ID: 526595
Sample Name: Sales Order List.exe
Cookbook: default.jbs
Time: 19:37:50
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

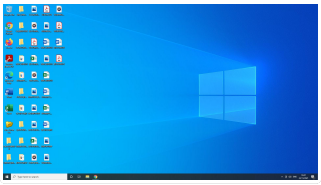
Windows Analysis Report Sales Order List.exe

Overview

General Information

Sample Name:	Sales Order List.exe
Analysis ID:	526595
MD5:	80bad0903ee7ec..
SHA1:	35aecf6fe3ac24a..
SHA256:	260e6b75d7616e..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

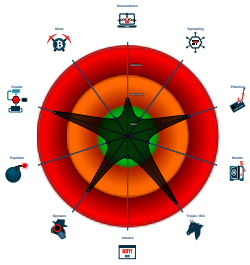
GuLoader AveMaria

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

Signatures

- Found malware configuration
- Yara detected Generic Dropper
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected AveMaria stealer
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64native**
- Sales Order List.exe (PID: 5788 cmdline: "C:\Users\user\Desktop\Sales Order List.exe" MD5: 80BAD0903EE7EC98805678673720CFD9)
  - Sales Order List.exe (PID: 6892 cmdline: "C:\Users\user\Desktop\Sales Order List.exe" MD5: 80BAD0903EE7EC98805678673720CFD9)
    - explorer.exe (PID: 4576 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
    - cmd.exe (PID: 6232 cmdline: cmd.exe /c REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "C:\ProgramData\images.exe" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 4528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
      - reg.exe (PID: 4904 cmdline: REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "C:\ProgramData\images.exe" MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
    - images.exe (PID: 4192 cmdline: C:\ProgramData\images.exe MD5: 80BAD0903EE7EC98805678673720CFD9)
      - WerFault.exe (PID: 4220 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4192 -s 740 MD5: 40A149513D721F096DDF50C04DA2F01F)
      - WerFault.exe (PID: 3440 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4192 -s 772 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=downloads;R"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.125547203981.000000000 22E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.125996962988.000000000 2330000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.125886367131.000000000 2330000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.125545111088.000000001660000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.125990940523.000000002330000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.Sales Order List.exe.18f3e10.3.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x3100:$a1: \Opera Software\Opera Stable\Login Data • 0x3428:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x2d70:$a3: \Google\Chrome\User Data\Default\Login Data
4.3.Sales Order List.exe.18f3e10.3.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
4.3.Sales Order List.exe.18f3e10.3.raw.unpack	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
4.3.Sales Order List.exe.18f3e10.3.raw.unpack	AveMaria_WarZone	unknown	unknown	• 0x51a8:$str1: cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q • 0x4efc:$str2: MsgBox.exe • 0x4dd0:$str6: Ave_Maria • 0x4470:$str7: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList • 0x3a90:$str8: SMTP Password • 0x2d70:$str11: \Google\Chrome\User Data\Default\Login Data • 0x4448:$str12: \sqlmap.dll
4.3.Sales Order List.exe.18f3e10.7.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x3100:$a1: \Opera Software\Opera Stable\Login Data • 0x3428:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x2d70:$a3: \Google\Chrome\User Data\Default\Login Data
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Direct Autorun Keys Modification

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected AveMaria stealer

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

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

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected Generic Dropper

Yara detected AveMaria stealer

GuLoader behavior detected

Remote Access Functionality:

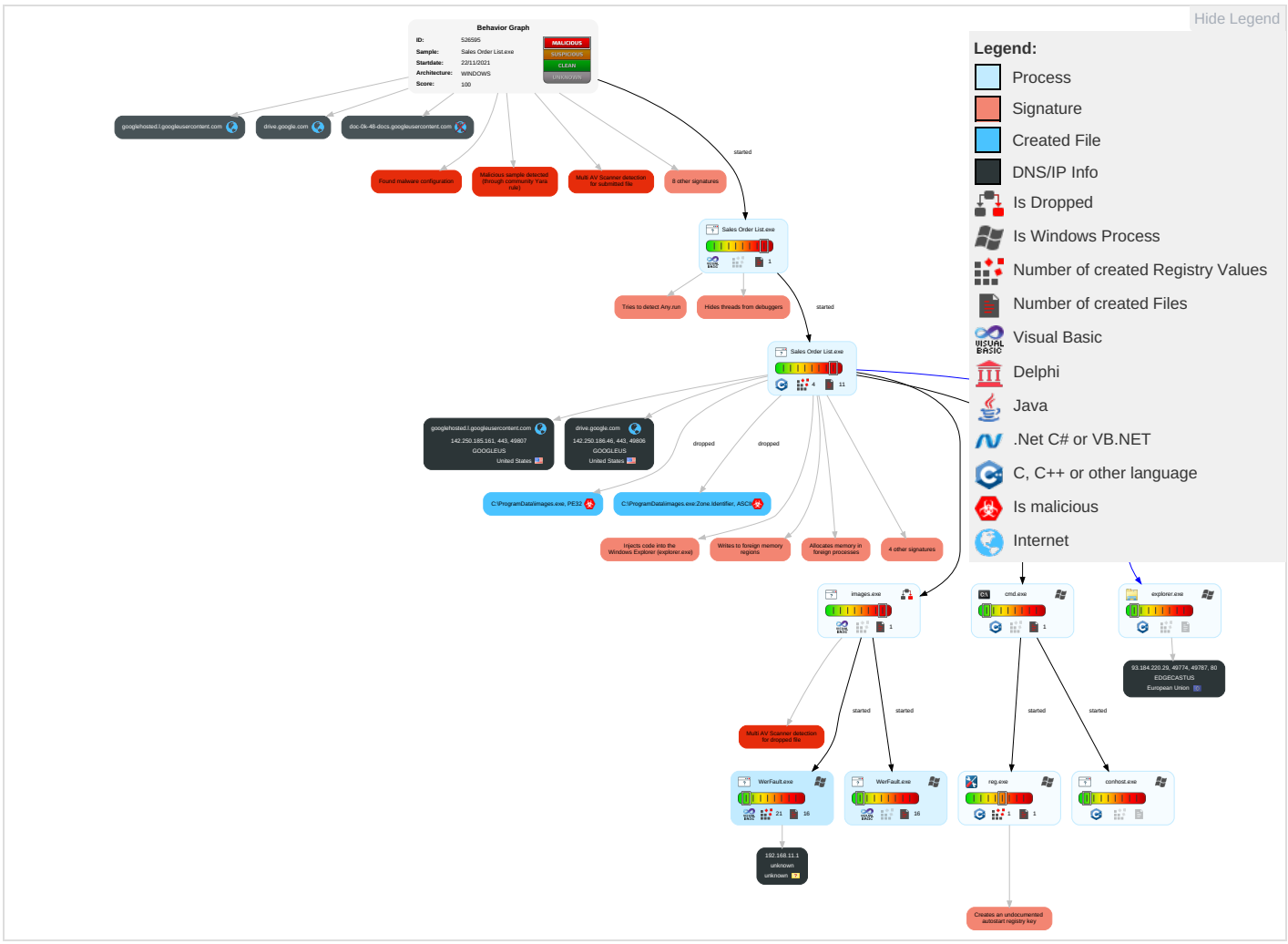
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Masquerading 3	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	E I N C
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Security Software Discovery 4 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 3	Security Account Manager	Virtualization/Sandbox Evasion 2 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 3	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Users 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F E

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Sales Order List.exe	40%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\images.exe	40%	ReversingLabs	Win32.Trojan.GuLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.3.Sales Order List.exe.18f3e10.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
4.3.Sales Order List.exe.18f3e10.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://outlook.comows.CB	0%	Avira URL Cloud	safe	
http://https://excel.office.comn	0%	Avira URL Cloud	safe	
http://https://powerpoint.office.com8	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.topqualityfreeware.com/	0%	Avira URL Cloud	safe	
http://https://watson.telemet	0%	Avira URL Cloud	safe	
http://topqualityfreeware.com	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.186.46	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.161	true	false		high
doc-0k-48-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0k-48-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/145unl5irik8qdpdmfh83ttj403osrln/1637606400000/11605847516605788748/*/14riMs-By6HjEY7hTtEKf9cx7RhIUcVvn?e=download	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.46	drive.google.com	United States		15169	GOOGLEUS	false
142.250.185.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
93.184.220.29	unknown	European Union		15133	EDGECASTUS	false

Private

IP
192.168.11.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526595
Start date:	22.11.2021
Start time:	19:37:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sales Order List.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@12/14@2/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:40:43	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
93.184.220.29	kr.ps1	Get hash	malicious	Browse	• /
	SecuredFolder.htm	Get hash	malicious	Browse	• status.thawte.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQnt%2BO7KdI35ubyUVwz39VP7XeuiQQU5wH8DBYYyn2yjOyHJ6NvYYE7hDkCEAghIHE0ISqj0Gwb1T5M8Uc%3D

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	Lamontagnem.html	Get hash	malicious	Browse	• 152.199.23.37
	EFT-11-22-201.html	Get hash	malicious	Browse	• 192.229.221.185
	Renee.schneider.html	Get hash	malicious	Browse	• 152.199.23.37
	Renee.schneider.html	Get hash	malicious	Browse	• 152.199.23.37
	Renee.schneider.html	Get hash	malicious	Browse	• 152.199.23.37
	AP_Remittance_SWT130003815_0.html	Get hash	malicious	Browse	• 152.199.23.37
	N64GUd01yF	Get hash	malicious	Browse	• 93.184.209.24
	wnRWWNwExD.exe	Get hash	malicious	Browse	• 93.184.220.29
	eFax document 805428.html	Get hash	malicious	Browse	• 152.199.23.37
	eFax document 805428.html	Get hash	malicious	Browse	• 152.199.23.37
	Customercare.html	Get hash	malicious	Browse	• 152.199.23.37
	VM30368688117.htm	Get hash	malicious	Browse	• 192.229.233.123
	Tekst.exe	Get hash	malicious	Browse	• 93.184.220.29
	voice9CT8-QJXF1Y-OWY9-6538-878.html	Get hash	malicious	Browse	• 152.199.21.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	in27996.html	Get hash	malicious	Browse	• 152.199.23.72
	SANDBOXME.HTM	Get hash	malicious	Browse	• 152.199.23.37
	#LYTNXI.HTM	Get hash	malicious	Browse	• 152.199.23.72
	rfq.exe	Get hash	malicious	Browse	• 93.184.220.29
	cbenson@palliser.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	atlanticare.org-Payslip-Details-691256-pdf.htm	Get hash	malicious	Browse	• 152.199.23.37

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	EVhIUVrKx8.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	#U0191ACTU#U0156A_gudqNItO_54357.vbs	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	pix2021.TZNZPOYJNN.msi	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	T1SN5sRQjf.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	Lamontagnem.html	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	EFT-11-22-201.html	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	aBGNeDS7yM.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	aBGNeDS7yM.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	ATT00001.htm	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	Renee.schneider.html	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	REF ID 398046279094.html	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	Chrome.Update.5947c2.js	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	Chrome.Update.5947c2.js	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	2GirCpksIO.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	HP7DYSoP6M.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	yRqB5VANT3.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	n#U00ba410000512664.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	1Fu7t9XR6E.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	justificante de la transfer.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161
	justificante de la transfer.exe	Get hash	malicious	Browse	• 142.250.186.46 • 142.250.185.161

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_images.exe_57d888b29fe7ab2cf088fdbce37499b180b0e399_39dd1f14_cce5b39a-312f-4d6a-a179-08e27df0d1ee\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8478396170633179
Encrypted:	false
SSDEEP:	96:YGTIFeXYXpgU+KsFY2gUoh7JfrvXIxcQGc6YQVcENcw3Ti+HbHg/TVG4rmMoVazR:YSIkgqtKbmIbV3PLjEADu76dfAIO8QM
MD5:	726233F268AF487916D11A48783A277B
SHA1:	73F09323FE011E46836EA48C0B6C6E2672FB532F
SHA-256:	9A06535409A1A8800CCA715AA0EF99DFD56FC7142F838FFC69476DEE450F5C0C
SHA-512:	E6EEBF38FE7840E6A080531551E774EC2B8BB10FFE26DFDA60458CBA0C04035A2E5B25BFA1C28D2AF00789592BF6111C034DFD01BAC8826F6E38A2E6DAB77A5A
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.0.8.3.6.3.8.5.4.0.7.1.1.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.0.8.3.6.4.0.8.9.9.5.1.8.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.c.e.5.b.3.9.a.-.3.1.2.f.-.4.d.6.a.-.a.1.7.9.-.0.8.e.2.7.d.f.0.d.1.e.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.e.5.0.8.d.6.-.9.b.3.c.-.4.8.c.e.-.b.0.c.2.-.9.a.c.2.8.2.d.1.9.0.9.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.i.m.a.g.e.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.B.a.n.d.i.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.6.0.-.0.0.0.1.-.0.0.1.1.-.c.1.a.2.-.7.e.d.0.d.8.d.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.d.5.a.0.d.a.e.e.1.6.6.1.e.2.4.9.2.6.5.9.4.3.0.6.0.a.b.b.a.a.7.0.0.0.0.4.2.0.4.!.0.0.0.0.3.5.a.e.c.f.6.f.e.3.a.c.2.4.a.d.a.f.1.6.c.0.4.b.7.8.7.e.9.0.a.c.4.c.8.4.5.e.b.0.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_images.exe_f17d4a87747d76beb8eb6ec81cef537fcdde6d7_39dd1f14_613b4565-8822-4610-a680-fd57c1b886b3\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.848572589416445
Encrypted:	false
SSDEEP:	96:YTTPF7YYXpgU+KsFY2gUor7JDSvXIxcQsc6tcElcw3B+HbHg/TVG4rmMoVazWLn0:YnPhqtKMmSpvSjEADu76dfAIO8QM
MD5:	7DAB837A1A80EA790A9363618F28ADBD
SHA1:	1D59EAE9899B281C100E26112C3730F8A9A485F4
SHA-256:	0CC025180D514E387C09D9E2050B162746A106E61E438BAC22A0E1F0FA190F45
SHA-512:	CF8F78A2CF5FCF3675AE183D2D13EED2C6F0F0339A41D9493F9F119C1572F89137CE6814C60A1E9EF5A60B456B2A38636C5FB89965572063DF265AD932C0554A
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.0.8.3.6.4.9.0.9.2.2.1.4.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.0.8.3.6.5.1.3.4.1.7.2.1.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.1.3.b.4.5.6.5.-.8.8.2.2.-.4.6.1.0.-.a.6.8.0.-.f.d.5.7.c.1.b.8.8.6.b.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.6.e.5.5.e.c.1.-.0.8.1.b.-.4.5.a.7.-.b.8.c.3.-.f.6.e.1.4.7.7.2.8.b.e.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.i.m.a.g.e.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.B.a.n.d.i.e.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.6.0.-.0.0.0.1.-.0.0.1.1.-.c.1.a.2.-.7.e.d.0.d.8.d.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.d.5.a.0.d.a.e.e.1.6.6.1.e.2.4.9.2.6.5.9.4.3.0.6.0.a.b.b.a.a.7.0.0.0.0.4.2.0.4.!.0.0.0.0.3.5.a.e.c.f.6.f.e.3.a.c.2.4.a.d.a.f.1.6.c.0.4.b.7.8.7.e.9.0.a.c.4.c.8.4.5.e.b.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC437.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Nov 22 19:40:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49428
Entropy (8bit):	2.2764484756070344
Encrypted:	false
SSDEEP:	192:DWGdU2O2Oamg80s+5MTfML70kDqQNTgYdgEnDUfVSzCkP5xVCFcEb4D9BcAjPV:Cp2OBaKA0kDqQVgNfVUxVCFcEb4D3
MD5:	A32CC57E95B135A03775F90374DC995B
SHA1:	083E228177F799BEE907FB1A4DE81B3D73E11341
SHA-256:	8C0F7FFE3BC51283DAE224EE37C186A77279BE22F629C0D0838AD40AA10B57C8
SHA-512:	0A1341A9F25A089658DE797267091DD8ED7AC28DB4336AE4976918CED9607111EDC47CFE6683D02506F5C5D51A1A31DD20D72D9415E238358AEB64F83A47A71
Malicious:	false
Preview:	MDMP..a..... .....7.a.....$...8+.....T.....8.....T.....H.....bJ.....GenuineIntel.....T.....`...1.a.....0..2.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7C2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6312
Entropy (8bit):	3.716692772422422
Encrypted:	false
SSDEEP:	192:R9l7lZNizL6qeYY89yxhprU89bdOsfYfm:R9lnNif6qeYY8UbdNfN
MD5:	273081CE0FBE3E7A4B6A7FFF7CD15508
SHA1:	005B7C88175F36C015E2769ECDCBBDA0C2FF364B
SHA-256:	816132BBE3824BC8C56BC8E56BCC19B1D4130B880CB176F5EBEBB2CDEBE1BD83
SHA-512:	88D67B70122F5CCE1B37BC71B8AAE7B5577BFCFEAE3CA657F2E69716F38111EEC63473AD0D6CFE73ABF894C96AFA87438597DBB1C1DF87C536C303C5456990EF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.1.9.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC959.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4815
Entropy (8bit):	4.497462564893132
Encrypted:	false
SSDEEP:	48:cvIwwtl8zskme702I7VFJ5WS2CfjkoF5s3rm8M4JVaqaFp+q8uTLgyNXnd:uILfkb7GySPfwJVrmxvgyNXnd
MD5:	8E8ACA891C0DAFDAD9B716CFCF16E35D
SHA1:	AFC2E8B7BC9F63788356F029B9CDC3B7BCE461B8
SHA-256:	40452B4A0C70CA3D191252F5BAFAB4D45A1640943CB2C7284CE6EEA081B816AD
SHA-512:	BE7148D25001E505F77322F4EAE9FA81DDAD355496D59A2D4D0D085FCC1AFE86DB6C1EFFE98F921D022B6D87E3C797A2E3D53FFAE1FA9E028B5C8C0C26A7456
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="221365342" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED6A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Nov 22 19:40:49 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46432
Entropy (8bit):	2.2247663829786646
Encrypted:	false
SSDEEP:	192:lVGdUO1Oamu80Fj9XRMTuML70k3qQNo1pUC+SzCkPr/78yC0J67GcwW2lvJMF0:fpPad9W0k3qQCAC+S/78yC022Xw0
MD5:	93DA37795E39DDBFC35B3FD49EFD3677
SHA1:	C8A82681CA147B3359C272635AF4600C3D626E17
SHA-256:	653599677A687AF787EFD41ABC1131C435F0A387633B9ABF612C1FF8A13BA26A
SHA-512:	72764C240C07B65258FFE6EB1E4BC175033A3DA61BA7E2CE2BAD79F4E0505FBEB6715704DD17019BFC8F12D1E71D166F47191FF6927D16D2D9C0CC3D348C0D8
Malicious:	false
Preview:	MDMP..a.... .....A.a.....8+.....T.....8.....T.....h.....bJ.....GenuineIntel.....T.....`...1.a.....0..2.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF0F5.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6318
Entropy (8bit):	3.71965123962902

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF0F5.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	96:R7IU6o7lZt3izS6qWgYtD3EOvzcuujulRZaMQU989bz2OsfSpsm:R9l7lZNizS6qWgY5VhpD989bqOsfSum
MD5:	CF08123302862458DFB30EC779525E8E
SHA1:	EB9C1D4C31F4F91D7FDA061F6EB859F649EB82BD
SHA-256:	8F2F9ABE5B08E3BB2F5D79D9C9942B72A820C49547F58FF0509CEBB7BA76733D
SHA-512:	94D19CA7FE6EA154EF167E5696654801650C641497AD235D1952863C34AA57B79FE93C00A373EFA54F3B4C35AB182498B0E9220C30E9222F08E713A9CB686AEF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.1.9.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF28C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4819
Entropy (8bit):	4.4952153447217285
Encrypted:	false
SSDEEP:	48:cvIwwtl8zskje702l7VFJ5WS2CfjkoGs3rm8M4JVaYOqFIVjq+q8uJlOQyNXnd:uILfk67GySPfTJV38Fqx/jyNXnd
MD5:	58F740B602AFA8D8CB8AA8499E07AC1D
SHA1:	42C251BD39F06CCC85A621E0FFECD604C17D27AE
SHA-256:	FB4E46665816F4DA83ADE7D64B5AA3CBAD643AB9E5C6990B6382436F306BCD83
SHA-512:	78A14FBFBA655633D8B86611DC11CB3E943FB807E44DB260816762EE44932E670D95F6601E7A64FD4C1F70C010F9484D1DB95A0455F45D598291F2E01E085C34
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="221365343" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\ProgramData\images.exe	
Process:	C:\Users\user\Desktop\Sales Order List.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	5.002958856412811
Encrypted:	false
SSDEEP:	3072:trejCYyLGrRxfFNEv6QN744ndRkHDwLVly5Mrc0yvhXeJ:treiGrRNFMjN6jIVCMrcbeJ
MD5:	80BAD0903EE7EC98805678673720CFD9
SHA1:	35AECF6FE3AC24ADAF16C04B787E90AC4C845EB0
SHA-256:	260E6B75D7616EFD29C05151F1CE95BBAB1AAF8703F86F62C4D9BC6D308A56B8
SHA-512:	9A88B4EA27BBC8B83C0722C715C12B3667D6138D27D2FABB315A8A8C4DDCB020962625D1AA75C56D7E2082BBDED7FFAA3512B482F1A4BA138D1877A55E848E9B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....G.....0.....L.....@....@.....:.(....`.....0.. .....text...l/.....0..... ..`.data.....@.....@.....@....rsrc.....`.....P.....@..@...I.....MSVBVM60.DLL.....

C:\ProgramData\images.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Sales Order List.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

C:\ProgramData\images.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\~DF052E41D7F13B5154.TMP	
Process:	C:\Users\user\Desktop\Sales Order List.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.01191323271951
Encrypted:	false
SSDEEP:	384:wcZ0tADSVlx6JQhynrV7Vr9wrCIM/ZUYVPzBAPN:wcZeADSV/6qhynrV7VxwrrMvqPN
MD5:	6C4C01A4316CD9338DE51EC175EBF11D
SHA1:	8C5D5B07E0ED6AAC72705F516E25BEAEA891EFA0
SHA-256:	95876F7C1242672418DB201C02D70276EE9CC4345394DEAD3500619A39DA28F0
SHA-512:	9F60729E865B0414DB4792F76465EDCE1595D22E884D01C07389A312474D1CE916E4CF73275D5AA0CB411D8EBB0617EF661CD10467AD838FD1B0B388C44823D
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF9DCB19D0128ED2C8.TMP	
Process:	C:\ProgramData\images.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.01191323271951
Encrypted:	false
SSDEEP:	384:wcZ0tADSVlx6JQhynrV7Vr9wrCIM/ZUYVPzBAPN:wcZeADSV/6qhynrV7VxwrrMvqPN
MD5:	6C4C01A4316CD9338DE51EC175EBF11D
SHA1:	8C5D5B07E0ED6AAC72705F516E25BEAEA891EFA0
SHA-256:	95876F7C1242672418DB201C02D70276EE9CC4345394DEAD3500619A39DA28F0
SHA-512:	9F60729E865B0414DB4792F76465EDCE1595D22E884D01C07389A312474D1CE916E4CF73275D5AA0CB411D8EBB0617EF661CD10467AD838FD1B0B388C44823D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	2359296
Entropy (8bit):	4.229022675301259
Encrypted:	false
SSDEEP:	24576:53LsOZS1hnA9WpZhOnzm9VxS70YagmcnYJ2:53LsOZS1hnA9WpZhyS9PSYYagmcnYJ2
MD5:	DCE0352F52A581AE193E3739AEB94EF8
SHA1:	85D78703929E839540AAE2177A83D4CF3B6AE1FF
SHA-256:	CC33452D33B55B127F0687AA6A986AD18D21ED02F66556C65C2532FF2B938445
SHA-512:	7A50534F145F8912201DA957EFC11A1E16A62013D79B69EF863B1684D21AF6492B79271FB68AD191220565A2D69D3C5461D4BD136D6EBDA3A882D55CE314D856
Malicious:	false
Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm.~.+..... ....~..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	4.160771825952116

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Encrypted:	false
SSDEEP:	1536:S3hrUgdf3Q43IjRGaqnv5nTsb71c+rUgdfteceDetoWLrI:wyKf4CKfteceDetoWLr
MD5:	8984087B2EEE85640E7CF7DA8CCFC985
SHA1:	D7FDCAF6E0BFEE4A88F98EE76563B6775FEB4543
SHA-256:	12147707FDFF3EBBD9180DF79A8C93918D7CCE69C73D26808CBE7B5E4358D451
SHA-512:	50D7079563A500851C3009A64132161DA05E05779860A423BD58EBBBEEDCCE2073A0EFF12E88AA88E55D2FB5585AFC56990DAE07BB51EA94A81A3E2F61E499DD
Malicious:	false
Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm.~.+..... .....~.HvLE.N.....P .....V....L!.=.fR.....hbin.....5.#.^.....nk,....S..... .....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk .....(.....@.....*...N.....)...InventoryMiscellaneousMemorySlotArrayInfo.....mG.....nk .$4./T..... .....Z.....Root.....lh..(.....A.....nk .4J....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.002958856412811
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Sales Order List.exe
File size:	192512
MD5:	80bad0903ee7ec98805678673720cfd9
SHA1:	35aecf6fe3ac24adaf16c04b787e90ac4c845eb0
SHA256:	260e6b75d7616efd29c05151f1ce95bbab1aaf8703f86f62c4d9bc6d308a56b8
SHA512:	9a88b4ea27bbc8b83c0722c715c12b3667d6138d27d2fabb315a8a8c4ddcb020962625d1aa75c56d7e2082bbded7ffaa3512b482f1a4ba138d1877a55e848e9b
SSDEEP:	3072:trejCYyLGrRxfFNEv6QN744ndRkHDwLVly5Mrc0yvhXeJ:treiGrRNFMjN6jIVCMrcbeJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....G.....0.....L.....@....@.....

