ID: 1637
Sample Name: Statement of Account.exe
Cookbook: default.jbs
Time: 12:33:16
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

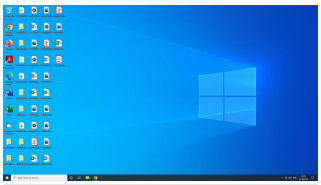
Windows Analysis Report Statement of Account.exe

Overview

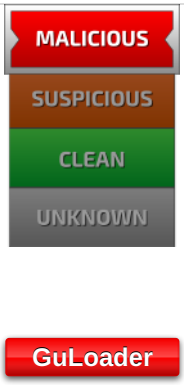
General Information

Sample Name:	Statement of Account.exe
Analysis ID:	1637
MD5:	0fb63e5eb6af1af…
SHA1:	5e7e1db40c9104..
SHA256:	0b65815d462586..
Infos:	

Most interesting Screenshot:



Detection



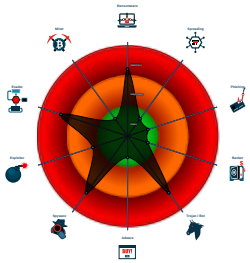
GuLoader

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

Signatures

- Potential malicious icon found
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- May check the online IP address of …
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64native**
- Statement of Account.exe (PID: 9068 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 0FB63E5EB6AF1AFF086E3C2A2321F716)
  - RegAsm.exe (PID: 3604 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)
  - RegAsm.exe (PID: 7740 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)
    - conhost.exe (PID: 1572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- UserOOBEBroker.exe (PID: 1456 cmdline: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 7740	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

May check the online IP address of the machine

System Summary:

Potential malicious icon found

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

GuLoader behavior detected

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

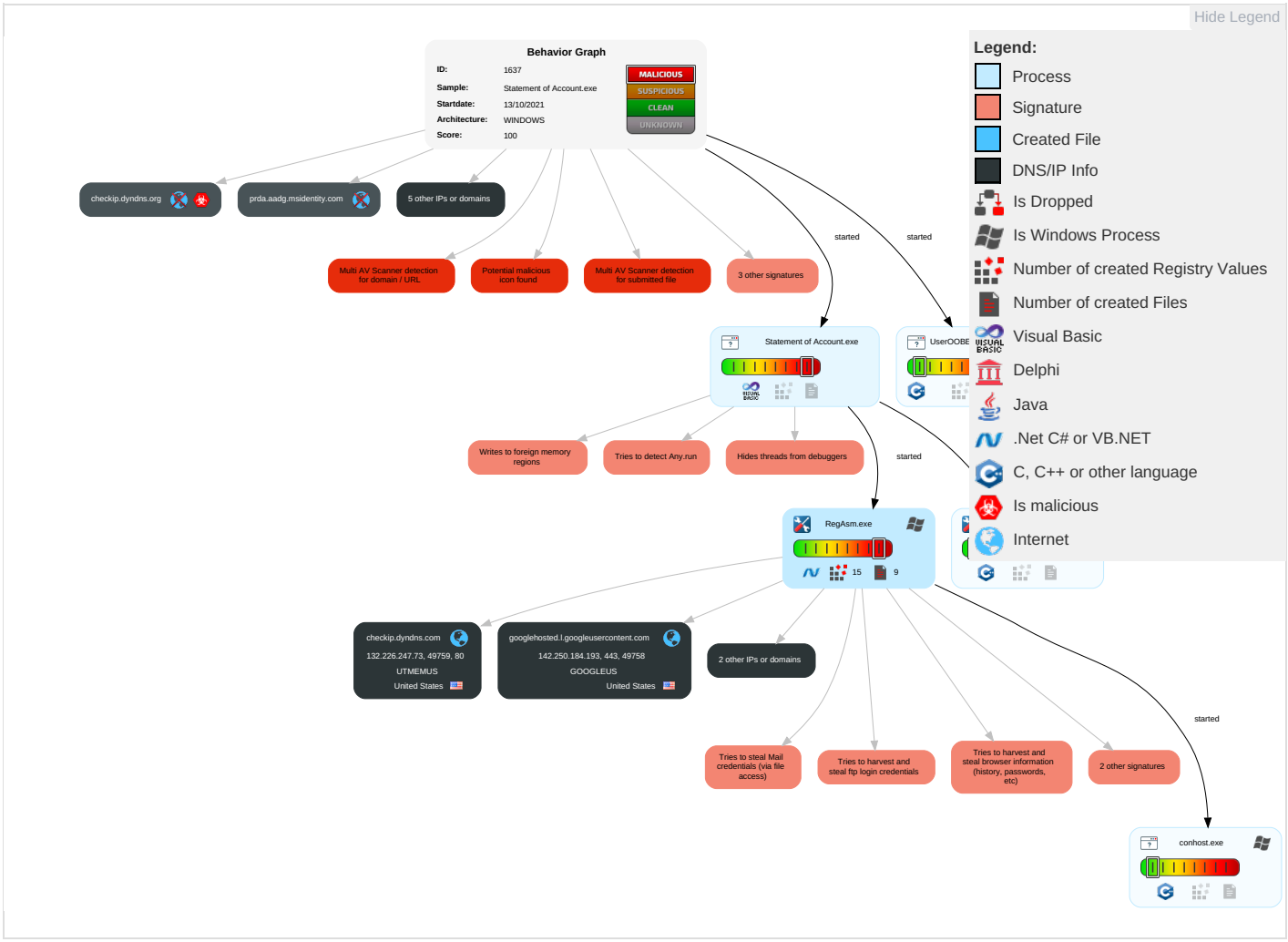
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping 2	Security Software Discovery 3 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 1	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Network Configuration Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Ca Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

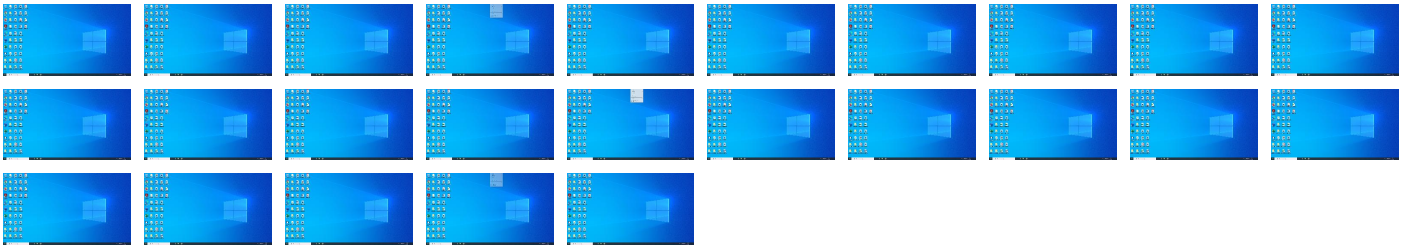
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Statement of Account.exe	21%	Virustotal		Browse
Statement of Account.exe	23%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
windowsupdate.s.llnwi.net	0%	Virustotal		Browse
freegeoip.app	3%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/	6%	Virustotal		Browse
http://https://freegeoip.app/xml/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	1%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/102.129.143.96	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://freegeoip.app	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	178.79.242.128	true	false	• 0%, Virustotal, Browse	unknown
drive.google.com	172.217.168.46	true	false		high
freegeoip.app	104.21.19.200	true	false	• 3%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.184.193	true	false		high
checkip.dyndns.com	132.226.247.73	true	false	• 0%, Virustotal, Browse	unknown
doc-08-4k-docs.googleusercontent.com	unknown	unknown	false		high
checkip.dyndns.org	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/102.129.143.96	true	• Avira URL Cloud: safe	unknown
http://https://doc-08-4k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/3ec96pm2v8cjj8osvev6ltnouevou20i/1634121375000/08714151441044389622/*/1fuTtg-3dZntlAsxF1yPdYhIzZ_wio3sJ?e=download	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.46	drive.google.com	United States		15169	GOOGLEUS	false
104.21.19.200	freegeoip.app	United States		13335	CLOUDFLARENETUS	false
142.250.184.193	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
132.226.247.73	checkip.dyndns.com	United States		16989	UTMEMUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1637
Start date:	13.10.2021
Start time:	12:33:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Statement of Account.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	34

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@7/0@4/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.19.200	Exodus.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	c9414f9e7ec6f3ba759335ac414092b357b131bda6c54.exe	Get hash	malicious	Browse	• freegeoip .app/json
	9cbaafcc5fabe81105cbe09a869c1576dcb8c09c53386.exe	Get hash	malicious	Browse	• freegeoip .app/json
	c9952fbf329b8a9b3400196c5bfefb8c48bdb7a8a3c8f.exe	Get hash	malicious	Browse	• freegeoip .app/json
	3eb7ffbfa401fcfac54abc23f156c158739984ef654d8.exe	Get hash	malicious	Browse	• freegeoip .app/json
	4d913859382da5788bbf0eff507ebccb7bd850509e6e8.exe	Get hash	malicious	Browse	• freegeoip .app/json
	b185909f484fb9247ee23e1ca9bc8a9914db5a8b41caa.exe	Get hash	malicious	Browse	• freegeoip .app/json
	b185909f484fb9247ee23e1ca9bc8a9914db5a8b41caa.exe	Get hash	malicious	Browse	• freegeoip .app/json
	dd5f86db6c95b6c128a9e805868f9bfde5d52105b93f5.exe	Get hash	malicious	Browse	• freegeoip .app/json
	dc5c22ee0782235867ae0363443252f867d0bae4056cd.exe	Get hash	malicious	Browse	• freegeoip .app/json
	6e4f659019bf327df05eb4aa7db3a381f01f8e35157cb.exe	Get hash	malicious	Browse	• freegeoip .app/json
	c5577bb5b44d4876cc6e6a0260dd0f0956bd70b945793.exe	Get hash	malicious	Browse	• freegeoip .app/json
	ASM9WQK4L9.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	LLjDnAaBT8.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	JThZQQQwZA.exe	Get hash	malicious	Browse	• freegeoip .app/xml/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Loader.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
132.226.247.73	signed copy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	sKlqSynAox.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	RFQ010-SSH012021.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	q5oqrkn1Eu.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Statement of Account of Sep 2021.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	rUrO6qPzwT.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SCAN_20161017_151638921_002.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	429n7f9Oyf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	L75ca55zsv.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	dHzzhVBJvg.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	25678023400.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	GT09876545678.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	267890987654235678909876 54.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	xqB7Jghpih.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Products Details and Order reference.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	256789876542TRT.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order APO-074787648.xlsx	Get hash	malicious	Browse	• checkip.dyndns.org/
	68765578980878 - Purchase Order_PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Quotation Requested No. ATOMYU14.21.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order 4102021.pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 178.79.242.0
	heX1kOkwqy.exe	Get hash	malicious	Browse	• 178.79.242.0
	mixsix_20211013-084409.exe	Get hash	malicious	Browse	• 178.79.242.0
	2rd Quater Order Quotation.zip.xls	Get hash	malicious	Browse	• 178.79.242.128
	DOC REC EIPT.html	Get hash	malicious	Browse	• 178.79.242.128
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 178.79.242.128
	emil.franchi@global.com #Ud83d#Udce0 VGX47BBSBJ44838.HTM	Get hash	malicious	Browse	• 178.79.242.128
	DHL Lieferschein,pdf.exe	Get hash	malicious	Browse	• 178.79.242.128
	Payment_MT103.exe	Get hash	malicious	Browse	• 178.79.242.0
	Doc-CS3.exe	Get hash	malicious	Browse	• 178.79.242.128
	SecuriteInfo.com.Suspicious.Win32.Save.a.28039.exe	Get hash	malicious	Browse	• 178.79.242.0
	oG3zl54AA5.exe	Get hash	malicious	Browse	• 178.79.242.128
	dNIT8STqLN.exe	Get hash	malicious	Browse	• 178.79.242.128
	Revised Quotation F657.exe	Get hash	malicious	Browse	• 178.79.242.0
	Quotation Request.pdf.exe	Get hash	malicious	Browse	• 178.79.242.0
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 178.79.242.128
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 178.79.242.0
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• 178.79.242.128
	COPIA DE PAGO.exe	Get hash	malicious	Browse	• 178.79.242.0
freegeoip.app	v9RV3IPlV0.exe	Get hash	malicious	Browse	• 104.21.19.200
	BTL_01145120_160850IMG.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_0211678531077.exe	Get hash	malicious	Browse	• 172.67.188.154
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	company-profile.doc	Get hash	malicious	Browse	• 104.21.19.200
	MV VTC GLORY.doc	Get hash	malicious	Browse	• 172.67.188.154
	PO # 7800017872.doc	Get hash	malicious	Browse	• 104.21.19.200
	BTL_01145120_160850IMG.doc	Get hash	malicious	Browse	• 104.21.19.200
	RQL_0506111780.exe	Get hash	malicious	Browse	• 172.67.188.154
	L8SM7IA2Pq.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Artemis7FC3D3787CC9.2543.exe	Get hash	malicious	Browse	• 172.67.188.154
	Orden-CVE6535 _TVOP-MIO, pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	ABONOF2201.exe	Get hash	malicious	Browse	• 172.67.188.154
	NEW P.O3421280.exe	Get hash	malicious	Browse	• 172.67.188.154
	COMPROBANTE DE RETIRO SPEI No, 79433161.exe	Get hash	malicious	Browse	• 104.21.19.200
	signed copy.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO09858.exe	Get hash	malicious	Browse	• 172.67.188.154
	NS. ORDINE N. 141.exe	Get hash	malicious	Browse	• 104.21.19.200
	Re RFQ-ROExp0081021.doc	Get hash	malicious	Browse	• 172.67.188.154
	IMPORTS INVOICE.exe	Get hash	malicious	Browse	• 172.67.188.154

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	xHSUX1VjKN.exe	Get hash	malicious	Browse	• 23.227.38.74
	v9RV3IPIV0.exe	Get hash	malicious	Browse	• 104.21.19.200
	dtMT5xGa54.exe	Get hash	malicious	Browse	• 172.67.173.247
	BTL_01145120_160850IMG.exe	Get hash	malicious	Browse	• 172.67.188.154
	IMG_0211678531077.exe	Get hash	malicious	Browse	• 172.67.188.154
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 172.67.188.154
	emil.franchi@global.com #Ud83d#Udce0 VGX47BBSBJ44838.HTM	Get hash	malicious	Browse	• 104.16.19.94
	New Order For Chile.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	MV VTC GLORY.doc	Get hash	malicious	Browse	• 172.67.188.154
	PO # 7800017872.doc	Get hash	malicious	Browse	• 104.21.19.200
	Preliminary Closing Statement and Fully Executed PSA for #U20ac 520k Released.html	Get hash	malicious	Browse	• 104.16.18.94
	KDiuvfHzkH.apk	Get hash	malicious	Browse	• 104.16.86.20
	BTL_01145120_160850IMG.doc	Get hash	malicious	Browse	• 104.21.19.200
	Potvrda narudzbe u prilogu.exe	Get hash	malicious	Browse	• 162.159.130.233
	Revised_Purchase_Order.htm	Get hash	malicious	Browse	• 172.67.219.206
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	RQL_0506111780.exe	Get hash	malicious	Browse	• 172.67.188.154
	L8SM7IA2Pq.exe	Get hash	malicious	Browse	• 172.67.188.154
	l4puxn8v7H.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Linux.DownLoader.16.15940.30355	Get hash	malicious	Browse	• 104.21.36.108
UTMEMUS	BTL_01145120_160850IMG.doc	Get hash	malicious	Browse	• 132.226.8.169
	signed copy.exe	Get hash	malicious	Browse	• 132.226.247.73
	sKlqSynAox.exe	Get hash	malicious	Browse	• 132.226.247.73
	New Order Inquiry No.96883,pdf.exe	Get hash	malicious	Browse	• 132.226.8.169
	Orden-CVE6535 _TVOP-MIO, pdf.exe	Get hash	malicious	Browse	• 132.226.8.169
	RFQ010-SSH012021.exe	Get hash	malicious	Browse	• 132.226.247.73
	q5oqrkn1Eu.exe	Get hash	malicious	Browse	• 132.226.247.73
	Statement of Account of Sep 2021.exe	Get hash	malicious	Browse	• 132.226.247.73
	Hesap hareketleriniz.exe	Get hash	malicious	Browse	• 132.226.8.169
	rUrO6qPzwT.exe	Get hash	malicious	Browse	• 132.226.247.73
	W0TQR8HOH9.exe	Get hash	malicious	Browse	• 132.226.8.169
	SCAN_20161017_151638921_002.doc	Get hash	malicious	Browse	• 132.226.247.73
	429n7f9Oyf.exe	Get hash	malicious	Browse	• 132.226.247.73
	L75ca55zsv.exe	Get hash	malicious	Browse	• 132.226.247.73
	dHzzhVBJvg.exe	Get hash	malicious	Browse	• 132.226.247.73
	2ddsccx6Bp.exe	Get hash	malicious	Browse	• 132.226.8.169
	Wire Transfer Slip.exe	Get hash	malicious	Browse	• 132.226.8.169
	34567892.exe	Get hash	malicious	Browse	• 132.226.8.169
	25678023400.exe	Get hash	malicious	Browse	• 132.226.247.73
	w3ckECsT7j.exe	Get hash	malicious	Browse	• 132.226.8.169

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	v9RV3IPIV0.exe	Get hash	malicious	Browse	• 104.21.19.200
	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 104.21.19.200
	BTL_01145120_160850IMG.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_0211678531077.exe	Get hash	malicious	Browse	• 104.21.19.200
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 104.21.19.200
	MV VTC GLORY.doc	Get hash	malicious	Browse	• 104.21.19.200
	PO # 7800017872.doc	Get hash	malicious	Browse	• 104.21.19.200
	BTL_01145120_160850IMG.doc	Get hash	malicious	Browse	• 104.21.19.200
	RQL_0506111780.exe	Get hash	malicious	Browse	• 104.21.19.200
	L8SM7IA2Pq.exe	Get hash	malicious	Browse	• 104.21.19.200
	l4puxn8v7H.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Artemis7FC3D3787CC9.2543.exe	Get hash	malicious	Browse	• 104.21.19.200
	Black King fast Setup.exe	Get hash	malicious	Browse	• 104.21.19.200
	Orden-CVE6535 _TVOP-MIO, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	ABONOF2201.exe	Get hash	malicious	Browse	• 104.21.19.200
	NEW P.O3421280.exe	Get hash	malicious	Browse	• 104.21.19.200
	ajjVYRO.vbs	Get hash	malicious	Browse	• 104.21.19.200
	COMPROBANTE DE RETIRO SPEI No, 79433161.exe	Get hash	malicious	Browse	• 104.21.19.200
	signed copy.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO09858.exe	Get hash	malicious	Browse	• 104.21.19.200
37f463bf4616ecd445d4a1937da06e19	ZAM#U00d3WIENIE.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	Potvrda narudzbe u prilogu.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	art-1881052385.xls	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	184285013-044310-sanlccjavap0003-7069_pdf (5).exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	DOC 10132021.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	WIRE ADVICE.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	WireCopy.html	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	UGS2021100716241.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	RFQ_Project 20211012 thyssenkrupp Industrial Solutions AG 6000358077_PDF.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	WireCopy.html	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	Rust_hack_v6.4.2_x64_stable.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	0810202 import Inquiry ref- November order 2021.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	Document-10122021 81258 PM.html	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	ajjVYRO.vbs	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	IMG-pic 0699821.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	HJmXSL9b6P.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	WAYBILL.EXE	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xzH2c9tl13.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	doc-379851424.xls	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193
	xzH2c9tl13.exe	Get hash	malicious	Browse	• 172.217.168.46 • 142.250.184.193

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.361190831487217
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	Statement of Account.exe
File size:	135168
MD5:	0fb63e5eb6af1aff086e3c2a2321f716
SHA1:	5e7e1db40c9104297c3b05b26c97a788eb92401b
SHA256:	0b65815d462586870177898072a1500ec014a390eb466e a0dd716567ada4109a
SHA512:	4dfd892dec9c4182005f668b201063085c6868085c2f556 791c5654516ce9a4be9c7a7c887e0da182f7cfb29c5690c f45638fb6749bf49e7ba74929d82c35a82
SSDEEP:	1536:5sYs89TfPXmlAo30SC66Biy2bbMSekC7dY5Kwc hyuGWawkANvv0LLhQ4sZiDNmMN:5JXS0SC6aiyCYU Kw7T3hBd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....u.W.....`.....h.....@.....B..

