B215CF5D
SHA-256:	71B92CE435FCA0EE9A4E5EA18E1EDFDFC2F819DF37FB592D70D7B6EC32D6BF09
SHA-512:	56F00EC561D4A3F5AAB4EB6A581635DE4A4DD44327A623FB67526C2BF818D86F565B338DDDAE8FC3A32135CD70617A4CF7CCE5EF74F642D81F463628F99E60I2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\2d-0e97d4-185735b[1].css

Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\627[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1200x627, frames 3
Category:	dropped
Size (bytes):	58094
Entropy (8bit):	7.870519899753681
Encrypted:	false
SSDEEP:	1536:XczUTkYefrO+W5CYYuBwmfw/YV+v36vdA5:sori47xBwmfw/YV+v3udA5
MD5:	9057ED4B0D8BC1E3D6FD6DCB5CCB5D39
SHA1:	F43425475E4658E57AAB857BFCC1C1FC79F83B01
SHA-256:	9CCCB6B7BD77517EB84D765E237DA38800E702C39EE54E547D42510718A4B53E
SHA-512:	961D8AE3D3B37CD439661A2A072D226B3ABF8DE651773E94059FFF9C7EE6879CF115882AE6C25B07E9850879DF48D12DBDE5DB999ECFD1802B34235AE48AE008
Malicious:	false
Preview:	......JFIF............C.................................... $.' ",#..(7),01444.'9=82<.342...C..........2!.!222222222222222222222222222222222222222222222222222......s...."..}.....!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br....$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(........[.?.._...gk...j.../..h@x.H..K..i1J:.V.a...^}M.}.-..9..i...u..d...H9...$ph..4.E...$r..Z\._...L..}iA>...7.....;'#4d..{.Q.&.....}......vx.h.ZOsJ=E..N:..F3G..@...4w...8...j.2s.\.S.:.......H8..t.d.&....R..........t......}M.I...s@........9.dw..`/=..4.({.R.}i)G..r:.K..%(.@.>.d.Oj(....'....s.h.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBPfCZL[2].png

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBX2afX[1].png

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[3].htm	
Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305279142191786
Encrypted:	false
SSDEEP:	384:veAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOVQWwY4RXrqt:Q86qhbS2RpF3OsVQWwY4RXrqt
MD5:	5015CB2F36436FBD31DA601C411B75A3
SHA1:	556D4BFEA0AFDE9123575B8BF41BB9A96FFFB549
SHA-256:	C2561AD28587CE88C5A351E2BEFF8811052FC38F05512D580DFA71BBE430B2B1
SHA-512:	695CC9D1A93DBBDB2A28AAB813AAF99DCB52667D9EBF21CEA60A8750740B672213BC2CA6903C5EF828D462559CC0DD2F401C3307B3AD5291F3ACC3C89EDB8B0
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"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\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9Xsiltnuy5zlux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\fcmain[1].js	
Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	39494
Entropy (8bit):	5.051273180999047
Encrypted:	false
SSDEEP:	768:U1avU4u3uPPgW94ECpl6NsaRcg6S0ouo8eMcYXf9wOBEZn3SQN3GFl295oErCplq:kQU4ueQWmECpIyAcg68RzYXf9wOBEZnl
MD5:	488F43CB1509765E23D515358D471211
SHA1:	FACB27280FB3DB8EF3F4EE6D377FBE3B76D65C27
SHA-256:	1B8D58BDD404D2D07B0FF809EBFA41B7579DFFDE98EBD9F6F3971C6413CD333E
SHA-512:	31DC3C30A2CEF3296560357DF4F68350F6F04C3D5883F4FFEDD87749ADD9A5035729D1ABBDF96637AD5461ADC308E837885898C359E8E7B9CA4FE0953DC44BA
Malicious:	false
Preview:	;window._mNDetails.initAd({"vi":"1635520908501934183","s":{"_mNL2":{"size":"306x271","viComp":"1635520119872563448","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"170721342","l2ac":"","sethcsd":"set!N9|7094"},"_mNe":{"pid":"8PO641UYD","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=722878611#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><link rel=\"dns-prefetch\" href=\"https:\/\/contextualtag.media.net\"><style type=\"text\/css\">body{background-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type\" \/><script type=\"text\/javascript\">try{window.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"722878611\"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\iab2Data[2].json	
Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\iab2Data[2].json

Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with y our online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices ","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\info_48[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC13 4
Malicious:	false
Preview:	.PNG........IHDR.../...0.......#.....IDATx^...pUU..{....KB........!....F......jp.Q.......Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{...........[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po......... .....X..;.=.P......./...+...9./..s.....9..|.......*.7v.`..V.....-^.$S[[[......K..z......3..3.....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t......N}..%.v..:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".. ....}I$....^.re..'^X..*}.?.^U.G..... .30...X......f[.I0.P`..KC...[..[..6....~..i..Q.|;x..T ....s5...n+.0.;...H#.2..#.M..m["3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..I[..a.. .N,,.h......5...f*.y...}...BX{.G^...?.c......s^..P.(..G...t.0.:.X.DCs.....]vf...py).........x..>-..Be.a...G...Y!...z...g.{...d.s.o.....%.x......R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a).t..e.j.W........C<.1.....c..I1w....]3%....tR;.,..3..-.NW.5...t.H..h..D..b......M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery-2.1.1.min[2].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B 50
Malicious:	false
Preview:	/*! jQuery v2.1.1	(c) 2005, 2014 jQuery Foundation, Inc.	jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports =a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window: this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.ini t(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",len gth:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a) ;return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\navcancl[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2713
Entropy (8bit):	4.1712007174415895
Encrypted:	false
SSDEEP:	24:r3avxU5hzsIVmVMeLmVMyHf63lboxMCLxvriN6LOAPAnQay78eLx5Tb87nVkEhML:upU0GVeLVGBXvrp4n/1a5TI7Ve/G79KX
MD5:	4BCFE9F8DB04948CDDB5E31FE6A7F984
SHA1:	42464C70FC16F3F361C2419751ACD57D51613CDF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\navcancl[1]

SHA-256:	BEE0439FCF31DE76D6E2D7FD377A24A34AC8763D5BF4114DA5E1663009E24228
SHA-512:	BB0EF3D32310644285F4062AD5F27F30649C04C5A442361A5DBE3672BD8CB585160187070872A31D9F30B70397D81449623510365A371E73BDA580E00EEF0E4E
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-/W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="res://ieframe.dll/ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.... <title>Navigation Canceled</title>.... <script src="res://ieframe.dll/errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="res://ieframe.dll/httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:navCancelInit(); ">.... <table width ="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rows pan="2">.. <img src="res://ieframe.dll/info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\rtbsmpubs[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4104
Entropy (8bit):	5.548700500840635
Encrypted:	false
SSDEEP:	96:xB6IHrSx23smsxXRwoTT4WNbhbv7pxuaxG+TbOYdE1:xB6ILGxm4W7W7bv7psa1ndE1
MD5:	12F612D2D2C99035322A15FA5A29D2BD
SHA1:	D018A4D54E5579EAA4429C95C673CF2524830B53
SHA-256:	50886E6E456C6FF90ACBA7DB6A32DCC5F1E2AB0B3B15D1D87F4D63B58BBF2D58
SHA-512:	33D641E4AEBA741AC2B2E2E5E9537996C2029FB3FB7A48A34DDC567375BE64743220E9C4654B52D9D4BBAEA5C2E55B6BEC09249091DCABEE8996A154E3D13C BC
Malicious:	false
Preview:	window.hbCMBidxc.rtbsheaderBid3S0({"pinfo":{"4":{"adCodeType":"BANNER","adFormat":"html","ae":false}},"meta":{"auction_id":"111476758995940606_245760 539","region":"nydc","vcfl":false,"serverId":"c10-mowx-web-6","apid":1,"prvReqId":"60619533009195612163553367009","mowxLogs":{"SD":null,"PC":1,"SPRIG":1,"UCC": 2,"lr_seg_cnt":0,"GCID":0,"IAB2":1,"ip_exp_verd":null,"vsGap":null},"sp":{"ivt":3,"source":0,"to":3,"fst":0,"cst":0,"isReq":3},"int_id":"HM","pageCat":{"iab2":"379","goog le":"16","iab":"IAB12"},"vls":0,"mp_seg":[44412,15390,15718,17218,28447,33721,54934,53492,60148]},"tl":{"670468743":{"bl":{"4":{"metainfo":{"responseTime":31,"e xperiment":{"sfl":false,"ssBucket":0,"bfl":-100,"clt":0,"fl_rl":1,"ssProfile":0},"rstb":true,"ab":"0","crid":"670468743","mowxLogs":{"g_uid_sent":[],"BCN_BF":null,"epbc": "8CU157172","bsBucket":0,"ssProfile":0,"BCE":null,"lr":0,"BCI":null,"g_one_uid_sent":"None","uid_sent":0,"yhs_enabled":null,"SC":0,"lr_seg_deal":0,"BCT":null,"y hs_target_bidders":null,"BCN_Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\17-361657-68ddb2ab[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
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.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><Vp>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\2d-0e97d4-185735b[1].css

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	240569
Entropy (8bit):	5.307603888190693
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvzZkrqq7pjD4tQH:Fa0ULTAHLOUdvoZkrqq7pjD4tQH
MD5:	761B3F378259A12BDCDB434564758254
SHA1:	E44E177CE1D4B1514A124200C8589129B215CF5D
SHA-256:	71B92CE435FCA0EE9A4E5EA18E1EDFDFC2F819DF37FB592D70D7B6EC32D6BF09
SHA-512:	56F00EC561D4A3F5AAB4EB6A581635DE4A4DD44327A623FB67526C2BF818D86F565B338DDDAE8FC3A32135CD70617A4CF7CCE5EF74F642D81F463628F99E60E 2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\2d-0e97d4-185735b[1].css

Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption, .todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead {bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\438b6cb0-a592-4ebb-a44e-fa3f43b1be41[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.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):	57101
Entropy (8bit):	7.969493344434981
Encrypted:	false
SSDEEP:	1536:ivBvsAh74/SknU0dWyHjfwzTxIy4WrCUCXa3o6W:ipvsGeSkU08+czOy42CUCKY6W
MD5:	AE0540B7D08516A487C533F3EA298DD9
SHA1:	0374FCD7712DBD530AA6314C2E6EF6E52027EC20
SHA-256:	11FAD098D49B6D6863FF3A49C2C94A7149B04D9224E6329C13E3346280C22709
SHA-512:	C403E1C1444A6B56F1FC319B724F46FEE5455D63BBE54FBD45667AE72B72018193FAE4B50605FC24CB7F4BE81151A75E75355BCD205E088747C6BFD761CAC33
Malicious:	false
Preview:	......JFIF............C...C..,,.".................................K........................!..1A."Qa.q .#2.....B...$R...3b%4.Cr..&5S.Dc.................................F........................!.1A."Qa..2q....B....#.$3Rbr..4CS..%..&s.............?...U..!...W.\..z..C..s..R..t.BBRv...{.{.,HjP.!.. P76...?......4.I.......=.MJ.n.......=.n/n._V....n<.gQW..v.....\X.m7.I.z..oA..}...W6..v......e;6..d.`=...._........nm.&...w.{.s`H....8C.*.P!6......O.....iP ...or;.....P.Z.....?t.b...'.#..P....XX. .o.=.q.#..u.../..c..9.......|\i.V....I...5....k..J.......p/.o..=.w..2.V.!N.)...~.6=A..c.|..-G{t.@.F...o.K..Pp.A.b.....~...z..k..m..\=.iK..,.`@......#.&.)d'...q....F......:...y......m..-n.].....~.......m.c..{ .GV...~.........}q.q....b.A.s..}.<)...r>...c._...4.V..jQ..N..m........).@..t..7...q.r.....E....|<..#....$..l....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\55a804ab-e5c6-4b97-9319-86263d365d28[2].json

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\82a15848-8a9a-450a-b8af-e7cab8fe8d26[1].jpg

Process:	C:\Users\user\Desktop\SEMqjw.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):	73552
Entropy (8bit):	7.95813226199884
Encrypted:	false
SSDEEP:	1536:GbG7HOMf1zJgeOof0ZYx2A67ZR6ti244AoMPehW+xY1/uBi6XhcSBt/R:GCH59zSvYxeotiz4xHwCYiiSBP
MD5:	2786EE3207DF42D9EA8B4F8C1C791CED
SHA1:	97C9DEE9F16C1CA6E624EF1E6B225019E8F46BA8
SHA-256:	04DACDE5508118F5BE89889105055C676378299861EBB32D38D3E184579BF879
SHA-512:	1375255A583558B8623E7DFF04173A0AB3AA788EEDE2FAD798CDADEF343190EF21BA8CBC5261711F95082822B0249093940F43E4A53F734A686FC12B83750ED2
Malicious:	false
Preview:	......JFIF............C...C..,,."..M........................!..1.A."Q. .#2aqB...3..$Rb...4...%&CDSr...U.cs.......................................?......................!.1.."AQ.a#2q......BR...3..$%Cb..Sr...........?..9r.. .3.O8..?..=y.s..JP=.....K.....w.S.`..(.....|.? p:...O..f|n.`.SrP.@'..I?...P./.....~.=..^<.q...s......{N.~.).c,#.......$to..@.<}..............U.SJ...v.S...)>s...o..r../!%3.(m...9.../....Ui....D...T0...rp......f........$..w1..9..~...R[%N....F8... ?....7N|..x.`.q..x.x.......!.m.............CW.&....1.T.|..d+...u..%.5..z.\...@.o~G.3....Yn......'.....[(............x.u.-....I..G.{y#....Qu..F....*CI. q...?....;Z...+r....H*..6..+.....=C..?7....2X TG...Ko....|,w.......`. ..<p8..{..{u:v.i$....#.d.ps..]b.`I().'8........T..T.`.....T..LB.N..H>..z...k....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bullet[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	
	.PNG........IHDR...............ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;I.Zj.\l.5o.7q.<..aw.<..dz.E...........1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.........z`....#tRNS................................./,....mIDATx^..C..`.......S....y'...05...|..k.X......*`.F.K....JQ..u.<.}.. ..[U..m....'r%.......yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\cfdbd9[1].png

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
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...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s....c..............2]E0....M...^i...[..]5.&...g.z5]H....gf....I... .u....:uy.8"....5...0.....z.............o.t...G.."....3.H....Y....3..G....v..T....a.&K......,T.\.[..E......?........D........M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P...........9.....yI.<...9... ..R.e.!`..-@........+.a..*x..0......Y.m.1..N.I...V.'..;.V..a.3.U....,1c-..J<..q.m-1...d.A..d.`.4.k..i.......SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\de-ch[1].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	420837
Entropy (8bit):	5.441332263903117
Encrypted:	false
SSDEEP:	3072:GfyJUixx+TTkJ88iFrFr7wBlNHH35YJErBhtSG+JJcwifPxLa:GfyPOTL4Bft/+gTfPs
MD5:	857E753B9FAE83CA611E1E9D6C5C7ECA
SHA1:	CC4F21E1907E8DE41BB4AFC16786AC6C607CD3FE
SHA-256:	F5EC427AA62CC4EDB1CB40828C36FE05DC127A9B319A58CEC0E0692499EC3341
SHA-512:	8191877EBFBEDE3BF4A63A19AFFF505A5270AC604EE4ED4F28DD29669136FB9FEC69C9559188AC7EDD1DEA4F26821BE0E814F3DEF1E6F2ACA491A647145D3E B9
Malicious:	false
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:20211023_253454 34;a:232ac1ee-2e70-4147-82e3-eda3293b4dbc;cn:7;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 7, sn: neurope-prod-hp, dt: 2021-10-26T21:10:41.6410920Z, bt: 2021-10-23T00:12:11.4726061Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck:} ;xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-10-29 15:22:37Z;axd:,f:msnallexpusers,muidflt21cf,muidflt28cf,muidflt298cf,muidflt312cf,moneyh p3cf,bingcollabhp1cf,platagyhz1cf,modsplitabu,artgly3cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh20200521msncf,msnsports2cf,csmoney6cf,1s-br30 min,btrecrow1,1s-winauthservice,1s-winsegservice,prong2c,1s-pagesegservice;userOptOut:false;userOptOutOptions:" data-js="{"dpi":1.0,"ddpi": 1.0,"dpio":null,"forcedpi":nul

---

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\favicon[1].ico

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXll1pe/WNN00000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\favicon[1].ico

SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286‹A9
Malicious:	false
Preview:	...............(...&... ....N...(....... ....(... ...@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\medianet[1].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	411816
Entropy (8bit):	5.4875459526335195
Encrypted:	false
SSDEEP:	6144:zHmkYqP1vG2jnmuynGJ8nKM03VCuPbTXEoJuzYmK:z1vFjKnGJ8KMGxTCYmK
MD5:	DC6F86793187337E72A1A5A95A3C745C
SHA1:	FF62F04182811B244997EDDBDA428E70A54EFE8A
SHA-256:	CFAC2D1EE8286D37ED2E2D90C6047F72E79AFCDC532DFF53257653287DF3B1E0
SHA-512:	D74C5FB517B5838D2F594E80FD23B6CAD90F510736C4435DAFCCA96DD46760F54CA474E5E99CB94C57758C1B1B02AF58E9BC797EE7372DFC0149E163598D21‹D
Malicious:	false
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\medianet[2].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	411816
Entropy (8bit):	5.487502274339047
Encrypted:	false
SSDEEP:	6144:zHmkYqP1vG2jnmuynGJ8nKM03VCuPb/XEoJuzYmK:z1vFjKnGJ8KMGxTeYmK
MD5:	69BBD52FDE752171804301F8333BB623
SHA1:	9758E19959F404E55FBA5FBA3608D3BCF5636913
SHA-256:	249EAB5B00BD0179793BAE09B67A45600655F12482595285C04F18B79A1050B0
SHA-512:	D94B80C43E78C43C65F57748820C243AA62C7437A07190183C783010D0F8BE892FA838CE997B395CAD8FB156E80227BC4E460F3A92290B641BB13B51F3C80D2D‹
Malicious:	false
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\otTCF-ie[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168‹BA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\otTCF-ie[1].js

Preview:	
	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\px[1].gif

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A(910
Malicious:	false
Preview:	
	GIF89a.............!......,...........L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\17-361657-68ddb2ab[1].js

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\4996b9[1].woff

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\52-478955-68ddb2ab[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\52-478955-68ddb2ab[1].js

Category:	dropped
Size (bytes):	396910
Entropy (8bit):	5.32436826291309
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/Ms1JuKb4K7hmnidfWPqIjHSjaiCr1UgxO0DkV4FcjtIuNK:CW/ycnidfWPqIjHdT1btbcjut
MD5:	60F0A61A7D41A83C882D8013072D46CC
SHA1:	8ECE4A278B5074FE9DDDC01798740D8C9E895E83
SHA-256:	9F453B838BFF02D3B98E6F0BE4FEA285CE93D41D0829A18490A6F60974A2CAE5
SHA-512:	1FF49B6082FEF3BD54782F4F5DF6C6AB27FBCE5F5A44ACBCCF87F970BB49664F14C584B2A659E5FBBDB990D249DB7CCB459C00E5B8FD4396D138DA6FF059EA EC
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMa rker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or nu ll";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ErrorPageTemplate[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...ma rgin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_grad ient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...back ground-color: #F4F4F4;..}.. .a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\auction[1].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6983
Entropy (8bit):	5.918186297767972
Encrypted:	false
SSDEEP:	96:8zTVgT1Tomz60kYJS40NyZwaNQ1jeHpQ9eKD6pT6ezk2A3FGalxYJD9M1qYUauC:/l60k00c6FgkZ3calMD9MWaR
MD5:	5907834310A3FC2E84473AED9591DA54
SHA1:	B4283C9EC31B3538E91D8B822ABEC54EEED5D885
SHA-256:	A70BD90DF6C3CCE9A7DC49532AFD28474A070345E5CA8CC83FD1CD33C1742B84
SHA-512:	D30A1EC455358D3A550A57717F666FA07F97AA262C5F65E19DE6BBCFDA57EE045615FAD36F2D7A396B067D56413649D67A086C93314E0FD9734BD9DC96D4142
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_86b122c311d4bb82d3334d47c8bf4e85_8568df6d-0482-4a85-a7ea-67ae46966bc3-tuct8759752_1635520978_1635520978_Cli3jg YQr4c_GInInM2VzaGe5AEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaIiuzvz94c6FCXAA"},"tbsessionid":"v2_86b122c 311d4bb82d3334d47c8bf4e85_8568df6d-0482-4a85-a7ea-67ae46966bc3-tuct8759752_1635520978_1635520978_Cli3jgYQr4c_GInInM2VzaGe5AEgASgBM Cs4stANQNCIEEje2NkDUP_____wFYAGAAaIiuzvz94c6FCXAA","pageViewId":"d9125748a25347aeaba6c1d7a3e5ee7a","Requ estLevelBeaconUrls":[]}">..</script>....<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"appnexus","e":true}" data-provider="appnexus" data-ad-region="infopane" data-ad-index="2" data-viewabil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\checksync[2].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305320756363584
Encrypted:	false
SSDEEP:	384:veAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOaQWwY4RXrqt:Q86qhbS2RpF3OsaQWwY4RXrqt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\checksync[2].htm

MD5:	628E31DADB7B4D48F4D4F66B8215312F
SHA1:	E9524559546544083EB850C66DC2617D3925B556
SHA-256:	45BE9BF6468D90F25610BA835FE47DA70AEB31C6044023C69A7CED5924AB8F83
SHA-512:	049A7F09B8E37526681DCB31FD4ABA57A6DEAE9A2CD1D1DB9099610B589C952C2679D8579D8C3A91D33BDDBD1699BD7DCC97CC57215E8B2F784A5073B7A52 4E
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"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","cook ie":"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\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\de-ch[1].htm

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	421200
Entropy (8bit):	5.4404219326081495
Encrypted:	false
SSDEEP:	3072:bfTJUSxx+wTkJ8liFrFr7wBlNHH35YJErBhtGG+JJcwif1xLa:bfTzOw24Bftb+gTf1s
MD5:	6C8153A3E5AF2D7B87F81A54A9136529
SHA1:	4E2A8DBC0DD04B5E835E60A72F963D1E5549B033
SHA-256:	FF70D431905FD2AC22DCA450B1BA0120E13648EB122F7BECD14C96B36CE514D2
SHA-512:	2ECACE208ECADCEBE529E9E0F70DE49640EE7B95546845A2937F692CF776CC02D410702A76B67840EB3A08D059D8E0A20AFAB416E394E0A811BCAFA9C39BC5 BB
Malicious:	false
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:20211023_253454 34;a:d9125748-a253-47ae-aba6-c1d7a3e5ee7a;cn:12;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 12, sn: neurope-prod-hp, dt: 2021-10-26T21:47:51.6057616Z, bt: 2021-10-23T00:12:11.4726061Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck:};xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-10-29 15:21:24Z;axd:;f:msnallexpusers,muidflt12cf,muidflt15cf,muidflt18cf,muidflt55cf,muidfl t261cf,pneedge2cf,pneedge3cf,startedge1cf,moneyedge1cf,starthp2cf,audexhp1cf,audexhp2cf,modsplitabu,gallery3cf,onetrustpoplive,1s-bing-news,vebudumu04 302020,bbh20200521msncf,msnsports2cf,msnsports5cf,1s-br30min,btrecrow1,1s-winauthservice,1s-winsegservice,prong2c,1s-pagesegservice,netcoreaa1cf;userO ptOut:false;userOptOutOptions:" data-js="{"dpi":1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\httpErrorPagesScripts[1]

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\location[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2 481

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\location[1].js

Malicious:	false
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otBannerSdk[1].js

Process:	C:\Users\user\Desktop\SEMqjw.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
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf|{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[])).next())})}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otFlat[1].json

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12282
Entropy (8bit):	5.246783630735545
Encrypted:	false
SSDEEP:	192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYLp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAk
MD5:	A7049025D23AEC458F406F190D31D68C
SHA1:	450BC57E9C44FB45AD7DC826EB523E85B9E05944
SHA-256:	101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5
SHA-512:	EFBEFAF0D02828F7DBD070317BFDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A906
Malicious:	false
Preview:	.. {.. "name": "otFlat",... "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCIgcm9sZT0iZGlhbG9nIg5nIiBhcmlhLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpdiBjbGFzcz0ib3Qtc2RrLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWNvbHVtbiI+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5IiBjbGFzcz0ib3Qtc2RrLWNvbHVtbiI+PGgzIGNsYXNzPSJvdC1jb25zdGdl0YSBwbbBvcmlciB0byByWwm92aWRlIOjwvaDM+PGRpdiBjbGFzcz0iQtZHBkLWNvbnRlbnRibiQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90RmxhdCI0aHJlZiBvdC1zZGstY29sdW1uIj48ZGl2IGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI48ZGl2IGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCIgY2xhc3M9InY2h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otPcCenter[1].json

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	47714
Entropy (8bit):	5.565687858735718
Encrypted:	false
SSDEEP:	768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI
MD5:	8EC5B25A65A667DB4AC3872793B7ACD2
SHA1:	6B67117F21B0EF4B08FE81EF482B888396BBB805
SHA-256:	F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988
SHA-512:	1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F2068
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otPcCenter[1].json

Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIlJlIG90WZHZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZylgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyljj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBLWxvZ28iIHJvbGU9ImltZylgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkIlPSJjbG9zZS1wYy1idC4taGVhZGVyIiBjbGFzcz0ib3QtY2xvc2UtaWNvbiIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkIPSJjbG9zZS1wYy1idC4taGVhZGVyIiBjbGFzcz0ib3QtY2xvc2UtaWNvbiIgYXJpYS1sYWJlbD0iQ2xvc2UiPjwvYnV0dG9uPjwvZGl2Pg0KPGRpdiBjbGFzcz0ib3QtcGMtc2Nyb2xsYmFyIj48aDMgaWQ9Im90LXBLXJpdGxlIj48Zb3VyIFByaXZhY3k8k2 gzPjxkaXYgaWQ9Im90LXBLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGVhZGVyIiBjbGFzcz0ib3Qtc2RrLXJvdyBhXZHY3k8L 2gzPjxkaXYgaWQ9Im90LXBLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGVhZGVyIiBjbGFzcz0ib3Qtc2RrLXJvdyBhXZHY3k8L ib24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWl0ZW0iIGRhdGEtb3B0Z3JvdXAiilc2lyL2l5YXRIZnZlc2Vlm5lcIsIdIXJhhc2VIIENvb2tpZXMiIGNlczwvaDM+PGRpdiBjbGFzcz0ib3QtZGVzcklvbiI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Zb25ZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otSDKStub[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16853
Entropy (8bit):	5.393243893610489
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF8 22
Malicious:	false
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieNam e="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupu bconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE ","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.st ubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=! 1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t||{})[o.Unknown=0]="Unknown",o[o.Bann erCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtbsmpubs[1].js

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4107
Entropy (8bit):	5.542912492804555
Encrypted:	false
SSDEEP:	96:qqB6+UrSx23h9mswMq5kTWcWfbhbXQaaxGQcNQtYdE1:fB6+cGG9mAqkWNbXQaa23dE1
MD5:	EB8599508A5B05AD8D8E0CCE567F9B0D
SHA1:	BB3FC5F083F79D24E7B625D6B8A603BACAF06548
SHA-256:	A09F0BCED145F86B484A5FDB7F95DA79C3AEE89D3F67EF7553BA544F78CED08C
SHA-512:	728573321888C0415ECA47764CE59EB162B975AC3683FCBFAA603A599BC1268336C28B06F0367B62EA26A88C65271D09B9112CD113DEC91EFCE0B3BC30A297E
Malicious:	false
Preview:	window.hbCMBidxc.rtbsheaderBid3S0({"pinfo":{"4":{"adCodeType":"BANNER","adFormat":"html","ae":false}},"meta":{"auction_id":"73150185802781682_3066967 66","region":"nydc","vcfl":false,"serverId":"c10-mowx-prod-1","apid":1,"prvReqId":"23721107665880866616355553328200","mowxLogs":{"SD":null,"PC":1,"SPRIG":1,"UCC": 2,"lr_seg_cnt":0,"GCID":0,"IAB2":1,"ip_exp_verd":null,"vsGap":null},"sp":{"ivt":3,"source":0,"to":3,"fst":0,"cst":0,"isReq":3},"int_id":"HM","pageCat":{"iab2":"379","goog le":"16","iab":"IAB12"},"vls":0,"mp_seg":[44412,15390,15718,17218,28447,33721,54934,53492,60148]},"tl":{"976531914":{"bl":{"4":{"metainfo":{"responseTime":27,"e xperiment":{"sfl":false,"ssBucket":0,"bfl":-100,"clt":0,"fl_rl":1,"ssProfile":0},"rstb":true,"ab":"0","crid":"976531914","mowxLogs":{"g_uid_sent":[],"BCN_BF":null,"epbc": "8CU157172","bsBucket":0,"ssProfile":0,"BCE":null,"lr":0,"BCI":null,"g_one_uid_sent":"None","uid_sent":0,"yhs_enabled":null,"SC":0,"lr_seg_deal":0,"BCT":null,"y hs_target_bidders":null,"BCN_Y

C:\Users\user\AppData\Local\Temp\~DF15D6617A413C302B.TMP

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.3613836054883338
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	679672A5004E0AF50529F33DB5469699
SHA1:	427A4EC3281C9C4FAEB47A22FFBE7CA3E928AFB0
SHA-256:	205D000AA762F3A96AC3AD4B25D791B5F7FC8EFB9056B78F299F671A02B9FD21
SHA-512:	F8615C5E5CF768A94E06961C7C8BEF99BEB43E004A882A4E384F5DD56E047CA59B963A59971F78DCF4C35D1BB92D3A9BC7055BFA3A0D597635DE1A9CE06A34 6
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF15D6617A413C302B.TMP

Preview:	.....................>.. ....

C:\Users\user\AppData\Local\Temp\~DFCE2978FA1CCF84BD.TMP

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.3613836054883338
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	679672A5004E0AF50529F33DB5469699
SHA1:	427A4EC3281C9C4FAEB47A22FFBE7CA3E928AFB0
SHA-256:	205D000AA762F3A96AC3AD4B25D791B5F7FC8EFB9056B78F299F671A02B9FD21
SHA-512:	F8615C5E5CF768A94E06961C7C8BEF99BEB43E004A882A4E384F5DD56E047CA59B963A59971F78DCF4C35D1BB92D3A9BC7055BFA3A0D597635DE1A9CE06A34 6
Malicious:	false
Preview:	.....................>.. ....

C:\Users\user\AppData\Roaming\GlobalMgr.db

Process:	C:\Users\user\Desktop\SEMqjw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	158
Entropy (8bit):	4.417251221671609
Encrypted:	false
SSDEEP:	3:LDIdyGK3M7/U9TqMm9HwXoveBG8uU9TqMm9HwXove7V8reKvRiQGVXVK8E:3Tu/UxqMm9HiovV8uUxqMm9HioveQpGU
MD5:	DE99847E0C87EF4021E1216C7C1F8218
SHA1:	FDAEFB41CFF17A3AB6C6263C96FCF401215B552F
SHA-256:	5B286D103AEB37283D4CD668B477109B96976F12E063DE5B2FA7A2F4CCA88907
SHA-512:	C0C4A47C5924F76FD89F26001A64DA50EDEF5F5ED887BF0D53EC25584EBA8CBB2B235EBCD02F71CAD107F5805AAB92032F8BF4ABF044667546B0A999D3A287 2
Malicious:	false
Preview:	[Profile]..config1=c03ffea51228692909f5ef02221df8f2..config2=c03ffea51228692909f5ef02221df8f2..config3=..config4=1b3d82ff206f2697db14bb5ee90b3a8d..config5=1..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.88728452647213
TrID:	- Win32 Executable (generic) a (10002005/4) 99.66% - UPX compressed Win32 Executable (30571/9) 0.30% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SEMqjw.exe
File size:	655048
MD5:	1eeced28416a157bb6c1915c75f01bd3
SHA1:	eb423477cacd23647bc3a5af5f7b86e64e41826a
SHA256:	b5070e72b3a0b2f30e8333b2bb37e3db553bba74d24869 a302cf65d1af4c568f
SHA512:	853ffaca2e0fdaa7cc56484fe09cf9de9ad52298e3ed8bf9 3cc3ce8624746f62a53885b683196a2924e848e6882543 d7fe947daa12439be06cd7b56cbdde7e19

General

SSDEEP:	12288:BnkNowLbiumijG/sJcj0lV/cDM5cr4sLjLXuDMIC0 3IKDfIbOOAUGJiF2tdm:Bkt3xbk2cj0XcDM5exyBT4KD0 OO8ndm
File Content Preview:	MZ.....................@................................8...........!..L.!T his program cannot be run in DOS mode....$......._.t....... ....3.......3.......3..;..........I..............I...K...I..8.............8 ..............G.......Q.......C..

File Icon

Icon Hash:	a2a0b496b2caca72

Static PE Info

General

Entrypoint:	0x5a14c0
Entrypoint Section:	UPX1
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x61308606 [Thu Sep 2 08:06:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	15067c0e1192397d25d55aa213865b7e

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 1/22/2019 4:00:00 PM 1/26/2022 4:00:00 AM
Subject Chain	• CN="Anhui Shabake Network Technology Co., Ltd.", OU=è¿è¥, O="Anhui Shabake Network Technology Co., Ltd.", L=Ma'anshan, S=Anhui, C=CN, SERIALNUMBER=91320804MA1MKN9Q0G, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.1=Ma'anshan, OID.1.3.6.1.4.1.311.60.2.1.2=Anhui, OID.1.3.6.1.4.1.311.60.2.1.3=CN
Version:	3
Thumbprint MD5:	82131D9B33E4A0F9B769F39D1A877284
Thumbprint SHA-1:	361AA4713F3588E09B44F3AB6F574B2F118A0CAC
Thumbprint SHA-256:	0C1FB0A95313A99C6EBEB09E403D0F876B8028DE6FE08F7C8FA499708CFFAEFD
Serial:	010FADBCE9936CE0F10987519C38EBCC

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x109000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_ DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX1	0x10a000	0x98000	0x97800	False	0.990924092409	data	7.93044575348	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1a2000	0x7000	0x6200	False	0.183354591837	data	3.9708189817	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/29/21-17:21:40.244432	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
10/29/21-17:22:07.450292	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 17:21:37.660000086 CEST	192.168.2.6	8.8.8.8	0x6957	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:38.783749104 CEST	192.168.2.6	8.8.8.8	0x9f9a	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:39.156991959 CEST	192.168.2.6	8.8.8.8	0xd0d1	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:39.825139999 CEST	192.168.2.6	8.8.8.8	0x9f9a	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:47.460014105 CEST	192.168.2.6	8.8.8.8	0x5683	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:47.961390972 CEST	192.168.2.6	8.8.8.8	0xe8a3	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 17:21:48.027539968 CEST	192.168.2.6	8.8.8.8	0xf29c	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:48.583543062 CEST	192.168.2.6	8.8.8.8	0x7a68	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:49.494415998 CEST	192.168.2.6	8.8.8.8	0x6346	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:54.463187933 CEST	192.168.2.6	8.8.8.8	0x46ea	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:02.018100977 CEST	192.168.2.6	8.8.8.8	0x20dc	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:06.016551971 CEST	192.168.2.6	8.8.8.8	0x3c09	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.039350033 CEST	192.168.2.6	8.8.8.8	0x3c09	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:15.579539061 CEST	192.168.2.6	8.8.8.8	0x595b	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:18.526875019 CEST	192.168.2.6	8.8.8.8	0x693a	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:27.040719032 CEST	192.168.2.6	8.8.8.8	0xb2a	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:32.370229959 CEST	192.168.2.6	8.8.8.8	0x4653	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:47.709912062 CEST	192.168.2.6	8.8.8.8	0x2b23	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:48.527937889 CEST	192.168.2.6	8.8.8.8	0x7bd2	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:51.098109961 CEST	192.168.2.6	8.8.8.8	0xd350	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:53.733124971 CEST	192.168.2.6	8.8.8.8	0x43dd	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.168602943 CEST	192.168.2.6	8.8.8.8	0x5cf5	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.173607111 CEST	192.168.2.6	8.8.8.8	0x74c6	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.264389038 CEST	192.168.2.6	8.8.8.8	0x2844	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:55.419728041 CEST	192.168.2.6	8.8.8.8	0xb32e	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:59.392890930 CEST	192.168.2.6	8.8.8.8	0xa8b8	Standard query (0)	dcdn.adnxs.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:59.399033070 CEST	192.168.2.6	8.8.8.8	0xe793	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:15.127218008 CEST	192.168.2.6	8.8.8.8	0xa1ea	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:36.646533012 CEST	192.168.2.6	8.8.8.8	0xafb5	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:58.029892921 CEST	192.168.2.6	8.8.8.8	0xb52f	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:19.532994032 CEST	192.168.2.6	8.8.8.8	0x44bd	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:41.298774958 CEST	192.168.2.6	8.8.8.8	0xdadf	Standard query (0)	w.nanweng.cn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:21:37.921220064 CEST	8.8.8.8	192.168.2.6	0x6957	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:37.921220064 CEST	8.8.8.8	192.168.2.6	0x6957	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:37.921220064 CEST	8.8.8.8	192.168.2.6	0x6957	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:39.175995111 CEST	8.8.8.8	192.168.2.6	0xd0d1	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:21:40.113857031 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:40.113857031 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:21:40.113857031 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:40.244338989 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:40.244338989 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:40.244338989 CEST	8.8.8.8	192.168.2.6	0x9f9a	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:47.489105940 CEST	8.8.8.8	192.168.2.6	0x5683	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:21:47.981981039 CEST	8.8.8.8	192.168.2.6	0xe8a3	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:21:48.053543091 CEST	8.8.8.8	192.168.2.6	0xf29c	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:48.607000113 CEST	8.8.8.8	192.168.2.6	0x7a68	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:48.607000113 CEST	8.8.8.8	192.168.2.6	0x7a68	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:49.513668060 CEST	8.8.8.8	192.168.2.6	0x6346	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:49.513668060 CEST	8.8.8.8	192.168.2.6	0x6346	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:49.513668060 CEST	8.8.8.8	192.168.2.6	0x6346	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:54.482708931 CEST	8.8.8.8	192.168.2.6	0x46ea	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:54.482708931 CEST	8.8.8.8	192.168.2.6	0x46ea	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:21:54.482708931 CEST	8.8.8.8	192.168.2.6	0x46ea	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:02.281805038 CEST	8.8.8.8	192.168.2.6	0x20dc	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:02.281805038 CEST	8.8.8.8	192.168.2.6	0x20dc	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:02.281805038 CEST	8.8.8.8	192.168.2.6	0x20dc	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.328141928 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.328141928 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.328141928 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.450149059 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.450149059 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:07.450149059 CEST	8.8.8.8	192.168.2.6	0x3c09	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:15.597419977 CEST	8.8.8.8	192.168.2.6	0x595b	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:15.597419977 CEST	8.8.8.8	192.168.2.6	0x595b	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:22:15.597419977 CEST	8.8.8.8	192.168.2.6	0x595b	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:18.546717882 CEST	8.8.8.8	192.168.2.6	0x693a	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:18.546717882 CEST	8.8.8.8	192.168.2.6	0x693a	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:18.546717882 CEST	8.8.8.8	192.168.2.6	0x693a	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:27.442821980 CEST	8.8.8.8	192.168.2.6	0xb2a	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:27.442821980 CEST	8.8.8.8	192.168.2.6	0xb2a	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:27.442821980 CEST	8.8.8.8	192.168.2.6	0xb2a	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:32.389811993 CEST	8.8.8.8	192.168.2.6	0x4653	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:32.389811993 CEST	8.8.8.8	192.168.2.6	0x4653	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:32.389811993 CEST	8.8.8.8	192.168.2.6	0x4653	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:47.731515884 CEST	8.8.8.8	192.168.2.6	0x2b23	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:48.549268961 CEST	8.8.8.8	192.168.2.6	0x7bd2	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:51.119666100 CEST	8.8.8.8	192.168.2.6	0xd350	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:51.119666100 CEST	8.8.8.8	192.168.2.6	0xd350	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:51.119666100 CEST	8.8.8.8	192.168.2.6	0xd350	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:53.752207041 CEST	8.8.8.8	192.168.2.6	0x43dd	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:53.752207041 CEST	8.8.8.8	192.168.2.6	0x43dd	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:53.752207041 CEST	8.8.8.8	192.168.2.6	0x43dd	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.194608927 CEST	8.8.8.8	192.168.2.6	0x5cf5	No error (0)	ad.doublec lick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:22:54.194608927 CEST	8.8.8.8	192.168.2.6	0x5cf5	No error (0)	dart.l.dou bleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.195230961 CEST	8.8.8.8	192.168.2.6	0x74c6	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.195230961 CEST	8.8.8.8	192.168.2.6	0x74c6	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.195230961 CEST	8.8.8.8	192.168.2.6	0x74c6	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:54.285630941 CEST	8.8.8.8	192.168.2.6	0x2844	No error (0)	cvision.me dia.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:22:55.438694954 CEST	8.8.8.8	192.168.2.6	0xb32e	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:22:55.438694954 CEST	8.8.8.8	192.168.2.6	0xb32e	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 17:22:59.414424896 CEST	8.8.8.8	192.168.2.6	0xa8b8	No error (0)	dcdn.adnxs.com	secure-adnxs.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:22:59.418042898 CEST	8.8.8.8	192.168.2.6	0xe793	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Oct 29, 2021 17:22:59.418042898 CEST	8.8.8.8	192.168.2.6	0xe793	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Oct 29, 2021 17:22:59.418042898 CEST	8.8.8.8	192.168.2.6	0xe793	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:15.146856070 CEST	8.8.8.8	192.168.2.6	0xa1ea	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:15.146856070 CEST	8.8.8.8	192.168.2.6	0xa1ea	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:15.146856070 CEST	8.8.8.8	192.168.2.6	0xa1ea	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:36.665920973 CEST	8.8.8.8	192.168.2.6	0xafb5	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:36.665920973 CEST	8.8.8.8	192.168.2.6	0xafb5	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:36.665920973 CEST	8.8.8.8	192.168.2.6	0xafb5	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:58.049412966 CEST	8.8.8.8	192.168.2.6	0xb52f	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:58.049412966 CEST	8.8.8.8	192.168.2.6	0xb52f	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:23:58.049412966 CEST	8.8.8.8	192.168.2.6	0xb52f	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:19.554090023 CEST	8.8.8.8	192.168.2.6	0x44bd	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:19.554090023 CEST	8.8.8.8	192.168.2.6	0x44bd	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:19.554090023 CEST	8.8.8.8	192.168.2.6	0x44bd	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:41.318238020 CEST	8.8.8.8	192.168.2.6	0xdadf	No error (0)	w.nanweng.cn		47.102.38.15	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:41.318238020 CEST	8.8.8.8	192.168.2.6	0xdadf	No error (0)	w.nanweng.cn		106.14.178.247	A (IP address)	IN (0x0001)
Oct 29, 2021 17:24:41.318238020 CEST	8.8.8.8	192.168.2.6	0xdadf	No error (0)	w.nanweng.cn		47.103.45.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49735	104.20.184.68	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:21:48 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: geolocation.onetrust.com Connection: Keep-Alive
2021-10-29 15:21:48 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 29 Oct 2021 15:21:48 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: 6a5d654f7936062d-FRA
2021-10-29 15:21:48 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	192.168.2.6	49808	104.26.7.139	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:51 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: btloader.com Connection: Keep-Alive
2021-10-29 15:22:51 UTC	1	IN	HTTP/1.1 200 OK Date: Fri, 29 Oct 2021 15:22:51 GMT Content-Type: application/javascript Content-Length: 10157 Connection: close Cache-Control: public, max-age=1800, must-revalidate Etag: "643eb1aad6ba3932ca744b96ffc00048" Via: 1.1 google CF-Cache-Status: HIT Age: 2166 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=FiFUZGppY4dhd0%2BkQcuguaUxNU7Q0jR8Ouat3ONrOy05o4CKSMI1STgCTFkMGgo1WZ7wqiroLT403mra2awuL0puMHsHzms3SKMMPy7GMd7pmKSWMHte8SICB9Xedw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a5d66d6193e3244-FRA
2021-10-29 15:22:51 UTC	2	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 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 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}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(functio
2021-10-29 15:22:51 UTC	2	IN	Data Raw: 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 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 5d 29 2c 74 5b 30 5d 29 7b 63 61 73 65 20 30 3a 63 61 73 65 20 31 3a 69 3d 74 3b 62 72 65 61 6b 3b 63 61 73 65 20 34 3a 72 65 74 75 72 6e 20 Data Ascii: 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