File Icon

Icon Hash:	0ceefedec6f67c0c

Static PE Info

General

Entrypoint:	0x40134c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x47ABAEC7 [Fri Feb 8 01:22:15 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f27a613fda76c14f4eab7dc0085d799e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x22f6c	0x23000	False	0.367292131696	data	5.18350124338	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x24000	0x13f0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x90bd	0xa000	False	0.346240234375	data	4.35051738239	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 19:40:20.993186951 CET	192.168.11.20	1.1.1.1	0x2a23	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Nov 22, 2021 19:40:21.695991993 CET	192.168.11.20	1.1.1.1	0xa94e	Standard query (0)	doc-0k-48-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 19:40:21.003087044 CET	1.1.1.1	192.168.11.20	0x2a23	No error (0)	drive.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Nov 22, 2021 19:40:21.727973938 CET	1.1.1.1	192.168.11.20	0xa94e	No error (0)	doc-0k-48-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2021 19:40:21.727973938 CET	1.1.1.1	192.168.11.20	0xa94e	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.161	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0k-48-docs.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49806	142.250.186.46	443	C:\Users\user\Desktop\Sales Order List.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:21 UTC	0	OUT	GET /uc?export=download&id=14riMs-By6HjEY7hTtEKf9cx7RhIUcVvn HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache
2021-11-22 18:40:21 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 22 Nov 2021 18:40:21 GMT Location: https://doc-0k-48-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/145unl5irik8qdpdmfh83ttj403osrln/1637606400000/11605847516605788748/*/14riMs-By6HjEY7hTtEKf9cx7RhIUcVvn?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-oLxZszB0BcYP3TMe60uaAA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=bd1QtAnK97hsI4O0PC7VeHHZYPkVM_fEdc2jyrNcwwPu2Yx4SOv2v8XvjOcyhRdt_evGRfcN3abCX_ZiOeg-CiMjgIpnvyrXH95C0QX2pqXR5VywQnN97bJ6hkuZxOUou4rp18bW8U8cwx1O_vjYibOqv0awmvg8FJU4CwcICFY; expires=Tue, 24-May-2022 18:40:21 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-11-22 18:40:21 UTC	1	IN	Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 6b 2d 34 38 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 31 34 35 75 Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0k-48-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/145u
2021-11-22 18:40:21 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49807	142.250.185.161	443	C:\Users\user\Desktop\Sales Order List.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:21 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/145unl5irik8qdpdmfh83ttj403osrln/1637606400000/16058475166057887 48/*/14riMs-By6HjEY7hTtEKf9cx7RhIUcVvn?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-0k-48-docs.googleusercontent.com Connection: Keep-Alive
2021-11-22 18:40:22 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdu2mM_0RGOTanM6Rq3SOy92hypDGEwlbNfnSJdfdnTlvNvsD2TOGuIz4daFc4yp hD19X_KCgSC1tc4Ffr7W-DM Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Cl ient, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visib ilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-R eason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-T ype, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-M eeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="wamar_TRmuqY33.bin";filename*=UTF-8''wamar_TRmuqY33.bin Content-Length: 156224 Date: Mon, 22 Nov 2021 18:40:22 GMT Expires: Mon, 22 Nov 2021 18:40:22 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=96J0GA== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-11-22 18:40:22 UTC	6	IN	Data Raw: fc e5 46 c8 62 1e 25 57 bb 48 db 18 dc 0d 1e 8f 5c 86 92 2c 29 4c 78 f0 81 bd 1c 4e 04 93 64 7e 5d 04 b3 0b 89 03 9d 2e 55 a8 00 c7 94 50 09 d5 07 78 93 60 9b f8 12 72 f4 67 3f 8e 72 cc fa ab c8 d1 05 c4 11 35 9f 96 c9 2f 1d 27 a3 af 8b 53 bc 8c 5a 9c 4b b5 bb 5b 53 c4 c4 16 e8 34 b4 41 c1 d0 d2 e5 9d af 02 91 63 62 a6 55 c8 7c 55 d4 eb df d9 47 bf 64 b9 1f 1f 0a ad 82 2a 0c 04 8a dc 17 2f 57 0d 2f 64 ba 42 80 09 4e 47 d7 90 56 5a db 30 57 f6 ee b4 03 b6 9a ea fc e6 5d 72 91 c2 89 99 37 67 e4 30 b4 36 11 17 68 7b ad f8 3a 80 f6 78 52 7b 44 ea a4 3c 41 9b 19 6a 51 f2 c3 5d f8 15 51 4c 82 95 d9 b3 65 3e 28 bc 1d 2a 17 b6 db 37 ef 7c d9 57 4e a7 fc f7 e6 1d 87 6e 85 d7 47 1b 3b fd c8 5a 8a 44 ab 9d 48 b4 c7 8f d9 d8 14 e9 b0 d9 8c ca 43 df 0f 81 07 2b 67 96 Data Ascii: Fb%WH\,)LxNd~].UPx`rg?r5/'SZK[S4AcbU|UGd*/W/dBNGVZ0W]r7g06h{:xR{D<AjQ]QLe>(*7|WNnG;ZDHC+g
2021-11-22 18:40:22 UTC	9	IN	Data Raw: 79 38 e6 53 15 a4 a8 cb 4f 01 c5 b4 5b a5 2a 9a dd 19 72 89 81 b6 9f f4 44 27 ce 82 f9 9e 52 91 17 b8 7b d4 b5 1c 10 bd ec 52 23 83 44 64 ea 05 bb 16 7e 5a 5c b5 fb cf fe a3 a2 24 e0 e2 ef 2e b9 b3 6a 13 21 23 e9 c0 41 f0 69 20 08 cb 7d b8 bc 6d ec 02 3c 46 fd 13 ba 57 d3 b8 c1 06 f5 c0 1c 72 37 46 f4 bb 40 1f 1d cf 2f 14 09 02 78 5a 4e b3 de 67 06 0f 57 2e a0 df 8d aa ec c8 cc 78 13 03 f5 ce e2 b2 30 d2 b5 0d 44 a3 66 7b 74 b8 dd f5 38 43 d6 da a4 c9 c8 97 cf 45 da a3 83 fc 3e d1 01 29 6c 1c e9 73 eb 74 6a ab bc d5 00 4a 20 02 77 c4 dd fa 97 90 1d 0f 9b 18 b0 c3 39 12 13 29 0a 9b a7 89 d5 fb 1d 0f 6c 0f 3a a9 bd 90 97 59 65 dc 04 84 d3 8e bf 17 9d 81 91 0c 69 12 4d 14 d2 22 fb d8 4d 49 b8 7b 89 93 d1 e4 f9 3b b5 70 b5 44 4c cc c4 a5 9b 50 36 0c e6 fa b1 Data Ascii: y8SO[*rD'R{R#Dd~Z\$.j!#Ai }m<FWr7F@/xZNgW.x0Df{t8CE>)lstjJ w9)l:YeiM"Ml{;pDLP6
2021-11-22 18:40:22 UTC	13	IN	Data Raw: ec df aa 6a bd 8e fb 46 3f 97 cc 58 74 d9 3a 25 78 14 4e 1e 83 0d 8b b9 10 bb be 87 65 45 45 0f a2 43 6d 83 1f 83 5a 14 55 4c 7b a6 3f 8f e7 a9 70 19 e3 5a 83 d7 00 75 45 7b 94 13 d1 9a 05 9c ac d4 09 3a 43 51 a7 9e 0a fb 28 35 c3 e4 9b 04 6b f2 76 34 4e e3 5c 19 53 27 a2 3c 70 fb 53 2d f8 6a 33 20 ec 88 35 5e b4 22 f3 f9 76 a8 e3 89 77 da 79 65 3d e5 e3 e0 fb b7 6a 29 ef 00 55 b2 db ad 97 7f 24 8d e5 65 62 1b 79 db 09 46 2e 7a b6 a5 41 c7 82 89 3e d7 ca bb 87 23 5d 8d 94 ad 79 17 8f c5 99 a1 44 7e 59 2f 28 42 1f e8 cb 8d c2 79 e1 e8 f3 f3 84 58 52 99 59 86 43 16 8d 47 50 61 de b5 13 7c 38 72 6e 0a d8 6d 59 a1 dc 3b 90 9e 7b 13 4d 6a 1a b2 e2 26 87 d2 18 38 eb 21 62 2e da 66 5c e2 62 a5 cc 38 fa c5 ce 61 72 26 53 af 37 40 cb 7e 42 ba 0c 39 be c7 16 57 47 Data Ascii: jF?Xt:%xNeEECmZUL{?pZuE{:CQ(5kv4N\S'<pS-j3 5^"vwye=j)U$ebyF.zA>#]yD~Y/(ByXRYCGPa|8rnmY;{ Mj&8!b.f\b8ar&S7@~B9WG
2021-11-22 18:40:22 UTC	17	IN	Data Raw: b2 64 d1 8b 53 32 67 10 a8 36 34 78 1c 12 84 38 65 3e df 41 f0 cd 8f 08 6b de 93 a9 63 70 bd 60 56 bb 20 5f 9b e9 50 c4 f0 14 7a 60 c8 84 1a 56 14 36 63 fa 61 f9 cb f4 66 ea d7 a1 b6 c9 1d dc 79 19 10 7b b8 ee a0 76 ec d2 a8 59 0c e2 41 65 44 1d 9b c6 94 14 d3 e8 06 3b 0b f2 42 5a d7 b9 56 7e f7 0d 26 b1 05 3b 87 f3 5c e6 95 c9 d5 90 fc 52 d5 a0 68 ef c3 55 57 b9 1b a7 1c 58 9a 92 3d 57 81 47 d0 67 e4 9a 46 23 e9 6d ab da 84 b9 83 7c 64 31 9f e1 c2 32 8b 5f 00 ff 4b 02 29 74 22 37 e3 95 f6 27 02 4c 21 21 d8 75 40 b1 82 f6 12 61 da 83 a9 08 fc b6 a6 ac 4d 0e ce 9d 92 99 c4 16 d3 c5 45 19 aa 19 58 db de 4a 9c b2 fc b3 4a 44 d0 d5 9a 99 d4 ec 34 e1 ca 2d 81 81 b3 ca 24 7f 99 e8 bb 2d 9a 20 6c a9 2b 14 56 9c 4f 32 2f a9 75 1b 87 e8 8a 7a e5 31 72 2d f7 1e 6e Data Ascii: dS2g64x8e>Akcp`V _Pz`V6cafy{vYAeD;BZV~&;\RhUWX=WGgF#m|d12_K)t"7'L!!u@aMEXJJD4-$- l+VO2/u z1r-n

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	18	IN	Data Raw: c0 05 c9 85 97 77 eb 83 1c bb 4e 1f cb 07 65 97 96 9e 24 10 31 f2 8d 6c 49 52 ab 2c a0 08 57 0c 7b a5 39 f0 af 8e 81 bb 66 31 57 84 3a 48 ad 7c df 80 02 7d 3a 7f 4c 4d f9 88 a2 4f 6b 3f db 15 61 9b fc 5a 3d d6 07 5c eb 03 84 67 10 88 16 63 bb 49 0c 33 a9 0d a2 03 f7 2a d3 57 1c 1c ca 59 33 af f9 6b 14 7d a0 ef 9b 15 16 6f 6a 1d 3a 09 a2 d6 8b 17 ac b1 f3 d4 07 b6 91 70 53 72 51 f7 f2 ce 63 13 6b 72 d2 22 2d 75 a1 9b dc 3f f4 2b 05 4b ff b5 e6 39 a1 bb 2d 19 8b f8 8f cb 4b 37 8d 54 30 cb c4 47 d8 da 95 58 f3 46 c5 da 71 5a 55 91 87 22 93 56 bc 66 a4 f0 54 90 2a f7 c8 d2 7a 63 91 30 78 14 3f 18 e8 e9 76 7b 59 a8 8d 94 ad 36 e0 a7 d9 02 89 36 84 bc d4 8d c4 1b 6a 8a 9c 73 8f b9 61 94 aa 8c e2 78 f4 cb 07 92 1c b3 fd c2 87 ad d3 e9 d0 27 a7 c3 ef 58 5e ee 3f Data Ascii: wNe$1llR,W{9f1W:H|}:LMOk?aZ=\gcI3*WY3k}oj:pSrQckr"-u?+K9-K7T0GXFqZU"VfT*zc0x?v{Y66jsax'X^?
2021-11-22 18:40:22 UTC	19	IN	Data Raw: 9f 2d 11 ce de ab 15 c8 4c 4e 60 8d 70 eb 50 8f a7 19 82 b5 e9 06 be c9 4e 2a 7c 67 ff 02 ec b8 4e 91 3f 08 d2 25 22 d6 34 ca 23 eb 84 f4 a2 88 59 45 a5 92 f3 78 85 87 81 03 c0 a5 e3 56 1f 84 7d db 5c ac be f6 3f 93 b1 3c 7c 2a cd 90 ae fc b9 8f f3 d5 65 ac e1 8c ba 7b bc 7f d4 7b 11 8e d0 47 02 ba d5 2a 70 35 5d c6 31 1c e9 5a 60 6d 41 40 a8 5f 60 e4 98 98 bc f7 e6 2d 9f 62 b0 35 12 12 e5 8e 78 52 55 99 87 54 f9 d7 f0 66 2a 97 bb fa 64 7e ab 5d cf 85 82 25 02 db 28 9f 35 7f 7e 1b c6 54 7a 74 1e 0c fa ef 6a 69 32 a4 d5 cf ee a5 74 ac 8f 44 b2 37 be 4a 44 d0 db 2c 01 e3 17 cb 3f 89 29 6e 27 1a 62 24 ca 79 ac 96 59 aa 45 31 bd 3c 58 2b 26 b8 34 21 b1 41 d6 c8 a9 82 7c 86 f5 dd 15 0e bd 21 4c 9b e6 39 53 d0 05 1f 8a f6 f7 c1 ba d6 20 ac ca ad 3b 71 ca f7 ca Data Ascii: -LN`pPN*|gN?%"4#YExV}\?<|*e{{G*p5]1Z`mA@_`-b5xRUTf*d~]%(5~Tztji2tD7JD,?)n'b$yYE1<X+&4!A|!L9S ;q
2021-11-22 18:40:22 UTC	20	IN	Data Raw: 60 18 e2 2d 49 e1 98 d7 2c bb b7 42 66 b2 4f 5c 5c f1 c5 0f cf 88 f8 43 33 90 43 0c 6a e5 11 00 b7 04 77 87 df ed 71 75 27 53 d6 c1 7d 43 a2 6f c3 02 ea 60 7a da 05 3d 8b d4 b6 9f 6c ac f7 cd 0b c6 f7 81 01 ef 7e 8c 03 40 35 75 a2 65 5b ce 85 72 97 11 9f 27 16 00 7b 10 e1 ab a5 df 38 a9 71 12 cb 40 df 8c ce 96 4f e6 45 f1 3c 38 32 76 9a d7 f4 9c 51 fb a3 9e 38 1e ca 63 5a bd db ff 64 19 35 c0 31 72 3d da 05 10 f7 2e b4 98 f5 f5 14 f6 7a 41 80 41 c5 d1 dd fc 7d 8e 37 2c fc b9 3f f5 60 0b 11 82 ac 8f 24 73 c8 72 5d 30 c2 1c 43 bd 2e 6d 4f e8 35 76 01 31 3f 33 8d 6f 8e e4 cd 67 fd e9 81 f8 ec 28 a0 98 d2 fc 83 87 ad a5 eb b2 0a 05 7b 8d 0b 0b cb 0d e9 1c cd ac ed 65 55 20 37 74 98 21 f1 5f b4 8c d4 d2 f5 af 89 f1 c5 81 30 4b af fa f3 f9 bf 27 d6 ad b6 36 66 Data Ascii: `-I,BfO\\C3Cjwqu'S}Co`z=I~@5ue[r'{8q@OE<82vQ8cZd51r=.zAA}7,?`$sr]0C.mO5v1?3og({eU 7t!_0K'6f
2021-11-22 18:40:22 UTC	22	IN	Data Raw: b3 66 c0 18 93 89 cc 41 84 05 53 6b fb bc 29 aa 63 78 a9 e2 11 00 37 ab e9 53 a7 86 31 9b b5 bf 06 89 50 15 90 24 26 aa 02 4e 3f e3 06 af 28 d2 25 24 de 34 1c af e7 6c a0 b0 a8 21 87 c3 59 a6 ad aa 51 e6 f7 c8 85 07 00 ef a6 b1 06 26 d0 37 bb 10 94 c9 44 3d a7 09 2e a5 05 38 95 f3 5c 92 26 87 05 1c f4 ba 39 c1 7b 9b 0d 9b 5f 6f 28 54 6c 0a ee 53 3b 97 ad ad 7a 9f dc 63 4d 9d f6 30 81 94 97 ec 08 1d bb 84 15 a4 ca 8c b2 0a f8 74 37 c7 68 26 42 81 16 18 b3 5c 4d 68 17 ee 96 65 fe bb 8b b0 e5 8c 5e dd 88 15 46 b6 f3 cf e1 73 8b 95 49 5c 31 c1 7f 30 26 1d 27 09 db 67 d0 e0 74 0b ca c0 c0 b7 de e5 cb 40 60 ea 34 b4 ca 84 d8 51 1d bf a0 8d df 62 62 a6 5a 4c 41 54 d4 eb 5c 21 57 b0 eb 13 1f 1f 0a a2 06 b2 0d 04 8a 51 f0 9d 26 57 ef 21 f4 8b 38 7c 34 c2 75 2c 3f Data Ascii: fASk)cx7S1P$&N?(%$4l!YQ&7D=.8\&9{_o(TlS;zcM0t7h&B\Mhe^FsI\10&'gt@`4QbbZLAT\!WQ&W!8|4u,?
2021-11-22 18:40:22 UTC	23	IN	Data Raw: 30 49 2a 26 2b 54 20 e8 20 5c 36 17 61 42 f6 45 e2 a8 1d dc cf b8 4a 7d 3b 32 98 30 0c 0c f0 30 cc 11 02 31 20 1c d4 3f 21 98 af 16 89 31 8b 3c af 20 c3 ca 09 5d 2d a5 38 fe 14 89 8e 2b e9 31 de 05 38 8b db b6 9f 6d 03 3f 32 f4 27 b6 d0 6c 3e 05 93 55 40 b5 0c 03 01 21 b6 82 8a 12 20 ed 70 e2 ae 77 72 45 47 a1 12 ad 52 ab 14 3e 3b 2e d3 1b ed 09 4b 17 b7 7b 3c 67 fd b1 52 30 13 93 17 16 53 58 3a 82 09 59 b3 f3 7b 3c 92 c4 8c 85 d3 87 c4 81 2a f3 79 87 a0 fc ec 27 93 22 91 d7 49 ca 57 f9 14 77 fa d3 3a 7b 06 b3 c5 0d 57 19 a1 fd 13 2f f5 b4 65 0c b2 0b 26 13 55 97 75 12 19 be 3a ae d1 52 ed 9a eb 8b 63 a9 43 6e a7 08 43 0f 0e 97 be 18 37 82 81 63 5a 14 d7 c2 2f 2b 72 fe cf 2c f8 f0 e0 32 27 2a 89 9d b4 dd 93 67 aa 82 d2 4d af d4 5f 59 e2 b7 a6 95 81 0b 26 Data Ascii: 0I*&+T \6aBEJ};2001 ?!1<]-8+18m?2'I>U@! pwrEGR>;.K{<gR0SX:Y{<*y'"IWw:{W/e&Uu:RcCnC7cZ/ +r,2'*gM_Y&
2021-11-22 18:40:22 UTC	24	IN	Data Raw: 39 0c f9 e9 43 a9 8f ec 36 01 60 a4 eb 92 2f 84 44 46 a6 7b 05 55 d0 4c 41 2c aa 11 b8 0c e6 ba 33 12 ab 9d 9b e2 bb 1b 4f 6f 16 72 93 9f 9e a6 4c 8f d6 53 ff cc 88 e7 88 28 a4 a1 c9 1d dc f8 3b 10 7b b0 c5 b0 21 5b fb 0a 6f 31 6d 04 e6 12 70 00 8e 6f 8f 9a 19 38 d8 c9 b9 70 81 19 40 c3 69 9f f3 29 a1 60 72 a7 0d a3 6d bb 71 48 52 f8 df ce 1b 6c e0 5c a2 fe bf a4 48 84 20 bf 5d 4f 92 9f f1 93 88 12 65 cd b3 3c c1 03 dc 7b 9a 04 13 53 68 14 5b df 54 71 5b f8 8b cc 85 93 6d 9f 01 5e 18 30 91 64 bb 2f 6f c3 ee 44 b3 96 11 be bc 4b 56 99 49 8b ba 0c 52 a5 b6 4b 7e aa 7a bd e7 d7 cd a2 50 df b4 ea 56 ac fb dc d7 d1 a7 5d 4e 82 ec 3b 4f 5b 10 dc 77 49 c1 d0 59 90 95 fe 53 1a af 34 4e 7c 12 83 aa 85 ba 52 9c ab 34 a8 e9 f7 03 d0 52 7d a7 40 f0 62 74 02 95 59 8e Data Ascii: 9C6`/DF{ULA,3OorLS(;{![o1mpo8p@i)`rmqHRl\H]Oe<{Sh[Tq[m^0d/oDKVIRK~zPV]N;O[wIYS4N|R4R}@btY
2021-11-22 18:40:22 UTC	26	IN	Data Raw: 8d 7e 67 92 38 32 c7 1c c4 c1 d0 c6 01 a9 26 86 f7 08 a0 f3 39 7a b8 0c 6c 4e 45 e2 28 ca ab 8e b8 4c c0 46 2c d3 6d 41 f7 a0 bd 8e 67 bd b9 9e 4c da 14 85 70 7d 0f 8d 31 00 1b 53 91 6d e0 06 5d a0 6b 50 2b 6f cb fe 52 40 e4 21 3d b3 86 58 a7 12 cb c7 d3 23 20 b2 4d 04 c9 db e2 10 80 34 ba 04 b0 e2 2e 0d d6 62 cc 19 14 d7 1e b2 9b 16 63 bb 2a 21 4a 05 f6 aa 22 55 f6 d3 90 44 dc 30 57 23 c4 66 be 02 89 df 5d 9c 3a ef fc 1d 5c b1 cf 9f d8 94 1f 27 36 a9 4d 46 61 db 3c 33 8e 64 cc 7d 04 a0 f2 b2 dd c6 19 90 d1 95 ca 57 23 77 30 72 ea ff b1 c6 5a 9b 9d e0 65 c2 b1 9f ef 79 34 8d 0d 36 c3 c4 14 ab 98 23 b4 2c 37 7b 3d ac 9a e3 1e 1b b5 66 2a 84 e8 bf 81 a8 f3 e0 0c 1f 59 37 32 f2 2d a6 44 b2 0f 3d c3 84 a3 f0 dc f7 54 1b da b7 a2 41 75 43 7b 90 9b df 7d 85 94 Data Ascii: ~g82&9zlNE(LF,mAgLp}1Sm]kP+oR@!=X# M4.bc*!J"UD0W#f]:\'6MFa<3d}W#w0rZey46#,7{=f*Y72-D=TAuC{}
2021-11-22 18:40:22 UTC	27	IN	Data Raw: d0 e2 99 23 cd 3f 4c 45 26 6f 8f 0e 83 ee d2 61 13 9c 3f 7f 43 fb 8a c7 16 13 b8 04 e3 ef 11 8e 64 96 94 25 97 55 be ca 54 32 20 aa c8 97 8b fc 50 b0 0c 5c dd 49 f5 39 97 ec fd 70 15 eb 89 68 9f 73 d8 bc 78 2d b3 6a a0 75 97 64 2f f0 20 cb b8 01 04 a5 39 46 8b 28 04 05 eb 3b 81 0f 3c 10 2c 6d e7 d6 a2 6c d7 a6 d3 b1 f0 29 2c 6c 39 f2 bb cf 89 85 f6 91 04 1c f5 5a 73 8b 0b ed 6f 2b c0 dc e7 cd ea 58 ec 25 6d ec 31 d7 91 50 85 60 5d ef c1 fb b8 86 b8 dd 46 c9 f7 90 35 e0 6d a3 82 69 02 e5 07 8b fa 00 29 70 21 76 07 90 b7 c1 e3 01 79 24 9a 7d a7 86 7e 17 66 a7 e0 de a2 c5 42 76 79 23 b9 b5 8a d4 4f 57 3d d0 1f 80 d3 98 d8 23 fd d4 0d 5f 45 99 c9 c0 59 ea 0a 40 92 f7 e0 61 61 48 16 48 9d 2a 6e 63 24 c5 1b 7f 6d 3f a2 b5 74 de 91 17 d0 6f 8c b0 d2 bd 1d 1c fa Data Ascii: #?LE&oa?Cd%UT2 P\l9phsx-jud/ 9F(;<,ml),l9Zso+X%m1P`]F5mi)p!vy$}~fBvy#OW=#_EY@aaHH*nc$m?to
2021-11-22 18:40:22 UTC	28	IN	Data Raw: f0 1a 05 fa fd 11 b1 df 9d 8e bc 9a 63 16 86 91 32 b5 51 9b e8 ec 73 24 56 ce d5 20 81 ed 5b bd 72 f0 6f 4e c1 87 23 81 57 d0 82 50 e2 4e 8d 03 56 7f bc 0b 38 bb 4e 97 41 88 ea ec 96 97 2d 19 a0 b3 72 31 74 df e6 c1 ea 24 0e 78 d2 2e 37 7b 23 47 0f b1 1d b0 19 5b 47 41 f6 7c 5d 0d fe c7 31 b9 b1 81 4a 0f 5a f2 b0 93 f8 87 48 3b 0c a6 0a 07 48 8b 9e 69 72 1e aa f3 98 e1 c8 59 9b 8a a6 33 3c c2 10 d1 d3 6f 1d 4d 72 10 f2 ed 3d e6 1a 76 ab 10 9b d9 ef 74 db 6f f9 0b 1e 91 e9 56 68 b9 ef 7c 24 b2 65 b2 0a ca 12 f4 b1 06 a4 63 9d d2 88 a9 3d 76 4e 00 dc aa 75 30 76 7b b2 f0 cb 4d b1 bb 1f 5b 83 f4 e6 e5 bd c8 8d f2 7c 4f 3d 1c 85 1c 5b 83 d0 37 6f 99 22 9a a7 1e 3a 7e 44 6b 70 2b 28 c6 be cb c0 7e 9d a9 bc 2e f5 63 91 9f e7 cf 6c df b3 bb 07 a2 ba 80 9a b0 7d Data Ascii: c2Qs$V [roN#WPNV8NA-r1t$x.7{#G[GA|]1JZH;HirY3<oMr=vtoVh|$ec=vNu0v{M[|O=[7o":~Dkp+(~.cl}
2021-11-22 18:40:22 UTC	29	IN	Data Raw: 11 56 59 4d 73 b8 68 76 cc b1 15 1a 6b 82 4c 0f 8d 83 7b 56 64 a8 ee 54 c5 b7 25 35 0d bf 73 8e be 4e 12 0e 0c 78 08 13 fb c7 bd de 57 97 12 62 de 93 d1 90 ca db ae 14 df a0 25 69 c6 be 63 86 2e 4c b9 92 10 a5 80 e6 68 28 eb ea 65 9a 74 e9 1d a4 c9 97 fc 94 2a dc c1 9f 90 ed 91 37 e0 bd 2d ae 95 d5 ad 92 06 2c 84 95 23 15 34 c0 33 6e be 72 16 97 b2 71 90 a4 48 a9 6a ef 77 3a ec a0 a7 60 d2 20 61 bd 82 b3 6e 30 ef d3 b9 d0 f2 63 1d d8 d7 a6 2b fd e5 a2 6d bb 5e 1e 56 0a e6 fa 84 e8 18 25 07 d1 fe 36 a8 d5 6e c8 ef 47 c6 fb ba 89 cc 9c f9 6c d3 f4 c1 dd ec 2d 88 42 e9 26 b4 68 bb 0f f5 64 af ac 56 a3 f9 36 3f be c3 92 43 4a 54 c1 11 78 2f 17 0e 8e f6 fe 32 53 43 92 ca 8e d1 d9 8b b6 74 68 56 1c f7 53 38 07 f1 ad 4a ad 36 34 5d 26 47 41 e8 a0 95 93 41 31 ad Data Ascii: VYMshvkL{VdT%5sNxWb%ic.Lh(et*7-,#43nrqHjw:` an0c+m^V%6nGl-B&hdV6?CJTx/2SCthVS8J64]&GAA1