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x578A7516 [Sat Jul 16 17:55:34 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c727a98e677fb7bd25bb06d2a2d956f1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19ef0	0x1a000	False	0.567673903245	data	6.83550763896	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x4562	0x5000	False	0.396142578125	data	4.61030929614	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:36:35.853833914 CEST	192.168.11.20	1.1.1.1	0x1c19	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:36.757107973 CEST	192.168.11.20	1.1.1.1	0x86e	Standard query (0)	doc-08-4k-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.728669882 CEST	192.168.11.20	1.1.1.1	0x655b	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:36:40.465620041 CEST	192.168.11.20	1.1.1.1	0xf65a	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 12:35:50.271889925 CEST	1.1.1.1	192.168.11.20	0xc31a	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 13, 2021 12:35:50.271889925 CEST	1.1.1.1	192.168.11.20	0xc31a	No error (0)	windowsupdate.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:35.878083944 CEST	1.1.1.1	192.168.11.20	0x1c19	No error (0)	drive.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:36.811844110 CEST	1.1.1.1	192.168.11.20	0x86e	No error (0)	doc-08-4k-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 12:36:36.811844110 CEST	1.1.1.1	192.168.11.20	0x86e	No error (0)	googlehosted.l.googleusercontent.com		142.250.184.193	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:38.737804890 CEST	1.1.1.1	192.168.11.20	0x655b	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:40.475270987 CEST	1.1.1.1	192.168.11.20	0xf65a	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Oct 13, 2021 12:36:40.475270987 CEST	1.1.1.1	192.168.11.20	0xf65a	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Oct 13, 2021 12:40:23.662216902 CEST	1.1.1.1	192.168.11.20	0xcd19	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-08-4k-docs.googleusercontent.com
- freegeoip.app
- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49757	172.217.168.46	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49758	142.250.184.193	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49760	104.21.19.200	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49759	132.226.247.73	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 12:36:39.021188021 CEST	5740	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Oct 13, 2021 12:36:39.258580923 CEST	5740	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 10:36:39 GMT Content-Type: text/html Content-Length: 106 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 30 32 2e 31 32 39 2e 31 34 33 2e 39 36 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 102.129.143.96</body></html>
Oct 13, 2021 12:36:39.343060017 CEST	5741	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Oct 13, 2021 12:36:39.580378056 CEST	5741	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 10:36:39 GMT Content-Type: text/html Content-Length: 106 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 30 32 2e 31 32 39 2e 31 34 33 2e 39 36 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 102.129.143.96</body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49757	172.217.168.46	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:36 UTC	0	OUT	GET /uc?export=download&id=1fuTtg-3dZntlAsxF1yPdYhIzZ_wio3sJ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:36 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 13 Oct 2021 10:36:36 GMT Location: https://doc-08-4k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/3ec96pm2v8cjj8osvev6ltnouevou20i/1634121375000/08714151441044389622/*/1fuTtg-3dZntlAsxF1yPdYhIzZ_wio3sJ?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-R6Vf9Z1fyRDXu2Hc4+2o4g' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=En1B0TEcCSHUXKf6a0RJ7Voo2gqcqt6DiRP8_jFmYKBuqARp0EGEl3S7FQQmMzYE3YDtJIRO0usrgaHqlaly1hnh3a-g2xq3FD463nYitrk1H7iS2xYH1HqYVNwepQOiMKY85T0I4hKydQKe8cRQVYLNRaTad-woJtmtPfZ2CsQ; expires=Thu, 14-Apr-2022 10:36:36 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-10-13 10:36:36 UTC	1	IN	Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 38 2d 34 6b 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 33 65 63 39 Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-08-4k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/3ec9
2021-10-13 10:36:36 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49758	142.250.184.193	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:36 UTC	1	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/3ec96pm2v8cjj8osvev6ltnouevou20i/1634121375000/08714151441044389622/*/1fuTtg-3dZntlAsxF1yPdYhIzZ_wio3sJ?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-08-4k-docs.googleusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdtybi6Oe1Av3p4uccnbHsaNuDjw-OVTS2oe8EnP62HDwhe2JzxioZXOiTBT1-Kc5Qek0vQTB-J7WzZtQJeDm7w Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="BEN_QnfobHfVxI41.bin";filename*=UTF-8''BEN_QnfobHfVxI41.bin Content-Length: 123968 Date: Wed, 13 Oct 2021 10:36:37 GMT Expires: Wed, 13 Oct 2021 10:36:37 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=LfY16w== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-13 10:36:37 UTC	5	IN	Data Raw: a5 f5 7d f9 c2 ac cd 36 40 26 a0 d8 02 82 17 c4 20 50 5b 29 23 90 16 3f fa ce 5d a4 5e 1a 49 da 9b 5d 11 a0 86 64 42 e6 27 d4 86 fe e3 18 8a ff e3 e8 30 de 3c be e5 1a 2a 46 23 70 58 af b5 81 24 0a ff 3f bf 38 05 9f 93 6b 58 ca 4b b0 b6 5a e1 17 4d bd 85 58 cb 98 53 c8 5c da 1f 73 76 31 19 44 11 40 13 ff b0 77 39 d1 34 30 cd 98 75 c2 67 8f 79 e4 b4 6a 77 ff 7d b8 75 2b 58 0e 1f 29 4a 14 79 97 4c 06 70 84 87 c2 17 3f 83 12 70 e1 f0 4a 8c b9 35 51 76 3d 79 c9 6a 40 67 5a aa a6 15 99 6d 90 e6 f5 f5 59 d3 cd f9 0b f6 20 be 1e c5 d5 74 61 a9 45 7d 3c a2 2d ea 48 a0 c0 04 08 df c1 91 10 3d 54 6f d8 b9 06 16 e3 94 ba 50 76 35 ac 42 48 c7 46 4a f1 3e 81 ed f2 cb f0 f9 80 7a 08 be 77 7d 0d a9 87 e3 1e 01 32 69 a3 d2 86 a0 32 8e 4f 0a b8 f4 c4 41 be 7d 24 0a 06 ce Data Ascii: }6@& P[}#?]^I]dB'0<*F#pX$?8kXKZMXS\sv1D@w940ugyjw}u+X)JyLp?pJ5Qv=yj@gZmY taE}<-H=ToPv5BH FJ>zw}2i2OA}$
2021-10-13 10:36:37 UTC	9	IN	Data Raw: f2 4a 91 74 e5 a1 20 c2 7a 07 74 4c a9 8f 18 ed 2c 09 5d 1d 1a 05 c4 de 24 c9 01 8e 73 ea f7 c7 06 cd 03 a0 94 32 0f c8 bc dc a1 49 73 4e 10 ed d5 a5 2a d5 f9 b4 4c 8c 63 06 ca 53 5e 4d 59 44 10 0e b0 39 ff d6 c4 8f c0 a3 82 25 61 27 be aa 3b c5 2b 2d 44 a5 ed 65 7a 89 5e 71 76 20 dc 72 32 7a 00 92 b2 52 7e d4 55 ec 01 d1 c3 2e 51 49 f2 f5 14 c7 d0 dc 5e 7a a1 82 f4 1d 3b e8 24 33 59 d5 ba d6 18 33 24 db e7 50 90 4b aa 9d 6f d5 c2 a3 76 0d a7 19 cc 42 d4 1e ba e4 70 15 74 5c a1 0a f3 c1 66 f9 cc 03 c3 bc 7e b7 1d 58 e4 02 2f 45 b1 dc e8 88 b7 8f c1 06 cd 02 e2 f3 2c b3 4a b0 92 b1 69 dd 41 14 e3 3c 87 5c c3 b5 72 a5 b7 3c c0 97 1c 8e fc bc dd 27 9f 6c d2 d2 ff 9f 15 ff 14 9d 5e 64 dd 60 18 e0 38 a0 35 d0 12 d8 a3 e9 94 9b 0f 87 2e 08 f7 02 58 04 12 f0 9d Data Ascii: Jt ztL,]$s2IsN*LcS^MYD9%a';+-Dez^qv r2zR~U.Q!^z;$3Y3$PKovBpt\f~X/E,JiA<\r<'l^d`85.X
2021-10-13 10:36:37 UTC	13	IN	Data Raw: 6c b1 61 94 90 c8 a3 99 1e 36 66 17 ee 11 38 a9 df 6c 05 93 20 a0 04 8b a3 51 33 1a 17 57 ee f6 ec ba 2d 32 81 ae 0c 6a 91 ba 03 42 5f a1 e1 66 f5 ff 67 d1 72 6a db 28 56 b4 2f ec be 03 61 c2 5a a6 8d 64 42 6b 14 33 b9 2e 14 58 00 f0 c6 08 09 6e 06 c0 c5 91 99 5d b5 28 ae 95 00 0f 82 ef 7f b6 48 45 92 f0 e4 64 2d ab 59 70 4e 69 44 0b a6 3e 57 ce 2a ff 4d 02 7f bd 08 4b 13 70 25 1c 07 6b ee 17 50 aa 0e 01 5e f6 1e b7 d9 12 40 0c 94 4c 6c d4 4c 8a 7a 25 4a e7 d8 68 c7 6d 3f d1 79 84 c7 7b 33 e1 20 a3 d9 de 08 10 42 87 c7 80 40 88 84 ee be 17 7a a3 fa 95 14 69 82 df 83 15 0c 96 fd c6 4f 54 dd 2c ef a0 5b bb 9b 16 7d 37 66 26 70 8c 46 da ca f4 82 28 c9 08 ba 2c 20 9f ce ce 30 d0 10 de f2 fe 64 98 13 6e 09 9a e5 d9 63 5c ba 04 0f eb 3a f6 72 4f 0c 14 4f cb 7b Data Ascii: la6f8l Q3W-2jB_fgrj(V/aZdBk3.Xn](HEd-YpNiD>W*MKp%kP^@LlLz%Jhm?y{3 B@ziOT,[}7f&pF(, 0dnc\:rOO{
2021-10-13 10:36:37 UTC	16	IN	Data Raw: ee b6 05 72 c5 34 40 e5 33 75 c2 6d fd 18 f0 b4 1a 5f 90 7d b8 7f 44 65 0e 1f 23 44 23 92 99 4c b4 6a 4e b7 7d 65 cc 4e 33 2e 9a 91 28 aa a6 87 3e 11 45 09 ac 38 40 11 34 b4 b7 6c b9 0f f1 ee c1 80 37 f9 d6 32 3f b2 1f 9e ff a8 ba 1a 6b 45 48 70 3c 86 3c ec 3a 15 d6 04 78 a7 2f 91 10 7b 27 33 cd 35 df 85 ec 94 ba 5a 19 8b ac 42 42 27 38 4b f1 35 84 ce 31 cb 2a f2 93 73 7e a1 77 7d 09 db b6 dc e6 70 24 41 e3 d2 86 aa 24 72 4e 19 b2 a5 ce 6d 92 6c 2d 1d 6b 0a 87 42 1d 16 59 27 af ae b2 a1 bd 0a 46 4f 0d 3a 85 44 68 cc 04 74 77 5c 61 39 6f e7 22 0d 09 34 da 92 4d c9 b9 42 96 d8 1b 30 02 40 a6 8d 47 ba 70 58 53 40 e9 fa c0 f0 e8 94 0b a1 19 d1 13 1b 8f a3 1f 8c 3a 22 30 68 b9 9f d0 95 1e d2 70 95 e0 ca 20 94 1e 46 0d 6a fe 34 1a ef 5c 7e 0f f0 59 a3 2d db d3 Data Ascii: r4@3um_}De#D#LjN}eN3.(>E8@4l72?kEHp<<:x/{'35ZBB'8K51*s~w}pArNml-kBY'FO:Dhtw\a9o"4MB0@G pXS@:"0hp Fj4\~Y-
2021-10-13 10:36:37 UTC	18	IN	Data Raw: db 0d aa ae 24 14 dd e0 f9 2e 4e 7a af e9 eb ef df 41 6e 2e a7 98 50 bb b6 59 fa c7 9e e3 9b 16 d4 8d bf dd 51 2e 41 dc db fe 3d 16 ff 6e 2c 72 6a da 61 88 e3 38 da 84 ff 1c ce be 16 97 9b 75 34 02 65 29 68 0f 77 6c 8d 3f 42 8a 62 19 5f b8 35 8a 85 d5 ee ba 1d 3c 18 84 33 87 0d 2d 30 2c 1d 50 1e 00 c9 ab 5e eb 56 28 88 a2 35 fc 4d da d9 69 50 6b 17 fa 38 05 95 e5 ce 4c ca c4 3c 77 5a 59 1d 22 7f 85 58 c1 98 6d eb 5c da 1b 00 b5 31 19 4e 02 4b 6d e0 b0 77 3d a3 05 31 cd e8 63 ea 07 8f 79 ee a2 94 76 ec 71 a9 79 07 d4 1f 14 3e 2b cf c3 99 46 b2 79 62 ad 7a 07 78 58 5c e0 89 99 33 ac c9 56 35 6f 6a 18 a4 4e 0b c3 34 c4 c3 0e 7f 0f f5 cc 87 91 3c 8d 85 97 2b b6 11 cf 3e a8 be 63 b7 87 48 7a 59 41 2d ea 42 a0 d1 0f 19 89 eb 59 10 71 5f 6c c9 33 c0 64 83 94 b0 Data Ascii: $.NzAn.PYQ.A=n,rja8u4e)hwl?Bb_5<3-0,P^V(5MiPk8L<wZY"Xm\1NKmw=1cyvqy>+FybzxX\3V5ojN4<+>cH zYA-BYq_l3d

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	19	IN	Data Raw: b4 10 16 fb dc 1e b7 d2 e9 56 1b 22 69 7e c2 5b a2 df 25 4b ed f7 73 c1 74 ea fc 7b ae d6 5a 34 f7 8a 8b e2 de 11 1a 4e 91 b5 8b 7b b8 f4 81 1e 78 8e a9 f7 ed 17 40 b2 af 90 17 25 cf 7c 5f 4b 31 3d 2b c4 b2 4a 62 fb 9b 55 03 6c 52 03 86 46 f3 89 fc 93 2a 78 a1 ba 06 2b 9c ca ce 21 d7 7e 74 ec e1 6e 84 5e 7f 00 b6 2d 37 77 4d a8 73 1b eb 3d f7 5e 53 1d 3b 56 df 7b 31 10 d2 50 ea f7 c0 2e d1 6a a0 9e ea c9 c0 e4 dc ab cf 5b 04 7e ed df d9 2d d1 90 9c 1c 8a 63 24 ba 79 5e 4b 59 6d 3d 0e b0 3e ff ff b5 38 0c a5 8e b5 13 27 be bf 0b e9 58 2d 4c a3 ed 5b 0e 89 4f 77 56 ca a9 72 32 f1 3f ba d8 53 5b c4 27 8f 75 d1 b3 8a 74 76 f8 a8 16 c1 a0 56 02 62 d3 e3 f6 35 31 4a 01 2c 2b 8a c3 d6 68 97 01 e9 e9 d5 92 4d da 17 fb ce b0 36 74 25 63 bb e9 58 a6 97 64 e4 00 b1 Data Ascii: V"i~[%Kst{Z4N{x@%|_K1=+JbUlRF*x+!~tn^-7wMs=^S;V{1P.j[~-c$y^KYm=>8'X-L[OwVr2?S['utvVb51J, +hM6t%cXd
2021-10-13 10:36:37 UTC	20	IN	Data Raw: f5 68 8e b4 2f 08 9e 80 8e 33 5f 1c 54 5a 35 af ad 92 90 a5 7e 58 0b 87 42 59 23 59 18 a8 70 8c bd f2 cb 28 f8 80 7a 02 be 77 7d 0f a9 87 dd e4 00 32 69 81 d2 86 a0 30 8c 4f 0a ba b4 c4 41 9c 7d 24 0a 06 ce 87 42 15 16 59 0c a6 ae a3 a8 a9 65 82 4f 26 0e 85 36 30 dc 7a 21 78 5d 9b 07 b9 e7 22 06 09 0d da 92 4d bb e5 52 e8 89 33 5f 06 3e 8e 87 9a 36 03 eb 53 40 91 c4 1e f0 98 94 d5 cf 10 b2 40 6d 47 d3 15 58 4c 33 44 64 69 9f a0 95 c0 cd 73 93 f3 bf b1 9d 32 56 0b b7 56 39 a3 db 5c 78 6a e3 53 a3 0f 81 0d 6b 90 18 14 e5 b4 c6 fe ba 5b 4a 5c e6 29 32 ca 19 03 48 46 c8 6d 61 e6 f2 65 d0 4f 70 d2 2b 57 b3 05 e6 ad 0b 72 da 72 a4 8c 64 75 04 18 7b b9 34 5a 70 50 f1 dd 32 dd 73 b3 c3 ed 90 ba 5d bf 2a a6 f4 ac 27 80 e4 74 ce ec 3b 92 80 c6 27 05 fb 5f 58 11 b7 Data Ascii: h/3_TZ5~XBY#Yp(zw}2i0OA}$BYeO&60z!x]"MR3_>6S@@mGXL3Ddis2VV9\xjSk[J\)2HFmaeOp+W rrdu{4ZpP2s]*'t;'_X
2021-10-13 10:36:37 UTC	22	IN	Data Raw: 95 5d c9 37 42 c0 b4 3e 70 83 be a9 ed 4f a1 ae bf 6a 69 a3 47 53 db a9 d9 65 16 5b ef 0e b8 68 75 a1 93 f9 d2 17 37 3d 71 d3 f9 f5 39 bd ac 35 a5 dd 90 e2 55 9d f2 af 99 c2 a8 44 41 64 4b 6a 95 51 b1 bc 0b a5 d6 96 f2 52 06 2a 60 e5 dd 57 3c 5a c8 d4 83 86 18 fb ea 56 69 7f c3 15 26 e4 b6 b9 86 f0 1c cd 5f bf 85 93 69 0d af 17 e6 76 1c 0e 03 89 41 06 8e 4a 5b a1 b9 2c f3 31 ca fd c4 7f f3 34 8f 4b 5f d5 2d 40 55 10 40 18 65 73 ab 4f e8 51 dc f9 52 21 ed 31 b7 db 78 5f 43 28 ce 27 1e 9f e7 7a 51 46 29 4f b6 5b 71 8c 4d bd 8f 2b c6 99 13 c2 26 da c1 63 76 23 1f ba 07 54 13 ff b2 18 38 d1 34 3a cd 44 7d ea c5 8f 79 e2 92 63 5f f3 7c b8 7f 2b df 18 37 b7 44 0b c5 bf 5d b7 73 62 a6 7c 3c 73 4e 32 34 89 99 3b ac fb 47 f5 ec 4f 08 a4 4a 23 06 27 f4 cc 61 8e 0f Data Ascii:]7B>pOjiGSe[hu7=q95UDAdKjQR*`W<ZVi&_ivAJ[,14K_-@U@esOQR!1x_C('zQF)O[qM+&cv#T84:D}yc_|+7D]sb|<sN24;GOJ#'a
2021-10-13 10:36:37 UTC	23	IN	Data Raw: a4 44 81 18 fc a0 74 c4 89 25 e3 a0 cc 5d 42 bc 5e 58 11 cb 61 19 d4 7c 43 bc 21 9e 25 53 68 40 64 5c 12 71 0a a8 2a d0 b5 41 55 be 10 64 c8 ae 1e c7 b7 20 57 1b 02 cb 6c d5 4a a5 cc 2d 5c fe f7 41 60 79 ae fc 6a a7 dc 63 ac e4 b0 9a e8 ca f6 19 5d 8b a4 80 6a 0c f6 81 18 06 70 c6 ef e6 17 62 91 a3 86 02 08 c1 3b c4 4f 5e df 27 d5 b5 d0 af fa be 6c 3d 7d 5c 66 9b 47 db d3 ef 9c 53 bf a0 ba 26 39 9c db c1 53 19 5d 74 82 91 74 8a 1a 75 14 49 3d 16 7b 3f f3 6e 1b 9b 55 ed 5f 42 17 07 c4 dc 6a 38 62 90 28 ea 87 a9 34 f8 03 aa 8a 12 ca 88 9e d3 d9 4f 44 2c 60 82 c5 de 2d f3 eb 62 1f ec 72 03 b8 db 41 4d 29 2a 1a 0f b0 32 eb 29 c7 58 53 b0 9f 8c 70 1e 69 b8 0b c1 23 3e 59 b3 fe 65 51 b0 5e 64 47 f4 46 61 25 e6 30 83 a5 3c 41 c3 27 ad 17 2f b0 9f 6c 4f 98 84 0e Data Ascii: Dt%]B^Xa|C!%Sh@d\q*AUd WlJ-\A`yjc]jpb;O^'l=}\fGS&9S]ttuI={?nU_Bj8b(4OD,`-brAM)*2)XSpi#>Y eQ^dGFa%0<A'/lO
2021-10-13 10:36:37 UTC	24	IN	Data Raw: 9e 8a 2f bd df 54 29 00 58 34 cb 5b 33 19 3d 12 da 79 a8 02 e3 38 86 93 2e e2 bd 84 31 a3 75 c1 39 b9 aa 08 d2 94 50 70 36 ad 0a fb 5d b3 db 15 01 9e 9c 00 38 70 54 6c d2 26 bb bc 98 86 ae 78 74 34 ac 48 60 61 46 68 fb 26 95 ac ea dc fc eb 98 7a 11 b7 66 65 9c b6 a7 ec ed 11 3b 78 9b 43 99 df cc 88 64 0b ae a7 d8 50 82 50 9a 1d 17 c4 96 5a 04 06 59 34 9d af a3 a8 ab 74 88 63 12 21 8e 36 63 e1 7a 21 18 7b 64 11 a0 ca 2c 16 6d 80 f6 b6 47 b9 c7 6c e9 f9 11 1b 07 29 af 8c 51 ad 1e fa 4e 53 fd 84 19 c9 ed 9f 0b b0 01 d0 0a 7d 91 b0 00 97 37 25 c8 06 63 bf c1 bf 0d 82 62 b6 cc bd b1 88 06 90 1a ab ee 11 40 d8 5d 7e 75 f0 73 88 22 9a f2 2d b3 0b 1e 4c 83 c6 d6 bb 5c 40 88 bc 18 0b dd 0b 17 6a 57 cf 6d 6c dd b3 74 d7 69 7f f0 12 49 a5 d3 ff a1 03 71 db 4b b9 1c Data Ascii: /T)X4[3=y8.1u9Pp6]8pTl&xt4H`aFh&zfe;xCdPPZY4tc!6cz!{d,mGl)QNS}7%cb@]~us"-L\@jWmltiIqK
2021-10-13 10:36:37 UTC	25	IN	Data Raw: a4 bf ad 3f 92 b3 40 5c ca 3c b6 04 c7 bb 02 1d 45 5a 80 3c c6 a0 74 7b 62 c2 e2 e2 0b 63 55 00 2a 21 b1 bc 08 48 b4 29 f5 95 d5 98 58 d4 3f 5b c0 df 03 75 0d dd 93 dd 5f a6 b5 b8 f0 13 b3 79 11 d3 bf fb 1f 16 5b e9 0c b5 73 57 b7 6b d0 c1 1d 27 2b 62 de ea f8 52 aa 83 a8 bf ca e0 f3 5c 11 6f af 42 c3 8e 36 41 44 05 19 98 51 aa 86 76 a5 03 9e e5 88 50 fc ed ae dd 48 31 c4 97 dc 8d 83 1d fd 7d 38 6d 64 de 3a 1d e2 38 da 97 f5 0f 46 b8 c9 98 41 68 ff 1c c1 6b 2a 0f 07 13 8d 3d 5d 81 43 49 5d 36 56 e7 2f 1b c6 e0 6f fd 12 84 26 f8 42 77 30 26 1c 52 1c 66 87 c2 4f e5 c9 4b 20 56 f7 eb eb 29 8e 69 50 6e 2c b9 31 0c 11 fe 74 48 10 a5 4b a0 45 49 3f 67 bc 85 52 cb 91 05 d9 59 cc 16 fd 1f 20 1d ca 78 9a 3b d5 b1 77 33 d1 47 99 cd 98 73 d1 61 a7 f0 e4 b4 60 66 f9 Data Ascii: ?@\<EZ<t{bcU*!H)X?[u_y[sWk'+bR\oB6ADQvPH1}8md:8FAhk*=]CI]6V/o&Bw0&RfOK V)iPn,1tHKEI?gRY x;w3Gsa`f
2021-10-13 10:36:37 UTC	27	IN	Data Raw: 66 f3 e6 7c c6 6b 40 92 05 7e 87 04 ec b4 6c 56 d3 5a ac e2 8c 7f 6b 12 52 0e 3e 50 5e 13 f8 cc 31 17 90 b2 d3 cf 80 b1 4b 4b 38 bd ed b5 04 ae f3 5c 27 83 57 98 91 c9 42 ad ab 5f 52 0a 60 6c b9 aa 39 45 af 2e ec 4d 72 43 10 0b 63 f0 71 00 00 08 d8 cc 76 81 9b 1a 66 bc 80 1f b7 de 58 d6 1b 08 63 57 36 5b a2 d9 36 4f ed ef 7d b3 78 af fc 0b b9 e5 0a 36 f7 b0 9d 1c dd 19 1f 3c 83 b4 8b 23 9e dc e1 18 17 70 bf 09 e4 48 7b 8e be 9c 3d 48 e4 d7 f9 4f 5e cf 0e d2 ca 15 9b f4 ce df 12 7b 5b ab a9 5e a9 a9 da 93 50 04 84 a3 3d 2e 2e ef d4 53 39 61 74 82 5c 4b 90 0b 7a a2 92 22 75 74 52 bd 01 b9 c3 b9 f7 5e 48 0e 1e 44 d4 7b 37 14 eb 3a c2 b1 c6 2e f3 83 ab 9e ec cd e8 8f cd ac de 8d 3f 17 fc d8 ce 2b c7 1f 62 e3 73 63 0c 14 69 7b 65 6d 45 00 04 a3 36 ff ff 94 38 Data Ascii: f|k@~lVZkR>P^1KK8\'WB_R`l9E.MrCcqvfXcW6[6O}x6<#pH{=HO^{[^P=..S9at\Kz"utR^HD{7:.?+bsci{emE68
2021-10-13 10:36:37 UTC	28	IN	Data Raw: 18 ee bb 5b 2f f9 d7 30 cd 92 64 c7 08 0f 79 e4 be 7b 7e d7 c5 b8 75 2d cb 0b 1f 29 44 20 e3 99 64 51 79 49 ac 7d 07 74 3c e7 01 89 e9 56 a0 c8 47 38 7e cf 18 a4 40 0b e2 34 c4 cf 72 bc 0f e4 c2 f5 83 36 f3 d4 81 03 d2 6f ed 34 be 44 13 15 82 3a 73 37 86 5d fc 60 c0 c0 04 02 99 7a 92 4f 62 59 7d d4 19 e2 b0 0e ab ba 50 77 10 ba 30 a7 0e 46 18 53 10 97 b4 50 ee 32 8a f0 5c 00 ce d5 58 14 b8 83 7f c3 1a 40 87 9d d2 f6 02 17 97 5e 0f 1a 91 d8 33 9e 62 24 7a a6 e6 04 42 17 1c 4a 01 da a5 a3 a8 af 74 8f 67 4b 30 85 4e f9 ce 7a 51 73 5c 65 00 ad f0 f4 14 61 e3 dd 83 41 f7 48 b5 17 06 1b 30 d8 2e a1 a5 73 be 03 e1 40 4e e3 bd 57 f0 e8 94 d5 b0 10 ea 54 68 47 a3 1f 86 3a 33 25 07 70 9f 87 9e 1e a0 19 95 e0 ba b0 98 1e 46 4d b4 ee 10 29 eb 58 7e 79 e2 52 a3 47 8b Data Ascii: [/0dy{~u-)D dQyI}t<VG8~@4r6o4D:s7]`zObY}Pw0FSP2\X@^3b$zBJtgK0NzQs\eaAH0.s@NWThG:3%pFM)X~ yRG
2021-10-13 10:36:37 UTC	29	IN	Data Raw: 2b b9 1c fc 0c 00 cb 79 58 22 d9 45 00 04 98 dc ff d7 c2 2b 09 a3 9f 99 13 24 bf b9 7b d7 03 4d 4c a5 e7 65 84 8a 5e 74 24 e1 dd 72 42 e1 17 f2 b2 53 51 d4 d9 a4 5c c2 bf 9d 78 72 cd b5 9b f8 a0 7e 7a 47 c5 97 36 31 4b 3a a3 0f 3c ab 1a f3 70 e3 71 e7 95 a5 30 6e c3 2e 4e 6c 95 2a 06 e3 c9 bb 99 fc 83 a4 a9 e1 a2 92 4d 33 d3 a0 f1 b1 b4 73 6a 1d b1 73 6f ba 13 f1 c1 1d 22 26 6f f6 ae f8 15 a0 5e 07 bf dd e4 f3 5c 00 68 b8 4f d0 87 ce 46 75 47 27 78 ae 4e 49 71 a5 19 8e c0 a0 25 fc ed b5 ce 59 3d 61 9d dc 8d 88 c8 ff 64 15 7b 3a ce 12 37 e3 38 d0 97 e3 0d c8 d1 81 96 9b 7f 48 0a 17 e6 60 0f 07 12 c4 3f 42 8f 51 6f 5b b8 43 f9 20 c1 ac ca 6e ec 18 9b 25 c0 de 2c 30 2c 6f 04 35 6f 79 83 18 e1 47 28 f0 41 2b 8f 33 a5 d4 6f 5b 68 4d 2e 1d 05 ef f8 62 59 ca b2 Data Ascii: +yX"E+${MLe^t$rBSQ\xr~zG61K:<pq0n.Nl*M3sjso"&o^\hOFuG'xNIq%Y=ad{:78H`?BQo[C n%,0,o5oyG(A +3o[hM.bY