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:51 UTC	3	IN	Data Raw: 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 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 3d 7b 22 74 72 61 63 65 49 44 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 21 65 7c 7c 22 6e 75 6d 62 65 72 22 21 3d 74 79 70 65 6f Data Ascii: }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={traceID:function(e,t,n){if(!e||"number"!=typeo
2021-10-29 15:22:51 UTC	5	IN	Data Raw: 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 61 2c 61 70 69 44 6f 6d 61 69 6e 3a 64 2c 76 65 72 73 69 6f 6e 3a 62 2c 77 65 62 73 69 74 65 73 44 61 74 61 3a 6f 2c 73 69 74 65 49 6e 66 6f Data Ascii: site_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain:a,apiDomain:d,version:b,websitesData:o,siteInfo
2021-10-29 15:22:51 UTC	6	IN	Data Raw: 6f 2b 30 29 29 2c 6d 61 78 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 28 31 30 30 2a 28 73 2b 75 2a 28 61 2b 74 29 29 29 7d 2c 61 2b 3d 74 7d 29 7d 76 61 72 20 64 3d 74 5b 65 5d 3b 69 66 28 6e 75 6c 6c 21 3d 64 Data Ascii: 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(100*(s+u*(a+t)))},a+=t})}var d=t[e];if(null!=d
2021-10-29 15:22:51 UTC	7	IN	Data Raw: 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 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 65 74 75 72 6e 20 69 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 73 77 69 74 63 68 28 65 2e 6c 61 62 65 6c 29 7b 63 61 73 65 20 30 3a 72 65 74 75 Data Ascii: teEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;return i(this,function(e){switch(e.label){case 0:retu
2021-10-29 15:22:51 UTC	9	IN	Data Raw: 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 65 6d 6f 62 69 6c 65 7c 69 70 28 68 6f 6e 65 7c 6f 64 29 7c 69 72 69 73 7c 6b 69 6e 64 6c 65 7c 6c 67 65 20 7c 6d 61 65 6d 6f 7c 6d 69 64 70 Data Ascii: true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge |maemo|midp|mmp
2021-10-29 15:22:51 UTC	10	IN	Data Raw: 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b 7c 72 74 7c 73 65 29 7c 70 72 6f 78 7c 70 73 69 6f 7c 70 74 5c 2d 67 7c 71 61 5c 2d 61 7c 71 63 28 30 37 7c 31 32 7c 32 31 7c 33 32 7c 36 30 7c 5c 2d 5b 32 Data Ascii: v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc(07|12|21|32|60|\-[2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49815	172.67.69.19	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:54 UTC	11	OUT	GET /px.gif?ch=1&e=0.6358356914721921 HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ad-delivery.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:54 UTC	12	IN	HTTP/1.1 200 OK Date: Fri, 29 Oct 2021 15:22:54 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34 sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Fri, 29 Oct 2021 14:44:06 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 2365 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:\/\/a.nel.cloudflare.com\/report\/v3?s=uNN7uBc3ikZ6zW%2BrCdk21Az%2FMlXK 9DAlnZu54uXxzKSwEzHM%2B0gfOV9G1kJqdKoIzD9gnQrT9vSGwjLZTxIkjuh7Y01pqTqSnzObP3FX9fWjlN5gPUBt 6yT45d5pkHMfRA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a5d66e92f99062d-FRA
2021-10-29 15:22:54 UTC	14	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 00 00 00 01 Data Ascii: GIF89a!
2021-10-29 15:22:54 UTC	14	IN	Data Raw: 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49814	216.58.215.230	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:54 UTC	12	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ad.doubleclick.net Connection: Keep-Alive
2021-10-29 15:22:54 UTC	14	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Fri, 29 Oct 2021 09:29:54 GMT Expires: Sat, 30 Oct 2021 09:29:54 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Cache-Control: public, max-age=86400 Age: 21180 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-29 15:22:54 UTC	14	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii: (& N(

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:54 UTC	15	IN	Data Raw: 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 1 1 11 11 11 11 11 1 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 1 1 11 1 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 1 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 1 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 1 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 1 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 1 11 1 11 11 11 11 11 11 11 11 11 11 1 11 11 1 11 1 11 11 1 11 11 11 1 11 11 1 11 HjI#I vA} S3 HjI#I vA} 11 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49826	87.248.118.22	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	15	OUT	GET /lo/api/res/1.2/z3nJ.i0wJLUKE.PUO3hx1w--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/ https://s.yimg.com/av/ads/1634277746662-1414.jpg HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: s.yimg.com Connection: Keep-Alive
2021-10-29 15:22:59 UTC	16	IN	HTTP/1.1 200 OK Content-Length: 217987 Access-Control-Allow-Headers: X-Requested-With Access-Control-Allow-Origin: * Cache-Control: public, max-age=2592000 Content-Type: image/jpeg Edge-Cache-Tag: 38932453914941579984742420851352231563 4,41593064833971211187228565 7998251086336,ae7a14591aaf8d474cdb3f92111c923e Etag: "019c4e8e1e43845adf8a3e821c73b996" Last-Modified: Tue, 19 Oct 2021 15:32:33 GMT Server: ATS Status: 200 OK Timing-Allow-Origin: * X-Request-Id: 6256e01a8e0a04a15e6a937a1cbbd939 Accept-Ranges: bytes Date: Tue, 19 Oct 2021 16:21:16 GMT X-Served-By: cache-wdc5538-WDC X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1634660476.241437,VS0,VE241 Age: 860503 Strict-Transport-Security: max-age=15552000 Referrer-Policy: no-referrer-when-downgrade X-Frame-Options: SAMEORIGIN cld_cache: MISS cld_hits: 0 cld_id: 6256e01a8e0a04a15e6a937a1cbbd939 cld_by: cache-wdc5538-WDC cld_latency: 241 Connection: close Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff
2021-10-29 15:22:59 UTC	17	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 96 00 96 00 00 ff e2 02 28 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 18 00 00 00 00 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 00 00 00 00 00 00 00 00 00 00 00 00 00 61 63 73 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 f6 d6 00 01 00 00 00 00 d3 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 64 65 73 63 00 00 00 f0 00 00 00 74 72 58 59 5a 00 00 01 64 00 00 00 14 67 58 59 5a 00 00 01 78 00 00 00 14 62 58 59 5a 00 00 01 8c 00 00 00 14 72 54 52 43 00 00 01 a0 00 00 00 28 67 54 52 43 00 00 01 a0 00 00 00 28 62 54 52 43 00 00 01 a0 00 00 00 28 77 Data Ascii: JFIF(ICC_PROFILEmntrRGB XYZ acsp-desctrXYZdgXYZxbXYZrTRC(gTRC(bTRC(w
2021-10-29 15:22:59 UTC	18	IN	Data Raw: 04 fd 61 8a 5d af 96 ee 31 0e f8 8f 8d ff 00 d0 0e ad 7d 6c f9 84 93 8c 8c 4a 86 78 cf 1d b2 39 fc f8 00 75 5b b7 51 ff 00 dc f5 c7 fa 64 e7 ff 00 eb 10 fc da fb f5 cc c4 bd 90 ca da 32 31 71 f5 04 f3 6f 4c de 30 3d d6 32 55 84 f7 57 a4 92 38 19 c9 c0 f9 7b 9e 3e 84 76 1d 79 0a 55 da 9a 73 01 49 1f fc 89 f9 c7 a5 84 a6 ec 6e c3 27 d7 d3 db 47 87 22 6e 49 dc 9e 7d c7 b0 3d f3 c6 33 f5 e0 7e bd cc 89 6a b8 6c 8f 91 f7 dd dd 78 8e 43 82 21 3d 70 88 4a b1 8c 64 70 41 07 20 f7 c6 06 09 c6 4e 4e 7a 72 55 db 7e e1 c3 26 f1 86 75 7c 7c a1 b3 59 b6 61 57 61 08 73 da 73 f7 6f 09 11 65 32 e2 a3 4e a7 4c 40 57 c3 cf a7 4a 6f 0f 42 9a c8 52 b6 3e d1 c1 4a 94 d3 a9 71 97 1c 6d 46 eb 7f d3 e3 0d c0 ad de 63 eb 0c b1 3a a1 6f c9 8f 49 bc 16 97 63 48 79 31 e9 17 72 5a 44 Data Ascii: a]1}lJx9u[Qd21qoL0=2UW8{>vyUsIn'G"nl}=3~jlxC!=pJdpA NNzrU~&u||YaWassoe2NL@WJoBR>JqmFc:ol cHy1rZD
2021-10-29 15:22:59 UTC	20	IN	Data Raw: 83 f2 ef d3 90 01 2f b9 a1 41 55 b6 42 7b 7c fb 80 46 40 23 27 f4 19 c7 e7 db b7 4e 59 0c da fb f7 f2 d6 14 24 49 fc 4b e3 b2 b2 3e 67 04 6e 39 c7 1b 89 47 71 c0 3c 71 cf 42 85 09 2f a7 03 d3 df fc 73 f3 39 f9 25 3c 63 07 bf 4a 14 21 4b 47 0a 00 02 02 b9 38 f7 c1 38 e4 80 01 e3 b1 c6 39 ef 81 d2 85 08 ae b5 85 1d dd c6 47 07 27 39 3c fb e3 9e 00 24 12 08 fa 0e 9c af db fe 91 0f 47 c5 dd 12 7f 87 88 db fc 48 e8 6a 49 23 76 ae e9 1a 41 f9 11 7d 53 33 8e 0e 09 27 94 9d a7 04 e4 76 c8 e9 92 fb 4e 89 5f fb ad 96 e6 3e 9d db b3 78 ed 51 03 67 d6 8f fd be 3b c7 d3 9e e8 eb ad b4 15 23 24 70 31 ee 32 77 76 2a 23 92 a4 e7 bf 6f d7 38 f4 b6 ec ac 7f 98 df fe 9f 6d 1e 6e f8 a6 ca 21 98 24 78 11 6e 2e 47 84 21 54 da ca 9c 27 b2 23 21 20 1c 92 3f 12 cf 1f 97 b0 cf c8 Data Ascii: /AUB{|F@#'NY$IK>gn9Gq<qB/s9%<cJ!KG889G'9<$GHjI#vA}S3'vN_>xQg;#$p12wv*#o8mn!$xn.G!T'#! ?

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	21	IN	Data Raw: 91 c0 c9 07 87 5c 57 b9 56 ec a5 09 09 c9 4e d5 91 91 81 8e b3 42 59 33 a6 97 76 7b 77 16 e7 60 79 c6 a0 2f 0d 3c b4 f0 1c 34 cb bc fc f8 08 2e b8 db 92 79 c8 f4 f2 83 9c 29 59 04 82 9d c0 6e 52 92 a3 bb d9 49 c6 30 b1 d1 50 92 6f cc 01 e4 60 0b 58 d7 bb 7c 5b 3f 0f 8c 16 ed 7a d1 3c ef b8 55 93 91 82 45 2e 9a 54 90 79 49 f5 28 fd 7e 5f 4d 96 c2 41 4d 1f 25 1e f7 23 e7 18 cd bd 79 e8 3c 0c 4d 12 50 0a 8f b0 23 9c 8c 63 1f 3c 0c 73 d8 7c fa be 57 c0 9e ef 43 15 4a cf b8 7a 08 28 86 8f 71 80 71 92 39 ed c7 7e d8 23 1e 91 dc 9c f4 38 22 32 ef f9 08 f4 b4 f0 12 00 04 1f cb 3c 7c b2 47 d7 a1 af 21 0f 8f c9 46 52 47 07 76 7e 58 e0 8c 73 fd 46 7d cf 6e 87 0a 08 be 82 33 f3 cf f2 c7 63 f9 02 7f 2c 7d 3a 50 a1 2d d4 12 4e 71 ee 79 23 8c a8 e3 f9 64 63 1d 0e 66 9d Data Ascii: \WVNBY3v{w`y/<4.y)YnRI0Po`X|[?z<UE.TyI(~_MAM%#y<MP#c<s|WCJz(qq9~#8"2<|G!FRGv~XsF}n3c,}:P-Nqy#dcf
2021-10-29 15:22:59 UTC	22	IN	Data Raw: fe d4 a4 34 b3 d7 30 93 30 92 e0 4b b9 1d 9c 95 6d e6 fc 2c 46 6f f5 e7 41 ba 49 2a aa 96 4c a3 31 48 be 3c 03 e1 c6 e5 8b 5b b4 34 68 d6 0d 2f f1 85 79 da ba 7d 5d d2 ca 1d 2d 30 5a 9a e2 1b 6e 64 84 6c 94 96 0c 76 fe 29 96 97 b4 25 0d 48 52 c2 d0 f7 2e 36 1c 79 48 5a d6 a4 15 4b a5 e9 45 76 cb d9 b3 e8 53 2d 38 2b a6 84 95 49 01 4a 04 80 12 14 d7 72 6d a3 87 bd e0 3d 20 fc 32 e8 d7 4a 3a 51 47 d2 fd a9 32 68 5e cb 97 8a 60 c4 d4 ea ea ca a6 75 f3 9c 80 54 94 d8 dd 20 80 1c 38 0c 35 58 54 14 88 10 aa ca dd 55 8e d1 91 5c 3f f0 95 7a 80 65 c9 b0 02 ff 00 01 55 35 86 21 40 96 96 d2 94 26 7c 59 49 46 5b f2 d4 bd ef 47 a8 2a a8 a8 02 ab 12 13 53 52 be ba 62 46 81 41 d3 95 b2 3e b1 f0 4f e3 df 4e 28 7a 69 d3 89 a8 d9 29 1f dc db 0a 52 f6 75 02 c6 53 9a Data Ascii: 400Km,FoAI*L1H<[4h/y}]-0Zndlv)%HR.6yHZKEvS-8+IJrm= 2J:QG2h^`uT 85XTUVN9zeU5!@&|YIF[G*SRb FA>ON(zi)RuS
2021-10-29 15:22:59 UTC	23	IN	Data Raw: ed fb a1 1e b0 d0 dd 25 58 fc 2c b6 9c 9c 1c 61 84 fb 73 83 c7 bf bf d7 a8 49 96 12 15 fe 62 e5 ad ed f5 89 6a 53 90 75 01 87 36 d3 de 97 88 a5 b8 a1 55 04 0c 10 43 80 02 07 6f 57 62 70 08 3f 2c 64 8e ff 00 3e 96 01 c7 cb e9 0b 1a b7 c7 cb be 1a 5c 6a 3e 52 a0 42 f7 2b 1f 40 40 19 00 93 8e 14 08 f9 7d 7a 6e 03 bc 43 d0 ad 1e fe a2 15 a1 c7 26 9b 19 2e 15 10 96 47 19 db eb d8 70 4f b9 f6 ed 81 f5 1d 08 a0 82 46 23 e7 f5 87 62 1b c3 f3 86 d4 98 db 26 b6 40 c1 dc 08 3b 70 02 41 4f 07 83 9c 80 3b 9e 77 74 c5 06 6d 4d dc ef 82 85 8c 39 b9 63 c7 85 fe 71 93 7f 69 bb 79 be f4 6d 04 67 65 95 77 28 80 4f ff 00 32 bf 46 1d 86 41 39 64 8c 0f 6f 60 07 59 2e 93 a4 7e 66 96 c3 fc 03 a7 f9 84 6b ba 32 07 e5 ea 08 01 fa e1 7f fa 7d f9 c6 64 a1 8c a9 5d c9 dc 55 f2 c9 56 Data Ascii: %X,asIbjSu6UCoWbp?,d>\j>RB+@@}znC&.GpOF#b&@;pAO;wtmM9cqiymgew(O2FA9do`Y.~fk2}d]UV
2021-10-29 15:22:59 UTC	24	IN	Data Raw: fd 20 88 84 ad ca 21 20 06 c2 76 80 09 fc 60 0c 1c 9c 12 41 39 c0 f5 60 ec f7 4f 4f c4 9d fe b0 b0 1d 08 f7 e3 01 3d 0d 2a 40 52 52 4a 30 52 af 49 dd c6 46 49 00 27 7e 7d 27 0a 04 83 90 42 79 0b 1a 77 f9 1f a4 39 97 bc 7b ee f7 df 05 d1 4e 52 d0 ad a9 23 1b 50 9d c7 8d a5 47 27 1d c7 1c 64 9c 67 2a ec 53 85 8c 6f f5 8e 61 51 2e 4e ef 7e fe 70 99 59 8b b5 49 48 4e 76 27 6a b9 c6 78 39 51 c2 89 3b 78 20 12 41 23 8e 7a 24 b6 51 27 36 f7 ef ed 0a 66 9d ff 00 28 4a a1 d3 8b f5 fa 03 3b 72 99 35 ea 33 28 3c 28 fe f6 a5 19 9f 4a 78 c6 54 b0 9c ee c9 cf 24 f3 d1 14 a0 52 52 33 df f2 76 36 80 84 07 7f e3 eb 1d cf ca 84 4c c9 c9 00 80 99 f2 01 c1 2a db 97 57 9e 77 6e 56 4a 12 af 51 00 8c e0 2b 83 d5 3a 90 a1 31 44 76 5d f5 6f 4d fa f9 ee 8b 74 97 96 92 6e c3 5b e5 Data Ascii: ! v`A9`OO=*@RRJ0RIFI'~}'Byw9{NR#PG'dg*SoaQ.N~pYIHNv'jx9Q;x A#z$Q'6f(J;r53(<(JxT$RR3v6L* WwnVJQ+:1Dv]oMtn[
2021-10-29 15:22:59 UTC	25	IN	Data Raw: af 48 6d b6 50 bd db bd 24 1e 70 33 d1 c7 6d 2a 96 c0 85 21 49 cb fa ad f3 81 05 94 2d 33 01 65 21 49 58 6b 76 92 41 1e 63 c6 2a 2e ac 51 9d b4 e9 93 d5 4e 52 dc a4 d6 5e 32 da de 8f 32 23 ee 49 1e 72 21 c6 92 9f 31 b5 a4 47 d8 f3 5e 63 ad 3c b6 50 3c 96 de 60 22 4a e9 2a b6 53 ad 2b 4a 18 a2 c3 0e ed f9 77 6f dd 9c 7a c6 c6 e9 3c ba 9a 65 4b 2b 41 a8 5a 50 15 8b 2e c3 00 05 f8 65 9e f1 14 c1 d5 3e f4 c6 d7 22 26 30 e0 52 b2 95 f9 4e 24 9f 2c 23 28 52 54 9e dc ba 01 24 65 47 07 bb 24 c8 ea 82 92 05 c9 7e 24 eb a5 f8 07 8b fa 4a a4 89 b2 a6 a8 c9 1d b0 2c b2 2c fa ba 33 e6 af 18 9d 74 ca bd 16 2d 48 79 96 e4 5a ba 8b 22 2b 51 e5 b6 ec a8 ac 3a b7 5b f2 94 f4 42 db a1 e9 09 e0 b4 95 c9 6c 29 3b f6 94 ab d5 d5 26 d7 d9 15 75 64 26 41 5c b5 1c d6 83 85 65 ef Data Ascii: HmP$p3m*!I-3e!IXkvAc*.QNR^22#Ir!1G^c<P<`"J*S+Jwoz<eK+AZP.e>"&0RN$,#(RT$eG$~$J,,3t-HyZ"+Q:[Bl);&ud&A\e
2021-10-29 15:22:59 UTC	27	IN	Data Raw: 66 ea b8 cf 2c d3 4d 41 49 ca 47 1e a1 db 9d c3 27 9c 1c 93 dc 13 f4 57 e2 e7 ad 3c d3 db 2c cc 2d 6e 57 f3 f6 ef 1f 36 26 cc ca 0a 7b e2 05 c5 fe 99 6e b5 de 26 ff 00 0c 54 d4 8f 12 9a 2a 00 ed ab 1a 60 ad c7 04 90 dd df 4c 70 10 49 c9 dc 53 9e f9 03 82 71 81 d1 76 61 27 69 d1 db fe 73 78 5e f1 17 6a a8 8d 9d 5c 37 c8 39 6e 0e 6f 9b 67 e9 1d 57 21 83 e4 7e 12 9c e0 82 12 0e 54 38 c9 fc 81 e3 18 ef c7 5e a4 48 65 0d 71 97 cf 50 e3 d2 3c c9 bb 69 df 85 20 fb d5 f9 96 86 d5 65 3c 4d 3b 7f f9 8a 48 c1 03 21 38 09 e0 f2 4f b7 1c 76 1d 04 86 16 0e ed ef f8 e7 a4 4b 51 16 20 df 81 cb df 8f 84 47 71 99 06 7a 15 b7 84 af 3c 9e 42 86 41 27 82 72 01 27 9e 3b 74 d6 37 ec 8f 7b af ef 94 74 76 81 b9 e3 a7 87 83 78 da f1 f2 e5 6c 62 3e ec 00 a5 6d e4 f1 c8 da 48 c8 e3 Data Ascii: f,MAIG'W<,-nW6&{n&T*`LpISqva'isx^j\79nogW!~T8^HeqP<i e<M;H!8OvKQ Gqz<BA'r';t7{tvxlb>mH
2021-10-29 15:22:59 UTC	28	IN	Data Raw: 20 17 56 22 43 81 64 d8 fc c3 e4 61 9d 71 5e 56 8d b4 14 6e 2b 96 81 45 c1 c2 53 54 ab 42 86 b3 90 55 b7 6b ef 21 79 21 24 f6 ec 0f 0a c7 55 95 3b 53 66 d3 95 09 f5 d4 f2 b0 82 6e a1 60 ce f9 dd 80 7e 36 d0 bc 69 36 67 44 fa 4d b6 d7 87 63 ec 3d a5 b4 52 c0 bd 35 34 c5 bb 8d e5 29 4e 7b 89 b6 b9 c2 0d 32 fa b2 6b ee a1 8a 2d d7 41 a9 3a e8 0a 43 50 ea 91 5d 71 c0 e7 2d 96 db 0f 05 a9 2e 00 76 14 83 bf 1f 5e a2 d3 6d ad 95 56 a6 a6 af 91 3b fd 2a 09 c8 6f 24 8f bf 84 4f da 5f 87 fd 35 d9 12 7f 33 b4 3a 3b b5 29 24 27 e3 eb 69 26 05 06 cf 2c 59 72 e1 0e 52 9e 4e 12 47 b6 47 1c e0 64 60 9f 7c e4 63 1f 97 3d 5a 61 33 43 cb 0e 9d ee 08 39 e4 44 64 9a 62 1d 42 5a 96 97 29 64 fc 48 50 f8 92 a0 a6 20 a4 d8 be b6 e5 a5 25 ae 49 c6 3d bb 7f 79 ea 31 48 22 c0 03 ca Data Ascii: V"Cdaq^Vn+ESTBUk!y!$U;Sfn`~6i6gDMc=R54)N{2k-A:CP]q-.v^mV;*o$O_53:;)$'i&,YrRNGGd`|c=Za3C 9DdbBZ)dHP %I=y1H"
2021-10-29 15:22:59 UTC	29	IN	Data Raw: b7 4e 88 a8 94 da 3c 48 6c 2c 2c e1 96 d6 16 92 46 d0 b6 d6 a7 0b 8c 38 36 00 85 b4 b4 2c 6d 4a 92 a4 29 29 57 52 90 25 8e d6 00 1f 24 92 2c d6 ef 27 d2 d0 0a dd ad b5 2b 00 44 ea c9 8b 4a 00 09 96 54 a1 2b 92 90 92 1f 33 ac 4c 1a 63 a8 72 a1 cd 8f 66 5d d2 96 b9 27 2d 50 2b 32 3b 55 d6 4d 4f fd f3 56 3d 02 b2 cb 63 28 58 da 9a 9b 08 5b cd 24 3e d4 86 fa 32 46 3b e2 1b 83 0d 3b 8c 55 99 8b 1d 93 85 95 f1 e1 4b 5b 2c 29 bb 80 c2 ce f7 d6 2c db 18 52 7f 12 9c ca 46 3d b3 91 b4 90 79 e7 8c fd 40 3d 35 48 04 84 86 07 53 be cf 1c eb 18 60 40 69 79 84 9b 9c 59 12 55 ad b8 41 8f 83 0e 0f 48 51 39 c0 56 d1 b7 80 38 4f 6e e5 5e e0 8c 29 47 b0 18 69 4e 06 49 d4 bf 85 fe 4d ee ed 2b 70 cd e7 f6 8f 0a a7 39 82 36 1c 76 dc 47 6f d3 f5 ed 9e fc 7e 64 c4 19 99 c0 e3 f6 Data Ascii: N<Hl,,F86,mJ))WR%$,'+DJT+3Lcrf]'-P+2;UFOV=c(X[$>2F;;UK[,),RF=y@=5HS`@iyYUAHQ9V8On^)GiNIM +p96vGo~d
2021-10-29 15:22:59 UTC	31	IN	Data Raw: 8c e0 73 c7 7c f4 35 81 96 e6 dd bd fd 2d 0e 8c b0 fb 42 a2 97 b5 33 4f 8a bd 7b 34 fd 67 1c 14 a3 cd b9 6a c0 ed 20 90 a2 a0 c7 3c 9e c9 ce 31 d7 9e f4 c3 fe 2e 97 ff 00 80 af fc e3 73 d1 44 e2 a6 aa bb 7e ba 7f fe 18 8a 00 b8 bc 92 53 d8 ab 24 0e c4 76 cf 04 64 27 3c 60 f1 c9 24 8e b2 89 05 9c 16 7e 0f 94 6a 7e 12 5c 3e 97 f5 d6 01 72 12 76 8c a4 11 92 0f 1e c4 fa 4e 30 40 f9 00 70 ae 7b fb 75 c2 4b 94 93 6d ed df 04 b3 38 48 7c d8 37 ac 26 b9 11 b0 72 50 94 8f 50 e4 1c 9e 53 8c 9c 1d a3 27 dc 8c fb 67 90 18 4a 46 bc 6f 68 72 52 55 7c 20 1e ed 77 c2 4c d4 34 d8 39 48 23 1f f2 9e 72 0e 01 c1 03 8c 9d a4 82 31 c1 29 e0 f4 1e b9 3e df e9 0f c0 78 43 61 d6 9a 96 e2 d9 42 78 40 c9 58 20 04 81 9c 63 f1 0c f2 0f 00 1e 73 f8 4a 4a 88 84 15 9c 44 e1 bf 37 03 c3 Data Ascii: s|5-B3O{4gj <1.sD~S$vd'<`$~j~\>rvN0@p{uKm8H|7&rPPS'gJFohrRU| wL49H#r1)>xCaBx@X csJJD7

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	31	IN	Data Raw: 30 42 a4 3c ac 28 05 72 a5 ba ae c4 02 38 56 01 03 2a 09 c7 74 fa a6 25 23 11 06 ec 09 e1 93 e5 f7 ee 88 a7 33 df f3 f7 c6 13 de 8d b7 0a c6 d2 92 55 b7 1f 89 3b b6 64 72 a4 13 80 b5 00 00 49 48 c6 4e ee 24 21 2f 73 c7 3f 77 81 ad 4d 61 ce 2c ce 8e b2 a1 66 02 50 11 ba ab 52 57 19 ed 96 42 4e 0e 48 25 3c 91 9e 0e 53 cf be 9f 66 02 28 ee 1b b4 fa ea c4 67 19 8d a0 5e b1 7f e8 57 cc fc e1 fa f2 30 4e 31 ce 01 cf eb ed fd 7b e7 f5 ea 7a 8b 9e 56 f7 ef c7 38 82 2f 04 d6 9c f1 81 d8 0c 63 18 c7 7f 6f 71 83 fa ff 00 37 20 b0 25 56 4f f5 66 ea d1 20 7c fc a1 68 4e bf b5 3f d4 ad dc 2d 78 8f 75 33 53 2c 6d 20 b4 6a 57 be a1 5c 10 6d cb 76 98 ca 96 fc c9 6e 61 6f bb b5 4b 6e 1c 08 c9 0a 7a 6c c9 03 01 98 d1 d0 b7 56 4e 42 76 65 62 15 76 d1 a4 d9 f2 0d 55 6c d4 c8 Data Ascii: 0B<(r8V*t%#3U;drIHN$!/s?wMa,fPRWBNH%<Sf(g^W0N1{zV8/coq7 %VOf |hN?-xu3S,m jW\mvnaoKnzIVNB vebvUl
2021-10-29 15:22:59 UTC	32	IN	Data Raw: 14 44 2c 57 04 eb 41 34 07 1f d2 53 bb c4 7d 62 3c f3 d9 a3 7c ff 00 3d 20 f0 03 b5 af 31 c7 9c 44 82 94 bc 7a 5b e0 8c 11 85 64 e0 85 03 c7 e4 3f 23 ee 31 d5 1b 38 c2 c4 b1 5b b3 ff 00 51 3e 47 38 b6 05 96 ae 49 f2 60 5f c3 cc 6f 86 a5 c7 62 c1 b9 83 4d 4b 6e 44 59 d0 54 25 d1 ea d4 f7 13 12 b1 42 9c 52 a6 d3 2e 97 28 a5 c4 a1 4a 41 0d ca 87 25 99 34 da 9c 60 60 d5 60 cf 84 eb b1 96 93 50 25 3e 35 04 b1 b3 83 90 f5 6e 19 36 e8 72 a5 a5 6c 52 52 08 c8 62 03 2b 8f 3d 3d 35 88 6e 2b 75 89 ed fe c3 ea a5 36 13 c2 ac af 83 a1 5c cc b1 f0 b4 5b 99 e2 da d4 d3 0d 7a d6 e5 bb 77 21 b4 3c e2 a9 0f bf e4 cd 21 d7 ed 9a 94 d6 7e 3a 05 3e 54 8a 90 16 b9 b2 14 0a d0 a4 a5 49 70 03 ab 26 1c ee 4b 36 f8 8f 3a 4a 08 69 8c 95 1d 72 17 6d 7e dc 6f 10 bd 95 a4 1a 97 a5 15 Data Ascii: D,WA4S}b<|= 1Dz[d?#18[Q>G8I`_obMKnDYT%BR.(JA%4```P%>5n6rlRRb+==5n+u6\[zw!<!~:>TIp&K6:Jirm~o
2021-10-29 15:22:59 UTC	34	IN	Data Raw: 4e 5e 59 44 ed e1 8a dc 96 9f 10 1a 59 53 7a 2c 86 61 3d a8 56 5b 70 65 2a 3b 82 2c 95 c3 ac c4 54 a4 33 21 40 36 b7 23 94 a0 3a 8d c5 c6 f2 92 b0 02 87 45 d8 ea 42 f6 a5 12 52 b4 e2 13 c0 c2 b2 01 25 41 c3 0b b8 61 cf 91 22 23 ed 54 a8 6c ca e5 90 54 9f cb 92 e2 f6 0e 4f 83 bb 1d 78 c7 45 8a 71 91 29 31 4b 89 f8 8f 2c 49 f2 52 40 5f c3 f9 85 b0 e9 49 f6 2e 25 49 e3 3f 81 58 ed cf a5 ac 7e a2 c0 bf 68 9b 71 61 9e a2 cf c1 f7 47 99 a4 12 84 a8 24 84 e1 05 c0 b8 eb c1 b8 f2 68 65 dc 53 61 43 4c 78 d2 df 4c 67 64 c8 82 c3 21 dd c8 4b cf 54 d6 86 e0 34 82 46 0b b2 9d 79 96 9b 07 f1 b8 e2 52 0f 3d 25 28 04 84 eb 61 df b9 ff 00 9d d0 59 72 d4 a2 e3 20 f9 f2 30 87 02 3e 65 82 7b 14 28 e0 0e 36 ed dd ed f9 71 fa fc cf 4d 20 83 84 e6 cf 9b d9 9e 3a 4f 65 47 40 e9 Data Ascii: N^YDYSz,a=V[pe*;,T3!@6#:EBR%Aa"#TlTOxEq)1K,IR@_I.%I?X~hqaG$heSaCLxLgd!KT4FyR=%(aYr 0>e{(6qM :OeG@
2021-10-29 15:22:59 UTC	35	IN	Data Raw: e2 c0 65 b5 a8 44 ae ae 91 b3 a9 d7 53 3d 76 94 e5 32 8d dd 63 78 e3 f2 b5 e2 fb a3 9d 1c da 3d 28 db 14 db 27 67 49 54 e9 d3 e6 04 3a 7e 19 2e cf 32 62 98 84 25 9f b7 96 51 c8 ef 8a bf 16 da 81 e2 be ef 95 72 dc 75 07 28 9a 77 4b 93 2d 36 8d 9a cb ab 11 69 b4 f6 f2 94 17 9b 68 a8 4c a9 49 c3 2a 95 29 69 53 8f b8 5b 65 bf 22 32 32 7c 17 a4 1d 20 ab db 15 aa a9 9c 94 99 29 59 4c b9 46 60 12 d1 a0 52 c0 2d ab 31 11 fa 89 f8 3f f8 3b 43 f8 7b b2 29 ea 41 93 33 69 cc 08 99 53 52 bc 2b 58 59 0e b4 4b 51 0e 42 4e 4a 0c 2d 6d d1 5b 9a bc 63 d2 a1 a6 24 06 cc 67 54 af 84 72 6a 8b 4c ce 5a 9c c0 4c 65 a9 90 e1 0a 25 38 f2 19 6d 94 14 84 87 5f 52 92 95 0c d4 fa 50 b9 ab 13 94 26 12 94 a8 7e c4 4b 07 2c 1a 2c 91 67 19 0b 9b 06 8f a7 b6 6d 5d 1a 29 d5 2e 9e 4a d2 bb Data Ascii: eDS=v2cx=('gIT:~.2b%Qru(wK-6ihLI*)iS[e"22|)YLF`R-1?;C{)A3iSR+XYKQBNJ-m[c$gTrjLZLe%8m_RP &~K,,gm]).J
2021-10-29 15:22:59 UTC	36	IN	Data Raw: 0d 34 fa 14 b4 41 b9 ea 70 d8 59 82 b7 e6 2d 4e 86 62 45 74 3e e4 a5 ba d4 84 25 e8 8a 8a 50 c1 6c 7b 4a 6f 5c 69 2a 53 4d 26 8c 54 a1 53 16 89 44 1c 26 5b 80 e0 07 b1 6c cd 9e 0b b3 e5 aa 4a 6a 64 2c 8a a5 4a 20 25 53 b5 24 38 67 bb a8 7c 23 51 76 8a 4d 59 66 af a6 eb 1f 7b ca a9 57 6c 56 55 ba 35 d0 ea dd 97 71 d9 08 05 49 4b 77 4c 83 e6 c8 ad 5b ec b6 a2 94 de 04 19 b4 c8 49 f2 ee b6 67 45 f8 9b 87 a3 53 2b ac 01 68 50 49 00 3a 4a 99 4a 36 77 19 9f 2c ef 78 53 3b 09 29 23 11 56 a2 e1 3b c3 de c3 2e 42 1e 8c 3e dc d4 a2 62 15 19 c6 e4 30 c9 6d e8 09 08 86 f3 45 86 83 2f 47 f2 d6 f3 4a 6d f6 82 1f 4a da 71 6d 2d 4b 52 db 3e 5a 92 04 ac 65 73 31 1c f2 2f cb 8e 4f c1 b8 67 02 96 02 52 01 20 9e ed 7d fd a0 95 56 2e e6 d5 94 e4 80 54 01 c9 dc 78 52 49 e7 f8 Data Ascii: 4ApY-NbEt>%Pl{Jo\i*SM&TSD&[lJjd,J %S$8g|#QvMYf{WlVU5qIKwL[IgES+hPI:JJ6w,xS;)#V;.B>b0mE/G JmJqm-KR>Zes1/OgR }V.TxRI
2021-10-29 15:22:59 UTC	38	IN	Data Raw: 5e fc e1 8c 77 1f 03 03 25 28 db b8 23 76 07 19 c9 07 8c f0 9c 27 e8 12 06 4f b8 e4 74 29 8a 04 58 83 8b 36 f4 fb fa c3 d2 95 12 ec 4b 70 3d d1 64 3c 22 d7 2a 49 d7 3b 52 82 89 2e 39 48 9d 75 5a 73 64 d3 1d 5a dd 84 a7 e3 4e 6b ca 9c 96 37 00 d4 b8 ce 37 1d c6 24 23 69 49 40 42 bc c4 28 a3 a2 ec aa 0a 75 6d 3a 2a 85 62 c6 9a 89 5f 0b 30 40 13 2e 48 b0 62 45 f8 e7 94 44 da 75 33 7f bb 6b 25 61 60 64 af 0b 83 7c 8b 0e 36 f7 94 6d cb eb 92 ed e6 ea 37 e5 b4 d3 92 d2 40 09 4e 10 99 ef 01 c9 0b 00 15 97 54 a0 12 94 ac 60 76 4e 7a f4 82 16 16 a4 bb 8d 06 65 9f 3d 5b 78 3a 9d d1 e7 c7 17 54 0a 94 92 9c 29 01 9a c4 4b 00 83 c4 1b 1e 31 19 ea fd 4d 0d ea 1b 70 24 2b 6b 30 2f 0d 24 71 8d 8d ac ec 53 d5 86 de 70 7a 41 01 1b 20 36 12 36 90 95 25 47 79 c8 4a 41 30 9b Data Ascii: ^w%(#v'Ot)X6Kp=d<"*I;R.9HuZsdZNk77$#iI@B(um:*b_0@.HbEDu3k%a`d\|6m7@NT`vNze=[x:T)K1Mp$+k0/ $qSpzA 66%GyJA0
2021-10-29 15:22:59 UTC	39	IN	Data Raw: 3f f8 88 73 ca 28 69 0b 75 c2 96 d0 d2 4b 8b 71 64 25 08 42 12 56 b7 16 a3 80 10 80 37 28 9c e1 20 e3 e5 d1 56 4a 4a a6 5c a5 09 2a 27 40 03 1b 9d 06 7f cc 46 42 7e 14 00 54 b9 b3 42 12 00 75 12 48 00 0e 27 97 38 e2 4f ed 36 f1 c3 5b f1 29 e2 46 e4 b3 29 12 54 bd 23 d2 ca d4 9b 6e d4 a6 a2 6a 99 83 3e 55 37 31 eb 17 5c a4 b5 e8 7e 54 e9 c9 79 a8 cf 28 2b c8 a7 b4 cb 68 ff 00 8e f2 ba f2 1e 94 54 d4 6d 15 ac cb 98 51 5c 37 31 e0 66 cb d9 bd 14 4f e6 e6 c9 97 33 69 d7 cb c7 36 64 e0 3f 42 95 49 0d f1 7c 2a c6 14 73 b0 20 e6 5a 28 2d 47 51 e2 34 98 11 5b 84 99 32 5b 43 ca 69 a6 de 53 5b e3 84 32 1a 71 6d 25 05 48 09 52 48 23 25 c7 81 da 94 80 02 95 83 a7 d9 13 a6 89 a9 98 54 64 82 9c 65 8f 68 e2 c8 13 a8 62 4f 0c e3 ec Data Ascii: ?s(iuKqd%BV7(VJJ*@FB~TBuH'8O6[)F)T#nj>U71\~Ty(+hTmQ&nnfO3i6d?BI|*s Z(-GQ4[2[CiS[2qm%H RH#%TdehbO
2021-10-29 15:22:59 UTC	40	IN	Data Raw: d4 f7 c9 ff 00 4d 67 7f 11 a6 a6 20 aa b5 11 c0 df 08 51 c2 54 a3 82 55 8e c0 61 44 9e f9 c1 00 28 00 3e 78 1d 06 95 4c 41 e4 3b af ea 3f 9d 61 d3 ae 4f 1c 51 06 3f 65 6b 61 b0 89 36 a4 57 62 cc 8d 4d ab d4 17 36 d2 12 1a 6a 1c 54 a6 35 3d d5 b9 68 21 ef 25 8a 43 ef c8 95 22 54 8a 33 b2 51 43 96 a5 ad 30 9a a1 3e e3 92 a4 dc 25 48 52 5c 7c 47 3e 7d fb 87 77 38 af 21 65 56 ee bf cb db c2 e3 6d c6 ac c0 6e 6d 3d 7f 10 c3 85 c4 93 b1 c6 5d 61 e6 55 e5 bf 12 64 69 01 12 21 cb 8a b5 f9 72 61 cc 6a 3c 88 ee 82 87 10 93 8c 91 1f 10 ef f4 30 f5 02 13 7c f0 fb f3 88 d2 e1 a1 4c 1e 66 1a 74 85 85 9f 41 28 3c 64 f0 46 3b 01 f4 f9 83 d4 d4 61 c5 2c ab 4b 8f 0d 4c 46 52 4a 92 5b 30 3c 22 5c f0 cd 6b 4e 91 6f 6b f4 16 16 da 71 12 6a fa 49 73 c3 61 b7 5f 5b 25 d7 1c 4b 41 a4 Data Ascii: Mg QTUaD(>xLA;?aOQ?ea6]M6jT5=h!%C"T3QC0>%HR|G>}w8!eVmnm=]aUdi!raj<0|LftA(<dF;a,KLFRJ[0< "\kNokqjIsa_[%KA
2021-10-29 15:22:59 UTC	41	IN	Data Raw: 21 55 62 84 1c e3 01 3c 83 8c 7a b2 08 d7 4f 28 2d 43 b1 63 77 96 a3 e2 70 b3 db 37 22 0a 26 2d 83 2c 91 a4 6a df d9 9e 7e 2b 57 f4 a9 f4 54 68 75 34 4a ba a6 b7 f1 74 44 25 11 17 f0 8f 3f 23 63 7e 5c f9 a9 f4 2a 36 1e da e2 92 83 94 86 9a 3e 91 63 b2 a4 a5 35 32 ca 59 b1 0c 93 84 78 11 7f 38 83 b4 a6 93 4b 37 11 27 b2 4f bf 7b e3 a2 4a bd d3 6b 5b d7 a3 51 ae 4b 96 db b7 de a8 04 b1 49 66 bb 5b a5 52 65 d5 9f 35 49 6c ba c4 06 aa 13 18 76 a0 b4 39 e4 02 d4 56 df 53 6b 7d 1e ef 23 76 ca 6c c9 68 9c cb 56 10 a0 c2 f9 dc 1d e3 74 63 25 a1 73 29 55 d5 a3 11 c6 a2 6c ec 09 f9 fa f9 47 37 c5 c7 6c d4 b5 aa b5 6c c7 b9 2d c9 37 1c 3b 9b 4d 5f 93 6d b5 5c a5 3b 70 44 62 1b 15 19 ca 91 26 86 89 8a aa c6 61 b4 2e 3b 85 f7 e2 21 94 a6 43 2b 0b da eb 7b 85 32 64 9e Data Ascii: !Ub<zO(-Ccwp7"&-,j~+WThu4JtD%?#c~*6>c52Yx8K7'O{Jk[QKIf[Re5llv9VSk}#vlhVtc%s)UlG7ll-7;M_ m\;pDb&a.;!C+{2d