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	31	IN	Data Raw: 50 9b b4 64 74 21 bb 45 8c 27 bd 06 67 f4 87 de 52 23 15 b4 80 f3 71 aa 1c ae a5 01 07 f9 ef f9 1f 36 d5 9a 83 e6 f1 c9 29 ee 60 bc d7 ef c4 1e 66 2c c9 17 3b 44 7f 00 4f bb e7 d2 58 b5 c0 7b 75 e7 14 0f 92 62 d7 96 91 27 15 dc 6f 31 2a 04 df ee 95 28 3d 8d 10 dd 1d 85 d7 69 55 39 f7 35 02 93 06 ef 02 25 ba 33 0f 43 30 7f 1c 6e f7 61 a7 e0 01 5b 94 09 40 8a b8 a2 2e 87 6e 89 dc 26 23 2a 18 5d ab 27 35 cc 28 57 2f 55 03 77 87 f5 1d 9e 38 96 5a 8e 55 c7 1f 75 d3 2c b7 dd 5d cc 59 dc f4 d5 9d f8 87 40 18 06 90 6f 11 d7 2c 0c bd 97 ba c9 06 5d 5f f2 c2 db f9 2b dd 68 fe c4 e5 c2 43 0a 86 ff 84 bd ff 82 cb ab 66 3a 8f 2c df f9 f7 a9 24 f0 df ae d3 6c 4e 33 dc 56 5f 14 f5 e7 bd 77 c9 aa 00 90 d0 a7 bd 22 69 70 a8 45 3f f9 18 d9 37 41 1c f7 aa bb 65 9b da 3d cd Data Ascii: Pdt!E'gR#q6)`f,;DOX{ub'o1*(=iU95%3C0na[@.n&#*]'5(W/Uw8ZUu,]Y@o,]_+hCf:,$lN3V_w"ipE?7Ae=
2021-11-22 18:40:22 UTC	32	IN	Data Raw: 09 4f 7b 41 2b c0 7a cd 71 69 b3 dc 7a 9e e9 bb 43 c1 1b 12 d6 ad 17 0a a2 45 c3 b4 84 fd 47 67 ba 50 8e cf d5 9b 67 8f 3f 5f b7 f3 a0 ed 18 86 2c 4c 5d b6 48 78 ca d2 2f 9b 5f 21 ca 1d be 7d 46 62 bc 70 52 fe 7e 8e 0c 60 38 a5 a9 2c 7f d4 ec 5c 67 93 fd 24 7f 04 1d 4c 28 d2 a6 c9 0c 0d cb c5 93 8b b5 99 a9 21 04 2e 16 a2 ca 19 08 62 9f 6d c1 0f 56 9d 97 99 9d 5e 29 5d a3 87 c1 3c 70 58 f3 09 1c 85 f1 14 66 08 a3 6d d6 57 fc 02 ae df c4 0f 90 34 79 e9 25 b2 ea 58 6c a3 d1 86 38 19 91 af 29 60 af 41 45 e5 b7 30 38 55 70 13 7f 84 ca 75 b4 d6 8b 64 52 91 36 9c e1 48 93 87 54 05 07 95 ff fb 20 ac 7e 60 69 9a 23 7f 7e 59 05 79 c6 22 9f 47 b8 92 db cf c2 4e 74 6a 2f 46 5f 9e 1b 89 0b 01 ae 28 74 97 03 52 da 0c 63 ff 91 33 5b 13 c4 4d 62 cc 00 e5 ca 35 2f a5 f1 Data Ascii: O{A+zqizCEGgPg?_,L]Hx/_!}FbpR~`8,\g$L(!.bmV^)]<pXfmW4y%Xl8)`AE08UpudR6HT ~`i#~Yy"GNtj/F_ (tRc3[Mb5/
2021-11-22 18:40:22 UTC	33	IN	Data Raw: 06 86 27 dd 3b 34 35 e0 73 0c 86 4a 33 b4 31 d6 0e af 38 f8 f8 bf 0c 97 f0 5a 0e 06 bd 7c 8a b0 74 b2 1f 81 6e 31 36 c3 61 ef e8 a5 63 8c e9 c6 a3 78 f4 23 4d b5 42 eb 0f 8b 79 8e 6b 0f 56 5e 80 ac 29 3f 27 c4 97 0c 41 f7 f0 30 86 58 5a cf 26 30 da 1c 2d c8 ae 49 37 ce 74 07 c3 79 2b e4 86 d0 62 3a 20 2f 7e 86 0a 3f 2d 45 c4 49 79 eb 9f 25 26 7b 74 3b 32 03 bc 3b ce b4 aa d8 e7 51 8b cc ce c5 3d 7e 81 0f 95 99 aa e3 c0 f3 0a 88 64 a5 84 fe 4c 9c 0b 30 f4 ca 60 a5 3f 13 f1 e8 ee 4e 00 f7 b5 2a 01 21 dd 4d 98 3a 4c 6d 1d 5c 50 c2 0b 55 fa 1b ac 5a 6d c4 07 75 05 8e de a5 60 b6 79 0c 97 92 e0 51 d2 22 2e 01 58 0a 27 3b fc 17 9a d2 e2 81 af b2 e7 bb 0a 9a 3b bd 67 04 7b 67 65 5c 28 71 c7 7d 11 1a d8 10 44 ee d2 4e b4 28 e4 a6 af 03 1a 45 e8 6e 2d 14 17 63 a3 Data Ascii: ';45sJ318Z|tn16acx#MBykV^)?'A0XZ&0-I7ty+b: /~?-EIy%&{t;2;Q=~dL0`?N*!M:Lm\PUZmu`yQ".X';;g{ge\(q}DN(En-c
2021-11-22 18:40:22 UTC	34	IN	Data Raw: f4 50 aa 0c 17 27 94 72 32 41 35 8c 5b e8 89 6e 34 fa 9d e6 d7 4c 72 2f 37 63 4c 68 7d 69 32 86 9c ac 9b 8e a8 b7 85 bd cf a3 8f 4b 75 d5 06 95 0a fc e6 7c cf 06 18 38 e0 0a d0 93 20 b1 41 84 d7 a2 c6 ac 22 ef de bb d9 cc 4f 5a 68 ad 5c 62 9d 61 1f 0c ea 49 be de 90 17 68 e8 5c e4 6e 99 85 f3 7f 82 37 6d 2e 9f 07 da 41 84 b0 be d3 b8 65 31 72 56 f5 b9 7a 8f 69 04 ee df 5b 2b 0c 3c ed 8b e2 d3 8c 94 ba 7f 82 19 5d bf 98 5f 01 84 75 ed fc 7f 5f f5 3a 39 97 77 47 68 22 c1 2b 0f 69 da 3a 43 32 67 24 48 48 ee 7a 31 d8 81 ad 7a 9f 28 a5 66 8d b7 38 69 de 2f 47 a3 a3 ca 37 45 4c 4b f4 fd e5 59 28 dd cb 6c fb 6f 7e 9c d8 a3 b7 60 46 71 ac c1 35 40 5a ea f6 12 4b 40 ba 22 ca 77 72 ff a4 61 95 db c2 93 78 29 c8 69 d8 af 6f 66 5c f1 d7 34 46 8c d1 a9 5b c7 fa 5b 90 Data Ascii: P'r2A5[n4Lr/7cLh}i2Ku|8 A"OZh\baIh\n7m.Ae1rVzi[+<]_u_:9wGh"+i:C2g$HHz1z(f8i/G7ELKY(lo~`F q5@ZK@"wrax)iof\4F[[
2021-11-22 18:40:22 UTC	36	IN	Data Raw: 5b d9 18 72 0c 2b d2 78 68 bc d6 4f 86 cb ce ac 26 63 0d 64 8e f4 91 b2 50 d6 48 58 b7 b1 66 cc 37 7b 9f 13 15 fd fb f0 e8 34 4f 48 fa 10 d6 e3 c3 be 31 10 64 c2 ef c3 da a9 ce 2a 1b f8 af 24 39 37 18 e4 fd 86 c4 0c fd 52 d3 cf cc 94 0e 50 c5 e3 8d 3d e6 f1 44 16 94 ac 47 6e 99 d5 59 25 98 2c a3 72 24 43 24 ea 79 92 88 7d 1c 2d 94 b8 00 a3 86 e1 3f 87 21 21 d7 f6 b1 ed f7 26 e0 f0 7a 32 4e 25 c9 c8 84 c6 64 6c aa 34 2f 99 0a 1b 6d b0 c7 8a ab 77 90 69 95 55 e3 e0 6f 43 48 45 38 a9 0d 96 da ca 3b 1b e2 5c 8c 04 b8 48 6d 38 dd 59 0d 15 10 8d 92 e8 00 e2 36 2a 7d 76 9d 98 5a ac 8b fa be 46 75 ec 05 b0 44 10 1e 50 78 98 05 65 be 0e 22 78 fe 39 9d d4 94 fd 09 b5 39 9c f9 9a ad db 4b 92 df 85 ac ec 40 b5 f6 6d 05 be c9 3c d6 b5 87 dd e0 e8 ab d2 57 60 d7 96 d8 Data Ascii: [r+xhO&cdPHXf7{4OH1d*$97RP=DGnY%,r$C$y}-?!!&z2N%dl4/mwiUoCHE8;\Hm8Y6*}vZFuDPxe "x99K@m<W`
2021-11-22 18:40:22 UTC	37	IN	Data Raw: 1a 56 1e 30 39 cc 75 0d 21 e0 dc f3 51 16 78 13 4d 6f 89 48 c2 50 d4 a4 70 c4 14 25 92 da 44 d5 c9 5a 82 f9 fb f1 31 59 af 42 62 24 d8 e2 42 e4 18 53 12 52 d0 ca 1a f1 85 8b 5a ea f8 8b 60 12 b0 8f c7 d5 6f c8 f0 37 c8 dc ad 71 64 22 f8 30 94 55 67 49 65 12 d7 1d bc 5c eb 8e bf 45 f3 9f 5e f2 72 0c b3 0f ed 4c 65 aa 89 50 cc 1e 7d cd 69 d2 07 1e b5 76 97 68 57 94 39 a3 a8 76 6c 25 51 a6 f3 03 00 3a 48 29 c4 f0 26 1c 2c a8 55 a7 1c 79 38 da ce d6 7e 7c 2c 9d bc d1 ac fc f6 4d a7 54 ea 87 82 52 f8 5d 05 8f 84 64 86 0a 8c 73 e2 e6 0c 26 24 a2 e0 4f 6e ba 72 ed 5a 65 9d 44 eb 57 2b de d2 13 78 94 ca b3 b5 f8 ad 26 02 4d 7b b4 b2 d9 3a 87 be 7a 6d 59 b3 8f c9 18 16 ee 96 33 57 40 7e f6 3e 4b 40 ba 22 ca 79 fa d7 3b 2a f1 af 89 47 d2 3d c8 c6 25 16 b4 d8 a3 53 Data Ascii: V09u!QxMoHPp%DZ1YBb$BSRZ`o7qd"0UgIe\E^rLeP}ivhW9vl%Q:H)&,Uy8~\|,MTR]ds&$OnrZeDW +x&M{:zmY3W@~>K@"y;*G=%S
2021-11-22 18:40:22 UTC	38	IN	Data Raw: 1d 97 44 e5 7a 3f cd 3b db a6 2a 56 3e e6 8d 87 0d e6 97 95 0b 75 f1 79 d3 0a b0 25 63 3e 84 d1 a5 a8 e1 a5 65 bc 22 f9 35 1b e8 36 7b 12 3d 21 16 be c7 8f 95 3f b0 72 64 20 a7 5d 12 1a 5e d3 6d 08 59 51 a6 79 6e 04 2c f0 ac 03 73 3c c4 d9 fd f2 a6 64 74 83 c0 0f 85 a9 90 94 1a 30 9a 98 f0 30 0b 7f 56 3c 20 1c 07 a6 30 9c 35 f2 8d ba 86 0a cc 3b 2b 69 82 79 b5 2e c8 7b 61 42 2a ea 60 70 ce 41 ff cf fc 1f 03 22 74 c4 b9 3c a5 27 2f 7b d0 ab cf 32 89 45 de 9d 8e a5 c2 86 e0 10 b0 81 29 fd ef 77 9b 3e bc d1 1e 38 43 2a 8c 8b 35 a5 de cc 7a ce bd 48 ba 6d 3c 98 e8 7a 26 51 64 59 53 db 11 d5 7e a6 2b d8 ae 3f 88 62 55 80 23 59 c5 f6 8b 05 99 ab 5d bf 98 ef 28 22 93 22 87 8b 45 99 00 10 01 2a d9 ed 25 af b9 4d c5 60 6f cd b6 e9 a7 75 fc 37 e7 0a e4 05 e0 9a 29 Data Ascii: Dz?;*V>uy%c>e"56{=!?rd]^mYQyn,s<dt00V< 05;+iy.{aB*`pA"t<'/{2E)w>8C*5zHm<z&QdYS~+?bU#Y]( ""E*%M`ou7)
2021-11-22 18:40:22 UTC	40	IN	Data Raw: 49 d8 a6 71 79 d3 4a a0 51 e4 ee 69 09 ba fb 7c 05 47 1d 13 dc fc 8a f7 e1 0c e3 4e 9d 10 3f 32 db 7a d0 10 c4 5a 1b e1 e2 d8 1e 48 a8 61 2f 9b 8f 11 5a 67 cc 07 ce 53 9f 2b 23 79 43 84 be 51 67 53 0f 3e 3e 96 b2 dd 9b ec ce 7e f0 30 a8 b2 b1 0e ed a0 c2 4a 74 e8 f6 87 d7 aa 64 15 46 34 16 d2 97 f9 a8 15 63 ba cf 8f ae 48 86 f8 76 17 6f d9 a2 15 df 8e 80 4f 3a 66 d8 5c dd e5 79 8f c0 98 63 ed 7b cc 5c 41 c3 04 a5 51 26 cc b9 6e 6f 43 29 c9 56 59 55 12 8e 5f 5a 51 61 39 d3 ab 8d 1c 0a bf 0b 35 59 ee 33 43 73 d0 62 6f b6 fc 59 70 56 9a 69 c5 ee 87 61 21 45 07 d3 29 a4 56 6b 39 54 41 26 37 4b 92 28 15 6d bb 32 e4 93 74 bc e0 1f 95 9f eb 5b bf 6c 8f 57 0c 9c 3e 29 93 87 26 37 fb 48 3e 92 98 ac 27 31 69 9a f8 bd 37 d1 05 0d bc 22 9f 41 b9 52 1b a6 6a 7a 74 18 Data Ascii: IqyJQi|GN?2zZHa/ZgS+#yCQgS>>~0JtdF4cHvoO:f\yc{\AQ&noC)VYU_ZQa95Y3CsboYpVia!E)Vk9TA&7K(m2 t[lW>)&7H>'1i7"ARjzt
2021-11-22 18:40:22 UTC	41	IN	Data Raw: 54 12 60 9a f1 4e 87 ee 69 ac 8b fe 66 ac c4 5d 3f e5 e8 90 1b c5 da 8b 92 33 0c aa 94 0a 38 88 f4 58 d5 1a 9e 5c 26 63 df f9 f5 b5 11 a6 66 ea 7c 57 f1 d9 47 63 77 7b 74 40 88 47 12 68 cc 26 27 31 fe 2a 97 8b 78 32 4a d1 9b fe a9 bb 74 ae a6 ea ac 49 a0 48 a8 ba 5d 18 d9 a4 16 5c 38 df 92 cf ee a9 8c be c4 17 4b 69 8d 30 3f 8e 15 43 46 61 4a dc 6c c1 e9 07 b3 00 b4 7b b9 54 86 7b 1b d0 0e 7e 7d 9b 28 b1 0b 4f 42 bd bc 9b 36 6e 90 ff a4 60 f1 77 c4 27 b8 3d f3 89 01 ef 05 16 85 cb 45 89 cc 53 51 cd 00 48 12 e7 eb 1b 55 28 32 63 2e 4b a1 12 97 06 a2 ac 47 70 d6 83 1d 98 7c 72 e7 cc 7c 6b 98 88 8a ab 05 20 a2 56 ff 98 9c 35 07 fe 55 ea 1b 53 47 6e 3b 12 25 26 30 cb 88 95 07 96 78 98 aa 69 d5 22 fd 87 01 1d 35 81 12 58 0b cf ba ff 7d 1e 6d 4e bb 4f 65 5c ec Data Ascii: T`Nif]?38X\&cf|WGcw{t@Gh&'1*x2JtlH]\8Ki0?CFaJl{T{~}(OB6n`w'=ESQHU(2c.KGp|r|k V5USGn;%&0x i"5X}mNOe\

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	42	IN	Data Raw: eb 08 34 e5 f4 5b 49 f8 d6 0e 05 12 cf ac a2 c9 53 5d 53 99 61 22 eb 60 39 8d 2c f9 bc 58 2b d3 2a 77 05 2c 42 ed 33 65 12 07 3e da 80 55 ed 88 54 9b d4 d2 68 ea b8 17 64 5a 15 e6 c9 a4 d3 b3 41 d0 55 a7 23 f8 6a 1d 14 ec 05 ea a0 fa 85 f9 03 4e 9c 22 bc 3e 8f 04 6b 1c b4 ae 61 4c 75 4e f6 03 77 5c 5b a8 d9 e3 ea 07 c2 cc 50 8d 41 55 ef 5f ad 74 04 e3 5a 64 08 94 48 ec 17 0c 8c af e1 5c ba 4a 99 ef d7 c7 42 33 93 34 c8 bf b4 4d f0 f6 23 cd 85 49 99 a2 f3 69 57 3b 4c c8 39 82 1b fc bb f1 05 96 5d f0 ce 33 7a 1d a4 83 58 e8 60 a3 ed fc 4c d7 2e e8 6f 6c 77 ad ab 02 68 d8 f5 9b 79 e3 05 33 ea 58 e5 01 a9 f4 3d 9c d5 52 85 60 92 f8 a5 1a 48 cf 3a 8e 6c 3b 79 6f ca e3 d0 b0 47 f1 46 e7 07 8b 03 a9 e5 39 ab 9a f0 01 b3 df 31 c9 f4 e8 6b 9a 57 60 f7 44 35 02 45 Data Ascii: 4[IS]Sa"`9,X+*w,B3e>UThdZAU#jN">kaLuNw\[PAU_tZdH\JB34M#IiW;L9]3zX`L.olwhy3X=R`H:l;yoGF91 kW`D5E
2021-11-22 18:40:22 UTC	43	IN	Data Raw: 50 0a 3c fc 9a a9 1b c2 c7 d6 ef 25 1d 60 93 2c 58 0b 71 56 81 74 69 98 53 54 59 c0 32 6d db 2b 26 eb 64 49 1e 81 0c 12 6f 1a fa 5b f1 0b ff 1a 28 98 9c 5f d8 84 b5 91 d2 7f 87 44 9e 09 4e 04 27 bf 26 6b 91 eb be 11 c7 11 38 a7 78 2f 9b 7f 00 c5 cd b5 da 29 d1 c4 a0 bd 56 31 a1 5d ec 5f d6 54 be 45 1c e1 f6 44 e2 40 d9 a6 23 35 44 b1 45 3b 68 e4 ed 60 ec b6 4a 17 14 b9 74 18 26 18 25 1d 86 bc 08 30 77 a9 54 f2 e4 0c 4e 57 2d 2e 43 36 02 b5 d1 f9 05 ad 62 3d c1 48 e1 2f 77 10 37 c4 cd 7f 83 5a 04 38 d0 f5 18 18 c3 ad 0c 49 f1 5a 9d d8 01 d1 bc 22 ea 91 ef 22 10 c2 c2 4d da c3 56 f2 af 9c 62 a5 22 1d 50 60 d5 54 bb 6d 38 ee 88 92 bc 7a f7 2d e8 97 15 5e 3a 82 50 8e 67 9e 90 c9 6d 3b 54 25 be c0 a7 fa ef 74 bd 8b ee a7 4c dd 57 66 85 01 b2 41 ac 12 f8 7c 8e Data Ascii: P<%`,XqVtiSTY2m+&dlo[(_DN'&k8x/)V1]_TED@#5DE;h`Jt&%0wTNW-.C6b=H/w7Z8IZ""MVb"P`Tm8z-^:Pgm ;T%tLWfA|
2021-11-22 18:40:22 UTC	45	IN	Data Raw: 0f d4 9a e1 61 6a 20 3f 89 64 44 23 07 8c f2 17 a2 fb 93 6d 05 3e 66 4d 27 c7 12 d5 95 ec ea d9 22 30 7f 8d f9 44 05 26 1b 18 3b 8a 03 c0 e2 0b 52 4d ef 59 3e d0 01 09 1e 91 47 aa 34 7a d8 10 69 b3 72 34 c9 9c b3 68 a6 d3 a3 8d 93 b0 1d 30 57 c3 db c6 ba 53 67 6e 4b 31 5f e9 9e 80 ee f1 6b a7 66 c5 66 b4 5d f6 8b df 41 84 66 54 e8 a4 57 5d 9b 06 92 f6 f5 ad 60 07 dd 3f e2 47 d2 44 60 4a 62 c0 90 1e 4e 18 b4 f5 1d 76 ff b8 46 61 54 a2 65 59 bd 59 49 4b 6a 9a 60 ba fe 50 de 71 45 dc 23 cf 92 fb 92 73 47 c1 0f 56 40 80 d5 91 51 1c 79 4c a2 7e 4e 29 78 d6 c1 68 24 2d f3 fa fc 58 92 ac 1c 46 ba 8f 5a 80 2b 0f 29 66 6e da 71 02 11 db a3 9a 29 fd c1 79 ee cd 60 e4 ee 80 09 5f 09 de 21 7b 67 45 98 dd 51 a3 5b 35 3b 5c 91 3b 2f 73 4b 68 78 fe f9 f3 a0 0f c0 68 44 Data Ascii: aj ?dD#m>fM'"0D&;RMY>G4zir4h0WSgnK1_kff]AfTW]`?GD`JbNvFaTeYYIKj`PqE#sGV@QyL~N)xh$-XFZ+)f nq)y`_!{gEQ[5;\;/sKhxhD
2021-11-22 18:40:22 UTC	46	IN	Data Raw: cb 1f 61 d3 2f c8 1f 38 24 5a d4 4c 06 b1 ac fb ad 03 3d 38 3e 6f de 6c 60 ca 2c 93 2f 8e e3 ed 31 6e e0 ed c4 54 46 a2 6d 50 6e 2a c6 ea 19 72 87 cf 02 87 7d 74 1b 02 0e 33 56 5c b0 ea 31 6c f5 b5 91 b1 ed 1e bc 22 7d 3f 4f e8 36 7b 14 ae 8c 84 76 38 9a 75 a7 b8 03 6b 97 68 f7 f2 4a 51 64 93 30 f3 40 a9 47 ac bc 08 a0 a3 5c 04 69 e4 89 ab 76 2b c9 d4 73 cf b8 c1 d2 87 4a 1b b4 be 08 84 11 32 99 d6 46 61 1c 23 40 1c 16 d6 b3 8d 31 ff 47 92 f7 b3 e4 06 5d 59 27 4d bb 96 83 39 7a ad 6f 1d f1 fe 9d 6f a4 c9 0f be 27 43 b5 4d e5 02 7d d0 bd 27 55 cb 45 76 23 f1 12 6a 86 8a 12 d4 30 a1 0a 5b 77 9b 2e bc 77 ed 70 fa f2 fc ca bc b1 7b 90 1d 8c 42 ce cc 9b 80 67 fd 76 dd 8f c8 d2 17 ff e2 8a c5 35 d3 55 ea 1b 25 ad 2a c4 07 75 a9 a7 42 9a a0 f7 79 87 38 a4 bf 93 Data Ascii: a/8$ZL=8>ol`,/1nTFmPn*r}t3V\1l"}?O6{v8ukhJQd0@G\iv+sJ2Fa#@1G]Y'M9zoo'CM}'UEv#j0[w.wp{Bgv 5U%*uBy8
2021-11-22 18:40:22 UTC	47	IN	Data Raw: f1 ea d1 dc 97 85 c2 52 6c 12 79 5c 6c d5 f6 21 84 8f 28 3d 77 17 34 8b f0 01 65 aa 6e fc 7a a7 05 cf e2 4c 07 4d 25 ef 2c d0 2a 50 3e d2 8e 8d c6 a2 9b 49 c3 fd 82 03 2a e9 bd 1f c0 ef 41 b3 3d af d3 0d 35 24 6a 3a 6d 16 1c 52 40 17 a6 7d 6f 4c ce 7a c0 17 9a dd 85 1d 30 2b f8 47 cf 3f 8b 9a 1a f1 82 50 46 26 06 3e 43 44 cc b4 40 27 9b c9 7e c7 76 56 74 d0 64 7c 2d 12 22 92 ea 11 91 1d 50 eb 20 54 3c e9 50 c6 b6 67 72 ed a9 40 20 15 e8 b4 96 f7 76 ff ba 4e 95 7b 2c f6 76 41 c1 34 7f 03 b2 7b cc 28 50 e6 00 81 81 93 f1 69 8d 10 f7 ab 11 52 a9 ef 5a f8 7d 10 59 5d fb 90 93 b1 d4 be fa 7f 97 f8 bb 77 0a e8 f5 92 26 63 01 17 04 ba d8 76 7b 9b 05 99 0d bf 64 88 75 59 65 ca 60 0e 93 af 2b 60 6e 9d 25 a4 ea cf 96 5d 40 e0 85 16 95 51 13 a4 a2 5c b5 1c f8 24 45 Data Ascii: Rly\l!(=w4enzLM%,*P>I*A=5$j:mR@}oLz0+G?PF&>CD@'~vVtd|-"P T<Pgr@ vN{,vA4{(PiRZ}Y]w&cv{duY e`+`n%]@Q\$E
2021-11-22 18:40:22 UTC	49	IN	Data Raw: 97 f4 31 78 5b 42 a4 c0 8c fd 24 1e 86 ea e6 78 36 9e 38 db 8c 91 d1 79 79 2f ce 2b 8f 3d c7 e8 78 21 e1 e9 49 0f 1d ef 8e 1c 3b 74 e3 93 25 47 71 c0 32 6d af b8 3d c7 6b 90 f1 bc 41 c2 87 82 a2 2f 43 5a fb d5 63 67 63 b7 10 7d 1d 6e a6 3a 22 64 ca 76 19 70 17 bd 36 77 91 7d aa 11 c7 11 38 a3 19 02 c3 68 1c f2 7f be b9 0c 81 d3 84 8a e4 32 c2 40 a0 5f 5c 3f 7a e0 0c d1 5a ba 1d cb 1f 23 27 e8 69 72 41 4f 1c 00 be 08 f0 b5 c2 62 45 75 97 f5 97 59 25 98 17 09 a9 b6 ca 56 43 a8 4d e4 06 d6 a6 9a c8 7b e2 3c 3a 3d ac 31 57 81 56 2b 12 91 9f 84 00 b0 86 f4 4d b2 33 cc a8 4b 93 dc 48 c5 89 f5 0e 4d 6a e0 8a 12 6c 60 9c 95 ef 77 21 72 c4 e0 12 4e 15 8e 14 5f 53 2e d3 1b 96 38 bd 18 33 96 54 e0 bc 76 dd 53 14 3a 95 99 1d 5c b1 09 d7 55 ea 1b 16 b6 15 85 07 fc 15 Data Ascii: 1x[B$x68yy/+=x!I;t%Gq2m=kA/CZcgc}n:"dvp6w}8h2@_\?zZ#'irAObEuY%VCM{<:=1WV+M3KHMjl`w!rN_S. 83TvS:\U
2021-11-22 18:40:22 UTC	50	IN	Data Raw: cb 63 cd 45 3b ad ca 0f c4 f5 7f 75 ac a8 23 d7 ef cb 08 e1 d2 28 6c eb 53 f6 89 82 52 8d fa c1 1f bc f7 cb 86 a5 fb 5e 94 26 a7 ad 27 5a df 68 13 57 5d 57 42 ce cb c2 f5 86 18 23 af 40 54 db 08 c5 ac d5 6a 2e 9e 00 9a 71 48 bb af 7b 31 6d 96 eb 29 46 01 ab ef b3 65 73 28 d1 43 d9 94 e1 b8 8d ad 95 36 27 fd 9f b4 bd ec de 2a 15 e6 08 7e e9 31 6c 1e ac bb c2 3d 98 ed 4f ba 61 2c 22 d4 67 d4 73 55 eb 57 d6 05 63 78 ad e2 de 93 37 ab e9 5b 7b a7 d5 3c 4a 16 72 0d 9f 9e a5 b0 8f 06 f1 ff cc 8b e4 ac 28 Data Ascii: cE;u#(lSR^&'ZhW]WB#@Tj.qH{1m)Fes(C6'*~1l=Oa,"gsUWcx7[{<Jr(
2021-11-22 18:40:22 UTC	50	IN	Data Raw: 5f eb 52 a6 30 fd fb 04 86 59 bf f2 c9 a1 ea 51 a6 a3 e4 49 85 f3 18 b8 f0 a9 9b 9e ad 65 22 ff 86 4c 28 e7 bd b1 31 4f 68 13 d9 12 03 80 79 4f e6 6e 1f fa 13 f8 ad 57 a0 f1 8c 03 9d 75 48 bc a7 bb d9 a5 d6 c3 92 ac 3f 0b de 1b 0f cd 1a c2 c8 96 ab 68 13 df 15 f5 14 4b ce ca 9b 77 ea ae 8b 6d 0c ac 0c f8 ff 5a e0 e3 52 25 a8 99 af ee 9a 57 bd 3f 19 bd 67 51 31 88 de 8d 49 0c aa ec 49 da 6a f4 ed 66 af cf 94 a4 50 37 d7 a8 63 d7 a6 73 a5 19 b4 c1 f7 0a 9e 81 3c 9d 24 64 5c 89 b8 2f 2d 0d 33 f9 02 91 ee 27 56 de 04 2c bd 6c 92 20 26 af 21 32 b9 1f 46 39 52 09 67 fd ec de 70 f7 6a d2 40 63 85 3b c1 c7 f7 89 44 1e 81 9c cc 57 9b 6a 68 69 ee d3 28 08 41 58 d8 6d 47 37 74 bd fb d1 22 72 45 57 53 74 fa 2d 33 e2 fb 97 a8 7d 4c 66 04 c2 29 46 76 49 9b 19 59 ae 71 Data Ascii: _R0YQIe"L(1OhyOnWuH?hKwmZR%W?gQ1IIjfP7cs<$dV-3'V,I &!2F9Rgpj@c;DWjhi(AXmG7t"rEWSt-3}Lf) FvIYq
2021-11-22 18:40:22 UTC	51	IN	Data Raw: e8 a9 79 2b 6f fe d8 d2 5a ac f6 ad 9e e2 c1 ef 31 de 47 fe b7 8c 7c ca 78 08 d7 3e 7f 86 4d fc a4 d0 7f 8f 03 48 a9 99 1d 46 a5 c2 86 01 e2 64 2f 00 10 19 02 aa a5 16 5d 91 2b 5a 79 37 35 40 0e 2c e5 01 e6 bd 9b df 3c d0 40 fd 76 54 9b 94 51 d3 d7 98 aa 4f 92 9c 40 fe 69 ed 32 a1 0d 3a 7e 56 78 4b 0a 54 06 f2 48 8f 74 e7 50 d2 7d f3 38 13 91 9e b9 a9 f6 62 39 9e e0 b8 e5 3c 01 e7 13 04 10 37 f8 c8 2f be c4 34 db d0 46 04 1a d8 40 9e f3 ca 75 70 5a 5e 7d e6 c3 93 f9 bc f8 69 7c fd c8 83 0f 4d a6 43 5a f2 2d a2 9f 4a 66 70 41 32 f2 01 dc 69 31 92 73 27 2a 0c 69 41 37 e9 58 55 7c c4 a6 53 a1 a3 e1 63 cb eb 6a f5 78 67 74 c8 79 fa cd 7e ce 8f 08 46 e5 d6 b2 8e 29 65 38 ce 92 87 1e 0e b0 fd d2 37 d3 fd 71 28 c8 7a 06 02 d0 e3 c0 f2 30 ac 6f 3d b5 02 ed 0c 4a Data Ascii: y+oZ1G|x>MHFd/]+Zy75@,<@vTQO@i2:~VxKTHtP}8b9<7/4F@upZ^}i|MCZ-JfpA2i1s'*iA7XU|Scjxgty~F)e 87q(z0o=J