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	31	IN	Data Raw: e0 ca b6 b0 7e 46 09 be f8 ef 31 84 4f 72 14 ef 7e ee 18 06 ec 3e 90 1b 32 4b ee 25 d1 ba 2d e2 a7 b8 05 b8 db 01 71 32 73 ce 1d c4 d0 ec 65 d3 c1 49 cb 71 b8 ac 05 9c 1c 26 7b c3 5f 04 a8 78 0d 6b 07 7a c9 9c 78 db 00 f1 d7 2b 0e 10 b8 c0 c5 95 aa 50 9d 7f ae e6 ae 8f 89 e5 74 c0 83 57 83 87 db fb 3e ac 4e 5f 0a 6f 7a e1 54 c6 bc bc 2b 32 5d 57 40 04 0b 4b 19 62 0e 0a 27 99 cb 04 5f 60 1a 16 f9 cd 02 b7 d8 37 56 1b 08 7a 7f d2 5b f5 de 25 4a 87 ff 79 c1 6b ae fc 7b eb cd 6a 37 ec 8a 8f e2 a2 09 1a 4e c2 b5 8b 42 88 eb 9d 30 06 7b a9 fd 95 16 58 82 df b8 57 05 f9 50 cc 4f 58 bd 25 c5 b8 4c b7 f3 cc ef 12 6c 22 66 85 47 db df da 95 08 c3 a1 ba 26 26 84 f3 fd 20 d7 7f 73 9d f4 6f 8b 1c 68 da a4 38 11 67 4a 85 66 1a eb 3a f0 4f 45 6f b3 1f df 0b 58 1c fb 37 Data Ascii: ~F1Or~>2K%-q2seIq&{_xkzx+PtW>N_ozT+2]W@Kb'_`7Vz[%Jyk{j7NB0{XWPOX%Ll"fG&& soh8gJf:OEoX7
2021-10-13 10:36:37 UTC	32	IN	Data Raw: df 58 3c f8 9f 81 ce 1b be 71 3f cc 9a 20 84 86 6e fa ef a8 3d b6 45 59 67 ef 95 06 58 cb 92 00 c5 22 d1 1f 73 72 20 14 6c 57 40 13 f5 30 7c 39 d1 30 30 cd 89 72 d5 b1 9c 7e f5 b3 7b 71 c1 9d 46 8a d4 d8 0e c1 39 61 23 f7 99 4c b8 6a 47 a6 52 46 73 4e 39 fa 89 99 13 ed d5 47 3e 11 4f 18 a4 59 23 06 34 93 c8 61 b9 65 f4 c6 87 90 37 f3 a4 d3 2b b2 6e f6 0e ac ba 6c 05 87 48 32 36 86 3c ea 57 bc e8 15 09 8f 8e e3 99 43 55 1c f0 73 af ad 89 9e ba 56 05 3b ad 42 4e 2c 41 1a 63 10 80 cd 9d c2 2b f8 86 5c 06 96 12 7d 0d a3 8b d5 df 33 33 69 83 d5 e9 aa 33 8c 49 1d 62 a7 c2 57 8d 7a 1c 1d 05 ce 87 45 06 11 2b ac 81 ae d3 c7 a7 64 82 49 00 37 94 43 0b 73 5f 51 07 33 69 10 aa e1 31 03 61 e3 dd e0 93 ec a8 3b 87 f5 1a 30 00 2d 81 9c 42 96 b5 eb 53 46 f0 9d 16 f8 c4 Data Ascii: X<q? n=EYgX"sr lW@0|900r~{qF9a#LjGRFsN9G>OY#4ae7+nlH26<WCUsV;BN,Ac+\}33i3IbWzE+dI7Cs_Q3i 1a;0-BSF
2021-10-13 10:36:37 UTC	33	IN	Data Raw: 0d f4 46 bd 71 1f eb 3a e6 59 55 cb 00 3d ce 7c 26 16 c4 d7 14 08 39 2e f9 dd b0 bb c4 fd e8 8f d6 b8 c7 5b 04 40 ed df d5 f3 f9 ff b6 5d 90 63 0c ca 79 5e 4d 4a 45 00 0e e7 39 ff d7 ae 39 0c a3 9e 9d 61 27 fa b9 0b c0 30 1d 48 a5 91 72 7a 89 0d 71 56 f3 dc 6d 2e df 2e 93 b2 59 29 3d 13 a7 73 f9 f5 8c 74 54 8a a8 10 b4 ae 7f 7b 64 d8 e2 84 8f 6e 4a 71 45 22 a3 b8 d0 4e 97 29 a4 95 d5 98 47 d2 06 79 cf b0 30 73 62 dd ba e9 58 b1 65 ab e2 16 a4 56 79 c4 be f1 c1 11 4a ee 6f 11 5c 7c c7 02 f6 c0 1d 20 3a 65 cf ef 8a a3 8f de 7c d0 d1 e1 f3 5a 02 6b a8 88 c4 f2 0b 64 64 31 76 94 51 b1 b0 62 a0 d6 9b cd 3e 11 fc eb ac d5 46 35 65 8e da a5 b7 17 ff 6e 50 4d 7a d2 18 58 0b 38 d0 9d dd ba c8 d1 d0 84 92 6e 2c 1f e9 e7 63 05 16 18 96 c1 43 9d 41 4e 54 94 29 d0 c3 Data Ascii: Fq:YU=|&9.[@]cy^MJE99a'0HrzqVm..Y)=stT{dnJqE"N)Gy0sbXeVyJo| :e|Zkdd1vQb>F5enPMzX8n,cCANT)
2021-10-13 10:36:37 UTC	34	IN	Data Raw: f7 97 01 40 e2 af 90 1b 13 07 59 d7 4a 2c cd 2a c4 c8 5c 94 94 be 7d 3d 7a ac 0a d3 55 d7 c8 f0 bf 6d bb 2c 85 2c 2a 8d ef d8 53 cd 49 74 82 5c 4b 9c 13 dd 25 af 4c 77 52 4d cd d3 3e f2 2b f3 fc 67 07 61 d4 c1 7b 47 b2 df 2c fb f2 64 0b e5 71 a0 81 ec b9 4a a7 5f ab c9 51 3f 1d 93 d4 df 2d fd ee 91 34 ca 63 0c c0 f9 55 4d 59 41 00 0e a1 3f e8 01 d7 3f 1d a4 9f 9b 5f c7 40 46 f4 c1 2b f3 5c 80 c5 47 7a 89 45 62 58 e2 f4 22 32 f7 35 4c b2 53 71 83 3b a7 03 d1 b3 8c 74 4d 80 a8 16 90 a1 7e 7b 08 d2 e5 f6 0d 4b 4a 01 6e 2b a2 b9 cd 58 95 01 bd 94 d5 92 09 da 3f 5b ce af 2c 5c 1c d6 bb e3 2c 3b 89 b8 94 28 f1 51 41 d9 b5 f1 c7 65 55 e8 1d b7 72 7b c5 ff df c1 6d 49 3e 63 de ee de 13 82 bb 0c bf d7 ec fb 65 22 6e af 99 c4 ef d5 40 64 47 0e 42 43 b7 a0 62 a2 ff Data Ascii: @YJ,*\}=zUm,,*SIt\K%LwRM>+ga{G,dqJ_Q?-4cUMYA??_@F+\GzEbX"25LSq;tM~{KJn+X?[,\,;(QAeUr{mI> ce"n@dGBCb
2021-10-13 10:36:37 UTC	35	IN	Data Raw: bb d2 f6 02 17 9b 46 a8 9d ac b6 31 b8 7d 54 a8 21 d7 96 46 b5 33 43 7e 4a b0 a3 d8 09 40 99 5e 08 92 a0 58 0b c5 65 51 07 fe 4d 92 aa e7 28 14 6b 8c d1 92 47 cd b9 46 c0 bf 1b 30 0c be 8f 8d 47 ba 03 eb 42 47 f4 43 14 f7 f9 99 1a b6 2e 20 eb 8b b8 a3 1f 58 2a 16 1e 33 70 9f da 8c 10 a0 5b c4 e0 ba aa 46 1e 46 23 f5 f2 11 32 db 5c 7e 05 f0 52 a3 05 dc d2 3e 90 70 16 5d 9c 47 fe ba 5d 04 82 af 0d 01 ce 1d 03 3e 54 ce 6d 24 f5 f5 65 d7 7c 70 f9 12 57 b2 0f 9e 7e 3b 60 a2 72 e0 8d 64 75 61 18 7c ca 30 51 58 06 fa da 4a 91 4b b3 b0 aa 98 ba 5d b3 1f a8 ce c1 0f 82 ef 78 cc ba 64 93 80 cc 2a 42 a1 5e 58 1d 7e 9e 12 ac 2f 50 bb 13 fb 4c 72 68 37 1a 4c 61 d1 25 0a 7f a6 c7 05 55 b8 17 11 c2 8b 6c 01 fd 37 26 74 04 68 7f d4 48 a6 d8 34 4d 9f 2a 5c c1 0b c1 f0 7a Data Ascii: F1}T!F3C~J@^XeQM(kGF0GBGC. X*3p[FF#2\~R>p]G]>Tm$e|pW~;`rdua|0QXJK]xd*B^X~/PLrh7La%Ul7&th H4M*\z
2021-10-13 10:36:37 UTC	36	IN	Data Raw: f3 5c 1b 7c a2 e7 c8 80 df 45 75 4c 31 de 50 b1 bc f1 ae c7 9e e1 88 11 ed ea a8 0b 44 3a 58 ca cd 8b bc f6 01 9b c0 7b 7b 0c 02 12 cb 0c d0 97 ff 1e c6 d1 fe c7 9b 7f 2f d5 17 e6 5a 4e 1b 12 80 3f 42 8e 4a 4c 5f b8 3f af 21 c1 ee a0 6f fd 18 94 39 e8 cf 69 30 26 1c 5a 28 6b 09 d7 5f e1 47 60 fa 41 3c fc 22 b8 fc 78 51 6f 35 ce 18 3e 9f e7 43 1e ca b4 45 bc 5a 5f 64 43 bc 85 5e c0 9f 61 5a 79 da 6f 1c 7f 30 19 42 37 46 3b 9a b0 77 33 dd 3c 09 fe 99 75 c2 60 e0 73 e5 b4 6c 60 25 6e be 63 38 df 36 08 28 44 0b c4 88 4b c0 d9 6c a6 0a 79 7f 4f 33 22 84 9e 28 ab bb f1 1b 11 3f 77 a8 4b 23 00 27 c0 ce 70 be 7d 21 e3 87 f0 58 ff a5 97 2d a1 6a fc 3b 80 0c 10 04 81 5b 78 27 8e 01 a9 4e 88 f5 05 08 85 eb a7 11 71 5f 03 30 35 af a7 ab 23 ba 50 70 26 a5 53 41 33 b8 Data Ascii: |EuL1PD:X{{/ZN?BJL_?!o9i0&Z(k_G`A<"xQo5>CEZ_dC^aZyo0B7F;w3<u`sl`%nc86(DKlyO3"(?wK#'p}!X-j; [x'Nq_05#Pp&SA3
2021-10-13 10:36:37 UTC	38	IN	Data Raw: 1f 62 1b 08 63 6c dc 5b 8a 8f 25 4a e7 20 79 c1 51 ef e0 7b af cd 6a 36 f7 a9 8b e2 de 5f 1b 4e 80 df 8a 53 88 e4 81 18 17 3e a9 f7 e6 0c 58 86 af ec 10 05 f9 18 c6 4f 4f ce 34 d8 90 5b bd f4 b4 0f 06 51 52 79 a4 00 db d9 f6 99 20 a0 d2 b4 2d 2a 8a c1 c9 53 45 5a 74 82 91 67 8a 1a 79 26 b1 16 62 74 4d b7 7d 13 d2 09 f6 5e 42 1a 7c 30 de 7b 31 07 20 24 ec e1 d5 29 c1 14 a1 9e ec ce f9 88 ae 0b ec 5b 5c 7f e1 de df 2b f4 f8 8d 1b fe d5 29 ca 09 31 41 58 45 06 1d b4 3f ee d0 b6 ec 29 a3 fe f2 6d 26 be bf 18 c4 3a 28 64 13 ed 73 7c 9a 47 60 5e ce 9f 74 1a c2 3e 92 b8 3c 6d c3 27 ad 6c 39 b3 8c 7e 76 37 a8 16 c1 b3 77 6a 6b c7 1b f7 0e 41 5b 0b 3c d5 a3 ab dd 79 9a 2d d7 bd 36 92 4b d0 2e 4f a1 30 30 74 07 c6 b2 c1 e6 a6 bf be f7 05 b7 51 41 f8 9f f1 e9 f5 5b Data Ascii: bcl[%J yQ{j6_NS>XOO4[QRy -*SEZtgy&btM}^B|0{1 $)[\+)1AXE?)m&:(ds|G`^t><m'l9~v7wjkA[<y-6K.O00tQA[
2021-10-13 10:36:37 UTC	39	IN	Data Raw: 90 0b 41 51 6c a4 34 af ad c1 94 ba 41 76 2a b0 6a 59 26 46 62 83 f4 bf bd 82 e3 6c f8 80 70 0a be 71 0e 03 a8 87 db ed 07 40 4e c3 d2 f6 cf 3b 8d 4f 0c 9e b2 ec 24 9e 7d 2e 06 0c f7 b4 43 17 16 5e 63 ae af a3 ae bc bf 91 49 1b 23 82 7c 6e c4 7a 51 70 4d 62 63 0a c2 22 77 09 fe db 92 41 c4 af 5a ef 8b ad 15 06 4e eb 81 46 be 05 f8 57 47 f2 92 75 24 cd 9e 7b df 1c c1 15 72 54 a6 0e 83 12 85 36 07 76 8c d8 8e 16 8c 30 92 c8 8f a1 98 14 29 3f b5 ee 1b 5d 33 5c 7e 0f cb e5 a3 05 8d c0 37 81 13 03 a3 9d 44 f4 ab 57 56 7c ae 1f 11 ef 12 2f 54 7d 2d 6d 66 ff e4 71 b8 e3 6c d1 09 47 bb 2d 54 be 03 66 c1 5f a6 8d 64 54 4b 18 52 5a 3e 50 52 07 e0 da 4a d7 4b b3 b0 aa 9d ba 5d b3 56 2e e6 a4 05 aa 01 74 c4 85 44 97 80 dd 29 5f a8 5e 58 6b 7f 6c 61 aa 39 49 aa d5 ef Data Ascii: AQl4Av*jY&Fblpq@N;O$}.C^cI#\|nzQpMbc"wAZNFWGu${rT6v0)?]3\~7DWV|/T}-mfqlG-Tf_dTKRZ>PRJK]V. tD)_^Xkla9I
2021-10-13 10:36:37 UTC	40	IN	Data Raw: 74 7d b8 b2 e8 5e a0 99 be cc 65 b7 51 4b df b7 c8 f2 17 5b e9 1a de 73 7d b7 6b ed 1b 0e 20 21 71 d9 d0 ef 14 aa de 0b ae da 92 53 79 11 1f c0 95 c2 80 d9 4c 63 50 1e ea e6 94 b6 01 ca cb 9f e5 8e 02 f8 ea ae da 25 e9 6c cd ac e2 8e 17 ff 62 2c 7e 6a d7 3a 81 e3 38 d6 84 fd 1c c0 fd 95 91 b3 4a 24 0b 1d 89 46 0e 07 18 ef d7 42 8e 40 77 e8 b8 3f fe 33 c8 ff c3 7a 03 19 97 33 f9 c5 3b ce 27 0e 4a 09 64 25 bd 76 02 47 22 f0 50 28 93 bd a4 d4 63 41 66 17 04 38 05 99 84 6e 58 ca b4 64 96 5a 71 f4 4d bd 8f 5f da 9f 61 1c 79 da 6f 1c 7a 30 19 42 7e c0 13 ff ba 5f dd d1 34 36 de 9d 75 d3 63 fd 7a e5 b4 1a 61 d7 1d b8 75 21 ce f0 1c 38 41 79 c0 98 4c c2 6f 61 c6 7a 16 79 58 cd 27 d6 8a 35 bd c5 6b 73 0c c2 27 a4 4a 22 23 22 b6 00 23 b9 7f 57 e3 90 89 95 d6 bc e5 Data Ascii: t}^eQK[s]k !qSyLcP%lb,~j:8J$FB@w?3z3;'Jd%vG"P(cAf8nXdZqM_ayoz0B~_46uczau!8AyLoazyX'5ks'J"#"#W