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	43	IN	Data Raw: 6f 09 38 51 4e 00 c1 0a ca 78 39 3f 87 d2 77 0c 11 c1 51 27 1e 56 73 99 29 4e a7 3d 07 bd 7d e7 11 d6 a2 0e f2 7d 8f 7a c5 a4 d3 46 f1 62 51 89 c9 2a 55 4d 79 f4 8c ee aa cc 1d 92 0f 39 07 3c 83 cf b6 7a d0 52 ff 00 c2 f7 a7 d2 28 67 ff 00 c5 1e 5f 2c 8f 8c 32 7c 42 d4 e4 50 74 2f 59 eb 71 5c 5b 72 69 5a 59 7f 54 18 75 a2 7c d6 9e 8b 6d 54 9d 42 db c6 55 bd 3b 37 0d b9 50 23 39 1c 60 1b 41 6b 97 45 58 65 d8 9a 75 01 71 fd 3c f9 1e 3c 2f 13 36 2a 71 ed ad 9d 2d b1 e3 ab 96 42 73 c9 40 5f 76 4e fc 8c 7f 37 76 ef 48 75 dd 46 a9 55 6b 0c b4 d2 eb f4 c5 d0 96 b6 d2 98 e8 83 56 61 8d b4 fa 91 42 30 95 2a 53 8d 30 dc e5 b8 95 2d d0 eb ce ad 5b c9 3d 79 2c 89 33 57 4a d3 9f 12 16 b9 c9 7b d9 4a 29 df 6b 8f 9c 7d 74 36 99 a1 ac a6 02 5f 50 17 4d 2a 95 92 19 ff 00 Data Ascii: o8QNx9?wQ'Vs)N=}}zFbQ*UMy9<zR(g_,2|BPt/Yq\[riZYTu|mTBU;7P#9`AkEXeuq<</6*q-Bs@_vN7vHuFUkVaB0*S0-[=y,3WJ{J)k}t6_PM*
2021-10-29 15:22:59 UTC	44	IN	Data Raw: c4 1f ca d0 30 b1 93 3e ed a6 34 5f c7 c5 f9 c0 29 e6 ff 00 bc 54 df fe 6d 39 73 bc cb 58 d6 da de 22 99 b4 64 ad 03 28 ca 95 93 db 20 0c f1 9e 47 1c 1c 8f f3 1d 57 80 f6 11 2e 62 f7 e8 48 de 5f df f3 11 7d fb 6c d6 d5 4e a7 3f 6f 98 6e 4a 81 51 a8 cb 91 4d 9e 94 a6 15 56 33 90 e9 6d 98 ee cd 69 a7 e6 52 5c 6f 6a 97 1a 7b 11 a6 47 69 c5 62 7c 37 63 b8 a7 98 9a 9e c2 10 4b ea 38 d8 f9 38 88 66 f3 09 f6 df c9 88 de 9b 12 35 4d f9 55 0a 2e fa 35 cd 08 30 cd 72 89 57 6b c9 79 69 53 6a 54 38 b7 0d 3d 97 24 07 5b 5b 29 26 8b 73 53 9c 98 7e 19 bd d4 c9 f5 2a 61 9b 4c 93 29 13 55 62 91 6b 39 e7 7c f9 0b 70 b1 dd 04 60 c4 bb 11 e7 dd f3 fb c2 bb b1 e2 55 1b 70 08 e6 25 46 20 40 9d 4d 7b 62 df 8c 5e dc 86 9d 0b 69 4b 6a 5c 37 d4 d3 bf 0b 50 8c 54 cc af 2d c4 14 b5 Data Ascii: 0>4_)Tm9sX"d(GW.bH_}lN?onJQMV3miR\oj{Gib|7cK88f5MU.50rWkyiSjT8=$[])&sS~*aL)Ubk9|p`Up%F@M{b^iKj\\7PT-
2021-10-29 15:22:59 UTC	45	IN	Data Raw: a3 da f1 c3 0e 53 74 7b 4c 23 51 2d 19 0d b0 ca 24 c1 b8 26 f8 91 a7 d1 ae f9 ad ca 2d 25 6a 93 25 ea 7a 29 bb 24 17 db 61 98 6e 3d 11 4d b9 25 4e 29 bb 5a 7c c5 6d 6a 14 4b 53 04 ce 49 50 26 c4 11 ae f1 c3 2b 6e 78 66 cd 91 29 14 53 97 31 24 e3 a5 24 30 c8 ea 01 16 cb 22 5d 98 e5 03 f8 95 ba 2b d6 6f db 7d e1 de a1 6c b5 0d 9a 8d c9 aa 16 55 85 72 d4 e4 c2 6e 7a a6 db b7 ae 9b d3 29 77 34 24 89 04 aa 3c f9 30 83 8e c7 a8 31 e5 3f 01 d4 36 b8 cb 0d 97 19 51 26 29 69 db 67 1a c5 a5 c9 ec bb 0b cb fe 9d 39 8e 2f a0 86 00 8f ee 75 14 a5 88 5d 43 16 c9 96 48 f0 c9 b9 5a 3a 4d 8c df 2a 23 b1 e7 18 1f 21 8c 8e c1 5e c4 a4 03 9c f0 09 c0 d4 28 12 a4 ab 3e cb f1 3d 9e 43 d7 e7 19 94 dd 0a 7b fe a9 1f fc d9 72 e1 08 b5 26 f7 c9 64 10 33 c7 b7 ab 6f b9 19 29 f6 ef Data Ascii: St{L#Q-$&-%j%z)$an=M%N)Z|mjKSIP&+nxf)S1$$0"]+o}lUrnz)w4$<01?6Q&)ig9/u]CHZ:M*#!^(>=C{r&d3o)
2021-10-29 15:22:59 UTC	46	IN	Data Raw: 73 cf 1b 48 ff 00 ea a4 ec 9e 14 46 33 82 78 dc 79 27 19 20 5e 53 0f d2 5d b2 16 f1 f6 22 8a 75 ea 17 fe 93 e9 02 5e 56 f4 5b ba d7 b9 ed 59 c9 4b 90 ae 6b 7e b5 6f cc 0b 01 4d 98 f5 9a 74 9a 73 e9 52 73 ea 49 4c 85 15 0c 02 47 61 9e 83 3d 1d 64 89 f2 6c f3 01 f0 66 cc b8 f7 ba 09 43 32 6c 9a ca 94 ab 0a 69 a7 26 73 eb 84 2b 53 9e 9b ed c3 38 fe 68 fa 95 a5 37 06 96 eb 76 a4 59 b7 4c 62 d3 96 15 f3 59 a1 4a 86 b6 d6 d4 89 66 93 54 79 0d 90 55 b0 86 e4 b2 88 cf 36 a4 a8 85 34 b0 a4 e5 2a e7 c9 36 a6 2a 49 ea 02 a7 a9 28 38 30 31 2e e5 dc 8d c1 ec 3c 6f 78 fa 81 33 a7 56 d3 6c ed a2 1a 74 89 d2 e5 92 94 f6 88 58 0c 48 2d bb be 2a 9e a5 55 2b b4 3b 9a b7 05 11 d3 01 4c cc 71 c8 cb 6d 28 ca 22 4b fd fb 25 20 80 ad a1 0e a5 29 da 72 47 24 a4 80 3a d4 6c 9a Data Ascii: sHF3xy' ^S]"u^V[YKk~oMtsRsILGa=dlfC2lJi&s+S8h7vYLbYJfTyU64*6*I(801.<ox3VltXH-*U+;Lqm("K%)rG$:l
2021-10-29 15:22:59 UTC	48	IN	Data Raw: f0 ba ed 51 58 c6 71 c8 23 bf 3d be bd 48 aa 43 d1 52 76 1d 49 93 50 dc 1a 62 3e 5e ba bb c0 e4 ce 4f 5f 50 a2 2d d7 48 d6 df e1 cc d7 4d fc 43 0d 62 3b 93 4c cf a7 60 00 e4 76 7b fd 0f 20 fc c6 3b 8e ab 24 ca 66 24 5e ce fb f8 b5 86 e0 de b1 35 73 4a b2 7c cf be 3d fe b0 dd b8 29 cd 43 fb a5 2f 4c a2 c7 8c fc ca 80 72 6d 4a a6 cd 2d 10 cb 50 62 bc 95 19 2f 84 f9 6b 50 6d 41 2b 41 c0 dc 94 bc d3 ad 29 43 a9 33 24 99 88 48 4c c9 28 6b b2 d6 a4 9e f1 84 fa dc 6f 26 06 85 f6 94 fd a2 e3 4d e0 30 b1 f7 ca 23 0b c6 c4 a3 56 84 4a a5 2a b5 4c 5d 56 03 2e 39 4c b9 2d 3a bd 2e 7b d0 1a 94 fa 83 d1 9f 72 23 92 22 a6 9d 3e 4c 75 aa 4c 0a ab 0f 50 ab 0e 31 e7 98 f1 e6 b1 1a 64 77 01 d4 29 32 fa c9 6b c4 02 8f 56 71 31 dc ec 2e 77 71 b6 b0 4c 6e 92 42 58 82 d7 71 Data Ascii: QXq#=HCRvlPb>^O_P-HMCb;L`v{ ;f^5sJ|=)C/LrmJ-Pb/kPmA+A)C3$HL(ko&M0#VJ*L]V.9L-:.{r#">LuLP1dw)2kVq1.wqLnBXq
2021-10-29 15:22:59 UTC	49	IN	Data Raw: 5a e4 28 26 65 5e 43 0f 6f 5c f9 6b d9 21 a9 08 4f 9c a0 84 27 08 c1 e5 51 49 96 06 04 04 90 18 31 2c 01 b3 00 4f b7 80 cc ac 9b 33 1f 59 34 a8 4c 48 0a 0d 98 19 3b 0f 7a c3 39 1e 06 7c 2e 4b d5 09 9a c6 f6 97 c6 73 52 aa eb 90 ed 4e ed 17 25 e1 f1 d2 8c 8b a9 77 d3 c1 51 d3 70 0a 62 10 e5 d2 a5 d5 fc a6 e0 b4 d3 6e a8 c7 43 62 20 f8 7e 82 bd 91 4d 36 70 9f 31 09 13 10 42 84 c5 15 03 88 6b 62 d6 e4 c7 7c 21 b4 aa a4 cb 12 e5 cc 51 41 18 30 61 4b 04 ea 2e 97 be 4f 73 6b 42 5d eb e0 d7 c3 dd e1 ac f4 1f 11 35 fb 19 f9 fa c1 6a 57 69 77 2d 02 ed 37 45 dc c1 a7 d6 68 b0 51 4c a7 4d 4d 0d 8a e3 56 e4 83 1e 13 69 64 b3 26 90 e4 57 d2 01 90 d3 ae 15 2c 06 66 ca a7 15 5f 9c 0c a9 b6 4e 27 56 40 32 75 6b 0c 98 5e 08 36 95 4a a9 ff 00 2a ea 44 a2 4a b0 00 96 b9 75 Data Ascii: Z(&e^Co\k!O'QI1,O3Y4LH;z9].KsRN%wQpbnCb ~M6p1Bkb|!QA0aK.OskB]5jWiw-7EhQLMMVid&W,f_N'V@2uk^6J*DJu
2021-10-29 15:22:59 UTC	50	IN	Data Raw: 48 90 0c d9 c9 42 4b 5a e3 9b 3b b8 ef dd ba 13 a8 31 53 7e 5a 14 6b bd 9a 42 a8 eb af aa 7a 7e ef 54 85 4c 2c 7c 05 66 a1 49 5e d9 1f 0d 10 48 f3 7e 01 4f 03 e4 23 67 9e 10 5c 52 9b 2e b8 c9 2d 52 9e b4 24 a4 12 59 c6 60 35 f3 02 ef ae e3 0e 9e a3 22 69 96 6f a8 2d 7f 0e 1c 62 35 d4 98 14 ca 05 3b 33 5f 61 a4 8f c6 a7 56 90 90 84 e5 58 52 d7 c0 e0 04 a8 f7 da 42 48 39 e8 b3 25 04 e1 bb 9b d8 68 78 0e 1e 5c e1 4b 9b 65 1e 01 9e db f2 e3 f3 31 57 74 93 5a 2c c6 3c 4e 69 0d a3 4b 9b 1a 5d 42 af a8 14 58 2c 08 eb 4a 9b 6d c0 97 9f 5b 8e 14 9c e1 b6 d9 3c 84 b8 01 ee 13 c8 ea 45 34 b5 09 89 5e 45 2e 47 02 d6 3e 7b 9b 48 8f 51 31 2b 96 b9 6c e9 58 c2 a7 c8 a4 e6 3b f8 69 1b 72 a7 9c 79 b2 52 48 42 92 e0 da 42 54 78 20 79 61 78 da b2 94 a9 05 69 71 29 c2 5b dc Data Ascii: HBKZ;1S~ZkBz~TL,|fI^H~O#g\R.-R$Y`5"io-b5;3_aVXRBH9%hx\Ke1WtZ,<NiK]BX,Jm[<E4^E.G>{HQ1+lX;iryRHBBTx yaxiq)[
2021-10-29 15:22:59 UTC	52	IN	Data Raw: 3c 67 1d fe 29 7b 94 a2 a8 92 aa cc b6 0c 99 9f e9 7c ae e7 5f 26 3c a2 4c ca 3c 4e a9 6e 90 6f db cb 5b 68 7c b9 b6 71 64 6d 4b d2 cb bc 3c b6 a9 75 66 9a a8 2b bd 2a a6 05 3e a5 b8 f2 a6 da 6d e3 e4 4b 23 82 4c 17 e5 63 b1 c1 1d 5a c9 9f 26 76 aa 47 fa 9b 87 b3 7e e6 8a 85 cb 9b 2d 0d 22 dc fe 8e d8 c4 96 cd 1d a0 af de 25 49 c7 07 8c 73 83 8f 60 7e b8 23 9f 7c 03 d4 e4 c9 60 e2 e3 45 68 7e 59 81 bf 3c cc 47 eb 58 b1 17 f0 1e f4 e7 01 2e d0 64 56 51 5a 62 a0 1b 69 b8 0b 8d 32 23 91 cb a5 e6 c1 42 d2 5a c0 43 89 70 14 fa 0a 1d fc 47 d4 92 9c 0e b9 d4 24 af 11 7c 80 b1 cf 3f a9 ee 68 7f 5c 70 14 86 cd ed 7c c7 db d8 b4 3a 65 c1 b0 63 c6 99 32 87 56 b9 66 cf 45 36 e8 a7 35 12 55 bd 32 3b 45 ea ad ab 5e a3 a1 a5 b8 60 a0 a0 89 b5 08 ed 05 6f d8 95 2c 29 e5 Data Ascii: <g){|_&<L<Nno[h]qdmK<uf+*>mK#LcZ&vG~-"%ls`~#|`Eh~Y<GX.dVQZbi2#BZCpG$|?h\p|:ec2VfE65U2;E^`o,)
2021-10-29 15:22:59 UTC	53	IN	Data Raw: 78 1b 83 2b 6f 57 53 5f 10 58 17 ed 15 1b f7 1f 63 58 bc 9f d1 6d 99 59 d9 13 12 92 77 06 df bc 00 1b 5b f0 78 7c 5b 5a a0 6b d2 52 a7 94 fc 19 1e 61 c3 4f 1c 24 9e 14 3c 89 0d 84 a9 b5 00 4f 96 4e ed be 95 79 84 1c 8d 1e cb e9 08 aa 5a 13 35 40 12 c1 77 b3 9c d9 ce f7 23 33 9e b1 8b db fd 0e a8 a1 96 a9 94 58 66 24 3a bb 59 61 1a 80 96 cf 7e a5 f2 d6 68 bc 7c 51 d9 3a 31 6c d2 1e d4 ef da 44 d3 6b 32 9e 66 99 5b a1 db 35 4b 85 b3 2d 86 55 23 e0 67 aa 94 cb e2 34 d7 a3 a5 e7 62 b4 e2 5b 72 63 6c 3c 59 f3 5c 65 d0 74 d5 7b 5e 9a 82 4e 3a 81 37 01 01 58 d0 82 a0 cd 6b 8d 6d 71 18 6a 6d 97 55 5b 3b ab a7 54 93 31 24 24 a1 53 02 55 88 1b d8 e9 bb 52 22 12 7f ed 2c f0 98 f3 05 4a bb ef 18 ed 94 f0 e3 da 69 7b ed 20 e3 9c 35 47 75 5b 7d 43 2a 1c 60 85 0c 8e 4d Data Ascii: x+oWS_XcXmYw[x|[ZkRaO$<ONyZ5@w#3Xf$:Ya~h]Q:1lDk2f[5K-U#g4b[rcl<Y\et{^N:7XkmqjmU[;T1$$SUR",Ji{ 5Gu[}C*`M

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	54	IN	Data Raw: 57 66 2c 12 8a da 73 a9 29 98 4f 37 09 2e da bb e9 08 6c bd a4 9c e8 27 a1 98 76 a5 04 f7 64 79 bd b2 cb 43 25 d8 de 21 bc 3b 33 22 2b 8e eb e6 8a 84 34 d0 73 1f ed 56 c2 56 e5 25 b2 50 31 fb 42 49 5e 40 05 38 cf 7f 90 ea 30 da 14 45 6e 9a b9 2a b1 ec 82 49 3c 9c b1 ef 1f 50 59 94 35 c2 4a 81 a4 9c 90 e9 01 58 01 01 ec 5d 92 48 b5 bb dd e2 2b d4 ad 69 d2 8a ec 89 0e d2 b5 67 4c aa 09 71 4e a8 18 7a 85 67 49 04 13 94 e3 ca ac ac 91 8c 0e 01 ed 9c e4 f5 5b f9 99 2a 9a a6 9a 92 0d f3 0d c3 88 77 7f 93 c5 92 64 d4 a2 48 49 42 9c 58 f6 43 b7 85 83 77 98 a6 f7 3d ed 6a 4a 5b df 0f 79 da 32 52 49 4f ee 2e ab 7d fe 41 3d 82 27 ab 77 e8 73 80 49 cf 6e a4 26 6c 93 9a d0 38 39 fa c0 c4 b9 c3 fe 5c cf 0f aa 4c 57 eb 9a e2 b7 5d 0e 36 dd 7e df 75 67 2a da dd 6a 90 bc Data Ascii: Wf,s)O7.l'vdyC%!;3"+4sVV%P1BI^@80En*I<PY5JX]H+igLqNzgI[*wdHIBXCw=jJ[y2RIO.}A='wsIn&l89\LW]6~ug*j
2021-10-29 15:22:59 UTC	55	IN	Data Raw: 97 ab 13 41 5c b4 e0 00 bb 72 e3 dd f5 68 d6 53 74 ab 66 54 53 61 33 91 2d 40 a5 92 5c 4d 77 19 68 c0 67 67 61 ba 32 e6 e5 d1 3d 55 b4 2a 8e d2 2e 3b 0a f0 a0 cc 8a b7 1b 72 9d 5a b7 6b 11 64 30 a6 9d 58 5a 4b 12 61 a5 d4 e1 2b 08 3b 10 50 a0 70 92 a4 84 ab ae cb aa 54 95 2d 06 59 04 f6 43 82 46 67 3e f3 ef 28 d6 d3 6d 6a 6a 89 12 fa aa b9 09 b0 73 31 41 ee 34 e3 9e 6d dc 4c 7a a5 69 d5 e7 54 a8 42 a6 c2 b5 ab 0e cc 77 cf 75 6c 39 4b 92 d3 e4 34 86 8a 1d 63 73 29 42 63 b6 85 24 15 bc 0b 6d e4 17 94 80 77 01 a6 a9 38 97 06 a5 7d 97 c4 99 59 2c 03 7c 40 82 6f cc 16 66 2e 6f a4 d9 bb 52 8a 57 66 a6 be 4a 05 ae 95 24 2b 3b d8 96 c8 f9 be 91 30 2e ee a2 d8 31 05 1e ee ad 46 a5 d4 23 bc 96 9f 83 1d 2f 55 1d 6e 40 69 48 50 90 d3 0a 54 76 9d 42 58 c2 d6 14 16 37 Data Ascii: A\rhStfTSa3-@\Mwhgga2=U*.;rZkd0XZKa+;PpT-YCFg>(mjjs1A4mLziTBwuI9K4cs)Bc$mw8}Y,\|@of.oRWfJ$+;0.1F#/Un@iHPTvBX7
2021-10-29 15:22:59 UTC	56	IN	Data Raw: f5 15 c4 28 0a 84 29 39 5d 25 85 fc ed ef 74 29 94 c1 63 b3 86 63 e8 39 5b f9 bd f9 46 81 69 66 bc 54 26 d3 98 9d 67 5e 94 8b fe dc 43 68 57 c3 39 50 4d 61 2c 34 08 1b 04 84 bb f7 b5 31 48 57 ee d2 cb 8e 06 50 72 3c 82 90 01 b8 a6 ad 60 92 89 98 d0 d6 4b f6 82 73 bf bf 10 d1 59 3e 8a 5f 6d 38 30 28 58 b8 7e 59 37 0b 1b 68 d1 6c 6d 6d 65 b3 e6 6b 66 1d 61 12 2d 8a 83 a0 27 6c d2 a9 74 a5 39 c6 12 8a 9b 08 42 98 05 58 c1 9f 16 2b 29 27 0a 7c 91 b8 db ca ad 96 af f1 01 41 b6 64 5f c0 73 7c b2 8a a9 94 53 42 bf 48 85 01 77 63 9d ec 3c 39 44 c7 0e 13 12 d9 4c 88 8e 33 21 87 d6 a5 b3 22 3b 8d 3e cb e8 51 c8 5b 6f 32 a5 b4 b4 93 d8 a1 44 63 18 51 cf 16 08 12 66 5d 3d bd ed 98 dd ee fe 0d 11 71 4e 4e 34 cc 49 4e 4c 74 f0 f4 77 e5 06 dc a2 2d 5b 42 10 9f c8 91 8f Data Ascii: ()9]%t)cc9[FifT&g^ChW9PMa,41HWPr<`KsY>_m80(X~Y7hlmmekfa-'It9BX+)'|Ad_s|SBHwc<9DL3!";>Q[o2DcQf]=qNN4INLtw-[B
2021-10-29 15:22:59 UTC	57	IN	Data Raw: f1 e1 00 35 0e 91 51 4d 2d 2b 4f 63 12 7a b5 24 a1 4a 6e c1 27 b2 14 35 0d 9f 38 fb 7d 6b d5 a1 a5 51 68 0e d5 69 57 fd 79 ca ad 31 55 c9 0f 59 f6 dc ba f4 2a 3c 56 d0 65 3a e4 d7 d0 fb 28 71 d4 32 85 3a dc 58 cd 4b 98 e0 4e 50 d8 71 c4 f5 15 09 26 50 14 82 67 58 e1 4a 56 05 76 42 ae 90 35 50 56 56 c9 ef ac 4e 9c 92 15 3b f3 c3 04 b1 2d 68 28 b1 51 22 d6 40 b8 04 97 73 90 72 43 08 bc 7a 79 59 b3 3c 4b e8 32 8b 12 be fa b7 ae 8a 53 bf 01 50 76 3b b1 64 a6 4c 55 0f 82 9a d3 73 58 53 d1 6a 30 df 4c 77 c3 85 97 43 6f 25 c5 1f 88 42 94 a7 3d 1f 65 2d 1b 57 65 fe 5a ad 05 5d 5a 8c 95 05 95 a5 78 c2 49 27 88 00 16 e3 70 5f 2f 11 db b4 9f dc db 61 73 a8 89 46 32 89 89 29 08 52 59 61 ef 99 4a ae c5 25 f7 da 39 12 d7 bd 45 d5 dd 3a d4 7b b3 4f a5 5e 0e 29 76 c5 cb Data Ascii: 5QM-+Ocz$Jn'58]kQhiWy1UY*<Ve:(q2:XKNPq&PgXJVvB5PVVN;-h(Q"@srCzyY<K2SPv;dLUsXSj0LwCo%B=e-WeZ]ZxI'p_/asF2)RYaJ%9E:{O^)v
2021-10-29 15:22:59 UTC	59	IN	Data Raw: e4 f9 76 fd b2 b0 30 e9 49 8f 5a 52 65 6d 21 e0 da 56 67 b9 b9 bf 39 4b 7c 34 92 af 88 52 88 56 12 da 94 3d 0d 1f 87 14 b2 52 12 8d a1 5c a0 94 b8 23 aa 49 20 f6 be 1c 83 65 6d 44 61 d7 d3 aa d9 e4 ae 6d 15 2a 94 a3 72 71 a4 da d7 c3 6b 0f 6f 0d 1a be b0 d4 aa a9 44 89 b4 6a 64 48 e1 43 e1 63 b6 b7 d7 26 5b 4f 7f c3 f2 b7 ad 45 c5 3a 84 27 d6 a4 21 a6 b2 a2 ea 88 2d b4 bb 9d 9d d0 d9 34 77 35 13 e6 80 a0 42 a7 25 25 98 65 6d 3b 2e 3c f8 d6 55 f4 a6 7d 40 c3 f9 69 52 9c 10 7a a5 29 8d f3 2f ae e3 9e f8 44 6a bd 3e aa 40 76 8b 4f 64 a7 ce 52 a2 a1 c7 94 ec 74 7a 94 df c5 c8 53 45 96 99 2e 63 fd e4 30 e2 9f 09 71 0c c7 79 69 3b b5 f4 f4 fd 5a 53 2e 5e 15 01 ae 1c 2f 95 9c 5f d7 7b 65 19 c9 f5 7d 61 2b 56 31 ff 00 53 81 dc 6c 34 0f 04 4c 45 cb 7c 46 8d 1d 0f Data Ascii: v0IZRem!Vg9K|4RV=R\#I emDam*rqkoDjdHCc&[OE:'!-4w5B%%em;.<U}@iRz)/Dj>@vOdRtzSE.c0qyi;ZS.^/_{e}a+V1Sl4LE|F
2021-10-29 15:22:59 UTC	60	IN	Data Raw: 09 00 06 5a 5a db dd fc 5b 97 08 da b5 47 52 47 cf 71 00 80 4e 41 46 d5 1e 3b e3 d5 ca 54 41 28 dc 52 01 49 1d 6c 59 d0 00 b5 83 f1 f7 e6 7b e3 2a 49 73 de 3b a1 3a 43 6a e7 d1 95 14 a7 24 ef 07 80 02 94 72 14 14 a3 ff 00 30 01 64 e7 2b dd 90 92 24 39 1c 2f e7 0d 8b 29 6b 27 6d ad 42 4f 19 fb aa 2e 49 ee 01 40 57 27 00 e7 24 67 8e d8 ea da 57 61 3c c0 3c ad e7 15 73 7e 27 e2 7c 8f de 0c ba 9f 61 91 df 38 c6 09 f9 f6 fe c6 7e bd 28 19 bf 97 90 68 26 b6 c6 09 f7 fe 11 c6 7b 63 07 1c 11 f5 f9 91 f2 e5 e9 51 01 80 b9 2f c3 41 0b 9e 5e de 0b 2d 18 c6 79 c9 c7 07 9e 7d c7 6e 46 7d 23 39 e9 e9 c6 92 ee 3c fd 32 87 0c 20 10 31 25 f7 37 77 be e8 24 f2 70 90 41 ed 9c 9e e7 f5 e7 93 dc f7 fc bd ba 5d af f2 f0 04 38 dd 7e ee 06 1a 9e ce 83 82 83 85 8f 96 f7 df c3 48 Data Ascii: ZZ[GRGqNAF;TA(RIIY{*Is;:Cj$r0d+$9/)k'mBO.I@W'$gWa<<s~'|a8~(h&{cQ/A^-y}nF}#9<2 1%7w$pA]8~H
2021-10-29 15:22:59 UTC	61	IN	Data Raw: 1d 72 57 05 c9 2c 44 59 69 6f 29 a6 5c 4b 6f be d3 0b cb 8b 69 8f 31 a4 3c f2 12 5b 6b cd 6d 2e 29 21 49 cb 55 d5 95 60 07 0a 8d d2 56 30 a5 79 fc 2a 2c 15 7d c7 38 21 54 c3 88 17 64 8b e4 dc 03 8c 89 c8 0c cb 81 ab 40 89 a2 30 90 e2 90 c3 4d 85 91 e6 79 6d a1 05 65 03 09 2b 08 48 2a d8 14 76 93 c0 04 fc f9 04 c4 7e db 12 37 76 87 17 21 db 4c f7 77 c3 53 37 52 e3 82 9c 7f e4 06 f8 4d 7e 8e 09 3e 9e 4f 03 18 3f 2f 7e c6 f7 fc 22 7a 86 64 90 58 84 92 77 67 7e 43 d9 82 99 ac c0 92 09 c8 3f 86 5f 36 8c 4c fb 6c 29 72 1a d3 3d 03 71 b5 be cb 63 53 2b e1 e7 db 42 8b 69 f3 6d 29 0d b4 cb ab f2 d6 da 14 f3 a9 41 6d 0e 60 b9 e5 ad 28 2a 09 58 4e 5b a5 02 a2 54 89 5d 49 53 86 b0 0e d7 d0 c6 bb a2 7d 4c e9 95 29 9a 94 92 72 c6 43 3b 0d e7 2b 46 2a 69 3c 49 95 55 be ec Data Ascii: rW,DYio)\Koi1<[km.)!IU`V0y*,}8!Td@0Myme+H*v~7v!LwS7RM~>O?/~zdXwg~C?_6LI)r=qcS+Bim)Am`(*XN[T]IS}L)rC;+F*i<IU
2021-10-29 15:22:59 UTC	63	IN	Data Raw: f5 9d 6e b3 6c e6 d8 d2 a6 26 d2 6c 7b 8c 47 ba 9f 55 d7 51 7a 0d 26 6b f6 dd d9 6d dd fa 5f 2e 75 f1 16 2d c8 aa e5 5a de b9 ed 8a 9d 14 d5 ca a9 93 69 a2 cf a3 f5 c6 76 d1 a9 4c 2a 65 34 b4 cd 5f 58 d8 82 46 15 04 05 2d 2e 09 04 b9 6c 86 62 33 bd 2a d9 f2 a4 ec ba 79 e6 58 44 c9 a9 42 89 c3 84 a8 b0 05 46 cc 09 3b b7 06 78 83 7c 75 f8 4f d4 ad 58 f1 41 7a d5 6c d4 52 14 d5 f1 56 a3 d6 29 74 a5 3f 21 4f bb 50 91 1d a4 bf 09 c7 19 60 d3 9b 9b 26 73 4f 4d 76 13 d2 d1 3b 6b e1 ef 29 98 2a 41 7a 2e d9 e9 16 c5 d9 95 dd 45 4d 5c b1 3a a5 28 38 52 0a d4 0e 05 a9 45 41 21 e5 a4 25 04 a9 45 80 60 ec e2 33 74 52 66 4d a5 94 e4 b2 41 38 9c 0b 5b cc de c0 3e ba 45 71 4f 81 af 14 36 93 74 e7 6a d6 33 7f 05 7a b3 0a 9d 6e 4c 76 43 31 e2 4e 53 92 5c f8 53 16 a2 b4 Data Ascii: nl&l{GUQz&km_.u-ZivL*e4_XF-.lb3*yXDBF;x|uOXAzlRV)t?!OP`&sOMv;k)*Az.EM\:(8REA!%E`3tRfMA8[>EqO6tj3znLvC1NS\S
2021-10-29 15:22:59 UTC	64	IN	Data Raw: c4 14 54 c1 b0 eb 1a 7a 65 d6 d2 51 25 12 0b a8 86 c4 99 89 dc 55 bf 2c ef 91 25 86 90 d3 3e 08 3c 5d be a7 98 5e 84 df 49 8d 4e 78 53 d7 1d ba 69 65 d6 27 34 16 13 4e 9a 14 b6 7e 11 c3 f0 ca 44 68 ce a9 e5 a7 97 b6 38 90 b4 2e e0 74 87 a3 74 a9 9b 4f fd e9 49 d5 48 28 44 e4 95 01 d4 2e 61 01 12 e6 d8 60 52 88 ec 85 01 78 ad 54 8a b9 93 3a f5 cb 60 a4 85 62 eb 02 82 8b 66 19 46 dd fd f9 41 8a 7f 81 3f 18 f3 2a 4e d3 d1 e1 d6 f9 99 5e 8e 82 f4 0a 69 8d 4d 43 b1 90 88 c2 73 52 de 8e 9a ac 77 9c 94 98 af c1 7d df 3a 30 05 99 0d 3c 94 7c 3a d4 f4 89 5f 9e d9 6b 9e 89 08 a9 48 9d 35 1d 6c b9 01 04 cc 5c b4 a7 11 52 50 d8 94 12 96 59 20 76 50 a4 a8 d8 83 0c 0a 9e 84 03 31 49 48 c4 46 25 cc 42 52 6f a9 24 00 e1 f5 1a f7 c6 17 e6 81 ea ce 93 5c 02 8d a9 d6 a4 4b Data Ascii: TzeQ%U,%><]^INxSie'4N~Dh8.ttOIH(D.a`RxT:`bfFA?*N^iMCsRw}:0<|:_kH5I\RPY vP1IHF%BRo$\K

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	65	IN	Data Raw: 28 05 8e 69 ce d9 e4 32 d6 d0 2a 39 fd 5c f4 cf 5f c4 08 2d cb 78 07 78 d4 6a f9 da 29 35 b5 e0 d9 8a 71 7f 65 21 b6 0e 41 0b f2 12 95 f2 8c 29 45 5b 54 b5 12 76 e7 9e e1 5f 31 9c 82 ba 38 a5 ac 99 80 2c b9 75 64 0e 79 0c e3 58 9e 90 04 8b 2b 09 b6 10 c5 b2 e5 71 a0 03 96 b1 28 41 f0 b9 0a 0c 56 da 30 12 e2 d2 d8 dc 43 5b 79 52 5c df ff 00 37 ba ce e2 40 2a 1f cb a2 8e 8f 01 2f 0e 1e 59 3f 17 f1 f2 b6 71 1d 7b 79 4a 55 d6 73 dc 78 e7 e3 b9 bc e0 cc cf 0e 11 c2 19 40 82 4e cc 2b f0 63 9c 29 3c 9e 32 7d 47 1f 3c 63 1c 8e 9e 36 04 b4 b5 b5 39 ee 61 93 8b df 7e e0 f0 93 b6 96 c7 b5 9d af eb 9f f3 ea 55 3a 28 d5 a2 95 dc 49 82 96 17 4f 88 f2 92 f7 96 15 83 25 0a 86 af f9 55 b9 41 ed a4 ee 18 4e 08 c9 18 e8 c9 d9 32 69 d4 26 a0 0c 41 38 7c 73 d1 f2 bf 8b bc 0d Data Ascii: (i2*9_-xxj)5qe!A)E[Tv_18,udyX+q(AV0C[yR\\7@*/Y?q{yJUsx@N+c)<2}G<c69a~U:(IO%UAN2i&A8|s
2021-10-29 15:22:59 UTC	66	IN	Data Raw: b3 fa 7d 51 d3 ba e5 76 e6 7a d5 ab d8 a8 a7 26 64 aa 95 5d fa 4d 46 d8 6e 0a dd 69 0e cf 54 d9 3f 19 4d 2c b6 87 b7 f9 ed 79 8a 38 48 61 45 f5 33 bf 79 51 53 49 2e 96 a2 75 4d 54 93 4c 94 11 31 4b c2 51 85 ae 00 b9 0a ce f9 9b 41 76 6d 3d 75 4e d0 93 41 b3 e9 aa 2a 6a ea 96 99 54 d2 65 15 09 8b 9a ad 15 2f e2 29 3f b1 4c c0 85 13 ac 63 05 99 f6 80 68 d6 90 dd f7 8d 91 a0 9a 1b 4f 9f 44 a8 5c c6 43 13 67 d6 6a b6 f4 37 56 ca 1b 8b 2e 64 0b 62 2c 69 46 9d 4d 9d 3c 4a a9 31 14 bb 19 59 98 eb af d3 60 3f 22 4b 1d 79 64 ff 00 c4 5a 6d 9a 66 53 6c bd 9e 89 94 a1 67 0c f9 93 14 80 b2 49 7c 29 42 54 a0 35 bb 03 90 c8 c7 d4 fd 0f fe ce b3 3a 51 26 42 36 cf 48 d5 b3 76 a8 47 59 3f 66 53 52 22 aa 6d 3a 09 2c 66 ad 6b 96 14 a7 04 1c 38 98 8b 9b 45 97 b0 3c 73 dc 14 Data Ascii: }Qvz&d]MFniT?M,y8HaE3yQSI.uMTL1KQAvm=uNA*jTe/)?LchOD\\Cgj7V.db,iFM<J1Y`?"KydZmfSlgI|)BT5:Q&B6HvGY?fSR"m:,fk8E<s
2021-10-29 15:22:59 UTC	68	IN	Data Raw: 30 24 25 ce 6c cd de 4f bb 6f 49 34 52 3d 12 55 7e b9 58 d4 1a 84 84 c7 91 51 76 da b2 ef db b7 4c ed 04 43 6d b9 2e c8 62 9f 67 69 65 5a d3 a6 2b cd f2 89 43 49 8a e9 79 65 3e 63 8b 52 d3 b1 8a aa 9d 2d 1d 9a d9 8a c3 a0 2b 4b 97 0c 3b 32 97 c0 67 7b c5 8d 3e cf a6 56 24 fe 46 9d 28 59 75 2c 87 02 ee f8 fa cc f2 cd 03 5c 89 8a 07 74 4b f1 17 49 d5 85 c9 f0 ef e1 8e ab 41 15 ab 95 75 5a 25 7e bf 73 98 4d c8 b4 19 d2 08 a8 4c d9 4f c5 b8 6a 35 fa ec a5 22 6c a7 66 dd 35 49 b5 0a 75 39 69 82 97 a5 c4 86 b5 47 b0 a4 a3 9d 54 84 f5 b8 ff 00 55 1d 62 b1 3a bb 5a 38 58 97 77 d3 32 5d ad 11 eb 6a 29 f6 7a d3 36 58 96 1d 62 50 76 40 c2 4b 76 0c b2 b5 28 6a 71 00 0e a4 bc 6c b4 1b 9a ab aa b6 63 57 b6 bb e8 c5 0e 93 0e c8 d3 9a 4d c6 ab d6 c6 bb 2b f4 1d 4c f2 58 Data Ascii: 0$%lOoI4R=U~XQvLCm.bgieZ+Clye>cR-+K;2g{>V$F(Yu,\\tKIAuZ%~sML(LOj5"lf5Iu9iGTUb:Z8Xw2]j)z6X bPv@Kv(jqlcWM+LX
2021-10-29 15:22:59 UTC	69	IN	Data Raw: d3 48 b2 2d 4b ae 3b 68 96 e3 32 ac fd 44 ab c7 7e 1a ad cb 36 2d 21 4e 4a 54 4b 61 e7 6e aa ac ca 8d 12 eb 6a bf 75 4a 9f 49 4b 11 e6 dd 34 8b 76 86 05 42 0c 88 f0 fd 5b a1 9b 32 66 de a9 97 2a 9b ae 54 bc 6b 57 e5 66 cb 9d 35 32 d5 20 21 91 22 67 50 27 4d 4a 41 0b a8 29 4e 14 4e 5a d0 92 a4 a5 e2 be b6 74 a9 14 bd 74 ee a7 ac 2c 31 4b 72 a5 b9 2c 70 b8 42 01 cb 01 65 16 24 8b 83 12 fd bd 6e 5f 91 b5 36 c8 b5 ac cd 12 11 60 39 0e 75 02 af 12 a7 64 d4 a8 4c 1a 25 1a 97 06 1c 1a 7b ee 4b 83 48 b2 aa 10 27 48 66 00 46 4c 34 bc ba 9d 4a 3c 49 4f d4 ee 2a d3 2a 70 b3 be db 5d 03 db 3b 4e a2 45 24 89 55 92 94 66 0e b1 74 f4 a5 32 d6 89 3d 95 ca 2b 9c 89 48 ea e6 4b 00 28 28 a5 cf c2 f1 53 23 6c 48 09 eb 13 84 28 1b e6 99 8d 95 c3 90 18 ea 82 fe 91 2b 50 28 0a Data Ascii: H-K;h2D~6-!NJTKanjuJIK4vB[2f*TkWf52 !"gP'MJA)NNZtt,1Kr,pBe$n_6`9udL%{KH'HfFL4J<IO**p];NE $Uft2=+HK((S#lH(+P(
2021-10-29 15:22:59 UTC	70	IN	Data Raw: 71 b8 6e 27 be e8 f8 2d c5 2d 78 79 cc 0c 7e 27 96 32 02 4e 70 02 b1 bb 3e e9 00 fb 13 c9 e9 e5 38 45 90 96 3a db 8b f0 f7 6c a1 b8 c6 58 d5 77 6b 97 f6 3e fc 61 bd 21 6a 09 7b f7 aa 52 d0 ad 80 95 2c ed 48 25 3b 70 32 09 c9 1c 27 df b6 07 5d 42 12 a7 b0 b0 75 33 5b 11 b3 ee 73 93 e7 90 8e 15 cc 1b d8 bb 1b dc 0d 7e be 90 d0 97 53 a2 d2 23 54 5f ac 55 a0 44 45 1e 99 1e af 55 44 99 cc a5 da 7d 32 52 e6 c7 81 2e 53 3e 6a 5e 6d aa 84 ba 7d 42 35 39 45 a5 7c 7c b8 52 a1 42 0f 49 65 d6 c1 15 32 4d 3a 3a c9 a4 19 7a 82 a0 c2 f9 9c 98 5b 5b 42 42 26 d4 ab 04 b5 10 a3 70 45 ca ac e4 0b dd 86 ba 71 bc 51 ef 11 ba e3 62 df 5a 67 15 ab 2a e5 52 ec 6b df 47 f5 c3 52 e0 6a bd bd 39 f8 4f d0 e8 9a 54 c7 ec 36 a0 cd 8d 4f 7e 2d 3a ab 0e a9 6a cb b9 a6 46 29 9e e5 3a 6c Data Ascii: qn'--xy~'2Np>8E:lXwk>a!j{R,H%;p2']Bu3[s~S#T_UDEUD}2R.S>j^m}B59E||RBIe2M::z[[BB&pEqQbZg*R kGRj9OT6O~-:jF):l
2021-10-29 15:22:59 UTC	71	IN	Data Raw: 10 7b f4 a1 47 c2 40 e4 9e 94 28 2e b5 1c e7 1d f8 c7 bf 6f 9f fd 3a 24 bd 62 3c 00 48 ef db f3 3f de 7a 24 28 2e b5 77 56 3e 5c 67 f4 e9 42 80 f7 6e c0 c1 07 3f 3f 6f 7f ef e9 d2 85 1e 12 ac 1f d7 1f cc 0e ff 00 21 cf 7f a7 4a 14 7d 27 07 27 82 a0 00 e3 3f 2e ff 00 cb e5 d2 85 1e 73 8e 70 3e 7d 87 b7 bf 6e fd 28 50 1c 95 ff 00 ba 4b 04 f0 62 c8 e7 3f 36 57 c7 1f d3 a6 4c 0e 93 ef 3b 43 4f c4 9e f8 ad 9a c3 18 ff 00 b2 8d 43 21 38 dd 65 dc 2a 0a e0 9e 29 92 88 38 cf 3c a4 1f 6e 7b 91 8e a0 54 a3 fd da 70 cf b0 af fc 4b 0b c5 85 17 f8 f4 ff 00 fc 44 ff 00 e5 1e fc 0c 27 ff 00 a3 9b 65 0b da a4 bd 61 e9 87 98 4f 96 94 06 91 4d a8 bc a2 56 bc a5 bc 00 7f 85 45 47 6b 41 48 f3 02 d2 fd 96 a4 89 52 c1 f8 4d 24 a0 79 05 28 79 7b b4 0f 6b ff 00 89 30 ff 00 f8 d4 Data Ascii: {G@(.o:$b<H?z$(.wV>\\gBn??o!J}'"?.sp>}n(PKb?6WL;COC!8e*)8<n{TpKD'eaOMVEGkAHRM$y(y{k0
2021-10-29 15:22:59 UTC	73	IN	Data Raw: 6d 25 ab 50 ab d6 c4 0a 9d ad 29 89 54 37 cb 8d c4 91 0d 87 e2 b0 b5 47 79 d6 1f da d3 cc c6 75 2a 0f 34 e2 16 56 ca 0f 62 09 07 89 92 f0 b5 b3 6f 2f 7d f0 05 66 79 98 d2 0d 23 61 63 4f 63 15 7a 94 a6 ee b3 93 80 14 7e f0 3e c7 e4 3d bd bb e7 3d 59 4b ff 00 00 00 f2 df e1 cb bb d6 2a aa 3f e2 11 fe af 91 85 3d 33 8a 14 cb 67 81 fb ba 36 46 33 da 44 f4 91 dc 1f 6c fe a7 8c 74 da 11 d8 99 cc 7a b7 3f 1b c1 6b 6d 30 0e 00 72 ec e7 c5 b4 c8 93 16 fb 44 99 09 bd a1 a8 7b 47 9c 0e 47 6d d0 25 0e 3e 5f 8b b7 d3 f9 5f 52 7f 8a dc 1f c2 28 6b ff 00 c1 ef f4 bf ca 2e 9f 57 d1 46 32 1c 87 a4 7e e9 47 61 0a e4 75 f6 28 b5 47 e2 b6 b7 a5 33 4f 96 e4 76 9a 19 71 d7 90 d2 94 d3 68 e0 fa 96 e6 d4 e7 04 8c e5 23 3c 86 ac b2 14 77 24 fa 47 51 79 81 27 22 2f ef dd e3 99 4f b4 Data Ascii: m%P)T7Gyu*4Vbo/}fy#acOcz~>==YK*?=3g6F3Dltz?km0rD{GGm%>__R(k.WF2~Gau(G3Ovqh#<w$GQy'"/O
2021-10-29 15:22:59 UTC	74	IN	Data Raw: 42 89 5e 85 43 fb f6 80 ed 22 fa b8 e5 50 2d 33 67 c4 b7 af 15 16 6e 5a 9d 12 7d 46 91 5b af d1 a3 d2 ea b7 74 c3 19 4d f9 2e d4 99 4d 2b 68 d2 ce a5 d8 93 25 d6 a2 b5 6a 9b 4d 35 74 f5 35 b5 12 50 b4 12 93 3c 75 5d 65 14 e9 7d 67 54 95 c8 0a a7 b4 c2 a9 85 43 05 b5 3c c1 51 4f 3a 5c c9 b8 26 27 fc 27 1d 5a 42 75 ec a4 a8 85 eb 75 a9 0c e4 b3 c5 88 d0 1a cd 0a f6 f1 21 6c 4c b7 24 45 93 4f a7 4b d5 68 ee 33 47 be 64 d5 60 45 81 54 a4 49 92 22 43 b4 24 3c 89 b1 9f 85 57 66 5d 36 ef d4 fa 62 17 06 e5 ba 94 68 13 2b 55 c9 48 f3 63 fa 77 e1 66 cc 45 57 4a e9 36 8a 64 d3 52 a6 84 ed 54 4b a7 93 5e b9 92 64 cb ad 32 e6 04 4b 98 99 52 44 cc 00 e0 9b 33 ab 23 ad 0b 97 da 08 0b 55 7e d8 90 a9 74 00 62 52 89 99 4e 66 95 24 82 95 a5 4b 0a 0b 50 38 5d 88 29 4d bb 37 Data Ascii: B^C"P-3gnZ}F[tM.M+h%jM5t5P<u]e}gTC<QO:\\&"ZBuu!lL$EOKh3Gd`ETI"C$<Wf]6bh+UHcwfEWJ6dRTK^d2 KRD3#U~tbRNf$KP8])M7
2021-10-29 15:22:59 UTC	75	IN	Data Raw: 32 b6 50 99 72 55 91 42 a1 55 ea ee 29 ac c0 80 fc 84 a9 e5 a5 2c 7c 42 5b 22 38 71 6a 3b 42 15 20 b4 95 e7 20 a5 44 24 28 ed 49 8b 56 be a9 06 f9 07 b6 e6 b5 db d7 be 0d 22 59 9a bb 3d f3 e5 96 fb 0f 18 ce eb cb c5 dc 2d 07 a8 f8 91 8f 74 a5 37 5d 0b 49 ed 3b 4b 54 a9 ed ad ad 1e 8e 5c a6 88 26 37 c5 45 09 36 a4 0a cd 5d 9f 2a 18 ad 5f b0 ab 75 48 2f d4 5a 7d 74 e8 75 37 22 45 a7 4d 31 61 53 7a ac a6 aa aa 96 8a 95 17 a8 57 5b 28 a2 5e 1e af 1d 3a 98 a4 e2 b8 3d 5a 89 00 e5 62 62 ca 65 34 a9 ab a6 4a 7f 40 21 13 52 b9 a1 78 dc 87 24 e1 0d 9b 17 0e 03 96 71 19 7c db 57 07 8f bb d6 f4 f1 07 6a 6a dd e3 a1 56 4d df 66 d2 25 5c d4 ca 95 0a 35 cc f4 bd 3e a0 49 a2 a6 81 a4 42 22 42 62 d1 aa b4 d5 c1 bb 2d fa d5 76 1d c1 67 d5 63 4d ac 5c 2e 54 fe f0 62 1d bf 73 c4 Data Ascii: 2PrUBU),|B["8qj;B D$(IV"X=-t7]I;KT\\tjE6]*_uH/Z}tu7"EM1aSzW[(^:=Zbbe4J@!Rx$q|WjjVMf%\5>l"Bb-vgcM\.Tbs