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	52	IN	Data Raw: e8 5c 0d ea d2 53 63 86 dc 10 78 3a 98 0b 2d cb 1a a7 ec 0d 6e 0f 21 64 b0 26 95 aa 7e 2e f4 aa 5e f3 c1 0f 56 10 d0 7b 4a 92 e5 75 b3 d7 92 38 79 b8 2a c7 89 f1 be 3b 3a c4 b3 6d 53 97 01 17 0c ad 95 03 f5 25 86 d6 f9 b7 15 57 e8 f2 65 a2 b0 2a 4a 22 3f 6b 48 35 32 90 43 bd 2c 72 d3 bf 5b c0 ca 15 e0 2f 8f d0 01 5f 40 24 45 fc 60 87 be 22 6c 59 b3 5a a8 31 5d 27 d3 91 e8 60 92 f7 a5 15 e3 84 eb 87 00 3d 03 66 f0 d6 dd 7d 78 5a ca 60 15 09 23 e2 52 a8 07 dd bb 8d c4 a5 63 c8 71 b7 0c f8 96 7c f0 67 75 b4 aa 92 81 5f a0 69 24 d5 c1 ee 27 56 de 06 2c d6 38 ff 37 c1 bd 40 9b 3a db 3f 8f 6d f6 1d 86 41 7e 92 58 7d f6 45 64 92 2e e8 75 fc 89 7a b7 95 54 33 fe f8 4b cc 7e 2c f2 13 fb 35 ea 73 cc 69 0e e0 41 cc 1a b8 69 c6 1e 1a 87 0c b8 c0 f7 97 68 ac 99 97 f1 Data Ascii: \Scx:-n!d&~.^V{Ju8y*;:mS%We*J"?kH52C,r[/_@$E`"lYZ1]`=f}xZ`#Rcq\|gu_i$'V,87@:?mA~X}Ed.uzT3K~,5siAih
2021-11-22 18:40:22 UTC	54	IN	Data Raw: 0d e3 84 d4 61 bc 56 74 c9 15 9b de dc 38 2b b4 8d 18 25 e9 8c 5f fa 8a 0a ba ed ba d6 2a 38 47 53 08 12 c0 af 1b 62 79 01 96 a5 6c dc 60 6c aa a3 39 18 b4 0e 28 8e a2 b2 fa 7a 81 d7 6a bf fa d7 0a 6f 49 f1 a0 a9 0d 77 86 11 1a 3b ee 8e 73 42 e7 47 08 24 ea b1 52 6c f8 19 b8 e8 00 75 e8 ab c3 63 d8 a6 3f 84 da fd ae f8 8a 06 fc 87 21 28 1f cc e0 98 05 6f 1c f6 06 90 ae de 35 a8 12 14 ed cf ba ff b4 ca 9a 59 0a 75 65 b6 ac ea 4b 99 27 65 9b d5 71 c7 9c 19 b3 b9 58 38 2d c5 da ac 93 3f bd 3f 03 2b 8d 53 05 94 6b 43 37 60 e7 59 18 37 e6 35 44 4a fc c6 20 de d4 ff 37 2b 17 2d 92 2b da 44 c6 be 8a 45 72 48 88 e6 36 1f 80 24 a3 1e b1 db 32 e3 9d cd bf 87 60 34 0c 06 32 e0 fa 15 08 c5 91 ee 87 94 6d 22 4f ec 18 5e 2d 92 e7 26 c0 82 46 87 55 df 20 f3 74 32 dc 16 Data Ascii: aVt8+%_*8GSbyl`l9(zjolw;sBG$Rluc?!(o5YueK'eqX8-??+SkC7`Y75DJ 7+-+DErH6$2`42m"O^-&FU t2
2021-11-22 18:40:22 UTC	55	IN	Data Raw: 48 f4 86 31 9b b5 bc 06 94 1c 5e e0 0d ec e3 99 e8 e7 f5 66 43 75 10 a2 42 87 bf 7b b0 6c f9 3b a3 fb 77 8f 7f d8 eb 0f 1d 21 e6 6e 4b aa 0f dd d3 f8 7b 8e 92 55 2f e3 86 6d a4 14 0f e6 80 eb 59 12 88 74 87 ee 91 78 67 fd b0 48 53 6b 29 b6 a4 d8 06 c8 f1 82 60 c0 09 65 5d a5 bd e0 ee 7a 3e 37 c9 98 e5 32 f0 1d d9 d4 13 1d 9c 47 21 14 05 ee c8 57 1a 7d b4 ce 8e 3c 87 be 7e 6d 59 b3 66 2c ee 24 ac 7e 8f 2c cf 85 b0 89 42 49 dd 89 2a 70 49 0c 71 2a 74 dc 18 7a ca 36 9f 96 9a d0 08 bf 2d 11 8b de 8a 48 59 9c 4b 5d 0f 16 ec 3b 49 98 24 37 b4 41 29 79 9f 1a 62 22 4c 95 8b bf 22 aa 37 f1 db 30 ea df d9 af 6d e0 46 e0 48 f5 b8 c2 58 4c 04 d5 8c cb c0 d2 e1 ca 3c fc 26 30 5e 68 9e af 67 0a 9f fd 10 cf a7 0f 2c 8e 54 92 32 9f 0c c3 9f 9b 4a a9 76 17 53 c6 ce 14 fe Data Ascii: H1^fCuB{l;w!nK{U/mYtxgHSk)`e]z>72G!W}<~mYf,$~,BI*pIq*tz6-HYK];I$7A)yb"L"70mFHXL<&0^hg,T2JvS
2021-11-22 18:40:22 UTC	56	IN	Data Raw: 89 73 5c 1a 68 0f cf 5b 9a 0f b2 89 9f 18 59 25 13 0b 57 06 c1 63 d3 22 86 d4 69 4b a9 c5 c8 86 7b e2 03 fc b5 69 a6 df c2 3e 7d ae f7 9f 04 06 6e de 7f 83 5a 42 b1 2f 0a 16 95 c4 c0 f4 f4 0e a5 95 ee 8c 13 e5 eb a5 d0 03 27 cd a3 0e 55 fa b5 19 f2 fc 4f f5 21 57 f5 1c 8c bd 95 7e d8 d0 c3 b3 76 54 47 0c d4 16 fd 1d d1 7f 5e 33 03 67 56 58 da dd 8b 07 75 d3 b1 c4 81 52 f6 79 87 0d fe 69 15 36 ab 25 3a 1d 47 1a be 75 20 46 7d 37 1c ed b2 b1 44 f7 7c 10 03 98 6d ba 6f 04 48 4d 03 75 db 02 1a d8 04 47 d6 6e bc 60 d7 f3 6c 30 71 98 22 8b 05 c7 50 43 37 58 9f ac c0 76 6b f4 2d be fc db 19 de d4 22 f6 42 d7 94 da ad 32 27 1e 31 ec 89 36 e9 58 55 57 51 9f f4 5d 1a 41 06 f4 4e ff 0e 76 e6 bc 67 5b ee 8f 34 0d 02 19 cb 23 e5 05 4c ae a6 6b 10 44 a5 a8 38 92 72 ee Data Ascii: s\h[Y%Wc"iK{i>}nZB/'UO!W~vTG^3gVXuRyi6%:Gu F}7D|moHMuGn`l0q"PC7Xvk-"B2'16XUWQ]ANvg[4#LkD8r
2021-11-22 18:40:22 UTC	58	IN	Data Raw: 9b b9 67 40 bd e2 db b0 37 ab 0a 76 3b 0e f3 12 f8 19 65 04 cc ec 17 d1 22 56 00 75 d3 5b f1 a5 29 d0 a6 14 2d 41 7b 68 9a 60 5b a1 a8 21 84 5a 44 9a 83 28 04 e8 db 4c 45 f5 56 10 d3 30 c8 37 0d 11 ff 42 d3 b1 b1 31 53 68 2d fa 12 03 2f 81 ee 91 bb 39 c1 52 f8 d9 cd df 0f 94 6e 7b 85 cd 15 d5 21 a0 8d 25 f9 19 91 2a 8c 90 9f a3 cd e5 b7 bd 2c 26 d4 61 45 70 dd 49 40 5b 35 e9 4f fa 10 61 ef 76 93 f3 9e e2 6d 59 b3 b7 08 d1 30 ac 69 10 50 cf ac 8c 2d 9f 0e b5 18 5f b5 b6 0c 52 59 7a 5d 10 04 1d b1 1f 96 cd 2f 90 62 a0 00 e3 4a 05 8e 5a f6 4b 4a ce ab 7b c6 c4 16 68 cb a1 7d b1 91 d2 60 5d da 61 1c 26 82 f6 3d 1c e8 14 d4 66 92 2d af 05 3e 46 e0 4f 87 e0 7e c2 2e 4d 8a d2 83 d8 ad 86 6b 85 ec e0 c7 f7 87 7c 82 f7 b3 76 40 40 aa c9 61 3b db 84 08 35 14 57 be Data Ascii: g@7v;e"Vu[)-A{h`[!ZD(LEV07B1Sh-/9Rn{!%*,&aEpI@[5OavmY0iP-_RYz]/bJZKJ{h}`]a&=f->FO~.Mk|v@@a;5W
2021-11-22 18:40:22 UTC	59	IN	Data Raw: 83 04 e2 28 ba d0 cf b8 3e 5b 35 83 db 31 7e 7c b1 bb f8 2c b2 49 f3 dd bf 09 58 67 b9 38 ca 75 06 1a 8f 69 a6 e0 b6 0d c5 b8 9e 84 1d 0b 4e 9e fd 61 36 37 cc 3c 53 7c d3 a0 9b d3 1d 8b b2 4d 02 c3 63 4c 1a 09 ef 55 b2 05 7c 6c 49 b3 7a 63 a6 eb 40 61 ee 77 9b d1 95 2c 55 ef 06 7f b0 ee 21 c6 8e c6 e2 73 30 5c 17 3c 68 8f 41 84 ab ef ef 9e 33 ef f5 aa 44 7d 9c 3d 1e 1a ac 32 6d 12 56 9d 8f 82 34 fa 95 37 0c a9 ea bd 84 00 5f 65 24 ae 27 cd da 36 d8 49 66 ff 19 07 11 39 fe 20 4f 72 6b 93 98 f8 30 7b a9 25 55 9e 53 e8 aa c0 62 a5 57 cc 7b 25 ca 96 f3 ab 5f 8e 67 2a bb ec 9c 05 37 84 2c fb 20 c8 1c 6b 79 ed 1d 74 6f cb 66 77 22 28 82 6f 58 2d 0b 37 4c 5e be fe 87 52 3c 70 c3 1c c4 6f 21 98 7b 99 63 69 cc 6a f5 ac 5c 6d 77 7e 47 32 01 fa a6 c4 0a 4a 09 05 1a Data Ascii: (>[51~|,IXg8uiNa67<S|McLU|Ilzc@aw,U!s0\<hA3D}=2mV47_e$'6If9 Ork0{%USbW{%_g*7, kytofw"(oX-7L^R<po!{cij\mw~G2J
2021-11-22 18:40:22 UTC	60	IN	Data Raw: 2f 6e 87 52 ff 7b bd 5b dc fa 0c 1f 97 e2 35 14 81 be ba 99 07 34 41 c7 57 5e ca b5 16 98 d8 e6 52 e8 36 62 f5 86 57 f3 82 a4 d4 85 87 a6 71 24 bd aa 81 42 d1 33 c9 b0 78 0b b4 54 96 5e 3c 04 e4 2e 03 6d 5a 56 1f c2 b8 c5 7a 08 79 3a e2 ca 1c 69 7c 2e b5 0c 0c b8 fc 97 ab d9 92 ac 12 48 26 e8 db b8 a6 cc 60 b5 9d 8a cb 41 f3 c7 f7 ce 49 b2 92 5f 26 77 c3 b6 30 cd 5c f7 9d 3c de ec 1c 9a d1 35 e9 21 d0 67 31 02 93 cd 0c 17 dc 6c 90 43 3f e0 e7 0c d7 fb 05 71 17 da c8 fd 30 2d 82 26 02 ca 90 9f 35 9c 9e 60 66 a1 08 c6 6d 2c bd 65 60 69 46 ff 90 6a a0 b8 1f 1f fb 73 0a 25 13 18 ee 5b fb 28 8a e9 17 bf f9 bd 29 56 ab 1a 62 24 4f 69 ea 17 5a bd b3 05 aa 2b 03 dd f2 47 bf e7 41 1e 6a 3f c5 ce b9 4c 04 01 19 e0 1e 14 f2 64 e6 a4 ee 75 f0 ea dc ba 3b c1 8d f8 bd Data Ascii: /nR{[54AW^R6bWq$B3xT^<.mZVzy:i\|.H&`AI_&w0\<5!g1lC?q0-&5`fm,e`iFjs%[()Vb$OiZ+GAj?Ldu;
2021-11-22 18:40:22 UTC	61	IN	Data Raw: 45 e4 c8 69 a0 a3 b4 b2 d8 bd 86 bb 38 12 cb 95 8c 91 71 02 d8 35 28 c1 3f cb 00 c3 f0 5c 9c 3f 4a 0b 19 0e aa 80 c7 18 ee 4f 39 8b 03 20 95 78 6f 5b 51 7b a5 bd 73 88 87 f5 89 12 47 ce 3d 2b ab df b6 9f 8b 3d f3 bb bf 45 36 49 f0 22 5d 18 2e cf 2f 8c ac fd 00 49 cd 82 4d d4 2b ad 5c b1 78 0f ee 18 fc d0 cf 56 a7 77 26 b4 c2 cb 92 1d 8c 36 19 60 7a 6f 54 02 b1 11 e0 14 bb 55 ff 96 86 b3 cf 9b 66 38 92 e1 e6 d5 4d 52 99 df 24 3f bb 25 f6 79 47 4c 38 eb d4 d9 23 78 fe 66 0d 23 70 42 7f 8e ba b2 11 b9 b3 b1 44 92 df ad ad ea 92 51 ca 72 f2 34 cb d8 ff 15 95 9d b0 4e 3b fa 2a a5 eb 1a 95 6f 03 e2 95 bc 12 16 85 f9 24 85 a2 3c d2 b2 93 84 9f a5 99 72 aa 4b 03 fb 3e fb cb ef 1b e3 32 7e 24 81 7a 4c 22 6d 98 21 f9 b6 c0 53 2b a0 3a 3e 41 5b 6a f5 78 62 80 b4 ca Data Ascii: Ei8q5(?\?JO9 xo[Q{sG=+=E6I"]./IM+\xVw&6`zoTUf8MR$?%yGL8#xf#pBDQr4N;*o$<rK>2~$zL"m!S+:>A[jxb
2021-11-22 18:40:22 UTC	63	IN	Data Raw: 47 9f ba 34 d6 ba 27 b8 d9 d8 4b e3 8d 4e 75 42 2d 71 8e f3 d4 16 d6 de 16 b0 be 7e 65 b8 a2 50 0a e6 3d 0e f3 c8 4a fc d9 08 d6 13 63 84 e2 71 fd 1a be 4e 61 ec 42 f6 59 37 2e 62 c4 1e fa 98 43 e2 a8 72 8f 55 ae b3 87 19 45 6d 4c bc d5 7b 26 51 d3 e6 d2 5c 9b 27 7a 14 a1 71 85 0c 66 c1 68 f7 66 c9 07 65 e1 6d d8 47 b1 63 8f 42 0b ea 07 a6 ba de c0 0e 6b a2 9c 5c 65 a2 c2 f5 cf 6c 2c 14 ea e0 3b 91 93 bb 6f 89 0f d1 34 e2 74 60 97 4c cb 10 09 52 7b 9c bb fd 69 fb 43 71 6a 1d 4c a9 6c bb a6 fa 69 b2 f7 6e b9 3a 2d b4 df ee a0 9a a4 e6 9b a1 51 c5 8b c5 94 ed 20 2f e6 8c 2f de 72 d7 bc 08 b7 fc 0f b6 80 18 e3 88 80 32 98 e0 0e bf 07 4b 60 9d f4 f6 8d a9 35 43 91 ee 2e 82 41 20 37 13 2b 14 54 11 af 1d 54 b9 1f 94 46 89 92 a1 fd ec a7 bd f7 6a da 69 bf 7d 77 Data Ascii: G4'KNuB-q~eP=JcqNaBY7.bCrUEmL{&Q\'zqfhfemGcBk\el,;o4t`LR{iCqjLlin:-Q //r2K`5C.A 7+TTFji}w
2021-11-22 18:40:22 UTC	64	IN	Data Raw: d0 b9 31 85 42 a2 79 7d 93 32 aa ce 2a 79 51 24 63 c1 19 5b df d4 32 37 03 4f 05 13 a9 b7 d2 c8 46 49 da 44 56 eb dd cf f4 9a 0f 92 89 c7 7a a6 da 15 0b 6f 65 e2 a6 a9 54 f2 6e 1c 8d 08 d1 c5 d7 f0 a7 6e 05 0d e1 69 55 87 da 48 a8 7f ac 4d 88 fc bb b1 b5 a1 47 0d 62 f6 78 90 f8 85 ba 27 51 fb 99 4f 49 43 46 5b 85 c0 ef fc 8e 9a ee f4 12 42 96 87 e8 4f e7 5b c3 78 10 8c bd 18 90 9c 95 32 fd ff 41 a4 c9 87 17 a6 de 09 b1 6e e2 b9 26 1e ac 32 11 f9 7b 1c 14 71 cb 56 46 a0 76 03 59 f8 e4 50 3a 7b 7a fe 4d 47 da c2 01 82 71 33 3f 04 6b 72 c4 40 9a 48 3d b3 ee 42 4d be d8 f9 d7 bd d0 17 55 97 9d 33 13 9a 3f ee 76 81 90 e8 93 c6 ec dc b3 54 01 0c bc c8 83 36 4b b9 34 aa 90 62 a9 b1 ba 86 55 26 f1 83 0e 57 7b 7f 46 b1 df a3 35 74 6c 68 33 70 21 72 3b 90 6b 90 7b Data Ascii: 1By}2*yQ$c[27OFIDVzoeTnniUHMGbx'QOICF[BO[x2An&2{qVFvYP:{zMGq3?kr@H=BMU3?vT6K4b U&W{F5tlh3p!r;k{

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	65	IN	Data Raw: 50 bf af b2 d0 60 8f e5 0e d5 06 95 ca c8 66 77 f3 c4 3d a0 d1 c0 85 9f 38 55 62 32 d6 64 f6 70 1e 8f 1d 65 70 8d a2 53 9e cb d7 8e 1e f8 07 78 e2 09 a1 08 b8 e3 05 a0 d1 1b 6d 71 48 b6 cb ed b0 d7 e5 ee c1 3d 3c df 62 07 85 d8 4c e0 a2 e8 85 ae f3 fb 21 8f 20 d7 0b 4d 6b 9a 30 8c f5 04 92 99 91 b3 d7 92 b1 fb 38 83 84 4b a1 ed fc fc 08 87 60 98 f1 04 8a 9e dc 50 a0 e1 9c e0 d6 44 c6 8c d6 8c d7 20 66 3b 4c 59 f0 24 c4 d2 a6 98 6e 5b 61 3a 88 d3 67 d2 2f 85 fa 55 a4 e1 9f 0d ad cc 6b 31 4f 06 61 26 3a a0 9b 73 ff 67 f3 a1 27 50 3b ce 0b b4 06 5a d9 76 c4 6f 8d 24 3b a8 25 ae 32 49 1c 81 ee be 59 1b 85 90 9e e7 7c 5f 3c 83 8f 4a 04 fa 70 7b b4 1c c3 4f 81 ea e7 83 7e 27 44 10 a6 e0 fb 94 c3 e5 d7 3d a9 e2 08 22 7e 15 b0 16 1a 12 34 88 3a f3 0b 59 fb 09 1f Data Ascii: P`fw=8Ub2dpepSxmqH=<bL! Mk08K`PD f;LY$n[a:g/Uk1Oa&:sg'P;Zvo$;%2IY|_<Jp{O~'D="~4:Y
2021-11-22 18:40:22 UTC	66	IN	Data Raw: 09 7a 07 92 62 d7 c9 15 2f fd 0b b3 a8 ae 21 af 39 93 70 47 a0 90 48 ed 02 a7 a2 09 f3 29 13 ff 21 7c eb 72 c9 b0 51 69 bb 84 17 13 79 eb 09 40 36 8e 0a 40 be 9a 6a bc f8 d7 62 b5 88 ef e8 b6 11 0d 32 56 3f d1 12 c6 8a 9a c6 8c 96 89 1c 4c 66 5d 34 86 31 78 3d 3a 25 f5 07 99 37 5b 5c 3c 5f e6 da 3f ce cd 43 f5 86 20 69 4c e9 82 6a e0 34 9d 21 95 86 98 b5 e1 6b c3 ff f0 29 0e 65 45 53 c0 3f bc 9f cf 15 1f dc d0 98 36 c7 59 c4 cc 37 2e 51 a7 3f 23 79 47 cb ff a7 ec a0 1a 4c 54 46 a4 ec 09 fc 38 2a 8c 4c 14 0e 28 e2 95 70 33 3e 7e 5c c6 5c 57 d6 45 ee ac 13 5a d9 28 51 06 32 7c aa 19 a4 77 38 12 72 87 14 d7 dc d9 a7 df 8e 85 e1 7e 9a fc c3 d9 f4 12 3a a5 63 1e 10 dd 6a 90 68 7e 5a fe 98 65 a6 e2 e8 ee f7 17 96 65 12 23 25 30 c8 7b 0b 29 5b 5a 80 4e c3 f7 e2 Data Ascii: zb/!9pGH)!|rQiy@6@jb2V?Lf]41x=:%7[\<_?C iLj4!k)eES?6Y7.Q?#yGLTF8*L(p3>~\\WEZ(Q2|w8r~:cjh ~Zee#%0{)[ZN
2021-11-22 18:40:22 UTC	67	IN	Data Raw: b1 b5 ca eb 1c 72 1c f1 a7 ac e3 34 05 96 86 8f 9d 94 28 cb 02 f6 cd 58 ed 99 4a 42 51 7a 11 45 36 10 16 54 62 b9 95 f3 21 8a f8 83 77 6e 18 78 88 02 4b c4 f6 bc 22 99 b2 68 80 74 95 ca a8 fa 3f 97 46 16 bd 29 6e 9e c6 70 36 9e 38 af aa e5 e9 89 18 18 2f d4 70 b6 fe 60 4e 96 19 60 9f 2c f1 6c 62 ef 60 ce 9e 31 fd 95 56 31 b9 a1 00 86 71 80 64 e6 ff 41 b5 2a 61 35 8b 5b 85 c8 52 06 3f b8 2e 48 07 78 f8 65 b1 c6 27 43 dd 7d fc 87 00 40 26 60 86 5b cb 2c 3c 9a 20 c4 1d f1 87 9b 6e 3c 3a 1c 00 35 a2 dd f0 cd f9 26 5d 12 f7 5f 2e f9 c3 f0 4e c1 0d ba 69 0e 72 83 27 1b 8c 72 41 49 da 40 56 33 b8 cf f4 9c 0f 4e 89 26 0a a6 da c6 8f 71 89 31 4c 57 df e2 6a e4 c5 fc 01 48 8a 7b 21 05 2f 96 8b 73 de c2 87 cb ca b5 9f 6d 5f c7 cd 0b 18 39 65 0f 6a 02 1e 18 c3 2f ac Data Ascii: r4(XJBQzE6Tb!wnxK"ht?F)np68/p`N`,lb`1V1qdA*a5[R?.Hxe'C}@&`[,< n<:5&]_.Nir'rAI@V3N&q1LWjH {!/sm_9ej/
2021-11-22 18:40:22 UTC	68	IN	Data Raw: 8a 13 e5 fd bc 83 6b bb c7 04 4c 5e 7b af 8f 76 08 bc 05 f3 58 b4 97 f6 06 89 73 96 49 ca 3e c6 6b 6d b2 80 a1 fa a0 e4 75 eb 8d 9b f7 7f a3 b5 73 74 8d 7d 5b 9d e4 0d db f9 46 24 7a b7 1d 04 3a 8a 76 f2 a3 d8 e4 52 18 00 06 03 5a 06 9f ac d3 ca d5 1c 5e a1 9e c0 55 c1 ab c2 f7 cb 54 b7 71 ed ce 46 0d d9 75 31 48 39 b2 76 8c fa 14 75 8b ec b4 79 52 39 f5 44 5c df b6 34 f1 dc 95 86 45 c4 2f 65 a2 c6 59 7b a4 ee b9 6e ef 4a 6a fa 66 4c 11 dd 26 f9 4b 31 1e 56 1e 2b 8d 73 49 fc 57 56 4b 28 b2 0b 4c 22 5e 86 f9 63 3a 13 76 a0 c8 0e 70 c5 dc 43 55 bb c8 a4 29 7b 8e 9b 00 5c a8 d9 d1 60 35 41 0a d9 a6 34 04 61 d9 fc 1e 1b ff bd 16 72 7b ea 1b 6b 98 6b 29 76 08 4f c9 12 c1 d4 5f e3 b2 b8 30 c0 b1 07 c2 3b 5c 57 4b 00 28 16 a2 a3 e4 41 95 4b ab f7 07 a9 ef 58 f8 Data Ascii: kL^{vXsI>kmust}[F$z:vRZ^UTqFu1H9vuyR9D\4E/eY{nJjfL&K1V+sIWVK(L'"^c:vpCU){\`5A4ar{kk)vO_0; \WK(AKX
2021-11-22 18:40:22 UTC	70	IN	Data Raw: b1 cc b5 f9 23 d2 e6 6d 82 02 99 f4 3c 0b 75 82 10 df dd 65 20 bc 5e 11 1f 0a ca 9f 2f 6d b7 2a fe da 5b ed 12 df dc 57 7a 27 f1 46 1a 58 73 6a ae c3 a9 de 8a 6e 96 f9 2f 95 ca ac 92 fe 8c b8 a4 a1 1f e3 bb 0d f7 ba b8 12 56 39 00 6a 02 d9 6b 04 61 2c 96 17 20 2d 18 2a 2f a4 02 08 ae 07 2f bc fd f1 fd 04 29 e1 60 be ae e2 9a 72 1c f8 db e6 26 ac f7 1d 80 fb ae 93 3b 49 5e 1a f5 7a 0e 41 c2 0a f8 8c 59 f1 79 24 01 bf 6f 61 b7 f8 9f b5 c1 d2 43 e4 45 ca 50 b2 70 17 b5 bf 93 f4 80 fa 13 c7 65 1f 4f a7 22 01 97 1c 6c 5e 38 10 64 a4 a9 83 fc 56 31 a1 ef 58 48 8b 9e c8 e7 6f 4e ad 1b 2b 83 d9 12 0c ee 4a 7c 56 49 86 b4 be 8d 30 44 1c 46 f8 5e fd 5d 57 d2 ed 70 d1 a2 8d 31 d2 d3 6b 0d 2e b2 f9 8d 73 ed fb bb bc 45 5c 31 1c d9 b8 d3 3e c3 29 37 eb 9a da 81 ca 6f Data Ascii: #m<ue ^/m*[Wz'FXsjn/V9jka, -*//`r&;I^zAYy$oaCEPpeO"I^8dV1XHoN+J|VI0DF^]Wp1k.sE\1>)7o
2021-11-22 18:40:22 UTC	71	IN	Data Raw: 60 f3 2a 0d cb f3 13 8a 1b b3 fd 19 b9 7b 1d 9d 91 e0 23 ab ec 39 34 29 a1 6a 33 d0 35 48 80 fa 0d 69 ba 0d 26 92 7a 3b fa ce 53 7a 25 95 29 ad 76 9f 14 5a 9a f4 5d 82 d3 2e 86 7e db 10 7c ac 77 17 80 ef f1 f8 a3 f7 17 13 e3 5f 42 40 ce 7d 16 00 80 23 3d 3d b3 13 6c 12 b1 78 10 6f f5 9e 82 cf c0 02 de 30 d0 c8 c3 d5 21 ec 49 36 7a 4d da eb f3 a4 ea 46 51 fc 2c f8 02 8b ec 60 71 f9 c8 32 88 e5 3b e0 dc fc 8c 59 b9 9e 30 b6 6a e1 4f 15 78 0b e8 89 ba 34 6d fc eb e7 0d 9a ae e0 40 38 ff 7d 7e 61 57 d9 27 bd 44 6e 62 82 81 ef d8 8b 66 e2 cd 50 25 38 bb e8 45 32 3a 8c c5 ec a7 59 0e 37 a9 89 f2 f9 9f ba 91 db 7b 00 ee 3a c4 89 52 eb c8 3c c2 8d ee 4f 7e d2 4d 01 60 5c 68 ec 65 11 9b fb e1 01 32 0b 99 ea d7 e2 ce 40 d2 34 17 1e fa b8 43 e2 a8 aa 49 5d a6 7e e8 Data Ascii: `*{#94)j35Hi&z;Sz%)vZ].~|w_B@}#==lxo0!I6zMFQ,`q2;Y0jOx4m@8}~aW'DnbfP%8E2:Y7{:R<O~M`\he2@4CI]~
2021-11-22 18:40:22 UTC	72	IN	Data Raw: cb 02 c4 58 3b fc 92 bb 76 0a 8a 82 c9 c1 45 a0 ef 32 88 f3 92 71 54 91 c2 9f d9 f0 49 75 5a f8 a8 04 cc 67 76 01 41 41 67 3c 37 6f e5 16 05 82 1d 37 55 23 e5 fd 4b be ed 11 e3 0c 0e 3c cb 49 0a a7 8b e5 d0 35 f9 c4 c2 9f 2a 0e 5a f7 4d 08 97 7d b2 ca 42 7e 19 29 73 89 23 52 70 15 da 5b 30 d3 c7 31 f6 1f e5 81 7b 6b 2d 75 d4 f4 fa 36 87 01 96 8c 9c f0 2e 10 05 12 ba dc fc 64 fb ae dc 3f 47 65 af 18 c6 4d 8e c1 02 4d 41 4b c1 75 f7 5c f1 f2 62 01 87 98 76 af 89 b4 b5 18 1f a5 5c 7c 62 1d b4 06 96 3e 48 5f 26 5b 5f 2c 30 9a 23 18 c2 8d e0 66 b4 2e 58 48 06 0e 28 44 7b 01 a9 8e d5 56 0c 5f b6 6c 47 59 e4 00 b4 4d 61 b8 ad a6 c8 31 bf 85 8d 04 7c b7 8d c8 b0 6f 55 d5 4a 46 34 97 bb 0f 72 13 bf e2 0e 56 8f 56 26 36 27 0c 87 5d 2d 2e 45 3e ea d6 87 f5 e9 d9 d9 Data Ascii: X;vE2qTIuZgvAAg<7o7U#K<I5*ZM}B~)s#Rp[01{k-u6.d?GeMMAKu\bv|b>H_&[_,0#f.XH(D{V_lGYMa1|oUJ F4rVV&6']-.E>
2021-11-22 18:40:22 UTC	74	IN	Data Raw: 72 be 50 d8 df d4 87 b0 4e d3 7b 39 3b fc 26 f4 87 40 22 80 0a a8 c2 aa 38 46 66 21 08 cc 6b 98 19 db ed 8c 87 79 9f ec 01 c1 e6 5d e4 ff 9f 4d 29 1b e6 04 7f a4 e4 69 2d 10 28 21 2b 5c 24 a7 74 ad bd a4 53 fe f2 db 11 86 d8 26 d3 8e 27 f6 46 67 40 0a 7f 55 ae 04 89 0d 4e a6 3d a4 fa a3 c8 cb d9 f8 57 74 84 99 2a 8c a4 a6 c7 fb 8a ad e8 cb 08 47 1d 63 52 ba 82 7a 2c 86 12 36 6c a5 13 da 10 44 dd 15 1d e4 54 24 b1 81 b8 97 19 2b 86 e5 fd a0 67 f2 52 71 69 58 cb fa 00 c1 5b 65 b8 64 57 52 2a c9 c1 7f 65 9b 15 06 f2 31 4b af 7e 06 0a f3 2a c0 1f 2c 2d c7 68 27 7a ea b9 e1 07 70 f5 3a 14 a5 c9 5d f3 8c 9b 2d e9 47 c6 55 5a 1d b7 a3 f6 ad 64 16 be e6 06 81 4a b9 e8 4b 9c 9d 49 f1 8c 73 a6 b5 51 b5 e4 d6 13 bb 28 4f 81 41 8a 23 8f 4b c8 33 58 ba 43 e8 e7 e0 f8 Data Ascii: rPN{9;&@"8Ff!ky]M)i-(!+\$tS&'Fg@UN=Wt*GcRz,6lDT$+gRqiX[edWR*e1K~*,-h'zp:]-GUZdJKIsQ(OA#K3XC
2021-11-22 18:40:22 UTC	75	IN	Data Raw: 4e 77 43 8d c3 2a f2 d4 01 9f d4 10 90 79 ed 85 28 9f c7 f7 31 7c 4e f8 a3 72 a8 46 77 d4 d7 2c 64 27 85 8b 9f d6 be 59 06 3f dc 03 02 2f de d8 9b 16 f5 34 b4 d7 af bd e5 12 c9 91 7a a1 a1 a2 ae 18 41 10 54 96 b9 c2 fc 21 8a 48 2f 02 1b 69 d5 52 b6 c1 33 2a 7c 6f 0b 3b 4d 90 5b d2 3d c9 eb 69 e5 3e fe 33 76 78 9e 2c f4 cb 92 cc cc 4f 6e a4 81 7b e1 8e c3 8f 02 c7 c1 b4 9d 94 15 36 4f eb d1 71 1c b3 42 55 32 27 28 5e 2c 66 3e 06 04 86 81 40 94 37 a0 12 92 0c 8c 9c e6 e1 78 8d dd 92 6b ee e2 08 76 71 9d 9e f4 c3 f8 22 f6 b1 04 e0 bd 3e 97 2b 88 57 42 6a c9 26 1c a2 21 38 c6 1c 49 cd 5f 65 15 68 2c fe c1 dd c4 a1 65 f8 29 a5 87 f7 58 0f 8b c1 85 bc 1b 9b 11 c3 b8 42 ac be 4f 56 77 eb 83 1c b1 e7 3b 40 46 61 4f 01 33 25 f2 44 38 54 f6 0e 82 56 86 d4 c8 04 5d Data Ascii: NwC*y(1|NrFw,d'Y?/4zAT!H/iR3*|o;M[=i>3vx,On{6OqBU2'(^,f>@7xkvq">+WBj&!8I_eh,e)XBOVw;@FaO 3%D8TV]