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	41	IN	Data Raw: a6 57 e2 ef c0 2c 2d ad 52 5f 0a 6e 36 b7 8f 39 33 d3 27 ed 4d 74 7b 34 0c 5a 14 03 d4 2f 0f b9 a4 08 54 be 1c 05 d6 9d 1b 9f 6e 37 56 1d 1b 61 6e da 77 e1 d9 0d 7f ec fe 73 ae 4d af fc 71 c0 25 6a 36 fd 92 3c e2 de 0e 09 47 91 bc 9f ad 89 e7 8b 09 1d 6c 57 f6 f4 1c 79 89 83 86 39 e6 f9 5a cc 5e 5b a1 ab c4 b8 40 ad fd 96 c5 37 6c 54 1a 89 46 db d9 d7 b3 20 8e 42 ba 2c 20 8b db c9 53 03 5a 74 82 91 62 8a 1a 79 6f 37 3e 07 7e 65 59 71 1b ed 29 f2 5e 53 19 61 39 de 7b 47 06 d2 57 ea f7 cc 38 07 00 b1 9b 9e ca e9 8f ac bd e1 3b 2c 10 e7 c9 21 2e a6 ec 90 0d 80 4f 41 d7 f4 61 4d 59 44 25 18 c2 14 ba d7 b4 9a 29 b4 87 3f 44 3f cc c9 2d c1 5b 8f 69 bc fc 77 d8 ac 55 03 b8 fc dc 02 90 d2 24 83 b7 f1 7e de 55 a7 1c d1 c3 2e 5c dd 80 a8 1c d4 ad 00 70 62 d3 e1 e7 Data Ascii: W,-R_n693'Mt{4Z/Tn7VanwsMq%j6<GlWy9Z^[@7lTF B, SZtbyo7>~eYq)^Sa9{GW8;,!.OAaMYD%)?D?-[iwU $~U.\pb
2021-10-13 10:36:37 UTC	43	IN	Data Raw: 4f 1e b7 42 32 0e 18 87 cf 49 8c 0e f5 cc e8 b6 36 f3 ae f8 c3 b2 6f e7 16 1f ba 10 02 94 41 61 3f 92 d3 eb 5b aa d1 0e 1e 71 85 82 1b 60 5e 40 ce 1d 4c ad 83 9e ab 55 19 b5 ac 42 42 36 4f 40 49 35 80 bb e1 ce 2a f8 80 51 20 be 5f 9e 0d a9 8d da f7 07 40 bd a6 d2 f6 cf 3e 8d 4f 0c d7 34 c4 41 94 55 c0 0a 04 c8 94 47 17 07 5d 7e a7 af a3 d8 bd 4d e2 4f 0d 3a 93 ba 7a d4 7f 23 74 5d 65 61 bc cf 42 07 66 f8 cc 6c 44 96 bb 47 f9 f5 37 7d 1b b3 bb 8d 47 bf 26 fd 21 eb a4 95 77 52 cd 89 02 12 35 d8 67 04 61 a3 6f 24 1f 2a 27 03 d2 ba ca ed f0 be 73 e4 42 9f bb 89 1b e4 2c a8 9c 11 2d db 2c dc 2d 60 52 a3 0f 98 de 40 9b 1a 17 59 8d 5a d6 fc 5d 40 88 2f 07 1a fe 1d 03 42 44 c9 7a b0 e6 f2 65 d0 72 6a ef e3 a8 4d fa ec be dd 70 f7 72 92 8d 64 75 78 16 7a 91 6e 50 Data Ascii: OB2I6oAa?[q`^@LUBB6O@I5*Q _@>O4AUG]~MO:z#t]eaBflDG7}G&!wR5gao$*'sB,-,-`R@YZ]@/BDzerjMprd uxznP
2021-10-13 10:36:37 UTC	44	IN	Data Raw: ec 33 b4 2c c5 a0 bc 63 d3 fa a8 16 c6 85 68 6c fe c0 d4 e7 01 63 71 01 2a 21 b3 a5 c7 76 80 2f d0 ba c4 a2 5a eb 17 fb ce b0 3a 5c 36 d7 bb e3 4d 94 ae 89 f2 91 a4 66 50 e4 93 c8 d0 34 73 d2 1d b1 73 68 c5 6d b3 c1 6d 3f ba 61 de e8 f9 30 bc cf 04 33 8f e0 f3 5d b3 4a b8 88 eb 22 fa 59 75 6c 0f 02 78 8a b6 71 af 65 8a f1 9f 07 d4 ad be dd 5d 3d 49 cd cd bf f6 1d ff 64 24 53 9f d2 12 31 f0 0b c1 8c 87 0e c9 d1 a6 81 b3 1f 25 0b 1d f0 8e 0c 16 21 f2 3c 43 8e 3a 49 77 d8 3f f8 2a d7 10 c9 31 ee 20 95 01 c4 81 30 bd 19 1d 41 19 4a 1f d9 3a a8 47 52 58 64 3a ed 2f 06 f1 71 22 1f 19 bc 48 a7 ba 8e 7a 43 68 91 55 c4 b4 47 17 3d 1f a0 43 da ab b1 ed 40 a8 1f 6c 76 41 bb 6c 92 40 13 f5 a3 4e 47 da 34 30 c9 89 4c ea 21 8f 79 ee 34 61 77 ff 79 b8 75 3a d0 19 c9 3a Data Ascii: 3,chlcq*!v/Z:\6MfP4sshmm?a03]J"Yulxqe]=Id$S1%!<C:Iw?*1 0AJ:GRXd:/q"HzChUG=C@lvAI@NG40L!y 4awyu::
2021-10-13 10:36:37 UTC	45	IN	Data Raw: 48 56 c2 a7 c9 a5 12 67 70 7f ba ff 19 34 6b 68 d8 9c 23 41 52 a2 d4 c3 4a 8c 25 b3 b0 67 b9 38 5d b5 33 86 a0 a4 0f 88 f6 7f ba 88 57 92 84 dd 26 05 ed 5f 58 11 e9 4f 01 aa 3d 9d ac 0e c4 79 72 68 3a 18 52 13 59 50 0a 0f c3 15 04 55 b8 30 16 92 f0 1e b7 da 37 56 1b 7c 69 7f d2 6a a2 df 25 ef ed fe 79 d6 7b ae fc 7b af cd 6a 34 f7 ba 8b 5f de 08 1a 7c 80 b5 8b bc 88 f4 81 0f 17 7a a9 f7 e7 17 68 80 af 90 11 02 f8 5a c6 7d 5e ce 2b fd b9 4a bc e3 be 7d 37 6c 52 09 8c 44 db d9 fc c2 21 a6 a1 88 2c 2a 8c 49 cf 21 d7 68 74 f2 fe 6e 8b 1a 7f 00 b7 3e 07 62 4d bd 71 11 e9 3a f7 7e 40 1d 13 2a df 7b 37 54 fa 37 eb ec f6 2b f9 19 a1 9e ec 81 e8 8f cd ab ba ff 2c 10 e7 d5 ad f6 b2 ff ec 34 bb 62 0c c0 0b b5 06 59 35 28 48 b0 38 f5 dc c3 10 69 a3 8e 97 6d 2f 87 56 Data Ascii: HVgp4kh#ARJ%g8]3W&_XO=yrh:RYPU07V\ij%y{{j4_|zhZ}^+J}7lRD!,*I!htn>bMq:~@*{7T7+,4bY5(H8im/V
2021-10-13 10:36:37 UTC	47	IN	Data Raw: dc 9f f9 90 67 8f 78 46 91 7d 66 d8 df 9d 6d 3a f4 18 85 01 7f 0b c3 93 ee a6 6d 5e b0 52 56 72 4e 39 24 89 99 28 9d bd 4c 3e 11 54 30 40 4a 23 00 27 f6 d8 7b cb 0c f4 c6 f7 96 1f 93 a4 97 21 a4 91 ee 2f 9a c8 13 05 87 38 66 1e e6 2d ea 42 b6 3e 07 57 9c b3 80 27 5d 1b 71 55 0a af ad 82 b1 ac 22 20 78 ac 32 ea 02 51 79 e0 97 a5 a5 80 82 61 f8 f0 d8 25 a7 66 67 af 8c 9d af 85 4b 32 19 21 f7 9d b1 00 2e 6a 16 ca 3b 8f 41 ee df 0c 89 04 ce 8d 51 2f 68 52 0c a4 aa b2 90 83 23 82 4f 07 b0 8e 44 79 c1 7a 51 66 5b 72 c7 b9 e0 33 00 77 f4 e4 47 bb 36 57 4b e8 27 0b 15 2e 0a 84 8d 4d ad 3a eb 7b 10 e3 95 0d 2e e8 9e 21 b0 10 c0 54 68 47 a3 1f 86 3a 33 25 07 70 9f 60 9c 1e a0 b0 97 e0 ba b0 98 1e 46 4d b4 ee 10 29 eb 54 7e ec e0 52 a3 4c 8b d3 2f 90 05 0b 75 8d 56 Data Ascii: gxF}fm:m^RVrN9$(L>T0@J#'{!/8f-B>W']qU" x2Qya%fgK2!.j;AQ/hR#ODyzQf[r3wG6WK'.M:{.!ThG:3%p` FM)T~RL/uV
2021-10-13 10:36:37 UTC	48	IN	Data Raw: 5e 47 2b fb 4e 0e c0 2e 90 90 c4 38 06 af 86 ef 79 68 be c9 64 db 2a 2d 46 d1 e6 73 7a 92 42 6e 59 6f 86 72 32 f6 2c 96 bb 4c 6f d3 23 b1 1c de 9b a6 75 5e 8a a8 64 fd ef 7e 0b 71 d6 f3 e5 1b 5d 59 06 35 25 b1 b0 c7 6f b1 01 c0 95 d5 4a 5a de 2e 42 5f d1 85 67 0a c6 bf f8 56 b7 b8 d4 c7 00 b7 51 41 d3 bf c9 81 4d 73 bb 1c b1 73 54 25 6d fa cb a9 ba 26 65 c1 f0 a5 a0 b9 d9 1d b7 c8 36 e0 54 00 67 b9 b6 7c 91 da 50 63 56 76 b1 51 b1 bc 76 8d 81 9e e5 82 1a ed eb a8 0b 44 3b 58 cb c3 95 b3 8d e5 77 36 7c 6a db 09 ef 91 54 9f 97 85 62 9b d0 d6 9d 90 6e 2c 1e c1 f5 79 1e 0e 05 af da 9c 9e 6f 77 6b b8 3f f2 33 cb ee e2 3e fd 18 8e e7 e8 cf 2a 3a 0d 1d 47 32 6f 08 bb 5e e1 47 22 fd 41 e4 2c 3d b4 90 69 50 6e 24 8c 3a 05 dd 97 6b 58 81 b4 4f a7 5a 59 15 3e e9 84 Data Ascii: ^G+N.8yhd*-FszBnYor2,Lo#u^d~q]Y5%oJZ.B_gVQAMssT%m&e6Tg|PcVvQvD;Xw6|jTbn,yowk?3>*:G2o^G"A ,=iPn$:kXOZY>
2021-10-13 10:36:37 UTC	49	IN	Data Raw: ee 61 3f d3 4f 7a 2e a9 43 a7 2d 73 d3 3e 96 0d 9a c9 9c 57 ff 9f 4b 5f a0 32 63 f6 fe 19 09 51 50 df 68 70 6f f8 06 64 6d 6c a1 12 53 9a f4 ec be 09 73 d6 59 8a 81 6d 10 99 18 7a b3 21 6b a6 01 da dc 2e 10 68 a2 c6 d6 96 aa 5a 99 3b 85 f2 a4 0f 93 e1 06 fb 9a 57 e2 ef 63 2d 2d a1 4c 50 0a 61 69 a5 a3 33 68 bc 2d c6 4d 72 68 23 3b 4a 13 7d 00 0a 0f c3 cb 04 44 be 18 6d b0 8c 1e b3 d2 1c 56 1d 22 7a 4f d3 5b ae df 25 4a e7 fe 79 d0 7b ac 87 1f af cd 6e 3c dc ba 8d c8 cd 38 1b 4e 8c b5 8b 53 82 f4 81 09 17 78 d2 92 e7 17 6c 88 84 90 17 2f ea 6a c7 4f 52 ce 2b c4 b2 4a bc e5 be 7f 4c 0e 52 09 88 4c f0 d9 fa b9 3b 96 a2 ba 02 2b 8c ca 9c 21 d7 6e 74 f2 d6 3e 8b 1a 75 00 a8 c0 0c 6c 40 be 73 60 84 3a f7 5a cc 74 ed 38 cc 7f 26 14 d6 31 f3 fa d0 24 d2 72 ba 93 Data Ascii: a?Oz.C-s>WK_2cQPhpodmlSsYmz!k.hZ;Wc--LPai3h-Mrh#;J}DmV"zO[%Jy{n<8NSxl/jOR+JLRL;+!nt>ul@s `:Zt8&1$r
2021-10-13 10:36:37 UTC	50	IN	Data Raw: 48 d6 55 b7 5f e5 fd 0c ea 16 3c 9b 98 4a a9 10 e2 53 40 fc 82 0a f4 ff 44 18 be 13 d3 1a 65 49 b0 0f be 92 33 36 07 6f 87 dd 8e 0e b7 a9 97 1e be b6 66 1f 55 18 a5 ff 3d 64 c4 45 73 14 e7 43 aa 07 f0 bc 3e 90 1e 06 4d 0d 46 f9 ad 87 5d dd cb de 3a 01 19 03 42 44 c9 72 79 aa 96 2b d5 18 03 d1 03 52 a3 15 fb 64 92 71 da 47 f9 ef b6 1f df 84 65 a3 33 41 5f 17 27 ce 3f 1c 75 be d1 cc 86 6d 4e bc 26 b2 eb b5 07 95 3f 67 cc 83 7c a4 80 d3 33 20 ba 59 4e e5 68 57 13 bb 2b 6f 9a 34 f3 40 63 6c 21 02 49 68 1e 00 0a 0b d8 db 95 44 b9 0d cc ce d3 7a 65 f8 c8 56 1b 08 78 78 cd 44 fd bc 7a fe 71 fe 66 e0 76 bf ec 6e 79 de 7a 27 e7 ab 84 de 91 f7 e5 b1 9f 97 86 42 8c e2 a9 7d 16 7a a3 fd cc 17 b5 63 af 90 11 0d ee 02 d0 43 1b ea 2b c4 b8 4a bc f4 be bf ca 93 ad c2 71 Data Ascii: HU_<JS@DeI36ofU=dEsC>MF]:BDry+RdqGe3A_'?umN&?g|3 YNhW+o4@cl!IhDzeVxxDzqfvnyz'B}zcC+Jq
2021-10-13 10:36:37 UTC	51	IN	Data Raw: d1 dc 84 9d 60 31 07 15 f7 76 8b 2f 11 81 3f 44 9d 41 40 4a b4 2e f3 33 cc f1 dc 62 ff 09 82 bd f9 c4 05 34 27 1d 47 0b 61 16 bc 52 fa ca 40 fa 41 2c ef 32 bb cc 65 46 7c 2e a3 21 09 8e 9a 7c 8e d9 bf 50 ac 56 5b 06 46 95 86 59 cb 9e 00 c5 43 c1 13 62 79 20 08 46 00 4b 02 f2 98 73 38 d1 32 af d2 84 79 d3 68 9e 68 72 ab 63 1d 01 7f ab 67 3a ca 22 7f 36 59 07 c1 88 43 a3 68 df 8e 7f 17 73 48 20 37 98 8a 15 89 d6 59 32 00 40 09 b5 5b 2c 17 25 52 d6 6c d3 d5 99 e5 87 80 37 f3 a4 97 2b f2 34 c5 ac a8 ba 1a bd 18 48 5b 12 86 32 ca 44 b1 cf 15 19 9e 8b 80 01 e7 4a 60 b2 ef c3 8e 83 94 ba 50 76 35 ac 02 13 0f d4 68 f1 3f 39 22 f2 cb 01 e0 80 65 23 b2 66 72 1c b8 85 a6 95 00 32 6d 92 dd 97 b1 a4 3b de 64 27 b4 db 64 92 6c 35 1d d2 dd 96 53 06 0c 67 30 5b 51 5c b7 Data Ascii: `1v/?DA@J.3b4'GaR@A,2eF|!|PV[FYCby FKs82yhhrcg:"6YChsH 7Y2@[,%Rl7+4H[2DJ`Pv5h?9"e#fr2m; d'dl5Sg0[Q\

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	52	IN	Data Raw: 05 f3 4b c9 58 c8 bd 4c c5 b8 40 94 9c bf 7d 3d 7d 5d 11 1a 35 bc d8 fc 99 08 ce a0 ba 26 3b 83 d3 58 52 b0 7e 74 f8 d6 06 8a 1a 75 28 de 3f 07 7e 5c b2 6b 8d 5c 55 86 5f 42 17 6e 45 df 7b 33 10 c2 96 ea f7 c6 31 c6 0f a2 e5 9d c9 e8 8b af cd c8 5b 26 09 87 ac b8 2c f9 f5 b4 73 8d 63 06 dc 87 5f 5e 45 54 1c 22 ce 27 bf db c6 43 7e a3 8e 99 70 22 af b3 dd 4e 0b 2d 4c a7 c5 01 7b 89 45 73 2d 8d dc 72 36 e6 39 e1 d4 52 5b c8 36 a9 70 b6 b2 8c 7e 76 e8 a9 16 cd b1 71 6d f4 a0 82 f7 1d 41 62 69 2b 2b a8 a9 d9 7f 07 72 a6 94 d5 98 63 b2 3e 4a c4 a1 3f 6c 9b a4 dc e8 5e ac 97 d0 e5 00 bd 40 4e ca 29 82 a6 17 5b e3 35 d9 78 7c bd 45 93 c0 1d 2c 26 6d c4 7e 4f 7a db df 0c b5 a0 9f f3 5c 15 6f b0 db cf 91 d5 56 b2 52 13 89 5a a0 bf 4f 67 3f 61 1a 88 29 7a ec bf dd Data Ascii: KXL@}=]]5&;XR~tu(?~\k\U_BnE{31[&,sc_^ET"'C~p"N-L{Es-r69R[6p~vqmAbi++rc>J?l^@N)[5x|E,&m~O z\oVRZOg?a)z
2021-10-13 10:36:37 UTC	54	IN	Data Raw: 80 6c c1 41 9e 62 28 07 06 cd f4 24 16 16 53 12 ce dd c4 a9 ab 6f aa 27 0c 30 8f 55 72 dd a2 22 19 5d 65 1b 82 8f 23 07 6c da b3 93 47 c3 b0 63 ee f8 1b 36 15 39 9b 80 4a bd 70 8d 52 40 e9 8a 63 9a 9b f9 0a b0 1a e8 7a 75 47 a9 09 78 39 20 22 16 64 b3 d9 80 10 ad 62 93 e3 6d b3 9f 01 49 04 b6 ff 16 b6 f3 5f 7f 05 e5 41 af 1a 9b de 3c 81 1d 93 4c 90 7f fa bb 5d 46 91 a2 13 0b f3 1b 12 45 26 a8 6c 66 ff e4 78 a4 0d 6d d1 09 47 b5 76 8a bf 03 6a fa 31 a7 8d 6e 57 03 19 7a b3 40 3a 59 00 fb f5 50 02 6e b9 e8 ac 90 bb 57 9d 3a af e6 a2 1c 8c fa 66 c9 81 2c e6 80 cc 29 3c ad 4e 53 cd e6 5b 01 aa 3b 41 ad 2c 9f 2b 73 68 3a 1a 47 60 1f 01 0a 05 d8 cc 77 33 bf 1a 1c fb e7 1f b7 d2 1f 3e 1a 08 63 01 b8 5a a2 d5 0d 22 ec fe 73 e9 12 af fc 71 be c3 42 32 f6 ba 8d 9f Data Ascii: IAb($So'0Ur"]e#IGc69JpR@czuGx9 "dbmI_A<L]FE&IfxmGvj1nWz@:YPnW:f,)<NS[;A,+sh:G`w3>cZ"sqB2
2021-10-13 10:36:37 UTC	55	IN	Data Raw: d5 50 6b 32 7e 99 50 bb 9e 19 a4 c7 94 f4 9b 62 92 ec bf d7 7f 55 48 cd d6 a5 eb 17 ff 6e 2e 6b 6a cb 9d 29 e3 38 d2 ec 83 0d c8 d5 61 f8 ea 7e 25 01 b5 e6 70 24 5c 12 9f 02 4f 8c 31 2b 5f b8 3b e9 26 d0 e5 1c e1 e2 18 84 3b 93 b6 2d 30 22 0c 58 1a 7e 0e d8 38 e0 47 28 eb 4e 5e 9b 3c a4 de 41 38 6e 3f b6 29 16 ec f9 6a 58 c0 9c 27 b7 5a 53 3f 24 bc 85 52 da 88 02 d1 d3 c4 1f 73 74 4a 6f 44 11 44 a4 d7 b6 76 39 d7 1c 45 cc 98 7f 60 67 90 46 e9 a5 79 1d ee 6d a9 6c a4 c6 0e 1f 2b 3f 7d c3 99 48 64 ce 5a b5 65 56 7e 5f 2a 33 5f 8a 20 bd d0 56 26 2f 0a e5 5b b5 3c 47 39 d5 c2 76 6f 1c fe d7 8c 91 3d cd bb 6d d4 4d 6f d5 1b a9 ba 10 1b c4 45 72 4d e9 2d ea 4c a3 44 95 13 71 85 82 0f 60 4a 55 d5 34 af ad 9c d0 b7 52 75 46 ca 43 48 2d 5f 02 82 52 81 bd f8 e3 42 Data Ascii: Pk2~PbUHn.kj)8a~%p$\O1+_;&;-0"X~8G(N^<A8n?)jX'ZS?$RstJoDDv9E`gFyml+?}HdZeV~_*3_ V&/[<G9v o=mMoErM-LDq`JU4RuFCH-_RB
2021-10-13 10:36:37 UTC	56	IN	Data Raw: a2 de 0d 27 ec fe 73 b5 6a ae fc 60 fe d2 7f 3b f5 c1 fe e2 de 0c 0b 45 91 b0 9a 58 12 56 81 07 00 77 b8 fc f0 c1 7b 89 be 9b 00 0f c7 15 39 b0 a1 d1 33 c9 ba 48 c7 86 be 7d 33 7d 56 86 ac 46 db db 87 ed 20 a6 a5 ad 46 f0 8e b1 be 21 d7 7b 1a 2a 44 46 83 1b 7f 06 bd 15 07 a9 f4 bd 71 1b e3 2d af 48 4e 58 09 3a df 7b 37 10 fa 37 3f 0a 39 d1 27 fe 5f 61 0f 34 17 70 28 56 36 a4 0d ee 12 20 f8 d3 06 00 b5 e2 73 9c 27 34 86 a1 74 a7 ba ff 49 4e c7 00 86 3a c7 f3 38 70 62 9e 89 40 46 f4 01 d5 d2 b3 71 13 8c 85 6b b1 8e a9 15 22 8d cd e5 c0 6d 4d 47 a4 3d d8 bf fc 2e 4c b7 8b a1 7f e4 e9 38 5f 33 84 9d 2c ba 09 e2 b4 c3 fe d5 d4 7c 82 df 64 96 1e 3f a5 d6 85 60 db 38 0f cc b0 30 74 0d d7 bb e9 2a 59 40 47 3a 20 c2 15 41 d3 be e5 3f 15 5c ff e3 b2 26 74 a1 93 fb Data Ascii: 'sj`;EXVw{93H}3}VF F!{*DFq-HNX:{77?9'_a4p(V6 s'4tIN:8pb@Fqk"mMG=.L8_3,|d?`80t*Y@G: A?\&t
2021-10-13 10:36:37 UTC	57	IN	Data Raw: ad 83 95 9f 46 61 ab 84 3e 49 27 4c 68 ec 39 82 95 11 cb 2a f2 91 7e 6f 3e 77 7d 07 d4 e8 dd e6 04 2c 65 81 d0 99 b0 2a a4 49 0b b8 b2 43 3c ee 7d 24 0e 1b c7 8b 40 15 09 61 16 8c a8 a2 a8 ad 18 f3 4f 0d 34 9a 4e 75 c7 01 20 77 5c 61 62 cc e6 22 0d 18 8f db 92 4d e1 c7 4a e8 f3 0d ce 07 2d 81 9c 42 92 08 f4 58 4c e1 82 6d 8d 99 9e 0b b4 0f cc 19 76 58 c7 75 ae 3d 32 36 01 70 9f d0 42 93 a0 73 94 e7 ad f8 8e 15 03 06 b4 ee 11 32 db 5c 7e ee 1d ad 5c f1 75 2c c1 93 e5 e8 a2 8e a8 01 45 7f bf 7d 50 3c e5 01 e6 41 bd aa 31 3b 99 0a 0a 1c 28 9c 93 ab fc a9 4d 9e 13 41 fc c6 2d a5 59 3e 9b 80 94 ad 85 46 c1 8e 62 08 fa db 27 fd 5e b0 d7 ee 90 bd 18 b7 39 ae e6 a4 0f 82 e5 d4 3b 7c a8 4c a0 b9 69 2d ab 5e 4c e5 6a 42 17 54 3a 1c bb 3d 12 4c 2d 96 21 7f 0f 13 71 Data Ascii: Fa>I'Lh9*~o>w},e*IC<}$@aO4Nu w\ab"MJ-BXLmvXu=26pBs2\~\u,E}P<A1;(MA-Y>Fb'^9;|Li-^LjBT:=L-!q
2021-10-13 10:36:37 UTC	59	IN	Data Raw: ab f9 11 aa 7c a0 0d b0 e3 da e8 4d fa 1d b1 62 13 b6 6d fa cb 1d fa 37 62 00 f8 dd 3d 9e de 0c b5 ce fe f3 74 41 6f af 93 1d 80 df 6b 25 0d 19 98 52 b1 b6 71 03 c7 9e e5 95 11 fc ed 7c dd 57 3d 47 cd dc 8d 82 16 ff 64 3d 7b 7b d2 92 36 e3 38 ff 97 f5 0d 67 d0 d6 97 94 7f 25 0b 17 e6 70 0f 07 12 80 3f 43 8e 4a 5f 9e b9 3f f8 e2 c0 ee ca 7e fd 18 84 7d e8 cf 2c 2b 16 19 41 cc 6e 09 ab 03 e1 47 33 fa 41 39 f6 29 af c2 65 46 62 20 a6 10 14 9e 97 61 2a 7b e7 4f c6 72 27 16 4d b7 ad 7b ca 98 19 db 58 a8 1c 72 76 41 0a 41 00 44 9d 96 a6 89 38 c2 32 21 cb b4 74 c2 67 9e 7d f7 b3 7c 64 f7 56 fc 64 2c c9 06 85 3a 4d 1a ca eb 21 e0 79 39 8e 05 17 73 44 20 2e 98 93 b7 c5 df b9 3c 02 44 09 af 66 2b 17 3e d2 53 6a ae 02 f5 c6 8e 93 3b e2 a8 bb 21 a3 66 c5 76 a9 ba 16 Data Ascii: |Mbm7b=tAok%Rq|W=Gd={{68g%p?CJ_?~},+AnG3A9)eFb a*{Or'M{XrvAAD82!tg}|dVd,:M!y9sD .<Df+>Sj;!fv
2021-10-13 10:36:37 UTC	60	IN	Data Raw: c3 59 1b 69 44 10 ae 2a 44 aa 38 e4 66 36 79 37 1a 43 89 62 09 1b 06 bb a6 56 55 ce 32 69 d2 8c 14 a4 d2 26 5c 95 61 7f 81 d0 48 a9 ce 2e 66 e5 ef 73 d7 e1 a5 eb 76 af cd 63 25 fb ab 87 ce d4 19 13 66 c8 b4 8b 55 ae df 97 18 17 6b a1 e0 31 04 60 93 a7 81 16 8b 90 a4 c2 5c 53 df 26 e9 16 43 af fa af 73 0e 4e 53 09 8c 46 dc aa 7c 92 20 ac b2 aa 3d 3a e3 41 ce 21 dd 6c 65 81 7f 6f 8b 10 6c 12 a6 2c 16 65 22 b8 71 1b c0 29 f8 80 4c 1d 02 2a f3 73 26 00 95 36 ea f7 cc 2e 25 12 af f1 f1 c8 e8 89 cf b8 df 48 38 28 6a df df 2d e8 ec 8d 08 16 70 19 b8 7a 5f 4d 29 56 16 1f a5 57 cd d6 c4 3e 24 ea 8f 9d 67 34 a9 a8 1e ae 1f 2c 4c a3 c5 3a 7b 89 49 62 4e f3 c9 1d 14 f6 3f 94 a1 4a 46 4f 18 a7 03 d0 96 9a 06 07 d5 a8 66 65 85 69 6a 7b 71 c0 ee 6f 3b 6c 01 5a 89 87 a1 Data Ascii: YiD*D8f6y7CbVU2i&\aH.fsvc%fUk1`\S&CsNSF| =:A!leol,e"q)L*s&6.%H8(j-pz_M)VW>$g4,L:{IbN?JFOfeij{qo;lZ
2021-10-13 10:36:37 UTC	61	IN	Data Raw: c8 61 c9 1c e3 d7 92 ef 05 f2 a4 91 03 fb 6e ed 38 bb ad 01 11 e8 7c 71 36 80 05 a3 49 a0 c6 17 10 9e 91 fe 36 70 55 6a cb 2c b2 20 bc 94 ba 51 53 23 de a1 1e 27 36 ca d4 22 91 a4 50 ee 32 8a f0 5c 00 ce d5 58 14 b8 90 7f c3 1a 40 87 9d d2 f6 02 17 97 5e 12 1a 91 d8 33 9e 62 24 7a a6 e6 04 42 17 1c 4a 1a da a5 a3 a8 af 74 94 67 4b 30 85 4e f9 ce 7a 51 73 5c 74 05 bd 31 31 13 77 e6 cb 81 c9 a0 56 4f fb e3 0a 2a 3c 56 7b 72 b8 96 45 ea 53 46 c5 eb 93 f0 e8 9a 64 33 11 c0 1f 67 5c 88 0d 94 21 1b b2 06 70 95 c3 83 0f bc 5b d3 e1 ba a6 be 1e 54 12 9c 6b 10 32 d1 4f 63 14 fe 7f 42 db 84 c1 25 6e 0c 04 5d 9c 4c 91 bb 5d 40 88 af d0 1a fe c7 13 67 7d fa 6d 66 ff e6 6a d7 4b 3c d1 03 5c 6c 05 ec 94 42 2c d2 5a a4 8d 64 7f c1 18 7a b9 23 50 58 00 36 dd 38 03 60 b3 Data Ascii: an8|q6I6pUj, QS#'6"P2\X@^3b$zBJtgK0NzQs\t11wVO*<V{rESFd3g\!p[Tk2OcB%n]L]@g}mfjK<\lB,Zdz#PX68`
2021-10-13 10:36:37 UTC	63	IN	Data Raw: db 81 a8 1c d4 bd 6f 66 4f 32 3b f9 0f 50 b4 17 39 2b a2 a3 b9 69 91 01 cb 95 09 92 4b 04 2f 6f e6 84 30 74 07 c4 a5 e9 76 f6 bf b8 ee de b7 51 6b 92 f3 f1 c1 14 5b e9 1d 1b 79 7c b7 70 fa c1 1d e1 37 62 de e6 f8 15 aa de 0c bf dd e2 f3 5c 11 eb ae 99 c3 af df 41 64 f2 18 98 50 be b6 71 a5 c7 9e e5 88 11 fc ed bf dc 57 3d 49 08 dd 8d 82 d0 fe 64 3f 6b 7b d2 12 73 e3 38 d1 8c c5 09 c8 09 d7 97 9b 22 25 0b 06 e6 70 1b 0d 06 8b 29 4e 98 47 40 45 90 2e f9 20 cb 9c 70 36 fd 68 ac 47 e9 cf 27 18 05 1c 41 12 7c 0d d9 5d e0 47 52 e9 44 3c f8 b3 cd c2 97 51 7c 39 ad 3e 29 9a 4a f7 59 ca b4 4f a7 5e 4a 10 5b ae 8d 73 8f 89 14 d9 54 40 0c 7a 67 38 6b 29 43 40 63 d7 cf 76 39 db 27 3a dc 92 fb ab 71 71 7b f7 bf 7b 7c d3 75 a9 7f 3d 42 05 08 24 44 0b ca 8a 40 a3 75 65 Data Ascii: ofO2;P9+iK/o0tvQk[y|p7b\AdPqW=Id?k{s8"%p)NG@E. p6hG'A\]GRD<Q|9>)JYO^J[sT@zg8k)C@cv9':qq{ {|u=B$D@ue
2021-10-13 10:36:37 UTC	64	IN	Data Raw: 94 5a a6 87 77 6c 74 32 52 a8 3f 50 52 72 32 87 38 73 46 f5 c0 c5 9b a8 49 a1 2a bb e1 8c c2 82 e5 7e d7 95 46 84 ac c5 2a 3e be 5f 60 81 68 44 01 a3 11 8e bc 2b e6 5e 65 79 27 27 42 1a 62 15 0a 37 4c ca 04 55 b6 32 db d3 8c 14 a4 c0 26 4e 37 01 61 6c c7 5b 9a af 24 4a ed ef 7d e9 b6 ae fc 71 bc d4 7b 2f db b0 9a e6 cd 1d 1a 76 d9 b4 8b 53 99 f1 a9 d5 17 7a a3 e4 fd 06 72 ae a5 81 14 16 ec 5a fe 0d 5f ce 2b d5 be 62 71 f4 be 77 24 77 43 12 a0 4c ca df ef 86 20 9e 8a bb 2c 2a 9d cd e6 ec d7 7f 7e e1 e2 7f 97 36 75 11 b0 2d 12 74 75 a9 70 1b eb 2b ff 76 8f 1d 13 30 cc 66 26 0d d6 3d fb ff d5 3b f9 3b 5d 9e ec c9 f9 86 f4 66 c9 5b 26 03 f3 ce c1 01 f3 ee 95 0f 99 63 34 2c 79 5e 4d 48 4f 28 c3 b0 38 f5 c4 db 29 13 8f 84 8c 6b 34 ab b9 33 0e 2b 2d 4c b4 e1 5b Data Ascii: Zwlt2R?PRr28sFI*~F*>_`hD+^ey''Bb7LU2&N7al[$J}q{/vSzrZ_+bqw$wCL ,*~6u-tup+v0f&=;;]f[&c4,y ^MHO(8)k43+-L[