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	76	IN	Data Raw: 7f 2e 94 28 0f a5 0a 3c 15 60 f6 07 1d f9 f9 fc bf 5e fc 7f 2e 94 28 f0 a5 93 ce 48 f9 9c fe 58 e9 42 8f 21 5d f0 7b f0 4f 48 0b db 33 0c c4 ca 63 95 bb a0 37 d7 ba 2b e0 7f f8 87 d2 7d b3 96 96 91 fd 4a 4f e5 9e dc f4 e5 a5 90 77 9c fc 0c 74 fc 49 ef f4 88 27 58 5a 1f ec a7 50 02 4f 02 c9 b8 89 c6 31 c5 32 59 3e dd ce 7f cf 1f 2a fa af f8 49 ff 00 e8 5f fe 26 25 d2 1f f7 89 43 4c 69 ff 00 c8 47 bf 00 f1 d8 7b 4d 2d e5 16 d2 e0 56 99 e9 e8 52 d4 06 36 7c 1c bc b6 41 ec 9d c8 4e ec 8c e3 23 b7 5d d9 40 14 4a 07 ff 00 d1 65 7a ae 39 b5 4f 69 77 ff 00 f0 a9 bc f2 1e 51 73 de a6 34 fc 80 d3 a5 e6 98 98 f7 ee 5b 6a 38 62 43 8e 30 14 b0 85 21 4c 95 b1 01 2b 69 1e 54 bf 2d 1b b7 e2 43 a0 16 52 ab 45 49 40 b8 f0 b5 bc b7 be 5f 58 a7 8a b7 ae fa 5b a6 91 27 9b d6 Data Ascii: .(<`^.(HXB!]{OH3c7+}JOwtl'XZPO12Y>*I_&%CLiG{M-VR6|AN#]@Jez9OiwQs4[j8bC0!L+iT-CREI@_X['
2021-10-29 15:22:59 UTC	78	IN	Data Raw: 47 fe 1c cf f5 1f fc 84 1e ab 30 7f cb ea 38 86 d0 e9 cc 45 b9 d1 c6 76 5e 51 55 ec 23 cd 57 e8 62 be 7f bc 7f 21 ef 71 42 7f 54 df 77 cd e2 86 bf fc 1e ff 00 5b 45 bf eb 45 14 63 21 c8 7a 47 ee 94 76 03 75 3b d0 a1 80 78 3d f3 df 1c 7c b8 cf 7f a6 7a 6a 98 86 de c3 ed 91 ce 10 51 4a c1 1a 0f 7e 1a 6e 78 c6 7f b4 39 db 4e c8 a0 d7 6a 53 db 44 86 5e 6b e3 5e a5 b6 02 95 3a 5c ad f2 97 19 b5 24 1f 85 65 0b 88 eb ef 48 6d 5e 64 73 e5 ac 1d e3 03 1f d2 41 4e 87 4a d8 e2 0d d9 16 0e f7 3b f7 6f dc 35 3a 9d 83 32 ab 10 5c 90 02 92 a7 27 78 c8 80 5f 93 77 bd ac 39 b8 d2 dd 4d 91 76 e9 d5 19 a9 ee cf 6e 1d 32 f6 bb 6d f5 be b6 4b eb cd 32 bf 26 a7 21 e6 9c 98 97 50 84 b1 6e 55 a0 53 e2 49 92 94 ac ca 49 90 db 6a 98 d2 50 c6 1a 72 0c a5 52 a6 59 06 9c ac 15 10 90 Data Ascii: G08Ev^QU#Wb!qBTw[EEc!zGvu;x=|zjQJ~nx9NjSD^k^:\$eHm^dsANJ;o5:2'\x_w9Mvn2mK2&!PnUSIIjPrRY
2021-10-29 15:22:59 UTC	79	IN	Data Raw: 95 56 ae ca 6e 38 0e 84 40 86 b9 b4 f8 6b ab b8 1b 5b c9 8d 04 d4 1d 8e 97 1d 08 cb ce ee 5a 1b 2d a0 ee 20 ad 94 3b f4 ef 48 76 cd 0f 47 f6 65 56 d0 ae 29 44 ba 72 3a 94 a9 64 cc a8 24 e2 4a 24 a4 1b ac cc 2a 0f 90 0e ef 94 51 a0 ab 12 3b 20 82 4e 22 00 b3 e4 5f 27 ca e4 db 94 65 e6 bb 5c e9 6e 6b d4 5b f2 bb 73 57 e8 f6 a5 d9 41 9e 9b 34 cd a4 53 ea 0e db 4e 53 12 c3 b7 bd 16 c9 8e 89 94 57 a5 54 6a 74 c4 c3 a9 c0 fb f2 23 95 6a cc e8 a6 90 f5 2d c8 55 26 22 39 f3 67 4a fa 42 7a 54 64 cd da 3b 4d 74 7b 27 68 a9 12 e9 3a a4 1c 08 9d 2d 49 22 5f 64 a4 b9 61 d5 4c 24 62 71 61 f1 46 9b 66 ca 4d 22 d9 05 25 53 9c 85 10 49 00 83 95 89 1a e4 5b 89 b0 13 0d 3b 59 e2 5e d6 ad b7 70 d6 63 d2 f4 d6 9f 5e a5 a1 cb 37 55 1e 6e 24 38 15 ba d4 69 0d 33 6b b1 32 91 31 Data Ascii: Vn8@k[Z- ;HvGeV)Dr:d\$J\$*Q; N"_'e\k[sWA4SNSWTjt#j-U&"9gJBzTd;Mt{'h:-I"_daL\$bqaFfM"%SI[;Y^pc^7Un\$8i3k21
2021-10-29 15:22:59 UTC	80	IN	Data Raw: 55 9f 05 d5 0d 32 6f c5 aa a2 ca d3 0b c3 52 2e 9a 4d d5 7c c9 bb 69 ba 83 2e 34 9a dd 91 5e ba e9 34 43 65 db ce 45 62 05 2e 66 aa c1 9b 5a b9 a7 db 94 29 50 6b d0 eb f5 2a ad 61 ba 23 aa 31 e1 45 a1 d9 ca a3 9b 35 53 26 a6 7d 3a 65 26 58 91 30 09 8a 18 52 42 83 a9 d8 17 39 69 96 f8 3d 6d 6c b9 d2 65 c8 95 21 52 a6 ad 40 26 6a 49 42 07 6a d6 4b 00 40 c8 ef 00 9d 23 69 53 76 d9 1e 28 aa 7a 29 af 76 23 b3 a3 65 69 d5 12 3d d9 57 b7 cd 55 84 b3 35 d6 ea df 6a e2 d2 48 35 02 84 38 eb 4f 41 7a 91 73 ea 2c b6 24 c7 71 d6 7c d6 a2 bc ca c8 f2 8a 4a a5 a6 a1 60 a6 99 52 52 02 92 71 39 0b c9 b0 e8 c3 80 61 66 c9 e2 1c b9 2a a5 42 e5 ae 7a 66 af 0a 4b 8b 14 85 12 4a 49 77 37 00 9e 63 84 50 8f 1b 3a 7e f5 b7 e2 4f c3 df 88 2a 4f 9a c3 40 af 4a ef 85 a3 05 a9 74 d7 9d Data Ascii: U2oR.M|i.4^4CeEb.fZ)Pk*a#1E5S&}:e&X0RB9i=mle!R@&jIBjK@#iSv(z)v#i=WU5jH58OAzs,\$q|J`RRq9af*BzfKJlw7cP:~O*O@Jt
2021-10-29 15:22:59 UTC	82	IN	Data Raw: 4f 1c b4 f7 78 ab c0 77 88 81 ee c9 74 c7 eb 77 63 b7 75 ad 2e e8 a1 be b6 62 25 d5 c3 8e fd 22 5c 07 53 1d 30 29 a9 62 6e f4 cb 9a b9 eb 9c 1a 4a a3 a5 96 fe 0c b8 95 38 7c 94 95 79 dd 7d 59 fe f0 a9 9b 5f 4f 3a 7d 04 b9 92 05 3c c5 2e 5a 90 b5 2d 61 02 9b 01 18 56 b5 ac b0 4a 81 0f d9 2e 4d b4 f2 29 e9 93 49 4c 65 ad 08 99 31 0a 2a 72 49 2b c8 eb 60 05 c3 07 2e 31 33 31 a3 be 31 ea 8c 55 a1 42 8f 1a 45 46 1d 34 5f f0 23 d2 22 22 b8 c3 d4 cd eb 44 7a 85 c1 36 35 1e 91 22 7b 71 a8 b1 5e 55 2e 20 54 f3 1a 59 ac a9 f7 63 51 e2 16 5d 7a a3 9f d9 e8 95 51 d2 4a 89 94 cb 9c aa 64 19 f5 08 95 35 6a 54 a9 25 5d 5f 5c 89 21 f0 ca 4a c8 4b a2 58 4a 12 52 59 37 68 e5 18 4b 31 38 94 03 13 7b e1 3d fa 37 ca d1 4b bc 3e 42 34 6d 7a b4 a0 fc 74 37 73 6d c6 43 42 9c a5 Data Ascii: Oxwtwcu.b%"\S0)bnJ8y}Y_O:}<.Z-aVJ.M)ILe1*rl+`.1311UBEF4_#""Dz65"{q^U. TYcQ]zQJd5jT%]_\!JKXJRY7hK18{=7K>B4mzt7smCB
2021-10-29 15:22:59 UTC	83	IN	Data Raw: b0 66 61 48 51 16 4e 10 18 bb 82 0d 81 8f 5f e8 d4 84 d5 f8 8a 20 00 13 70 c3 b5 6b 38 02 e5 c4 33 ad cd 6e 05 14 6b c2 9e fc 8a 3d 76 89 e6 51 2e 16 bc d9 4e 9a 7b f1 d4 ef c2 38 d2 d9 74 c9 5c 5a 8b 4a 71 c6 14 cb c9 65 6f 79 09 75 87 d8 6a 64 7e a3 d1 6d 49 72 66 f5 b2 64 29 13 2f db 04 93 7b 71 25 f5 1f 58 b2 ac d9 ab 32 e6 4a 99 84 85 12 50 18 58 3b b6 59 8c bb 8c 58 7d 3b f1 72 e8 ac 04 cd b8 d4 a6 1b ac a2 4c f6 1c 75 e5 49 79 ca 8d c5 56 ab d5 eb 04 c3 67 e2 8c a9 f4 c3 e4 c9 a8 29 0d c8 88 83 53 44 37 60 c7 92 c4 c7 b5 54 75 73 2a 65 e3 99 2f 0b b3 12 f2 88 2f f1 02 5d 89 bd c5 f9 bc 66 66 cb 34 a9 c2 9b ab 75 8e 2d 18 86 62 90 18 00 43 0b 34 6b 97 85 ed 5c a9 5e 95 f8 74 34 47 53 82 36 f9 6d bc a7 1b 42 3e 0a 36 67 4f 54 86 cb 6c 3a 98 70 ea 4e Data Ascii: faHQN_ pk83nk=vQ.N{8t\ZJqeoyujd~mlrfd)/{q%X2JPX;YX};rLuIyVg)SD7`Tus*e//]ff4u-bC4k\^t4GS6mB>6gOTl:pN
2021-10-29 15:22:59 UTC	84	IN	Data Raw: ca 3c 95 da 54 58 6f c9 87 26 b2 97 e9 13 3e f2 9b 19 d7 ad ca 35 40 46 a6 cb 2f a9 4d a5 ed a9 e9 ad 37 49 2b ea e9 2b e4 cb 3f 90 a0 ab ad 95 47 51 3e 5c d2 29 b0 62 42 65 4b b8 9b 50 b5 62 5b 97 29 05 c2 82 4b 45 e5 4e cc 5c 9d 9d 53 d5 14 4c 9d 25 d0 b5 4b 20 b1 b2 d2 a2 fd 96 65 24 0d f7 b6 e9 7e c8 bd 6e cd 53 f0 cf 6e 5c 94 aa 33 da 9a b9 a9 ab de d5 9a cd 26 75 12 97 70 b9 79 e9 dd 61 17 64 27 a9 b4 9a d3 ae 5a e9 99 71 55 e2 7d c5 56 ad 51 de 8d 02 d3 fb ce 93 30 c6 62 de 88 9a 7c cf 3b da bb 67 62 d4 6c 5a 44 6c f4 54 56 cb eb 17 5f 53 28 20 53 ae 9e 55 09 0b 9a a9 68 5a 54 95 94 a9 38 15 32 58 74 4b 64 b9 4b 24 c6 a7 eb d7 26 94 92 a4 ac 48 05 4a 38 6e b6 b0 23 71 d0 0c bb e2 c5 5a b7 ad 91 5e b0 1f a2 b9 44 99 5d 91 6c 55 24 d0 d5 a3 f6 cd 55 Data Ascii: <TXo&>5@F/M7I++?GQ>\)bBeKPb[)KEN\SL%K e\$~nSn\3&upyad'ZqU}VQ0b|;gblZDlTV_S(SUhZT82XtKdK\$&HJ8n#qZ^D]lU\$U
2021-10-29 15:22:59 UTC	85	IN	Data Raw: 26 15 10 b4 a0 a0 7f a6 f6 dc f7 3a dc e6 58 c5 15 d6 5d 51 a1 5d fa 9b a3 16 fd 0e 9f 5f a3 7e cb eb 8c a9 b7 05 16 e0 a4 b7 49 9f 4e aa 69 1e 8d cd d4 e6 e9 6e c3 6a 64 c8 ee c5 82 fc ca 4d 0e 54 d8 4f 3b 05 ba db 13 62 41 72 5b 10 da 94 e4 a3 19 e5 54 84 c9 94 8c 1f 95 9a 12 5f 37 09 04 9b 92 fd a0 4b 5f 9d a0 73 64 aa 43 4c 9c 71 99 c9 c6 96 22 d8 e7 28 38 23 fc 8c cf 96 e1 18 d7 e3 e6 c7 9d 7c 5f 3e 0e 74 82 1d 52 9f 01 77 2e a7 56 2e fa a4 8a 93 cf b2 88 f6 fd b5 45 76 9f 5b a9 b4 cc 77 19 9b 3e 44 08 b7 33 72 fe 02 98 f3 55 19 0a 0a 11 5f 61 cf 2e 4b 3c 48 0a 05 44 07 5b 95 16 cc 9c ce 56 73 c9 a0 88 01 4a 46 2c 4d 2e 69 c0 c5 41 bb 04 fa dc f2 dc f1 bb 7e 1b 6c 4a 7e 95 68 a6 87 e9 15 93 4e ac 33 a7 96 5d ab ab 70 6d b5 57 ea 2d 4a ae b7 45 b6 35 Data Ascii: &:X]Q]_~INinjdMTO;bAr[T_7K_sdCLq"(8#|_>tRw.V.Ev[w>D3rU_a.K<HD[VsJF,M.iA~lJ~hN3]pmW-JE5
2021-10-29 15:22:59 UTC	87	IN	Data Raw: 92 15 ef cf 6e 4f fd 7a e2 fe 13 dd ea 21 44 2f ab ea 1f ec bb 51 c9 38 2a b2 b6 e2 6e 52 4e 70 00 fb 9e 67 3c 7c b1 db f8 bb 0e 4f 50 aa ad 4f 3f ff 00 84 bf fc 4c 4e a5 04 cf 90 c0 1f d4 45 89 6b 38 e5 f2 f0 86 77 d9 fc 98 32 f4 b2 db 12 a3 a2 46 dd 37 b0 8a 43 8e 29 28 dc a6 26 a4 70 9e fc 8c 6e 24 01 df 81 c7 51 f6 72 80 96 92 ac 85 2c b2 79 62 53 fa c1 36 aa 70 2d 64 a8 5e ae 6b b1 b8 18 53 7f 3b 45 f3 9b 43 82 e2 42 1b 8e 5a 0a 52 dc cc 7f 39 d7 94 90 d9 0a 6d 2e 87 14 94 24 8d e7 3b 0a 96 ad 8d 00 a2 52 3a b2 3d 52 c0 29 0a 27 76 63 73 9e fd 46 f3 be 29 c9 0d 65 12 fc fd 98 87 a5 69 c5 cc ab 8a ab 57 55 cb 54 6a 8f 54 6e 52 98 b3 d6 fb ae b2 6a 12 2a 74 da 8a aa 2c 42 62 55 3a 37 9f 49 66 13 10 28 25 e7 1f 2d b2 87 8b ee 21 33 10 db 18 e9 9d 1d ab 5d 75 Data Ascii: nOz!D/Q8*nRNpg<|OPO?LNEk8w2F7C)(&pn\$Qr,ybS6p-d^kS;ECBZR9m.\$;R:=R)'vcsF)eiWUTjTnRj*t,BbU:7lf(%-!3]u

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	88	IN	Data Raw: 46 b9 6a 51 a4 50 be ea 9a 85 22 91 5e 65 f5 b7 20 51 ea 6a 64 ad b6 4b f2 0b 4f d3 e7 3a da db 81 21 3b d0 cb 8d 19 2c ca f2 f9 d4 c6 7d 34 94 2c a5 07 1a ee 2f 65 b5 cb b6 45 23 de 7e 9d 43 b5 06 cd 9b 29 60 2c 24 11 8d 2e dc 0e e3 9e 7e db 1b 2e da 0e a7 d9 17 25 cd 6d dc b4 4a ed 16 ed a7 aa 34 1a c5 2b 6e f7 1e 8e e3 6d 4e 87 31 a7 22 b8 e4 7a ad 32 a7 0d e8 95 0a 0d 56 03 b2 59 9f 01 e6 dd 8c a9 11 c3 0f 88 12 a9 0d 34 c2 27 28 04 64 16 d9 93 60 e0 b0 be 44 ff 00 a9 a3 7a aa 89 bb 42 91 35 d2 92 82 00 b4 a4 29 cd f5 23 30 5b 81 bb 16 86 d6 88 53 e4 de 1a c9 6e da ae d6 2a 14 b9 15 1b 8e 08 f8 a0 f3 f1 24 c6 99 16 52 5e 34 e7 94 fa 90 fc 57 25 79 31 92 eb 9b e2 f9 48 2f b0 23 34 b7 96 e4 7b ca 8a a3 b3 f6 78 08 2e a5 06 52 a5 80 10 91 7b 85 01 de 34 Data Ascii: FjQP"^e QjdKO:!:,}4,/eE#~C)`,$.~.%mJ4+nmN1"z2VY4'(d`DzB5)#0[Sn*$R^4W%y1H/#4{x.R{4
2021-10-29 15:22:59 UTC	88	IN	Data Raw: 0c 0d f8 ee e3 95 b3 8e bb b4 06 c4 a3 d9 2c 4a 81 1b cd 54 da 85 21 49 9a fa 24 3c f3 11 69 92 21 06 16 d8 79 c0 a5 14 ae 3a 12 1b 82 44 74 32 b2 52 12 b0 ea 87 55 54 bb 6a 68 a6 5a 7f c4 ba a6 2d 44 92 cc a0 03 6f 07 37 25 f9 c6 86 b7 a3 f2 82 a4 9e ca 8c 9a 89 73 40 29 0c 5d 92 a4 1c ec 01 24 1c e2 7c fb 37 35 1a d2 f1 91 60 3f 16 bd 29 8b 76 fa a7 44 8d 2e a3 6f 41 a9 a6 9a 2b 10 93 52 98 57 58 a0 16 94 b9 aa 6d d8 91 a9 4d cf 76 13 eb 4c 2a ba ea 4c cd 61 68 0a 4b de 89 b0 ea 28 f6 94 a9 94 f3 94 b1 37 ab 09 4a 52 b2 9c 25 81 24 0f f3 3d c1 19 5d b7 78 1f 4a b6 7d 45 35 4c c9 88 7e a6 7c e5 4c 33 02 5b 0e 25 11 84 37 64 84 80 c3 13 3c 6d cd 02 d3 14 b8 cd c2 a6 c6 83 45 a3 47 a9 53 a5 35 1a 23 b2 2a 4a 95 f0 72 a5 4c 9b 22 4b b3 a3 46 7a 34 89 72 16 Data Ascii: ,JT!I$<i!y:Dt2RUTjhZ-Do7%s@)]$|75`?)vD.oA+RWXmMvL*LahK(7JR%$=]xJ}E5L~|L3[%7d<mEGS5#*JrL"KFz4r
2021-10-29 15:22:59 UTC	89	IN	Data Raw: 1f 2a 15 8b aa d9 a7 da f4 3d 48 bd 6d 7a 94 78 d5 ba cc 6a b3 d4 7b ae af 21 0e c1 5d bd 32 63 55 b6 60 5b ad bf 0e 33 75 6f 36 ae c4 3a 2b ad d1 e9 d0 7e 39 a8 b4 94 3b 48 c0 74 b3 a1 12 fa 0b b4 bf be 36 75 54 99 1b 4a a7 65 6d 39 35 33 07 e6 17 b3 6b 7f 35 28 d2 cb a5 34 12 81 65 4a 33 31 c9 c4 8c 29 58 48 31 a5 91 57 25 66 58 9a c8 59 52 59 45 40 aa c4 66 a7 0a c3 bc 5b 86 51 5a b4 f2 91 4b 95 68 56 e4 55 f5 09 99 37 3a 35 2e 0d 35 76 95 cd 22 b1 46 a1 43 93 4e 83 59 31 94 b9 f0 0c 29 17 62 8d 6e eb 76 d2 b9 aa ac 2a ac cc ba 22 63 c7 5a 5a e9 de db 35 9f 9d e7 f4 76 82 b7 a3 a8 56 d6 db 55 d4 5b 43 69 ed b3 41 2f 65 d3 cb a8 a5 a0 5d 16 cf 4a a6 cb ac 3d 43 4b 9f 34 4f 98 11 3e 7c d2 d2 65 ac 25 64 12 90 4a 66 ac d4 a9 48 ed 20 a8 b2 49 03 fe ab 10 Data Ascii: *=Hmzxj{!]2cU`[3uo6:+~9;Ht6uTJem953k5(4eJ31)XH1W%fXYRYE@f[QZKhVU7:5.5v"FCNY1)bnv*"cZ^5vVU[CiA/e]J=CK4O>|e%dJfH I
2021-10-29 15:22:59 UTC	91	IN	Data Raw: a9 ac 42 a0 37 29 cf 85 34 d5 e3 b1 04 cd 8d 1c 84 39 6f f9 0d ba 5b 88 e2 7a 91 85 04 4c 59 3d a9 43 0a 46 fc 57 bf b1 96 e8 ae 5a 94 57 21 00 90 95 25 0a 55 f2 50 74 83 e0 ab 39 0f e1 14 b3 c0 bd ab 4f 77 48 e9 da b3 2e a0 8a f5 f5 ac 0d 2f 50 2f ba d8 46 3e 2e ec bb df 76 e5 b8 14 8d d9 52 23 aa a5 56 b5 71 98 4a bc a8 b1 63 c5 8c c8 4b 6c a1 22 2d 2a 31 85 ac 96 72 41 4b 38 cd f2 df 13 27 ac a7 0a 05 c0 fd c7 32 5d b2 61 de 77 e5 1b 1b e1 85 a0 98 b7 59 38 05 4e 53 13 bb 18 f7 a8 64 12 7f 8b dc fd 49 e0 75 69 4a 19 db 75 fc 4f d3 db c5 55 61 c4 52 4e 67 df ca 2d a9 8e 9e 14 95 72 78 cf 38 ed dc fb 13 f4 fc bb f5 32 21 40 6a 40 03 03 f8 41 c7 fd 7d ff 00 be 3a 50 a0 2e 94 28 0d 5c 9c 0e 4f 3c 7e 9f 4c 76 fd 7f cb a5 0a 0b b8 90 42 b8 19 c7 eb 9c f1 Data Ascii: B7)49o[zLY=CFWZW!%UPt9OwH./P/F>.vR#V[qJcKl"-*1rAK8'2]awY8NSdIuiJuOUaRNg-rx82!@j@A}:P.(\O<~LvB
2021-10-29 15:22:59 UTC	92	IN	Data Raw: 4c b9 f2 88 39 7c 5f fd 3d cc d6 89 0a 1f da 41 a3 09 7d 0f 56 97 88 2b 1d 6d 2d 45 52 2b 1a 23 7c d5 63 b4 95 b4 da 54 db 95 0b 4e 99 59 88 96 c2 c1 de b6 1c 79 2e 21 01 68 52 55 ea 4c c4 ed 94 15 a8 2a 45 52 94 ac b0 a0 1b b6 47 2c cb b5 9a 04 76 55 42 45 d4 8f 13 f2 1f 48 0d 9f b4 2b c1 8b f0 5a df ae 70 28 2f 3d 33 ce 11 af d8 17 2d ab 26 3e e6 d6 d3 a8 75 37 3d 1e 9a f0 5b 61 96 0a b6 79 e1 6b 75 4e 29 d5 b8 a2 94 cb a7 da f4 8d 82 6b a1 7a 89 88 20 a4 e7 a0 2c ce 4e fd d0 86 cd ab 48 7e a8 a8 1c 94 92 9b 86 dc 48 39 fd 5a 1f 0a f1 4b e1 da f1 a2 49 55 b5 ae 7a 5b 5b 09 4c 79 48 44 7b d6 8a db 8b 4b 4f b2 f2 b6 45 99 2e 33 ea 25 29 3b 52 96 16 bc e0 01 bb 19 94 aa 8a 65 25 d0 b4 92 92 e4 81 98 37 d4 3b 8b 97 1f 68 17 e5 6a 11 d9 54 b5 8c 4a cb 37 Data Ascii: L9|_=A}V+m-ER+#|cTNYy.!hRUL*ERG,vUBEH+Zp(/=3-&>u7=[aykuN)kz ,NH~H9ZKlUz[[LyHD{KOE.3%);Re%7;hjTJ7
2021-10-29 15:22:59 UTC	93	IN	Data Raw: 9a 10 a3 31 f7 8d 7a bb 2a 1a d9 96 29 30 83 ec 20 c6 8e f4 7a 8d 56 5b aa 6a 04 98 0c 43 a9 54 a1 1a 92 4a 14 47 5d 31 c5 b0 25 ee 39 93 f2 66 ce e6 00 b2 be b1 78 90 92 c0 dc 65 77 bd ef 6c fe 91 8c f5 3f 14 3a e9 73 dd 29 d4 6d 4b ab d2 af c8 a9 5c 38 b4 fb 72 ab 6f d0 e0 d0 18 82 d4 93 34 d0 69 92 68 ad c0 ab d1 23 34 87 1d 76 33 b2 25 d4 dd 72 40 4b b2 d9 98 b6 dd 59 b3 9f 43 4d 3d 29 94 b2 a2 e9 ec 94 e6 0e 4e 6f 76 7e 1c 32 87 d0 6d 0d a1 b2 f1 4e 95 37 1c b2 b0 f2 94 7b 21 24 8c 40 06 3c 7e 64 e7 1a 9f 46 f0 6d a7 da e6 ad 32 f1 5b a0 32 69 2d d1 aa 34 77 2a 77 3d b8 9a 92 11 2a 83 7c 51 d3 4d 90 f5 0e a2 c3 cd ca 44 1a 8b 24 54 19 96 ca 96 cb 46 4c 76 5e 8d 35 34 fa 84 67 5d c9 d6 22 b2 81 33 28 71 26 65 3a c3 25 6b 72 b4 b8 de c7 96 67 76 51 ea Data Ascii: 1z*)0 zV[jCTJG]1%9fxewl?:s)mK\8ro4ih#4v3%r@KYCM=)Nov~2mN7{!$@<~dFm2[2i-4w*w=*|QMD$TFLv^54g]"3(q&e:%krgvQ
2021-10-29 15:22:59 UTC	95	IN	Data Raw: f6 9b c6 a4 ad ea 8c 1b 42 87 1a 9f 69 d4 a7 4f 7e 44 f7 21 26 81 f7 39 93 25 d5 29 0a a8 4c 97 4e 1f ef 2f 49 42 96 5c 5a e4 1d 8e 93 9d 9d 02 29 cd 16 cd 55 3a fa f9 68 a3 92 99 05 99 2a 49 90 94 82 a3 62 d8 6c a4 fc 57 76 6b c5 90 09 00 75 77 96 53 d9 50 66 25 f5 cf 40 cf 68 ab fe 2f 9a a6 84 c0 45 46 1c 11 09 db 66 aa c5 6e af 56 7e 63 d4 ea 55 1e 4f c5 42 9a fc 1a 6d 2d c6 65 0a f2 e9 52 eb 6d 42 aa d4 65 b7 4b 89 10 d4 23 44 a7 d6 6b b2 a9 71 1b f2 3f c6 95 75 7b 00 93 2e 9c 2e 65 34 ca 7c 55 2a 33 04 be ba 6a 10 67 4a 92 94 92 95 c9 49 52 84 c2 46 14 92 90 0a b0 88 83 5b 37 06 16 0c 43 1c 4a f8 46 a5 d8 ee b1 05 c6 6d 72 98 a9 b6 3e 89 48 be 28 7a 7d 55 b4 5b a5 fd c2 f4 7a fd 5a 97 74 c3 b8 25 c4 a8 b1 1e 97 12 82 88 d5 e8 d4 b7 e9 e8 75 98 0f d4 Data Ascii: BiO~D!&9%)LN/IB\Z)U:h*IblWvkuwSPf%@h/EFfnV~cUOBm-eRmBeK#Dkq?u{..e4|U*3jgJIRF[7CJFmr>H(z}U[zZt%u
2021-10-29 15:22:59 UTC	96	IN	Data Raw: 4b 83 5a a2 db f5 3b 66 e2 6a bc fc 1b a1 b6 e2 42 a7 d4 a9 ae d4 e3 b2 98 88 8a d3 13 89 46 7a dd 92 b0 92 ce c5 c2 6e f7 6b 1b 96 d4 1c b4 14 b2 9e b1 29 50 05 42 e9 50 5a cc 09 f9 d8 1f b3 ba 2c 46 3c 28 e9 73 13 1b 75 a7 5a b5 e8 c9 09 79 b5 21 4a 8e 29 b1 d2 d3 9b 17 92 37 b6 90 41 2a 3b 87 20 e3 3d 48 a6 3d 82 07 da db fb f7 42 a9 57 ea 36 b7 e5 e7 e1 af 08 d8 7f 0d 08 3f 77 5c ca c0 04 cb a6 80 7e 78 13 c2 47 38 20 80 49 f6 1f 2e a6 d3 9f a7 ac 56 d5 db 0f bc ef 16 94 48 ca 70 01 18 27 b0 38 cf f3 39 07 bf e5 8f cb a9 91 0e 3d 95 24 8c 1e 54 70 4f cb 93 f2 ed f5 f9 fe 9d 28 50 12 92 06 48 c0 f9 fe 7e dc 7f d7 f2 eb ad c4 79 fd 23 8e 77 1f 11 f5 82 6e b8 94 1e 78 3d bb b0 67 27 eb fd ff 00 2e 98 54 01 6c f9 7d da 1e 94 95 07 cb 9f d9 e0 Data Ascii: KZ;fjBFznk)PBRnw;,<(suZy!J)7A*; =H=BW6?w\~xG8 I.VHp'89=$TpO(PH~y#wnx=`g'.Tl}
2021-10-29 15:22:59 UTC	97	IN	Data Raw: 9c 96 10 b7 2e 0a 53 c0 46 43 e8 68 94 04 94 86 c2 12 42 52 0f 55 73 64 4d 5a ce 19 d3 5b 37 c6 05 bf ef 76 6f 23 16 52 67 52 a5 00 28 07 b0 cf e5 c3 30 d6 7c e2 ee f8 29 b0 b5 8e c9 b9 2e aa c6 ab dd 95 d9 31 1b 81 4d 8b 6b d1 dd d4 d8 d7 95 1e 4a a4 a2 a6 d5 59 f4 c4 a5 dd f5 9a 73 2f 34 15 4e f2 d5 22 12 9e 50 49 4b 4f c7 f5 79 92 a8 65 29 20 2a 6a e5 b8 df 51 de 3f 6e 7b cf b2 29 cb 4a ad 2c 62 b6 e2 d2 bc 38 16 fe 78 46 92 7c 44 d9 69 da 5a 91 25 b5 10 9c 16 9d 71 b7 00 e1 49 18 41 4a 81 c0 1e a0 01 4f 70 3b 0b 27 04 95 04 49 56 f3 75 38 b5 f1 61 01 46 c7 cf ba 2b 9c 95 d7 02 06 58 92 03 9d 00 7b 71 88 22 95 fe cc 75 03 53 b5 6e d9 bf f4 ea c4 95 61 e9 5e 96 ca b9 aa 12 aa 36 2d ad 32 af 71 dd d5 09 4d c6 a7 53 e9 d5 6a cd 32 7b 8a 34 56 5a a8 55 27 Data Ascii: .SFChBRUsdMZ[7vo#RgR(0]).1MkJYs/4N"PIKOye) *jQ?n{)J,b-8xF|DiZ%qIAJOp;'IVu8aF+X{q"uSna^6-2qMSj2{4VZU'

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	98	IN	Data Raw: 6b 98 8a 64 14 4c a9 60 54 92 a4 91 c8 62 ed 0c f2 70 3c b4 31 31 15 18 c4 a0 6c 45 9f 53 ba fb df 5e 1c 6f 5d 34 a3 48 34 ef 59 f4 a2 25 76 b1 43 72 3d 6a 04 bb ee c6 aa b9 2c b1 32 a6 cd 42 c4 bc 2b 11 9d 96 85 36 b7 23 b2 4b 15 38 f2 5e 89 15 6e 44 2c c9 00 79 8a 43 cf 3c 85 29 50 eb 12 a6 d4 5e ee e2 df 76 e3 68 6a a7 e1 9b 35 24 16 21 9f 36 03 5c ef dc ed a4 51 5f 10 de 0a 6d 4d 38 a7 49 bf 29 34 07 eb 7a 6b f1 80 6a 35 bf 44 61 53 aa 36 9b 5b c2 cd f7 68 42 52 81 99 4a 4b 29 13 ea 76 f3 8b c1 a7 26 6b 34 b7 21 4d 83 16 53 53 02 96 95 a0 82 e1 29 0f 76 24 b6 5e 3b fe 50 d4 cc 41 92 a4 2e d8 89 29 0d 6b 8f 76 71 68 7a 78 3b 55 63 c1 e6 bb 43 b0 2b f3 99 aa f8 6c f1 5b 16 89 02 c8 bf 69 49 4b d6 e5 3e fa a8 44 8f 2b 4f e6 bb 39 cd cd 37 1e b9 1e ac 68 Data Ascii: kdL`Tbp<11lES^o]4H4Y%vCr=j,2B+6#K8^nD,yC<)P^vhj5$!6\Q_mM8I)4zkj5DaS6[hBRJK)v&k4!MSS)v$^;PA.)kvqhzx;UcC+l[ilK>D+O97h
2021-10-29 15:22:59 UTC	100	IN	Data Raw: 52 06 e2 c5 e2 5c c5 55 53 ca 9d 30 d2 cd 51 4a 54 4f 64 bd 86 40 5d d5 c0 5c e4 cd 15 26 6e bf 6a 66 ba da d7 04 4a 0d 36 55 a6 d2 d2 fc 5b 75 ba eb 32 17 71 54 57 54 a1 41 7a 42 ee cb 68 37 f0 6c 5b ac d4 a5 42 84 f5 72 ad f7 d3 33 a9 c9 aa 47 72 db 43 ad b8 cc ef 9a b6 af e2 17 48 36 e9 ad 5d 47 47 b6 a6 c8 a7 a6 a8 aa a2 91 51 2a 7c e9 b5 b2 cc b0 94 cd 08 45 2a 65 a2 59 2d 86 62 a6 2e d8 bb 07 0b 0c dc 9d a1 5d 5f 4b 50 94 52 55 52 a8 29 a4 cc 5d 3c d4 15 28 17 52 70 a9 20 b1 74 dc d9 41 cb 38 68 d1 3d 23 aa 47 6e cf d0 48 12 6e 24 41 97 41 b5 4d 3a b5 4b 4d 42 3b 62 a5 2a 2d af f7 7b 7f 16 c3 35 19 4c 08 89 71 a7 2a b1 9b f8 89 aa 86 af 85 60 2f f1 b8 8f 7f e8 a5 40 56 c1 e8 c4 a2 66 49 5d 3d 22 65 55 48 5a 56 99 8a 12 a9 70 02 ca 67 75 5d c9 2a Data Ascii: R\US0QJTOd@]\&njfJ6U[u2qTWTAzBh7l[Br3GrCH6]GGQ*|E*eY-b.]_KPRUR)]<(Rp tA8h=#GnHn$AAM:KMB;b*-{5Lq*`/@VfI]="eUHZVpgu]*
2021-10-29 15:22:59 UTC	101	IN	Data Raw: 86 bc 75 49 b4 c9 4b 95 5a 4d ca e4 1a d8 69 5f 10 ca 64 44 a7 34 f0 71 82 5a 41 54 65 fc 7a d6 97 fc 94 79 ce 05 87 09 75 0b 00 61 52 5a 61 52 d3 d9 56 1c c3 82 a2 ed de 5a 0e ac 78 25 92 0e 15 25 d3 6c db 36 d6 cd fc 88 ab d4 79 f6 6d 25 dd 55 d4 fd 6e bd e0 69 9d 8b 44 bc ea 51 aa ce 5c 92 45 ae b7 99 82 f3 68 a6 ba fc f9 a2 3b ed 53 e6 52 de a7 3a d7 dd 6c 3f 36 a5 1e 73 2f b2 f3 31 d7 11 d5 d7 54 7e 5a 4a 97 3a ae 74 b9 28 43 3e 39 89 1d c9 0e 09 3a 80 1c 93 a3 c4 89 54 d5 15 44 26 9e 54 c9 a4 dc e0 42 88 03 42 a5 36 14 8f f5 11 c5 a2 1c d5 2f b5 03 ec c5 d4 3d 2f d4 5d 23 57 89 4b 29 9a 4d d1 64 dd 36 3a 1e a6 d1 2e 89 51 a3 b7 5e a4 d5 e8 8e 4f 88 f4 4a 0b cf 3d 1e 24 bd ce 99 58 c3 af c1 52 83 8b 75 21 6b e1 ab a4 32 41 93 37 12 66 05 60 29 4a 89 Data Ascii: uIKZMi_dD4qZATezyuaRZaRVZx%%l6ym%UniDQ\Eh;SR:I?6s/1T~ZJ:t(C>9:TD&TBB6/=/]#WK)Md6:.Q^OJ=$XRu!k2A7f`)J
2021-10-29 15:22:59 UTC	102	IN	Data Raw: f3 8c e3 eb d2 85 1e 4a f8 c7 60 49 19 c9 3c 03 f4 23 bf e4 3f d5 42 80 0a 88 ce 49 3f 4c fc b9 cf fd fe b8 e8 88 f8 4f 33 c3 41 0a 3c 95 63 07 b9 23 27 9e 7f c3 f3 e8 70 35 2b 41 e3 f4 f7 ca 3e 15 9c 7a 73 9f 97 1c ff 00 67 b7 47 19 0e 43 d2 07 1e 77 93 dc fb 72 38 ee 7f 4f ef e7 d7 61 41 69 6a 4f c1 cb f6 1f 0b 23 b1 ef 86 57 9e ff 00 af bf fa f4 b2 87 23 e2 1d fe 86 21 45 54 41 25 20 e7 09 04 60 e7 93 9c e0 1c f2 3b e7 9c 01 91 83 82 23 28 90 3b 20 17 b3 1c 9a 24 00 0a 85 ac 18 ef c8 7c fd 4e f8 21 16 ac fa f7 05 48 75 69 c9 0a 4a dd 5a 92 40 52 80 e1 4a 27 1c e4 27 f0 fd 3e 41 12 d2 5c 2a 50 72 e0 90 90 4f 30 ec 09 61 6d f9 5e 1e b9 d3 59 92 a6 63 a9 d3 2f 7c b5 83 32 61 d0 2a 6d 94 d4 68 d4 6a 82 4a 70 53 3a 99 06 5e 70 3f 8b e2 18 5f 04 f7 cf 71 df Data Ascii: J`I<#?BI?LO3A<c#'p5+A>zsgGCwr8OaAijO#W#!ETA% `;#(; $|N!HuiJZ@RJ">A*PrO0am^Yc/|2a*mhjJpS:^p?_q
2021-10-29 15:22:59 UTC	103	IN	Data Raw: 78 6a 88 4c c7 3d a4 4e 00 36 6d a6 99 7b dc e2 af eb 2e b0 cb d4 5b 7b c2 9f 88 74 b6 dc 7b 9b 49 7c 4d 58 ba 67 ab b1 a3 e0 aa 87 58 9d 73 9b 02 b5 21 ed 9e b6 29 b5 e5 d6 29 92 a3 a9 7b 59 d9 22 2b 4a 56 56 90 a7 c9 69 d3 a5 2d 7f 16 15 05 28 ea 5f d9 3b fd 06 b5 75 21 68 06 ce 0a 46 eb 39 cb 9b e5 68 b8 37 7b e8 a6 ea 26 a5 45 73 d0 ed 59 88 01 0d 2b d2 5d 4c 4f 8e 9a 5e 4e 48 2a 6c 07 19 4a d5 b0 90 e0 29 c8 3b 87 51 a7 21 97 34 36 61 59 0c d8 e5 ab c4 89 0b 25 28 23 ff 00 50 3b f8 9f 0d fc 37 44 03 e0 86 4b 92 34 ff 00 5e 63 ee 01 cb 3b c5 46 a4 f9 47 69 ca 60 d7 a2 50 e4 cb 42 93 9c a5 0a 5a d8 5a c7 00 a5 27 b2 79 04 97 25 3f 96 07 fa 5d c1 b1 7b 5f e5 9f 28 74 c5 7e aa 9e ee 9b 65 6b 9d d9 db cb 84 4c 95 71 1a 81 73 21 a9 8c 87 ed bb 80 48 85 53 Data Ascii: xjL=N6m{.[{t{I|MXgXs!)){Y"+JVVi-(_;u!hF9h7{&EsY+]LO^NH*IJ);Q!46aY%(#P;7DK4^c;FGi`PBZZ'y%?]{_(t~ekLqs!HS
2021-10-29 15:22:59 UTC	105	IN	Data Raw: 4a a0 e5 0a 43 05 68 30 2b 49 a6 c9 98 e4 4a ab c5 b2 ef c1 3a d2 4b 51 1c 8f 3b cd 0c cb 8e 57 a1 44 ea 4a b9 4f 29 73 27 02 a0 0a d1 28 a9 20 e1 0a 29 20 cd 52 41 4b 94 92 90 0b 86 cd de 15 5d 26 d1 a1 fc a2 76 8c 85 d3 99 d4 dd 72 3f 32 58 cc 1d 6a 92 99 a3 b2 18 2a 5a 52 52 f9 a4 bd c4 3c 25 5c ca 29 25 aa fd 7d b2 a0 76 e6 05 de 85 f1 ea c1 ff 00 77 19 c2 b2 40 23 23 b0 19 e9 b3 64 cc 9a a9 56 c0 94 28 4b 42 f0 29 2b 75 58 07 c6 52 c5 c6 22 dc f5 66 a6 72 58 0c 72 12 05 cb 28 92 40 cc 61 29 1e 77 6d 63 9d 9f b7 17 58 aa 0f 58 f6 1d 80 8b a2 b3 3e 04 ea 85 5a a1 2e 99 55 17 33 10 da 9b 18 43 4c 47 d8 8d 5c 43 11 5c 96 96 bc e4 97 e2 a5 4e 25 0e 34 95 1d a9 23 a9 54 b4 d3 53 39 21 72 93 85 45 41 15 58 7f 51 4a 40 75 25 47 3c 16 38 6e cf 6b c5 75 7d 62 Data Ascii: JCh0+IJ:KQ;WDJO)s'( ) RAK]&vr?2Xj*ZRR<%\)%}vw@##dV(KB)+uXR"frXr(@a)wmcXX>Z.U3CLG\C\N%4#TS9!rEAXQJ@u%G<8nku}b
2021-10-29 15:22:59 UTC	106	IN	Data Raw: d8 06 0a 41 76 8d 09 b3 7c 39 fd 9d 76 d3 75 f8 76 86 a1 db 2f c9 af c3 a0 d7 e6 39 a8 fa 27 68 d9 37 b5 b7 4b a5 b3 53 b6 23 fd ef 6f eb 8d 81 70 db 36 ad 3a b9 54 a1 54 aa 54 8b 72 3d 2a 91 75 d5 db f3 af 3a ac 79 30 aa f1 aa 32 6b 27 f4 2b 62 a9 12 a5 4b af ae 92 99 09 57 54 99 15 73 fa d5 25 44 15 2a 69 13 9c b3 00 1c 1c 22 cf 12 cf 48 76 9c fa 89 eb a9 a0 a5 0b c4 97 32 e9 f0 ca 76 39 14 60 ff 00 a9 8b 12 01 00 44 69 ac 3a 01 e1 63 4d f4 d2 bf aa 92 ea 7a 49 a8 74 0a 55 bc e5 cb 4e b5 ec bf 05 5a 31 7f 6a 4d d3 4e 72 a3 12 97 11 56 bd 16 c4 a8 e9 a4 8a f4 77 27 d4 62 07 aa 8d 7d df 4b 8b 09 4e d5 15 21 31 42 0b 95 e8 e8 36 c7 99 34 26 67 48 36 f5 36 20 70 2a 56 d0 75 2c 82 cd 86 6a 17 89 39 bb 5e cc 22 44 ee 92 ed 44 49 09 46 ca d9 ea 40 67 58 91 7d Data Ascii: Av|9vuv/9'h7KS#op6:TTTr=*u:y02k'+bKWTs%D*i"Hv2v9`Di:cMzItUNZ1jMNrVw'b}KN!1B64&gH66 p*Vu,j9^"DDIF@gX}
2021-10-29 15:22:59 UTC	107	IN	Data Raw: 89 07 77 7d 2d b2 b1 dc 7f 12 a8 84 93 f3 1c fc f3 cf 4d fc ac 80 4b cc 98 ff 00 fc 65 8c b9 0d fe 10 71 52 8f fd 3f ff 00 74 92 fd e5 ed bb 2b 71 26 36 d1 a7 86 46 33 9c 73 df fe d9 fc fe bf 9f 4a 22 2f e1 3d de b0 a4 db 87 8d d9 e5 39 e7 23 f4 c7 f7 fa 0e 8a 8c 8f 38 0c 1c 4b 98 c7 bf 20 e7 bf 4f 86 2f 2e ff 00 91 81 c3 c0 fe 1e f8 e7 db f3 fd 33 fe 9d 74 66 39 8f 58 14 7e 2e 71 f2 23 93 f2 ed fd 7f bf 7e 8f 0a 00 2e 13 9f f1 ff 00 3c 74 a1 40 64 fb 93 f9 f5 c2 59 9f 7b 42 80 cb 89 c7 04 03 f2 3d fa 22 52 f7 39 42 80 54 bc 67 dc e7 9f f1 ff 00 1e 9e 52 91 76 f3 3f 58 51 e3 77 be 79 03 1c fb f3 9c 0f cb f3 ff 00 3e 9b d6 70 f3 fb 40 e6 69 df f2 8f 0b 73 00 01 df db 1e c7 04 8e 3e 9d be bd fa 20 b8 07 7c 0e 3c 05 f3 9d de c0 83 8f 7f f3 c9 fe fe 6a 14 15 Data Ascii: w}-MKeqR?t+q&6F3sJ"/=9#8K O/.3tf9X~.q#~.<t@dY{B="R9BTgRv?XQwy>p@is> |<j
2021-10-29 15:22:59 UTC	108	IN	Data Raw: a8 64 c6 da 8f a7 7c 5b 2d 0a af ac 2a b7 f1 25 71 e4 bc db e6 5c b5 aa 42 97 21 e9 70 24 d2 bc d9 68 f8 9f 87 97 21 98 72 e4 34 d4 b9 0c 3b 31 96 9c 5a 10 f2 50 eb 88 50 ea 7a 41 55 41 3a 50 bc e9 3e 23 8e 5c 0e fc b5 cd ae 24 7f 67 ce 8d f4 f3 66 55 99 b2 86 c8 da 72 01 34 55 74 ea 64 4c 2d d9 33 25 8b 66 2f af 8b 45 f9 d1 8b 8e 55 eb 6e 2a c0 2f 14 ea 5d 84 cd 4a a3 6a 26 32 92 b5 ea 2e 9c aa 44 9a 95 56 05 19 c2 b4 99 17 6d 91 21 f9 15 66 a9 6b 2e 48 9b 6f aa 52 a0 25 f7 20 38 d8 d7 51 d7 d2 ed 34 26 74 a6 c7 84 12 90 58 82 d7 0d ce c6 cc 2f 76 b4 7c 67 d3 ef c3 ce 90 7e 1d ed 55 ec ad af 47 31 74 e6 62 c4 8d a0 84 2b f2 93 65 e3 3d 5a d4 a0 02 71 2c 76 88 e3 9e 51 24 cb 7d cf 10 36 44 9b 3e 89 54 8b 40 f1 01 a4 b5 04 dd fa 5d 5c 0a 11 a3 57 a4 c3 52 Data Ascii: d|[-*%q\B!p$h!r4;1ZPPzAUA:P>#\$gfUr4UtdL-3%f/EUn*/]Jj&2.DVm!fk.HoR% 8Q4&tX/v\|g~UG1tb+e=Zq,vQ$}6D>T@]\WR