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	76	IN	Data Raw: d4 bb 6a 59 be 60 f0 46 2d 98 a4 b2 4e d0 53 a1 a3 59 6c 53 58 6a 53 70 53 f5 72 f0 56 64 e6 b7 05 19 2c 6e ee de 2f d7 59 7e a0 69 1f 2d 7d 27 03 34 43 70 84 21 11 e8 a9 11 70 f3 91 3b 0a c4 d8 68 6b 0d a1 47 0d a0 42 2c 2f 40 35 fd 1c ee ad 29 7f ac 42 5b 62 4e 79 42 a7 40 52 f7 17 39 ce 41 c7 85 86 60 99 67 c1 57 6d 8d 92 00 93 ea ec ee 99 d5 39 20 2d ca a8 72 68 e8 4e c8 41 0e a8 c4 b4 34 45 06 0f 5b be a4 7c 98 36 43 f9 27 fd 56 4a 5d f2 0f 35 cc 90 0d 5f d3 57 b1 dd e1 ae fb 6f 8c 66 b5 47 90 f1 7e e8 89 72 ed cf fd cf c0 1f 65 56 b5 cf e0 62 d2 a1 b8 07 2e 27 f7 e3 d8 7d 4b c7 7a 26 79 6e c0 3d fb e8 31 13 35 43 ce 5f 23 b3 ae b4 a5 73 38 35 82 0b cf 9b 06 64 22 d5 15 05 37 72 ca 0d b5 93 09 a0 06 af cc d2 9f 3e 28 4e 2e 1c e2 bf 6f 98 93 b7 74 36 Data Ascii: jY`F-NSYlSXjSpSrVd,n/Y~i-}'4Cp!p;hkGB,/@5)B[bNyB@R9A`gWm9 -rhNA4E[[6C'VJ]5_WofG~reVb.'}K z&yn=15C_#s85d"7r>(N.ot6
2021-11-22 18:40:22 UTC	77	IN	Data Raw: a2 5f ec d6 eb df 59 ac b8 0e a3 a6 1e 0a ad 02 72 84 4b 82 5f 7f 85 31 9d 05 2c 77 ee 75 00 8b cd fa 2c 0e 3f 57 ef 77 0f 4f 3b 0b dd 08 35 14 ca 3b f4 ea 83 56 04 df 04 a6 15 57 5b 70 91 14 33 1d 54 97 a8 91 97 f9 05 a1 be a7 e7 be 10 54 62 b9 07 f7 21 8a 13 1e 15 2f 95 b0 39 81 d6 38 70 0e d5 a3 3f 77 70 e3 87 3f a8 55 e2 25 7b ea 0c 5f 91 9e bb a0 d9 9e 38 a9 17 66 4c 57 fb 53 8d 7b 02 72 24 d6 98 5e e2 9f 41 ea 15 07 37 d7 12 74 fe 47 33 85 dd 4d 7f 65 b8 d6 c9 4d 64 49 ff 43 55 2a 86 77 8b 5b 85 cb 7a be 4c 53 9c 48 92 f5 dd ae 59 be 6f ea 4a f7 b1 8f 68 bd b4 77 d7 ff fd 11 b1 dd 51 ca 31 7d ef 0c e3 79 32 79 a7 ed 5c d8 f2 74 51 f7 59 38 7c c8 2e f1 c3 93 2b d9 7f 02 fa 10 ba 0d 36 47 3e 08 7e b0 c5 39 fb 00 a0 61 5a 9a 07 b2 ea d0 07 b1 9b 9d b9 Data Ascii: _YrK_1,wu,?WwO;5;VW[p3TTb!/98p?wp?U%{_8fLWS{r$^A7tG3MeMdICU*w[zLSHYoJhwQ1}y2y\tQY8|.+6G> ~9aZ
2021-11-22 18:40:22 UTC	79	IN	Data Raw: f3 c0 b9 77 7b 25 84 1a 4b 0d 58 e3 64 aa 24 f9 82 37 c9 3b c8 c9 f2 db 6e 53 5f 62 79 fa f8 a6 18 8f 43 54 87 c8 8f c2 3e 3d a2 02 9e cd 5b 01 9f 91 e0 2b ee 20 ee a1 d2 90 bf d7 69 bc 55 87 7c 34 e4 f7 f9 76 75 eb 7c 60 cd 53 05 3d b5 80 eb 13 a1 e4 9c 2b 0c 53 7a 97 c1 0d 88 4c 65 88 53 62 4b 0d 79 99 bb c2 33 e1 c0 69 72 6d 76 f2 78 62 3a 5a e9 0c f7 82 52 5f 60 ab ec 11 8b 48 76 2d 09 97 6a 85 49 8a 08 cb db 63 1a 26 76 c4 58 df 1c 0a 53 d6 ec 8d 78 4f b5 67 dd eb f5 af 25 51 dd 6f 58 2b 6d 59 44 3a 95 86 43 b2 bc 71 eb 3c af 7b d0 95 41 e3 dc 75 16 60 fe 4c 8a 23 a5 cc d9 30 7a fe f3 d0 67 d8 b4 30 bd 54 3b 03 ba 05 98 f0 5e a5 47 16 43 a9 9b ec 44 5a c8 3c d8 4b 80 84 d2 6c cf 3a 8e cc d4 ce 55 81 02 86 35 41 0a 12 83 20 f6 23 16 96 32 0b ea ac 16 Data Ascii: w{%KXd$7;nS_byCT>=[+ iU|4vu|`S=+SzLeSbKy3irmvxb:ZR_`Hv-jIc&vXSxOg%QoX+mYD:Cq<{Au`L#0zg0T ;^GCDZ<Kl:U5A #2
2021-11-22 18:40:22 UTC	80	IN	Data Raw: c5 da 94 dc af 89 61 e0 9c 59 20 cb ff 72 d4 81 df 8f b8 aa 7c c8 5e 1f 60 ad 0f 67 f1 8d 8d 83 58 c6 0f f2 8e 81 07 22 38 8d c2 ff f4 e5 39 65 57 05 2b f6 c0 d3 2e 89 7c 09 c4 4e f0 49 75 5a f8 aa 01 11 c1 2f de 9d ba 4a b7 57 e2 bb 1a ed c9 4b be 10 b5 6c 5f e7 54 3b 69 2b 51 79 96 22 fe a3 6b c9 91 96 fb fe 81 c8 1d f3 fd 35 b4 fa 03 92 7d 49 b8 12 52 39 02 33 50 88 94 7b 59 a2 e5 46 80 66 af 99 35 6d 42 a5 27 9e 7a dc 6b 6f c1 f2 5c 96 ba 41 5e f5 28 55 1d 12 b8 60 ee e9 38 84 45 e9 13 44 e5 8f ba 10 df eb fb 3c 3e 0d 79 7e 94 0a b8 34 6d 24 1b 8c 3c 3f aa eb ca 90 72 e4 7d e1 a3 3a 63 be bd 8a 14 3f 09 87 2e 4d b4 9d 70 f1 72 6b a4 31 f2 fa 08 b9 25 c0 d3 84 88 ef d6 af e0 7c b1 f2 0e db be a5 89 79 8d 0a 84 ba 2c 30 e1 48 cb b2 4f d1 b8 3b c8 84 3e Data Ascii: aY r|^`gX"89eW+.|NIuZ/JWKl_T;i+Qy"k5}IR93P{YFf5mB'zko\A^(U`8ED<>y~4m$<?r}:c?.Mprk1%|y,0HO;>
2021-11-22 18:40:22 UTC	81	IN	Data Raw: b3 4d f6 f4 c8 59 5f 37 f1 21 5a 99 72 b2 c9 d7 8e 85 f0 a8 b4 f1 b0 d5 d8 5e ca 38 3c bd 9c 70 fe 57 c4 6f 2f 1b a0 3c 0e 45 5a 6a f5 93 ab 7a 37 0c 83 c4 64 76 46 4b 46 6e 22 12 87 b0 4e 4c 4e e7 a1 ae 3c eb fb 65 48 6f 50 f0 b4 b5 2d 06 89 75 2b 30 df bf e1 8b d5 1f 94 53 0c 37 d3 ba ae 00 53 b2 df c6 57 8b da 9a d0 de 2f ff 1a 42 08 35 9c f9 ac bd 04 42 a7 76 f2 a5 d8 18 81 51 65 7d 2b 82 90 61 03 ec 95 8c 48 76 5f 92 30 ea 52 14 35 f7 64 80 a5 d7 5e c5 7c a6 ad 12 ff 54 c1 4d ff ef 50 9f 53 25 03 1e 7d 72 39 93 44 5c e3 6d 99 44 85 e3 04 ab 8a 2f 25 49 c2 50 84 d2 10 0c ef 19 56 60 e2 5c c5 e7 f1 2c e1 7d ce 38 f2 35 33 26 8f b4 30 bd 18 39 03 ba de 22 01 5e 58 4b f6 26 83 9f 42 44 27 c4 c4 d8 4b 5d 36 27 c8 21 81 70 64 7c d1 b7 5b d0 12 c9 be f5 3a Data Ascii: MY_7!Zr^8<pWo/<EZjz7dvFKFn"NLN<eHoP-u+0S7SW/B5BvQe}+aHv_0R5d^|TMPS%}r9D\mD/%IP V`\,}853&09"^XK&BD'K]6'!pd|[:
2021-11-22 18:40:22 UTC	82	IN	Data Raw: 6c 95 18 cd 0b c6 ff 7d 6c 39 29 6c aa 48 8a 76 1c 44 a4 c2 86 b9 e4 b1 bb c0 f9 3c 89 64 ad 87 ad 9f 8a a6 98 d4 90 dd b8 1c 6f e2 01 f8 e8 63 a1 75 9f 15 49 ae ee 9b ba df 5a 5c 5c b7 cf bb bd 00 e2 52 cd c2 49 4a 8d be 40 3c fb ef 7c 34 5f 8f 37 c6 af 2d af 3d 06 1d 47 1a 8e 14 68 74 44 8d 90 5a 3a f0 44 92 d7 bd 14 22 ff 43 c8 72 78 49 03 bd eb a9 68 62 d8 13 bf 3a 25 71 81 73 89 e9 cf 67 c1 0f 4b a8 0c 43 dd 0c 86 89 59 ba ee 85 9c a5 eb 6f cb 6c d3 9a 6d f7 dd 83 71 9b 94 66 a1 cc 38 10 de e8 61 df 8d 6b 1d e1 2c b7 7a 7d 47 59 1e 47 23 4b 1f 15 f3 f9 64 03 72 fd 49 46 04 15 bb ba e3 cc 6f 67 6c a6 d2 ed 3f 06 69 bc 6f 78 21 ac 69 ba 4d 26 92 5e ac 03 94 ed 6f 6b 1a 7d 79 83 1e 1b 49 10 15 d2 8d 6e 2e 7f 32 80 35 0d d6 2e e4 0d 51 a1 f8 a3 22 b1 1d Data Ascii: l}l9)lHvD<docuIZ\\RIJ@<|4_7-=GhtDZ:D"CrxIhb:%qsgKCYolmqf8ak,z}GYG#KdrIFogl?iox!iM&^ok}yIn.25.Q"
2021-11-22 18:40:22 UTC	83	IN	Data Raw: ed 18 84 59 0c 3c 8f 81 90 06 c8 8c ba 28 50 dd 85 d7 0e 2f e4 bd 97 e8 b5 34 ab 09 20 a5 66 34 97 8d 70 93 ac 36 04 cf ad 52 05 eb f1 79 ec 65 58 da 69 46 93 a3 e0 62 c4 13 c0 24 b2 77 42 69 cd e5 5c 32 5a 1e 27 60 95 c5 35 ed 59 6c 9b ef ca f2 48 7d ba 89 5f 8e 22 07 ef 21 c6 0f 67 c2 b1 ac 96 65 2b 55 a2 09 d6 9f cc d2 f2 09 7e 7d 7b 7a 5a 6d 1a 8e 3b ed be e2 5e 40 62 e9 76 d1 1d 67 d8 00 3b a5 ac a3 d0 49 a5 ec 4f 0c fe d4 db 4a be 91 5d 9f 3d 75 62 f0 6f 9c e9 eb a1 20 1b 48 2b 14 54 94 ab 3c 01 4d 1f f7 51 b0 7d d5 87 cf 62 80 13 6a a6 86 9f da fd a8 b3 48 0a 03 b3 2c b7 76 74 f8 18 9f 7e 2c fa d3 40 40 d2 7c b8 44 ee 3f f4 1b ba 69 8d ba 25 9d 7c ce cb d3 f2 20 ee 66 57 97 4f 41 c4 a2 76 48 c8 e6 fd 82 3a 06 3d 21 fe 3e 0e 00 23 9d b4 32 8d b7 92 Data Ascii: Y<(P/4 f4p6RyeXiFb$wBi\2Z`5YlH}_"!ge+U~}{zZm;^@bvg;IOJ]=ubo H+T<MQ}bjH,vt~,@@|D?i%| fWO AvH:=!>#2
2021-11-22 18:40:22 UTC	84	IN	Data Raw: 0a 37 a8 dd 57 bf c6 93 c4 6b 38 c5 8b 51 33 a3 c4 cf 7d 0f d8 83 ee a5 40 9a 00 88 e2 2e ff fe f9 53 e7 83 e8 e0 ae 77 64 f9 c8 ec fe 42 9f fd 78 ee 34 2e d3 1b 1c 01 e8 ec 61 44 98 12 bc 76 05 ef 74 59 5a 0b 98 95 35 06 68 54 ea 1b 27 33 c3 3b 57 71 dd 3c c3 88 45 0f 91 3c 65 fa e4 69 8f da 77 7a 4f cb 57 7a 71 38 7e ea 1a 74 49 f3 b1 2e 1e c9 21 ec 11 46 bd c8 5a 86 f0 7e bd de 5a 13 4e b0 17 be b1 24 49 9f bc d4 6f 71 12 51 12 12 b9 00 37 8d f8 9f 90 fe 76 6b 86 15 ae 9f 37 16 de 7a 7e 11 47 ae f9 6d 1c cd d8 f2 11 9d 6e fe 92 67 9f 22 4d d1 ac 5f 1a 5d 06 04 d2 6a f5 04 20 bc 3b 81 93 46 94 0d 02 ec 14 3e b4 48 75 5e 96 1d d9 19 d3 50 7c 42 d3 8d 19 8e 70 55 0d f4 74 b4 8e 10 23 3a 70 cd 27 9f b8 13 1c c4 78 12 ef f7 b4 fe 21 00 a4 f6 77 ac 50 3e 0b Data Ascii: 7Wk8Q3}@.SwdBx4.aDvtYZ5hT'3;Wq<E<eiwzOWzq8~tI.!FZ~ZN$IoqQ7vk7z~Gmng"M_]j ;F>Hu^P|BpUt#:p 'x!wP>
2021-11-22 18:40:22 UTC	86	IN	Data Raw: 79 2a 3b 05 20 07 4b 22 5c 57 aa 47 a1 da 68 0c 5d bc 85 c7 9b 3e f0 dd 53 df fa b6 2f 2f 9a ec 5c 54 ef 67 21 65 84 68 f7 66 0d 28 87 ed 59 d6 5e fc 54 73 53 d1 d4 d4 40 0d 13 35 01 15 dd a5 28 6c 29 b1 48 6e ff 72 16 65 51 46 ab af b5 a0 aa 8d 67 09 c1 ca 30 1c 2d b4 7c 8f 54 e4 9c 55 51 92 87 26 3c 3f f0 54 07 96 bb fa e2 b2 e0 61 44 73 82 ec bb e3 8d 68 43 8a 92 7e 69 89 6d 44 4d 3a ed b8 d1 ba 25 e8 c5 d9 a3 dd c5 63 ec 33 82 62 b4 3c c5 6f ec d1 b0 65 a9 34 eb 1f 03 d4 d2 b0 16 43 83 7d ab 62 a6 55 9b 2a 02 be eb 54 00 b8 aa 14 ca 5e 1f 87 de 9a 7c 65 98 2d 93 08 ff 58 67 9b 05 b7 16 79 08 fd 9f 8e b7 7f 33 23 1e a2 4d 8e 57 fa d6 f7 ca 14 86 be 67 e2 e1 c1 5b 27 06 96 14 25 06 f3 76 cd f6 ed 2f 69 ec 99 1c bc 54 18 18 fe 1c cc e8 39 ef a7 86 c9 55 Data Ascii: y*; K"\WGh]>S//\Tg!ehf(Y^TsS@5(l)HnreQFg0-|TUQ&<?TaDshC~imDM:%c3b<oe4C}bU*T^|e-Xgy3#MWg['%v/iT9U

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	87	IN	Data Raw: 86 a6 a1 0a 0d a0 65 cc 93 f6 62 f4 45 60 74 ce 92 b3 88 a4 1f e9 4a 75 c4 b9 b1 45 39 c4 88 a6 49 8b bd 57 4b 76 0a 8d c0 ce 86 01 5f f7 6e e1 e1 e9 26 73 e9 8a 5f ed 98 08 79 3f 91 68 ec cb 90 48 07 51 99 df 68 34 67 fd fd 11 18 37 84 40 74 0d d1 63 86 ee 18 e2 92 f1 ce 6d f6 84 b7 52 99 7f e7 ef 08 20 d7 ec 31 0c e3 31 dc 87 75 00 c2 bf 37 f2 82 71 45 07 f0 dd 4d e6 bb 0a f6 38 bd 67 f8 c8 3f 06 fd ea 71 2d cf 24 d6 9d e6 9e fb 32 da 34 37 6a d4 6f 30 67 ad 43 ed 62 d4 ea 45 8d 4b 33 a6 c8 3c 29 88 27 aa c1 b9 77 a6 f7 c7 f8 dc 83 4e b3 da 48 1f bf 8a 43 0b b0 e9 60 72 b6 15 10 2f a0 4e 08 7d be c5 5c 04 74 f3 02 f4 77 73 6b 7f 78 f5 bd 91 ee 85 38 47 e7 6b c8 e6 88 a0 7d 5b 81 d7 43 55 10 aa 58 e4 ff 06 a1 90 9a 63 ce 32 21 ea 81 12 97 52 a3 a0 cd 2c Data Ascii: ebE`tJuE9IWKv_n&s_y?hHQh4g7@tcmR 11u7qEM8g?q-$247jo0gCbEK3<)'wNHC`r/N}\twskx8Gk}[CUXc2!R,
2021-11-22 18:40:22 UTC	88	IN	Data Raw: e3 8e 01 00 33 0b c9 31 6c f6 92 12 5f b8 b3 c9 eb 84 33 4b 00 d8 fa 5a 39 ae f1 69 04 e0 9f 67 dc 0d 56 10 80 ed 65 30 e4 87 4c 54 56 bd b1 f8 83 98 6a a1 ed ac 2c 5f c9 71 00 68 9d d2 8a 13 80 43 e8 12 c7 5d 8c b6 ce 44 6e 5c 65 f2 4f 0c 81 dd 3b 9f 48 e8 49 c1 ab 32 69 de d4 13 1d b4 47 21 14 9d 96 40 6e 6e d8 9c d7 33 93 87 28 8a 1e 6c a5 37 ec f7 8e 53 15 9d a2 45 7d e1 95 30 e3 22 8b cf 1c 3a 2b d8 5e bc d7 b1 b4 66 3a 77 d1 77 d0 e2 a4 a4 51 fe 56 ec 2c a2 63 b4 8c e7 7f 67 b0 c1 fe 62 ad 4b be f8 4c f6 49 9d af 02 e4 3a 9d d2 71 b0 f1 d9 f0 67 df d9 47 40 10 9d 4b e0 7e 89 d2 c2 df cb 75 2d 31 c9 7d 45 ef 56 fa e7 1c a0 02 8a f6 4d 62 17 80 40 aa c8 a5 f7 99 cd 17 34 60 d6 be 58 da 9a f9 76 16 63 be 15 57 5a 5c 41 a0 80 2b 54 e5 66 d5 38 17 bd e0 Data Ascii: 31l_3KZ9igVe0LTVj,_qhC]Dn\eO;HI2iG!@nn3(l7SE}0":+^f:wwQV,cgbKLI:qgG@K~u-1}EVMb@4`XvcWZ\A+Tf8
2021-11-22 18:40:22 UTC	90	IN	Data Raw: 58 db 0a 99 46 b3 72 04 b3 cb fe 79 ec e1 4e c0 78 2e c9 7b e2 86 e3 ae ec 31 de 49 03 db 31 a2 9f 0f de c3 b9 ba 45 3f 8d be 14 cb e5 50 e0 8a d8 1e 0f f7 3d f3 7e ab f3 76 7d 95 07 44 4e d0 bc 00 0a 5a 03 f2 c7 8c 3d 21 51 76 1d 8c bd e7 06 30 a5 32 fd b1 51 3c f9 87 17 fe 1d 5c 3a 6b a8 55 ea 1b 27 0f 6e 58 52 75 dd 24 33 8e 5e ff f4 83 5d c1 25 26 d7 09 b7 af a6 cb 05 85 89 89 37 42 ee ad ee 5a 5b 90 e1 65 e8 00 fb 52 bd 0c cb 05 b2 0c a5 17 55 97 62 85 17 23 6f 25 e6 d2 0b 08 3a 8e 66 a9 43 ed 00 8e bc c8 08 7c f5 b9 ab 3e 79 eb 0f ec b4 08 29 a6 76 6c 34 e2 0a 1c c8 fd 76 4a 40 27 37 43 98 21 fd ee 6e 90 44 75 8b 4f 74 18 46 09 5f fb 98 3e 3f 7e 5e cd 5e 16 61 1c 46 a9 14 19 4c b5 a6 6a 98 19 5e c6 b8 6c 4b ec 20 50 78 21 09 1c 74 b7 7e 75 6a d3 b4 Data Ascii: XFryNx.{1l1E?P=~v}DNZ=!Qv02Q<\:kU'nXRu$3^]%&7BZ[eRUb#o%:fC|>y)vl4vJ@'7C!nDuOtF_>?~^^aFLj^lK Px!t~uj
2021-11-22 18:40:22 UTC	91	IN	Data Raw: 1a f3 76 64 39 73 87 97 13 e8 5c 67 aa 89 00 33 0b 99 bc 28 d2 a6 42 d2 34 97 e1 ef 84 33 a3 a8 21 04 a5 51 a6 f3 69 04 6d 1b 43 c0 0f 56 10 d3 bd 8d d7 5d 79 b3 d7 92 b1 3c 7c a7 80 68 a1 ed fc 7f 0c a3 6d 53 97 88 52 f8 52 80 2b 84 64 86 5d 01 32 ea 58 6c 5c 65 a2 b0 19 91 af 7a 9f 1b 65 cd e5 b7 30 69 de 84 ec 08 90 35 60 14 a4 ca 64 02 1a f8 74 ba 89 6c 78 ab 72 1f 18 b3 df 68 44 71 ac 96 65 a8 30 7a 09 ed ea 1c dd 60 ca f4 b6 f3 27 a1 85 8b 95 c4 12 35 9f 96 cd 2f 1d 27 5c 50 8b 53 04 8c 5a 9c 4b b5 bb 5b 13 c4 c4 16 e8 34 b4 41 c1 d0 d2 e5 9d af 02 91 63 62 a6 55 c8 7c 55 d4 eb df d9 47 bf 64 b9 1f 1f 0a ad 82 2a 0d 04 8a d2 08 95 59 0d 9b 6d 77 63 38 08 02 8a f6 c4 3e 33 a8 10 27 84 81 d3 71 d7 f7 ca 9f 87 33 1c fe b6 a9 fb 52 47 96 45 da 16 78 79 Data Ascii: vd9s\g3(B43!QimCV]y<|hmSRR+d]2Xl\eze0i5`dtlxrhDqe0z``5/'\PSZK[4AcbU|UGd*Ymwc8>3'q3RGExy
2021-11-22 18:40:22 UTC	92	IN	Data Raw: da 02 09 f0 30 0b 17 42 b8 f7 dd 29 5c 55 49 57 1e 1d 31 4b 19 73 84 d4 65 a0 4f f1 51 bb b4 f3 0e 47 ba 47 31 95 ec 1a 59 90 c2 d6 ef da ea 23 5a eb b2 49 cb 99 82 b3 d5 6d 57 55 8a 7d 6a d3 0e c7 12 4d eb 63 bb cb ee 47 78 d6 2d 90 08 47 51 82 ca 9f 2e e1 d0 da 0b 1b 0a ef 53 4b a8 ec fe 19 10 ce d2 5c d1 39 5d 42 07 1f d4 99 d4 bd ba df c4 ad 75 1d 5f ef e4 57 8e 7b b6 b0 34 f5 f3 85 22 78 fe 4d ca 56 0f 5a d1 ca 46 9a 28 ff 12 cd 44 df d5 ff 74 47 73 1b 9b c9 f1 55 5e 29 b7 29 97 5d ff a1 36 1a a9 9b 2d 07 b6 7a 5f 76 04 3a ed 29 43 64 35 f7 f3 55 2a 06 1a 4d 94 16 8e 43 11 85 61 95 62 59 9f 9d 9e 08 01 15 73 50 db 01 36 ac d7 97 fa 1b 57 9e 4a 9b 3a 37 6b b7 10 de fb b3 22 28 8f 02 f7 b5 ab 5e 5a ae 5a 59 67 fa 5a d9 76 ef 64 28 b4 c4 d2 3f 43 ed d4 Data Ascii: 0B)\UIW1KseOQGG1Y#ZImWU}jMcGx-GQ.SK\9]Bu_W{4"xMVZF(DtGsU^))]6-z_v:)Cd5U*MCabYsP6WJ:7k"(^ ZZYgZvd(?C
2021-11-22 18:40:22 UTC	93	IN	Data Raw: bb 66 04 58 61 d9 e6 10 2e 5a af 4f be fa c6 9a ec 1f f2 51 87 24 26 aa c8 73 40 6e eb c8 28 d2 e7 2c f2 55 e4 92 8a f6 47 ca c7 4f 24 c6 3e c8 97 00 70 04 74 2d e0 69 37 79 bf d8 e9 d7 5d 79 e3 a2 e0 d4 7f 1d cb ec 68 a1 ed fc 7f 0c a3 6d 12 b7 f8 27 8a 37 a0 5d ed 16 f2 28 60 5e ca 3e 19 32 06 d6 d9 76 ff 8f 0d fe 68 45 ae 84 db 5c 0c ba aa cc 5c f8 5c 13 34 cd b9 44 63 3a 9e 15 ce e8 00 58 ce 00 6d 77 c1 f3 48 25 1f c8 b6 0c c6 54 13 6a 8c 9e 79 ae 40 ab d4 c5 96 55 c8 ea fe e6 e4 77 47 ed f9 bf 0f 74 49 7c 24 e3 36 24 e5 37 ec 27 d0 d6 3e 7d b0 a5 62 81 5b da 61 ae b6 f2 91 f5 ca 22 f0 13 12 ca 3c ab 1d 21 bd 84 b1 d9 47 bf 3c e1 47 47 52 f5 82 2a 49 61 e8 a7 6f 95 59 0d d2 03 1d 06 5b 7c 6b e4 91 f2 0a 33 f4 43 5e f7 f5 b6 1c e4 c5 96 fc ea 57 32 9b Data Ascii: fXa.ZOQ$&s@n(,UGO$>pt-i7y]yhm'7](`^>2vhE\\\4Dc:XmwH%Tjy@UwGtI|$6$7'>}b[a"<!G<GGR*IaoY[|k3C^W2
2021-11-22 18:40:22 UTC	95	IN	Data Raw: 8d 40 25 d3 bc b8 a4 8d cc c4 cb b4 eb 08 83 30 6e 17 30 46 41 1c 13 59 44 98 32 b3 ec 31 d7 56 ef 79 4e e4 60 5d 4c 2e bd 7b 8e 86 7e ba b1 31 92 c2 51 c3 cb f7 f6 84 e5 3b 12 f4 09 b2 e8 84 5b 0a f2 55 cb 45 89 f5 52 a5 8f 86 e3 12 84 eb 5a 95 80 77 e8 2e 2c a1 74 c7 22 f2 a0 ca 70 2e b7 90 7a 8c d8 18 6f 2c 6d 67 8e 76 31 10 16 d2 37 ff 59 5c 5b 82 17 55 8b 1b f0 32 de c4 68 75 35 71 aa 05 7c f7 59 87 34 fa 90 50 b3 22 0c fe 28 ca 57 7a fc 7d 8e ba 2e f8 a3 b2 d8 44 7c 9a 3b fc 08 07 ce 37 e2 0d db 8e 4c 17 09 97 d8 b0 73 be 5d 25 44 d7 47 95 3a 8e 14 a9 26 ed 9b 0c 9c c8 4c f7 a9 59 43 6b 18 60 06 14 7b 46 44 2b 14 7b 6e 23 09 19 8f 32 53 a1 1d 75 84 36 03 98 46 72 52 90 c2 d4 7f b1 cf b9 c7 95 7e fb c2 78 37 0c 06 32 6b f2 fd 49 1a 6e 44 ed 93 e0 e4 Data Ascii: @%0n0FAYD21VyN`]L.{~1Q;[UERZw.,t"p.zo,mgv17Y\[U2hu5q|Y4P"(Wz}.D|;7Ls]%DG:&LYCk`{FD+{n#2S u6FrR~x72klnD
2021-11-22 18:40:22 UTC	96	IN	Data Raw: b4 20 db 7b fc 9b a3 a4 13 d6 34 ee 41 41 6b 52 b7 c8 18 62 79 af 2c f3 fe b5 85 8d 58 97 40 e8 28 67 cb 89 74 33 6e 99 bc 28 d2 a6 42 d2 34 97 bd ef d2 33 ca a8 57 04 c4 51 ca f3 0d 04 04 1b 1f c0 5a 56 63 d3 d8 8d a5 5d 59 b3 93 92 d0 3c 08 a7 e1 68 fd ed b8 7f 69 a3 0b 53 f6 88 27 f8 3e 80 5f 84 38 86 11 01 5d ea 3f 6c 35 65 cc b0 39 91 eb 7a fe 1b 11 cd 84 b7 30 69 de 84 ec 08 cc 35 23 14 cb ca 09 02 75 f8 10 ba e6 6c 24 ab 36 1f 6a b3 be 68 23 71 c3 96 0b a8 6c 7a 5c ed 99 1c b8 60 b8 f4 96 f3 63 a1 e4 8b e1 c4 73 35 c3 96 81 2f 72 27 3f 50 ea 53 68 8c 7a 9c 18 b5 cf 5b 72 c4 b0 16 8d 34 b4 41 c1 d0 d2 e5 9d af 5e 91 20 62 c9 55 a5 7c 3a d4 8f df b6 47 e3 64 fd 1f 6d 0a cc 82 4d 0d 6b 8a bc 08 c9 59 58 9b 1e 77 06 38 7a 02 aa f6 80 3e 52 a8 64 27 e5 Data Ascii: {4AAkRby,X@(gt3n(B43WQZVc]Y<hiS'>_8]?l5e9z0i5#ul$6jh#qlz\`cs5/r'?PShz[r4A^ bU|:GdmMkYXw8z>Rd'
2021-11-22 18:40:22 UTC	97	IN	Data Raw: 76 69 d5 cf c0 74 74 8b fa 97 13 83 35 3e a7 cf ee a0 f8 d2 b0 d2 da cb 65 95 42 6a 63 27 0f 15 79 3a 2a 25 ce 27 c6 e1 45 cc 33 df 30 5f 81 6b 5d 2d 2e c8 2d 83 f3 66 ce ab 43 bb a7 3e c3 ac be 9f ea 8b 4f 32 91 4d c0 89 ea 2f 6f 93 21 cb 65 89 b0 0e dd c2 f6 8a 7e e7 84 28 e7 ef 12 9b 5c 43 a1 12 97 56 80 fc a5 35 48 d3 f9 1d e0 bd 7d 33 2c 38 01 fd 1f 54 62 64 b7 17 99 1d 33 3a fa 63 7b ea 7e ac 4a 92 a1 07 75 56 2d cb 63 10 9e 79 f5 67 9f e4 36 d2 4d 78 86 4d e4 57 1f fc 05 8e df 72 f8 ee b2 b1 18 1f d7 49 93 67 7d bd 5e 8d 61 bd e2 38 76 55 cb 9d f6 17 d7 3a 57 21 b2 1b f3 6f e1 67 d1 43 b1 e9 0c bc b8 08 85 c8 36 37 0d 79 09 5a 78 3f 23 21 58 72 55 0f 4a 7c 77 e3 5b 27 a1 41 75 c8 6a 6c f4 21 1d 3b f7 ac bd 5f df 8b ca a6 bb 0a 91 a3 0b 37 63 06 5c Data Ascii: vitt5>eBjc'y:*%'E30_k]-.-fC>O2M/o!e~(\CV5H}3,8Tbd3:c{~JuV-cyg6MxMWrIg}^a8vU:W!ogC67yZx?#!XrUJ|w['A ujl!;_7c\
2021-11-22 18:40:22 UTC	98	IN	Data Raw: 05 51 99 c3 82 75 42 e6 b8 6e a2 3d 41 89 7d cc 3d f1 6c f3 82 38 5c 0b 8b 35 64 aa 58 68 42 02 ea 6b 0a 61 e0 a4 04 df 00 24 62 6e e5 81 c0 ac 42 2b be 3d 08 3e b3 54 5f 60 f8 a7 5c ef b8 e3 db 8b a1 67 9a c4 dd c0 61 6d 3f 6e a4 b2 ef 19 05 0c 20 c2 f5 7d 11 a4 52 86 3f 56 be 67 00 b7 8a f5 da 91 2a b1 00 bc 44 f6 c5 8f b4 36 34 9f 1f 05 64 ee 51 9a 16 4f 94 72 37 97 d2 79 07 4a 7f 64 19 2c 27 01 e6 ce 5f 20 7c a0 cf b4 58 18 8b 89 99 45 be 40 02 d3 bd b8 ae 8d d8 c4 fe b4 d2 08 95 30 78 17 1e 46 2e 1c 22 59 51 98 2a b3 e2 31 e4 56 c0 79 77 e4 3f 5d 1e 2e ff 7b d7 86 49 ba ab 31 98 c2 0e c3 98 f7 ae 84 b8 3b 03 f4 7c b2 b8 84 4b 0a a0 55 89 45 b1 f5 36 a5 83 86 ba 12 d7 eb 19 95 df 77 af 2e 01 a1 20 c7 17 f2 ca ca 03 2e e4 90 2b 8c bd 18 33 2c 38 67 fd Data Ascii: QuBn=A}=l8\5dXhBka$bnB+=>T_`\gam?n }R?Vg*D64dQOr7yJd,'_ |XE@0xF."YQ*1Vyw?].{I1;|KUE6w. .+3,8g