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	65	IN	Data Raw: db 1f 05 9c 18 cb 5b 79 bd 7d 70 5c 36 68 a6 cb 29 d3 1d 2c d4 56 36 1e 3d 50 4b fb f5 50 ce e5 67 68 74 3d 6b cd 25 4d 3b 00 ea f9 4f 89 21 c5 ea a7 c3 42 9f d0 e2 59 d7 52 83 5b dd ce 62 65 eb 64 50 66 f3 4f 86 21 c3 8b 61 71 db eb fa 75 1f 68 0e ef 02 ce 98 e0 a1 8c 61 4f 06 98 27 78 1f 7f 4b a2 4c f3 c9 97 a6 04 aa e5 09 6f cb 05 1e 68 da a9 8f 93 6e 46 00 ee b7 d4 c5 41 e3 3a 78 db d1 97 24 ea 7f 24 0a 04 ce 87 42 17 16 59 0c a4 fe e2 ec fb 24 c6 1f b9 30 85 44 3b 96 30 13 76 5c 64 11 aa e7 22 07 6a f2 da 92 31 fd 86 7b c6 ca 2b 03 37 07 84 8d 47 be 06 eb 3f 40 e3 95 b7 cc e8 9e 28 ce 10 c0 09 49 47 a3 2f b8 3a 33 15 54 04 ed b9 f1 79 d3 73 94 e0 ba ec e3 1e 46 31 ef ee 11 11 8e 0f 7e 81 35 52 a3 15 8b d3 3e b3 5d 42 14 d8 57 fe ba c9 96 82 af 90 0e Data Ascii: [y}p\6h),V6=PKPght=k%M;O!BYR[bedPfO!aquhaO'xKLohnFA:x$$BY$0D;0v\d"j1{+7G?@(IG/:3TysF1~5R>]BW
2021-10-13 10:36:37 UTC	66	IN	Data Raw: 03 65 09 f7 53 6b 5c 28 fa 17 3d b8 21 ae d4 c2 5d 1b 2a b6 38 0e 8f e3 7e 52 ca 67 41 c2 4f 53 17 e5 b2 f1 4d c1 98 95 c7 a2 c1 15 73 d5 26 e7 5f 1b 40 ca e8 b0 60 2f d1 cd 24 29 85 7f c2 5c 85 0d f1 be 6a 16 ed 09 ad 73 2b 06 13 02 35 4e 0b 30 8e 38 a7 73 49 eb 61 62 66 48 33 50 8c 84 25 a6 c9 51 26 65 5a 16 a4 79 02 6a 20 ce c9 ca a7 4b e9 cc 87 17 13 f3 b3 99 2b 18 63 47 28 a2 ba 03 21 c2 49 62 36 42 33 33 68 b2 c0 58 1f 56 a4 be 11 55 4e 6c d8 27 af 63 9c 4d 9a 5a 76 2e 8d 36 5d 21 46 d2 ef 28 9c bb f2 f4 34 e5 9c 70 00 00 62 09 18 a3 87 b8 e7 74 27 63 83 c5 9c d4 27 8a 4f 64 a5 69 c1 4b 9e 14 2e 76 07 c4 87 f4 16 60 7d 06 a4 b1 b6 d4 a8 6f 82 c1 18 46 a1 4e 79 96 6f 2d 74 56 65 9a ba 93 37 09 66 49 c2 18 5c df a8 d5 fe 1d 06 3e 06 b8 8e 07 5c b4 03 Data Ascii: eSk\(=!]*8~RgAOSMs&_@`/$)\js+5N08sIabfH3P%Q&eZyj K+cG(!Ib6B33hXVUNl'cMZv.6]!F(4pbt'c'Odi K.v`}oFNyo-tVe7fl\>\
2021-10-13 10:36:37 UTC	67	IN	Data Raw: ff 65 8a 1a 7f ff 93 3e 07 2d 4d c7 71 14 ea 3b f7 5e 42 7b 26 7c f5 76 37 90 fa 38 eb f4 c6 2e f9 09 be 9e ec c4 e8 0f dc b1 c8 58 2c 10 ed 47 da 2d f9 f2 9c 98 8c 40 0d ca 78 4e 4d 03 7e 93 3f bd 38 6c d7 86 39 0f a2 8e 9d dc 26 be b9 4a c1 be 2d 07 a4 ef 72 7a 89 49 7c 56 e2 9d 72 a7 f7 70 93 b0 52 5b c2 a4 a6 03 d1 f2 8c e1 5e d3 a9 14 c6 a0 7e e3 63 d3 e5 b7 1d de 4a 56 2b 21 a3 b8 d6 32 84 01 c1 cc d5 07 4b 81 3e 4b ce b0 30 d8 22 6a bf e4 5e 3e bf e4 5e 3e bf e3 e5 00 b6 51 41 87 85 0d e7 1b 5b 72 1d d3 78 7c b6 6d fa b4 35 d4 0e 6f de 73 f8 7c ab cd 0d bf dd 48 f3 5c 11 36 af 06 c3 e9 de 52 65 41 19 5d 50 b1 b6 28 a5 58 9e 8c 89 02 fd ed bf c2 56 3d 49 94 dc 12 82 7f fe 55 3f 12 53 c5 12 06 e3 a2 fa 88 f5 3c c8 6b fb b0 9b 6e 25 0e 15 c9 70 3e 07 bf a6 08 42 Data Ascii: e>-Mq;^B{&|v78.X,G-@xNM~?8l9&J-rzI|VrpR[^~cJV+!2K>K0"j^>QA[rx|m5os|H\6ReA]P(XV=IU?S<kn%p>B
2021-10-13 10:36:37 UTC	68	IN	Data Raw: 07 67 f2 31 96 c6 c9 aa 4b e5 d8 1b 30 06 3e 82 95 10 a5 09 eb 50 40 37 b0 07 f0 e8 9e cd b2 c7 dd 9c 74 44 a3 eb a3 3a 33 36 07 b6 9d 23 97 90 a0 77 94 ec 9c a0 98 1e 46 8a b4 b2 1d a0 db 58 7e 2d c5 52 a3 05 8b 15 3c c5 08 80 5d 98 57 2a 9f 5d 40 82 af ca 18 29 04 8a 42 51 ce 99 43 f5 f5 74 d7 a5 6e 22 0b d8 b2 00 ec fe 25 60 d2 5a a6 0e 64 23 67 8a 7a bc 3e 78 7e 00 f1 dd 38 c5 6c e6 d2 52 91 be 5d e9 1f ae e6 a4 0f 93 e5 8b c0 fa 57 97 80 db 0c 2d ab 5f 58 1a 69 af 05 2b 39 45 bc 26 cd 4d 72 68 30 0d 53 44 6a 0a 0a 08 c9 43 22 55 be 1a 16 d0 84 dd bf 47 37 51 1b 05 48 7f d2 5b a2 d9 3d 1d f6 f4 79 c6 7b 12 da 7b af cd 6a 25 ff 7d 89 53 de 0f 1a 4a a7 b5 8b 53 88 e7 89 f9 23 cc a9 f0 e7 36 49 82 af 90 11 16 f1 b0 fb f4 5e c9 2b ee 99 4a bc f4 be 6c 2f Data Ascii: g1K0>P@7tD:36#wFX~-R<]W*]@)BQCtn"%`Zd#gz>x~8lR]W-_Xi+9E&Mrh0SDjC"UG7QH[=y{{j%}SJS#6l^+Jl/
2021-10-13 10:36:37 UTC	70	IN	Data Raw: 97 1b 23 f7 d1 8e 97 a3 2c 25 0b 17 e6 66 0f 47 2f d1 3e 1a 8e d5 7e 5f b8 3f f8 36 c1 47 e6 51 fd 40 84 a6 c9 cf 2d 30 26 0b 41 0c 5b 36 ab 06 e1 d8 03 fa 41 2d fc 2b a4 52 6b 6f 6f 67 bc a7 24 9f 97 6b 58 dc b4 e8 85 65 59 4f 4d 74 a4 58 cb 98 13 de 5c 1d 37 4c 76 69 19 db 30 40 13 ff b0 61 39 8f 13 0f cd c0 75 5d 46 8f 79 e4 b4 7c 77 a3 5b 87 75 73 d8 91 3e 29 44 0b c3 8f 4c 30 4a 76 a6 22 16 ec 6f 33 24 89 99 2f ac c6 75 01 11 17 18 3b 6b 23 06 34 c4 df 61 16 3b ca c6 df 80 a8 d2 a4 97 2b b2 79 ed 33 9e 85 10 5c 87 d7 51 36 86 2d ea 5e a0 83 35 37 8f dc 91 8f 50 55 6c d8 35 b9 ad 69 ac 85 50 2e 35 33 63 48 27 46 68 e7 35 53 90 cd cb 72 f8 34 29 00 be 77 7d 1b a9 3d ed d9 00 6a 69 7f 81 86 a0 32 8c 59 0a d7 83 fb 41 c6 7d bb 2b 04 ce 87 42 01 16 5b 3a Data Ascii: #,%fG/>~_?6GQ@-0&A[6A-+Rkoog$kXeYOMtX\7Lvi0@a9u]Fy\|w[us>)DL0Jv"o3$/u;k#4a;+y3\Q6-^57PUl5 iP.53cH'Fh5Sr4)w}=ji2YA}+B[:
2021-10-13 10:36:37 UTC	71	IN	Data Raw: bf 90 90 dd 05 69 d8 c6 4f 5e ce 3d c4 2c 67 83 f4 72 7d 03 e8 52 09 8c 46 cd d9 0b a6 1f a6 6d ba f4 af 8c ca ce 21 c1 7f c7 cb c1 6e 47 1a 03 87 b7 3e 07 74 5b bd 77 2e d4 3a 3b 5e 62 94 13 3a df 7b 21 10 81 1b d5 f7 0a 2e 3d 89 a0 9e ec c9 fe 8f 09 90 f6 5b e0 10 85 53 df 2d f9 ff 8a 1c 75 4d 33 ca b5 5e 41 d7 45 00 0e b0 2e ff 8f f4 07 0c 6f 8e 2d ee 27 be b9 0b d7 2b 47 70 9a ed bf 7a dd de 71 56 e2 dc 64 32 3f 3b ad b2 9f 5b 3a b5 a7 03 d1 b3 9a 74 11 b3 97 16 0b a0 e2 ef 62 d3 e5 f6 0b 4b 79 39 15 2b 6e b8 96 fe 91 01 c1 95 c3 92 ee f1 00 4a 02 b0 d4 e3 0d d7 bb e9 48 a6 0f 8e db 00 7b 51 c9 4a bf f1 c1 16 4d e9 da 85 46 7c 7b 6d d6 5a 1d 26 37 62 c8 e8 b5 22 95 de c0 bf 0d 7c f3 5c 11 6f b9 99 9c 84 e0 41 a8 41 6d 06 50 b1 b6 71 b3 c7 4f d8 b7 11 Data Ascii: iO^=,gr}RFm!nG>t[w.:;^b:{!.=[S-uM3^AE.o-'+GpzqVd2?;[:tbKy9+nJH{QJMF\{mZ&7b"|\oAAmPqO
2021-10-13 10:36:37 UTC	72	IN	Data Raw: 32 7a 4f b8 9a b4 c4 41 9e 7b 2c 8d 12 2f 84 b4 17 5e 78 0c a4 ae a3 ae b3 32 99 45 0d c7 85 ff 5b c5 7a 51 77 5a 6d 54 ad 24 21 f0 66 37 f8 92 47 c9 a8 4d e0 b5 1c f7 05 c9 84 43 65 be 03 eb 53 46 eb 07 0c 67 e8 66 0b 68 32 c0 15 74 47 a5 17 19 31 ed 34 ff 70 7e f2 9f 1e a0 73 92 e8 bb b5 0f 1e bf 09 5f cc 11 32 db 5c 78 0d ea 47 7d 07 72 d3 ca b2 1a 17 5d 9c 51 f6 18 48 d7 82 55 0c e4 dc 19 03 42 55 c8 65 d6 e0 2b 76 2d 63 6b f2 03 56 b2 05 ea b6 f4 62 45 5a 5d 8d 75 5c 6b 18 7a b9 38 58 51 03 2f df c3 03 74 90 c0 c5 91 bb 5b bd a2 a9 71 a4 f3 82 c1 57 c4 83 57 92 86 c4 80 2a 75 5d a4 1b 44 67 01 aa 39 43 ba 23 9b 4a e5 68 cd 0b 7c 30 71 00 0a 0f cf c3 8d 52 60 18 eb d3 cc 3d b7 d8 37 56 1d 00 35 74 45 5b 5c df 6f 69 ed fe 79 c1 7d a6 8e 70 71 cf 94 36 Data Ascii: 2zOA{,/^x2E[zQwZmT$!f7GMCeSFgfh2tG14p~s_2\xG}r]QHUBUe+v-ckVbEZ]u\kz8XQ/t[qWW*u]Dg9C#Jh|0 qR`=7V5tE[\oiy}pq6
2021-10-13 10:36:37 UTC	73	IN	Data Raw: af 9b c3 8c e1 41 64 40 19 0a 7c b1 b6 73 a5 9e ac e5 88 10 fc 79 96 dd 57 3f 49 56 df 8d 82 17 ff 94 03 7b 7b d0 12 3c e3 38 d0 96 f5 b1 cb d1 d6 95 9b eb 1f 0b 17 e7 70 a7 20 12 80 3e 42 3b 7b 5f 5f ba 3f 0a 0f c1 ee c9 6e b4 2e 84 39 e9 cf 0c 01 26 1d 43 18 0b 27 ab 5e e2 47 56 dd 41 2d f8 3d 7f ed 69 50 6e 3f 1b 12 05 9f 95 6b 29 f1 b4 4f b7 5a 04 23 4d bd 84 58 65 b5 13 c8 5e da 7c 5e 76 31 1a 44 c2 75 11 df b4 77 f8 e3 34 30 c8 98 5c eb 67 8f 7f e4 92 4d 77 ff 7a b8 97 1a d8 0e 1e 29 19 37 c3 99 4d b2 ae 75 a6 7a 14 73 66 01 24 89 98 39 40 f9 47 3e 13 4f 47 9d 4a 23 07 34 b8 fb 61 b9 0e f5 4f ae 80 37 f2 a4 a8 10 a2 7f ef 3e a7 83 10 04 86 48 74 16 86 2d e8 48 b1 c8 04 08 8e 84 2e 09 71 55 6e d8 5e be ad 83 97 ba 13 65 35 ac 46 48 1f 4b 68 f1 34 80 Data Ascii: Ad@|syW?IV{{<8p >B;{__?n.9&C'^GVA-=iPn?k)OZ#MXe^|^v1Duw40\gMwz)7Muzsf$9@G>OGJ#4aO7>Ht-H. qUn^e5FHKh4
2021-10-13 10:36:37 UTC	75	IN	Data Raw: 69 f7 ff 5b a2 de 25 34 c6 fe 79 c3 7b dc d7 7b af ce 6a 2b db ba 8b e3 de 0c 3a 4e 80 b7 8b 42 80 f4 81 19 17 39 ba f7 e7 15 68 ba a2 90 11 04 f9 ff e6 4f 5e cf 2b c0 98 4a bc f6 be 6c 3f 6c 52 08 8c eb c1 d9 fc 91 20 e5 b2 ba 2c 29 8c f2 c3 21 d7 7e 74 57 de 6e 8b 1b 7f ad ad 3e 07 75 4d b9 51 1b eb 38 f7 4f 4a 1d 13 3b df d1 16 10 fa 35 ea 44 e7 2e f9 00 a0 e5 f7 c9 e8 8b dc a4 df 5b 2c 15 ed 9c cc 2d f9 f9 9c 24 81 63 0c cb 79 fb 6d 59 45 01 0e 1a 19 ff d7 c6 38 bf 82 8e 9d 62 27 c5 a2 0b c1 2f 2d 43 b3 ed 73 7b 89 4b 51 56 e2 de 72 23 ff 3f 92 b3 53 c8 c7 27 a7 01 d1 0a ac 74 5e 83 a8 9f e4 a0 7e 7f 62 90 f6 f6 1d 4e 4a 39 27 2b a2 b9 d6 fb 94 01 c1 97 d5 2b 6b da 3f 49 ce 15 10 74 0d d6 bb 7a 5b a6 bf ba e4 b9 97 51 41 d0 bf 78 e2 16 5b e8 1d 14 42 Data Ascii: i[%4y{{j+:NB9hO^+Jl?lR ,)!~tWn>uMQ8OJ;5D.[,-$cymYE8b'/-Cs{KQVr#?S't^~bNJ9'++k?Itz[QAx[B