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	110	IN	Data Raw: 1c a9 a1 88 0c 46 b8 63 b4 c0 55 38 d1 df 7f cb 7a e7 ab 4e 01 f7 5c 4a aa 0b 62 42 42 0c 7d ab ad 46 c5 d9 28 ae a4 ae 9d 4d d7 55 d2 cb 9b 2e 92 78 29 3d 49 9c 0a 66 97 48 00 76 58 dc 41 a6 6d dd a8 29 aa e9 27 d6 99 74 f5 4a 93 3d 54 d2 65 02 17 d5 2c b2 8c c2 eb 0a 05 4e 40 53 30 0c 1d e2 44 d1 29 9e 16 74 4a f0 ad dd 76 ec 7f 13 95 33 55 a6 54 e9 30 e8 37 2c 3d 1d 93 6e db 50 eb 17 09 ba 6a ed 5b 70 28 f5 6a 2b b4 ff 00 bd 2b 24 49 a9 25 c9 2f 09 8b 6e 22 9f f3 17 0a 3a 81 a9 68 29 b6 7a 54 8a 69 4c 82 a5 ba 6f 75 29 4a 59 99 c8 93 dd 93 c0 ea f6 85 65 6a c4 ca ea d9 95 55 01 28 44 b9 93 27 2d 69 4d 2c b9 69 96 89 41 04 94 a0 a4 a6 ec 01 d2 2d 7a 3c 55 f8 7f 79 b4 a9 eb 4f 58 90 a1 94 84 9a 0d 82 47 23 95 ee 45 e8 e6 67 09 fc 5b ca 14 31 bd 01 5d 4a Data Ascii: FcU8zN\JbBB}F(MU.x)=IfHvXAm)'tJ=Te,N@S0D)tJv3UT07,=nPj[p(j++$I%/n":h)zTiLou)JYejU(D'-iM,iA-z<UyOXG#Eg[1]J
2021-10-29 15:22:59 UTC	111	IN	Data Raw: 26 ce 92 95 96 c5 d8 c4 16 40 39 b1 0c c3 53 18 db 1f 53 35 65 ea 95 ca 6c 9d 01 b1 ad 1d 25 b8 eb 16 75 6a af 7c 6b 96 94 5c 36 55 c9 4e a3 44 14 b9 55 7a 0d 81 5b ba 28 f6 66 97 d4 29 95 6a 15 29 e8 a8 85 57 f8 2a a2 e3 d5 ea b5 e9 d7 52 6a ef 22 b3 17 cf 93 d2 7a ea 39 72 8e d0 fc 3f db 73 43 2f f5 28 4c bd a5 36 50 04 12 54 03 19 09 56 60 87 36 b1 0e d1 b7 9b d1 fa 09 aa 1f dd fd 35 d9 8a 4a 93 79 33 65 2e 8d 29 71 a1 59 51 5a 83 30 49 38 4b dc 41 ca f7 89 cf 07 cb a3 dc 76 b5 fd 63 d8 62 e7 6e ad 52 53 28 52 74 1e 8d fb 2a 82 dc 58 cd d1 ed 29 74 0d 7e a3 0a b5 0a 8b 32 2b f2 e2 4c ac cd 9d 56 a9 3d 3a 42 26 49 95 1d 70 a0 45 b3 91 d3 59 35 32 c2 8f 46 7a 4b 4b 25 36 06 75 1c c4 a8 d9 99 62 5c cc 4b 4d f2 24 8f 48 ab 9d d1 99 b4 d8 95 fd fd b2 67 92 Data Ascii: &@9SS5el%uj\k\6UNDUz[(f)j)W*Rj"z9r?sC/(L6PTV`65Jy3e.)qYQZ0I8KAvcbnRS(Rt*X)t~2+LV=:B&IpEY 52FzKK%6ub\KM$Hg
2021-10-29 15:22:59 UTC	112	IN	Data Raw: 8c fd 3b 8f f3 e7 fb e3 a5 03 21 ac 60 a5 45 cc d3 6a 47 27 8a 7c e3 80 46 32 22 bd 9c 72 07 a4 67 9f d7 df ae 2b e0 57 34 fc e1 e8 f8 80 df ef dd a2 96 cb ae b9 02 99 3a 74 56 5e 97 2e 24 09 32 62 c4 8e da de 91 26 53 6c a9 71 98 61 b4 65 6a 53 8f 25 09 09 1c a8 f1 d4 25 ad 49 96 a2 06 2c c1 7d 12 d9 ee 04 72 df 13 46 1c 49 04 58 a9 86 e0 4e be 71 4c 2f df 1d 5e 14 f4 9e d5 d2 9a 15 d1 7c c1 b9 eb 75 4d 2c a1 9a fd 06 dc 62 95 74 b6 db 51 a3 aa 8a f4 7a e7 99 57 89 0d b9 72 65 41 a9 53 e5 53 54 e3 d3 e1 ae 9a f7 c6 22 32 d1 1c 2a be 6d 6d 2c 94 cb 4c cc 6a 54 c5 32 98 b8 0f 9b ef d3 b8 88 9b 2a 86 a2 64 c5 96 47 56 d6 26 c5 39 5c 5d 9c 0f 1e f8 a1 30 bc 53 f8 3f 88 a0 68 f5 ad 7c ac ad b5 07 62 7d cf 66 59 eb 7d 95 34 b0 e4 77 50 e2 ab d5 37 0b 91 9c 43 Data Ascii: ;!`EjG'\F2"rg+W4:tV^.$2b&SlqaejS%%I,}rFIXNqL/^\uM,btQzWreASST"2*mm,LjT2*dGV&9\]0S?h|b}fY}4wP7C
2021-10-29 15:22:59 UTC	114	IN	Data Raw: 35 38 8e 27 e1 2a 14 99 c9 c2 98 99 19 c4 a7 6b cc ab 63 88 de cb ec 3a c2 dc 6d 65 a5 aa a8 a0 58 9b 25 41 08 eb 0b a5 25 82 83 bb 10 08 7b 67 f3 11 53 d2 ce 87 ec 4e 9d ec 9a bd 87 b7 a9 93 50 27 ca 5b ce ea 92 b1 48 b0 09 41 41 20 94 ab 79 04 6a 6d 9c 59 7a ae a3 c6 bb 6e db 5e ea 8e e4 75 2f 5c 58 0b 91 54 87 01 b4 d2 a8 7a af 12 28 43 92 af 2b 2d 96 4f c3 33 74 47 42 16 fd f9 64 31 99 6d 34 a3 70 d1 d3 36 94 67 26 97 e9 14 95 a9 ad 93 2e a2 5e 14 cc 52 40 5c b4 1b 0c 20 24 96 1b d8 92 5b 33 93 c7 e5 57 e2 47 e1 fe d3 fc 3b e9 0c fd 95 57 2c cd a6 9b 39 49 d9 93 f0 11 2d 74 c4 f6 0a 8e 45 49 41 00 df 37 c8 64 f4 f1 11 a3 ad eb a6 94 ea 26 a0 d9 4a 16 ae a4 d6 ac aa 82 75 02 8b 1f 73 14 8b ea 4d 0a 83 56 8d 4f b9 9c 69 ac 35 0e e7 8d 43 a9 55 a8 75 5a Data Ascii: 58'*kc:meX%A%{gSNP'[HAA yjmYzn^{/\XTz(C+-O3tGBd1m4p6g&.^R@\ $[3WG;W,9I-tEIA7d&JusMVOi5CUuZ
2021-10-29 15:22:59 UTC	115	IN	Data Raw: 87 78 5c d4 3a 7a ed aa 5b 0c d1 de 8b 47 35 fa 84 39 ea 83 19 d5 45 72 44 96 69 2c 46 79 c8 9f 0c 95 17 14 f3 0d 36 e1 6b 0c 54 b5 11 9a 41 02 c4 8c 58 78 e1 21 8b 6e 36 3a c3 a5 96 53 91 8b 52 97 23 13 11 67 07 10 7d e0 b8 7b 45 7b f0 73 4b ba 7c 49 f8 71 d7 ad 5e af dd 12 a9 d7 46 9a 5e a8 b7 6d 8a 55 af 41 a5 aa 95 57 8e a6 eb 7b d1 54 8b 56 5b f5 07 67 28 41 86 ef c5 43 aa c4 69 08 f3 5b f8 45 29 f4 39 1a 9a 96 4d 7c f9 13 c9 ab 72 9a 82 90 f4 b2 ce 10 e4 00 1d 36 c8 0b 5a fa 80 f1 77 32 ae 4c b5 53 7f b8 24 05 81 89 a7 d4 f6 b2 cd 95 7e 3e 67 43 5e ee 3b eb 5c 6c 87 9d 76 bd 1a 23 34 e6 e3 7c 53 ce 33 47 49 96 b5 c3 4c 85 c8 62 21 5d 41 b4 a5 48 da a5 38 9c 05 3c 52 ca 12 37 28 ee 2a 25 56 02 c6 af ff 00 f1 e9 8e bb 8a 7c 41 cc e6 da 91 53 68 59 47 Data Ascii: x\:z[G59ErDi,Fy6kTAXx!n6:SR#g}{E{sK\Iq^F^mUAW{TV[g(ACi[E)9M\r6Zw2LS$~>gC^;\lv#4|S3GILb!] AH8<R7(*%V\AShYG
2021-10-29 15:22:59 UTC	116	IN	Data Raw: 4a 62 6d 1e 9b 50 7a 90 2a 53 aa 2e c1 89 4f 8d 25 86 96 82 d0 14 57 d5 a7 12 fe 32 00 c4 ae 04 ea 39 f8 43 d3 2d 4a 72 b5 15 20 e4 09 24 06 7b b1 2d 9d fe 7a c5 fc 9d a9 a8 88 a5 35 26 41 90 87 3d 61 69 53 9e 61 79 4a 09 25 47 78 2a 2a 0d 94 e7 85 65 5e 92 7d 59 77 5a d9 29 bb be d0 8c 87 d4 77 df e4 23 d6 ac d9 36 e6 aa e9 9a 99 ae b5 23 e1 6a d0 8c 98 8e b8 d3 f8 31 0a 48 4b 8c be 96 92 95 b6 36 95 05 a1 c1 80 95 95 29 60 29 25 4e 18 e5 a4 8d c0 92 de f8 9f 1b 34 76 4a 84 a5 a9 1d 9b 9e d3 6a 77 9e 5d d1 ce a6 a6 f8 53 89 0e ef 71 36 b4 83 20 46 4c a9 cd c7 5a d3 1d c4 94 cc 69 b6 92 ea d0 de 5d da 9f 33 05 41 2e 29 78 25 ce e0 c3 0a 4e 13 64 e2 72 32 1c 08 b0 cb 71 f5 89 22 57 68 16 0c da 69 f7 f1 d2 1f f5 1b 41 cb 42 3d 36 87 5e d3 4a 14 87 9c 65 48 Data Ascii: JbmPz*S.O%W29C-Jr ${-z5&A=aiSayJ%Gx**e^}YwZ)w#6#j1HK6)`)%N4vJjw]Sq6 FLZi]3A.)x%Ndr2q"Whi AB=6^JeH
2021-10-29 15:22:59 UTC	117	IN	Data Raw: 00 01 86 5b 4a 73 8c 64 76 03 03 03 b9 44 b4 0c 92 cd ef 9c 32 08 48 98 bf 31 64 3c e6 c2 4e 02 96 bc 80 9f 7e 49 e7 3d b3 9f d3 27 ae e1 03 27 1c be ef 01 51 72 c3 4b 77 ff 00 3e ef 11 fd f3 24 3f 6e 54 da 53 ee a3 ce 69 96 56 52 e2 d2 a0 db 93 a1 21 cd aa 0a ca 49 4a b0 48 23 39 c6 71 c7 4d 9c 46 04 83 aa 98 ef c2 c1 d8 e9 c2 1f 28 29 27 17 ee d2 df 5d 38 fa 34 31 2d da 0d 12 c9 ad a2 15 b5 18 d3 23 54 ad 5a 7c fa a0 66 43 f9 a9 54 91 39 51 85 4a 7a d6 e1 54 a9 88 8a 1a 8a 87 de 2a 5a 22 b4 d4 66 8a 59 69 0d a4 40 25 06 62 41 24 14 a7 32 f9 b9 0d 7d e3 8f 94 a5 2d 67 0e 26 cc e4 00 cd b7 7b dd 6c fc 69 9c a4 c4 b7 16 c2 76 84 b7 fb 36 10 8e db 5b 3a 79 64 2d 28 c7 60 13 b8 a4 01 8c 27 1d 3e 5a 80 49 00 d9 9c 73 1c ee fe f2 8e 4c c8 01 fe 5f 31 a3 ff 00 Data Ascii: [JsdvD2H1d<N~I="QrKw>$?nTSiVR!JH#9qMF()']841-#TZ\fCT9QJzT*Z"fYi@%bA$2}-g&{liv6[:yd-(`'>ZIsL_1
2021-10-29 15:22:59 UTC	119	IN	Data Raw: 53 e9 f2 62 ad b2 1e 6c 15 25 0a e4 2c 6d 4a 93 df 85 7a bd f3 90 32 3e 7d 48 05 d2 08 d4 67 0c 49 29 51 07 2e 1d f6 ee 3e f2 87 c4 48 e8 5c 65 ed 09 57 9a de 54 92 54 52 4a c8 dc 06 41 e1 5b 9c 51 38 07 8c 7b 70 54 a5 c1 07 2e 43 c8 ee f7 be 38 55 85 d5 91 bf f1 14 93 48 ad 8a 13 9e 22 7c 61 96 d1 cd 02 d5 d0 64 b6 d8 1e 4e 63 42 ab eb 92 aa cc 80 8c 15 95 c2 4b ee 34 4e d7 52 eb 2d 15 12 d8 79 b7 c6 99 69 ea a7 81 66 5a b8 e4 e7 5f 6c 5e 08 a5 7e a4 95 86 75 20 3f 7e 7e 11 3f ca 8c f5 32 14 c6 dc 0c 3a 96 64 d4 52 97 98 0b f2 9c 65 a9 92 95 04 24 29 4b 52 53 f0 22 32 36 93 c8 4e 46 d4 90 91 1f e1 03 77 bf 1e 30 59 73 14 a1 fe 6c 47 70 b7 f2 f9 f9 c1 1a 34 ef 84 aa 47 98 bc 39 06 b3 4f 79 95 14 65 27 cf 86 f3 ac 29 fd c1 2b 2a 54 74 bb 1c b7 85 a7 62 52 Data Ascii: Sbl%,mJz2>}HgI)Q.>H\eWTTRJA[Q8{pT.C8UH"|adNcBK4NR-yifZ_l^~u ?~~?2:dRe$)KRS"26NFw0YslGp4G 9Oye')+*TtbR
2021-10-29 15:22:59 UTC	120	IN	Data Raw: 19 62 1b f3 8f b5 bf 0d 7f 08 ff 00 0f 17 d1 e4 d7 74 ed 1b 63 6b d6 d7 d3 7e 6a 6e ce a3 ac 3b 3e 9f 64 a1 52 84 dc 13 a6 cb 0a aa 54 f9 52 cb 4f 44 d4 84 ca 9a 0a 54 cc 44 6d 17 86 0f 12 34 dd 5c af 5c 1a 77 57 9d 45 a9 57 a9 34 91 77 5a 17 4d bb 0e 6d 3e 85 7f 58 a6 6b 14 59 73 fe ee 9d 26 6b d4 8b 92 db ae bc d5 3a b7 4e 54 c0 99 d0 66 d2 ab b0 21 c5 87 2d d5 0d 97 e1 c7 4c ea 7a 55 49 32 56 d1 97 29 3b 42 42 12 b5 cd 91 d9 93 39 3f 0a 89 43 9e aa 68 51 ed cb fd bc 2d 1e 51 f8 f7 f8 35 b2 7f 0f 51 b2 7a 51 d1 1a 9a a9 fd 10 db ca 99 2e 54 9a d9 92 a7 54 6c ca c9 21 4a 55 38 a8 94 48 aa 96 b4 8c 68 98 e5 9b 09 63 68 b7 32 28 6c b9 3e 9e bc 70 99 d1 0e 4a 89 e3 cf 6c 8c ed 09 04 00 7d 27 70 23 be 01 20 75 e8 d3 65 8c 2a 24 d8 5d 87 d4 38 8f 9b d1 38 a9 Data Ascii: btck~jn;>dRTRODTDm4\\wWEW4wZMm>XkYs&k:NTf!-LzUI2V);BB9?ChQ-Q5QzQ.TTl!JU8Hhch2(l>pJl}'p# ue*$]88

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	120	IN	Data Raw: b9 bb ad 62 ec 59 8f 44 7a 3b 29 6d 35 05 3b 1e 4b 6b 05 4e a1 41 48 2c 3a ce 00 6d 4d 1c e1 d0 40 5b 6b 42 42 42 db 46 ea f4 80 95 a9 b5 2d ca fe f7 c5 aa a6 3a 04 c6 ed 61 22 fc 98 bd ed be f1 61 d9 49 9b 41 ab 42 08 52 dc 99 47 a9 c5 0d ee c6 f5 4a 82 fb 0d a0 28 82 32 54 b4 e0 94 28 00 49 23 b6 64 84 ac 80 92 77 6e f7 c3 3e 51 15 33 13 a8 f9 07 ee bc 72 89 e1 ae 76 a5 4c fb 41 34 63 4f e2 d9 f7 cd 62 92 cf 8b 4f f6 c1 7b d6 3f 62 2a af 5a d4 28 37 3d 2e 15 ca dd 45 ca a3 94 d9 14 98 76 f8 69 9a 7a a1 ce 72 5b 0d b4 f4 56 0c 29 0b f3 12 55 41 5d 59 b3 11 51 4d b3 eb ea 68 3a da 9a 91 21 12 67 55 c9 44 d2 14 3b 21 32 d6 a4 a8 a9 d8 00 1d d9 85 e2 e7 67 51 57 2a 5d 45 65 3c 9a 94 53 d3 c9 5c e5 cf 14 f3 16 87 48 74 80 a4 a5 48 18 b2 ed 35 f4 11 a7 3e 1c Data Ascii: bYDz;)m5;KkNAH,:mM@[kBBBF-:a"aIABRGJ(2T(I#dwn>Q3rvLA4cObO{?b*Z(7=.Evizr[V]UA]YQMh:!gUD;!2gQW*]Ee<S\HtH5>
2021-10-29 15:22:59 UTC	121	IN	Data Raw: f4 e9 ae 53 fe 34 48 53 13 56 01 7c 99 00 26 9d 73 65 96 59 0a 77 72 0e 79 65 c3 52 d1 1e 73 7e 6a 5a 48 b0 39 be 43 2f ac 72 f9 f6 29 3f 6a 54 7e d3 5b ce 46 9c c8 ac 4a b0 e9 d6 0c ba 5d 1e 55 6d f7 a4 55 66 2e 44 eb 0e bf 75 c9 9d 96 9a 69 a5 cf bf aa 77 55 5d 31 e3 b2 dc 48 82 58 6a 28 72 33 69 90 f1 4a 8a 15 4e 07 fc c4 82 b1 77 c8 82 de 03 f9 80 a5 94 2a 54 1c 25 24 b3 b6 4f c3 db f7 47 71 a8 5e 5b e0 9c 10 00 1c 72 3b e4 8d a3 39 1f 2f 6e d9 ea 5c 41 82 e7 95 7b fe bf 99 c7 1c 1c 13 c8 27 b6 46 7a 50 47 4e 00 0e 61 f5 e2 5a df 63 1e 8a b2 ac 0c 63 1f d0 f7 1c 93 df dc e7 94 f1 d2 81 c1 75 81 bb 04 e0 80 46 46 30 07 c8 9e 01 c9 23 eb ef d7 00 6d 49 e6 61 41 17 b8 07 ea 0f 23 e7 ec 91 9f 97 cf df ea 79 eb b0 a1 1d e2 3d b2 a3 f9 63 07 df 19 fa 7b e3 Data Ascii: S4HSV|&seYwryeRs~jZH9C/r)?jT~[FJ]UmUf.DuiwU]1HXj(r3iJNw*T%$OGq^[r;9/n\A{'FzPGNaZccuFF0#mIaA#y=c{
2021-10-29 15:22:59 UTC	123	IN	Data Raw: 3e e9 da 85 3d e5 a9 49 2a 0a 08 0a 59 ec 10 9c fa 41 c9 1d 5c 51 cb 4c 89 12 d0 d7 00 05 8d 5e d7 cc 5d 8b 0e 5a 98 6d 3d 0c bd 97 4a 89 12 d9 4a 29 73 31 b0 97 76 ca f9 3d b4 e1 11 3b 15 47 dc a8 a9 84 4c f8 54 89 3b 43 69 73 68 71 b7 41 48 f3 16 9e 10 94 90 06 46 46 0f 7e 3a 9d 53 26 5c a4 85 bf 59 8c 5d 26 c1 20 82 5c 07 2f b9 ad cb 7d de c1 33 51 53 25 3d 71 18 e6 25 89 16 37 05 99 fd 0f 8d a2 67 b5 ea 2d 30 b0 ec e9 25 29 da 41 0d 95 3e e1 20 80 1b 50 59 56 d6 dc 20 92 41 38 4f 3d c8 c5 04 e9 3d 60 59 94 97 4f ee 0e cc 7c 0e bf 68 fa 6b a3 35 26 50 90 27 ad 44 20 0c ee e4 0b 59 ec 1c 8b 5c 07 e7 17 23 4b e7 c6 7e ad 4f 84 a8 2d 4f de 1a 48 8e b0 76 79 6a 50 05 a0 b4 a9 25 1c 61 4a 50 50 e3 03 23 8e a9 97 29 49 51 00 e0 dc 46 87 ed 9e 7e 57 8f 73 d9 Data Ascii: >=I*YA\QL^]Zm=JJ)s1v=;GLT;CishqAHFF~:S&\Y]& V}3QS%=q%7g-0%)A> PYV A8O==`YO|hk5&P'D Y\#K~O-OHvyjP%aJPP#)IQF~Ws
2021-10-29 15:22:59 UTC	124	IN	Data Raw: e4 92 1b a9 45 65 72 9f 50 71 f5 a1 0b 3b 56 55 b5 c3 6d 5d 9c 8a fa 49 d4 73 12 3f de a5 4b 92 99 af 88 ca 29 58 57 58 06 a6 cc 53 6b 18 83 4f 35 52 42 16 8e c9 93 8d ef 75 83 66 39 33 06 b0 7c f4 31 6d 34 af 44 b4 6e 87 a7 d6 64 5b ba a9 5f 8b 79 8b 66 8e ed da d5 ad 52 a3 54 ad a6 6e 37 a0 b6 f5 65 36 f4 ea ad 85 1a a5 2e 86 99 ee 3e 29 32 2a 0d 33 35 d8 01 85 ca 69 a7 8a 9b 4f a1 6c 8a 1f c9 ec ca 2a 74 29 d3 26 9e 5c b0 40 62 c9 4b 5c 71 23 2b ee 8c 8e d1 9c a9 b5 75 0b 21 8a a6 39 0e 45 ed a9 df c5 ef 0f 29 fa 75 a0 2c 0f dd dd 1a 88 d2 92 92 47 90 e5 9c 8e 70 ae eb 72 cc 42 92 79 e4 64 27 b7 be 7a b1 29 3f d4 77 7b bc 40 05 5f d3 e7 0c d5 69 de 87 bb 2f cb 5d df aa 2d b2 a2 a1 e6 b7 2f 4f 9c 53 61 4a e4 86 97 66 a8 e4 72 a0 90 e2 89 19 1c 8c 82 d3 Data Ascii: EerPq;VUm]Is?K)XWXSkO5RBuf93|1m4Dnd[_yfRTn7e6.>)2*35iOl*t)&\@bK\q#+u!9E)u,GprByd'z)?w{@_i/]-/OSaJfr
2021-10-29 15:22:59 UTC	125	IN	Data Raw: a9 74 a7 29 32 fe 19 6d 40 ae 4a 96 b8 d1 a4 7b ef 40 3f 14 e7 74 b0 ae 87 6c 6c 29 bd 1e ad 5c b5 4c 91 d7 ce 4c ea 75 a5 2a 48 09 54 e4 b1 44 c9 84 f6 01 49 05 bb 44 38 7f 92 bf 1c 3f b2 45 67 e1 66 cb 4f 49 b6 0f 4a e8 7a 53 b2 42 04 da aa 15 21 34 55 f4 32 56 a0 25 d4 c9 97 2e 64 f9 55 12 4e 20 95 8e b5 33 12 56 3f 4e ca 6b 7f 67 6a ac 15 dc b0 e1 d5 2a 0b 6d 13 a4 90 83 4e 9b 4c a8 3c ee 5b 75 d4 a6 2b 33 55 08 37 21 d2 da 5b 6d 2a 7a 50 79 c5 a1 29 6d 79 0a 1a 7e 9a f4 8e 5f 42 7a 39 b5 fa 4f 5d 4f 36 75 2e c7 d9 ea ad 9f 4f 2f fc 75 84 cc 42 5a 58 f8 54 08 59 21 45 40 bd 99 8c 7c cb b0 f6 6f f7 e6 d1 a2 d9 34 ea 4c b9 b5 b3 3a 99 4a 5d 92 e1 24 92 a0 03 84 a4 fc 4c 1c 00 75 0d 1a 1f 69 57 74 c2 5c 68 ab 4d c1 74 87 5c 90 ba 63 49 f8 4b 45 cd f5 96 Data Ascii: t)2m@J{@?tll)\LLu*HTDID8?EgfOIJzSB!4U2V%.dUN 3V?Nkgj*mNL<[u+3U7![m*zPy)my~_Bz9O]O6u.O/uBZXTY!E@|o4L:J]$LuiWt\hMt\cIKE
2021-10-29 15:22:59 UTC	127	IN	Data Raw: d7 45 62 83 70 db 77 ad 72 4b c8 ac 4b a1 c1 45 36 0d 0e 44 0a 9b 34 cb a2 8c c9 a6 42 9d 45 9f 1e 6c 0a 55 44 c7 1b 1b 89 b2 44 64 c5 8c de e1 d4 d3 d5 03 34 4a 12 bb 6a 2a 2b 4c 94 61 56 bf 18 b9 70 33 1b b2 df 02 5f 5a b4 22 59 99 39 01 16 08 9c 57 66 39 17 20 83 bc 6f 8f d6 36 b9 69 05 83 26 8e 6a 92 29 cf 29 52 54 e4 77 64 18 c8 42 e3 a1 28 6d b7 b2 a5 94 29 4b 6d d6 d4 b5 29 6b 50 59 23 72 f8 51 08 38 42 4e 14 97 53 58 d8 f3 cb 95 9f ea 75 21 4b 18 5c 0c 9c a7 40 6c ff 00 ea c8 b7 08 b3 7a b3 e3 b3 41 e1 69 a3 30 24 bb 49 a9 b5 3d 72 21 b9 09 b7 22 29 a4 a0 05 b9 e5 3a 86 c2 d6 1b 59 5a 12 a1 e9 de a2 11 92 14 47 53 a7 cc 4f 56 99 7d 58 ba 7e 27 de 2d 66 ef 67 e1 ca 1c b9 0a 4c c3 db 2b 01 b0 96 cd cb b3 83 e4 de 11 4d 7c 16 6a 6e 97 df 7a df ab 53 Data Ascii: EbpwrKKE6D4BElUDDd4Jj*+LaVp3_Z"Y9Wf9 o6i&j))RTwdB(m)Km)kPY#rQ8BNSXu!K\@lzAi0$l=r!"):YZGSOV}X~'-fgL+M|jnzS
2021-10-29 15:22:59 UTC	128	IN	Data Raw: 4f 18 f9 a0 ef bb 12 c0 d3 c7 12 85 b9 bb 4d ad c6 bd 1b 54 a1 ff 00 9a 54 50 8c 85 2d 04 82 b5 84 e4 13 8e 72 41 cf 5c a1 73 28 67 98 56 9f b9 44 0f 4f 62 15 61 f8 37 b8 6d da e7 e1 f4 be 50 0f 8c bd 71 d6 9d 28 ac 58 cc e9 b0 6e 0a 2e 0a 7d c2 ed 55 f9 54 8a 65 56 47 9b 4d 7e 8a dc 27 84 13 e5 aa 23 08 42 27 64 f5 a5 78 bc a2 de 48 0c ed 5b aa e6 4e 47 c0 cc 4b 67 7f 0c b2 7f 1e 70 d9 32 e5 2c 1c 6f ea 33 cb 86 40 e7 7e 51 40 2a fe 21 fc 59 dc a9 5a 27 ea 16 a4 47 43 84 8f 26 de 7e 95 6d b6 73 b7 84 7e cf 9a 59 29 c9 07 85 a9 40 02 0a ca 46 7a 8a 99 95 4a 2c 40 6b dd ce 87 bf 4d 35 d1 f5 27 51 20 9f 88 77 fd 62 10 bf dd d4 9a d3 50 9e af ae f8 b8 24 3a 97 14 eb f5 da bc 8a ab aa 3e 6e 4a 94 ed 42 b0 fa c9 1c 91 95 11 b4 84 84 63 d4 38 a9 53 55 7c 6a Data Ascii: OMTTP-rA\s(gVDOba7mPq(Xn.}UTeVGM~/#B'J/ExH[NGKgp2,o3@~Q@*!YZ'GC&~ms~Y)@FzJ,@kM5'QwbP$:>nJBc8SU|j
2021-10-29 15:22:59 UTC	129	IN	Data Raw: 1c 9c 6f f0 8f ce 5f ed 7f 24 0f c4 6a 3a a5 0b 54 6c a9 4a 2b 48 b2 ca 16 52 6e c1 d8 d8 6e dd 19 1d f6 82 da 7a c1 73 42 b3 ef 5a e6 97 cb d2 ea 76 9d aa e6 b5 e5 11 75 37 7c d1 2f a6 35 ce ab 6c db 15 3a c1 b8 5a 8f 4e ab 53 6e aa 55 52 9d 47 52 60 dc b4 76 59 b8 69 b5 5a 83 94 ea 94 19 94 08 d4 7a ee d2 5a 82 64 cc 0a 42 8f 6a cc 31 64 0b f2 1c 5f 81 17 8f 92 d5 83 1a 14 82 ea 51 c2 d9 1d fc ae dc 21 8d e1 e5 72 6b fa ff 00 7e d3 62 15 15 35 4c 83 45 29 42 42 54 db a1 97 03 fb 40 da 00 41 53 78 48 f4 ef c2 c1 29 50 e8 09 49 23 11 60 17 f0 df 26 df 9e ee 7a 3d ec 70 42 16 00 72 c1 d4 33 b3 7d f5 1c 77 45 e7 d7 7b 96 95 6e 35 6a da f0 95 e7 54 e8 ad ae 4b 4c 21 58 4c 55 3b 1d 51 cb af a0 72 a2 b3 95 04 a8 ef 2a f2 d6 7d 1d 9d 35 46 5a 00 cd 86 9a 65 7c Data Ascii: o_$j:TlJ+HRnnzsBZvu7|/5l:ZNSnURGR`vYiZzZdBj1d_Q!rk~b5LE)BBT@ASxH)PI#`&z=pBr3}wE{n5jTKL!XLU;Qr*}5FZe|
2021-10-29 15:22:59 UTC	130	IN	Data Raw: e9 37 15 36 4c 2a 9c 7a d5 cc fb 33 69 b4 d9 11 dd 9b 6f 2c ce 6a a3 22 04 fb 6a a5 40 62 6b f3 63 b9 32 24 f8 cd 34 db 48 66 4d 4d c7 c3 83 cd 86 ed 60 59 ac d9 d4 ab d8 5f 96 99 27 a9 a6 92 89 55 33 a6 22 74 89 e6 99 08 55 24 d0 96 00 26 58 08 c4 50 06 30 a4 84 c7 d5 9d 18 fc 40 d9 f4 7b 08 52 d6 f4 af 6e ec dd a5 32 b0 a3 f2 e2 4d 0c ea 39 54 b2 4a 57 2e 7a 24 ae 4f 5a 67 a2 72 42 e5 95 4e 64 ca 63 77 b3 6a 93 e2 66 bf a8 1e 20 1c b8 f4 ef 47 f4 d1 84 a6 3a aa ad d7 ee b7 35 62 34 ef ba ea 11 e3 56 be 1e af 2a 87 aa f4 1a 6c f9 29 71 4e 34 ec 88 54 ea 3a 65 a6 27 c6 18 14 f7 de 54 76 41 b4 fa 3b b2 a8 b6 2c af ef 6a 55 6d 59 73 2a 11 51 f9 12 89 73 e4 4b 9a 95 9c 49 18 91 89 21 0a 04 02 fd a4 87 b6 51 6f 23 f1 d7 a5 53 ba 4c 27 6c 9e 92 ed 89 73 a9 68 Data Ascii: 76L*z3io,j"j@bkc2$4HfMM`Y_'U3"tU$&XP0@{Rn2M9TJW.z$OZgrBNdcwjf G:5b4V*l)qN4T:e'TvA;,jUmYs*QsKI!Qo#SL'lsh

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	132	IN	Data Raw: 8a 4b e2 03 0b 97 08 c6 ae bc 55 22 24 98 91 aa 29 a4 d3 ae 7d 45 34 8a 75 56 ae 78 54 c9 88 95 2d 4b 52 9a ca 0a 37 24 a5 d2 a6 b7 6b 20 f7 74 a9 bb 42 6a 24 49 ab ae 9b 2e 89 08 5f e9 cc 96 a2 95 02 c5 29 20 12 12 d9 05 32 88 f1 8e ab 29 9e 1b bc 5d 69 27 84 38 da 65 e1 c7 4e ed 7a 8e ab dd 14 31 6b 5c b3 28 17 6d 91 63 52 34 de c1 22 7a a3 db 16 44 86 5b 95 0d a9 54 da 64 b5 53 d8 5d b5 4e 88 b9 35 f9 cd dd 82 b1 1d fb 3e 9e dd da 0d a1 4b b5 ab 12 9f f7 75 fe 9c ae be 5a 03 2d 13 2a 12 02 65 19 8e ab 22 5e 25 ac 25 8e 23 67 49 00 c5 5e 0a 45 d6 4a 5c ca a9 29 a6 97 39 29 38 27 2d 5f a7 70 42 86 00 14 a2 2f fe 5b ef b6 63 6a cf 82 cd 75 b1 35 0b c3 c2 af fd 3e d4 3d 2b d3 36 2a 36 76 9f 4c bc 29 f7 06 99 33 12 8b 74 d4 3f 68 2e b9 4e d2 a3 51 2f fa c5
Data Ascii: KU"$)}E4uVxT-KR7$k tBj$I._) 2)]i'8eNz1k\(mcR4"zD[TdS]N5>KuZ-*e'^%%#gI^EJ\)9)8'-_pB/[cju5>=+6*6vL)3t?h.NQ/
2021-10-29 15:22:59 UTC	133	IN	Data Raw: 72 4b 17 3b a3 a0 3d 84 25 b9 92 ae dc 7d 00 fd 3b 93 ec 79 fa fc fb f5 d5 84 e0 42 95 64 e2 50 00 7f 53 b9 b6 96 f1 b1 d6 3a 12 95 32 54 e0 a7 11 2e fa 94 e1 66 7b 33 e9 df 9c 1a 12 15 8e 0e 3e a0 e7 23 1f 4e d9 c7 3f cf bf 54 bd 63 76 5e f6 e7 f7 f7 a4 4e 21 b3 b4 27 4e b9 e1 d3 1b cc 99 09 6c 8e c9 dc 09 5f cb 8c fb 1c 93 9c ff 00 a8 2a b6 ad 3d 02 0a e6 ad 09 b1 2c ab 92 c2 e1 85 f8 6f b9 8b 0d 9f b1 ea 36 84 d0 99 72 56 a7 20 32 41 21 89 cc 64 37 7b 11 1c 56 f5 44 84 94 44 74 24 60 8d c3 39 3f 2c 7b 7b e4 9c 7e 5d c0 eb cc 76 e7 e2 12 90 b2 8a 0c 29 8e 9e a0 3f 3f b5 df d4 ba 3f f8 69 d6 cc eb aa 10 a1 bd 0a d2 fb 9f e6 77 18 62 49 bf 03 9b 95 25 f5 38 4f 3e a5 2b 1f cb 27 9f 6f fa f2 3c cb 69 6d bd a9 b5 96 57 3a a1 4d 88 92 90 a2 3b 88 d3 d2 3d a7
Data Ascii: rK;=%};yBdPS:2T.f{3>#N?Tcv^N!'NI_*=,o6rV 2A!d7{VDDt$`9?,{{~]v)???iwbI%8O>+'o<imW:M;=
2021-10-29 15:22:59 UTC	134	IN	Data Raw: d8 ac ab 79 66 ad 7b 56 29 d6 dc 25 a0 a8 8f 35 9a 4d 29 37 4d d4 85 11 ff 00 d6 b5 7a 15 05 78 f4 f9 a9 e5 28 7e 25 b7 c1 dc df 76 81 99 60 3b 2b bc 1f b5 fc 63 30 be d4 bd 35 bc ea 3a 61 6d 6b 19 99 4c 9f 36 c6 9c ba 35 76 15 bd 43 95 02 34 7b 6e be 5a 50 98 f3 b3 ea f5 89 f3 d5 0a a7 1d ac c8 0e 40 60 22 4a d7 f0 0d 64 e3 31 d2 4a 43 3e 8d 33 93 2c aa 60 3d a0 2e 40 7c fe be c4 7a 2f e1 e6 d4 fc a6 d1 55 12 a6 84 25 49 05 89 b1 27 46 ef 6d 7d 23 9a 8a f4 a9 8e 4a 54 82 e2 8b 4b 71 6b 24 15 14 2b 9c 28 fe 03 dc 11 90 49 e4 e4 f2 7a f3 6a 89 72 92 a4 00 c0 96 60 2c e5 98 e4 cc ca df 9f 28 f7 74 2a 76 20 52 49 2a d3 3b 5d 8d 8f 2f 95 a1 ba fc d4 48 88 de 16 b5 6d 1e 58 78 ee 25 2b 41 21 2b ce 01 29 00 8c 0e 00 18 cf b7 50 a4 c9 4c b9 ab 49 1d a5 2b 18 19
Data Ascii: yf{V)%5M)7Mzx(~%v`;+c05:amkL65vC4{nZP@`"Jd1JC>3,`=.@	z/U%I'Fm}#JTKqk$+(Izjr`,(t*v RI*;]/HmXx%+A!+)PLI+
2021-10-29 15:22:59 UTC	135	IN	Data Raw: e2 d7 3e 97 8a c4 2e e1 2d 70 91 61 9d 85 b3 f0 87 ed 0e 2b 4b a3 b9 1c b8 e3 47 c9 88 ea 5e 6b 62 56 85 c3 7d 13 59 50 0e 21 c4 6d 05 8d ae 25 4d af 72 43 89 41 6c ad 0a 05 97 64 b1 cc 37 a0 88 d3 dd 4a 76 3f 6b 43 42 b9 6f ba 2a 4d 3c 26 a0 37 23 70 12 04 75 a5 c4 fc 4b cc 45 4a d4 b4 4a 4a 37 b2 1a 4b b9 0d 7a d0 08 1b 94 ad c5 e4 94 0c 46 c2 dd ef 90 ef dd e3 02 4b 85 65 ce 33 bb ed 2a d2 ed 4f d4 3f 0d 29 85 62 41 4d c1 5f b5 75 3e d3 b9 6a 14 78 0e 86 aa 55 bb 66 2d 3a e8 a6 d4 e8 91 98 92 86 9b 9b 50 5d 52 7d 19 70 e0 37 24 3f 53 97 4f 66 2c 44 bb 39 f6 18 78 a8 9e 10 a4 e3 18 41 23 b4 ab 0e 1c b9 b1 df 94 0e 64 b2 ef 2c e2 7c c0 d7 86 9d de df 11 bc 1f 58 75 ca e8 ab d7 e8 f5 6a 85 9b 57 b5 a6 1a cd 16 b7 1d d9 54 da 9d 1e e6 84 fa 57 11 71 f6 fc
Data Ascii: >.-pa+KG^kbV}YP!m%MrCAld7Jv?kCBo*M<&7#puKEJJJ7KzFKe3*O?)bAM_u>jxUf-:P]R}p7$?SOf,D9xA#d,	XujWTWq
2021-10-29 15:22:59 UTC	137	IN	Data Raw: ed b2 d2 dc ca 7d d5 56 9b 73 32 b8 54 84 43 69 d6 a7 d6 26 bb 4c a3 db b4 c5 44 92 97 61 ca 32 2b f5 15 c7 7e 33 c1 c8 0f b6 fb a9 71 0d c6 2e bb d4 d5 6c ba 6a 44 4d 4d 3c b4 e3 42 bf 48 25 82 70 35 c0 6d 48 27 0e 4e 40 72 c6 1f 5d d3 7d b9 b6 09 fc e5 64 b0 27 a1 29 98 a9 69 38 ca 8a 5d 4a 2a 7f 87 36 70 d8 98 c7 61 96 a6 8b f8 6c 91 ac 4e 48 d3 f9 31 2c 6d 3a d3 48 ce d3 6d aa 1d 32 4d b5 4d 83 32 fa 21 ba 4a 93 15 14 9b 4a 8b 0a 7a 68 ee c8 bd 96 dd 49 96 5e 7d d8 35 aa 24 67 65 a9 e6 83 c7 1d b7 2b 7a 4b b3 a5 2a 6e c8 a4 a6 a8 9c 52 a0 84 ce a4 aa 98 16 08 ed 19 86 5d 5c ae da 86 10 14 03 d9 e3 9b 3e 8b 62 6d 01 2a 56 d4 db 55 d3 51 2d 41 49 eb ab 69 e4 2d 4a cc a5 02 65 34 c5 04 1d 06 23 a0 7b c5 d8 b2 e8 d3 e6 56 e1 db 3f 74 c0 a8 5b 75 16 27 40
Data Ascii: }Vs2TCi&LDa2+~3q.ljDMM<BH%p5mH'N@r]}d')i8]J*6palNH1,m:Hm2MM2!JJzhI^}5$ge+zK*nR]\>bm*VUQ-Ali-Je4#{V?t[u'@
2021-10-29 15:22:59 UTC	138	IN	Data Raw: 58 c1 cd cd d9 af 9c 6c 64 56 0a 8a 6a f9 6a da 28 a7 98 b9 2a 4a 24 aa 8c cc 2a 38 4b 7e bf ed dc fe 59 c7 62 d6 4e a6 d2 2a f4 aa 4d 52 9d 50 83 3a 9f 55 8d 1a a1 4e 9f 12 54 69 b1 27 47 92 ca 5f 62 4c 59 71 d6 e3 12 98 7d b7 52 fb 6e b0 e2 9a 79 b5 a5 c4 95 20 a4 f5 eb 32 e6 4b 50 44 c4 9e c2 92 14 92 c1 36 29 dc 32 6c ad 1e 53 3a 54 c4 12 85 62 52 90 a2 95 16 25 cd d8 bf 28 5b bb 6f 98 4e 30 b7 5d 7a 33 7b 1a 48 2e 37 b1 a0 00 fc 44 a0 13 b9 64 9d ea 73 d8 6d 0a e3 03 a6 ce 99 98 49 7e f7 1b 8b 0f 1e ef 18 6c a9 4b 2b 1d 82 c0 df 46 6b 83 76 dd c6 d1 c1 07 db 15 a9 96 fd ef e3 73 53 6a 16 73 f0 e7 51 e9 74 8b 32 dc ad 55 21 94 b8 c4 8b ae 8f 48 0c 56 12 24 35 b9 b7 9c 85 1d 74 da 33 e5 2a 50 6a 5d 2e 43 0b 3f b8 50 19 da a9 61 4b 0a 7c 27 b4 4e b7 3e
Data Ascii: XIdVjj(*J$*8K~YbN*MRP:UNTi'G_bLYq}Rny 2KPD6)2lS:TbR%([oN0]z3{H.7DdsmI~IK+FkvsSjsQt2U!HV$5t3*Pj].C?PaK	'N>
2021-10-29 15:22:59 UTC	139	IN	Data Raw: d1 9a d9 8a 9b 29 e4 05 e2 48 c2 5a ee da 6e 6e 2f 0e 8a ab c0 d1 6b 20 9c 7f e4 f5 2e 78 1c 18 4f 0e 07 7f ef bf 1d 68 14 5d 0b 0c c1 21 98 7b b6 51 88 0a 52 a6 e2 29 c2 08 b0 16 cb 3f 95 b9 86 df 8c 8e d4 b7 53 65 f2 49 55 2a 40 20 13 93 be 22 d3 93 b4 8d db b2 9d a0 e7 8c 9c 75 09 5f 02 ff 00 d2 7d fb e5 13 3f 74 af f5 0e fc a1 76 ca 9e 61 e9 2e 8f a9 2a 52 02 ac d8 ca c2 55 ca 8b 35 b6 0e 14 06 70 06 37 8c 6d 39 c9 50 e0 76 88 7e 90 3f e7 f0 33 f7 8e 74 74 fd 0f 0e 3d de 31 4d 3c 70 56 8b ab d2 f2 56 9f 4f ed 78 c9 29 ca 41 36 c2 73 92 0f 3c 23 8f e2 03 91 8e 3a 75 66 5d e3 e5 00 92 9e df 32 7c 62 90 46 9e 15 e5 92 b3 92 71 ca 95 e9 0a 29 09 cf a8 61 20 61 c2 00 fc 19 ea 1a 3e 1e f3 06 c0 74 23 df 8c 79 b8 65 ff 00 bb c1 dc 4f e1 73 81 b5
Data Ascii:)HZnn/k .xOh]!{QR)?SeIU*@ "u_}?tva.*RU5p7m9IPv~?o3Ttt=1M<pVVOx)A6s<#:uf]2	bFq)a a>t#yeOs
2021-10-29 15:22:59 UTC	140	IN	Data Raw: a1 a7 1b 8c dc a7 10 a6 15 37 a3 5b 22 b7 6d 55 22 74 e4 ff 00 b9 a1 4f 34 a8 31 20 1b 82 fe ef a1 8f 1b fe d0 3f 8a bb 0f f0 bf 66 54 6c 4d 87 58 89 dd 28 ae a6 99 26 49 94 a1 d5 50 d3 ad 05 0a 9a c9 2c 16 c7 08 20 38 50 30 8d 68 6a ed 1a f3 85 57 99 a3 76 8c 8b a2 2d ba e4 e8 b3 66 d5 64 ca a1 41 81 36 13 8a 43 b0 02 97 6f 55 eb ec 55 25 a9 0c 9a 54 1b 36 81 5e 69 2e 21 6d 09 49 52 64 3b ec 72 e9 e4 53 84 c9 94 a2 64 80 02 13 a2 40 f8 80 07 43 cb 5d f9 7e 5b cf 9f 3e 74 c9 d3 a6 cc 54 c9 d3 66 2a 7c d5 cc 51 54 c2 a9 ea 2b 38 94 6e 4b 9d 77 b6 65 a2 39 f1 05 a7 1a d1 54 b5 aa 97 23 d7 65 db 65 5b 72 67 c2 ad dc ca af 37 a1 89 6e 15 88 e0 9f 58 62 25 cf 26 d3 b0 a2 6b 1c bb 05 0e 45 8a c5 4d 98 97 3d 6e f1 97 1a 21 72 65 8d 71 c3 91 2d 99 45 52 e4 96
Data Ascii: 7["mU"tO41 ?fTlMX(&IP, 8P0hjWv-fdA6CoUUU%T6^i.!mIRd;rSd@C]~[>tTf*	QT+8nKwe9T#ee[rg7nXb%&kEM=n!req-ER
2021-10-29 15:22:59 UTC	142	IN	Data Raw: 84 02 4a 91 31 ca 84 80 2c 5c b2 8f 26 e1 c7 30 d0 fa 87 21 e7 59 42 95 51 91 b5 4e 0c 2a 42 94 ae e4 01 ca ca d4 73 90 48 48 f6 05 49 1e d9 9a d9 95 a0 2a f5 09 1b f1 aa cd f5 61 61 9c 4c ea e5 28 00 7a 95 3c ca 52 81 8b ea c3 56 68 65 5e d2 d0 c3 ac a1 fa 9f 96 a2 d8 21 04 b2 81 b3 b6 42 78 18 51 e1 40 13 90 90 a3 ef d7 9d 6d bd ab 5b 2a 60 0a 9b 52 45 8b 99 8a 60 06 59 28 72 d2 27 c9 a2 90 41 29 90 90 46 5d 90 cf a3 86 3d f9 f1 8f 56 c1 0e b0 54 cd 42 9a f3 4a 75 0d 95 c9 6a 2b c7 93 92 16 95 36 06 02 7f 13 84 93 9e 54 01 c1 56 87 a3 55 f2 ea 50 9e ba 69 2e d9 cf 5b ff 00 e4 1b 22 3b ef 14 7b 4a 45 62 26 1e a7 a8 07 4e c6 5d ed 98 7c b3 b5 f7 88 cb c4 de 96 e8 d5 56 8d 27 54 ab 13 6e cb 2f 52 ec 8a 4a a7 d3 b5 2f 46 ea aa b3 ef 68 89 a7 45 99 22 04 2a
Data Ascii: J1,\&0!YBQN*BsHHI*aaL(zRVhe^!BxQ@m[*`RE`Y(r'A)F]=VTBJuj+6TVUPi.[";{JEb&N]	V'Tn/RJ/FhE"*