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	99	IN	Data Raw: 8f f3 22 1b 1f ef 00 de bb 7f 6f a2 3e 24 65 80 41 46 1b f2 ea ec cb 63 72 c1 4d ec ca b2 89 0d 28 b3 ec d1 ae 28 f0 c3 36 6c ef fc 84 99 2a 09 2a d2 96 c0 41 29 a9 cb 4b 34 41 e8 7c b6 29 85 3d 52 e1 b2 c1 29 13 da 4c af 6c 26 be bb 65 79 02 39 8c cd 37 2b 85 dc 84 d5 0f 79 13 4d 6a 99 6a c2 72 84 5b 65 cc 66 46 92 c9 9f b9 4c dd 23 f7 9c f2 31 63 96 13 72 1c d8 90 cf 88 3c 61 42 e9 53 4a e5 3f d5 2b 16 ff ec 4e bc 8b 4f 4a 4c b1 4b 9f 7b 8e 20 97 7b a6 9b c0 a4 1e d6 7c ee 73 41 2a 52 c4 c8 00 62 16 af 4f f3 c3 b5 a8 8d 08 97 63 e8 18 67 cb 89 74 33 6a 99 e0 28 9e a6 2d d2 57 97 80 ef e8 33 ff a8 66 04 ca 51 c9 f3 0e 04 01 1b 26 c0 0f 56 4c d3 fc 8d a7 5d 09 b3 93 92 d0 3c 08 a7 e1 68 fd ed b0 7f 63 a3 0e 53 f6 88 3e f8 0e 80 6c 84 0b 86 32 01 55 ea 34 Data Ascii: "o>$eAFcrM((6l**A)K4A|)=R)Ll&ey97+yMjjr[efFL#1cr<aBSJ?+NOJLK{ {|sA*RbOcgt3j(-W3fQ&VL]<hcS>l2U4
2021-11-22 18:40:22 UTC	100	IN	Data Raw: dc 1c 7a 55 15 e7 ed 18 34 9b 6b 6a 23 f2 a6 de 1b 7b 92 8b 2d 95 52 74 e7 3e b8 7b 83 2a 9c b2 54 68 58 ba 50 57 de 69 34 73 51 db 0e 6e 13 d3 d2 46 b6 38 47 5a 0b a4 f2 f0 f0 72 7f 8f 58 38 4c 87 39 1d 33 ca c2 1d 9d 8e 95 ed e2 96 04 ac a1 dd c0 32 24 50 03 c2 d3 9b 7e 72 69 41 92 87 1c 74 d0 0e ee 72 56 d7 14 63 c1 f8 96 b5 f9 59 de 6f cf 22 82 b1 a1 e8 53 7b e7 79 60 02 ee 38 e9 75 39 f1 11 6b ff e3 16 32 39 51 10 29 02 7b 64 a9 b6 2a 45 08 80 a3 99 37 73 e4 89 f2 45 e2 03 52 b6 cf ca c1 f9 be 94 97 c6 be 67 f0 40 0b 44 42 30 61 7f 57 59 25 cb 46 d6 8d 42 8b 25 ab 10 2b 8b 06 33 2d 6b c8 15 e2 f0 0a ba ed 31 de 91 3e a6 ac 85 9f f2 8b 52 32 97 4d d7 89 f7 2f 4b 93 36 cb 31 89 9c 0e d3 c2 e3 8a 12 e7 eb 28 c6 ef 2e 9b 7d 43 f5 12 82 56 bf fc 96 35 6d Data Ascii: zU4kj#{-Rt>{*ThXPWi4sQnF8GZrX8L932$P~riAtrVcYo"S{y`8u9k29Q){d*E7sERg@DB0aWY%FB%+3-k1>R2M/K61(.}CV5m
2021-11-22 18:40:22 UTC	102	IN	Data Raw: 03 f8 1d c4 ea 32 de 6f 4e e5 68 ad 87 5f 7e 1f 9d 00 b3 ff 5c 2e 80 77 52 65 ae 53 06 1b 9e ae 9d cb 63 72 84 4d 94 ca f2 89 61 28 f2 ec a3 dc 4d 85 b1 52 42 9f 99 84 e1 2a 6c 76 d2 df c0 02 7d e8 8a 08 67 0d a3 2f db 07 e2 58 20 99 9c a4 4c 13 a2 10 ca 14 26 dd eb 0a 0b 72 56 f5 ae 19 4e e0 af fc a6 6a 31 13 2c 6a fa 4a a9 50 e1 5b 17 cc 48 64 f7 e9 e7 96 29 9a 23 a5 ee b3 54 2d f1 47 17 26 bc e2 a6 a8 48 4b 6c ba 36 67 9d 0e b0 06 16 ce ec 63 bc bb 4f 70 4c 99 4b d0 7b c7 4e be 0f 8e ff 83 c8 57 ba 55 c0 35 25 0a 3e eb a4 54 62 16 e3 2b 81 d8 d0 9d dd 0a f8 70 8d 38 12 d8 ec 41 57 6f eb d9 5b a1 a6 42 80 40 fb af 9b d7 47 c2 dc 54 77 f1 3e e2 9c 1a 41 1f 69 2c b2 0f 56 10 81 c9 e1 84 38 0d ff b6 e1 c5 6b 15 c9 b3 5a e4 9f 8e 10 7e a3 6d 53 97 c6 26 b9 Data Ascii: 2oNh_~\.wReScrMa(MRB*lv}g/X L&rVNj1,jJP[Hd)#T-G&HKl6gcOpLK{NWU5%>Tb+p8AWo[B@GTw>Ai,V8kZ~mS&
2021-11-22 18:40:22 UTC	103	IN	Data Raw: 32 da 77 78 0b 48 5a e2 f7 1a a0 99 75 37 36 49 95 ae 77 41 e8 19 05 51 94 c3 aa 75 27 e6 dc 6e fc 3d 1a 89 5a cc 14 f1 5d f3 c1 38 48 0b f4 35 03 aa 35 68 30 02 ae 6b 1c 61 a1 a4 23 df 56 24 2e 6e f2 81 95 ac 00 2b fc 3d 51 3e e8 54 73 60 96 a7 4a ef e7 e3 83 8b f2 67 c3 c4 aa c0 41 6d 50 6e c2 b2 c7 19 02 0c 33 c2 e8 7d 13 a4 7c 86 13 56 ba 67 10 b7 d6 f5 d7 91 38 b1 1b bc 22 f6 d7 8f 87 36 09 9f 59 05 2d ee 7e 9a 55 4f d3 72 1e 97 90 79 57 4a 33 64 48 2c 18 01 c2 ce 5b 20 28 a0 d7 b4 58 18 8f 89 97 45 8c 40 21 d3 f2 b8 eb 8d 9c c4 b7 b4 9b 08 d5 30 4a 17 62 46 08 1c 39 59 05 98 6e b3 af 31 8b 56 ab 79 11 e4 75 5d 59 2e a9 7b 90 86 7e ba ed 31 de c2 1c c3 85 f7 bf 84 ef 3b 5d f4 6d b2 ac 84 0a 0a d2 55 cb 45 b3 f5 4f a5 b2 86 fa 12 8b eb 41 95 8c 77 fa Data Ascii: 2wxHZu76lwAQu'n=Z]8H55h0ka#V$.n+=Q>Ts`JgAmPn3}|Vg8"6Y-~UOryWJ3dH,[(XE@!0JbF9Yn1Vyu]Y.{~1;]mUEOAw
2021-11-22 18:40:22 UTC	104	IN	Data Raw: c9 76 4d bc 7d 78 cf 5c e4 ff f9 76 f8 6e c4 8f 6e ac 2e 3d 95 68 dd f3 1b 1b 7e ef 74 de 9e 2f 72 f2 3b 24 0a 80 30 62 7a f2 c2 f1 97 63 35 e1 22 ec a5 82 ee 0d 44 9d 89 d1 80 28 c6 c3 3a 6c ed fc eb 99 47 09 13 d2 83 c0 57 29 9b cb 6d 34 7f e8 0f b6 43 85 39 52 ed b2 c5 29 13 da 10 af 48 26 9c bb 7a 79 02 39 b1 cd 78 2b 94 dc 9d d5 36 79 5f 4d 05 99 29 c2 31 84 37 65 90 66 23 92 86 9f f9 4c fd 23 c9 9c d6 31 6f 96 26 72 45 d8 89 cf dd 3c 3b 42 ba 53 1f e5 6d d5 69 16 be ec 1a bc 95 4f 15 4c e1 4b b5 7b e7 20 91 7b c6 9b a3 a4 78 d6 0c ee 15 41 25 52 ae c8 74 62 39 af 0c f3 bf b5 e9 8d 78 97 33 c5 71 09 c5 a4 73 52 65 fd de 47 aa 86 6f ff 55 fb 8d 80 f3 1e cd c7 0c 77 c4 3f c2 91 06 7c 40 71 2c a2 2f 7b 3d b7 d4 fe b6 3f 15 d6 fa a1 d5 11 1d d7 e9 1b 81 Data Ascii: vM}x\vnn.=h~t/r;$0bzc5"D(:lGW)m4C9R)H&zy9x+6y_M)17ef#L#1o&rE<;BSmiOLK{ {xA%Rtb9x3qsReGoUw?|@q,/{=?
2021-11-22 18:40:22 UTC	106	IN	Data Raw: b1 f3 56 64 8a b6 a9 fb af 56 96 45 2d 16 78 79 66 4b 87 d3 6e c9 fd 75 37 55 49 e7 5a 0a 41 9b e0 26 50 f2 ed aa 10 03 92 af 03 fb 3d 74 89 3e 21 24 f0 2a 79 b2 38 68 25 ce 50 2f de 4d 11 17 02 db 6b 6e 61 a3 a5 46 4f 3b 24 5a 40 cd e5 91 d8 13 0f ba 3d 38 3e 87 c4 6e 61 ca 1b 28 ef 8e cd 9f ef f7 13 cd c4 dd 8c 9b 6c 50 56 c3 b2 9b 37 00 68 20 b6 e6 59 0e de 74 e2 10 31 d7 67 63 33 52 f4 b5 89 58 b1 6f 92 4b 92 d0 fb 89 12 49 9f 79 05 02 72 93 9b 75 5b f1 72 6b b9 8a 1d 53 3e 30 40 1a 2c 7b 01 a9 7e 81 21 08 30 a0 b4 37 36 8d ed 93 31 83 64 66 d3 cf b8 c1 cd 11 c5 97 88 b1 08 f0 1e 62 73 23 32 00 38 61 59 25 98 46 b3 4d 30 8b 52 ab 79 2b ca 45 0f 79 0a 90 38 a3 86 0a ba ed 35 1e c3 3e ef ac f7 9f aa c8 69 66 d0 15 f1 dc 84 2f 0a 93 65 0b 44 89 e5 0e a5 Data Ascii: VdVE-xyfKnu7UIZA&P=t>!$*y8h%P/MknaFO;$Z@=8>na(lPV7h Yt1gc3RXoKIyru[rkS>0@,{~!0761dfbs#28 aY%FM0Ry+Ey85>if/eD
2021-11-22 18:40:22 UTC	107	IN	Data Raw: c7 55 d1 e0 62 d3 99 19 ee 95 f9 e7 e8 90 bd 05 f4 12 5d e4 85 41 77 f8 06 7c 8e 32 e2 d7 3c e5 52 15 f2 5f af a8 ee 00 c2 47 2e 2e f8 cf 25 65 7c e4 63 1b 1a 19 f0 cb b1 c5 e0 4d 2c 7d 83 89 23 90 9c ec 79 6b 29 85 c3 52 6c 9f 6c 38 98 2a 1c 76 d2 5f 5e be 28 e8 c2 08 34 8d f8 2f b6 87 81 58 52 19 a5 a4 29 93 c9 10 af 94 55 dd bb 8a 6f 72 39 75 ce 19 2b 60 a8 fc d5 ea d7 af 4c 6a ad 4a c2 d0 8f 5b 65 4c 66 64 92 e9 1d 39 4d 9a 63 0a 9d b3 5f 82 97 47 22 89 d9 e2 cf a8 3c 4b 86 15 52 67 05 a1 d4 06 ba 61 ed 63 bc bb 4f 70 8a 25 4a d0 79 7a 21 be ad 32 9a 83 4e eb d7 55 fa 88 40 0a 52 eb c8 54 0c aa ae 4f f3 9f b5 e9 8a 78 d5 50 9a 25 17 de cd 65 50 79 e0 cc 5c d2 82 42 90 77 e5 98 9f f0 7c d3 cd 4f 45 c9 36 c9 81 00 70 05 76 13 b2 60 20 79 b7 d8 ff d7 6c Data Ascii: Ub]Aw|2<R_G..%e|cM,}#yk)Rll8*v_^(4/XR)Uor9u+`LjJ[eLfd9Mc_G"<KRgacOp%Jyz!2NU@RTOxP%ePy\Bw |OE6pv` yl
2021-11-22 18:40:22 UTC	108	IN	Data Raw: 5a c6 77 70 84 81 5b 71 94 85 af fe f3 56 5a 97 da cc ba 52 f4 94 02 b6 79 1a 18 24 7e 8e c7 75 8e 99 a3 36 12 2c 93 ed 6d 33 e9 7c 04 25 b6 aa ac 10 18 92 e4 1c ec 6a 74 89 73 c8 28 94 5e b0 c7 4a 1a 6e d4 41 13 c3 1b 0d 10 76 b4 19 17 36 d3 a4 b6 de 7f 41 2e 28 cd ed 95 ff 1b 51 ea 3d 5a 3f c1 26 78 05 86 ce 7f 9d ef 91 94 8b c7 63 ff a1 a9 84 5e 01 14 07 b0 d7 f8 6d 1d 7e 38 95 87 7d 85 a5 49 e3 06 10 be 0b 06 e4 91 8f d0 d4 21 b1 2b bf 6e 99 d2 ee 84 77 17 f3 16 66 02 ee 70 99 39 20 92 13 07 d1 91 1c 57 4a a8 60 7e 4d 12 75 ef a1 58 73 61 ce c4 d8 52 57 86 e3 97 26 96 40 fa d3 8c ca a4 ec ca a1 c7 c6 d1 6b 95 43 78 40 42 46 8e 18 01 30 57 ec 33 d2 e1 61 f9 39 df 1c 48 90 06 5d 4b 2a 9b 1e 96 c0 63 d6 88 61 b1 ab 50 b7 c9 85 9f 84 48 38 60 91 2c d6 d9 Data Ascii: Zwp[qVZRy$~u6,m3|%jts(^JnAv6A.(Q=Z?&xc^m~8}!+nwfp9 WJ`~MuXsaRW&@kCx@BF0W3a9H]K*caPH8`,
2021-11-22 18:40:22 UTC	109	IN	Data Raw: 2a 52 6b 6f 41 1f 97 8f 0a 2a 0f 62 9e 87 e0 a6 6c 99 5e 3b 59 b9 94 0f 46 df 4e 1d d3 0f 90 9e 8d 13 f8 6e d8 8f 71 cd 03 51 ab 0d d5 87 17 74 70 84 45 a6 ff 2f 40 f2 34 56 00 e1 27 07 4c 9b c0 95 a4 14 37 99 1a ec 64 82 cd 64 5b ed 8d a5 bf 40 c8 a6 21 1f fe 9b e1 d8 2a 09 2f d3 98 a5 76 64 8d b8 7b 55 6a 8d 6e b6 3a 84 1f 37 ed f9 c1 50 40 ae 71 db 71 26 f3 bb 49 11 13 4b b9 a2 6e 4e 92 8b fc d5 34 79 50 3f 0f f8 3e a7 14 e1 28 0e b8 09 14 c5 e9 9f c3 1f df 71 96 ae 9d 55 41 fa 47 72 48 da b0 aa cf 6d 3e 27 c8 2a 31 84 62 a0 63 53 b6 bb 63 bc da 4d 22 29 fe 04 a0 1e a9 6b db 02 cb e3 d4 a4 37 d4 07 8b 52 0e 7a 37 85 83 31 1b 53 d7 0e f3 d0 b7 bb e8 1f d2 7d 9d 31 2c cf f0 45 4b 5c 99 d1 2a 80 c3 25 83 41 f2 93 96 d2 52 cf dd 44 41 dd 10 a6 f3 01 06 3f Data Ascii: *RkoA*bl^;YFNnqQtpE/@4V'L7dd[@!*/vd{Ujn:7P@qq&IKnN4yP?>(qUAGrHm>'*1bcScM")k7Rz71S}1,EK* %ARDA?

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	111	IN	Data Raw: c8 25 3b 34 79 58 4b a4 92 a8 52 33 0f 10 69 e1 f5 9f 1e b4 96 a6 d8 f5 5c 69 8e f7 cd 9f 1f 22 fb 27 bf 64 0b 79 b2 3f ac ce 6e b8 ea 79 45 14 2d 83 ae 18 0f de 4d 2b 01 bb f0 ec 5b 1f 8a e7 6e 95 72 38 cc 7f 99 2f c2 18 dd d6 54 04 0b ba ed 57 e9 1b 11 03 76 88 1f 1c 08 bd c3 12 b0 7a 4d 34 0f d6 f8 b1 ac 72 f0 8f 7e 4a 47 f7 20 48 0e ba d5 72 9b eb 80 99 cf f7 13 cd c4 dd 19 32 2e 22 17 b2 c6 c8 6d 00 65 2f a5 d3 12 36 cd 60 e7 00 2f 80 67 63 f4 aa ac e5 c5 6a 83 41 d8 4e 9a b1 9f e8 71 1e eb 34 6a 66 9b 54 ff 33 26 9d 17 25 f6 8e 1c 77 32 06 64 29 7c 28 40 f9 87 04 64 44 ec a3 b4 37 18 e4 89 f2 45 e2 40 52 d3 cf b8 c1 8d be c4 97 b4 be 08 f0 30 0b 17 42 46 61 1c 57 59 25 98 46 b3 8d 31 8b 56 ab 79 2b e4 06 5d 2d 2e c8 7b e2 86 0a ba ed 31 de c2 3e c3 Data Ascii: %;4yXKR3i\i'"dy?nyE-M+[nr8/TWvzM4r~JG Hr2."me/6`/gcjANq4jfT3&%w2d)|(@dD7E@R0BFaWY%F1Vy+]-.{1>
2021-11-22 18:40:22 UTC	112	IN	Data Raw: 48 24 17 32 67 89 61 d1 2e db a3 78 37 0c ee 37 6b f2 fd 01 cf 9a 4f 2e 98 6b 62 2f 11 51 7e 61 71 a7 6e a1 ec 15 2b ff 0a b3 be ad 37 ad 2f 92 ce 65 e4 ec d1 9d eb cd fb 5f 53 94 06 b9 92 88 09 29 b6 fc de 56 5b bb c6 1f f2 ae 48 82 94 70 99 01 67 22 6a 1e 09 28 9d 55 89 78 7b 60 8b db 28 bb dc 6c 11 2e 09 76 6b cf 21 88 ea a0 40 f8 dc 76 ec 2f b6 be 2a e9 0e 0d fa 2d 6d 37 ea f8 c3 10 26 dd 02 39 79 ec ac bd 44 5d 0f c8 90 77 35 82 23 17 4d 6a d1 29 bf 6c c8 d0 b5 84 65 99 13 d6 cf d3 4c 9a 57 a2 af 73 d8 00 92 47 72 9e bc 64 cf a8 5a 72 05 be 26 89 a4 b0 d4 06 16 ce a8 e7 cb 83 3a 92 43 2e 0c d6 74 70 6f aa 3f 05 d4 bb 21 97 a2 79 a6 b8 16 2e 16 60 08 1c 61 c7 24 05 f7 1a 7c 9c 8a f3 95 5a eb 9d 8c ae 02 02 30 ca d1 87 eb 9a a9 05 0a 7c 14 23 c7 c9 18 Data Ascii: H$2ga.x77kO.kb/Q~aqn+7/e_S)V[Hpg"j(Ux{`(l.vk!@v/*-m7&9yD]w5#Mj)leLWsGrdZr&:C.tpo?!y.`a$|Z0|#
2021-11-22 18:40:22 UTC	113	IN	Data Raw: 6d 8d ae b9 04 8a d2 49 9a 49 4c c3 24 14 23 04 3b d0 c7 7d cd cd 3c d7 14 03 c6 0a 4f 71 5f f7 ca 9f 02 e8 68 2a fe 22 ff 76 0f 57 ad ca 52 77 ce 98 7a 67 79 6e cc d1 97 7b 71 41 a2 25 c2 4e 25 18 ab 9b ff 43 e7 14 07 e5 08 ac 75 3e a4 c1 c1 0d 32 72 c1 f2 c7 df 25 86 ae 2d 64 63 28 e3 09 22 92 68 96 20 ea ee 5e a9 b7 af 45 2b 97 5a b9 af aa 63 02 42 3c 31 39 57 55 9f 09 e6 dc 24 83 a7 ee 53 16 1c 53 c4 a8 2d 73 e0 54 7d f9 74 ef 14 8d cd 00 f9 cd 65 06 75 e7 dd 8d a9 28 26 e8 f5 dc f6 7c d8 5a 71 60 0b 36 f7 f0 04 a2 2a 32 9c b1 8e 06 7f 71 99 b5 a4 f3 41 ab df 68 25 16 6a 19 ef 5d 08 53 49 2a 0a 3a 7f cb ed f9 24 37 1b e4 89 f2 41 e2 40 52 2c 30 b8 c1 35 be c4 97 b4 be 08 f0 70 0b 17 42 46 61 1c 57 59 25 98 46 b3 8d 31 8b 56 ab 79 2b e4 06 5d 2d 2e c8 Data Ascii: mIIL$#;}<Oq_h*"\vWRwzgyn{qA%N%Cu>2r%-dc("h ^E+ZcB<19WU$SS-sT}teu(&|Zq`6*2qAh%j]SI*:$7A@R, 05pBFaWY%F1Vy+]-.
2021-11-22 18:40:22 UTC	114	IN	Data Raw: 53 97 a8 52 f8 52 86 2b 84 64 92 5d 01 32 ea 58 6c 5c 65 a2 b0 19 91 af 7a df 1b 65 8d cb d3 51 1d bf 84 ec 08 a8 35 60 14 a4 fa 64 02 1a f8 74 ba 89 6c 78 ab 72 1f 18 b3 df 68 44 71 ac 96 65 a8 70 7a 09 2d c4 6c b9 01 be 95 b6 f3 4b a1 85 8b 95 84 12 35 9f 94 cd 2f 1d 3d 5c 50 8b 53 04 8c 5a 9c 4b b5 bb 5b 13 c4 84 16 e8 74 9a 33 b2 a2 b1 e5 9d af e2 90 63 62 a6 05 c8 7c 55 d6 eb df d9 5b bf 64 b9 1f 1f 0a ad 82 2a 0d 04 8a d2 08 d5 59 0d db 6d 77 63 38 08 02 8a f6 c4 3e 33 a8 10 27 84 81 d3 71 d7 f7 ca 9f 87 33 1c fe b6 a9 fb 52 47 96 45 da 16 78 79 48 3f e2 ab 1a ed 99 1c 37 55 49 e7 ae 18 41 9b 19 6a 51 f2 c3 de 75 7b e6 8b 6e 95 3d 74 89 3e cc 7b f1 2a f3 b2 38 68 0b ba 35 57 aa 69 68 73 02 db 6b 6e 61 d3 a4 46 df 38 24 5a 6e a4 81 f0 ac 72 2b 8f 3d Data Ascii: SRR+d]2Xl\ezeQ5`dtlxrhDqepz-lK5/=\PSZK[t3cb|U[d*Ymwc8>3'q3RGExyH?7UIAjQu{n=t>{*8h5Wihskn aF8$Znr+=
2021-11-22 18:40:22 UTC	115	IN	Data Raw: 20 94 ef 77 d3 a7 07 85 5a 4c d2 d6 04 ca 35 2e 93 18 69 a8 fd 91 77 08 00 ec 79 52 a4 10 64 d2 9e bb 39 6c 72 09 e7 71 0a 1b ac 32 da 4d 7b 51 7e 39 42 41 34 d7 86 92 d6 e6 e4 50 5b 66 5c 9e c8 0a 58 f2 84 7e 8e ba 3e 9b 7a 96 49 44 1f 9a 08 7f 9d 21 b2 b0 eb 0e bd 8e 70 ad 5b 87 9d b0 77 be 3a 25 6d d8 b8 47 60 0d 35 aa 43 ed ac 3f 4a 80 83 28 88 dd c1 64 fd 00 5b 14 3f 07 aa f9 3a f0 c0 cb 61 e7 1c cd 66 2a 93 3d 41 b2 48 18 21 72 3b dc 27 24 b7 1b 75 46 59 d4 ba fa c5 f1 73 28 7e 7a e6 a6 d9 31 0e e3 5d c9 b8 1f b3 19 94 19 5e 61 73 a3 52 58 f4 88 45 38 50 e4 ff ca a4 b4 45 03 1f 3d 1a 6b 07 ad e5 a1 c9 1e 23 1b e7 75 ce b7 d0 ec ba f4 de 61 fc ba d9 1a f2 ae f1 20 61 41 3a 05 61 86 a6 e1 f2 3d a0 e0 d1 dc ad 5e cc d6 a8 9d fc 84 96 9c 8d 52 c2 de c0 Data Ascii: wZL5.iwyRd9lrq2M{Q~9BA4P[f\X~>zID!p[w:%mG`5C?J(d[?:af*=AH!r;'$uFYs(~z1]^asRXE8PE=k#ua aA:a=^R
2021-11-22 18:40:22 UTC	116	IN	Data Raw: 7d a6 81 69 a1 ec fd 7e 0d a2 6c 52 96 89 53 f9 53 81 2a 85 65 87 5c 00 33 eb 59 6d 5d 65 a2 7c d5 5d 63 b6 53 d7 a9 01 29 7b fc a5 12 cc 65 54 b4 3d 28 9d c8 ee 74 54 4d b9 22 f2 0a 80 48 e3 f9 5b 3c cb 96 e3 b5 39 25 d2 41 80 71 f1 d1 66 ae 38 ad 28 41 0e 3f b7 03 81 cd 00 7c 3b 07 57 88 96 cd 6b 96 d7 df ab 89 5c 81 57 5a 9c 4b d3 38 64 13 cb 40 c7 e8 34 b4 c2 bf d8 d2 ea 19 68 02 91 63 2a 2d 1a c0 1a d6 ed a7 d0 5c fe bf 64 b9 79 9c 73 af ed 25 88 aa 8a d2 08 f3 da 74 9f 0c 78 e6 9b 08 02 8a 90 47 47 35 cc 1f a2 1c 81 d3 71 9f 7a 8e bb e7 00 e3 bb 85 60 72 2e 63 f6 00 e9 d6 30 f0 0c 1b c2 26 49 ec d1 97 fa aa 5c f6 b9 18 41 a6 3a 6a 51 32 b6 b1 fe 3f c2 eb 2a 18 76 76 8a fd ff b2 7a fa b2 0a 38 58 0b ba bc 13 8e 09 97 66 d6 dd 6b 6e 25 58 e8 62 bf b5 Data Ascii: }i~lRSS*e\3Ym]e|]cS){eT=(tTM"H[<9%Aqf8(A?|;Wk\WZK8d@4hc*-\dys%txGG5qz`r.c0&I\A:jQ2?*vvz8Xfkn%Xb
2021-11-22 18:40:22 UTC	118	IN	Data Raw: 45 c1 78 1b d8 37 79 75 5a 6c 20 60 1c ea c4 89 2e 43 ed 9f 87 4f be 75 cf 95 3c d3 90 f5 bf 41 e7 cc 64 b5 72 21 75 54 10 2c 59 d8 00 08 ff 38 82 63 ef f3 1b ac 32 d3 7c 07 65 56 71 f8 cc 58 7c a1 c3 ea b0 c3 af c7 4b 7a fe 4d 82 da 6f 3e 87 71 45 3a 73 25 fa 38 41 57 88 49 fc 2b 8a fd 2e c1 84 b8 cb 2a 17 55 7f 75 4b e8 41 72 a8 34 76 18 95 6f c6 ec 66 bc f8 b1 0e bc c8 40 7c 94 7d 07 23 f0 65 1e 06 3f 46 12 eb 3a f8 cb 03 23 da 2f fe eb 6d 09 f6 24 0e ef 62 20 07 24 a3 6c 98 d2 b4 35 47 59 6a 42 72 e7 5c 1f 49 35 fb 58 20 74 0d 62 4e 22 24 2f f5 b6 69 98 19 e6 2c f8 e7 76 60 3f c1 40 69 90 28 33 35 ba 34 a2 08 43 fe 60 a3 f1 29 a4 61 3f 93 d7 d3 89 66 d1 e0 ab 2e f2 77 24 65 c8 d0 8e 0b be 27 e5 ef 2f fb bd 69 e4 87 b1 52 41 a5 c9 c8 c9 90 03 55 8e 5d Data Ascii: Ex7yuZl `.COu<Adr!uT,Y8c2|eVqX|KzMo>qE:s%8AWI+.*UuKAr4vof@|}#e?F:#/m$b $l5GYjBr\l5X tbN"$/i,v`?@i(354C`)a?f.w$e'/iRAU]
2021-11-22 18:40:22 UTC	119	IN	Data Raw: bd bd 8d d7 5d 79 93 d7 92 c1 3c 7c a7 ae 01 c5 8c 88 1e 28 96 6d 53 97 88 22 d8 52 80 ab 85 64 86 73 73 56 8b 2c 0d 5c 65 52 91 19 91 2f 7b 9f 1b 4b bf 81 d6 44 08 fa fe 96 72 f4 57 07 14 a4 ca 14 21 1a f8 c4 ba 89 6c 56 d3 16 7e 6c d2 df 68 64 55 ac 96 4d a8 30 7a 27 84 8e 7d a9 01 ee c6 b6 f3 27 a1 cd af 95 c4 0a 35 9f 96 e3 46 79 46 28 31 af 60 04 8c 5a 9c 2b 91 bb 5b 7b c4 c4 16 c6 5d d0 20 b5 b1 f6 d1 9d af 02 91 ab 46 a6 55 2c 7c 55 d4 c5 b6 bd 26 cb 05 9d 29 1f 0a ad 82 2a 3d 04 8a ea 08 95 59 23 f9 1e 04 63 38 08 02 8a b6 c4 3e 5f a8 10 27 aa f1 b7 10 a3 96 ca 9f 87 63 1c fe d6 a9 fb 52 69 e4 36 a8 75 5c 49 79 3f e2 ab 1a 8d c9 1c 37 d5 48 e7 ae 36 33 e8 6b 09 75 c2 f1 de 75 7b e6 8b 6e 95 3d 74 89 3e cc 7b f1 2a f3 b2 38 68 0b ba 35 57 aa 68 79 Data Ascii:]y<|(mS"RdssV,\eR/{KDrW!lV~lhdUM0z'}'5FyF(1`Z+[{] FU,|U&)*=Y#c8>_'cRi6u\ly?7H63kuu{n=t>{*8h5Why
2021-11-22 18:40:22 UTC	120	IN	Data Raw: 32 f4 4d b2 89 84 2f 0a 93 55 cb 45 89 f5 0e a5 c2 86 8a 12 e7 eb 28 95 ef 77 9b 2e 43 a1 12 c7 56 f2 fc ca 35 2e d3 90 1d 8c bd 18 33 2c 38 67 fd 76 54 10 64 d2 17 ff 1d 5c 3a 82 63 55 ea 1b ac 32 92 c4 07 75 56 71 cb 05 10 f7 79 87 67 fa e4 50 d2 22 78 fe 4d ca 57 7a fc 7d 8e ba 72 f8 ee b2 b1 44 1f 9a 49 fc 67 07 bd 37 8d 0d bd 8e 38 17 55 97 9d b0 17 be 3a 25 21 d7 1b 95 6f 8e 67 a9 43 ec e9 14 bc c8 08 ef c8 59 b7 6b 79 60 5a 14 3f 46 21 2b 72 7b 0f 23 7c 18 e3 30 27 a1 41 45 c8 36 ec 98 21 72 3b 90 ac d4 5f b1 8b b9 a6 95 0a fa a3 71 33 0c 06 7a 6b f2 fd 29 16 6e 11 90 d1 e0 a6 6b 98 19 5e 2d f8 e7 76 28 bc 05 78 aa 5c e4 ff c5 49 80 03 a8 af 44 c9 1d 4e 8c 07 c3 ce 78 2a 31 df 27 fe 9a 41 4d 9d 13 4d 0b e7 6e 45 4e a6 e8 dc f3 44 52 92 39 8d a4 e6 Data Ascii: 2M/UE(w.CV5.3,8gvTd\:cU2uVqygP"xMWz}rDIg78U:%!ogCYky`Z?F!+r{#|0'AE6!r;_q3zk)nk^-v(x\IDNx *1'AMMnENDR9