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	76	IN	Data Raw: 77 0f 3e 6e ae d1 b5 67 5b bf 36 12 60 df 27 87 6b 6c 17 3c b5 83 c9 22 f3 6b 7a 21 bd 4e 74 08 a2 96 dd f8 08 db 62 62 d1 4a 82 a5 8c b6 0b b9 aa 63 42 e7 7e bd 00 93 ce 5e 41 57 36 4d 00 4d ad a5 a0 75 67 23 4c 5a 2b 29 41 90 c6 da 4c f2 57 8c 12 70 f5 e5 04 8f f1 e6 87 b8 c3 61 49 67 f4 3e 3c f7 3d d3 96 4d be 02 ef 04 5b 3d 97 f6 f3 2d 8b 26 bc e1 c3 4d 6c 73 af 16 82 42 35 e8 05 81 9c f2 bf c0 a2 82 97 07 99 7e 9a 17 45 5e af d4 1d c3 d8 78 61 45 ef 4b a7 52 90 95 32 dc 1a 6f 5b c4 5b 07 b9 0a 5b 5c ad f5 19 ef 0c 2b 47 d4 cc 9c 7f ab f9 8d d4 9d 4d 30 00 af b1 a5 f1 dd 0f 99 d1 87 a1 e7 68 8e 68 f4 76 b3 3e 29 5b 6c e4 4d 34 52 6a 66 dc 53 9d e2 59 81 26 39 e6 c5 0b d0 fa 5f c7 7a 56 08 9f 50 21 3c ab 4a 4e bf 65 2d 05 37 22 e9 b0 62 e8 f4 60 e6 30 Data Ascii: w>ng[6``kl<"kz!NtbbJcB~^AW6MMug#LZ+)ALWpaIg><=M[=-&MlsB5~E^xaEKR2o[[[\+GM0hhv>)[lM4RjfSY &9_zVP!<JNe-7"b`0
2021-10-13 10:36:37 UTC	77	IN	Data Raw: eb 47 a0 e8 a3 ee 00 ae 57 01 c2 bc e5 55 16 64 f2 f5 bf e5 7c e5 4c 65 c1 81 26 aa 40 62 e0 6c 15 fd c5 06 bf 3c e4 a5 46 34 7b de 9b 13 89 c9 40 f0 41 61 9e 08 bd c7 71 f2 dc 40 e7 69 15 fd fe 2a c9 5e 3d 95 cd 88 8f 8b 16 1f 64 66 79 72 d2 f6 37 bd 3a d2 97 a8 0c 7d d0 de 97 07 7e 4d 08 1f e6 d0 0e 6a 11 82 3f c3 8d ff 5e 76 b8 9c f8 fb c4 c0 ca 7d fd ad 80 17 e8 d4 2d 8e 22 33 41 3b 6f ea af 70 e1 6c 22 16 45 03 fc 0e a4 de 6c 7e 6f 04 bc 32 00 b1 97 28 58 26 b0 61 b6 11 59 07 48 93 85 0b cb 92 16 e6 5c 81 1f 79 73 1f 19 27 11 6d 16 d1 b0 1c 39 86 31 1e cd eb 75 a6 62 cf 79 6f b4 02 74 bf 7d 3b 75 f9 dd 4d 1f 52 44 b9 c6 da 4c 31 79 9b a3 33 16 d0 4e df 21 ea 99 42 ac 7b 42 5d 11 cc 18 76 4f 4a 06 97 c4 c9 67 39 0f 7e c6 ef 83 b4 f3 37 97 43 b1 ec ed Data Ascii: GWUd|Le&@bl<F4{@Aaq@i*^=dfyr7:}~Mj?^v}-"3A;opl"El~o2(X&aYH\ys'm91ubyot};uMRDL1y3N!B{B]vO Jg9~7C
2021-10-13 10:36:37 UTC	79	IN	Data Raw: e9 96 2d c3 5c 98 3e d2 44 69 a9 d9 66 07 2b 84 4e 72 4e 8b 0b 23 10 51 26 b1 0f a1 c8 44 73 05 1a 7e d0 ec 38 0c d8 5f 55 9b 2e d2 7f ba 58 02 f9 9e 4a 85 fd b9 e7 c0 ae 94 78 4f eb d1 36 9f b9 8b c5 65 08 72 4d a0 92 30 53 e0 f7 c1 3f ac 7a c1 f4 87 30 d3 82 c7 93 91 22 42 5a ae 4c fe e9 90 c4 d0 49 7c d3 05 7d 5f 6f b2 2e 37 46 b3 da fc bb 9b a6 c9 b9 0c 02 37 ca a6 22 57 54 cf f2 96 6d 2b 31 c4 00 df 3d c7 5f f6 bd 19 18 0b 11 4c 5e 2a 1e 13 16 64 7b 5f 13 da 1b 51 f7 ae 2d d4 03 83 9f df c9 d9 8e e9 ab f8 5a a6 10 76 de 48 2d 62 fe 32 1c 17 62 09 cb e2 5f 4a 58 de 01 1f b1 a3 fe ca c5 a3 0d 8a 8f 06 60 26 be b3 0b c1 2b 00 4c a4 ed 78 7a 89 4f 5f 56 e3 dc 52 32 f7 3f bd b2 c0 53 5a 2f 3a 0b 73 bb 2b 7c f2 88 52 1e c4 a9 79 72 6e da f5 ff 0b 42 61 08 Data Ascii: -\>Dif+NrN#Q&Ds~8_U.XJxO6erM0S?z0"BZLI}_o.7F7"WTm+1=_L^*d{_Q-ZvH-b2b_JX`&+LxzO_VR2?SZ/: s+|RyrnBa
2021-10-13 10:36:37 UTC	80	IN	Data Raw: 2b 8a 3c 7d c1 7d b0 2c fc 89 8b f6 3a 70 aa 76 25 40 61 01 2c 9e a9 51 17 e7 5b 60 22 90 39 a9 49 d5 c0 15 0a 8e 84 d2 11 06 55 87 c6 34 af ee 82 ed ba ca 72 34 ac 42 49 8a 46 6f d2 37 80 bd f3 64 2a 2c a2 78 00 fe 76 cc 0d c5 80 de e6 43 33 da 83 e2 80 a2 32 cf 4e bf b8 f7 e6 45 9e 7d 25 bd 04 94 a4 40 17 16 58 b5 a4 e5 ae aa ab 65 83 f4 0d 28 a1 46 79 86 7b 5c 76 78 67 15 aa a4 23 08 67 88 f9 96 47 8a a9 5a e9 9f 38 34 06 7d 85 b6 46 39 1a ee 53 03 e2 a8 06 9a f1 9b 0b f3 11 ff 14 38 62 a6 1f c5 3b 72 37 59 55 9a d0 dc 1f e3 72 a9 c4 bf a0 db 1f 03 08 f9 ca 14 32 98 5d 39 04 36 73 a6 05 c8 d2 77 91 dd 36 58 9c 11 ff 7d 5c c0 87 a9 0c 1a ff 9e 01 f1 71 c9 6d 25 f4 7c 76 de 7c 6d d1 43 57 3d 07 53 9a 04 60 d2 5b 63 8f 25 7a 69 18 7a b8 f9 52 bf 09 f3 dd Data Ascii: +<}},:pv%@a,Q[`"9lU4r4BIFo7d*,xvC32NE}%@Xe(Fy{\vxg#gGZ84}F9S8b;r7YUr2]96sw6X}\qm%|v|mCW= S`[c%zizR
2021-10-13 10:36:37 UTC	81	IN	Data Raw: 6c 51 17 fe 1f 80 6c 8f 15 3f bb fa b7 63 a4 f6 f2 f4 f7 ee 95 96 79 1b 39 d7 2c 40 c1 d1 94 c6 0a 85 7d 06 81 f2 30 b0 8f 94 54 56 e3 4d 14 3e a6 00 69 f5 9c 4e 50 4e 7c d4 d2 ab 1d 66 f0 98 30 d4 3e 58 c6 aa 75 62 99 ab f8 fa 15 63 e3 00 60 33 49 83 93 2c af 4a 79 e9 1a d2 ad c6 5a 98 88 3d 90 b7 29 15 01 a6 88 fe 43 50 7c 7e 82 84 a6 72 61 ce 82 75 9d 25 7e 3f 7b 9e 5d 71 e3 1c 99 97 92 68 bc 8e 97 c4 d8 36 6c 0b c8 64 91 9b 91 fd 3f 82 90 11 00 5f 93 1f d9 79 a1 1f 79 18 e1 b6 18 5f 91 2c 65 66 ea 99 56 41 7f 0a 7d f4 0b b3 0b 22 89 24 59 a3 68 f6 98 69 37 0a 4b e3 5e 6a ed fa 38 2d a8 d9 26 c2 0f 0b 5b 4d ce e0 2c 94 fe 7c ba 31 89 6a 11 1b 58 6d 11 43 0c 13 20 2f af b5 3e 8b 8d 8c d7 75 80 24 dd 20 b4 e0 35 36 aa 29 f0 30 65 8c 47 5c 68 10 4e 87 c6 Data Ascii: lQl?cy9,@}0TVM>iNPN|f0>Xubc`3l,JyZ=)CP|~rau%~?{]qh6ld?_yy_,efVA}"$Yhi7K^j8-&[M,\|1jXmC />u$ 56)0eG\ hN
2021-10-13 10:36:37 UTC	82	IN	Data Raw: 9d d8 7d f8 02 0c ba 1b 1a 2c 2d 24 00 5b c0 54 90 b6 a0 7c 6d d7 ef 9d 31 55 d1 cd 6e a2 5f 48 28 e1 8c 07 1b 89 08 14 22 a1 b0 1b 42 95 50 f3 c0 37 1f a3 53 c6 03 b2 d1 cd 01 2a e8 ec 77 b3 c1 7e 0b 00 92 90 82 75 0f 2b 75 4b 2b f1 fd 95 21 e5 64 ac d1 b4 e6 2a da 6f 38 a1 da 55 17 79 93 da 9d 3f a6 fc ca 9d 70 c3 04 2f a3 cd 9e b5 73 38 9d 59 d0 0d 1d b7 09 9b b5 7c 26 56 03 bf 84 97 72 d9 b6 7f d6 b3 84 94 38 70 23 c0 fe ad e4 ab 20 64 2c 6a fb 3f c3 da 18 c7 c7 4d 5f 4d a3 13 52 02 8f 34 3d 1a b4 af f9 e7 7b d1 27 50 17 17 b7 71 43 8a 57 be e4 db 4a ad bf b3 e5 f2 1c 25 46 7e 85 02 60 74 7d e6 4b 6c d8 23 2c 2a d9 53 ba 41 b2 87 a9 6e bc 74 e8 56 8b cf 66 55 5f 7f 2e 79 1d 6d fb 2c 8e 24 22 1c c0 ac 1b a6 24 f2 86 ef d2 5c bc e7 a4 70 28 d6 8a 68 5b Data Ascii: },-$[T|m1Un_H("BP7S*w~u+uK+!d*o8Uy?p/s8Y|&Vr8p# d,j?M_MR4={'PqCWJ%F~`t}Kl#,*SAntVfU_.ym, $"$\p(h[
2021-10-13 10:36:37 UTC	83	IN	Data Raw: 84 f2 c1 f6 7a 2a 6c b4 bc 64 5c af 35 13 60 b7 2b d3 60 c3 b2 50 f4 76 72 5d db 32 8a ee 24 30 e7 e9 7e 75 93 51 62 2c 31 a2 08 66 a7 90 17 a3 02 02 b6 6f 33 b2 43 85 d2 66 60 91 35 c8 fe 0b 13 0e 18 09 dc 4a 0f 0f 69 9f b9 57 74 3d c7 b9 a9 f4 bb 0d c7 56 cd 83 d7 7c d5 8c 1a a0 ec 20 c1 f4 b5 41 48 ab 38 3d 6f 36 0a 60 c7 5c 43 cf 4e 98 12 34 01 5c 6e 05 72 1c 65 0a 68 ac bf 5b 18 df 79 7e ba e2 7b f9 b9 5a 33 1b 4f 0c 0b 97 37 c7 b2 40 24 99 8d 3b b8 2f cf 9b 35 ce a0 0f 36 90 df ff bd 91 5b 5c 3b ec d9 c5 32 e5 91 81 7f 72 0e f6 b1 92 7b 04 cc ce fd 74 05 9e 3f b2 10 3f be 5b 8a d9 27 d9 f4 cd 18 43 33 33 79 fc 08 ba b4 99 93 47 c3 d5 e5 79 59 e9 b8 80 40 ba 1a 74 81 9b 1a d4 4f 0c 65 c5 70 66 19 28 bd 16 7e 9f 65 a7 2c 2d 7e 76 49 ac 35 56 7d 9f 37 Data Ascii: z*ld\5`+`Pvr]2$0~uQb,1fo3Cf`5JiWt=V\| AH8=o6`\CN4\nreh[y~{Z3O7@$;/56[\;2r{t??['C33yGyY@tOepf(~e,-~v I5V}7
2021-10-13 10:36:37 UTC	84	IN	Data Raw: 8e 24 2d b1 44 e3 a6 06 25 1f 7c d3 54 69 fa f4 1f 31 a5 da 0e c2 2e 2b 7e 2f c8 f1 3d cb d9 60 bb 39 b7 7d 1f 0f 75 7c 37 72 32 7a 8f c4 1e 56 bf 75 44 b9 ea 1c a0 12 fb 1c e4 e1 04 1a 9e 13 d9 12 4e bc 48 6a 47 27 7f aa f6 22 e2 16 20 c8 0e 73 01 0f 47 50 fb f0 5b d9 bd 22 3e 57 23 79 c3 39 62 72 40 b6 a0 03 cc 7b 90 c6 c4 ef 5a 83 cd fb 4a c6 06 82 50 fa df 7c 65 ff 29 04 5f e9 43 99 09 d4 b4 76 61 ed f1 e5 75 71 14 1f ab 50 c2 cf ef ed ea 22 19 51 d9 21 3c 66 32 1c 83 5c e2 c8 86 ae 2a b9 f3 09 65 d3 15 11 74 ea e8 ad 9f 72 5b 0e eb a6 c7 d4 46 fe 26 68 cd c0 a1 41 ce 1c 56 6b 69 8f f5 30 76 6f 18 78 d0 dc ca ca de 11 e7 4f 4c 43 f6 21 14 a7 16 28 34 33 08 61 cb 89 5b 46 12 86 a8 fb 25 bc dc 2e e8 ab 6e 5e 72 57 e9 e8 04 d1 6e 9b 32 34 8a f7 6e 9c 81 Data Ascii: $-D%|Ti1.+~/=`9}u|7r2zVuDNHjG'" sGP[">W#y9br@{ZJP|e)_CvauqP"Q!<f2*etr[F&hAVki0voxOLC!(4 3a[F%.n^rWn24n
2021-10-13 10:36:37 UTC	86	IN	Data Raw: 62 17 39 f0 1e 7f 8e 56 f7 0d 3b 6e 67 5f b2 55 74 7f 97 47 85 99 a3 40 8d 4e cf fa 89 a5 e8 dc a5 d8 bd 3e 41 3e a3 ba ab 03 b4 9e f5 70 8c 2f 6d be 1c 1d 2c 35 29 00 65 d5 4a 91 b2 a8 0b 3e 8d ea f1 0d 27 cb ca 6e b3 18 1f 62 c1 81 1f 7a ca 3d 08 26 96 ef 40 1c 93 53 fe b2 3d 2f a6 4b cb 2d b5 df e0 74 3c e3 da 6f b7 d4 50 1f 0e bf e5 bd 74 27 26 01 79 52 d1 cc b3 05 bf 59 ac f9 d5 e1 2e ae 60 19 ab d3 45 06 64 a3 c2 b9 2c c9 cb d7 87 6f db 51 02 bc d1 85 b3 79 37 e9 7a d4 0d 23 c2 1f 96 c1 6e 43 43 3d ab 9a 94 15 d9 bb 78 e0 98 8e 92 3e 7d 0a fc ea af 80 99 28 08 24 4a ec 22 d4 d7 1c a5 80 fb 91 da 74 8f 9d d0 b3 24 58 1a b9 ae e8 e3 7b ff 23 5a 0f 29 b7 63 42 86 4b a4 c4 81 7f ad b0 bb 97 d6 1a 48 64 65 9f 23 7b 75 77 e1 52 42 da 19 1a 1c f1 4b 9d 4d Data Ascii: b9V;ng_UtG@N>A>p/m,5)eJ>'nbz=&@S=/K-t<oPt'&yRY.`Ed,oQy7z#nCC=x>}($J"t$X{#Z)cBKHde#{uwRBKM

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	87	IN	Data Raw: 3f 80 94 4b 42 69 48 ed e9 22 cc 03 a9 10 32 9a e5 73 bf 98 fb 65 f1 7c a7 7a 06 2e d7 77 eb 6a 41 59 71 19 fb b5 ed 1e f3 07 e6 89 d4 c7 da 6b 2f 65 d0 8b 63 32 88 2c 1b 66 8a 33 cf 43 e4 bf 5a f5 68 17 2e f9 39 9a df 2f 40 c0 da 6a 7c 9b 6b 03 10 30 bd 02 13 87 96 11 9a 02 02 b0 64 33 c0 05 bf db 71 16 bb 39 c3 dd 0b 16 05 6c 37 d8 50 31 3f 65 83 dd 6c 6c 27 dd b4 a0 f6 de 2f b5 72 cb 9f e8 60 e5 82 11 b6 83 1c f7 f9 80 42 4a cc 3a 2a 5e 1f 21 6f de 78 31 db 58 a9 3b 17 06 44 43 2a 7d 15 6c 6f 7d c9 98 7d 26 ca 7f 7b fd cf 71 d3 bd 73 39 76 26 2a 10 bf 2b cb b3 40 38 ed aa 10 ac 1e dc fc 2f c0 98 1a 46 92 c8 8b a1 ab 7a 68 2b ee c1 de 20 ed 86 81 5f 72 0e ed 92 8b 72 0f e3 db f5 57 6a 8b 1c b3 21 3d ba 42 ab d6 1a d3 9d d0 09 52 1e 52 4b e5 32 98 b6 92 Data Ascii: ?KBiH"2se|z.wjAYqk/ec2,f3CZh.9/@j|k0d3q9l7P1?ell'/r`BJ:*^!ox1X;DC*}lo}}&{qs9v&*+@8/Fzh+ _rrWj!=BRRK2
2021-10-13 10:36:37 UTC	88	IN	Data Raw: 0c 25 6c 72 92 2f 4c 6f 73 f2 4c 42 e9 2f 2b 00 f0 5a 99 44 a4 9c b9 6e af 6d ea 4d 81 a2 48 78 43 71 31 7d 1d 7a ab 11 91 22 50 9b 35 42 8e 4e a4 99 08 3e 0e 58 d9 55 60 f1 e3 28 34 ab c7 3c b6 15 29 72 23 fc e6 3b ae eb 60 c8 3b bf 6b 2c 25 44 7a 27 74 33 60 ff f5 0f 50 a5 64 42 a2 fb 10 b1 14 8f 3e 81 c0 29 02 8d 0f dd 1b 5f 88 7c 70 4a 21 78 b0 99 0b d7 0d 19 d4 15 75 32 2a 57 56 ec ea 4a ac 84 26 57 7d 0e 7c c0 38 46 75 47 c4 ae 04 cd 50 b4 b2 f3 e1 54 9b c9 f2 45 c6 1c ed 59 cd ce 4f 49 fe 0c 1f 55 f3 40 8f 26 d4 b3 04 7b ea f0 ce 51 03 32 19 b5 50 c1 d9 f0 94 ff 28 1f 46 d8 31 48 40 23 1c ae 51 e9 ce 93 a9 46 9d e4 32 6f cd 03 0e 0d da e2 a9 b9 64 5b 1a e2 b0 ea c5 56 c4 20 79 cc c7 c4 0a fb 04 57 0a 5b a5 e2 3b 64 16 b6 b3 19 d4 6f 1a 8d 11 82 1d Data Ascii: %lr/LosLB/+ZDnmMHxCq1}z"P5BN>XU`(4<)r#;`;k,%Dz't3`PdB>)_|pJ!xu2*WVJ&W}|8FuGPTEYOIU@&{Q2P (F1H@#QF2od[V yW[;do
2021-10-13 10:36:37 UTC	89	IN	Data Raw: 0b 3f b7 2b a3 dd 3e e3 a0 d1 19 56 15 52 40 e2 2f af b0 9d ff 49 dc c4 fb 5e 58 ed b3 ce 75 b8 3e 06 80 9f 17 8b 59 10 70 ce 7f 75 06 2c c4 71 7c 8e 4e a8 17 31 4f 76 5b bb 02 37 63 9f 43 b5 b5 a9 4a 80 03 c7 fb 98 96 a3 ea a5 ab ba 3e 58 4f a6 ba a6 2d ba 8d f9 7d f8 06 5f bf 1b 15 28 20 45 4f 7e d5 56 ac a2 a6 73 69 da 8e d0 00 57 e8 d0 79 b5 5e 4c 20 ee 88 0a 7a ca 20 1f 22 83 b5 1c 41 bc 5a eb b2 03 29 ad 44 c2 70 a2 f8 e9 0d 5e c2 eb 64 be d0 0a 32 0f a3 8a 84 69 00 2f 78 2a 69 e1 ca af 18 e5 45 a4 e6 a1 e0 24 a3 74 2f b7 b0 62 11 6a be c8 9d 2c df f4 dd 9d 00 fe 35 24 bd cb 98 a7 6f 30 8c 64 b1 2a 05 c4 19 9f ac 33 75 52 01 ab 9a 91 61 d3 f0 4f cd a4 90 87 33 76 1d ce e9 ab f9 df 26 01 35 46 d9 23 c2 d3 1c c7 ab e7 e5 c5 64 90 99 d6 ad 3b 44 49 8f Data Ascii: ?+>VR@/I^Xu>Ypu,q|N1Ov[7cCJ>XO-}_(EO~VsiWy^L z "AZ)Dp^d2i/x*iE$t/bj,5$o0d*3uRaO3v&5F#d;DI
2021-10-13 10:36:37 UTC	91	IN	Data Raw: 23 aa ad 0a d3 5c 68 fd aa cf c3 e8 1c 3e 7b 21 ab be 0e 84 a9 f2 3b 80 e0 1d f3 51 95 c7 ef fd 17 4d f5 95 a5 51 02 1b 47 2d 3d c8 2d 4a f4 8f bb ed 20 55 ce be cc 5a b4 db 63 43 b3 3a 42 46 82 b0 ce 64 c3 c0 9b 00 c1 32 e2 ba 36 e8 cf 22 0b 13 fd 19 f0 7b 5f 07 78 11 1e 14 cc 2e 2b 82 dd 64 e1 a6 8c e3 96 3a ea 34 6e ed 0a cf 93 bf 07 dd fe 76 fa 85 31 75 b3 df 70 df 8f 42 8e 66 a1 d7 2b 62 be 7d a5 e0 d1 d5 e3 6d 9a 3c 1d e9 dc 68 9c 2a 8d bb e0 a7 ab 91 12 b8 bf e7 bd 37 51 38 51 81 0c 7d 15 3f 54 e2 08 ff 22 e6 45 bc 3e 2c da 2b 3c ea 7d 3f 71 eb a1 ab 89 ed ce d0 88 87 eb ed cf bc fc 7d 9f ed b8 96 c9 dc c7 fd 00 e5 b0 74 02 a6 b3 0d b4 d0 4c 58 92 b7 00 be b9 a5 a5 b5 dc 3d e4 1f 0b a9 4a 02 41 c4 04 fa 78 49 94 10 70 b2 ba f7 53 03 7d 3d a8 aa 9b Data Ascii: #\h>{!;QMQG-=-J UZcC:BFd26"{_x.+d:4nv1upBf+b}m<h*7Q8Q}?T"E>,+<}?q}tLX=JAxIpS}=
2021-10-13 10:36:37 UTC	92	IN	Data Raw: a6 25 bd 22 2a 71 7e 6f 75 79 30 d4 68 02 00 60 ba ae d5 cd 33 32 3f f5 46 e7 e1 df 94 6d af da 70 a4 d0 4c 56 d3 71 06 4a ed 5d e3 25 e2 9f 79 9f b0 ba d7 32 f9 d8 48 d6 5f 9a 0b 7d 3d a1 2e 51 77 a8 61 18 40 93 3a 6d f3 98 fe be 95 84 6f c5 19 b1 5e fa f2 7f ad bd 50 e9 38 d4 b7 e4 9c aa 0b a9 d9 35 40 f7 58 25 0b f2 75 f9 89 b4 a2 02 38 8f 57 98 69 10 d0 0d 9c ab ea e9 85 44 d8 e9 c6 7b 76 e8 02 09 a9 30 22 27 c8 08 f4 46 d7 3f 17 b2 ea ff a6 34 ab 9f 3e bd b1 c6 fb b6 1b 04 4c 5d c6 f4 63 ee da c2 a1 8c 99 51 04 39 43 76 fa e9 98 94 94 e4 97 be 06 fb 6f 1b c0 7d a5 23 73 5a 1d 37 1c 1b 2a c0 0a cb 36 b2 47 05 ad d9 1a 48 9f 89 3b fc 7c 83 04 2f bb b5 65 17 0f 10 af e1 a5 5f f6 1b 42 3c 29 50 c3 e8 35 63 d0 84 a1 98 ff dc e2 1e bd 1b 43 ad 17 3f c7 db Data Ascii: %"*q~ouy0h`32?FmpLVqJ]%y2H_}=.Qwa@:mo^P85@X%u8WiD{v0'"F?4>L]cQ9Cvo}#sZ7*6GH;|/e_B<)P5cC?
2021-10-13 10:36:37 UTC	93	IN	Data Raw: 52 bf bb 6a 7b c7 13 c4 12 1b e5 f3 71 78 20 e2 08 87 cd df 6f 0a 36 90 21 36 2a 18 f8 c5 14 27 62 f8 d7 3f 40 2f ac c7 52 5a 1e ec 94 6a c0 4e 03 01 7f 5f be a3 8e b4 cf d4 3a a9 64 64 3f 38 20 49 1e 07 c3 95 31 a3 21 9e 6a b0 df f2 11 d1 36 c2 e2 ef 08 83 e8 cb f0 72 da 1b 0d bb 76 8e e4 f2 ac 87 03 d1 db 80 56 37 05 48 7b f4 46 ec 1f 23 b6 26 56 22 dc 73 45 2f 72 dc 79 30 61 80 f9 2f 3f f3 33 de e7 72 dd 98 d2 b6 fb ad 0e 9d f2 6c 38 7b 85 d8 1a 61 23 cc 27 7c 12 ce 66 ff b1 96 1a 02 cd d7 89 a0 ce eb 2e 6e b1 9b 12 8a 23 78 fe 5b 0b 85 48 bc 6c 6a 3b ae e1 4a 05 16 2b 30 d2 b5 f3 3c 5a 4b c7 f4 98 ac 2a cd 11 16 0f fd 5b a5 14 2c 33 21 e5 da fa fe 0b 31 df cb b0 32 0e 58 97 08 bf 57 5b bd 62 ea ae 6c 02 3b 6b da f5 e9 d3 07 ae e0 7d fe c1 0f b3 26 60 Data Ascii: Rj{qx o6!6*"b?@/RZjN_:dd?8 I1!j6rvV7H{F#&V"sE/ry0a/?3rl8{a#'|f.n#x[Hlj;J+0<ZK*[,3!12XW[bl;k}&`
2021-10-13 10:36:37 UTC	95	IN	Data Raw: f0 cc 35 65 eb a7 98 fb 8b 51 85 50 1e 1a 6b 90 f8 55 fe ef 01 ca 37 e4 21 00 0e 5c 00 58 ad 3d 31 3f 23 e9 24 9c b0 b8 5b 7b fc 4e db 76 e5 bb 73 54 f8 17 41 96 9e 4b 11 1e 7a 09 8e 08 f4 0d 7a 66 fd fa bf b9 f2 9c d6 de 11 4e 60 9b eb f6 5e 06 31 a8 76 15 9e 53 f9 f4 8f bb d1 3b 30 a8 01 be bc 8d fb e3 7a b8 4d 2d 18 66 75 91 1e ae 74 9a 3e d6 28 ea 90 fd b4 ae 24 d0 f2 5c 86 ab 18 3f 01 a0 54 af a9 b6 09 28 9d ed 44 83 c5 05 2f d2 7d a1 4e 67 ed 2a c5 ac 5d 47 db 11 05 e0 86 0e ec ed a9 42 19 db e1 be 52 d5 b9 6a d8 9b 68 de 6c 04 ba 86 1c c3 60 85 ec df 6f 5a 7c 32 bf dc 3c 5a 95 06 83 50 bb a0 41 18 9f c8 dd fc 2f 7a 2c bb 8b 01 ee 1f 33 0d 5a 6d 5a c9 c4 6c e8 2f 55 7c c2 92 16 08 b7 a4 d4 44 c8 03 da fa 3f e0 48 2e 9d d7 8d 0b 87 a2 9a 9c b2 d3 63 Data Ascii: 5eQPkU7!\X=1?#$[{NvsTAKzzfN`^1vS;0zM-fut>($\?T(D/}Ng*]GBRjhl`oZ|2<ZPA/z,3ZmZl/U|D?H.c
2021-10-13 10:36:37 UTC	96	IN	Data Raw: ec 41 01 30 34 5e d0 c4 06 a2 0c 96 c3 0a 6d 36 66 f2 99 8a b0 41 07 47 a8 45 61 b1 bf 19 73 1c e3 ac a6 0d 76 7c 3d 30 fe d9 41 cb 02 bb 3b 0d 93 00 63 71 5a 35 fe 43 50 bf 9d 92 a9 a5 5d 70 62 3d ab 10 db 82 7b ae 47 fd 88 5e d7 6e 3a 1a b2 75 3e 69 2a 9b 90 9a b6 f1 67 f1 ea b2 a3 6f 80 ff 61 f5 e2 5f 68 99 13 b8 5a 38 7e 81 42 a5 6b 86 55 cf ca aa ab d2 f0 f3 e5 b2 44 e1 5c a8 9d 47 41 f9 45 e5 28 3b d6 ed 80 80 01 d7 ba 22 97 84 e7 77 77 dd 59 e5 e4 f8 f2 00 6a e7 76 98 d7 4a 98 49 f0 cc cb de a6 f9 fe ff ae ff 82 b9 8f 3e 8b 8d 22 27 c8 2d d8 32 79 0b 0b d7 93 6a fe 6a d8 10 1a b0 1f ef de c7 71 46 ed 56 ec ca 64 c4 16 ba c9 f8 80 40 30 ff 36 0b f9 3e d8 ed c3 0c 92 80 d9 95 06 77 61 7a aa 17 63 23 6f 88 4e ee 53 95 b2 b1 59 18 66 13 c8 98 43 f6 70 Data Ascii: A04^m6fAGEasv|=0A;cqZ5CP]pb={G^n:u>i*goa_hZ8~BkUD\GAE(;"wwYjvJI>'"-2yjjqFVd@06>wazc#oNSYfCp
2021-10-13 10:36:37 UTC	97	IN	Data Raw: 44 72 aa 0a 43 8e 2b ec 44 33 68 46 0b 3b 13 1c 00 0a 00 88 cb 72 55 ce 1a 62 d3 ef 1e 84 d8 05 56 1b 05 28 7f a4 5b d2 df 50 4a 9d fe 1d c1 7b bd bd 7b d9 cd 19 36 94 ba e3 e2 bb 08 7e 4e b3 b5 b9 53 88 e5 c0 18 41 7a fa f7 be 17 26 82 e2 90 56 05 ab 5a c6 40 1f ce 5d c4 cf 4a d5 f4 d0 7d 0e 6c 67 09 8c 57 9a d9 8a 93 57 a6 d4 ba 5c 2a e8 ca fd 21 e5 7f 74 ff bc 6e e7 1a 1e 00 d4 3e 6c 74 29 bd 71 0a a9 3a 9b 5e 23 1d 70 3a b4 7b 5e 10 99 37 8f f7 c6 3f ba 03 c6 9e 85 c9 89 8f b8 ab a4 5b 45 10 83 df df 3c ba ff fa 1c e5 63 6d ca 0c 5e 29 59 2c 00 7a b0 38 f2 94 c4 5e 0c ca 8e f3 61 42 be cd 0b c1 3a 6e 4c c3 ed 1a 7a e7 4f 14 56 96 dc 41 32 c5 3f 92 bf 10 5b ae 27 c6 03 a6 b3 b5 74 6b 80 a8 07 84 a0 12 7b 03 d3 92 f6 24 4b 7f 01 49 2b c4 b8 d6 67 d2 01 Data Ascii: DrC+D3hF;rUbV([PJ{{6~NSAz&VZ@J}lgWW*!tn>lt)q:^#p:{^7?[E<cm^)Y,z8^aB:nLzOVA2?['tk{$KI+g
2021-10-13 10:36:37 UTC	98	IN	Data Raw: 03 15 b2 44 ec f8 03 25 d2 1f a6 8d 6b 32 6b 77 7a d6 3e 3c 58 69 f1 ab 38 66 6e b3 cf 88 91 cb 5d d3 39 da e6 d6 0f e3 e5 0d c4 83 46 dc 80 ff 2d 1f ab 2c 58 78 69 25 01 c4 39 34 bc 2b fd 03 72 29 30 5d 4b 52 71 50 0a 5c c9 9d 04 16 be 1a 07 9d 8c 5f b7 8e 37 17 1b 58 69 28 d2 68 a2 ed 25 4a e2 b0 79 80 7b f8 fc 37 af 98 6a 05 f7 88 8b e2 d5 46 1a 2f 80 c3 8b 3d 88 80 81 18 18 34 a9 b6 e7 41 68 d0 af c5 11 4b f9 08 c6 4f 53 80 2b a5 b8 3c bc 83 be 4e 37 5e 52 09 81 08 db b8 fc e5 20 d1 a1 d4 2c 5e 8c ca df 6f d7 1a 74 9d fe 39 8b 7b 7f 74 b7 5d 07 1c 4d bd 7e 55 eb 73 f7 0d 42 4e 13 7f df 29 37 46 fa 37 e1 b9 c6 47 f9 70 a0 eb ec a4 e8 8f d7 e5 c9 36 2c 71 ed b6 df 43 f9 ff 93 52 8c 0c 0c b8 79 33 4d 30 45 73 0e c4 38 ff da 8a 38 43 a3 dc 9d 35 27 f1 b9 Data Ascii: D%k2kwz><Xi8fn]9F-,Xxi%94+r)0]KRqP_7Xi(h%Jy{7jF/=4AhKOS+<N7^R ,^ot9{t]M~UsBN)7F7Gp6,qCR y3M0Es88C5'