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	143	IN	Data Raw: 4b b9 ae 84 a9 5b 90 b6 f7 a5 66 b0 97 10 d2 55 82 86 d0 56 92 90 52 a0 90 91 9d 17 47 ea ea 6a 42 51 3e a5 73 c0 4e 20 85 2f 1b 14 90 01 60 49 17 24 6e d5 e3 1d d2 8d 8b b3 e8 90 67 53 ec f9 12 14 b5 02 54 89 78 49 49 72 c4 e5 c5 af c7 74 1d f1 2b 6a dd b5 4b 96 91 16 65 4e e0 9b 49 8f 39 89 12 69 b2 ab 97 34 c6 9c f8 76 25 25 29 52 25 55 5f 8e 30 e3 c8 71 38 69 00 24 0c 2c 63 06 f3 6b d3 54 f5 66 6c a5 36 04 13 67 dd a7 d7 27 3c 22 87 61 1d 9f 33 1c b9 b2 50 1c b3 e1 76 e4 de 66 22 9b cd 54 17 34 0b 50 6d 75 5a d2 13 25 aa 5d 21 ba 5a dd 9d 39 e8 ed 49 f8 b7 d4 e2 d5 15 f7 d6 d3 cb 53 51 e3 a1 41 4d 38 b2 23 e5 4a 42 4a 55 d6 69 1b 5e 52 36 3d 54 99 80 99 c1 44 12 c3 3b be 7a 5f bc 86 d2 34 23 61 26 6e d3 92 b9 60 75 2c 2d a6 9b ad 6b 9f 9d a2 8d 69 77 Data Ascii: K[fUVRGjBQ>sN /`I$ngSTxIIrt+jKeNI9i4v%%)R%U_0q8i$,ckTfl6g'<"a3Pvf"T4PmuZ%]!Z9ISQAM8#JBJU i^R6=TD;z_4#a&n`u,-kiw
2021-10-29 15:22:59 UTC	144	IN	Data Raw: 00 d8 8c 9b 71 3a 7c a2 e6 94 2b b2 12 2c 0f ce e4 b7 9f 16 87 74 0a c2 df 47 92 1d db 80 09 19 3b 81 e3 bf 7f 6e 79 cf b8 ed da 3c c9 58 48 c2 2c 45 dd ae 47 84 6a e8 e7 85 a7 0a fe 24 90 06 ed ff 00 38 70 53 56 b7 42 f7 3e 48 48 3e f9 ce 30 71 fa e3 e7 f5 e3 a8 d3 42 92 05 b5 f1 e1 c3 37 7e 11 70 84 2c 80 40 b6 fb db f8 e5 68 53 43 8e 20 2c 28 15 05 67 0b ee 40 20 67 8e fc f1 f4 fc fa 6a 0a 8b 66 da f0 ef f9 3c 4a 12 54 b0 ca 0c 0e ac d6 fb fb d1 c8 88 81 01 4f 25 05 45 67 24 1e 76 9f f1 e3 8f a0 ff 00 09 72 e6 61 1f cf cb 99 10 74 d3 a1 39 0f 7e db 7c 16 94 a5 84 a5 19 23 00 71 fe 1c 9e dd b8 3f a7 63 d1 90 1e 60 5d f3 6f 1d 33 dd 9e 7a 43 67 53 e2 d3 c7 4e 5b f7 72 e2 2e 6e 9a fb ad 1d 6e 66 31 83 90 7b 91 cf 3f f4 ea d2 52 8a 4b dc 02 a7 ee d0 eb cf Data Ascii: q:|+,tG;ny<XH,EGj$8pSVB>HH>0qB7~p,@hSC ,(g@ gjf<JTO%Eg$vrat9~|#q?c`]o3zCgSN[r.nf1{?RK
2021-10-29 15:22:59 UTC	146	IN	Data Raw: ea be a2 30 c5 06 95 43 b9 ab b3 a7 b9 19 f6 5a a5 5b b3 9f 7e 43 e8 71 59 63 cc 8e c2 90 a6 12 19 9c a4 e1 25 45 04 9c f5 99 a3 e8 9d 7a 67 28 d3 ec d9 fd a7 09 50 42 88 4b 96 7c bb db b9 84 7a c7 ff 00 69 3d 19 a5 a6 42 f6 8e d9 a4 a6 b0 21 7d 6c ae d1 67 ed a5 dc 03 9a b2 71 c7 3b 1b 63 68 3d ce 5b 8f 22 e1 14 7b 7d a9 09 4a a5 4b a9 4e 65 f5 29 2e 24 3a d2 9b a5 52 64 3b 2c ad 41 5e 6e 5d 2c 25 c2 39 03 90 a8 e8 f6 d7 aa 9c 9e b2 6f e5 c4 81 d4 9c 4e 3b 59 5c 13 98 f6 ed 19 5e 90 7f 69 df c3 9d 81 4e 51 4b 52 bd af 5e 01 64 d0 9c 52 49 16 67 4b a7 95 fc 6e cb 1a 81 72 69 4f 87 6a 22 ee a9 2c 55 ae 17 5e 89 53 70 d6 aa 70 9b a6 c1 8d 51 82 c2 5e cc 3a 1b 8e 3c d9 a7 b6 b5 c7 32 2a 13 e7 cc 94 ca 94 54 dd 2d d4 f2 8d cf 46 7a 23 45 d4 52 ba d9 Data Ascii: 0CZ[~CqYc%Ezg(PBK|zi=B!}lgq;ch=["{}JKNe).$:Rd;,A^n],%9P=IoN;Y\\^iNQKR^dRIgKnriOj",U^SppQ^:<2*T-Fz#EMR
2021-10-29 15:22:59 UTC	147	IN	Data Raw: e3 53 55 d5 a0 5e 16 f5 67 55 15 01 13 e5 db 96 9b 0c 53 e9 92 96 e4 66 67 d5 e4 cf 45 06 9f 05 d7 c3 4f 96 14 fc b9 d1 d0 95 b9 19 f0 d3 c5 1e 63 2e e3 c9 54 e4 a0 ce fd 39 73 93 85 7d 92 5c 10 01 b0 cc b7 88 d3 84 67 96 b6 4a a7 e1 aa 0a 43 b8 9d 2d 68 49 c2 72 4e 20 01 e1 9d b3 8e 75 f4 d7 c6 af 87 2b 9d d8 30 f5 e7 c3 9b 51 27 79 84 39 78 51 53 1a a9 29 69 75 c7 5c 5c 8a bc 68 9f 76 cf 94 f0 79 6e 38 a7 98 2e b9 b1 45 26 22 92 31 d2 56 cf 9f 2d 38 13 52 8b 68 14 2e 0b 0b 97 dc ed ae f8 8e 2b 50 55 8a 64 a2 01 b1 71 98 3e c5 c3 e7 78 d2 2b 7a c8 f0 27 ac 76 95 bb 52 b6 ad fa 05 d1 44 b9 2e fa 4d 99 e6 5b eb 66 9d 71 5b 15 aa c8 02 3c 8a c4 35 b5 16 a9 4e 66 2b ae 47 53 80 e5 d9 2c 3a a7 e1 09 de 52 db ea 01 13 10 bc 2b fa be 6f 7f 7b cd a2 78 9c 99 89 Data Ascii: SU^gUSfgEOc.T9s}\gJC-hIrN u+0Q'y9xQS)iu\\hvyn8.E&"1V-8Rh.+PUdq>x+z'vRD.M[fq[<5Nf+GS,:R+o{x
2021-10-29 15:22:59 UTC	148	IN	Data Raw: b4 3d 32 db 73 56 d3 2b e6 e7 b8 e4 07 1f 16 72 49 d6 18 0f 45 bf e9 b3 69 6f 2b 58 b5 59 b3 46 6c 44 a5 34 dd cc f4 96 e2 c6 2d 94 a1 94 84 37 31 c6 e3 bc 18 60 b8 ea 95 e5 22 e6 55 36 d3 8b dc 0a 9b d8 53 ed 0a 8a 79 12 28 41 4c a9 14 f2 91 22 4a 50 c9 4a 25 cb 01 09 4a 43 d8 01 60 03 33 01 68 ab eb a7 4e 9b 31 7d a9 93 a7 4c 33 96 55 22 5a b1 15 1c 45 4e 6e 49 b9 ed 5c e6 46 71 e2 d0 95 a9 76 e5 7a 7d d3 46 d6 0b d6 91 32 73 8e a6 6c f4 cd 2e 16 4b d2 9e 2b 5b e6 4d 3a 51 4d 49 f6 57 15 97 94 d3 08 67 6b 7b d8 69 b2 e3 ab 70 f4 db 5e b3 6f 4d 5c ca 6a 84 f6 92 1c 62 7c f3 cc f8 f8 42 da 35 4a ae 94 99 55 b2 95 39 12 d9 28 40 96 01 4e 17 04 e1 4b 8c fe e0 c3 72 f8 d2 2a 86 a8 55 93 59 b9 75 4a ec b9 aa 5e 70 f3 9e 95 76 25 99 11 de 42 d4 3c b7 54 dd 32 22 Data Ascii: =2sV+rlEio+XYFlD4-71`-6Sy(AL"JPJ%JC`3hN1}L3U"ZENnI\Fqvz}F2sl.K+[M:QMIWgk{ip^gM\jb|B5JU9(@NKr*UYuJ^pv%B<T2"
2021-10-29 15:22:59 UTC	149	IN	Data Raw: 34 84 b6 d1 97 32 97 16 4c a2 d3 25 4a 2d b6 64 ba e7 96 d9 52 fc a4 e1 b0 a5 04 75 eb 54 cb eb 69 e4 cd 26 f3 25 85 ab 81 3d c3 bb 84 79 a4 e1 d5 54 4d 94 18 09 6b 28 4f 14 8b e5 cd f8 c2 d0 74 9e 47 d7 fa 8e 7b 01 c9 f7 fe 7e dc 9a 38 b2 08 0d f7 f7 ef 98 2e ad 5e c4 e4 72 3e 43 f2 00 64 9c fc fe 5c f4 a0 70 92 f2 c8 27 1d b0 49 27 39 4e 7b 9e 7d f3 c8 c0 3c f2 7a 50 49 7a f7 7c e1 35 e5 28 e4 64 01 9e 78 c9 e7 24 1c f6 c8 c9 c6 33 93 83 f9 28 24 25 3a ac 11 8c e3 90 30 01 ee 73 8c e0 e0 8f 74 e3 8e 39 e9 42 8c a9 7a b6 9d c5 00 f6 f9 77 e4 e3 fc f8 e7 8f cb af 8e 57 2d 4a 18 c9 cb 3d 6f 9e 59 65 73 bc ef d7 ed 74 95 04 8c 0a 29 cb 2b 73 f7 cb 48 4e 54 b4 38 ee e7 4f 1d c6 4e 3f 3f f4 e7 fa f4 02 c9 b3 03 c7 51 ef bb 94 4c 94 d6 c5 73 6f 8b 3e 3a 67 ed Data Ascii: 42L%J-dRuTi&%=yTMk(OtG{~8.^r>Cd\p'I'9N{}<zPIz|5(dx$3($%:0st9BzwW-J=oYest)+sHNT8ON??QLso>:g
2021-10-29 15:22:59 UTC	151	IN	Data Raw: 27 2b 23 1c 24 81 c0 39 e5 f2 80 0b 4b 5a fe b0 29 a0 29 04 9d de 3c 3e 71 a0 92 3c a7 82 1b 90 db 2f b6 b4 21 25 a7 50 87 9b 56 47 62 87 12 b4 2b b6 33 8e de e3 a9 aa 4a 57 f1 80 ae 60 18 88 85 2a 53 75 6b 5b c6 2e 30 2d 49 63 dc 44 35 66 e9 ce 9b 4f 7c 4a 9f 60 59 72 e4 83 bc 48 91 6d 51 dd 78 2c 00 42 8b 8a 86 54 54 08 49 dc 4e 73 d8 f5 19 74 54 93 3e 3a 79 4a e6 91 16 b2 76 f6 d9 a6 49 4c 8d a7 59 29 3a 84 4e 58 f9 c4 72 f4 7a 65 1f c4 4e 95 41 a4 c0 a7 d2 e2 fe cb d7 9d 54 6a 7c 46 21 c7 70 22 ad 4b 4e 4b 31 d2 d2 54 a4 a7 01 25 49 dc 13 90 08 e9 d2 a8 e9 65 1f d2 a7 94 9d 2c 91 78 8f 37 6b 6d 4a b9 2a 55 4e d0 ad 9c b0 bb 15 d4 4d 24 5b 36 7d 78 8d 7b e3 2c 68 34 69 13 a8 50 54 dc d7 a3 a0 d3 20 38 fa be 0a 9e f3 e1 d6 e1 b2 96 f0 93 1d e2 0e e4 f2 Data Ascii: '+#$9KZ))<>q</!%PVGb+3JW`*Suk\.0-IcD5fO\|J`YrHmQx,BTTINstT>:yJvILY):NXrzeNATj\|F!p"KNK1T%I e,x7kmJ*UNM$[6}x{,h4iPT 8
2021-10-29 15:22:59 UTC	152	IN	Data Raw: e8 d3 69 36 b9 a3 6a 3d 12 e9 aa 55 dd ae 26 9b 16 a7 36 5a 69 d0 26 4a ab a2 9c cb 54 78 10 d0 ea 8c 8a 8c 74 a9 f8 ba 5d 9b 46 76 7c c4 aa b2 a5 44 4e ec 4b 96 a5 76 42 d4 32 4d 86 f2 da db 94 64 3a 4f d2 79 1d 20 a7 14 94 3b 3e 4c b1 4d 33 ae eb 12 84 a4 99 49 37 c9 9c 6a c7 36 de f1 41 74 e3 51 b4 66 a5 4b 81 4d b9 74 32 dc d4 2a d2 27 c6 fb aa 93 48 b0 29 d5 6a 93 b4 46 e1 43 8e cf df 15 06 52 dc a5 48 91 21 99 8f be b5 48 7e 63 a9 7f 70 2d 24 b4 b2 f9 d2 aa 25 cd 98 7a e5 90 bf 82 e6 c3 fc ba 5f 3d d7 06 31 e0 ca 98 80 85 49 48 50 de 3b ef e7 71 7e 31 a1 1e 1b ac ed 3d 37 6c 59 d6 77 87 88 5a 4b 59 ae cd a7 47 8f 26 ad 0a a3 4a 86 d4 a8 d3 57 2d 12 a2 d3 2b 75 ba a4 15 c9 a5 30 a7 9e 44 d4 d3 5a 5b 11 db 5b 22 5b 67 6e 63 cc 54 f5 19 69 38 94 ea 00 Data Ascii: i6j=U&6Zi&JTxt]Fv|DNKvB2Md:Oy ;>LM3I7j6AtQfKMt2*'H)jFCRH!H~cp-$%z_=1IHP;q~1=7lYwZKYG&JW-+u0DZ[["[gncTi8
2021-10-29 15:22:59 UTC	152	IN	Data Raw: 0c b0 9c d0 92 ce 7e 9d cd 97 11 1b b5 64 d2 5f a7 14 a5 8b 86 65 72 2b 51 8a 22 c7 9b 2e 97 20 c7 f5 b6 e0 f2 65 25 2e d4 18 6d b4 87 19 f8 57 24 c9 87 b0 b4 18 62 2a 59 1d 5d 4a 94 52 0a 14 b7 01 99 f3 b0 fa 58 0c a2 0c c5 cb 24 14 20 02 f7 61 bb d4 9d fe 0c c2 33 77 c5 05 93 4c b1 f5 0d 88 54 fa 34 44 42 95 0e 5d c7 19 a3 0e 23 8f c7 5d 7e e2 ac ca 79 a8 af 49 94 d9 82 94 48 54 ad a9 69 b7 58 73 73 8a 61 68 04 05 79 ef 49 e4 61 ad 43 e4 64 a4 f8 ad 7b b7 37 7f 7d b7 1b 02 6e 3a 15 37 fe b2 81 ff 00 b1 1c f7 c4 14 b6 a9 bf 06 a9 c4 d3 99 6d 4d 95 06 5d 98 d9 5c 77 1b 77 73 a0 47 87 54 66 4a 7f 74 56 86 19 4b 81 5c 07 d0 1d 4a 12 d8 ce 28 32 12 05 f3 d3 21 cf f8 8b 96 0e fe fd da 13 59 a8 24 2d 80 58 f2 d9 5a 9b 5b 5e 4a 66 3e 5d 42 55 b5 0a 4a 9e 96 87 Data Ascii: ~d_er+Q". e%.mW$b*Y]JRX$ a3wLT4DB]#]~yIHTiXssahyIaCd{7}n:7mM]\wwsGTfJtVK\J(2!Y$-XZ[^Jf>]BUJ

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	153	IN	Data Raw: 87 bb 8f 9c 71 32 d6 d8 0b bd df d8 1c 7d 77 44 4d 56 ac 32 b5 b2 c9 83 41 4a dd 4c 82 f3 ca 75 9f 2d d3 b5 c5 2c a0 84 a9 61 4b ca 70 3d 43 cc 01 0a 6b 68 52 d4 09 cb 94 1c 8c 61 47 41 2c 29 b2 cb b5 da cb d7 8c 4b 95 4f 38 04 e4 cd 67 cb 2c cd b5 19 73 b1 84 99 95 2d 8d c7 43 0d 42 5c 70 ea 54 59 1f 02 ea 12 b2 a4 f9 89 69 66 2e 79 01 49 6d 4b 47 20 a5 2b 5a 82 94 a4 d7 8a 89 01 67 ac c4 6d fb 92 52 45 b5 1e 16 d7 38 95 d4 4e 56 4c c3 95 f8 6e cb de 50 c9 5d 41 cf 88 4f c7 53 55 2d d5 b8 e8 8e da a5 c2 78 79 23 e1 d2 b7 16 96 9b 20 fe f3 72 92 e7 c3 b4 1b f3 12 94 a0 25 45 6b 0f 5c 92 b3 d5 92 90 5b 22 47 2f 3e 25 b7 e7 05 12 96 03 2e db 86 79 67 ef 56 84 69 53 a3 94 e0 d3 fc b5 04 b8 a5 0d d1 92 84 24 2c 84 92 e0 8d b4 fe ec 9c 24 ba 16 ac 7e ef 60 e0 Data Ascii: q2}wDMV2AJLu-,aKp=CkhRaGA,)KO8g,s-CB\pTYif.ylmKG +ZgmRE8NVLnP]AOSU-xy# r%Ek\["G/>%.ygViS $,$~`
2021-10-29 15:22:59 UTC	155	IN	Data Raw: 12 c0 7c 2e dc 7d 93 1f 98 fd 33 d8 b3 36 2e dc ab a5 32 8a 09 9a b5 25 d3 62 90 48 e0 3e 45 bb a1 1e f6 9a 96 34 97 42 9a 20 6d 72 ca aa 29 01 24 15 02 9a ec d0 72 72 7e 98 1d f8 c7 1d 5e 4a ec a0 24 64 95 38 7f 7c 63 1b 38 62 20 ef cf bb 76 7b e3 3f bc 44 51 2f 3b ba e0 b2 69 f6 8d b3 59 b8 9f 6a 1d 75 c9 2a a7 43 75 d8 b0 3c f9 14 66 9a 5d 46 6a 8b 74 fa 7b 4a 5a 17 b1 c9 f2 59 4a b0 e2 93 bc 34 a0 41 52 85 cc c8 38 cc b6 76 7d ef dd 1d 96 ac 1e 97 7f 7d e4 c0 16 6b 85 8b 9e aa 1b 93 7e 5d 90 6d f6 3d 0a 72 8f 6d b4 8a fd 54 b7 81 86 1e a8 ba 63 50 e0 3c 48 29 2f 46 55 c0 41 e4 34 0f a4 f6 5d 2a b5 b3 e7 dd c5 9b c1 f9 c3 95 36 5f ed f3 3d cd e3 ac 5c cb 07 44 34 aa cd 0c c9 a7 5a 90 aa 55 26 8a 54 dd 66 e7 f2 ee 3a a3 6f 15 1c 39 1b e3 da f8 0a 72 fb Data Ascii: |.}36.2%bH>E4B mr)$rr~^J$d8|c8b v{?DQ/;iYju*Cu<f]Fjt{JZYJ4AR8v}}o~]m=rmTcP<H)/FUA4]*6_=\ D4ZU&Tf:o9r
2021-10-29 15:22:59 UTC	156	IN	Data Raw: db 67 11 90 9a 93 eb 69 28 8e fa ca 1c 8b 1e 3a 50 b9 12 9c 0a 44 48 ce 39 81 d5 7a 36 6c e9 6a 21 b0 83 a8 0c 74 bb bf 87 a4 4c 5e d4 91 3d ef 7d 03 90 e7 4b 35 e2 d0 dc 7e 0a 95 a6 57 e4 ab 1b 54 aa 8c 35 52 8d 06 81 56 6e 3d b9 b5 14 f9 b4 fa e4 26 a5 c5 7a 1d 52 73 2c 3a ea 23 3c e4 ba 64 bc 40 42 13 3e 9d 35 96 96 bf 20 2d 64 34 eb 95 9b 93 ab dc 9c ce eb db ef 78 02 eb 6c 00 61 96 85 ed a3 3d f4 fa 08 b9 ba 67 a5 5a 7b 40 5c 4a 35 ab 6d d2 a1 a8 36 97 27 d5 1f 8e 8a 85 55 e6 3c f6 5c 43 6e 54 e6 7c 44 a4 05 f9 e8 0a 65 89 08 65 38 46 d6 d3 e5 f4 31 24 15 62 38 87 7f 1c be fc b8 43 26 cd 33 13 88 ad 4f a3 1b 13 a7 86 83 48 92 f5 fe 8b 6a 5e 16 0e a0 35 5b a0 d3 6b 14 0d 3e b6 df fb 90 4b 1e 59 8b 76 c9 68 33 16 4d 2a 63 09 32 60 3f 05 29 0e 3e b8 4b Data Ascii: gi(:PDH9z6lj!tL^=}K5~WT5RVn=&zRs,:#<d@B>5 -d4xla=gZ{@\J5m6'U<\CnT|Dee8F1$b8C&3OHj^5[k>KY vh3M*c2`?)>K
2021-10-29 15:22:59 UTC	157	IN	Data Raw: ec ff 00 78 37 1f cb 9b ee fd e3 ed 76 80 a7 a5 92 0a 88 34 76 1b ab 3f ff 00 8b 9b f9 6f 85 d1 a9 ba e0 d2 90 a6 2b d6 2a 5b 69 2e a5 2d ae d7 b9 88 57 9a 92 94 e5 7f b7 21 60 b6 14 50 12 81 e5 a9 28 48 71 84 a0 a4 06 1e 89 03 da fc f0 26 d9 d3 9d 46 8e bb f2 1c 98 44 9f f6 b2 4e 94 5b b2 ac 6e 45 fa 90 fe 39 c7 a8 9a bf ae 31 10 db 72 2a d6 64 f6 d0 56 e6 55 43 b9 e2 02 a5 a9 0a 2a 08 62 f1 5a 13 b8 6f f3 12 94 ec 57 9a b5 24 27 80 42 7a 1f d6 93 8a b9 20 68 d4 e7 75 ff 00 79 e6 43 ef d2 0b 2f a6 54 f2 d2 bc 5b 3a 62 8a 75 4d 50 50 62 c7 3c 03 5b 43 c2 3e bb 6b 1e c2 86 da b1 c2 b6 36 94 96 da ba 10 b0 84 24 25 78 28 ac ab 6b 6f 6d 4a b6 7e f0 82 94 f9 85 dd a9 48 18 e8 3c c5 9c 49 da 00 01 66 fc a9 53 bd ee f3 13 f6 f4 e9 e9 a5 36 14 94 ec b9 c4 1b 9f Data Ascii: x7v4v?o+*[i.-W!`P(Hq&FDN[nE91r*dVUC*bZoW$'Bz huyC/T[:buMPPb<[C>k6$%x(komJ~H<IfS6
2021-10-29 15:22:59 UTC	159	IN	Data Raw: 65 6b c8 95 f8 61 b5 49 48 35 14 41 bf a4 cd 19 b6 85 17 f4 d0 c1 d3 d3 9d 99 9e 1a d2 ff 00 fa 92 d0 1b 96 19 8a 3c ee c3 48 27 2b c6 5c e7 1b 29 63 4f e4 12 76 6f 71 55 6a 68 de a2 12 14 91 ff 00 96 85 a4 05 20 79 6e 07 b7 24 64 28 64 af a9 28 fc 32 da 21 0c ba aa 66 cb b2 ac 45 f7 dc 07 f9 72 81 9e 9d ec dc 5d 99 55 02 e4 76 80 03 8d c1 39 f1 0d a6 56 86 e2 fc 60 38 87 14 e4 8d 3f 98 b5 2f 8d cc d7 e1 a5 68 c7 e2 19 2c 7a 90 46 7b a4 fe 10 96 c2 40 1d 71 5f 86 3b 4c be 1a 99 24 6a e3 86 fc b9 67 cb 7a 1d 3c d9 c3 29 73 15 ba dd a7 3c 2c 1f 9d a1 fd a7 7a 85 ad fa d3 12 b5 27 4b bc 35 ea 8d fb 12 85 26 2c 5a c4 cb 72 55 9b 36 3c 27 ea 09 97 26 1b 44 cd aa c3 79 b7 24 31 1d f5 34 36 fa d0 d3 88 70 24 a9 20 b5 3f 87 1b 4d 07 fe 26 99 ed 99 3d da 7f 10 d3 Data Ascii: ekaIH5A<H'+\)cOvoqUjh yn$d(d(2!fEr]Uv9V`8?/h,zF{@q_;L$jgz<)s<,z'K5&,ZrU6<'&Dy$146p$?M&=
2021-10-29 15:22:59 UTC	160	IN	Data Raw: 92 5b a9 3d a5 94 21 ed da 51 be f2 de d9 c5 32 d5 27 1e 8b a5 5a 0c 9d be b6 2d 1a d3 44 1e 14 a5 fd fd 38 14 0e 78 da 46 49 03 3e a2 af a0 f6 19 6b 1d 5a 57 a2 d8 86 be 76 17 68 f8 f9 72 ca 4a ca 81 0a 42 ca 70 31 0d 84 ef d5 af a7 d9 83 4e 94 3e 1c 30 95 e5 6b 70 2c 8d c4 20 3a af 49 3c 63 d4 80 4a 01 1b 95 80 a3 ce 7a 92 80 ff 00 b5 c3 8b bb 7d 8c 00 94 bd fb 2f cb ed 0f 48 21 06 3c 95 87 52 84 32 df 99 2a 51 52 59 66 13 41 19 5b d2 df 70 21 98 b1 d0 71 b9 e7 d6 db 63 80 a5 8c ed 53 d4 a4 27 35 0f 1f 67 c4 0f 0b c0 42 41 d5 cf 87 8e 70 91 6e dd b4 aa 65 32 7c 8b 09 8a ce a7 c6 54 c7 45 56 fd a9 5c f1 a8 da 5d 06 6b 2e 2d 0e 42 77 56 ee f7 e1 d8 b3 64 42 09 53 26 cf d3 26 ae bb 9d 08 65 45 bb 5e 64 94 ad 64 3f 99 96 1f b2 fc 7d f9 6b 05 4c 82 5b d1 b2 Data Ascii: [=!Q2'Z-D8xFI>kZWvhrJBp1N>0kp, :I<cJz}/H!<R2*QRYfA[p!qcS'5gBApne2|TEV\]k.-BwVdBS&&eE^dd?}kL[
2021-10-29 15:22:59 UTC	161	IN	Data Raw: 23 12 ca 1c 57 9c 88 75 3a 65 41 f8 ac 25 b6 59 8a 2a f3 1c 69 b6 9b 9a 14 cc 09 92 ec 4b e2 3c 03 79 fd b9 c4 e4 cc 1a 39 6d 5d af cc 88 a8 7a 4f a9 91 a3 28 38 eb 88 76 42 db 24 03 80 e9 5a 52 a2 82 a6 f3 b9 44 ed 4a b2 48 20 81 95 84 82 ae a1 ae 5d f3 ef 67 77 83 a5 44 a9 f1 80 37 37 b6 d7 f9 78 b6 d0 59 a7 d7 f4 ea e4 b5 fc c7 8a eb d6 cd d1 2a 64 98 e9 f3 26 bd 70 54 28 53 a5 b4 59 68 8f c5 4d 65 0b 7f 6f 96 af 50 65 09 0a 2e 25 b2 22 00 fd a4 10 73 df c4 6e f1 f9 41 16 a4 90 c9 2e fa 6e bb b7 f0 39 3d e2 69 7e b7 40 b6 ad 0a 15 1a 9b 56 ac d7 e1 c7 a0 c2 a3 53 23 d0 29 d2 aa 6e 41 6a 9f 02 54 24 41 a8 22 df 62 7b f1 19 95 4e a5 04 31 f1 51 d9 6d c4 b5 2d 94 a5 5e 5b d0 db 2e 25 28 38 53 1b 5c df 2d 19 ff 00 8d 21 89 4b 80 4f 86 7a fb d2 25 db 6d a8 Data Ascii: #Wu:eA%Y*iK<y9m]zO(8vB$ZRDJH]owD77xY*d&pT(SYhMeoPe.%"snA.n9=i~@VS#)nAjT$A"b{N1Qm-^[.%(8 S\-!KOz%m
2021-10-29 15:22:59 UTC	162	IN	Data Raw: c0 14 94 94 e7 d2 39 24 8c e7 18 01 d8 0e a8 47 81 e3 fe 6f 7e 67 8a 53 28 5d 7c 46 2e 3c bc a2 2e ab d8 8e a9 c5 04 b4 ee e1 ea 2b 3b 93 8c 6f c0 c1 42 50 4a b7 ab 2a c9 1e 91 9e 0f 47 4a 0b 0e c2 72 fe 93 ff 00 d5 ef 38 6a 94 1c 10 a5 71 0f c9 b4 3e fc 20 ac 6b 29 d5 14 2b cb 52 70 9c ad 3b 14 09 db b8 61 5c 0f 50 c7 23 3c 64 02 90 0f 48 a0 1b 14 25 c6 ac 7e ba c3 b1 a1 40 17 7d 0b b3 b8 de c3 cf ce 0d 48 b3 9c 4b 6e 6f 69 5b 93 92 38 e3 60 51 f5 05 7c bf 0a 4e 41 38 07 8e 86 a4 01 fb 01 ee 36 f3 84 e8 19 93 c3 09 6f 4e e0 22 28 ad d9 ae 79 8b 09 8c e0 01 6b bc 10 79 3e e7 1f 84 25 60 f7 4f 21 58 1f 2c b0 c9 04 93 81 ad fb 4b 1f 17 3e 0d 02 05 21 45 82 b2 3f 11 0a 19 eb 61 7f 3d ee 5e 23 da c5 92 fa 9b ca e3 29 28 da 84 82 50 73 95 13 92 00 4f 73 90 4e Data Ascii: 9$Go~gS(]|F.<.+;oBPJ*GJr8jq> k)+Rp;a\P#<dH%~@}HKnoi[8`Q|NA86oN"(yky>%`O!X,K>!E?a=^#)(PsOsN
2021-10-29 15:22:59 UTC	164	IN	Data Raw: 59 4c 4d db f9 1e ba c5 94 b9 78 1b 05 ee cd 97 2f 7c ad a0 79 52 18 0e a5 27 77 90 ea 55 9e 78 04 fc f8 ed 9f ef b7 11 ca d4 97 51 b0 1c 4b 9f e3 3e 51 79 25 0c 96 cd af 62 3c 3c 7c b9 c5 bd d1 8a 53 f7 34 c6 29 69 49 2b 1b 06 f4 8c e7 3e e0 7f 7c 7b 71 d5 c6 c6 91 fd e5 34 49 4a 5c d8 39 0c 0b f1 20 8d 6c 6e 32 8c 47 4c b6 a2 76 35 1c ca 95 04 a1 21 0a 24 96 b9 cf c0 fd ed 17 55 ad 3e 62 80 a4 09 4d a3 7e 01 56 f1 df 23 f0 73 f4 fa f7 eb 66 90 93 2e 98 60 9a 12 0a 43 dc df 81 f9 c7 83 af a5 d3 f6 b0 99 d4 cc 56 07 61 85 ff 00 69 ce db 9e 77 d2 19 37 65 1e 9c a7 92 e3 29 48 58 c1 20 76 1c 7c b9 fd 31 f2 fe 55 d5 74 b2 09 ec 8b 07 70 01 e0 da b7 98 b9 2d 1a 7d 81 b4 aa d3 2f 04 d7 32 ce 44 f3 b5 bb ce 77 df c6 36 99 49 66 77 9d 05 c4 25 6d 49 6d 6d a8 Data Ascii: YLMx/|yR'wUxQK>Qy%b<<|S4)iI+>|{q4IJ\9 ln2GLv5!$U>bM~V#sf.`CVaiw7e)HX v|1Utp-}/2Dw6Ifw%mImm