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	122	IN	Data Raw: 25 0b 6a 71 66 9a a2 3f 00 56 10 d2 91 bc 3c 7a 1f 88 93 b6 95 49 6d 26 61 97 ae ed fc f4 c9 62 85 43 f1 89 56 c9 b9 8f 4d bf a6 f3 57 80 d3 15 57 6c 5c 03 a3 9c 28 92 75 ff 60 6e d4 46 b9 93 28 e2 8a a0 b0 83 dc 11 74 17 b5 43 30 26 46 75 3e be 02 6d f1 e7 56 0b 9d 73 d0 ed 33 8e 53 69 ee d4 14 6a 06 5a ad 1a d2 d7 85 e0 33 33 28 25 32 8b 95 c4 99 41 bb ca 40 40 21 24 b5 18 08 2e e8 8c d3 d8 6f 91 b4 dd 87 c4 c4 16 63 79 b4 72 13 92 59 24 5c 47 1f b2 a1 e9 77 94 22 62 d6 36 ea 1e 30 58 3a a4 cc 07 9a d8 d8 85 40 05 5a e0 d3 e3 90 33 09 c5 07 75 e6 f1 50 0d ce 06 2f 12 b6 7a 65 30 01 48 a6 75 bd e7 21 8a 02 e1 69 f5 33 60 8f 4a f9 16 45 da 16 93 68 cd f6 97 ae 70 cd c7 f7 3f 3f 09 62 67 40 4e de e9 e1 1c f2 48 18 78 7b e4 8b 6e 14 dc 74 89 3e c8 74 b5 ec Data Ascii: %jqf?V<zIm&abCVMWWl\(u`nF(tC0&Fu>mVs3SijZ33(%2A@@!$.ocyrY$\Gw"b60X:@Z3uP/ze0Hu!i3`JEhp??bg@NHx{nt>t
2021-11-22 18:40:22 UTC	123	IN	Data Raw: 33 de c2 3e d5 ac f7 9f 84 8b 3b 32 f4 4d b2 89 84 2f 0a d3 55 cb 07 89 f5 0e a5 c2 86 8a 12 e7 eb 28 95 ef 77 9b 2e 43 a1 12 c7 56 f2 fc ca 35 2e d3 90 1d 8c bd 18 33 2c 38 67 fd 76 54 10 64 d2 17 ff 1d 5c 3a 82 63 55 ea 1b ac 32 92 c4 07 75 56 71 cb 05 10 f7 79 87 67 fa e4 50 d2 22 78 fe 4d ca 57 7a fc 7d 8e ba 72 f8 ee b2 b1 44 1f 9a 49 fc 67 07 bd 37 8d 0d bd 8e 38 17 55 97 9d b0 17 be 3a 25 21 d7 1b 95 6f 8e 67 a9 43 ed e9 0c bc c8 08 f7 c8 59 37 6b 79 60 5a 14 3f 46 21 2b 72 7b 0f 23 7c 19 e3 32 27 a1 41 75 c8 36 6c 98 21 72 3b 90 ac d4 5f b1 8b b9 a6 95 0a fb a3 78 37 0c 06 32 6b f2 fd 49 46 6e 11 ed d0 e0 a6 6b 98 19 5e 2d f8 e7 76 28 bc 05 78 aa 5c e4 ff f9 76 f8 6e c4 8f 32 ac 6f 3d e5 68 ad f3 5f 1b 1f ef 00 de ff 2f 2e f2 77 24 65 80 53 62 1b Data Ascii: 3>;2M/U(w.CV5.3,8gvTd\:cU2uVqygP"xMWz}rDlg78U:%!ogCY7ky`Z?F!+r{#|2'Au6l!r;_x72kIFnk^-v(x\vn2o=h_/.w$eSb
2021-11-22 18:40:22 UTC	124	IN	Data Raw: 1c 37 64 c9 2f 2a ec 05 20 4d 28 58 0c 96 62 e4 5f 67 e0 82 12 34 f3 d7 8c 87 d0 3d 97 f7 c2 4e 29 58 87 80 78 2a b9 d8 63 3f 6a ec b9 ab a8 52 e8 34 8f 34 c0 64 86 d7 85 38 d6 78 6c 4c 5f 23 8c 39 91 bf 0f 92 5a e6 34 e1 cb db d7 df 84 ec 08 7b 37 53 e2 29 8e 40 1a 4a 07 a3 3f 7f 63 fd cd 8d e0 e7 38 9b 4c 48 2e f2 cd ee 4d 6d b8 25 ed 67 43 22 6f d5 f4 85 0c ae dd a1 9b 16 3f 37 3a 18 6a cd 2f 1d 28 ea d3 0b 46 04 9c a5 b8 ce cd ae 5b 03 4f fa 9f 94 10 a4 4e 77 53 66 f0 9d bf fd b5 e6 ca b3 55 d8 f7 13 e8 00 dc 52 01 b7 e1 79 10 9b c0 ad 82 2a 86 51 ae 59 c6 7d 6c f0 64 92 fe 27 1c 2c 31 43 f9 72 bd db bd 10 37 7b a5 56 ad c2 f7 da 14 c9 0f f7 fd 3d e7 f3 38 46 1b 01 fe 32 1e f0 04 1b c6 fb 97 a9 bd 3c 67 aa 5c c3 8e 18 51 10 4d 4e 4d c1 03 5f 9f 47 c6 Data Ascii: 7d/* M(Xb_g4=N)Xx*c?jR44d8xlL_#9Z4{7S)@J?c8LH.Mm%gC"o?7:j/(F[ONwSfURy*QY}ld',1Cr7{V=8F2<g\QMNM_G
2021-11-22 18:40:22 UTC	125	IN	Data Raw: 06 4d 2d 2e a2 62 69 4e 60 ba 64 7c 22 3d 2b d7 8c f7 8f 0f c6 c7 91 e4 7d b2 99 09 57 13 18 64 41 1c 8d 7c 33 a9 f2 86 9a aa 97 f9 28 85 28 32 77 c7 43 a1 12 ec 97 34 b9 3a 35 ad 3b 95 94 c9 50 95 76 d8 68 0d bd 1c 5e 41 9b c7 1b df 1d 4c b1 cf 9f de af f7 25 33 9d 72 42 85 de 30 cf 88 55 03 29 78 12 0e 8e 55 83 dd 6d f2 6d ca 47 f1 b9 81 03 f7 9e d3 29 3b 86 c7 f7 9f c1 a3 63 8e f8 da 06 0c 34 c9 3d 18 e3 d6 99 da 17 d4 3a ad 66 de e4 80 7f ae 67 b9 13 12 fc 08 9c c8 18 9f c0 78 37 7b 86 15 a2 eb 2a 4e 01 2b 62 11 4f 4b 7c 09 e3 32 4d b8 ca bd a2 36 e5 d5 dd 8d 2e 84 8c d4 4f 3a c6 45 05 95 3a fb b3 bf 72 e0 ef 32 6b f2 70 31 5f a8 54 1d d0 6b 97 d3 48 0f 5e 3d 72 be 72 03 7d 86 90 af d5 d9 fb c9 76 e8 e7 81 62 bf e9 9b 6d 8f 28 c7 f9 0e e4 0a e3 20 de Data Ascii: M-.biN`d|"=+}WdA|3((2wC4:5;Pvh^AL%3rB0U)xUmmG);c4=:fgx7{*N+bOK|2M6.O:E:r2kp1_TkH^=rr}vbm(
2021-11-22 18:40:22 UTC	127	IN	Data Raw: 00 33 0b dd 9e 28 d2 8e 42 d2 34 b9 88 8b e5 47 c2 8c 13 04 a5 51 a6 9f 4b 04 6d 0f 43 c0 0f 78 79 b7 dc f9 b6 79 4a b3 d7 92 b1 bc 5e a7 80 58 a1 ed fc 51 65 c7 0c 27 f6 ac 66 f8 52 80 2b 34 46 86 5d d5 32 ea 58 42 35 01 c3 c4 78 b5 99 7a 9f 1b 65 cd d5 b7 30 75 de 84 ec 26 f2 46 13 14 a4 ca 64 02 5a f8 74 da 89 6c 78 85 00 6c 6a d0 fb 58 75 71 ac 96 65 c8 70 7a 09 6d eb 1c dd 4e b8 87 c4 90 03 91 b7 8b 95 c4 12 91 bd 96 cd 2f 1d 27 5c 50 8b 53 04 68 78 9c 4b 91 9b 5b 13 44 e6 16 e8 34 b4 41 c1 d0 d2 e5 9d d9 21 91 63 62 86 55 c8 7c 55 d4 eb df d9 47 bf 64 b9 1f 1f 0a ad 82 2a 0d 04 8a d2 2c b6 59 0d c5 4e 77 63 74 2b 02 8a 18 e6 3e 33 a8 33 27 84 95 f0 71 d7 db e9 9f 87 0f 3f fe b6 a9 fb 52 47 52 67 da 16 c8 5b 48 3f e2 ab 1a ed 41 1f 65 21 25 a1 dc 7d Data Ascii: 3(B4GQKmCxyyJ^XQe'fR+4F]2XB5xze0u&FdZtlxljXuqepzmN/'\PShxK[D4A!cbU|UGd*,YNwct+>33'q?RGRg[H?Ae!%}
2021-11-22 18:40:22 UTC	128	IN	Data Raw: a1 db 8a 31 08 6e 6f 47 40 da dd fc 64 2c 14 e8 41 c8 bc 0a ba ed 31 de c2 3e c3 ac f7 9f 84 8b 3b 32 f4 4d b2 89 84 2f 0a 93 55 cb 45 89 f5 0e a5 c2 86 8a 12 e7 eb 28 95 ef 77 9b 2e 43 a1 12 c7 56 f2 fc ca 35 2e d3 90 1d 8c bd 18 33 2c 38 67 fd 76 54 10 64 d2 17 ff 1d 5c 3a 82 63 55 ea 1b ac 32 92 c4 07 75 56 71 cb 05 10 f7 79 87 67 fa e4 50 d2 22 78 fe 4d ca 57 7a fc 7d 8e ba 72 f8 ee b2 b1 44 1f 9a 49 fc 67 07 bd 37 8d 0d bd 8e 38 17 55 97 9d b0 17 be 3a 25 21 d7 1b 95 6f 8e 67 a9 43 ed e9 0c bc c8 08 f7 c8 59 37 6b 79 60 5a 14 3f 46 21 2b 72 7b 0f 23 7c 19 e3 32 27 a1 41 75 c8 36 6c 98 21 72 3b 90 ac d4 5f b1 8b b9 a6 95 0a fb a3 78 37 0c 06 32 6b f2 fd 49 46 6e 11 ed d0 e0 a6 6b 98 19 5e 2d f8 e7 76 28 bc 05 78 aa 5c e4 ff f9 76 f8 6e c4 8f 32 ac 6f Data Ascii: 1noG@d,A1>;2M/UE(w.CV5.3,8gvTd\:cU2uVqygP"xMWz}rDlg78U:%!ogCY7ky`Z?F!+r{#|2'Au6l!r;_x72kIFnk^-v(x\vn2o
2021-11-22 18:40:22 UTC	129	IN	Data Raw: b5 e9 8d 78 97 13 e8 5c 67 aa 89 00 33 0b 99 bc 28 d2 a6 42 d2 34 97 e1 ef 84 33 a3 a8 21 04 a5 1d 2d 2f 3e 4c ec f7 a3 c0 0f 56 23 13 f4 00 ac d5 c0 b3 d6 92 b1 cf d6 24 7a 69 ae 68 e0 7e 0c a3 24 da cc 80 1a 75 16 a4 7b c5 ed d5 7d 32 e9 ab e1 6d 5d 65 a2 f8 90 d5 8b 5a da 28 a5 85 68 a2 7b 79 de 84 a4 cf 51 34 60 14 24 41 9f fd 0f 54 7b ba 89 e9 b8 a4 f7 97 18 b3 df 20 cf 3d 88 c6 2d 25 b4 5e f1 ed ea 1c 95 e9 8e d0 9e bb aa b4 5e 84 95 c4 57 06 56 de 44 73 39 07 19 63 4b ac 11 06 55 9c 4b 30 7b 2e 5c 4f 50 32 10 34 b4 41 4c 9b 92 1a 88 21 0d 91 63 2a 2d 19 ec 2c 19 59 67 fb d1 46 bf 64 f1 94 e7 42 20 97 b5 02 04 8a 9a 85 11 7d f5 9b 6d 77 26 0b c8 4a 03 b2 e0 16 7b 21 6c 03 a4 7e c6 35 d8 f7 ca 1a 47 47 15 b6 3d 66 04 47 20 99 45 da 5e f3 35 6c 6f 1d Data Ascii: x\g3(B43!-/>LV#$zih~$u{}2m]eZ(h{yQ4`$AT{ =-%^^WVDs9cKUK0{.\OP24AL!c*-,YgFdB }mw&J{!l~5GG=fG E^5lo
2021-11-22 18:40:22 UTC	130	IN	Data Raw: b3 28 e9 c3 72 6c cf fc e5 99 44 09 13 d2 b3 c0 5e 29 e8 cb 08 34 0d e8 2f b6 07 85 58 52 99 b2 a4 29 13 da bf e8 a4 78 dd bb 0a 79 7f 39 f5 cd e5 2b e0 dc 00 f5 6a 79 ef 4b 6a 99 0d 81 04 c8 5b 75 cc 66 22 93 e9 9f b8 38 ff 5b d1 b8 de 5f 2d 96 47 72 26 f8 e2 cf f8 3c 4b 42 94 3a 03 84 7a b4 22 23 ce ec 63 bc eb 6f 70 4c 35 4b d0 7b e9 52 da 1a fa fa 83 a4 ab f6 55 ee c9 41 0a 52 c5 ba 30 03 62 ce 6b 89 e5 cf 8d ef 1f 97 13 e8 a4 46 aa 89 38 33 0b 99 92 50 b6 c7 36 b3 34 97 d1 cd 84 33 3f 8a 21 04 8b 34 c2 92 1d 65 6d 1b 8f 84 0f 56 38 d3 bd 8d f9 34 1d d2 a3 f3 95 0e 7c a7 80 68 55 a9 fc 7f 18 a3 6d 53 b9 e1 36 99 26 e1 0f b7 64 86 5d 01 3a af 58 6c 0c 65 a2 b0 37 f8 cb 1b eb 7a 41 f9 e5 b7 30 69 86 c1 ec 08 06 35 60 14 8a a3 00 63 6e 99 50 8c 89 6c 78 Data Ascii: (rlD^)4/XR)xy9+jyKj[uf"8[_-Gr&<KB:z"#copL5K{RUAR0bkF83P643?!4emV84|hUmS6&d]:Xle7zA0i5`cnPlx
2021-11-22 18:40:22 UTC	131	IN	Data Raw: dc 78 aa 69 78 43 02 db 5e 5e 61 d3 fe 76 df 38 a7 6a 6e a4 2b c0 ac 72 e2 bf 3d 38 d0 b7 54 1d 75 fb a7 1d db bf e3 ed d4 a7 67 ac 4e ec c0 32 d4 61 6e c2 5a aa 19 72 0b 73 c2 87 4d 46 a4 0e d5 40 56 d7 17 51 b7 f8 6a 87 91 59 0f 5d bc 22 2b 83 8f e8 cc 49 9f 79 28 31 ee 38 fe 46 4f f1 e1 58 97 e3 cd 01 4a 51 85 1a 2c 7b 0f 9d ce 2a 1f 3c a0 a3 c4 03 18 e4 18 c6 45 e2 fc 66 d3 cf 5d f5 8d be ce a2 b4 be 27 c5 30 0b 59 77 46 61 63 62 59 25 38 73 b3 8d f8 be 56 ab 89 1e e4 06 78 1b 2e c8 37 d4 86 0a cb db 31 de 56 08 c3 ac 4c a9 84 8b d3 04 f4 4d a7 be 84 2f 4a a4 55 cb 20 be f5 0e 27 f5 86 8a ab d0 eb 28 65 d8 77 9b 37 7b a1 12 85 6e f2 fc 95 0d 2e d3 02 25 8c bd dd 0b 2c 38 97 c5 76 54 0b 5d d2 17 bd 24 5c 3a e1 5a 55 ea 65 95 32 92 77 3e 75 56 a5 f2 05 Data Ascii: xixC^^av8jn+r=8TugN2anZrsMF@VQjY]"+Iy(18FOXJQ,{*<Ef]'0YwFacbY%8sVx.71VLM/JU '(ew7{n.%,8vT]$\:ZUe2w>uV

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	132	IN	Data Raw: ae 1a ad ba f2 cc 75 41 e9 ec a6 b5 46 e8 ae 36 42 c8 b3 d3 d8 5a 79 33 aa b6 b4 02 48 9d b3 4f 51 79 ac 4a c0 44 e4 28 21 d8 b2 d3 40 7d b7 7d cb 3a 47 a8 c3 4d 1c 06 7d 90 bb 5a 4a 90 af bd d5 0b 0c 6b 0a 0f ed 0e a7 26 c7 3a 15 bf 31 64 e5 80 f1 fb 21 fe 0d c4 e9 cb 76 48 e2 03 17 50 9b 83 bf db 6b 4b 23 cf 2b 20 80 7a 9b 73 7b 8a 89 15 cf bb 38 19 22 f4 26 b4 55 a6 55 c6 3c eb ef cd d1 3a 92 30 98 46 41 6b 27 93 8f 31 16 40 c0 23 86 f2 d0 e9 fa 11 f9 7e 85 38 49 cb fc 78 74 6e ed ea 47 be d3 2f b7 34 f6 94 97 cb 46 d7 e5 44 77 d6 30 c1 96 69 73 04 75 2e ad 6b 78 71 a6 c5 c2 a2 29 34 d6 a4 e1 d0 5b 19 a7 e1 1d d9 be 99 0b 5a cc 01 26 fa ed 52 8f 3b ee 46 e9 00 a8 3c 74 4a b9 3d 18 0a 0a ce c5 74 f4 af 10 f0 62 26 a2 8b d1 59 0e 9d ec 8d 66 f7 50 04 14 Data Ascii: uAF6BZy3HOQyJD(!@}}:GM}ZJk&:1d!vHPkK#+ zs{8"&UU<:0FAk'1@#~8IxtnG/4FDw0isu.kxq)4[Z&R;F<tJ =tb&YfP
2021-11-22 18:40:22 UTC	134	IN	Data Raw: 51 a1 16 90 44 97 e5 38 05 68 d3 66 32 c4 0d 3b 07 70 b2 05 09 20 d3 d3 2f b1 55 49 3e 40 c9 e2 99 ff 17 45 eb 6e 4c 4c ee 3a 7a 21 ca ca 7e 86 dd 86 83 ef c5 13 de ad b3 a7 65 6d 27 07 ac df f6 7d 5c 61 22 ab d4 18 1a c0 5d f2 00 3f b9 00 34 b7 95 96 dc c2 3c c5 2b ce 4b 80 d4 fd ac 57 0f fe 79 72 6b 80 55 f7 11 61 9c 11 02 c4 86 0d 76 38 38 12 4c 5e 3f 60 dd af 2a 4d 6b c9 f0 d1 43 41 8d ec 9e 21 b2 32 3d b0 cf cf a8 e3 d3 a9 f3 9a d3 6b 99 63 6e 63 1b 2f 04 70 33 09 57 f7 25 b3 e0 58 ef 3f e8 16 45 8a 63 3e 59 2e bf 12 8c eb 67 de c3 5c b7 a6 57 80 c3 99 f1 e1 e8 4f 32 99 24 d6 e0 c0 46 79 f0 3a a5 2b ec 96 7a a5 b5 ef e4 7f 8a 8f 06 f8 86 13 f2 6a 2a d2 71 a8 38 9c 99 a9 41 2e be f9 79 e5 f4 76 72 48 5c 25 88 10 32 75 16 d2 60 96 73 31 57 e6 4d 38 83 Data Ascii: QD8hf2;p /UI>@EnLL:z!~em'}\a"]?4<+KWyrkUav88L^?`*MkCA!2=kcnc/p3W%X?Ec>Y.g\WO2$Fy:+zj*q8A .yvrH\%2u`s1WM8
2021-11-22 18:40:22 UTC	135	IN	Data Raw: 08 e9 37 0b 54 87 da bc ae 10 01 80 2a 89 ca ef e0 69 41 d2 99 a5 93 58 e0 ad 52 1b f6 92 e9 f4 4e 27 1b bb bb a9 4d 5c 9c 84 78 51 63 e8 42 df 63 ec 17 27 ed e2 d6 4c 63 bb 62 ca 5c 43 bc df 6f 0b 72 4e 9c a3 74 46 84 f2 91 bc 0e 10 5c 38 1e c9 38 a7 20 e5 29 00 84 03 05 f6 8c ed 96 21 f3 47 cc d3 c6 45 7f f3 34 17 52 d8 95 a6 c6 51 26 26 94 3e 0e 81 67 9a 73 62 9c 89 10 d9 cf 4f 1d 25 fd 22 9f 0e b3 73 db 0f d8 f4 ef d1 3a b3 55 99 5c 2f 67 3f 8f e6 39 0b 72 c6 00 86 eb e6 8c f9 2e f8 7f 9d 31 02 aa e4 69 57 62 d6 c9 5c 81 ce 2d a0 40 da 92 88 84 44 ca c6 4c 69 c1 7f cb 9a 0d 6d 22 6e 37 93 67 39 62 a7 f0 fe b0 5d 14 da b3 fb fe 49 08 f2 ee 18 d3 88 8c 1e 7e c6 25 36 f6 ec 37 8a 52 f7 42 ea 09 eb 39 2f 5f 83 3c 05 13 10 d6 e5 77 e1 dd 1f ef 7a 17 a8 ad Data Ascii: 7T*iAXRN'M\xQcBc'Lcb\CorNtF\88)!GE4RQ&&>gsbO%"s:UVg?9r.1iWb\-@DLim"n7g9b]I~%67RB9/_<wz
2021-11-22 18:40:22 UTC	136	IN	Data Raw: a6 bf 01 1e e6 e6 03 c1 5c 07 e2 6d a5 1c 9f 4b 9f b2 4f 01 65 d7 58 33 84 04 05 27 63 a8 00 3d 08 b4 ca 27 b3 38 49 37 3a c5 f2 9b f5 1b 4e e3 59 38 49 ee 3a 70 0d ae 89 70 82 da 82 9e e0 cf 0e c9 a8 b9 c0 5f 00 39 01 83 d6 ed 78 1c 6f 24 c2 f0 14 1a c9 63 e2 5c 3b ba 0e 0c f6 9c 83 d4 ff 3a d4 6f d1 4f 9f de ce 9b 55 1e f1 1d 05 75 87 56 f7 18 2b df 1f 06 fe 8c 38 41 29 34 0a 4d 2c 16 6c c0 a1 69 4c 67 d3 c6 b4 40 71 8a e4 9f 21 cc 2d 3f ba a0 fb ad e2 cd a1 97 d9 d3 61 9f 73 79 72 23 32 04 5f 3f 2c 4b f3 46 c4 e4 5f e6 3b cf 57 46 89 6f 32 6e 5c ad 1a 96 e3 49 d2 98 5f b5 c2 53 ae c5 98 db e1 f8 58 57 9a 29 b2 fe ed 41 67 fe 31 e5 28 e4 9c 61 e1 a7 f5 e9 77 89 8f 28 f8 82 1e f4 68 2f d4 61 af 56 85 95 a4 58 43 b7 be 70 e1 d4 77 75 40 4d 14 95 76 39 7d Data Ascii: \mKOeX3'c='8I7:NY8I:pp_9xo$c\;:oOUuV+8A)4M,liLg@q!-?asyr#2_?,KF_;WFo2n\I_SXW)Ag1(aw(h/aV XCpwu@Mv9}
2021-11-22 18:40:22 UTC	138	IN	Data Raw: 4f 7a 97 74 9f ff 58 47 9c 1a 49 01 ae 24 03 6d 97 e7 9f 8c 06 06 a4 3f 9e a5 f0 dd 68 50 e9 ad d1 ab 49 f3 a6 1b 02 d8 99 f0 dc 58 7b 19 a0 8b a5 7a 5d bf cb 7f 5d 63 85 42 d2 29 f2 39 24 fc fb ca 6e 76 ae 55 dd 66 49 af ef 6f 01 06 6e f5 ba 78 5d 85 95 92 92 0f 0d 5a 09 6a ee 23 ac 3d e9 3f 4b bb 07 12 f7 a0 f1 d1 29 ee 6a e1 9c c4 50 5b f3 0e 1c 61 bd 96 81 dd 51 0f 27 cc 20 67 92 67 bb 6b 7b aa c2 14 dd cd 2a 39 22 de 2e a4 35 b2 4d fa 1e f8 e8 83 d3 36 a0 30 a7 5b 06 6f 26 bb a7 27 0b 62 c6 20 9d 9f c2 80 e3 15 fa 77 c6 2b 06 dc ec 49 5d 4c fc c8 78 bd d5 2b a6 5d f8 8f ef f3 52 d5 cd 68 6a e8 34 d5 80 08 63 08 1b 34 a9 61 3b 7d b7 93 fa b6 2b 1c fa b9 df d4 4f 0f c6 e7 0d a1 9a 9d 09 69 ea 03 1c e7 ed 3c f8 25 e9 45 e9 09 e2 73 76 53 9c 3d 25 32 2a Data Ascii: OztXGI$m?hPIX{z]]cB)9$nvUfIonx]Zj#=?K)jP[aQ' ggk{*9".5M60[o&'b w+I]Lx+]Rhj4c4a;}+Oi<%EsvS=%2*
2021-11-22 18:40:22 UTC	139	IN	Data Raw: 1a 3c 93 fd 7d 35 cd 76 06 24 9f a6 de 02 1a 90 ee 21 e0 49 21 e7 4e be 1e 81 4b 81 d7 70 0d 6a de 50 25 aa 1e 01 1d 6f b6 0f 40 16 b2 d2 23 90 4d 50 0f 00 d4 f3 95 dc 13 59 ea 75 5d 5f e3 31 6f 60 bd c6 6b 8a c1 96 99 dc e4 0e d8 a1 dd b7 5b 03 3d 03 a6 9c ec 78 04 69 0e b7 f3 2a 06 cd 7a e3 72 56 ff 22 63 b7 f8 f5 b5 91 59 b1 6f bc 82 b3 b1 8f c8 16 7b 9f 71 40 02 ee 38 9a 75 4f f1 72 6b 97 03 3c 32 4a 51 44 29 2c 7b 01 a9 ce 2a 20 08 a0 a3 b4 37 18 e4 89 f2 45 e2 40 52 d3 73 fd c1 8d be c4 97 b4 10 4d f0 30 0b 17 42 46 ad 59 57 59 25 98 46 b3 8d 31 8b 56 ab 79 2b e4 5e 18 2d 2e c8 7b e2 86 72 ff ed 31 de c2 3e c3 ca b2 9f 84 8b 3b 32 f4 d9 f7 89 84 2f 0a 93 55 4d 00 89 f5 0e a5 c2 86 8a 12 e7 eb 28 95 ef 77 cc 2f 06 d9 7b b3 06 80 93 a9 50 5d a0 90 c6 Data Ascii: <}5v$!I!NKpjP%o@#MPYu]_1o`k[=xi*zrV"cYo{q@8uOrk<2JQD),{* 7E@RsM0BFYWY%F1Vy+^-.{r1>;2/UM(w/{P]
2021-11-22 18:40:22 UTC	140	IN	Data Raw: c4 8f 32 ac 6f 3d e5 68 ad f3 5f 1b 1f ef 00 de ff 2f 2e f2 77 24 65 80 53 62 1b f2 ae f1 cb 63 72 e1 4d ec ca 82 89 0d 28 9d ec d1 dc 28 85 c3 52 6c 9f fc 84 99 2a 09 76 d2 df c0 02 29 e8 cb 08 34 0d e8 2f b6 07 85 58 52 99 b2 a4 29 13 da 10 af 14 26 dd bb 0a 79 72 39 f5 cd 19 2b e0 dc fc d5 6a 79 13 4d 6a 99 4a c2 50 84 5b 65 cc 66 64 92 e9 9f 96 4c 9a 23 a5 9c b3 31 2d 96 47 72 6b 82 72 cf ab 3c 4b 42 be 53 67 e5 f1 2a 06 16 76 ec 63 bc bb 4f 70 4c d9 4b d0 7b c7 20 be 7b 8e 9b 83 a4 57 d6 55 ee 35 41 0a 52 eb c8 54 62 16 af 4f f3 9f b5 e9 8d 78 97 13 e8 84 67 aa 89 0e 2c b1 97 bc 9c db 6b 63 6a 35 db 2c ce d0 5b ca db 01 74 d7 3e c1 81 08 69 4d 78 22 ae 61 39 64 f3 df e8 f7 2f 0c dd f7 fb df 1c 38 e8 d3 48 cc 82 98 1a 22 ae 60 59 b3 88 52 f8 52 80 2b Data Ascii: 2o=h_/.w$eSbcrM((Rl*v)4/XR)&yr9+jyMjJP[efdL#1-Grkr<KBSg*vcOpLK{ {WU5ARTbOxg,kcj5,[t>iMx" a9d/8H"`YRR+
2021-11-22 18:40:22 UTC	141	IN	Data Raw: 68 11 49 3f e2 2b e5 f8 99 3c 37 45 cc 27 db 14 cc d6 e5 82 01 0d 3c 21 fe 8b 0d 89 e5 66 6b 8b 9c 2e ec 7b e1 af 33 c6 26 e5 4e 56 65 da ef c1 38 20 51 88 01 6f 32 80 f7 10 20 2d 38 7a 6e b4 d7 0f b9 66 0b 8f 2d 6b c1 92 74 3d 60 da 6b 1d ef 8e e3 ed 8b 96 67 ac c4 dd c0 32 6d 50 6e c2 b2 9b 19 72 0c 41 c2 87 7d 74 a4 0e 86 72 56 d7 67 63 b7 f8 f5 b5 91 59 b1 6f bc 22 f6 b1 8f e8 36 7b 9f 79 05 02 ee 38 9a 75 4f f1 72 6b 97 e3 79 32 4a 51 64 29 2c 7b 01 a9 ce 2a 20 08 a0 a3 b4 37 18 e4 89 f2 45 e2 40 52 d3 cf b8 c1 8d be c4 97 b4 be 08 f0 30 0b 17 42 46 61 1c 57 59 25 98 46 b3 8d 31 8b 56 ab 79 2b e4 06 5d 2d 2e c8 7b e2 86 0a ba ed 31 de c2 3e c3 ac f7 9f 84 8b 3b 32 f4 4d b2 89 84 2f 0a 93 55 cb 45 89 f5 0e a5 c2 86 8a 12 e7 eb 28 95 ef 77 9b 2e 43 a1 Data Ascii: hI?+<7E'<!fk.{3&NVe8 Qo2 -8znf-kt=`kg2mPnrA}trVgcYo"6{y8uOrky2JQd),{* 7E@R0BFaWY%F1Vy+]-. {1>;2M/UE(w.C
2021-11-22 18:40:22 UTC	143	IN	Data Raw: eb 47 78 aa 26 a6 ff f9 d6 ba 6e c4 41 70 ac 6f c0 a7 68 ad df 1c 1b 1f b8 43 de ff 3d 06 f2 77 15 4d 80 53 36 33 f2 ae 88 e3 63 72 47 65 ec ca 5b a1 0d 28 6b c4 d1 dc 27 ac c3 52 46 b6 fc 84 de 03 09 76 b6 f6 c0 02 a6 c1 cb 08 98 24 e8 2f 67 2e 85 58 a4 b0 b2 a4 30 39 da 10 95 3e 26 dd e6 20 79 72 47 df cd 19 8c ca dc fc 19 40 79 13 bc 40 99 4a d6 7b 84 5b 4a e7 66 64 dc c2 9f 96 39 b1 23 a5 3c 98 31 2d 55 6c 72 26 32 c9 cf a8 2d 67 42 ba 65 4b e5 0e 86 2a 16 ce 64 4f bc bb fc 5c 4c 99 91 fc 7b c7 3b 93 7b 8e c7 ae a4 57 55 78 ee 35 ed 27 52 eb 11 79 62 16 a9 61 f3 9f 98 c7 8d 78 f5 3d e8 5c ee 84 89 00 83 25 99 bc fd fc a6 42 28 1a 97 e1 cc ab 33 a3 e2 0e 04 a5 38 89 f3 69 8a 42 1b 43 75 20 56 10 07 92 8d d7 a2 56 b3 d7 b8 81 3c 7c fe b0 68 a1 65 cc 7f Data Ascii: Gx&nApohC=wMS63crGe[(k'RFv$/g.X09>& yrG@y@J{[Jfd9#<1-Ulr&2-gBeK*dO\L{;{WUx5'Rybax=\%B(38iBCu VV<|he

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	144	IN	Data Raw: 75 88 d3 db b6 3d 23 e3 29 bf 5e 19 17 2c 53 87 ab 55 9d fc 72 73 27 20 91 cb 6a 41 ec 70 04 3c 9f a7 f0 3a 0b 83 e5 2a e7 54 02 ec 4c cc 34 83 4e 9a dc 59 04 39 ba 42 3e c4 04 05 17 2c 94 19 0a 08 bd c5 2a ed 38 74 36 0f dd d2 9f d9 1c 4f 8f 4a 51 50 ea 39 79 4e 9a cb 7c 96 dd 8c 98 e5 f2 67 fc a8 bc b9 61 02 25 00 a6 f3 9b 6e 1b 62 2c af e3 53 24 c8 6f ff 21 39 a2 09 07 f6 f8 a5 d9 f0 20 e2 00 c9 4c 92 e6 8f 9f 5f 15 f2 14 61 2c be 54 fb 0c 1c 9e 07 05 f3 b4 79 61 2f 3f 00 6d 5e 12 77 cc bc 67 45 7b d3 c2 d3 52 18 93 e0 9c 28 8f 24 7c 80 aa d6 a5 c9 cc ad e1 d1 cc 45 95 43 78 76 25 23 61 4b 18 0e 64 e8 36 f6 f5 58 ff 56 dc 10 45 89 6b 39 03 79 87 2c a3 f6 7a ff 95 58 aa c2 5f b6 d4 b0 fa f0 cf 5e 44 b7 2c c2 fa c5 2f 7d fa 3b a6 28 ed db 6f d0 ba c1 ef Data Ascii: u=#)^,SUrs' jAp<:*TL4NY9B>,*8t6OJQP9yN|ga%nb,S$o!9 L_a,Tya/?m^wgE{R($|ECxv%#aKd6XVEk9y,z X_^D,/};(o
2021-11-22 18:40:22 UTC	145	IN	Data Raw: 92 d4 04 ea 4a 2a 5f 91 89 11 7f bc 72 11 c4 31 89 9b d7 1b 9b 07 83 ea 46 e9 1d 4f 8a 1a fe 87 2d 72 71 88 57 de 92 4c 47 b5 12 50 3c e9 36 0e 7f a2 dc 9e a8 63 05 88 23 81 a7 e6 a7 60 4b f4 ab b4 a8 71 ec a6 3e 08 cf 8e eb fa 2a 64 15 bb 93 af 63 4d ab a4 65 59 6c 86 4b e4 62 f6 37 27 eb d1 c1 29 64 b3 7e c2 79 42 f3 d6 69 10 3e 56 94 a9 5a 44 8d b1 9d bb 0e 2b 76 3e 05 ec 38 a1 35 84 36 06 a5 35 01 fc 8d dc f9 21 f7 42 cb f8 f2 31 5a ff 29 1f 4b bc cc a2 cb 55 18 27 d4 37 24 8a 63 b8 67 78 aa ad 63 d1 d8 26 23 29 f7 2f 93 14 aa 4d df 15 ea cc 83 d3 3e b8 38 83 51 6f 67 31 82 9b 31 0c 72 ec 20 9e f2 d4 87 e9 2f 97 7e 8b 35 34 cf e7 64 60 7f eb d5 46 b5 e7 42 a5 5d f9 8c 82 e0 1d ce cb 48 57 c0 3f c2 a0 1d 76 04 75 24 81 0f 3b 73 ba ee e8 b9 39 2a c7 a5 Data Ascii: J*_r1FO-rqWLGP<6c#`Kq>*dcMeYlKb7')d~yBi>VZD+v>8565!B1Z)KU'7$cgxc&#)/M>8Qog11r /~54d`FB]HW?vu$;s9*
2021-11-22 18:40:22 UTC	146	IN	Data Raw: 4a e0 af be 18 b3 9e 85 ea f3 74 79 8a f3 db 89 3d 35 c2 20 a2 62 2f 79 25 56 86 c2 55 98 ed 5b 52 21 00 a3 ae 6f 28 f5 74 07 35 dc ae b7 11 12 a9 fe 1a d2 58 00 c0 7a cc 16 98 4e 9a fd 4d 1c 4c df 41 19 df 04 2c 16 74 a8 6b 19 08 bd c9 2b bb 16 49 33 0a cd ce 85 d8 35 4e fb 73 4d 53 c3 31 6b 13 ca ca 74 8b e7 ac 98 ff d1 02 d8 92 b2 ac 47 00 35 6e b5 db f5 74 1f 68 6f af ee 19 1d eb 7b f2 35 33 a3 31 0c db 8d 98 d0 91 34 d8 0b d5 6d 83 c5 c3 87 58 1c d2 0a 62 02 99 51 f4 18 22 95 5c 06 fe 87 10 7d 3f 25 28 46 42 1c 4c da a9 2a 4d 61 c4 ca fb 42 6c a9 ec 81 36 83 27 37 d3 b8 d1 af e0 d3 a0 b9 d9 d7 6c 99 7f 7e 63 0f 23 12 6f 36 3e 40 98 2b da e9 58 c4 23 df 36 5b 81 68 5d 5a 47 a6 16 8f e2 24 d7 84 55 b7 8d 4b b7 e3 87 fa ea 8b 56 5b 90 24 fd fc f0 7f 78 Data Ascii: Jty=5 b/y%VU[R!o(t5XzNMLA,tk+I35NsMS1ktG5ntho{5314mXbQ"\}?%(FBL*MaBl6'7l~c#o6>@+X#6[h]ZG $UKV[$x
2021-11-22 18:40:22 UTC	148	IN	Data Raw: 6b 5f 0f dc 90 20 3e 0b 63 a2 a0 85 c8 6b f5 70 26 48 8a b4 13 5c ff 6a 16 de 2e 8b 93 bd 13 8c 0f ad e3 41 ac 18 54 8b 05 c0 97 71 76 76 97 65 ac ac 4a 5a b1 18 4a 11 f2 3c 0e 5f 97 da 90 a2 0f 01 e1 20 81 8e f0 ff 44 46 ee 98 b0 b0 44 85 b4 3b 02 f2 91 e0 b7 47 64 32 a0 a9 89 6c 5a 9c aa 64 58 0d 85 42 f1 62 f1 1b 27 eb c0 c1 47 67 8e 71 dc 7f 26 aa d2 64 14 1f 5d db a0 74 6c 85 a8 bf a0 18 0b 76 23 1e cd 2b b1 3b 84 36 08 98 07 17 f9 ab f3 f9 2f f1 23 d2 f5 dd 5c 40 f2 69 1f 4b 8c 83 bc c3 7e 27 2d d9 38 67 88 63 81 67 65 a5 af 11 d9 da 3b 15 4c ee 22 be 16 aa 44 90 16 e3 cf e2 d7 3c 95 27 8b 54 35 6f 52 86 a5 00 03 65 c4 1c 9a f8 db 88 e1 78 e0 7a 86 31 0a ce a7 6d 5e 5f f8 cf 43 81 cf 25 bc 55 fb e1 82 e9 67 c2 db 4a 5d cc 34 ca 97 69 73 04 75 2e ad Data Ascii: k_ >ckp&H\j.ATqvveJZJ<_ DFD;Gd2lZdXBb'Ggq&d]tlv#+;6/#\@iK~'-8gcge;L"D<'T5oRexz1m^_C%UgJ]4isu.
2021-11-22 18:40:22 UTC	149	IN	Data Raw: 06 6b 6d 76 cf 80 a1 50 47 a8 67 4e ea ec be 15 f9 83 a3 f2 e2 60 79 8a f3 df 9e 3c 33 96 32 bb 60 1d 30 26 7e 86 cf 58 98 ff 7a 52 27 49 90 c7 76 2c f6 7d 44 26 93 b5 bb 3c 15 a7 ef 0a d7 48 12 ef 5b be 7b 86 4b 85 d7 71 06 48 d6 5a 24 cf 69 1f 1a 6c b6 06 0a 4f a4 c5 30 ba 71 4a 19 02 cb f2 95 ac 05 4a f9 58 71 50 c0 31 69 24 af d1 5e 8e fe 90 ac 8b e1 0e c2 a9 b0 a4 1c 1a 31 18 a7 fb f5 5e 17 78 05 a7 f1 3e 15 d4 7d c7 72 21 b6 11 06 fe 96 b2 d0 e5 1d d4 19 ff 43 86 c2 d8 e8 41 12 f1 14 68 66 c0 4f fb 03 2a b8 1c 2c f2 97 3d 57 3c 12 05 59 5f 2c 01 de af 5c 45 41 ce e4 d1 43 5d 96 fb 9d 37 b6 25 2a a7 8e b8 b6 e4 d0 a9 fa d0 90 7f 91 46 6e 5e 2c 01 04 68 12 2b 57 f7 34 e7 e8 49 ff 17 ab 0e 4a 92 63 14 43 69 ad 0f a7 f4 78 d5 9f 65 bb ba 4a 94 ac 80 f6 Data Ascii: kmvPGgN`y<32`0&~XzR'Iv,}D&<H[{KqHZ$ilO0qJJXqP1i$^1^x>}r!CAhfO*,=W<Y_,\EAC]7%*Fn^,h+W4IJcCixeJ
2021-11-22 18:40:22 UTC	150	IN	Data Raw: d0 f9 dc ee f0 6b 9f c6 0a 37 7b 67 44 0e bd 88 3d 14 0b 62 88 a4 e0 d1 02 f6 74 33 49 d6 90 17 5e d9 4a 0d de 0e 81 8c 9c 02 f8 19 a5 f9 57 e3 1a 49 b7 0d de 87 3e 69 6b ef 77 b7 91 42 43 96 59 53 04 f6 36 2d 6e 86 fc 94 b8 17 13 93 39 ec bd e3 ff 68 67 e8 98 82 b9 5c d5 aa 26 0f f7 fc f3 f0 44 64 1b b6 f1 b7 63 5f 8d 84 7d 40 5e 8d 5b e6 6e f1 3b 3a 99 c5 c5 5f 76 95 65 db 47 43 a9 eb 66 18 0b 5b 94 ae 72 79 81 a8 99 d5 1d 10 7d 20 07 fd 64 b5 31 f2 3e 2a b9 12 37 f7 9d cf fa 2d e3 41 c4 ff d8 63 4c e2 22 72 51 b9 94 aa e7 49 3f 11 df 27 31 8a 62 a0 6b 73 ce 9b 0a d2 d6 22 14 62 ee 2a a6 1e 88 55 ca 28 eb ef d5 cb 3b a3 38 8b 35 36 6b 24 8e 87 21 16 43 c1 3f 81 fa c5 88 ff 1d df 76 89 38 02 d8 89 77 5a 65 f4 d1 4c fc d1 23 a4 51 d8 94 9b d1 5d d3 da 44 Data Ascii: k7{gD=bt3l^JWI>ikwBCYS6-n9hg\&Ddc_}@^[n;:_veGCf[ry} d1>*7-AcL"rQI?'1bks"b*U(;856k$!C?v8wZeL#Q]D
2021-11-22 18:40:22 UTC	152	IN	Data Raw: 0d 04 8a d2 08 95 59 0d 9b 6d 77 63 38 08 02 8a f6 c4 3e 33 a8 10 27 84 81 d3 71 d7 f7 ca 9f 87 33 1c fe b6 a9 fb 52 47 96 45 da 16 78 79 48 3f e2 ab 1a ed 99 1c 37 55 49 e7 ae 18 41 9b 19 6a 51 f2 c3 de 75 7b e6 8b 6e 95 3d 74 89 3e cc 7b f1 2a f3 b2 38 68 0b ba 35 57 aa 69 68 73 02 db 6b 6e 61 d3 a4 46 df 38 24 5a 6e a4 81 f0 ac 72 2b 8f 3d 38 3e 87 54 1d 60 ca a7 1d ef 8e e3 ed 8b 96 67 ac c4 dd c0 32 6d 50 6e c2 b2 9b 19 72 0c 41 c2 87 7d 74 a4 0e 86 72 56 d7 67 63 b7 f8 f5 b5 91 59 b1 6f bc 22 a3 3a 63 63 63 6b 14 3c 0d 89 26 bd 48 01 46 37 73 6b d6 60 93 33 3f a6 39 ea 79 f0 ed cd 6f 1a 20 08 a0 20 58 2f 93 a4 85 a1 13 b5 cb 2a df 26 1f c1 8d be 4f d0 84 8d fe 7b 6f 27 9c 7d cf 24 e4 dc 1b 19 11 3b 47 06 75 9b 2e 22 3c db 61 c6 52 a9 ab c8 7b e2 47 Data Ascii: Ymwc8>3'q3RGExyH?7UIAjQu{n=t>{*8h5WihsknaF8$Znr+=8>T`g2mPnrA}trVgcYo":ccck<&HF7sk`3?9yo X/*&O{o'}$;Gu."<aR{G
2021-11-22 18:40:22 UTC	153	IN	Data Raw: c8 36 6c 98 21 72 3b 90 ac d4 5f b1 8b b9 a6 95 0a fb a3 78 37 0c 06 32 6b f2 fd 49 46 6e 11 ed d0 e0 a6 6b 98 19 5e 2d f8 e7 76 28 bc 05 78 aa 5c e4 ff f9 76 f8 6e c4 8f 32 ac 6f 3d e5 68 ad f3 5f 1b 1f ef 00 de ff 2f 2e f2 77 24 65 80 53 62 1b f2 ae f1 cb 63 72 e1 4d ec ca 82 89 0d 28 9d ec d1 dc 28 85 c3 52 6c 9f fc 84 99 2a 09 76 d2 df c0 02 29 e8 cb 08 34 0d e8 2f b6 07 85 58 52 99 b2 a4 29 13 da 10 af 14 26 dd bb 0a 79 72 39 f5 cd 19 2b e0 dc fc d5 6a 79 13 4d 6a 99 4a c2 50 84 5b 65 cc 66 64 92 e9 9f 96 4c 9a 23 a5 9c b3 31 2d 96 47 72 26 d8 e2 cf a8 3c 4b 42 ba 53 67 e5 0e d5 06 16 ce ec 63 bc bb 4f 70 4c 99 4b d0 7b c7 20 be 7b 8e 9b 83 a4 57 d6 55 ee 35 41 0a 52 eb c8 54 62 16 af 4f f3 9f b5 e9 8d 78 97 13 e8 5c 67 aa 89 00 33 0b 99 bc 28 d2 a6 Data Ascii: 6l!r;_x72kIFnk^-v(x\vn2o=h_/.w$eSbcrM((Rl*v)4/XR)&yr9+jyMjJP[efdL#1-Gr&<KBSgcOpLK{ {WU5ARTbOx\g3(
2021-11-22 18:40:22 UTC	154	IN	Data Raw: 64 76 78 55 68 2e c4 3b 48 b3 c5 3c f9 bb d6 3a bd 6b 4b a9 20 45 c0 0a a5 30 3d c4 1d 0c d0 9a fd 15 92 b2 f3 42 fd c4 fe ac b9 00 47 cd d3 9a 94 61 3e a5 8c e9 c5 4b a4 7b d8 d1 bb 2e f8 ad 06 03 78 7d d5 9a 2f 75 a5 2d 21 65 a2 f7 8b 41 f2 d2 05 5a 06 09 e9 bd 9c f8 dc c5 9e c7 0b 0c d6 3f 71 01 87 9e bc 5c 91 36 3c 5f 82 55 ce 91 6c ea 17 11 6e 5b e5 b4 b6 99 39 1e d7 08 65 0b e0 61 64 55 4c 92 97 da 00 d6 7f be 00 52 36 f1 43 f5 90 58 f6 5b 68 87 5f 2c 84 39 48 f4 a6 4b 4e 92 5d b0 12 60 b1 51 16 81 65 c3 0a a7 9d 87 8f 8a c4 c0 43 b9 e9 01 70 a8 6f 32 2d d9 02 ad 4a 78 bf 45 31 a0 8d 4e 4b 7d d3 53 c2 1b 73 39 97 f6 71 18 64 98 3b 8c f7 20 36 b1 d1 7c df 79 07 ea 90 81 4b b4 14 fd 38 8d 74 31 20 09 dd 2e ac 7f 97 25 ab 60 22 a2 55 89 94 0b af 6c 95 Data Ascii: dvxUh.;H<:kK E0=BGa>K{.x}/u-!eAZ?q\6<_Uln[9eadULR6CX[h_,9HKN]`QeCpo2-JxE1NK}Ss9qd; 6|yK8t1 .%`"Ul

Timestamp	kBytes transferred	Direction	Data
2021-11-22 18:40:22 UTC	155	IN	Data Raw: da 3d 8b 4e b7 d1 81 15 5d 73 68 fb 72 5f d5 12 10 08 ff 9f 5c 6c 27 b8 09 95 2c 39 35 90 a3 04 e4 35 c0 58 f6 c9 44 72 75 25 d5 e4 a2 92 30 ac 71 6a 5a cc 66 42 8a 88 a8 4c 6a 68 09 cb 03 42 ff 5b d0 ba 13 99 41 08 9d 5d 5f c6 18 2d ea d9 07 e9 e2 18 4d ca fb 1c c1 b8 58 5b 3f cb f5 c8 4f 5a fc d8 d1 d5 9f b8 d4 37 88 a7 30 eb 35 12 da f8 3d 57 0a c7 22 a2 c1 32 86 e9 21 fb 26 15 d9 f7 c5 08 fe d4 2f 8b 4b b8 c9 6f 36 8f 9f 16 13 3a 10 af 3c 27 dd bb 1a 49 53 09 8e fd d3 1b ce ed 92 e4 f2 48 b7 7c c6 a8 fc f3 ec b5 be 54 27 57 95 a3 1e ae 94 7e 92 11 b6 ae aa 03 09 a4 6d 40 13 ea d9 fd ee 0e 07 70 ed 61 3a d7 66 e7 68 24 b6 de 1d 8e 31 7d ff 7e 0c 79 79 49 73 12 7e 49 4b a9 4f 96 8f e4 8b dc d7 73 e2 60 11 fa 40 51 25 9c 03 c0 f3 86 6c be b6 a4 09 dc 43 Data Ascii: =N]shr_\l',955XDru%0qjZfBLjhB[A]_-MX[?OZ705=W"2!&/Ko6:<'ISH|T'W~m@pa:fh$1}~yyIs~IKOs`@Q%lC
2021-11-22 18:40:22 UTC	157	IN	Data Raw: 8a 54 46 91 64 ff 44 62 9d dc 8f ee 1a 88 16 8e b0 28 d3 9a a3 12 24 3c a4 ea 33 ad 0e 35 09 55 aa 5b d5 30 f0 b2 09 fc 3a 0a 87 29 a2 bd 0e ea e5 ee 31 f3 45 be dc 25 b8 8c d9 c1 ea 7d 56 7f 0b 2c 96 43 bb 05 1b 91 03 d6 bf 27 75 6e 34 dc 1e 23 99 a0 c4 51 bb c9 2c e5 6d 47 c2 b7 3b a9 59 48 e2 02 be 47 f0 17 d8 8f 70 55 46 87 66 6a cd 54 fe 4e a7 e6 c7 53 d2 ee 6a 7b 32 05 36 64 4e 9a d2 ce f6 4c 4b b1 54 06 50 b9 2d 23 1e f4 3d 23 70 b0 47 d3 22 a8 c9 92 71 e3 0e 0c b8 6e 97 fc b5 a4 17 4d 19 7e 90 b8 1c 4b 31 31 26 4d e8 e8 b6 5c 47 c7 0f 8a 91 19 b0 6f 78 22 f6 b1 9e d8 67 4b c7 49 75 32 73 08 30 45 8b c1 bd 5b 0c d2 be 03 4c 63 43 1b 23 48 1b 9a ed 19 13 3b 9a 90 f4 04 51 d7 dd c1 18 d1 c1 61 5f fc 2a f2 2c 8d 63 a4 05 8d bf c3 8b 38 c9 71 a2 52 f5 Data Ascii: TFdDb($<35U[0:)1E%}V,C'un4#Q,mG;YHGpUFfjTNSj{26dNLKTP-#=#pG"qnM~K11&M\Gox"gKIu2s0E[LcC#H;Qa_*,c8qR
2021-11-22 18:40:22 UTC	158	IN	Data Raw: 37 6b 79 60 5a 14 3f 46 21 2b 72 7b 0f 23 7c 19 e3 32 27 a1 41 75 c8 36 6c 98 21 72 3b 90 ac d4 5f b1 8b b9 a6 95 0a fb a3 78 37 0c 06 32 6b f2 fd 49 46 6e 11 ed d0 e0 a6 6b 98 19 5e 2d f8 e7 76 28 bc 05 78 aa 5c e4 ff f9 76 f8 6e c4 8f 32 ac 6f 3d e5 68 ad f3 5f 1b 1f ef 00 de ff 2f 2e f2 77 24 65 80 53 62 1b f2 ae f1 cb 63 72 e1 4d ec ca 82 89 0d 28 9d ec d1 dc 28 85 c3 52 6c 9f fc 84 99 2a 09 76 d2 df c0 02 29 e8 cb 08 34 0d e8 2f b6 07 85 58 52 99 b2 a4 29 13 da 10 af 14 26 dd bb 0a 79 72 39 f5 cd 19 2b e0 dc fc d5 6a 79 13 4d 6a 99 4a c2 50 84 5b 65 cc 66 64 92 e9 9f 96 4c 9a 23 a5 9c b3 31 2d 96 47 72 26 d8 e2 cf a8 3c 4b 42 ba 53 67 e5 0e d5 06 16 ce ec 63 bc bb 4f 70 4c 99 4b d0 7b c7 20 be 7b 8e 9b 83 a4 57 d6 55 ee 35 41 0a 52 eb c8 54 62 16 af Data Ascii: 7ky`Z?F!+r{#|2'Au6l!r;_x72kIFnk^-v(x\vn2o=h_/.w$eSbcrM((Rl*v)4/XR)&yr9+jyMjJP[efdL#1-Gr&<KBSgcOpLK{{WU5ARTb

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Sales Order List.exe PID: 5788 Parent PID: 1004

General

Start time:	19:39:40
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\Sales Order List.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Sales Order List.exe"
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	80BAD0903EE7EC98805678673720CFD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.125547203981.00000000022E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: Sales Order List.exe PID: 6892 Parent PID: 5788

General

Start time:	19:40:00
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\Sales Order List.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Sales Order List.exe"
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	80BAD0903EE7EC98805678673720CFD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000000.125545111088.0000000001660000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.125765591469.00000000018A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.125765591469.00000000018A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.125766752022.00000000018F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.125766752022.00000000018F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.125766920138.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.125766920138.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.125766406921.00000000018A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.125766406921.00000000018A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.125766059758.00000000018F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.125766059758.00000000018F2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: explorer.exe PID: 4576 Parent PID: 6892

General

Start time:	19:40:23
Start date:	22/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff7d13c0000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6232 Parent PID: 6892

General

Start time:	19:40:33
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "C:\ProgramData\images.exe"
Imagebase:	0x890000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: images.exe PID: 4192 Parent PID: 6892

General

Start time:	19:40:33
Start date:	22/11/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	80BAD0903EE7EC98805678673720CFD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.125996962988.0000000002330000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.125886367131.0000000002330000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.125990940523.0000000002330000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.125891818807.0000000002330000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000002.126072449802.0000000002330000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 40%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 4528 Parent PID: 6232

General

Start time:	19:40:33
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60d590000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: reg.exe PID: 4904 Parent PID: 6232

General

Start time:	19:40:33
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /t REG_SZ /d "C:\ProgramData\images.exe"
Imagebase:	0xf0000
File size:	59392 bytes
MD5 hash:	CDD462E86EC0F20DE2A1D781928B1B0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: WerFault.exe PID: 4220 Parent PID: 4192

General

Start time:	19:40:36
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4192 -s 740
Imagebase:	0x5c0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 3440 Parent PID: 4192

General

Start time:	19:40:46
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4192 -s 772
Imagebase:	0x5c0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Disassembly

Code Analysis