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	99	IN	Data Raw: de f6 75 ad 67 fd 79 90 b4 05 77 91 7d e7 75 4a d8 78 1f 29 55 65 c3 f6 4c c0 79 3d a6 15 16 1d 4e 52 24 ff 99 39 bd aa 47 5d 11 3c 18 c1 4a 57 06 59 c4 ae 61 cb 0f f5 d7 e4 80 54 f3 c1 97 5d b2 1b ed 53 a8 dd 10 76 87 48 7f 57 86 5b ea 29 a0 a4 04 65 8f ed 91 7e 71 55 7d b9 35 d9 ad e0 94 df 50 18 35 d8 42 2d 27 34 68 f1 3e e1 bd 84 cb 4d f8 ee 7a 74 be 77 72 6c a9 f1 dd 81 00 47 69 e2 d2 f4 a0 56 8c 4f 1b d9 b4 b2 41 f0 7d 4b 0a 70 ce ee 42 71 16 20 0c a4 a3 c2 a8 dd 65 f1 4f 6e 30 e4 44 17 c5 7a 40 10 5c 10 11 cb e7 50 07 02 f2 bd 92 32 c9 c1 4b e8 e8 75 30 69 3e e0 8d 74 be 31 eb 38 40 91 95 69 f0 e8 8f 65 b0 7f c0 71 74 74 a3 2d 86 51 33 43 07 19 9f d0 8e 7d a0 1f 94 81 ba cd 98 6d 46 6a b4 8f 11 5c db 5c 6f 66 e3 3e a3 64 8b be 3e c4 1a 65 5d fd 57 Data Ascii: ugyw}uJx)UeLy=NR$9G]<JWYaT]SvHW()e~qU}5P5B-'4h>MztwrlGiVOA}KpBq eOn0Dz@\P2Ku0i>t18@ieqtt-Q3C}mFj\\of>d>e]W
2021-10-13 10:36:37 UTC	100	IN	Data Raw: 5e 4a 79 45 2f 0e 90 38 ff c4 bf 38 3c a3 b4 9d 07 27 8c b9 76 c1 0b 2d 0b a5 af 73 7a 9c 3a 71 25 e2 b9 72 40 f7 12 92 d3 53 3c c2 42 a7 6d d1 c7 8c 75 de 0b e5 16 a8 a0 04 7b 0b d3 89 f6 71 4b 2b 01 05 2b 96 b8 f8 68 a1 01 e1 95 fd 92 28 da 50 4a a3 b0 40 74 6c d7 cf e9 37 a6 dd b8 88 00 d2 51 7a d3 9f f1 8c 16 08 e9 54 b1 3c 7c 97 6d cc c1 33 26 07 62 e5 e8 d8 15 fd de 65 bf b3 e0 97 5c 7e 6f d8 99 b0 80 ff 41 2a 41 4d 98 70 b1 83 71 8b c7 ac e5 b3 11 dc ed 91 dd 19 3d 0c cd 88 8d a2 16 bc 64 73 7b 29 d2 23 37 cd 38 e0 97 db 0d fb d1 e1 97 ab 7f 10 0b 2c e6 59 0f 07 27 e8 3f 36 8e 3e 5f 2f b8 05 f8 0f c1 c1 ca 0d fd 70 84 5c e8 ac 2d 5b 26 74 41 68 6f 27 ab 3a e1 3e 22 94 41 49 fc 53 a4 a7 69 7e 6f 50 bc 4a 05 f8 97 44 58 ca c5 73 b6 32 59 63 4d d0 85 Data Ascii: ^JyE/88<'v-sz:q%r@S<Bmu{qK++h(PJ@tl7QzT<|m3&be\~oA*AMpq=ds{)#78,Y'?6>_/p\-[&tAho':>"AISi ~oPJDXs2YcM
2021-10-13 10:36:37 UTC	102	IN	Data Raw: ee 79 32 b4 5c 0a 05 c3 52 ef 05 e4 d3 59 90 69 17 7d 9c 1e fe fe 5d 60 82 82 0c 3a fe 18 18 11 55 ad 6d 14 f5 90 74 b2 63 02 d1 70 56 da 05 83 be 77 60 f2 5a da 8d 44 7f 6b 5f 5a b9 42 50 78 00 a2 dd 56 03 0f b3 ab c5 f4 bb 7d b5 72 ae 83 a4 76 82 89 74 ab 83 30 92 e7 cc 48 2d d9 5f 55 1b 63 44 0c aa 33 43 ef 2b 8f 4d 00 68 55 0b 2e 13 1f 00 79 0f a1 cb 6b 55 ca 1a 36 d3 f0 1e 97 d8 37 5d 50 08 39 7f f2 5b de df 05 4a ed 8f 74 c1 71 ae f1 7b a5 cd 67 36 fd ba a6 e2 f3 08 37 4e ad b5 a6 53 a5 f4 ac 18 3a 7a 84 f7 ca 17 45 82 82 90 3c 05 d4 5a eb 4f 73 ce 06 c4 95 4a 91 f4 93 7d 1a 6c 7f 09 a1 46 f6 d9 d1 93 0d a6 8c ba 01 2a a1 ca e3 21 fa 7f 59 f2 d3 6e a6 1a 52 00 9a 3e 2a 74 60 bd 5c 1b c6 3a da 5e 6f 1d 3e 3a f2 7b 1a 10 d7 37 c7 f7 eb 2e d4 03 8d 9e Data Ascii: y2\RYi}]`:UmtcpVw`ZDk_ZBPxV}rvt0H-_UcD3C+MhU.ykU67]P9[Jtq{g67NS:zE<ZOsJ}lF*!YnR>*t`\:^o>:{7.
2021-10-13 10:36:37 UTC	103	IN	Data Raw: 50 4f 3f da 38 64 9f fe 6b 34 ca d1 4f d2 5a 79 17 3a bd ec 58 bf 98 7b c8 7c da 6c 73 02 31 78 44 65 40 66 ff c3 77 19 d1 57 30 a2 98 11 c2 02 8f 43 e4 cf 6a 47 ff 00 b8 75 ab 59 4c 1f 6a 44 79 c3 e0 4c c2 79 3d a6 54 16 31 4e 70 24 fb 99 40 ac b9 47 4a 11 00 18 d4 4a 46 06 5a c4 88 61 d5 0f 92 c6 e8 80 45 f3 cd 97 5f b2 07 ed 53 a8 ea 10 76 87 27 70 40 86 44 ea 2c a0 a5 04 7a 8f ac 91 39 71 75 6c be 35 ce ad ea 94 d6 50 13 35 c8 42 68 27 31 68 98 35 f4 bd 9a cb 0a f8 f3 7a 74 be 16 7d 79 a9 f2 dd 95 00 12 69 e0 d2 e9 a0 56 8c 2a 0a 82 b4 bf 41 ae 7d 59 0a 04 4e 76 00 17 55 59 7e a4 d7 a3 d8 ab 11 82 61 0d 72 85 07 79 b7 7a 28 77 2c 65 65 aa b4 22 62 66 86 da d3 47 a5 a8 2c e8 96 1b 42 06 57 84 f9 47 d6 03 86 53 10 e3 e7 07 9f e8 ee 0b d5 10 b2 15 00 47 Data Ascii: PO?8dk4OZy:X{|ls1xDe@fwW0CjGuYLjDyLy=T1Np$@GJJFZaE_Sv'p@D,z9qul5P5Bh'1h5zt}yiV*A}YNvUY~aryz(w,ee"bfG,BWGSG
2021-10-13 10:36:37 UTC	104	IN	Data Raw: f7 6c 42 5c 13 0c df 4d 37 27 fa 01 ea f7 46 db aa 03 cf 9e 8a c9 9c 8f ab ab a8 5b 5e 10 88 df 83 2d b4 ff f5 1c ef 63 7e ca 16 5e 3e 59 2a 00 68 b0 4c ff 8b c4 6f 0c ca 8e f3 61 43 be d6 0b b6 2b 5e 4c 85 ed 3d 7a dd 4f 2d 56 a1 dc 07 32 85 3f e0 b2 36 5b ac 27 d3 03 87 b3 e9 74 2c 80 db 16 ae a0 11 7b 0c d3 b9 f6 4a 4b 23 01 44 2b c6 b8 b9 68 e6 01 b2 95 f5 92 06 da 5a 4a bd b0 43 74 6c d7 dc e9 37 a6 d1 b8 83 00 97 51 12 d3 ca f1 a3 16 28 e9 64 b1 0a 7c c3 6d 9f c1 70 26 6b 62 8e e8 8a 15 c5 de 6a bf b4 e0 9f 5c 74 6f dc 99 9f 80 90 41 11 41 6d 98 3c b1 d9 71 ca c7 f5 e5 d4 11 c5 ed 8c dd 60 3d 7c cd 9f 8d c4 16 b9 64 0f 7b 4f d2 23 37 d0 38 e1 97 c4 0d f9 d1 b2 97 a8 7f 67 0b 2f e6 48 0f 46 12 b0 3f 72 8e 7b 5f 6f b8 0b f8 62 c1 dc ca 2f fd 2e 84 0f Data Ascii: lB\M7'F[^-c~^>Y*hLoaC+^L=zO-V2?6['t,{JK#D+hZJCtl7Q(d|mp&kbj\toAAm<q`=|d{O#78g/HF?r{_ob/.
2021-10-13 10:36:37 UTC	105	IN	Data Raw: d1 47 f2 03 84 53 27 e3 fc 07 9e e8 be 0b f4 10 a1 15 00 47 c2 1f 86 37 5f 36 68 70 f8 d0 f6 1e ce 73 e7 e0 ba b5 f7 1e 34 09 dd ee 76 32 b2 5c 10 05 bc 52 d6 05 f9 d3 52 90 1a 0a 28 9c 24 fe df 5d 32 82 c1 0c 7b fe 74 03 27 55 91 6d 10 f5 94 74 bb 63 19 d1 66 56 b2 18 9c be 62 60 a1 5a d5 8d 13 7f 04 18 08 b9 5a 50 07 00 87 dd 59 03 02 b3 b5 c5 f4 bb 5d c8 34 ae ec a4 22 82 c8 74 e9 83 7a 92 ad cc 00 2d 86 5f 75 1b 49 44 52 aa 57 43 dd 2b 87 4d 17 68 10 0b 00 13 14 00 73 0f a5 cb 6b 55 d9 1a 71 d3 e9 1e c5 d8 17 56 36 08 44 7f ff 5b 8f df 08 4a c0 fe 54 c1 56 ae f1 7b a5 cd 2c 36 98 ba fe e2 b0 08 7e 4e a0 b5 cd 53 fa f4 ee 18 7a 7a 93 f7 c7 17 23 82 c6 90 7f 05 83 5a a7 4f 53 ce 21 c4 f0 4a d3 f4 cd 7d 43 6c 68 09 ac 46 da d6 f1 93 2a a6 f4 ba 7f 2a de Data Ascii: GS'G7_6hps4v2\RR($]2{t'UmtcfVb`ZZPY]4"tz-_uIDRWC+MhskUqV6D[JTV{,6~NSzz#ZOS!J}ClhF**
2021-10-13 10:36:37 UTC	107	IN	Data Raw: 32 80 7b 42 ef 4a 2b 5f d9 3f a4 20 85 ee af 6e 9b 18 e5 39 9d cf 41 30 52 1d 1d 18 23 09 c4 5e 86 47 4b fa 2f 2d dc 3d e0 d4 08 50 1b 3f dd 38 05 1f 10 66 58 c0 b4 62 b6 77 59 3a 4d 90 85 75 cb b5 13 e5 5c f7 1f 53 76 62 19 2a 11 21 13 94 b0 12 39 f1 34 7b cd fd 75 bb 67 e3 79 8b b4 0d 77 98 7d dd 75 59 d8 2e 1f 04 44 26 c3 b4 4c 9f 79 64 a6 57 16 5e 4e 1e 24 84 99 33 ac 8f 47 51 11 3a 18 ca 4a 47 06 14 c4 8f 61 cb 0f 9a c6 ea 80 0d f3 84 97 69 b2 03 ed 5f a8 d9 10 6f 87 68 70 7e 86 4c ea 3f a0 ab 04 05 8f 8e 91 58 71 3a 6c ab 35 db ad b9 94 9a 50 77 66 f0 42 7f 27 15 68 85 35 e1 bd 80 cb 76 f8 b7 7a 53 be 03 7d 6c a9 f5 dd ba 00 67 69 f0 d2 e3 a0 40 8c 6f 0a fc b4 a5 41 ea 7d 45 0a 58 ce c3 42 72 16 3f 0c c5 ae d6 a8 c7 65 f6 4f 51 30 c9 44 16 c5 1d 51 Data Ascii: 2{BJ+_? n9A0R#^GK/-=P?8fXbwY:Mu\Svb*!94{ugyw}uY.D&LydW^N$3GQ:JGai_ohp~L?Xq:l5PwfB'h5vzS} lgi@oA}EXBr?eOQ0DQ
2021-10-13 10:36:37 UTC	108	IN	Data Raw: f4 93 7d 1a 6c 7f 09 a1 46 f6 d9 d1 93 0d a6 ac ba 26 2a ca ca a1 21 a2 7f 1a f2 9a 6e ab 1a 39 00 c5 3e 68 74 20 bd 4b 1b cb 3a b0 5e 2d 1d 7c 3a b8 7b 5b 10 9f 37 ca f7 85 2e 91 03 d2 9e 83 c9 85 8f b9 ab c4 5b 26 10 a5 df b0 2d 8a ff e8 1c b6 63 2c ca 78 09 11 59 06 00 61 b0 57 ff a0 c4 57 0c cd 8e c1 61 64 be d6 0b ae 2b 5a 4c ca ed 1d 7a d5 4f 24 56 91 dc 17 32 85 3f b2 b2 17 5b a3 27 d3 03 b0 b3 d0 74 1a 80 cd 16 a1 a0 1f 7b 17 d3 89 f6 69 4b 16 01 66 2b cd b8 b1 68 f8 01 af 95 f5 92 0f da 5e 4a ba b0 51 74 0d a8 b6 e9 54 a6 92 b8 c9 00 9a 51 6c d3 92 f1 ec 16 76 e9 30 b1 59 7c e4 6d 94 c1 7c 26 5c 62 bb e8 d8 15 e1 de 69 bf a4 e0 9f 5c 7e 6f c8 99 a4 80 ba 41 16 41 39 98 7d b1 9b 71 88 c7 b3 e5 a5 11 d1 ed 92 dd 7a 3d 44 cd d6 8d c4 16 90 64 4a 7b Data Ascii: }lF&*!n9>ht K:^-|:{[7.[&-c,xYaWWad+ZLzO$V2?['t{iKf+h^JQtTQlv0Y|m|&\bi\~oAA9}qz=DdJ{
2021-10-13 10:36:37 UTC	109	IN	Data Raw: 17 1b 59 06 a4 e8 a3 c7 ab 10 82 21 0d 54 85 64 79 83 7a 23 77 33 65 7c aa dd 22 27 66 a1 da fe 47 a0 a8 26 e8 93 1b 55 06 4a 84 80 47 b4 03 a3 53 2f e3 e6 07 84 e8 a4 0b 90 10 c1 5e 28 47 ea 1f f4 3a 5a 36 63 70 f6 d0 ea 1e cd 73 c8 e0 ef a0 eb 1e 23 09 c6 ee 31 32 9f 5c 1f 05 97 52 c2 05 d7 d3 7a 90 7f 17 3b 9c 36 fe cf 5d 2c 82 db 0c 46 fe 55 03 2d 55 a9 6d 0f f5 9b 74 f7 63 28 d1 62 56 c6 05 8d be 03 e0 53 57 a6 87 64 52 6b 35 7a 94 3e 7d 58 2d f1 f0 38 2e 6e 9e c0 e5 91 e8 5d db 39 cf e6 cf 0f e7 e5 54 c4 c8 57 f7 80 b5 2d 41 ab 30 58 7c 69 23 01 cf 39 31 bc 0b ec 60 72 45 30 26 4b 3e 71 2d 0a 22 c9 e6 04 78 be 17 16 d9 8c 58 b7 b7 37 23 1b 66 69 1b d2 7b a2 99 25 38 ed 91 79 ac 7b 94 fc 5b af 84 6a 44 f7 d3 8b 86 de 61 1a 3b 80 d8 8b 5e 88 fe 81 50 Data Ascii: Y!Tdyz#w3e|'"fG&UJGS/^(G:Z6cps#12\Rz;6],FU-Umtc(bVSWdRk5z>}X-8.n]9TW-A0X|i#91`rE0&K>q-"x X7#fi{%8y{[jDa;^P

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	111	IN	Data Raw: 94 e5 a5 11 d1 ed 92 dd 7a 3d 64 cd f1 8d af 16 d2 64 1f 7b 28 d2 7c 37 82 38 bb 97 90 0d e8 d1 9d 97 fe 7f 5c 0b 7b e6 1f 0f 60 12 e7 3f 27 8e 38 5f 7f b8 12 f8 0d c1 c3 ca 43 fd 35 84 14 e8 e2 2d 1d 26 10 41 12 6f 4f ab 31 e1 32 22 94 41 49 fc 1d a4 92 69 22 6f 50 bc 55 05 a5 97 4b 58 b2 b4 19 b6 3b 59 64 4d c9 85 55 cb 92 13 80 5c b5 1f 00 76 45 19 7e 11 60 13 fe f9 2b 39 92 34 58 cd fd 75 a6 67 e0 79 90 b4 36 77 aa 7d cb 75 4e d8 7c 1f 09 44 4f c3 f8 4c c6 79 28 a6 26 16 37 4e 56 24 ef 99 58 ac bc 47 52 11 3b 18 f8 4a 6f 06 5b c4 ae 61 d0 0f 9b c6 a7 80 73 f3 c5 97 5f b2 0e ed 3e d7 b7 10 0e 87 65 70 1b 86 00 ea 65 a0 ed 04 25 8f a9 91 3d 71 75 6c 8b 35 c1 ad e2 94 d1 50 13 35 8c 42 03 27 23 68 88 35 ec bd 9d cb 4d f8 e7 7a 65 be 05 7d 2d a9 aa dd cb Data Ascii: z=dd{(|78\{`?'8_C5-&AoO12"AIi"oPUKX;YdMU\vE~`+94Xugy6w}uN|DOLy(&7NV$XGR;Jo[as_>epe%=qul5 P5B'#h5Mze}-
2021-10-13 10:36:37 UTC	112	IN	Data Raw: af b9 6a 0c f7 9a 8b e3 99 54 1a 1a 80 da 8b 21 88 97 81 70 17 26 a9 a2 e7 64 68 e7 af e2 11 25 f9 1e c6 2e 5e ba 2b a5 b8 16 bc b0 be 18 37 0a 52 68 8c 33 db b5 fc e7 20 fa a1 f6 2c 45 8c ad ce 48 d7 11 74 d2 fe 2a 8b 7b 7f 74 b7 5f 07 74 30 b0 71 11 eb 17 f7 73 42 30 13 17 df 56 37 3d fa 1a ea da c6 0e f9 50 a0 f0 ec a8 e8 e4 dc ce c9 7b 2c 5b ed ba df 54 f9 93 9c 73 8c 04 0c ad 79 3b 4d 2b 45 20 0e 9d 38 d2 d7 e9 38 21 a3 a3 9d 4c 27 93 b9 26 c1 26 2d 46 a5 ab 73 15 89 3a 71 38 e2 b8 72 12 f7 79 92 c0 53 34 c2 4a a7 39 d1 93 8c 20 5e ef a8 64 c7 c3 7e 13 62 de e5 fc 1d 03 4a 6e 2a 58 a2 cc d6 52 91 21 c1 94 b0 ce 4b 8f 3f 09 ce f2 30 06 0d b8 bb 9e 5e d5 bf dd e4 72 b7 0d 41 86 bf 82 c1 73 5b 9b 1d 91 79 38 b7 0c fa b5 1d 47 37 3d de 81 f8 24 aa e6 0c Data Ascii: jT!p&dh%.^+7Rh3 ,EHt*{t_t0qsB0V7=P{,[Tsy;M+E 88!L'&&-Fs:q8ryS4J9 ^d~bJn*XR!K?0^rAs[y8G7=$
2021-10-13 10:36:37 UTC	113	IN	Data Raw: 65 f1 3f 80 f5 f2 a4 2a 8b 80 0e 00 84 77 5d 0d a8 c0 81 e6 41 32 04 83 bb 86 c7 32 e3 4f 56 b8 e1 c4 32 9e 18 24 78 04 ee 87 06 17 77 59 78 a4 cf a3 f4 ab 21 82 2a 0d 56 85 25 79 b0 7a 3d 77 28 65 4d aa ab 22 68 66 95 da fb 47 a7 a8 6b e8 bd 1b 51 06 4a 84 ec 47 be 7e e6 53 4a e3 b8 07 dd e8 b3 0b 9d 10 ed 15 59 47 8e 1f ab 3a 13 36 54 70 f1 d0 fe 1e cb 73 f1 e0 9a a0 d3 1e 23 09 cd ee 7d 32 b4 5c 19 05 84 52 c6 05 f9 d3 1e 90 37 17 70 9c 7a fe 97 5d 6d 82 82 0c 37 fe 34 03 4f 55 c4 6d 20 f5 9a 74 a2 63 02 d1 67 56 92 05 aa be 71 60 bd 5a cb 8d 5e 7f 4b 18 3b b9 53 50 31 00 96 dd 57 03 63 b3 ca c5 d9 bb 32 b5 4a ae 92 a4 35 82 c5 74 c5 ca 0b 92 cb cc 42 2d c6 5f 3d 1b 1d 44 60 aa 65 43 e9 2b 9f 4d 17 68 42 0b 6b 13 35 00 6b 0f bd cb 65 55 e2 1a 52 d3 e9 Data Ascii: e?*w]A22OV2$xwYx!*V%yz=w(eM"hfGkQJG~SJYG:6Tps#}2\R7pz]m74OUm tcgVq`Z^K;SP1Wc2J5tB-_=D`eC +MhBk5keUR
2021-10-13 10:36:37 UTC	114	IN	Data Raw: c9 04 b9 2f f5 8d 87 e5 37 8a a4 fb 2b dd 6f 8a 3e cf ba 75 04 f5 48 50 36 ab 2d c7 48 8d c0 29 08 a2 84 bc 10 5c 55 41 d8 38 af a7 83 d2 ba 3f 76 40 ac 2c 48 43 46 48 f1 73 80 cf f2 a4 2a 95 80 40 00 9e 77 38 0d c5 87 b8 e6 6d 32 0c 83 bc 86 d4 32 ff 4f 07 b8 be c4 09 9e 12 24 79 04 ba 87 78 17 36 59 0d fd f2 a3 e5 ab 0c 82 2c 0d 42 85 2b 79 b6 7a 3e 77 3a 65 65 aa bb 22 42 66 96 da f5 47 ac a8 17 e8 ac 1b 43 06 5b 84 ff 47 9e 03 af 53 21 e3 e1 07 91 e8 c2 0b f4 10 a5 15 12 47 c2 1f f3 3a 5f 36 73 70 c3 d0 d3 1e cf 73 f3 e0 d3 a0 f6 1e 66 09 f0 ee 70 32 af 5c 1f 05 e3 d2 2e 08 8b d9 3e bd 1a 3a 5d b1 57 d3 ba 70 40 af af 21 1a d3 19 23 42 06 ce 03 66 94 f5 1f d7 06 6c f1 03 1d b2 60 ec c7 03 0c d2 35 a6 ea 64 18 6b 7d 7a cb 3e 70 58 2d f1 f0 38 2e 6e 9e Data Ascii: /7+o>uHP6-H)\UA8?v@,HCFHs*@w8m22O$yx6Y,B+yz>w:ee"BfGC[GS!G:_6spsfp2\.>:]Wp@!#Bfl`5dk}z>pX-8.n
2021-10-13 10:36:37 UTC	115	IN	Data Raw: 5e ef a8 63 c7 ce 7e 0f 62 a0 e5 d8 1d 33 4a 6c 2a 47 a2 b8 c7 18 91 73 c1 fa d5 e6 4b b5 3f 29 ce df 30 18 0d d7 b2 87 5e c7 bf d5 e4 65 b7 51 50 a3 bf 90 c1 65 5b 9a 1d c6 79 13 b7 1f fa a5 1d 26 b7 e5 d3 e8 f2 15 87 de 21 bf f0 e0 de 5c 3c 6f 82 99 ee 80 f2 41 44 41 4a 98 3e b1 d7 71 ce c7 fb e5 a8 11 b7 ed da dd 2e 3d 25 cd b3 8d e5 16 98 64 5a 7b 09 d2 32 37 ce 38 fd 97 d8 0d e5 d1 fb 97 b6 7f 08 0b 3a e6 7d 0f 0d 12 c6 3f 2d 8e 3f 5f 31 b8 5b f8 00 c1 a8 ca 1c fd 77 84 54 e8 f5 2d 10 26 4d 41 71 6f 6d ab 39 e1 2e 22 94 41 20 fc 37 a4 84 69 22 6f 50 bc 4c 05 f0 97 08 58 a5 b4 23 b6 60 59 37 4d bc d2 04 cb d4 13 a1 5c bf 1f 11 76 50 19 2b 11 77 13 a3 b0 22 39 a2 34 55 cd ea 75 e2 67 cb 79 85 b4 1e 77 9e 7d e4 75 6f d8 6b 1f 4f 44 6a c3 ec 4c de 79 3d Data Ascii: ^c~b3Jl*GsK?)0^eQPe[y&!\<oADAJ>q.=%dZ{278:}?-?_1[wT-&MAqom9."A 7i"oPLX#`Y7M\vP+w"94Uugyw }uokODjLy=
2021-10-13 10:36:37 UTC	116	IN	Data Raw: b3 5a c1 8d 01 7f 37 18 16 b9 5b 50 2e 00 94 dd 54 03 0a b3 a2 c5 cd bb 5d bc 17 ae 8a a4 60 82 82 74 c4 84 19 92 af cc 6c 2d ab df db 16 69 4e 01 87 39 6e bc 06 ec 60 72 45 30 26 4b 3e 71 2d 0a 2f c9 98 04 3b be 7b 16 b8 8c 7b b7 f8 37 1d 1b 6d 69 06 d2 37 a2 b0 25 2d ed 99 79 a4 7b dc fc 5b af e0 6a 1b f7 97 8b cf de 25 1a 63 80 98 8b 7e 88 f9 81 12 17 3c a9 98 e7 62 68 ec af f4 11 25 f9 1c c6 3d 5e a1 2b a9 b8 70 bc d4 be 39 37 05 52 7a 8c 25 db b6 fc e1 20 c2 a1 b7 2c 20 8c 9e ce 4e d7 14 74 97 fe 00 8b 20 7f 20 b7 3f 56 79 4d b7 71 16 eb 30 f7 73 42 30 13 17 df 56 37 3d fa 1a ea da c6 03 f9 2e a0 b3 ec e4 e8 a2 dc 86 c9 76 2c 3d ed f2 df 00 f9 d2 9c 31 8c 4e 0c e7 79 73 4d 74 45 2d 0e 9d 38 d2 d7 e9 38 21 a3 a3 9d 4c 27 93 b9 26 c1 06 2d 41 a5 e7 73 Data Ascii: Z7[P.T]`tl-iN9n`rE0&K>q-/;{{7mi7%-y{[j%c~<bh%=^+p97Rz% , Nt ?VyMq0sB0V7=.v,=1NysMtE-88!L'&-As
2021-10-13 10:36:37 UTC	118	IN	Data Raw: b4 47 77 df 7d eb 75 45 d8 6f 1f 42 44 6e c3 b9 4c f9 79 2c a6 03 16 1f 4e 5c 24 ee 99 5e ac ac 47 4c 11 6f 18 89 4a 0e 06 19 c4 e4 61 94 0f d8 c6 aa 80 1a f3 a9 97 21 b2 29 ed 51 a8 cf 10 6a 87 2c 70 16 86 6b ea 3a a0 af 04 65 8f be 91 30 71 16 6c a1 35 cd ad e6 94 c8 50 30 35 c3 42 30 27 4b 68 fb 35 c8 bd 9d cb 59 f8 f4 7a 3a be 57 7d 0c 94 c1 dd 8a 00 53 69 f0 d2 ee a0 62 8c 2a 0a d9 b4 af 41 c2 7d 77 0a 68 ce ee 42 7a 16 1b 0c d6 ae cc a8 dc 65 f1 4f 68 30 f7 44 25 c5 2a 51 05 5c 0a 11 cc e7 4b 07 0a f2 bf 92 34 c9 a8 30 e5 f9 11 30 2b 3e a9 8d 6a be 2e eb 7e 40 ce 95 2a f0 c5 9e 2b b0 43 c0 7b 74 26 a3 74 86 5f 33 16 07 3b 9f b5 9f 67 a0 1f 94 8f ba c7 98 79 46 6c b4 9c 11 12 db 71 7e 28 e3 7f a3 28 8b fe 3e bd 1a 3a 5d b1 57 f3 ba 57 40 c4 af 63 1a Data Ascii: Gw}uEoBDnLy,N\$^GLoJa!)Qj,pk:e0ql5P05B0'Kh5Yz:W}Sib*A}whBzeOh0D%*Q\K400+>j.~@*+C{t&t_3;gyFlq~ ((>:]WW@c
2021-10-13 10:36:37 UTC	119	IN	Data Raw: c0 88 bb 29 d9 a9 b4 9e 41 27 bf b1 bc bb 77 7b 55 91 0d fa 7d 8f 5a 63 4a e3 ce 7e 35 f1 2a 80 ae 52 49 ca 20 a1 16 c3 af 8d 66 4f 87 ae 03 d5 bc 7f 69 76 d4 e3 e3 0f 57 4b 13 32 28 a2 b8 d7 6c 91 01 d3 99 d1 92 4b c8 37 4e ce b0 22 65 09 d7 bb fb 4a a2 bf b8 f6 18 b3 59 41 c1 b3 f5 c9 16 49 e1 19 b9 79 6e a6 69 f2 c1 0f 32 33 6a de fa e0 16 ac cc 19 b8 cd e1 f2 42 11 71 af 9e f3 81 de 40 74 5f 19 9c 70 b0 b4 6d a6 e7 9e ed 8c 31 fc ff a6 de 77 3d 47 ce da 9e 82 12 df 64 2c 7b 7f fa 12 24 e3 3b d6 85 e8 0e ce c3 f7 93 9b 7f 37 16 13 e6 70 1d 26 17 80 3e 43 9c 6b 5b 57 b8 2d e5 24 c9 ee d8 4f fe 1e 96 1d ec cf 2d 22 02 19 49 18 7d 2d ae 5e e0 55 0b f4 44 2d fd 3f b6 fd 6c 50 6e 2d 91 36 06 9f 97 65 5a cc ba 4b b0 47 4b 26 4e bb 97 6d c8 9e 01 f4 5f dc 0d Data Ascii:)A'w{U}ZcJ~5*RI fOivWK2(lK7N"eJYAIyni23jBq@t_pm1w=Gd,{$;7p&>Ck[W-$O-"I}-^UD-?lPn-6eZKGK&Nm_
2021-10-13 10:36:37 UTC	120	IN	Data Raw: 3a d7 25 49 7a 1e b0 28 27 6f ad 57 fe be 7d 41 83 ad 25 1b fe 3d 31 77 63 aa 5f 52 c7 c3 59 b5 57 0f b2 2e 62 8b 3c da 93 3a 01 eb 63 8b ee 5c 1a 52 29 4f 8a 0b 67 3d 65 97 dd 38 0f 6f b3 c7 f4 bf 8b 73 85 17 9e e6 a4 48 83 e5 6e ea cd 12 c6 c6 be 4c 40 ce 28 37 69 02 68 57 cf 4b 30 d5 44 82 70 04 5c 1e 3b 4a 13 25 0e 1e 49 bb aa 69 30 c9 75 64 b8 c8 77 c4 a8 5b 37 62 46 08 12 b7 4b 8c 91 60 1e cd b8 0b a0 16 cb 8b 14 dd a6 4a 02 f2 9a 89 e3 d0 06 02 4f 80 bf c6 2a dc 91 ec 68 7b 1b dd 92 ef 26 59 ac 9f be 21 2b c9 5a c6 49 7e cf 2a d5 38 e3 b4 f5 be 7c 37 6c 52 09 8c 56 da d9 f7 de 59 88 e2 d5 41 5a f9 be ab 53 d7 7f 67 f3 fe 60 c6 63 51 41 c7 4e 6b 1d 2e dc 05 72 84 54 f7 5e 4e 1c 13 3d 92 02 19 45 89 52 98 f7 c6 23 f8 03 a8 d3 95 e7 ae e0 ae c6 ba 5b Data Ascii: :%Iz('oW}A%=1wc_RYW.b<:c\R)Og=e8osHnL@(7ihWK0Dp\;J%Ii0udw[7bFK`JO*h{&Y!+ZI~*8|7lRVYAZSg` cQANk.rT^N=ER#[

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:37 UTC	121	IN	Data Raw: 0e 5c ea b5 41 b8 5f 5e 16 5f 3c 94 5e cb 9b 1d c6 52 d4 19 53 77 30 08 c5 64 47 13 fe a2 46 2b 50 59 34 cd 99 74 ca 61 88 7b f6 9d 78 5e f7 5d bb 74 25 c4 1f 9e 50 50 0c ca 8b cd cf 6b c8 c3 74 18 7d 53 36 35 08 18 33 be 48 56 3b 11 4f 09 25 cb 26 26 34 d6 48 ec bf 0f f7 c8 89 9d 2b f6 84 97 39 33 fe e8 1e a9 a7 15 0a 8f 68 73 2b 83 23 e4 55 a5 d1 03 00 9d 05 ec 1e 7f 5b 71 dd 24 2e 2c 89 86 3b 41 73 15 ad 4c 55 22 66 6f fd 3b 92 3c 67 c5 38 79 19 68 81 db 65 fc 90 bb 06 7c f4 81 ab 7b 02 b7 94 21 af 82 5d 8b a9 b1 c4 40 90 60 2a 0e 04 cf 86 40 11 16 58 0d b5 2f 0a ae ab 64 90 ce a0 3e 80 64 79 d7 fb c8 72 7c 65 03 2b 82 27 07 66 e0 5b 03 4e e9 aa 4a fa 78 7e 22 87 af 82 8d 46 ac 82 7a 5d 53 e4 9c 1b ed fa 1f ba ba 02 41 a4 7a 5a b1 9e 37 32 31 34 01 70 Data Ascii: \A_^_<^RSw0dGF+PY4ta{x^]t%PPkt}S653HV;O%&&4H+93hs+#U[q$.,;AsLU"fo;<g8yhe|{!]@`*@X/d>dyr|e+'f[NJx~"Fz]SAzZ7214p
2021-10-13 10:36:37 UTC	123	IN	Data Raw: 32 01 78 aa d9 f0 ef 20 e4 0d a8 90 fe 4b a9 81 d2 b9 48 06 24 0d e8 dd d1 2f f1 fd 94 14 8e 61 02 c9 77 5c 4f 51 47 02 00 b2 3a fd df c6 36 0e ad 8c 9f 6f 25 ac 38 1a c4 2b 2c 51 ab e3 74 5a 8b 4e 7f 47 60 7d 75 12 f4 37 8f b7 5b 53 e3 20 bf 0d df ae 84 69 56 88 aa 1e cf bd 76 66 6a ce ed eb 15 49 42 09 37 23 a0 b0 de 60 99 03 c3 96 d0 92 49 d2 31 42 d3 b7 3f 69 08 d9 a6 ec 5c bb ba ba f6 82 12 4c 44 c1 3e 10 dd 04 d9 40 1f b3 7b 6e 36 7c fd e1 1f 27 39 73 5c 59 fe 35 ab cc 8e 1a d3 e5 d3 5c 03 ed 16 9f e3 81 cd c3 d1 49 0b 9f 59 bf ab 74 ab da 9b f8 8d 0c f9 ff e3 d3 45 bc 58 d8 db 82 8c 04 8b 66 31 75 75 da 1a 35 fe 3d d2 95 f7 03 da 50 c7 92 bb 7f 37 89 56 f4 77 06 09 03 f0 2e 32 9f c8 96 42 bd 31 e9 50 d0 82 d2 67 fd 1a 95 bb 21 d3 3c b2 eb 1e 61 18 Data Ascii: 2x KH$/aw\OQG:6o%8+,QtZNG`}u7[S iVvfjIB7#`I1B?i\LD>@{n6|'9s\Y5\IYtEXf1uu5=P7Vw.2B1Pg!<a
2021-10-13 10:36:37 UTC	124	IN	Data Raw: 97 05 f5 e2 9f 19 30 88 d3 12 7e 49 bb 0d bf 27 36 27 87 d4 8e 50 3b 1c a2 6e 91 e2 bd a7 9b 16 5e 1b 34 4e 1c 35 d0 52 76 0d eb 5c bb 07 89 d1 26 92 1e 17 5c 92 4f fe ba 49 b8 83 af 0c 1a fe 19 03 42 55 ce 43 9e f4 f5 74 f7 63 6c d1 03 56 b2 05 ec be 03 60 d2 5a a6 8d 64 7f 6b 18 7a b9 3e 70 a0 01 f1 dd 38 03 6e b3 c0 c5 91 bb 5d ea 7a c1 94 e1 77 e7 a8 15 ad ed 57 ff f3 af 42 5f ce 3a 76 7f 05 28 01 aa 39 43 bc d4 c9 4d 52 28 30 0b 4b 13 71 00 0a 0f c9 cb 04 55 be 1a 16 d3 8c 1e b7 d8 37 56 1b 08 69 7f d2 5b a2 df 25 4a ed fe 79 c1 7b ae fc 7b af cd 6a 36 f7 ba 8b e2 de 08 1a 4e 80 b5 8b 53 88 f4 81 18 17 7a a9 f7 e7 17 68 82 af 90 11 05 f9 5a c6 4f 5e ce 2b c4 b8 4a bc f4 be 7d 37 6c 52 09 8c 46 db d9 fc 93 20 a6 a1 ba 2c 2a 8c ca ce 21 d7 7f 74 f2 fe Data Ascii: 0~I'6'P;n^4N5Rv\&\OIBUCtclV`Zdkz>p8n]zwWB_:v(9CMR(0KqU7Vi[%Jy{{j6NSzhZO^+J}7lRF ,*!t
2021-10-13 10:36:37 UTC	125	IN	Data Raw: b8 3e f8 6c c1 8b ca 09 fd 79 84 55 e8 9b 2d 42 26 7c 41 7c 6f 6c ab 33 e1 26 22 88 41 46 fc 4e a4 d4 69 50 6f 3f bc 38 05 a1 97 60 58 cb b4 00 b6 28 59 7e 4d da 85 31 cb f6 13 a9 5c b6 1f 35 76 58 19 28 11 25 13 91 b0 16 39 bc 34 55 cd 98 75 91 67 fb 79 91 b4 08 77 a9 7d 8c 75 05 d8 6b 1f 51 44 6e c3 99 4c b2 79 1b a6 63 16 72 4e 63 24 fb 99 56 ac ad 47 4b 11 2c 18 d0 4a 6d 06 55 c4 a4 61 dc 0f f5 c6 87 80 64 f3 ca 97 4a b2 04 ed 5b a8 9a 10 4f 87 2d 70 4f 86 41 ea 27 a0 a7 04 6f 8f e1 91 62 71 75 6c 8b 35 db ad f6 94 d8 50 56 35 e2 42 2d 27 31 68 f1 35 80 bd c6 cb 22 f8 81 7a 50 be 05 7d 62 a9 e3 dd 93 00 51 69 f7 d2 d0 a0 57 8c 3d 0a cb b4 ad 41 f1 7d 4a 0a 04 ce b6 42 39 16 69 0c 8a ae 93 a8 85 65 b2 4f 0d 30 bd 44 71 c5 7b 51 36 5c 16 11 d9 e7 47 07 Data Ascii: >lyU-B&|A|ol3&"AFNiPo?8`X(Y~M1\5vX(%94Uugyw}ukQDnLycrNc$VGK,JmUadJ[O-pOA'obqul5PV5B-'1h5 "zP}bQiW=A}JB9ieO0Dq{Q6\G
2021-10-13 10:36:37 UTC	127	IN	Data Raw: 46 db d9 fc 93 20 a6 a1 ba 2c 2a 8c ca ce 21 d7 7f 74 f2 fe 6e 8b 1a 7f 00 b7 3e 07 74 Data Ascii: F ,*!tn>t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49760	104.21.19.200	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 10:36:40 UTC	127	OUT	GET /xml/102.129.143.96 HTTP/1.1 Host: freegeoip.app Connection: Keep-Alive
2021-10-13 10:36:40 UTC	127	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 10:36:40 GMT Content-Type: application/xml Content-Length: 350 Connection: close x-ratelimit-remaining-hour: 1199 ratelimit-remaining: 1199 ratelimit-reset: 1400 ratelimit-limit: 1200 x-ratelimit-limit-hour: 1200 vary: Origin x-database-date: Thu, 07 Oct 2021 10:59:52 GMT x-kong-upstream-latency: 0 x-kong-proxy-latency: 1 via: kong/2.5.1 CF-Cache-Status: DYNAMIC 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=PUSci3fWcmQBKmKGmPNf5qVksi1kVH5AWvp9CQLcfduvK7pRcNOG%2Bp6iY8GnFgRLnh7I9TCTMOkiN5wLKFFSYS9aQx2c76JXOoEg5W%2BFucPhZ18mEP9pZ3hAdr9laY%2BA"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69d7eda14f94c2e5-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-10-13 10:36:40 UTC	128	IN	Data Raw: 3c 52 65 73 70 6f 6e 73 65 3e 0a 09 3c 49 50 3e 31 30 32 2e 31 32 39 2e 31 34 33 2e 39 36 3c 2f 49 50 3e 0a 09 3c 43 6f 75 6e 74 72 79 43 6f 64 65 3e 43 48 3c 2f 43 6f 75 6e 74 72 79 43 6f 64 65 3e 0a 09 3c 43 6f 75 6e 74 72 79 4e 61 6d 65 3e 53 77 69 74 7a 65 72 6c 61 6e 64 3c 2f 43 6f 75 6e 74 72 79 4e 61 6d 65 3e 0a 09 3c 52 65 67 69 6f 6e 43 6f 64 65 3e 5a 47 3c 2f 52 65 67 69 6f 6e 43 6f 64 65 3e 0a 09 3c 52 65 67 69 6f 6e 4e 61 6d 65 3e 5a 75 67 3c 2f 52 65 67 69 6f 6e 4e 61 6d 65 3e 0a 09 3c 43 69 74 79 3e 48 75 6e 65 6e 62 65 72 67 3c 2f 43 69 74 79 3e 0a 09 3c 5a 69 70 43 6f 64 65 3e 36 33 33 31 3c 2f 5a 69 70 43 6f 64 65 3e 0a 09 3c 54 69 6d 65 5a 6f 6e 65 3e 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 3c 2f 54 69 6d 65 5a 6f 6e 65 3e 0a 09 3c 4c 61 Data Ascii: <Response><IP>102.129.143.96</IP><CountryCode>CH</CountryCode><CountryName>Switzerland</CountryName><RegionCode>ZG</RegionCode><RegionName>Zug</RegionName><City>Hunenberg</City><ZipCode>6331</ZipCode><TimeZone>Europe/Zurich</TimeZone><La

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Statement of Account.exe PID: 9068 Parent PID: 2140

General

Start time:	12:35:06
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\Statement of Account.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Statement of Account.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	0FB63E5EB6AF1AFF086E3C2A2321F716
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 3604 Parent PID: 9068

General

Start time:	12:35:51
Start date:	13/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Statement of Account.exe'
Imagebase:	0x3c0000
File size:	65440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 7740 Parent PID: 9068

General

Start time:	12:35:51
Start date:	13/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Statement of Account.exe'
Imagebase:	0x780000
File size:	65440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: conhost.exe PID: 1572 Parent PID: 7740

General

Start time:	12:35:51
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6c1890000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: UserOOBEBroker.exe PID: 1456 Parent PID: 1028

General

Start time:	12:43:19
Start date:	13/10/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff600c40000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	low

Disassembly

Code Analysis