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	165	IN	Data Raw: 43 ea 69 d6 e9 d0 62 25 f5 3b 22 a0 fb 2e 25 a5 36 86 d9 6d f7 9d 6d a5 d6 6d 4a e9 14 f2 4c b9 89 18 94 2d 86 ee f7 0f 70 41 df c4 5d e2 4d 1c b5 ad 60 a4 33 1c cd b2 37 fa f1 6d f1 c5 26 a7 5f f5 9b d6 22 63 c1 5b 10 62 34 bf 22 05 35 04 ba 88 71 38 29 50 2b 2b 72 4c b9 2a 4a 15 26 53 8e 3b 2a 4b 98 53 ef a9 b6 98 4a 31 8a 56 34 80 94 e1 75 3b 0f e9 24 e5 7b 16 3b a3 45 79 4c 56 94 3f f5 83 71 60 39 db 4e ed 62 22 a3 69 b3 ee 4d 8f 53 93 5e 34 e7 99 95 1d e8 8e 44 9c 58 99 11 e6 5c 4a d2 e3 6f b0 a4 38 cb de 6b 4c ed 53 78 71 24 85 05 0c 6e 54 80 30 84 e0 77 d7 3c fd 07 96 fe 30 15 15 12 6e 99 81 57 05 44 0c 2d b9 f3 0d 9f 75 c5 a1 d1 53 d3 6d 3b 14 b9 94 da b5 d6 d5 3d 89 8d ba af 87 4b 06 49 f8 c2 97 14 cc c9 08 42 94 a7 4a 1f d8 fb 8a 51 2e 29 39 19 Data Ascii: Cib%;".%6mmmJL-pA]M`37m&_"c[b4"5q8)P++rL*J&S;*KSJ1V4u;${;EyLV?q`9Nb"iMS^4DX\Jo8kLSxq$nT0w<0nWD-uSm;=KIBJQ.)9
2021-10-29 15:22:59 UTC	166	IN	Data Raw: 61 58 8d 84 6d f8 74 e4 6d c9 da 71 b4 fb f3 83 f4 f9 f6 e9 9d 59 fe 91 e5 1c c4 9d e2 17 98 b2 1b 4f ab c9 03 3f 87 8c f2 b0 08 48 48 07 8c 8e 7d b8 4f b6 3a e7 55 fe 5f 3f bc 39 33 52 33 25 b9 1f 6d 06 4d 92 92 9f f8 18 e3 18 09 49 04 70 79 c6 40 27 24 1c f2 72 07 b7 5c ea 8f f4 8f 1f ff 00 9b 9f bc fb d7 9d ff 00 f9 42 53 f6 8a 1a 52 bf 72 70 14 79 db dc 90 01 1c a7 b0 00 67 24 9e 78 e3 a7 89 44 db 08 b6 f6 3f 58 61 98 14 5c 9b 9e 7f 7d 04 7c 4d b8 ca 48 01 9e 12 46 09 48 50 04 67 70 3c 02 53 ea 1e f9 1e de e7 a7 75 4d f1 00 0d 98 b3 b3 47 31 0b df 28 3b 16 de 69 2f 27 d1 b8 92 13 b7 07 18 05 44 9c 82 40 07 24 9e fe e1 5f 3e 98 a9 4e 6c 3b fe b7 1e fc 23 a2 68 49 b1 bf 7e 5b f4 87 53 34 3d c9 d8 10 46 7d b1 d9 5b 95 81 f9 14 fb 7f 31 8e 90 95 7c ad cf Data Ascii: aXmtmqYO?HH}O:U_?93R3%mMIpy@'$r\BSRrpyg$xD?Xa\}|MHFHPgp<SuMG1(;i/'D@$_>Nl;#hI~[S4=F}[1|
2021-10-29 15:22:59 UTC	167	IN	Data Raw: de f2 b6 46 d9 eb 1a 7a 6a cc 21 0e a1 6e 2d 99 ce df 46 82 d1 ab ae 9d cc 95 64 05 1c 15 1f ef 9e dc 64 fd 31 d4 d9 92 10 84 85 25 2d d9 2e ee ef dd 6f e3 c6 ea 45 69 52 92 71 87 00 7d 9b 7e ac 38 c3 b6 99 70 97 52 86 0b 80 2d 04 71 cf 18 e7 9f 62 71 c7 fd f3 d5 54 d9 40 a8 ad 98 b1 1a b9 6d 41 cc e9 c0 f9 45 8a 36 8e 35 e0 27 20 ee 7c 2c f9 91 f7 87 7c 25 25 f2 1c 53 c3 72 d5 c7 3d 81 39 1c e4 63 bf 6f 90 f7 ed d5 54 e2 b4 a8 b2 49 23 bf 97 a6 9b f4 b4 68 68 65 75 c5 2a 0b 7b fe d6 d7 56 0f cb 28 94 e8 70 db 2e 34 9f 31 2b 03 04 e3 9e 4f b0 f9 9e 33 9c 1c 9e 3d ba 88 4a d4 72 57 2b 9d ff 00 2d 35 dd 1a da 4a 65 25 3d a0 48 ca e2 fb f3 3a 65 7f e6 27 5b 7b 4f a4 5c 1e 51 82 c2 f3 84 fe 14 1f d7 b6 73 cf 1f 4e 3f 32 54 d3 4d a8 43 04 9e 2c 2f dd a7 3c ef Data Ascii: Fzj!n-Fdd1%-.oEiRq}~8pR-qbqT@mAE65' |,|%%Sr=9coTI#hheu*{V(p.41+O3=JrW+-5Je%=H:e'[{O\QsN?2TMC,/<
2021-10-29 15:22:59 UTC	169	IN	Data Raw: bf d7 1d c8 e9 62 1b c4 3f 2b 98 ad f7 2d 47 1e 27 b4 70 24 80 15 6b 5c e0 0e 7d ea 30 d5 91 ea 07 82 8c e4 05 10 07 24 7b 84 9e d6 7a e6 ff 00 c7 af 7c 3d 24 61 55 c7 8f 0c bd ef 8b e5 a3 ce 94 69 1e 95 24 1c 1f f6 6b 61 8f 71 c8 b4 e9 5c e3 be 38 c7 e9 f9 e4 ce 37 8f 11 11 55 f1 1e 71 c5 ef da fd a9 77 ee b6 fd a1 7a ab 65 53 a7 55 0d b1 a3 66 81 66 52 61 c4 75 f5 31 0c c6 b4 e8 13 eb 45 b6 12 76 19 12 aa f2 ea 0f 2d 38 2b 71 c4 b6 08 71 29 69 b4 e1 f6 a3 cc a8 50 7c 4c b5 06 d5 81 2d 66 d3 4d d9 69 1a 1a 50 99 72 31 61 ed 61 76 d4 d9 fe dc 32 8c d4 aa db 66 0b 29 55 42 b5 5a 6d 52 37 fc 33 0b 91 3c ce 9b b3 00 26 1d 3d bc 2d c4 05 ee 01 49 40 8e 95 94 21 6b 0a 51 eb 88 90 30 89 84 8d 45 cd c3 5b 2d 4f 0c c6 bb a2 22 e7 4f 59 2a 52 54 84 b9 62 6c 2d c4 Data Ascii: b?+-G'p$k\}0${z|=aUikaq\87UqwzeSUffRau1Ev-8+qq)iP|L-fMiPr1aav2f)UBZmR73<&=-I@!kQ0E[-O"OY*RTbl-
2021-10-29 15:22:59 UTC	170	IN	Data Raw: ef 11 1b 45 12 25 8d 5d 2e ec e2 f9 68 dc 38 37 7c 4c da f9 6f 51 de 95 6c 56 22 b8 1e 4c 96 65 53 4a 99 5f 9e c9 46 19 95 1c 3c e3 49 2d 36 f7 9c ec b5 15 b8 77 38 a7 5a 6c 29 4a 3c fa 6f 44 2a 90 85 8a 59 d3 12 d3 1d 68 c4 5b 12 c8 03 0a 5d ae c3 2c d8 eb 68 f2 be 9a 51 cc 98 64 d5 a2 5a 82 64 ff 00 88 c9 2c 84 02 48 52 b4 4a 59 dc 9b 58 c4 31 06 83 1c 27 84 ee 25 23 db 8c 7a 76 f2 38 c1 38 38 1f 3e 33 9e bd 00 20 1c 45 40 85 62 29 63 f1 00 32 ee ee 8f 38 44 ce ca 94 1c bc c5 64 1d c3 0b f2 78 76 41 a1 b2 08 0a 42 73 b8 f0 52 15 df 8c 0f f5 fe 87 1d 0f ab 05 57 07 50 fe fd e5 1d eb 0b 39 71 cd 3f 66 87 4c 6a 1b 1e 9e 00 3b 7b 6c 24 e7 d5 ce 31 82 78 03 38 38 07 8c e7 05 fd 52 07 b1 f4 85 d6 28 e8 af 0f 98 85 96 e8 ac 6e 4e d0 91 94 f0 4a 08 ce 41 04 7b Data Ascii: E%].h87|LoQlV"LeSJ_F<I-6w8Zl)J<oD*Yh[],hQdZd,HRJYX1'%#zv888>3 E@b)c28DdxvABsRWP9q?fLj;{l$1x88R(nNJA{
2021-10-29 15:22:59 UTC	171	IN	Data Raw: c9 03 b6 7f 2c f4 a1 47 35 d3 26 38 85 0d 89 24 01 93 9e 41 ce 7b 0c fb 73 8f f0 f9 7c a0 9c 2b 07 11 b7 9f 7e 76 cb 5f 58 fa ee 5c a0 a2 4d 9d df 3f e7 de 7a 42 33 b3 bc cc 95 12 14 30 71 db 1f 97 eb c7 19 1d 3c 4b 28 63 2e c0 e5 71 77 dc c4 fc bc 62 5c c4 e1 48 1c bd 0c 17 76 53 2e 20 04 ab d7 df 24 8f 72 3e bf 9f f4 e8 08 9e b9 5d 70 5d c5 f7 f8 7b e1 9c 1e 9e 76 0b bf 3e 7e fb b3 dd 01 b8 ea 94 80 a0 41 29 00 f7 e3 23 f2 e7 bf eb d4 6a 49 93 17 31 64 8b 29 44 86 dd a6 76 16 df bf 48 b4 a2 9b 34 2c e2 f8 5d c7 1b 86 1f 31 cc 65 04 04 d7 d0 5f ef 07 ee c1 da 79 f6 ed cf d7 f2 19 fa fc ef 13 84 24 37 c4 c1 f8 66 7d ff 00 31 7e 2a 13 d5 a4 25 b1 03 ea 4b 6f 63 c3 e6 20 f0 92 c3 24 02 47 e6 93 fe 27 bf 1f 4f a7 cb 90 cc 9e a0 92 95 3f 0e 5e 79 9f 4d d7 8b Data Ascii: ,G5&8$A{s|+~v_X\M?zB30q<K(c.qwb\HvS. $r>]p]{v>~A)#jI1d)DvH4,]1e_y$7f}1~*%Koc $G'O?^yM
2021-10-29 15:22:59 UTC	172	IN	Data Raw: 2d 20 fa a6 95 01 83 e9 49 03 76 46 37 64 90 33 9e fe 9c 92 46 31 9f 97 4a 1a 5b 58 87 ea b6 8d 76 a5 ad 1a 7b 7e 44 95 05 9a 3d b9 48 ab d2 a7 b0 e8 2b 9f 2a 45 4a 4b 2b 8e 98 c1 4c 96 58 8e 82 94 be e4 90 f2 5f 25 91 1d 28 f2 9d 52 d2 c5 e4 39 fd 61 e0 a1 8b 7a 3d db de ee e8 bc ba 4c ee dd 28 d2 e4 91 82 9d 37 b1 47 71 c6 2d 6a 50 c8 f9 64 9c 01 9e 3b fb e3 a7 c4 65 fc 47 bb d0 47 3a 7f 68 46 8f 69 d6 93 f8 90 d5 5b dd d8 b2 24 d5 f5 91 c8 d7 da d9 79 d4 a9 72 aa 35 2a 35 26 95 21 96 1b 8a 96 e6 b3 45 81 22 dd 9c 97 d6 97 84 a7 25 cc 79 2c ad 0d 3b e6 c5 cd 56 ca 42 6a f1 59 f3 24 8e 5e f9 98 b2 a6 98 b5 a1 b7 06 7e 56 6b 9e ef 38 ca 88 56 aa e4 46 91 54 a7 d2 e1 c4 99 58 4b ce 49 bb ab ca 82 c4 b2 c2 5e 01 f9 50 5a 74 f9 10 29 c9 4b 5f 77 51 a9 d4 76 Data Ascii: - IvF7d3F1J[Xv{~D=H+*EJK+LX_%(R9az=L(7Gq-jPd;eGG:hFi[$yr5*5&!E"%y,;VBjY$^~Vk8VFTXKI^PZt)K_wQv
2021-10-29 15:22:59 UTC	174	IN	Data Raw: b2 ca d2 0f 0b 4a da 75 4c 2f cf 11 92 bd 1d 24 d9 72 02 70 37 e6 13 79 05 f2 23 e2 23 4b b0 bf 8c 66 76 95 0d 42 9d 13 65 e3 a7 98 ea 9a ff 00 fa 65 c2 46 bb be f7 88 c2 e2 b6 dc b7 2b f5 4a 33 c9 5a 51 12 4e 23 2d 79 51 54 67 82 24 45 70 a8 e0 ab 74 75 b4 95 a8 67 0b 42 82 fd 61 67 af 4f d9 f5 a6 b2 8e 4c e1 f1 04 84 4d b7 ef 01 8f 86 bd cf 1e 2b b5 29 15 43 5d 3a 9c a3 02 42 b1 ca b3 7e 9a b2 1d dc a0 78 90 ce 3f 09 e1 49 03 9c fb 67 1b 40 24 63 f9 75 33 1a 1a b8 0f 7c 62 b1 7f 0f 7c 39 59 8a 8d ad f0 72 32 70 95 11 9c 13 c6 14 07 1c 64 fc c6 40 04 f5 cc 6a f7 ef de 91 d4 fc 22 16 23 c7 f6 c0 e7 24 8e 7b f1 ce 7d 80 ed c6 3f a1 3d 36 1d 02 bb 11 2a 04 e0 8d a9 ec 4e 72 49 3e fe dd 86 54 3b fd 38 1d 28 50 96 ec 00 e9 19 41 39 00 ee c8 38 3e 91 82 7f e5 e7 Data Ascii: JuL/$rp7y##KfvBeeF+J3ZQN#-yQTg$EptugBagOLM+)C]:B~x?Ig@$cu3\|b\|9Yr2pd@j"#${}?=6*Nrl>T;8(PA98>
2021-10-29 15:22:59 UTC	175	IN	Data Raw: f9 9d a7 8e c7 24 e0 9e 38 ec a3 90 1b 8b c8 ce 71 dc 81 d8 1e 71 c8 e4 e7 b6 4e 71 91 8e 7a 51 22 13 9c 57 24 9e fc 73 82 7b f7 e0 10 4f c8 0e 7a 50 a0 03 8e 30 14 46 41 03 1c 90 32 7f fb 5f a2 78 04 67 eb 85 0a 0a af ff 00 49 f9 76 c8 1e fd f2 92 3e 58 f9 f3 8e 3a 50 a3 9a 09 4e a5 21 44 a8 11 ce 7d bf b3 f9 1f d4 71 d7 c9 86 9c ab 32 47 79 1e 85 be 6d 68 fa f8 61 66 07 73 77 9d 77 78 73 86 dc d9 a9 43 65 21 38 27 b1 c7 e6 f2 3f d0 fe 78 ea 54 8a 63 29 94 a5 03 1e 05 86 7e 19 b1 b4 4a 40 20 61 0d 7b 7a fa 3c 13 Data Ascii: $8qqNqzQ"W$s{OzP0FA2_xgIv>X:PN!D}q2GymhafswwxsCe!8'?xTc)lf:,d,TkV`[O'$d &.?/~0t!o;)S:d~J@ a{z<

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	176	IN	Data Raw: 6a 3c d7 1c 81 19 b8 f5 2a 4c e3 f1 0b 93 39 2d 46 6e 32 50 fb cf 48 4b 6a 2a c1 4b 72 11 34 4b 04 9d fb 9f c3 8f bb e8 05 ca 70 09 53 13 a3 f1 e7 6e 3a 37 18 ce 2b f3 c6 3e bb cb d4 fa e5 fb 63 5e 93 ec b5 55 60 b7 45 90 fc 1a 75 b5 2e 7d 62 9a cb 91 64 a5 fa a8 9f 4a 9d 4d 62 4b d2 21 47 90 58 a7 c6 65 a8 59 2d a5 e7 56 b7 9f 78 5d 72 94 b2 50 a4 8b e4 4e be a0 1f 77 78 20 94 12 96 7b dc ff 00 3e 1e 10 f3 b4 fc 6d 78 a7 a9 29 2d ab 5c 2e 32 fa bc a4 2d 42 da d3 cd c8 e0 12 76 ae cd 21 5c 12 a4 af 1b 8e 49 09 e0 75 2c 4c 98 ce 56 0b ee 39 7b f2 e7 03 29 de 3c a2 d3 db fe 21 3c 4b d4 21 79 ce eb 65 cc f0 29 4e 36 50 34 ff 00 d4 b3 b8 90 42 6c f0 0a 94 90 90 93 b5 7b 42 49 51 20 8c f7 ac 5e ff 00 5f ac 34 a4 10 cc 07 74 2d c9 d7 df 12 d1 63 26 4b 1a cd 73 Data Ascii: j<*L9-Fn2PHKj*Kr4KpSn:7+>c^U`Eu.}bdJMbK!GXeY-Vx]rPNwx {>mx)-\.2-Bv!\Iu,LV9{)<!<K!ye)N6P4Bl{BIQ ^_4t-c&Ks
2021-10-29 15:22:59 UTC	178	IN	Data Raw: 0c 9e 24 35 7b 48 2a a4 4d 2a b9 2a f3 2a 9a 35 54 b8 e9 af d7 6d aa c6 c9 09 b5 dc 6e 73 15 76 6a 96 b4 85 4a 53 94 64 3f 3a 32 7e f5 a5 b0 e8 a3 cf 69 f9 33 15 10 3c e0 94 d5 df 4e 36 54 ca ed 81 b4 d5 2d 0c aa 63 2c ca 0c c1 48 96 52 a5 92 d7 32 80 cc 9d 78 43 7f 0f 36 c4 9d 97 d2 7d 87 2e 6c ef cc c9 5d 42 91 51 8b b3 84 cf a7 9d 29 09 73 76 c6 b0 40 7c d8 81 94 58 1f b4 e6 99 54 a0 8d 25 d6 0b 52 a4 a9 6d b5 47 7e 12 25 99 0d e5 d6 1a 7d aa 8c 66 9f 11 12 9f 21 c8 e6 4c b7 63 81 21 c4 86 88 22 52 de 6e 3a c7 82 6c 6e 89 29 33 7f 28 ac 29 52 87 c4 af 12 ce 2d 9b 0b e5 1f 58 6d be b3 f2 c2 b6 82 53 4e a6 61 d4 cd 27 0c c0 e7 fc 36 7c 4e 32 b7 81 88 a7 c3 87 da 0f ac d4 8a b5 ac 21 db 57 85 e5 1a 91 53 87 2a a5 12 91 4d a8 d5 1e 71 a2 e7 98 f3 8d 9a 63 2b Data Ascii: $5{H*M***5TmnsvjJSd?:2~i3<N6T-c,HR2xC6}.l]BQ)sv@|XT%RmG~%}f!Lc!"Rn:I)3()R-XmSNa'6|N2!WS*Mqc+
2021-10-29 15:22:59 UTC	179	IN	Data Raw: ce 0f 39 ff 00 0f 6e b0 f5 5f 88 b5 73 09 32 01 42 74 07 3d 74 f0 76 e3 dd f4 5e c5 fe ca 3b 06 4a 11 f9 c9 85 73 b0 8c 6c 49 0e 73 37 cb 23 71 ba d9 c4 b7 42 fb 3c 74 3e df ab 53 ae 1b 50 55 ad d9 d1 a4 32 65 a2 04 d9 6c 46 a8 c6 41 01 c8 73 99 69 e4 b3 2e 2b ad 15 37 e5 ca 43 ad a4 94 b8 84 87 1b 6d 40 74 ff 00 89 75 e8 21 33 00 52 4e a0 5f d3 d3 58 ee d4 fe ca 7b 0a 76 31 46 ae df 6b 78 cc 6e 63 ab e9 e3 78 93 aa de 08 2d da d3 7e 65 36 e2 76 31 59 00 25 d0 a3 93 ea 00 63 70 ed 91 ec 73 8e 4f 3c e9 29 bf 12 65 94 8e b4 38 36 39 3b db 99 d7 2e ed 63 cb 76 a7 f6 54 da d2 0c cf ca 4d 49 4d c0 04 ab 2d 37 e8 78 e7 68 8c ea 9f 66 55 f1 57 6e 40 b6 6b 11 2a 2e fe 30 95 ee 49 5a 80 c8 c6 01 3e a3 9c 82 4f 6e 33 d8 df 52 f4 e3 67 cf 6c 40 dd 9c 5b 23 9e e3 fc Data Ascii: 9n_s2Bt=tv^;JsIls7#qB<t>SPU2elFAsi.+7Cm@tu!3RN_X{v1Fkxncx-~e6v1Y%cpsO<)e869;.cvTMIM-7xhfUWn@k*.0IZ>On3Rgl@[#
2021-10-29 15:22:59 UTC	180	IN	Data Raw: a9 9d 4a b0 e6 2d 85 c3 eb cf bc f2 31 6e 35 46 f7 87 49 b5 2a 32 d4 cf dd ec 0a 6b de 50 58 0d 6e dc ca b0 41 50 1c ff 00 64 f5 ec bb 36 54 d9 d5 54 d2 52 82 84 12 92 43 30 21 c6 6f a9 fb be b1 f3 de d6 96 8d 9d b2 eb e7 d4 55 09 b3 02 26 07 2a 19 94 ab 0b 00 49 cf d0 f2 8e 77 ef ba f0 ab dd 05 15 9a 80 52 5c 4b d3 a4 a9 27 71 51 5a 7c c5 27 2a 3e e3 d2 52 92 9e 0a ca 41 ee 33 ef 34 52 fa aa 54 4b 03 08 97 2c 10 37 2a d7 8f 87 b6 cc ff 00 ce ed 2a c9 c0 bf 6d 78 8b fc 40 2b 2d 34 f4 7c f2 69 a2 40 20 a4 a8 14 1d ea 5e 15 e9 e0 a3 6a 55 ea 04 94 e4 6e 00 15 1e f9 3c f5 2c 64 39 08 a6 c0 9d de 67 eb 03 b7 20 6d 39 50 05 19 c9 27 18 29 da 07 bf 19 ca 88 38 db b4 0e 9f 8d 5b fc 87 d2 16 14 ee f7 ef 58 fa a9 db dc 6b 6b 85 07 03 b1 e5 47 27 00 0c 8c 81 90 a5 1c Data Ascii: J-1n5Fl*2kPXnAPd6TTRC0!oU&*lwR\K'qQZ|'*>RA34RTK,7**mx@+-4|i@ ^jUn<,d9g m9P')8[XkkG'
2021-10-29 15:22:59 UTC	181	IN	Data Raw: 52 52 bc 08 51 e2 e0 1e 1b f7 6b dd 12 91 b5 28 e5 24 cc c5 d9 58 62 97 dc 1b 36 b7 22 d1 12 cc f1 c3 12 3c 95 aa d5 d3 09 4f 97 9d 0c c5 b8 35 0a f5 97 50 97 31 68 48 4a 1f 7e 85 44 83 09 00 a7 0a 21 11 ee 09 9e 53 85 c0 89 0a 5b 6a 02 da 9b a2 c2 62 7f de 27 84 26 ce 46 77 7b 80 e0 5b 97 94 54 d6 f4 9a 5d 3c 95 cc a6 93 2e 66 12 c0 29 4a 19 e8 3c 6f 9f 0b bb ca 3a 75 f6 86 6b 45 a9 5b 69 76 eb 5a 65 6d b8 e9 5b 6e 30 2d ca f4 b8 4c b9 20 34 1c 71 e5 4f be 5e 65 f7 1c 65 b7 10 97 9c 42 5e 49 7c 25 b5 29 d7 32 8d 05 1f 43 36 29 5a 47 f7 9d 62 d6 43 2a 5a b0 4b 96 06 a4 12 92 e4 58 01 60 ce f1 9f 99 d3 1d ae 7f 52 5d 0d 34 a4 31 c4 b5 25 73 2d 99 21 21 60 8f f5 1b 58 58 45 e8 d3 7f b4 7f 59 e4 53 99 35 db 4b 4f ab 50 e3 38 a9 72 d5 06 9f 76 5b 93 aa 6d 2d Data Ascii: RRQk($Xb6"<O5P1hHJ~D!S[jb'&Fw{[T]<.f)J<o:ukE[ivZem[n0-L 4qO^eeB^l|%)2C6)ZGbC*ZKX`R]41%s-!!`XXEYS5KOP8rv[m-
2021-10-29 15:22:59 UTC	183	IN	Data Raw: a9 30 f3 70 59 a8 45 a7 4a 79 e8 89 f9 b6 aa 8e 96 7e d1 ab 3b 3e 76 29 32 67 4c 4c 99 c8 04 05 a0 13 90 2e c1 ed c3 94 7d c1 b0 36 84 ea 3d 95 b1 a6 6d 8a 55 22 aa 6d 3c a3 3e 4d 49 12 84 b9 96 37 c7 8b 11 d5 9f 58 23 e1 12 fb b3 5a d4 3a 15 bb a8 53 99 b6 28 15 09 54 c8 f5 0a ec 1a 5b 55 39 34 b8 8b 90 84 a1 f5 d2 e3 ae 3b b2 9d 6b e2 1e 5b 11 58 71 b4 3e 80 fa 5a 54 b7 9c 65 a6 f1 9b 4b 66 85 cd 13 67 2d 7d 40 9b fa d3 0a 95 da 56 9a eb 6b 7c a3 e9 5e 8e 6d 79 95 1b 26 67 f7 4a 24 2e b3 02 85 2c a9 64 c9 94 b9 85 29 c3 2e 64 e4 75 8c 70 e2 2f d4 90 ac 9d af 1b 95 e0 ce fd d7 3d 32 f1 8b 54 b1 74 de 95 61 3d a0 7a e9 3e 35 6a 83 69 5d f5 ca 83 93 61 c6 93 f1 d1 ee b9 86 2d 2e 3d 46 a7 41 5d c7 36 9f 53 bc 23 d3 e5 c5 75 66 5d 66 a2 94 c5 8d 4e 68 ca 83 Data Ascii: 0pYEJy~;>v)2gLL.}6=mU"m<>MI7X#Z:S(T[U94;k[Xq>ZTeKfg-}@Vk|^my&gJ$.,d).dup/=2Tta=z>5ji]a-.=FA]6S#uf]fNh
2021-10-29 15:22:59 UTC	184	IN	Data Raw: 01 bb 06 bd 9b 47 dd f6 8a 9a 6a 65 f5 a5 37 37 b5 9d dd d8 65 6c 8f 22 2d 9c 2c 52 eb 46 52 d4 97 16 d3 68 64 1d ad 0c 7a ca 3b 0d c0 fa b3 c7 6c 1f e9 d4 65 4e 29 41 50 0c 0e 47 30 ec 58 5f 2f 5e f8 ba 1b 2c a5 94 dd a5 10 0d f2 1d dc fb af a3 98 99 74 ff 00 cf ad 3c 85 c8 8a 12 c3 0e 6d 48 1e e0 12 02 88 c7 24 f1 cf b7 eb cc ca 19 82 70 0a 52 4a d9 ec 1d df 7d b7 77 dc df 28 cd f4 85 22 84 62 49 4e 32 83 d9 27 32 d9 fb 0d a6 97 be 9a 3d 6b bc 2a 4d 49 61 84 ad 95 04 6f f3 13 f8 53 cf be 31 91 db 1f 5c 75 a6 d9 d2 67 29 69 21 2a 4a 42 92 e1 8b 00 f7 7c b2 77 21 b4 cc 58 c7 cc ff 00 88 db 72 5f e4 17 25 6b 02 78 0a f8 54 1c a9 8f 66 d7 62 78 68 73 66 36 b3 61 50 ea 94 b7 99 79 96 bc c7 1b 56 00 4a 47 a8 83 9c 1c 73 c8 07 8f cf 19 cf 5a d1 28 a5 0e 09 Data Ascii: Gje77el"-,RFRhdz;leN)APG0X_/^,t<mH$pRJ}w("blN2'2=k*MIaoS1\ug)i!*JB|w!Xr_%kxTfbxhsf6aPyVJGsZ(
2021-10-29 15:22:59 UTC	184	IN	Data Raw: fc c8 4c e9 29 9b 24 a9 8e 34 83 d9 b6 ac 0e 97 d7 58 ce 2d 5a f0 e9 53 33 1f 7e 9c d2 16 d3 ea 70 b5 e5 fe 24 28 92 00 c2 79 4e 4e 39 1f d3 b7 56 7b 3f 6f d6 ec f9 e9 93 50 55 35 0a 60 32 00 0d 06 40 65 6c ed 17 1b 7b a0 bd 17 e9 5e cc 99 51 48 15 43 b4 24 cb c7 fa 69 f8 d5 85 c8 b9 20 f6 87 0c e2 ac 69 2d b7 58 b6 bc 44 69 f5 22 ad 1d e6 1c 6a b9 2d 7b 54 85 0c b7 1e 8d 57 92 1c 07 04 29 25 4d 00 0e 38 cf 24 8e de 97 41 57 2a b2 5c b9 88 56 12 b0 f8 41 ca ec c5 f7 6e 68 f9 37 6f ec aa ad 93 3e 74 a9 f2 e6 04 4b 59 48 5a d2 52 e1 36 7e f0 77 f9 46 c2 45 58 08 29 3d 82 b2 07 64 ab e6 72 38 e3 24 12 71 ce 40 00 01 d5 e2 71 0c 21 dc 10 fa 71 f7 f5 8c a9 c3 9a 4b 82 01 3b df 77 77 bb bc 1d 0e 0c 15 63 92 3b 13 8e 47 75 1e 38 1c e0 72 32 7a 2c 28 2a eb b8 07 Data Ascii: L)$4X-ZS3~p$(yNN9V{?oPU5`2@el{^QHC$i i-XDi"j-{TW)%M8$AW*\VAnh7o>tKYHZR6~wFEX)=dr8$q@q!qK;wwc;Gu8r2z,(*
2021-10-29 15:22:59 UTC	185	IN	Data Raw: 39 3c 1d a1 c9 3e 2a ac 49 8a 59 53 71 69 5a ae d3 08 20 0c 29 7a 43 7e f9 8a 39 24 e4 82 d8 3b 32 09 46 0e 13 91 d3 92 90 a7 7d 1a 3b 31 78 64 a9 29 55 fd 58 86 d3 46 fb de 2b 0c 67 60 c3 52 44 86 d4 5b 49 46 ef 2c 7a f0 a2 ac e7 05 40 12 38 0a 03 3c 03 90 0f 4d ec fe ec bd f3 82 76 95 2a 58 2a 25 c0 b5 9f 7d ad bf ce fc ec 2d 99 7c f8 50 81 11 31 b5 63 4e 35 1e eb 81 22 2b e1 51 ed 4a db 74 c9 2c cc 6d b4 2d 99 3f 12 e5 76 90 a4 b1 ff 00 19 a5 34 87 55 e6 79 84 16 d5 8d e8 73 ca 66 26 c6 c7 7b 3b f2 d3 74 35 74 f5 16 ea 83 92 58 3b e6 7c 1f e6 74 8a f9 e2 e7 5d bc 3f c6 a1 59 54 ad 16 b5 af 2b 46 d5 b2 d9 bc 6a 09 a1 5f 95 18 f5 19 c8 95 75 1b 75 f9 13 9d aa b5 5b ae 49 55 3c cf a3 ce 5a 1a 90 f2 64 61 c8 f1 61 34 e2 52 f1 84 29 b8 54 1a 51 7d 6f 9e e3 Data Ascii: 9<>*lYSqiZ)zC~9$;2F};1xd)UXF+g`RD[IF,z@8<Mv*X*%}-|P1cN5"+QJt,m-?v4Uysf&{;t5tX;|t]?YT+Fj_uu[lU<Zdaa4R)TQ}o

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	187	IN	Data Raw: 9f 65 c3 3e 27 77 cc 1f da da c1 bd 02 f1 6d e2 37 c3 96 98 6a 66 85 d0 ee 65 5c 1a 75 77 d3 6a 6d e9 c5 56 b7 2a 44 7b b3 43 24 d7 a7 22 45 5d fb 46 a6 10 1b a8 d1 64 d2 e7 55 25 53 29 32 d4 c7 ec d5 c2 e4 3a d5 bc fc 36 d3 51 a7 56 fc f2 ab a1 d4 f3 6a c5 4f ea a6 58 9d d6 90 30 00 e0 e2 63 d9 76 b7 3b f7 c7 a4 51 74 ca 64 bd 9f 2a 5a 65 a1 4a 93 25 52 02 94 15 88 82 96 0a 2c a6 7e ed 6d a4 52 68 f0 29 75 b4 4a a8 d6 35 26 e9 b6 21 51 a8 af 37 1a bd 5d a4 d0 a6 c6 6a 9d 1e 42 1b 74 2d 71 6d 14 dc 33 e6 52 58 cc c5 6d 83 36 b7 26 95 1d 46 9f 2a 48 86 a8 ec dd 4f 54 b9 52 e6 29 55 55 52 d3 25 c4 99 48 ea c4 b0 07 c2 94 bc b2 a2 91 70 ee 49 f1 8a 14 52 26 b6 5a 54 ba 39 15 09 9a 54 a5 ad 6a 9c 66 24 4c 56 25 ba 53 30 24 a8 e7 74 38 d2 ec d4 be e5 be da a9 Data Ascii: e>'wm7jfe\uwjmV*D{C$"E]FdU%S)2:6QVjOX0cv;Qtd*ZeJ%R,~mRh)uJ5&!Q7]jBt-qm3RXm6&F*HOTR)UUR%HpIR&ZT9Tjf$LV%S0$t8
2021-10-29 15:22:59 UTC	188	IN	Data Raw: 3e 57 ce 3e 0b e9 09 a5 3b 56 7f e5 25 26 96 41 50 52 25 a6 74 c9 b8 d8 33 15 2d 6a 1b 8d 86 62 d9 c1 56 93 80 32 7b f6 e3 ff 00 4f 3f 9f d0 7e 7e dd 5a 8b 80 78 45 3c 28 23 81 c1 c6 71 c9 c9 ff 00 ef 7f ea 7f d7 b0 a0 62 3b 93 d8 7c f2 4f ea 90 71 ef db f5 f6 e9 42 8f 38 c1 fd 72 0f 24 e0 83 8f cf b6 7e 7f 5e 94 28 67 d5 d6 0b 72 4f 7c 80 9e d9 04 ab 23 bf 23 e4 78 04 8f 96 3a e3 81 99 10 a3 f5 21 a5 26 1b 6a 18 23 6f 6d a7 93 d8 63 04 27 83 c9 e5 29 cf 38 ed d7 0b 2a cf c6 c4 42 f7 ef f9 84 da 93 0a 2a 27 69 e1 5f 33 bb 03 68 03 8c f7 09 39 c2 4f 07 38 38 e9 a5 00 0b 39 3f 7e 02 1c 15 66 c8 70 cf de f8 8d 6e 18 5b d2 12 01 24 82 08 dd e9 27 66 06 15 93 fc 45 58 c9 c9 29 20 80 49 e9 98 4d ac da 65 94 75 c3 7c 4a 7e 71 49 bc 66 5c ee 69 bf 86 8d 76 be 5b Data Ascii: >W>;V%&APR%t3-jbV2{O?~~ZxE<(#qb;|OqB8r$~^(grO|##x:!&j#omc')8*B*i_3h9O889?~fpn[$'fEX) IMeu|J~qIf\iv[
2021-10-29 15:22:59 UTC	189	IN	Data Raw: f6 de c7 a9 d8 95 d3 a8 ea 65 a9 0a 42 94 51 6b 29 21 44 12 5e c0 bd b3 f9 c2 e8 73 70 23 be 13 9e 4e 55 8e d9 f9 e0 67 f9 83 9f 9f 56 36 72 35 dd e5 ef e5 15 29 49 6e dd 8e 6d c3 43 ae 8d 04 56 ef 24 76 23 b2 b9 2a 24 fc 87 72 30 72 47 60 72 06 3b 8e 2d d0 1d 9f 80 23 7e 7e fe a6 d8 05 4b 60 33 43 a4 4f c5 99 f4 1d e6 cd 6e 7b c9 97 92 77 0d c9 57 b6 dc fa 80 ce 79 24 e3 bf 62 00 1f 4c 8c 91 89 d2 d7 31 48 4a 93 87 0e fb be ec ff 00 8e 50 f5 26 62 00 52 e5 ab 09 f8 48 07 b9 fd f7 35 e3 ce f4 9c 0c f7 38 1c 8e 00 f6 ce 3b 9f 63 8c 0c 1c 91 9e 52 52 08 72 f9 c7 20 9b ce 0c f2 15 81 c7 71 df e5 c6 47 1f af 7e 0f 4d 36 24 71 85 18 0d 73 5b 11 67 2d d9 11 12 10 57 95 00 31 8f 9f 61 ef f3 18 03 f9 67 af 9a 05 29 47 68 b1 4e ac 0e ff 00 bf 73 f2 8f aa 25 25 69 20 9b Data Ascii: eBQk)!D^sp#NUgV6r5)InmCV$v#*$r0rG`r;-#~~K`;On{wWy$bL1HJP&bRH58;cRRr qG~M6$qs[g-W1ag)GhNs%%i
2021-10-29 15:22:59 UTC	191	IN	Data Raw: 65 89 21 2c 05 d0 ae 39 fc d9 fe 70 ea 9a 93 29 21 32 e6 05 a8 8c 93 62 09 b0 7e 46 33 42 ef be 6b 17 ed 6f 7d 4d a9 5f 03 e7 f9 d0 68 ee 48 2f 2e 43 db 09 6a ab 5d db 84 3d 25 4d 86 d2 cc 3f 44 58 2d 86 90 00 f2 52 04 5a 89 9d 58 74 1c 2d 76 76 37 de de c7 17 87 ec ea 79 b5 13 ba d5 87 36 bb 10 ff 00 c7 ad f7 43 a6 8d 01 98 f1 41 8a 9d b5 12 80 9f 3a 52 41 09 dc 01 56 c0 86 d6 16 ad c1 18 0b 18 59 c9 59 5a 11 e5 ab 3d 50 b5 4d 98 14 be d0 7b 80 73 cb 2b f2 3f 52 23 73 41 46 11 26 61 0c 99 c5 ca 54 d6 1a 8b 7b df ac 3f 2c db 00 d4 6a 5e 65 4d d6 a5 34 54 1c 52 d2 b7 dd 46 e7 08 51 53 ca 5a 10 e3 af 70 16 13 ce c7 15 b9 65 2a 01 29 b2 a7 c2 50 90 89 78 48 7b 90 e3 3b e4 d9 6e cb 9e 51 1f aa 5e 35 2a 7c ee b0 fe e2 87 00 ee cf 2b 37 37 8b d1 a3 f6 65 1e 3d Data Ascii: e!,9p)!2b~F3Bko}M_hH/.Cj]=%M?DX-RZXt-vv7y6CA:RAVYYZ=PM{s+?R#sAF&aT{?,j^eM4TRFQSZpe*)PxH{;nQ^5*|+77e=
2021-10-29 15:22:59 UTC	192	IN	Data Raw: 92 fd 3d e9 2d 3d 16 65 52 93 2a 0d 56 5e 01 8e 60 dd 2a 51 26 e1 ef bb 88 8f 49 98 94 4d 29 09 21 05 09 08 20 06 0a c2 1c db b9 c3 f7 dc 88 ae 34 4b ce f0 b5 59 ac 8b 5e e8 ad db ad dc b4 a7 68 95 95 d1 aa 52 a9 6f d6 29 0b 93 1a 5a e0 c8 7a 2b 8c b9 26 3b 92 a3 47 52 9b 5b 8d 8c 97 23 95 16 df 90 d3 c0 52 25 cd 9e 95 54 27 ac 45 bb 23 37 df 7b 5b 3c b2 86 0c 49 c5 2f 11 4c b2 c0 e6 31 6f 6d cc e6 fa f1 19 39 2d 9d 41 a6 ce 5b 34 7b de 24 69 71 ca 81 62 a4 e2 25 22 10 da 85 ef 66 a3 1a 02 98 53 2e 3c d0 f8 74 d6 69 de 51 88 e6 1f a9 43 7d b0 f4 e8 f7 12 6a c8 29 94 b0 3a b4 86 96 06 89 c9 88 cb bc 7a 5a 2b a6 d0 24 4d 44 c9 6b 0e 56 90 ca 2f 9e 79 78 f8 c2 ec 88 8e c3 2b 7a 85 6e 36 b7 62 34 cc af 3a 95 56 a8 97 11 13 c8 4f fb c8 0e 3e a5 4c 82 a3 2a 32 Data Ascii: =-=eR*V^*Q&IM)! 4KY^hRo)Zz+&;GR[#R%T'E#7{[<I/L1om9-A[4{$iqb%"fS.<tiQC}j):zZ+$MDkV/yx+zn6b4:VO>L*2
2021-10-29 15:22:59 UTC	193	IN	Data Raw: 14 92 55 c9 ce 12 77 03 db b8 e3 a2 12 92 96 0d a8 1c 77 67 bb e6 21 b8 54 16 8d 05 df b9 ad cf 74 7d aa c7 69 9a 73 0e 29 21 08 4b 4a 52 94 70 76 0e 09 2b 51 04 65 5c 95 24 9e 53 c1 f7 ea 0c f3 d5 a1 4b 3d 90 03 97 b7 bc bc 62 64 a9 0b a9 9b 2e 44 b4 99 8a 5a c2 52 94 dc 92 a2 d6 f1 8c f9 d6 7d 4f 8d 3e b1 fb 33 4b 74 25 94 3c 90 ea d0 be 14 52 48 56 d5 e7 3e dc 83 93 ed d8 f1 f3 ef 4f 3a 4f 3e b6 64 cd 9d 4a a5 04 a1 2a 13 0e 27 0a 00 bb 00 9c f3 76 36 d2 3f 46 ff 00 b3 4f e0 cc 9a 49 b4 db 6b 69 ca 97 d7 76 2a a4 29 72 d5 d9 2c 08 0a c4 1d d8 5f 76 71 1f 52 6e 24 45 92 22 21 41 d2 84 80 94 e7 79 f6 e4 83 c7 7c f3 ec 7e 5c 63 c8 6a 31 cb 92 4a df 1a ae e7 27 dc 77 f8 dc 5b 8c 7e 8a 2d 54 c2 42 65 4b 05 49 4c a4 cb c2 93 60 52 96 24 5c 30 b3 c1 0a b5 c1 Data Ascii: Uwwg!Tt}is)!KJRpv+Qe\$SK=bd.DZR}O>3Kt%<RHV>O:O>dJ*'v6?FOIkiv*)r,_vqRn$E"!Ay|~\cj1J'w[~-TBeKIL`R$\0
2021-10-29 15:22:59 UTC	194	IN	Data Raw: 90 47 8f ab 9e 6f 11 45 c5 6d 4c 69 d5 3d f0 ce 25 a5 12 42 b6 12 9e 7f f5 63 1f 98 cf cf e9 d4 1a 89 6b 47 c1 a3 fe e0 06 ed 6f c7 ed 1a 09 33 c6 1c 2a 20 16 bd f7 6b ed dd ef 0c 47 29 39 5a 8f 97 cf 39 18 e3 b7 bf e9 f4 f7 ed d1 a9 26 34 b5 05 bb e9 ae 60 bd f9 f7 45 b5 18 42 81 75 06 27 57 dd 97 3f 0e 10 51 ea 60 2d 96 96 de 01 39 03 19 03 e5 fa fc 8f f9 74 c9 33 08 9c b0 49 02 fa 1e eb e8 1b ce cd 78 b3 95 2e 50 51 38 93 ab 77 80 06 7e f8 c1 05 c0 28 c2 03 6a 00 7b 9f 97 d3 f3 fa 7f 87 4c 9e 9c 73 1c 92 46 79 be bb b3 be 5a e7 c2 1e b4 76 81 00 3e f4 df 3d e4 58 77 de fa 34 7d 66 9f 21 2e 24 30 85 1c 91 eb 23 20 72 3f cb fa 83 f4 c3 8a d0 65 29 09 b3 25 c5 8d f2 07 be fe 3b ef 1a 4d 9a cd 2f 13 62 04 3d b8 1b f7 bf 1b be b0 f3 a7 83 0d 6d 2b 66 1c ee Data Ascii: GoEmLi=%BckGo3* kG)9Z9&4`EBu'W?Q`-9t3Ix.PQ8w~(j{LsFyZv>=Xw4}f!.$0# r?e)%;M/b=m+f
2021-10-29 15:22:59 UTC	196	IN	Data Raw: 84 e5 b5 1e c5 4a f4 85 a9 45 02 c2 92 7a 14 a7 7f 2b db 2d 34 3c 9f 2d 62 05 5e cd 54 b9 6a 50 ba 5e ee a0 fb f7 fd e2 c5 d1 a9 6e bc b6 14 f4 56 dd 75 c4 a1 2d 1e c2 42 5b 6f 72 4a 9e 70 a1 ad aa 25 d7 06 d4 ab 25 59 75 69 4a 96 83 70 72 71 a8 1e 9b b3 f2 8c d1 96 be b3 fc 80 f6 5c ea ee dc 2d 6d de 82 41 2e 1a 74 75 6e 75 80 83 ca 10 d9 ca 41 4a 42 52 b5 90 b5 29 6e 1d a0 f9 a5 c6 b6 b4 50 14 d1 08 23 ae 80 f7 36 03 cb 76 5f 2d 21 b3 a6 60 4a 90 43 15 03 b9 ed 7c c1 21 bc 73 8a d1 78 a8 cf ba 1b 70 0d a8 6e 34 85 3e 52 8f 2d 49 18 f2 8a 00 58 c0 07 d4 10 b5 5c 6f 6e 16 a2 9c 29 08 e7 01 73 a3 5b 5e 3c f5 8a f9 32 d7 39 2b 00 5c 29 c8 71 90 cf 75 98 0b 1c fc 63 a8 1b 11 7b 74 f6 c0 c1 e0 58 b6 86 00 50 ff 00 f8 76 9c 31 c7 be 07 b7 a7 9c e7 1d 19 21 92 Data Ascii: JEz+-4<-b^TjP^nVu-B[orJp%%YuiJprq\-mA.tunuAJBR)nP#6v_-!`JC|!sxpn4>R-IXlon)s[^<29+\)quc{tXPv1!
2021-10-29 15:22:59 UTC	197	IN	Data Raw: 2b e4 b4 96 88 42 10 80 42 09 0a 50 48 69 6b 4a 81 2a 40 89 ab 75 53 2f 47 21 07 be c3 3d 75 39 44 d9 13 17 47 4e 54 aa d9 57 f8 7b 04 86 76 01 c0 72 3d 05 ef 02 c1 a2 b3 2b 0d 32 1c 0e 29 68 4e 52 82 16 08 0e 23 71 42 54 16 12 f3 6b 0d ad d5 34 7c cc 17 11 bb 2a 58 9d 4d 21 25 65 49 18 46 e3 d9 29 b6 44 1f 10 3b b5 88 35 15 c6 62 65 cc 9f 31 53 65 28 2b b5 29 68 4a 51 80 39 eb 02 94 14 18 1b 05 e1 cc e1 8b 6f a2 d6 ed 7f e3 19 7d ac a5 e8 0e b3 2d 00 16 da 44 86 14 e7 90 e9 53 4e 2b 74 c0 bd af 31 21 b5 29 b8 ee 34 85 b2 b4 79 a4 f5 ac d9 a8 5a 3a c4 f5 b8 42 d2 04 b0 cf 81 60 b9 5d 8e a1 87 20 f1 88 da b5 68 9f d5 86 9d 35 1d 64 c2 27 25 b0 75 13 12 94 ac 15 0e d4 d6 00 61 67 19 80 cc d1 ba 1a 1f 70 c8 d3 48 d4 3b 92 d4 94 b4 a1 3f 0d 2e 19 77 32 18 85 Data Ascii: +BBPHikJ*@uS/G!=u9DGNTW{vr=+2)hNR#qBTk4|*XM!%eIF)D;5be1Se(+)hJQ9o}-DSN+t1!)4yZ:B`] h5d'%uagpH;?.w2

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	198	IN	Data Raw: c9 e7 3d fa ce 54 ae 74 fa ac 68 4f 67 36 1a 7b e0 33 8b 45 53 d3 49 41 42 98 f6 74 06 ed c6 e6 fa 9e f8 b3 96 5d ed 06 94 fd 35 6d cc 4e d5 13 e7 3a db c1 5c 92 72 30 92 08 03 b1 c9 e3 1f 9f 57 14 86 6c b5 a1 64 10 02 73 ce ed 7e 25 f2 f0 8c 1e d8 d9 a2 b6 4d 42 3a 80 43 bc b2 c0 b8 6e 6f f5 6d 37 45 ac b6 b5 55 b6 a7 b0 88 93 8a 55 e6 37 85 29 7b 92 a1 9e 49 1b bd f8 e4 93 81 8e ad 64 d6 cd fc ca 56 85 a8 00 46 7d 9d 7c 3d 1e f7 8f 21 db 5d 0b 44 da 69 a6 6c 91 74 ad 88 03 89 dc 4f a3 b9 bd ed a5 9a 75 7c 2a e2 b7 23 9a 79 6e 64 a6 90 94 b8 8d c0 ab 1b 46 4e dd d9 1d f3 fa 75 e8 fb 2e a0 d4 48 60 5e 61 ec 90 7e f7 6b b3 3e ba 6b f1 af 4c 3a 36 8d 93 b6 27 7e 61 e9 e4 a9 4e 95 61 2d 9b e9 be df 67 88 e3 55 eb 55 8a 7c 77 92 a7 fe 0d 44 13 b7 3b 79 c1 c8 Data Ascii: =TthOg6{3ESlABt]5mN:\r0Wlds~%MB:Com7EUU7){IdVF}|=!]DiltOu|*#yndFNu.H`^a~k>kL:6'~aNa-gUU|wD;y
2021-10-29 15:22:59 UTC	199	IN	Data Raw: c9 03 27 07 e6 01 3d fa b9 a5 e8 05 0a 15 8e 68 77 bf 8f 7e f0 fe da 33 1b 57 f1 e3 6d 54 a0 a2 9d 6a 4b ee 23 b9 f2 fe 59 9a d1 2c d1 e9 70 a9 ed 82 c3 60 ed dc 4a 88 ca 8e d0 91 92 0f b2 f7 61 39 f6 49 e0 67 1d 6c e8 76 45 2d 12 52 25 ca 96 02 00 01 c0 7e c8 b3 dd f7 9d 4e ed 23 c8 f6 df 4b f6 de dc 5a cc ea d9 81 2b 52 8a 81 59 01 c9 72 1b 70 36 01 9a 1e 11 de 40 ce d5 0e 42 81 fe 25 64 64 8c 13 d8 27 03 80 70 33 c7 7e ac c1 71 90 0d 66 19 58 0c a3 32 b5 62 01 d5 88 e6 49 cf dd f7 5e 1c 14 e9 00 ad a1 c9 00 a7 23 24 03 9c 64 7c f9 ff 00 2e 32 7a ec 31 21 d6 92 5a de bb d9 8e 4d 1c cc bc e6 6a 12 c2 b0 12 99 72 f6 e4 9e c9 75 78 19 19 e4 40 e0 24 02 3f 10 3d 0d 24 62 37 df eb 13 de c0 3d b4 6c be 82 0a 03 ea 74 92 70 56 a0 9c 9e c5 2b 38 c6 d4 9c 77 20 Data Ascii: '=hw~3WmTjK#Y,p`Ja9IglvE-R%~N#KZ+RYrp6@B%dd'p3~qfX2bI*#$d|.2z1!ZMjrux@$?=$b7=ltpV+8w
2021-10-29 15:22:59 UTC	201	IN	Data Raw: 75 b5 6e 53 53 3e 1f 2d ee c0 2e a5 d7 9b 4a 50 37 6b a9 c0 51 72 a0 58 02 05 8b 1e e3 a7 cb 84 65 6a 95 2d 0a 92 65 04 a5 53 4e 05 2e 6a 09 46 05 05 2b 16 4c 0c c2 91 ad 98 07 df 70 ad e1 32 a9 6e 06 62 2d 32 27 3f 4a 6d 92 94 a5 a0 98 73 29 f2 dd 14 f5 a4 07 58 21 49 75 4e 15 07 42 d7 b4 30 e1 f3 50 ad bd 5c 4b 49 25 2a 21 92 9b 97 cb 76 67 f9 e4 62 13 4e 3d 70 70 b5 cc fd 14 94 ad 38 52 2e 41 29 cc 8e 60 c4 d0 5b 89 53 a3 34 f4 96 5d 5c a9 76 92 5d 42 d9 78 2d f6 13 05 4a 24 a8 ad 5e 4a d4 2a 31 a7 a9 c4 34 36 aa 34 e7 14 10 c8 53 cb 12 e5 cc 40 59 b3 be ec 9b 2f 6d 7b f0 81 04 ce 04 a5 58 54 40 7c 24 87 f8 42 00 37 fe a4 28 e8 6e 22 ea 28 99 12 52 2a 4e b0 b7 9c 7f ce 42 a3 3c 97 99 52 b1 82 e2 54 94 84 3a db d1 e6 ad b8 cb 53 6a 6a 3b 0e 36 1b 49 Data Ascii: unSS>-.JP7kQrXej-eSN.jF+Lp2nb-2'?Jms)X!IuNB0P\KI%*!vgbN=pp8R.A)`[S4]\v]Bx-J$^J*1464S@Y/m{XT@\|$B7(n"(R*NB<RT:Sjj;6l
2021-10-29 15:22:59 UTC	202	IN	Data Raw: aa 5a 92 bc 13 01 c5 2e 74 a1 31 2c 41 07 12 6c cc 79 37 ce 15 50 e7 a9 58 1c 92 01 23 20 9c 60 7e 5f 3c 72 3e 7d ba 50 e6 3b 8f 81 83 0a 70 0e dd b3 83 ff 00 a7 00 10 32 33 9c f3 cf 4a 39 09 f2 de c3 6b 07 1b 4e d0 01 39 3e ea 23 07 bf b0 ec 41 cf cf a5 0a 1a 33 1c 2a 98 c2 11 8c 85 24 f6 03 03 93 ed c7 f3 07 b7 6e dd 28 50 e1 2a 29 64 6d db db 84 e3 04 00 06 47 23 1c e7 19 fa e7 b0 e9 42 82 7e 61 50 27 76 14 77 29 44 0c 70 7b 27 8f 91 29 cf 1d cf be 0e 14 28 6c 4f 05 61 c2 0a 78 56 08 38 23 27 19 23 70 4a 47 61 c9 56 73 df a5 0a 39 c6 f1 32 d9 d6 6f b7 0f c2 76 9d 37 e6 bf 4c d1 5b 0a 05 d9 55 6c 63 c9 83 54 a3 52 75 1b 58 da 7d c0 12 55 b9 e7 45 82 d1 42 90 9d eb 5b 08 50 3b 50 ae a5 22 c5 f2 e7 af 08 12 c8 c2 81 a8 0c 46 ee 7b ac 79 77 88 df d4 46 0d Data Ascii: Z.t1,Aly7PX# `~_<r>}P;p23J9kN9>#A3*$n(P*)dmG#B~aP'vw)Dp{')(lOaxV8#'#pJGaVs92ov7L[UlcTRuX}UEB[P;P"F{ywF
2021-10-29 15:22:59 UTC	203	IN	Data Raw: 5c 7f 5f d4 79 3c 41 fc 5e a6 9d b5 ba 29 4f b4 54 48 2d 89 6f 98 79 61 9d be 9f 23 12 d4 97 c2 92 9d a0 f1 ce 7b e4 63 81 b4 82 55 8c a4 92 07 cb b7 1d 7a 42 7a c2 a5 11 72 04 f1 e6 37 de d1 f2 20 71 31 60 90 48 42 43 f7 8f 3d 0f 7c 27 97 f1 9e ea 4e e1 9c 24 f6 03 07 db 91 c1 e7 6e 40 ec 7e 49 44 31 0e 1d 8f a4 3e 01 32 00 19 23 03 6f 21 59 24 10 3d 23 9c 8c e4 8c 14 fe 43 27 80 18 50 49 c7 49 38 49 c9 ce 79 23 b0 e0 9c 61 27 93 ee 47 18 c6 4f 4a 0e 32 1c 87 a4 66 ec 39 0a df 92 09 4e ed c3 6a 7b 7a b0 01 29 ca 81 1d b0 a0 4e 3b 91 d5 40 cc 73 11 d8 7b 45 97 90 39 19 da 85 7a 81 04 9f 52 33 db 95 03 9e d8 18 07 3c f3 d4 81 f2 3e 86 02 a5 3d b4 f5 f7 a4 2f 35 21 23 68 27 24 92 a3 91 83 90 15 fc 5b b8 23 bf b8 00 f0 72 7a e4 36 1c 51 a7 84 a5 38 09 Data Ascii: _y<A^)OTH-oya#{cUzBz,; 7 q1`HBC=|'N$n@~ID1>2#o!Y$=#C'PII8Iy#a'GOJ2f9Nj{z)N;@s{E9zR3<>=/5!#h'$[#rz6Q8
2021-10-29 15:22:59 UTC	204	IN	Data Raw: 8e 85 e1 28 50 5d 92 65 32 77 13 9c 52 54 cc 33 06 14 bb b9 7e ff 00 07 d3 e8 f0 0c 37 82 4a 9f 2f 02 31 b5 8c a8 00 84 00 52 a5 7e 20 5d dd b9 c0 9d e1 6b 46 f5 96 f0 95 24 07 25 18 4b bb f7 5c d9 b3 7f 7d f1 12 4c 85 a1 b8 f1 df 6d 37 8d de 7a c7 35 46 96 ed 56 4c b5 ef 3b d0 58 69 03 20 21 ac 29 39 6c 00 12 ae 4e e7 97 94 e1 3f 88 fb 07 9c 8f 23 e9 16 f2 50 c8 56 26 24 05 33 f0 1a ef f5 8e 97 ed 17 02 6c 8b 31 2a cf ff 00 81 f6 d0 52 b9 ca b1 43 82 14 77 63 03 3b 78 3c e7 3f 88 f5 c4 fc 23 bf e7 18 e9 df f1 73 b9 9f 58 31 51 a9 c3 a3 c4 9b 58 9e ea 1a 81 48 87 2e ab 35 e5 a8 25 b6 61 53 a3 b9 3a 6b ab 59 56 02 5a 8e c3 ae 92 78 48 46 4f 00 f4 95 f0 a9 f7 17 7d d9 69 c3 ef a9 81 17 c4 31 64 e0 0d da 33 fc fc a3 81 1d 16 a7 4b d5 5d 25 fb 40 7c 43 d4 81 Data Ascii: (P]e2wRT3~7J/1R~]kF$%K\}Lm7z5FVL;Xi !)9lN?#PV&$3l1*RCwc;x<?#sX1QXH.5%aS:kYVZxHFO}i1d3K]%@|C
2021-10-29 15:22:59 UTC	206	IN	Data Raw: b0 2c 78 ee d7 cb 3f 5b b3 25 d5 a2 64 b0 25 20 92 a5 61 98 a1 8a 66 36 38 04 d2 06 a8 70 34 ed 12 06 26 8b c3 a6 3a a4 ea 25 c7 0d b2 86 63 48 59 46 12 85 87 a2 4a 0d a0 31 2d 65 78 2e b6 97 63 c8 69 c6 4a 9a 53 8e 5a a3 95 b4 8d 8b 56 da 8a b4 4c 4b 7e e0 06 17 cc 1b e5 7b b3 58 ee 0c 23 19 59 41 3a 9c 28 a8 cb 90 15 88 09 52 c0 b1 5f ea 29 78 ad d9 9a 54 4a 6d d8 04 70 11 a5 3a 69 7d c6 b8 a2 c1 5b 92 41 8a a1 12 95 5b 83 21 d0 95 37 26 28 69 a0 e3 ac ba 56 dc d8 e9 79 2a 44 92 94 a5 6f c0 71 6b f3 d0 a0 b6 d9 8f a7 9e bc 27 1a b0 cc 2e 10 a1 9b 9b 5b d0 6f 78 c8 54 a4 8c 58 95 d6 0c 41 38 1d ee 5f b3 77 70 97 7c 79 9c 8e 51 b2 fe 18 75 41 ca 8c 0f f6 7b 59 96 65 4a a4 b2 5f b7 aa 4e bc 1d 72 75 35 e0 a7 93 4f 75 61 4b 6d 4f 53 96 5c 8c 87 1b 94 f2 9d Data Ascii: ,x?[%d% af68p4&:%cHYFJ1-ex.ciJSZVLK~{X#YA:(R_)xTJmp:i}[A!7&(iVy*Doqk'.[oxTXA8_wp|yQuA{YeJ_Nru5OuaKmOS\
2021-10-29 15:22:59 UTC	207	IN	Data Raw: e1 b0 0b 4d b3 e6 1c b8 39 e3 6f 7c 1e c3 8f 61 9c 1c 75 1e 9e 81 6a 51 d1 8a 8b 17 7c c6 fe f3 6b 35 cc 0b 6d 54 c8 a8 1d 82 09 01 9c 69 cb df 38 98 2d 7d 7f 45 2a 4b f1 18 79 11 9b 98 b5 3e a7 56 e7 ad 2b 2a 20 a5 39 3e e7 d8 63 9c f1 9e b4 3b 36 88 4b 13 14 dd a0 46 62 ef 62 df ce 83 47 8f 38 da c2 4c e4 a8 4f f8 10 0a 53 77 cc 6f f1 b0 cd e3 41 34 77 c6 54 ea 6d 30 51 99 74 3c 85 34 a6 ca d0 ef 2a 2a 0a ca 95 ef c6 47 3c 92 47 cc 71 b6 d9 d5 d3 04 9e a1 f8 ee 16 0c 5b 4d 39 f0 8f 9a ba 63 f8 73 4f b5 76 82 6a 70 ba 94 a1 31 36 7e ce 2f b1 be eb 06 84 ba 6e b0 c5 af ea d5 38 39 2f 7c 89 93 d4 b0 92 ac 8d ca 70 13 8e 4e 46 4f 3d 81 ef c6 33 d4 ed 8f 50 51 b5 92 15 92 88 4b 3d 9d ff 00 96 b3 f3 d7 03 f8 a3 d1 39 92 7a 07 55 80 1c 32 25 b0 b1 6b 23 2f 2e Data Ascii: M9o|aujQ|k5mTi8-}E*Ky>V+* 9>c;6KFbbG8LOSwoA4wTm0Qt<4**G<Gq[M9csOvjp16~/n89/|pNFO=3PQK=9zU2%k#/.
2021-10-29 15:22:59 UTC	208	IN	Data Raw: 92 5c db b1 68 cc 8c 0a 52 3e 25 39 19 b9 3e 3f 3d f0 c1 39 29 5f 68 06 bd 98 1c 86 ed 37 e7 dd 0e 2a 4b 92 2e 39 28 7c 32 f9 a6 a1 c0 da 3c e0 e0 4b ee a0 92 13 f8 8a 13 1d be f2 94 09 ce 42 46 5c 75 c0 d8 15 82 4b d8 13 bc 87 55 f8 e7 ef 9b 49 46 29 e7 72 45 9b 20 dc 78 6e b6 b0 b9 73 5c 46 81 18 53 e1 1c d5 25 35 e5 b2 ad 87 6c 66 89 0d 2e 7b 8a 5a ca 52 01 43 8c c2 4a 86 10 a4 a9 f0 14 36 87 25 d1 4a 35 0a 0a 9a a2 94 fe db 9c 80 63 cf 87 ac 43 ac 5f 50 54 99 60 13 61 96 59 3e 4c dd d9 b8 bc 16 b0 5d f2 24 fc 42 88 2a 25 3f bd c2 54 4b ca 24 ef 2a de 97 0e de 14 b5 8c 87 16 ac 90 14 49 3a 29 45 49 fd 34 3b 0d 6f 7c b7 37 0d 3e 51 9f a8 00 02 b7 75 2b 3c 45 d8 b6 47 93 3f 8c 5b 0d 3f a1 26 bd 2d 05 dd ca a6 45 d8 fc b2 b5 04 35 37 2e 29 68 82 97 77 1d Data Ascii: \hR>%9>?=9)_h7*K.9(|2<KBF\uKUIF)rE xns\FS%5lf.{ZRCJ6%J5cC_PT`aY>L]$B*%?TK$*I:)EI4;o|7>Qu+<EG?[?&-E57.)hw

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	210	IN	Data Raw: dd bf ed 39 0f 07 9c a2 dc 90 fe 2d 98 d3 5a 6d d6 9a a8 53 1f 69 71 e7 d1 aa ac 36 f3 88 62 a7 48 97 02 a2 c2 5c 75 b6 65 b6 87 1d 4b 89 5f 11 ee ee b4 75 28 b3 78 9d cf ef db c7 20 7f 68 bf d9 fb 79 78 3d bb 9d bb ac b4 55 eb fe 1e 6e ea bf 95 68 dc ce 3c a9 d5 0b 36 a7 30 bc fb 56 45 e6 f2 36 ba 26 36 84 86 ed cb 85 6d 31 0e e6 a7 b2 84 36 eb 75 c8 d3 e3 20 88 52 bb 4c a2 3b c8 cf 97 21 0d 9a 94 a5 16 48 36 cd 81 e7 98 ee df df 19 a5 16 a3 50 68 91 f1 1e 6b 69 6d 69 52 de 42 5f 50 00 36 92 10 54 d0 28 5a 52 02 72 b3 80 36 a4 e1 38 e8 89 9b 52 10 e4 82 d9 62 bf 01 9f be f7 02 22 29 e9 80 c7 85 95 a8 61 c7 81 1f 3b c3 c6 da b8 1f 2d a6 8d 53 5a 9b a4 3c a2 9a 7c a4 3c 88 c9 a3 c8 90 ff 00 9a ea 24 49 0b 43 28 a4 cd 7d 6e 3b 31 5e 63 6e 53 a5 94 d4 62 bd Data Ascii: 9-ZmSiq6bH\ueK_u(x hyx=Unh<60VE6&6m16u RL;!H6PhkimiRB_P6T(ZRr68Rb")a;-SZ<|<$IC(}n;1^cnSb
2021-10-29 15:22:59 UTC	211	IN	Data Raw: 01 5c 17 3d 39 b6 5b 97 13 fe 32 3f f8 94 12 36 8c 67 69 18 fc 39 c0 03 bf cf f3 e5 25 32 eb 27 aa 51 72 85 30 23 5d 49 1c f8 db bb 38 d0 1d b9 4e 53 d6 0c 38 90 1d 81 17 36 b6 a0 fd 07 84 35 56 ba 66 54 de 2e 94 b8 94 af 29 69 08 e7 b6 79 1f 3c 7e 63 9e 01 f6 eb 5f b3 e9 68 e9 c7 52 a0 ca 19 be 6f 98 d0 e5 a5 e3 33 b5 7a 55 51 30 19 72 a5 b8 76 60 2d cc ee dc 7c 63 e5 2f e2 26 ba d7 9e 5c 52 59 e5 25 64 0c 0c f2 3f 31 db 9e df 43 d5 92 cc b0 92 84 76 74 7b 07 0c ce 45 bc bd 22 be 4d 34 ca a5 89 d3 12 ed aa 81 b3 b6 44 eb de e1 bc 24 38 52 5c a7 07 77 29 49 65 c4 6e 69 c2 49 29 c2 72 70 33 ee 7b 1f 6e c4 11 d5 44 e9 4c 5c 17 2f cf d3 cb 9d 9a 36 3b 36 a1 54 fd 86 0c cc 1e fa 33 e7 66 f7 c5 cb 6f 6c 9f 29 07 e3 57 20 28 65 4d e7 24 12 7d 81 07 8e 4f f2 fe Data Ascii: \=9[2?6gi9%2'Qr0#]I8NS865VfT.)iy<~c_hRo3zUQ0rv`-|c/&\RY%d?1Cvt{E"M4D$8R\w)Ienil)rp3{nDLV6;6T3fol)W (eM$}O
2021-10-29 15:22:59 UTC	212	IN	Data Raw: 72 40 3c 02 91 c8 c8 fc 27 d9 aa 2c 09 1e ef 0e 4d d4 3d e9 1c e2 4e 70 fd e5 3c 8c e4 ce 9c 36 9d aa 23 fd e1 e4 90 73 82 41 05 39 21 39 56 3d 4d f4 c4 e8 75 2a 6e e8 b0 16 96 92 33 fb 11 1e 50 12 37 28 92 3d 6e e3 b8 50 f5 28 91 81 d8 e0 e3 2a ee 9d a0 71 8c 16 39 f1 29 24 e6 0d 8e ef 94 31 f5 03 53 ad ed 38 a5 87 ea ca 33 2a 92 5b 5a e9 74 46 16 94 ca 96 94 af 1f 17 25 c2 15 f0 54 d6 1c c2 24 4b 5a 54 b2 af dd 43 46 63 81 c4 21 38 19 b3 71 2d 1c 51 4a 14 4b 39 b7 3b 77 8e f8 ca bd 57 d6 cb 93 50 ea ce b6 c4 f5 b8 e9 0a 8e e4 c6 41 44 1a 74 4d db be 02 8c d6 e7 3c a4 20 82 1c 9a a3 e7 49 73 2b 75 d7 97 89 2f 46 9d 3d 21 da dc be 9e c7 7d a1 21 2a 9a b0 95 b9 1b b2 f6 7b 8e ed c2 23 ba 35 0f e0 db 52 d1 b4 2d 58 52 de 71 4b 58 01 6a c1 25 6a 0a 49 94 a7 Data Ascii: r@<',M=Np<6#sA9!9V=Mu*n3P7(=nP(*q9)$1S83*[ZtF%T$KZTCfC!8q-QJK9;wWPADtM< Is+u/F=!}!*{#5R-XRqKXj%jI
2021-10-29 15:22:59 UTC	213	IN	Data Raw: 21 09 56 13 94 16 ce f5 0d e5 07 9c 04 15 0c 25 66 e6 82 a1 24 24 64 45 dc b6 99 f0 c8 e8 22 9f 6a d3 05 48 9a 08 49 22 e8 c2 90 15 8c 64 2c c4 be 4d 60 33 36 bc 5f 0d 32 bb 27 47 f3 54 c2 de 5a 13 2a 43 ee b8 95 a9 a7 5a 69 4b 8a a6 83 2a 56 e6 63 b6 97 32 ea bf 78 85 84 e0 2d 6c e4 06 f6 54 55 0c 80 16 5d 40 86 2d e3 97 9d 9b 23 be 3c f6 a5 06 72 51 21 d6 26 4e 5b 4c 5a 09 0e 52 2c e4 64 e4 a9 25 21 88 c0 a2 f7 8b 4f 4a bc 54 ed 2a e7 6a 3c d7 19 71 ca 8c 74 b4 a5 2d 0e c4 72 5f c1 27 39 2e 3e cb af 14 a1 f5 b6 cb 65 b6 b7 38 cb 73 92 88 e5 1e 73 97 94 b3 92 f8 b5 36 24 87 77 17 e5 6b 0c 99 b9 c5 2a a9 42 f1 53 4b 99 85 29 24 92 90 f2 dd 2a 75 95 92 e7 12 4d 93 7b e7 7d 51 2b 37 7f 9c e5 59 b1 29 97 10 d4 e5 34 c2 dd 75 6d 30 82 a8 94 ad c2 33 aa 70 a9 Data Ascii: !V%f$$dE"jHI"d,M`36_2'GTZ*CZiK*Vc2x-lTU]@-#<rQ!&N[LZR,d%!OJT*j<qt-r_'9.>e8ss6$wk*BSK)$*u M{}Q+7Y)4um03p
2021-10-29 15:22:59 UTC	215	IN	Data Raw: d9 3e e3 fa 9e b0 40 01 60 18 68 37 46 f4 e6 79 98 6b cc 91 ca f0 ac f3 c8 e7 8c fa b1 80 08 07 9c f7 e7 b1 f7 1d 22 5e e6 39 0d f8 ef 87 1c 70 9c 93 9e 09 39 07 eb cf 6c f1 8f a6 70 01 1c 28 50 4e 50 68 af 94 ee c1 da 00 c0 c9 dc 7d 47 e6 47 00 8f cb a7 a3 33 ca 14 00 f9 88 36 95 24 02 38 23 6e 4f 03 bf be 71 cf f4 f9 74 8a 88 27 70 26 d6 fa 42 8a 3d f6 8f df b1 f4 f7 c1 0f 89 4b 82 3b 9f 0d 2a 66 95 d6 ec c8 2f 82 84 38 dc ed 49 5b 16 0c 47 1b 52 ca 47 98 d2 ee 4f 3f 00 ee 01 92 5b 0a 5a 7a 70 25 45 f2 1a 8d fe 5a 88 62 cb 02 35 20 f7 5b 38 85 be c8 fb 0a 35 91 e0 37 44 16 f4 56 db 99 7b c7 bb 75 0e 77 a4 fe f0 dc f7 9d 79 ca 44 85 85 e1 5e 63 d6 c4 3a 02 42 8e 53 e5 a1 ad b9 46 d5 17 4d 52 8a d2 0e 41 98 5b 7f bc e1 92 87 e9 b9 f8 86 5b b9 b3 7b 77 8b Data Ascii: >@`h7Fyk"^9p9lp(PNPh]GG36$8#nOqt'p&B=K;*f/8I[GRGO?[Zzp%EZb5 [857DV{uwyD^c:BSFMRA[[{w
2021-10-29 15:22:59 UTC	216	IN	Data Raw: 05 44 9c aa 9e c2 bd 5b bf e4 c1 0a 3c 80 14 48 c6 47 a4 1f 61 db de 36 68 29 a1 90 49 ed 14 a7 16 e3 d9 07 22 f1 f8 f9 d2 74 9f ef fd a8 a7 07 fd ee 6a 6d 6b 62 27 2c 9f 2e 7e 10 b8 eb 9b 72 a2 49 20 fb ee c6 7b 12 9c 95 13 9c 1d aa 00 71 8c 10 15 d4 dc 4a df e4 22 86 0b 3c b0 73 83 95 9e 00 c9 03 07 39 c0 db 9e 48 dc 79 1e db 78 e9 b0 a1 2d c7 53 9c 72 4f bf 20 02 47 19 49 04 64 1f 96 38 e3 e7 d2 83 20 b8 e5 6f 21 19 31 f7 e2 12 ae 1d 1b 90 13 c0 52 47 2b 50 ce 15 c9 51 08 21 40 e3 b7 03 19 ea a0 66 39 8f 58 71 60 2d 73 6b 65 ce fc 3d bc 1c 8f 70 a0 e3 2a 48 18 04 8c e5 45 09 1c 92 33 8d d8 00 77 04 81 9c 67 a9 29 ba 80 39 17 1e 22 1a ea fe 9f 3f b4 2a 1a d3 0e 2b 1e 6e 06 7d 44 28 91 8c 93 b4 61 4a e4 e3 3c 63 18 19 fa 1c 25 22 c1 47 3d d0 35 3b 97 0d Data Ascii: D[<HGa6h)I"tjmkb',.~rI {qJ"<s9Hyx-SrO GId8 o!1RG+PQ!@f9Xq`-ske=p*HE3wg)9"?*+n}D(aJ<c%"G=5;
2021-10-29 15:22:59 UTC	216	IN	Data Raw: c8 50 50 ed 90 48 00 27 69 ce 07 38 c1 1d 72 1b 07 0d 59 04 12 a7 88 20 a8 00 a5 64 91 95 24 70 02 37 24 00 30 41 1d f7 00 42 4f 4f 08 70 ef e5 f7 85 02 b7 51 49 01 79 4e 09 1b f2 a0 a2 4f a4 80 92 4a 52 46 10 9c 02 a0 77 1c fa b8 1d 3d 29 c2 fc 61 42 ab 32 52 e2 40 52 d2 02 b2 90 48 3e 66 14 08 2a 25 5b 46 77 10 ae 09 3c 67 6f 04 f4 e8 50 e3 8d 21 08 da da 4a 8f a7 bf 24 e7 d6 09 dc 55 91 b4 f6 03 76 d1 d8 7b f4 a1 42 d4 69 2d a9 09 25 20 a0 90 bf 52 b7 9c ed c2 4f 39 da 30 92 12 4f 73 d8 a0 e4 95 0a 0e a1 d0 0b 8a 48 da 12 a0 42 14 08 da 91 bb 29 ed ce 72 4a bb 67 f1 0c 81 b8 a8 50 bf 0d dd c9 04 64 a8 9f a1 ce 14 71 b4 14 e3 9d d8 e3 f9 91 d2 87 14 b0 77 dd e7 0e fa 71 56 52 72 a1 c6 0a 87 cc 80 39 3b 40 c9 20 12 4e 06 07 7f 7e 94 36 1f 34 64 90 fc Data Ascii: PPH'i8rY d$p7$0ABOOpQIyNOJRFw=)aB2R@RH>f*%[Fw<goP!J$Uv{Bi-% RO90OsHB)rJgPdq8wqVRr9;@N~64d
2021-10-29 15:22:59 UTC	217	IN	Data Raw: 8c 64 65 3b 69 10 d3 d8 00 90 7f 21 df dc 73 89 11 8c 5d a6 ce 50 be 5e 64 8e ec be f1 cd 0f fe 23 9b c6 4d 5e df f0 93 a2 14 c7 0b 93 ee bb e2 f5 bc 3e 01 bc ba e3 d2 e2 c4 a0 58 f6 e1 f2 d0 42 d7 e6 c9 bb 6b 8c a0 81 f8 db 75 3b 88 0a 49 89 34 ba b8 78 70 f9 40 c3 d8 b1 d0 e4 79 c5 87 fb 5d ac b4 db 7e 11 34 93 49 a9 2e 47 8d 16 da b5 45 81 11 4e 29 0c 46 87 48 b5 53 a4 16 ef 99 21 c0 92 db 10 e2 d2 a1 79 93 1e 5a 76 33 15 97 9e 73 6a 12 a3 d1 a4 a4 aa 70 49 f8 57 67 d4 68 e3 c3 88 ef 80 56 2a 78 a7 9a 25 7e f2 0b 7f 4e 10 d6 e6 da f7 47 1c d7 ad 3e 1d bd 5c 9f 42 75 c5 d5 24 d1 2e 3b 82 9c f5 42 95 56 65 ea 44 a6 a2 cd 4b 11 fe ec 4b d4 e4 ad 71 17 1d b1 21 b9 eb 6d 81 2d 97 81 43 28 4b 69 cc a9 cc 85 99 6a b6 04 92 15 aa dc eb cb cf 73 c4 6a 71 3a 6a Data Ascii: de;i!s]P^d#M^>XBku;I4xp@y]~4I.GEN)FHS!yZv3sjpIWghV*x%~NG>\Bu$.;BVeDKKq!m-C(Kijsjq:j
2021-10-29 15:22:59 UTC	219	IN	Data Raw: ed 52 81 6c 3e e7 96 a6 c0 4b 65 69 09 79 b6 97 90 82 5c f3 46 d5 93 d5 96 cc 9c 56 a4 15 76 ce 58 74 62 c3 31 bb 77 cc c6 77 6b 51 ca 56 39 85 29 ea 7b 52 a6 30 09 18 8d 8a 83 6a 03 32 ec a1 6b eb 17 8f 49 ee 19 11 af 08 51 54 eb 82 3a a9 ca 6f 24 2d 0d 8f 29 e9 8c b0 a2 84 23 6b 9e 4b 4d 2c be 95 38 ea d2 cc 81 b9 d3 e4 04 b9 e8 1b 34 25 0b 02 5a ce 22 09 c3 ba d9 36 b9 69 94 61 2b 91 2e 9d 29 52 d3 d6 f4 79 c5 3e 4b 4d e1 1e 5b 75 1a 0d 06 a4 ca cb 63 01 3b dd 72 68 04 15 b6 e1 6d 4b 4a 8e e3 d6 37 a7 f2 e6 7f 79 d2 92 a2 a4 2e 94 24 28 87 b8 21 4b e0 e1 c0 ef e3 1b 0e 80 89 63 65 4f a6 49 63 2e a6 65 51 52 98 28 ae 69 25 28 3f e5 67 be 76 Data Ascii: Rl>Keiy\FVvXtb1wwkQV9){R0j2kIQT:o$-)#kKM,84%Z"6ia+.)Rv)@'>GYTLz1%Q6>KM[uc;rhmKJ7y.$(!KceOIc.eQR(i%(?gv

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:22:59 UTC	220	IN	Data Raw: 1f df 19 ea 72 a6 51 3a 4c d4 60 c2 46 41 af bb 4c f9 e5 10 aa b6 a4 a7 49 59 01 58 93 91 bb f2 3b fc 73 22 15 e9 21 d4 3c c0 59 4a 1b c0 f3 09 3b 55 b8 fb 1e 47 d7 8e 8f 53 2a 9a a2 52 a6 ca 1f 0a 0d 9c 30 00 5f 9f f2 32 b4 49 91 51 32 ad 61 08 20 4b 47 69 c6 ad 9e 76 bf 07 d7 38 97 ed b4 3e cb ad bc 1c 56 d7 5d 01 5b 55 8c 24 e0 e7 db 3f cf e9 f9 50 4e 4c a0 8c 29 b2 b7 06 bb 7b bc 4c 4c 8c 25 f1 ab e9 f5 f2 e5 ba e3 d9 15 66 98 8f 05 b4 86 dd f2 70 e1 e7 71 e3 be e1 9e 4f b8 f7 c7 eb d6 7a b6 99 2a 38 94 19 b8 06 d3 bf 8f b1 1e 83 b0 10 24 4b b1 c5 61 73 c9 cb 59 fd 8e fb 17 6d 5c b4 ca 64 f6 a7 3a b6 54 e3 85 29 4b 2e 14 85 12 a2 38 08 27 3e 9f 7c 0e df 3e 73 49 51 21 4a 4a c0 24 4b 50 b0 b6 eb e8 35 f7 70 23 5d 4b b5 64 d2 2d 29 51 18 d5 6c f5 e3 cd Data Ascii: rQ:L`FALIYX;s"!<YJ;UGS*R0_2IQ2a KGiv8>V][U$?PNL]{LL%fpqOz*8$KasYm\d:T)K.8'>|>sIQ!JJ$KP5p#]Kd-)Ql
2021-10-29 15:22:59 UTC	221	IN	Data Raw: a1 c3 43 6c 33 16 5d 51 f0 3c b6 90 14 e9 73 d5 ff 00 1e 52 c2 1d d9 1f 7b 8e 10 d2 4a 1e 9c f6 d4 bc b0 86 95 e4 49 a7 a4 9a 26 39 4f 67 73 69 60 78 5f 9f 8c 3d 73 53 d5 76 41 0e dd f9 3e a4 b7 f1 0a 14 ba 63 f5 07 3c c7 5c 76 4c b9 2e a5 6b 2f 13 bc ee 0a 21 b2 12 bd bb 5a 27 05 0d 92 85 21 ad ae 82 94 a9 48 b4 51 32 81 2a 64 b0 c8 e6 72 ca f7 6f 0b c4 59 69 5c d5 00 c7 3d 6e 2f 7d 37 fb b4 48 0d b3 12 82 c9 52 92 d3 d3 5c 04 b2 da 12 10 4a ca 50 94 3a b0 ad 8a 69 07 d4 f1 46 5e 52 0a 8e e4 05 f5 0f 1c ca a5 30 70 01 7b 91 76 cb 5f 1e 5b e2 c5 41 34 c9 c6 b6 05 80 b6 a4 ef e4 f7 e5 c6 3f 52 d8 90 a9 0a 94 e6 d7 9d 5a 50 5c 2a d8 a6 93 b1 24 38 4f 25 08 69 a0 16 a5 2b 1c e3 72 b7 29 41 26 ce 53 a0 04 06 bb 39 6c e2 86 b2 6a ca f1 df 08 2e 00 f1 d7 77 d5 Data Ascii: Cl3]Q<sR{JI&9Ogsi`x_=sSvA>c<\vL.k/!Z'!HQ2*droYi\=n/}7HR\JP:iF^R0p{v_[A4?RZP*$8O%i+r)A&S9lj.w
2021-10-29 15:22:59 UTC	223	IN	Data Raw: 1d 61 36 c6 d4 91 b4 6a 70 9e b0 4a 92 4a 25 02 d6 17 6b 82 de 1c db 30 3d 0b 63 f4 66 a7 67 d3 cc 5a 44 95 29 43 12 ca 71 5d 5f bb 31 eb c0 e5 0b 1e 11 be d2 0d 54 f0 c7 a2 d4 9d 35 b5 f4 92 d5 be 68 71 eb b5 9a eb 35 aa c5 46 bd 0a 52 5f ac 35 11 32 21 04 52 ea 4c 31 e5 c6 31 12 e3 59 8e 54 a5 4a 5a 7d 28 4a 42 2a 15 39 32 e6 60 0b 6b 02 01 94 85 d8 bb 3a 89 70 38 5f 46 89 e8 a2 9f 3a 41 9c 99 6c 02 d4 83 93 95 26 c7 b8 bd b8 36 67 3b 32 3e da dd 0d 6e 58 52 9d f0 dd 64 ed 18 c0 62 b5 76 ac fa 8e 30 a0 aa be 02 b6 94 65 20 29 3c 82 15 df a2 7e 71 29 2d 31 6e 2f 84 89 69 43 e4 ef 86 e7 4b 9c bd 38 8d 97 52 c5 4c 2f 90 bb d9 f8 44 13 e2 63 ed 45 d4 7f 10 da 17 a8 7a 39 73 68 1d b9 6e d2 ef 2a 7d 1c b9 70 43 aa dc 12 25 51 57 41 b8 68 f7 44 4a 83 31 a5 4d 71 Data Ascii: a6jpJJ%k0=cfgZD)Cq]_1T5hq5FR_52!RL11YTJZ}(JB*92`k:p8_F:Al&6g;2>nXRdbv0e)<~q)-1n/iCK8RL/DcEz9shn*}pC%QWAhDJ1Mq
2021-10-29 15:22:59 UTC	224	IN	Data Raw: 26 6b 03 4b 0a 40 f4 5f 56 93 c9 0a 52 b6 23 21 74 54 94 6f 24 2b 1d fd 69 1c 05 8e 85 f9 da 35 ba 4c f4 6a 0b 3b d9 9d ac 3e b0 49 db 26 bd 08 7f ca ae ec c4 0c 9c b3 9e 59 97 d2 f1 98 be 3e 7e d0 eb 5b c5 8e a0 78 5d 4b 9a 31 7c db 36 6e 94 df 53 ee 7b b6 cd ae d7 ad fa 9d 52 fa 85 5b af e9 fa e5 c1 38 6a 2a 9d 19 98 91 97 f7 2d a1 5a a4 b2 a9 c9 79 a5 3f 52 7c b8 8f 2d 0b 0a 9f 4a a9 3f 97 5d 42 66 a7 ab 0e 1b 25 3e 6e 1c 65 e9 e9 02 a2 8e 7a 27 7e 5d 52 cf 59 65 27 72 9f 30 2f 7b 0e 31 a1 b1 be de 0d 1d a4 17 e3 37 e1 6b 5a 29 ee b6 57 b9 10 aa f6 63 28 4e c5 15 28 36 18 8a c3 64 ed f5 1d 8a 09 4a 4e de 14 09 5f 04 d4 29 2e 99 a8 b6 ef ab 11 68 ea a9 aa e5 16 34 e8 0f a9 fe 5f df 38 82 fc 51 fd b2 7a 7f e2 03 c3 d6 ad 68 c5 b7 a2 da b9 67 d5 f5 22 d8 66 Data Ascii: &kK@_VR#!tTo$+i5Lj;>I&Y>~[x]K1|6nS{R[*-Zy?R|-J?]Bf%>nez'~]RYe'r0/{17kZ)Wc(N(6dJN_).h4_8Qzhg"f
2021-10-29 15:22:59 UTC	225	IN	Data Raw: b3 38 7e 6e d6 e1 1a 4b e1 8d 89 b7 6e a6 d9 76 e4 70 e3 cd 35 21 89 af ed 4e fc 36 da 9b 38 5e 72 30 4f 7e 3e 5e dd 0b 64 51 2e 75 7c b6 4f 65 2a 06 fa 5c 7c bc 2f 6b 5b 11 f8 b9 b7 8e cc e8 a5 6e 39 ca 2b a8 90 a2 96 3f e4 b8 67 bd ef ba d1 d2 23 71 d3 16 24 48 f8 cf 90 ca 11 c9 40 c6 c0 50 70 72 0e c0 32 0e 12 0a 8f a4 0e 73 d7 b1 a1 84 a4 22 ce 80 01 1d da 0f ad e3 f3 1a a2 6a a6 ce 5d 41 38 8c d9 b3 09 df ae eb 73 e3 6e 30 9d 2f 24 0f 52 7f 11 1c 1e 79 27 04 04 e0 a4 9f 7c 82 31 c1 1c f4 a3 80 b8 78 2e a7 b2 90 9d d8 db c7 1f bb 24 63 67 2a 05 3c 24 28 70 0a 90 92 71 93 c1 1d 01 ec 23 b0 9e b7 96 14 4a 09 dc 4e 4a 89 46 40 3e db b8 40 0a 23 3b 7f 17 00 8e 33 d7 0d ad 04 0b 01 83 1c a3 9e 2f 8b 5b a9 da 16 53 92 3d fd 7e 9d cb d8 ae dc 0d b9 00 a4 7a Data Ascii: 8~nKnvp5!N68^r0O~>^dQ.u|Oe*|/k[n9+?g#q$H@Ppr2s"j]A8sn0/$Ry'|1x.$cg*<$(pq#JNJF@>@#;3/[S=~z
2021-10-29 15:22:59 UTC	226	IN	Data Raw: 90 b3 e7 23 ab 2a 39 42 62 0c e5 58 0b 82 72 71 a5 9c c5 5d 54 d0 94 94 8b da ff 00 5e ed cd 78 4e a7 d3 54 10 14 e2 9a 43 7c 1d a8 40 4a 8a 91 ea 4a 4f 09 ff 00 ed d6 37 ef 2a 19 3b 88 06 5a a6 63 18 5f 08 e0 33 1e 3e 11 5f 2c 75 80 9c f8 e5 bf 94 0f 22 8e 65 3d f1 2a 42 5b 49 c0 69 b3 b8 a5 94 80 9c 38 a4 14 a5 2b 51 48 de e9 42 52 91 84 9c 92 b5 e1 b2 56 10 e9 7c 4a 00 96 e1 bf ed bb be 24 09 56 04 64 6c e0 58 91 eb 0f 28 31 84 58 c8 4a 02 23 c5 42 0a 92 ea d0 37 84 e4 02 a2 9d df 89 d2 a2 b5 24 05 10 5e 23 3b 06 00 57 30 28 96 21 cb 3d d9 9e db 80 b9 06 24 a7 f4 92 33 7f ad f2 dd e3 e7 0e 9a 71 6d dd 8e 38 84 85 b9 e6 29 94 b8 12 bd 88 71 65 e5 13 90 70 a7 bc c0 f2 c0 1c 24 a5 08 3b 49 23 b2 42 c2 89 02 c8 18 94 74 48 05 89 f7 dd ba 08 18 03 6b 9b ff Data Ascii: #*9BbXrq]T^xNTC|@JJO7*;Zc_3>_,u"e=*B[li8+QHBRV|J$VdlX(1XJ#B7$^#;W0(!=$3qm8)qep$;I#BtHk
2021-10-29 15:22:59 UTC	228	IN	Data Raw: 26 dd 9f bc e2 26 c1 6e a6 75 3a 88 4c c9 33 0f 58 96 2e 9b e7 96 9c 1d cc 58 a2 d0 f2 d2 b0 1a dc a2 da 02 82 52 0a 80 1b 81 3c 85 12 a5 fa 78 0a 49 f3 33 93 8c 75 4c 99 81 4a 29 c0 48 49 62 1c 0c b2 dd c3 86 91 a7 44 82 40 18 c2 82 80 c3 6c c3 9c ed f3 86 a5 45 b6 84 a5 92 d7 a8 46 79 e5 7b 9d e0 80 46 ec 8d ca 5e 54 a5 1c 8c 2f 27 05 59 1d 5a 53 4d 4f 54 4f 56 48 2c 12 4d b7 f7 f0 7d 39 c5 4d 4a b0 2c a4 23 52 34 b5 db 8f 95 fb e1 89 7b fc 32 ec 0d 41 2f a5 09 09 a3 2e 4b 3b 92 09 4b b1 a4 c3 11 48 21 25 48 5f 9e e2 0a 1e fe 05 8d d9 1b 95 93 0c 5d 6d 2a 88 21 2b 56 04 bf f5 67 85 b9 10 46 43 bf 38 f3 14 55 41 b4 50 a2 10 d2 42 c0 39 e1 4a 86 23 6d c5 49 76 df 67 11 43 59 8d f1 4b 04 b8 d3 09 dc 12 56 a1 90 13 e8 2b 05 29 ce 02 46 4e 06 e4 a5 44 90 37 Data Ascii: &&nu:L3X.XR<xI3uLJ)HlbD@lEFy{F^T/'YZSMOTOVH,M}9MJ,#R4{2A/.K;KH!%H_]m*!+VgFC8UAPB9J#mIvgCYKV+)FND7
2021-10-29 15:22:59 UTC	229	IN	Data Raw: c3 a9 d1 97 6e 3b 3a 22 96 87 09 6d 3f 18 ca dd 59 c2 76 29 09 2e 97 14 36 90 30 53 ce 0a 80 3e f8 be 91 50 19 67 f3 72 64 90 93 65 10 13 93 f3 07 7f cb 87 ad 7e 1e f4 8d 29 a8 14 73 67 25 41 6c 10 0f 0b 16 b6 f3 ec 96 86 dd 56 22 69 f3 1e 4a 9f ca 02 b3 85 03 b7 23 39 1f df b6 7a cf a9 62 54 84 ae 5a 5f 17 c4 6d 99 bb 5f c7 cf 3c bd 3b 68 cb 46 25 ad c6 05 0d 75 b3 8e 37 63 e0 c5 b5 79 58 4b 8b 22 ae 94 be 76 c5 5b 64 38 90 30 92 71 81 db 82 3b 77 e4 70 3a 81 fd e0 a9 61 4e 19 57 ef cb d3 8f 3e 54 d4 35 12 e9 aa d0 14 46 02 b0 55 9e 16 2f a5 fc f8 1c a1 85 aa 49 91 42 a9 49 54 46 c3 90 de 2a f2 f6 02 42 42 b9 1d bb 77 1e de c0 f6 ea e3 62 c9 56 d5 9a eb 3d 91 7b 9c d8 b8 f7 68 d1 d4 48 45 62 71 c8 55 f7 a5 c7 f9 b5 62 ef c7 7b c5 78 a8 aa 44 a3 90 83 81 Data Ascii: n;:"m?Yv).60S>Pgrde~)sg%AlV"iJ#9zbTZ_m_<;hF%u7cyXK"v[d80q;wp:aNW>T5FU/IBITF*BBwbV={hHEbqUb{xD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49887	104.26.7.139	443	C:\Users\user\Desktop\SEMqjw.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-29 15:23:42 UTC	230	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: */* Referer: https://www.msn.com/de-ch/?ocid=iehp&AR=1 Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: btloader.com If-None-Match: "643eb1aad6ba3932ca744b96ffc00048" Connection: Keep-Alive
2021-10-29 15:23:42 UTC	230	IN	HTTP/1.1 304 Not Modified Date: Fri, 29 Oct 2021 15:23:42 GMT Connection: close Cache-Control: public, max-age=1800, must-revalidate Etag: "643eb1aad6ba3932ca744b96ffc00048" Via: 1.1 google CF-Cache-Status: HIT Age: 2217 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=DYccF50g8L0CKcnHrkialxanogTw45Pf V32WF5Z1W%2FzWVtv%2BHj%2FV20KVg81KpXxV87qYWCLFS8d6yEOmXhYGhBgBE6ulJtnZO3s14gK%2B UjSvg1MrrsNYFUYYfkHDnw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a5d68170b767028-FRA

Code Manipulations

Statistics

System Behavior

Analysis Process: SEMqjw.exe PID: 6564 Parent PID: 4808

General

Start time:	17:21:35
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\SEMqjw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SEMqjw.exe'
Imagebase:	0x400000
File size:	655048 bytes
MD5 hash:	1EECED28416A157BB6C1915C75F01BD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities   Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal