LAB 6

Name : ARAVINDHAN.K

ROLL NO :CH.EN.U4CYS22001

## Hard Disk Forensics

1. Define Hard Disk Forensics

Answer: The process of analyzing digital data stored on a hard drive to uncover evidence related to cybercrimes or data breaches.

2. What is an Image File?

Answer: An exact copy of the original data stored on a disk, capturing all files, partitions, and metadata.

3. What is Allocated and Unallocated Space?

Answer:

- Allocated Space: Areas of the disk currently being used to store data
- Unallocated Space: Free or deleted areas that may still contain recoverable data

4. What is Disk Cache and Disk Mirroring?

Answer:

- Disk Cache: Temporary storage area holding frequently accessed data to speed up retrieval

- Disk Mirroring: Process of duplicating data across two or more disks for redundancy

5. What is a Forensic Image?

Answer: An exact replica of a storage device captured for forensic examination without altering the original data.

6. What is Meant by Hash Value of a Hard Disk?

Answer: A unique cryptographic fingerprint generated using algorithms like MD5 or SHA to ensure data integrity.

7. What is Shadow Volume, Shadow Copy, and Swap Disk?

Answer:

- Shadow Volume/Copy: Snapshot of a disk taken at a specific time to recover previous file versions

- Swap Disk: Used to temporarily store data when RAM is full

## 8. Tools for Hard Disk Forensics

Answer:

- Autopsy
- EnCase
- FTK (Forensic Toolkit)
- X-Ways Forensics
- Sleuth Kit

## 9. EXIF Metadata

Answer: Contains information about an image file, such as camera model, date/time, and GPS coordinates.

## 10. Common Disk Image Formats

Answer:

- E01 (EnCase)
- DD (raw image)
- AFF (Advanced Forensics Format)

## 11. What is Bit-by-Bit Copying?

Answer: A forensic method of duplicating every sector of a storage device exactly as it is.

12. What is Cloning a Disk?

Answer: Creating an identical copy of an entire disk, including OS and files, for backup or forensic analysis.

13. Types of Latest Storage Devices

Answer:

- SSDs
- NVMe drives
- Hybrid drives
- Cloud-based storage solutions

14. What is BitLocker Encryption?

Answer: A Windows security feature that encrypts entire drives to prevent unauthorized access.

## Email Forensics

1. Define Email Forensics

Answer: Investigation of email content, metadata, and headers to detect fraudulent activities, phishing, and other cybercrimes.

2. What is X-Received?

Answer: An email header field indicating each hop the email took through servers.

3. What is Received SPF?

Answer: Sender Policy Framework (SPF) is an authentication mechanism verifying if the sending server is authorized for the domain.

4. What is DKIM Signature?

Answer: DomainKeys Identified Mail Signature is an email security protocol that validates email authenticity using cryptographic signatures.

5. What is ARC Seal?

Answer: Authenticated Received Chain (ARC) seal ensures email forwarding integrity across intermediaries.

6. MIME-Version

Answer: Specifies the version of the Multipurpose Internet Mail Extensions (MIME) standard used in the email.

7. X-Originating IP

Answer: Reveals the original sender's IP address before email routing.

8. Email Backup File Formats

Answer:

- PST (Outlook)
- MBOX
- EML
- OST

9. Email-Related Acronyms

Answer:

- FQDN: Fully Qualified Domain Name
- MUA: Mail User Agent
- MTA: Mail Transfer Agent
- TNEF: Transport Neutral Encapsulation Format

- MIME: Multipurpose Internet Mail Extensions
- MD5: Message-Digest Algorithm 5
- SHA1: Secure Hash Algorithm 1
- CC: Carbon Copy
- BCC: Blind Carbon Copy

Network Forensics

1. Define Network Forensics

Answer: The process of capturing, analyzing, and investigating network traffic to detect and respond to security incidents.

2. What is Packet Capture (PCAP)?

Answer: The process of recording network packets for analysis and troubleshooting.

3. What is Libpcap?

Answer: A C library that provides an interface for capturing network packets.

4. What is Promiscuous Mode?

Answer: A network setting where a device captures all traffic on a network segment, not just traffic addressed to it.

5. 10 Features of Wireshark

Answer:

1. Live traffic capture
2. Protocol analysis
3. Filtering
4. Packet decoding
5. Statistics generation
6. Coloring rules
7. Export capabilities
8. Decryption support
9. Customizable reports
10. Expert analysis tools

6. Use of Hex Editor

Answer: Used to view and edit raw binary data of files and network packets.

7. What is Malware?

Answer: Malicious software designed to harm or exploit computer systems and networks.

8. What is Address Spoofing?

Answer: The act of falsifying source addresses in packets to disguise the true origin.

9. "Catch it as you can" Method

Answer: A network forensic method where all traffic is continuously captured and stored for later analysis.

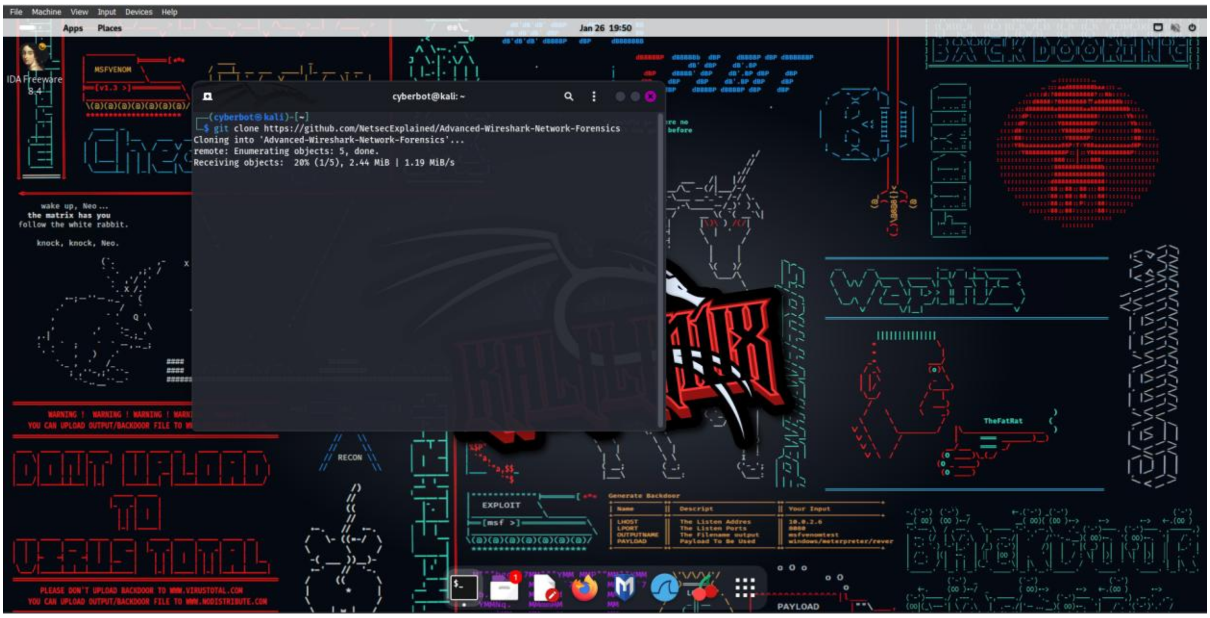
10. "Stop, Look, and Listen" Method

Answer: A method where traffic is analyzed in real time, and only relevant data is logged.

# Advanced Network Forensics Lab 6

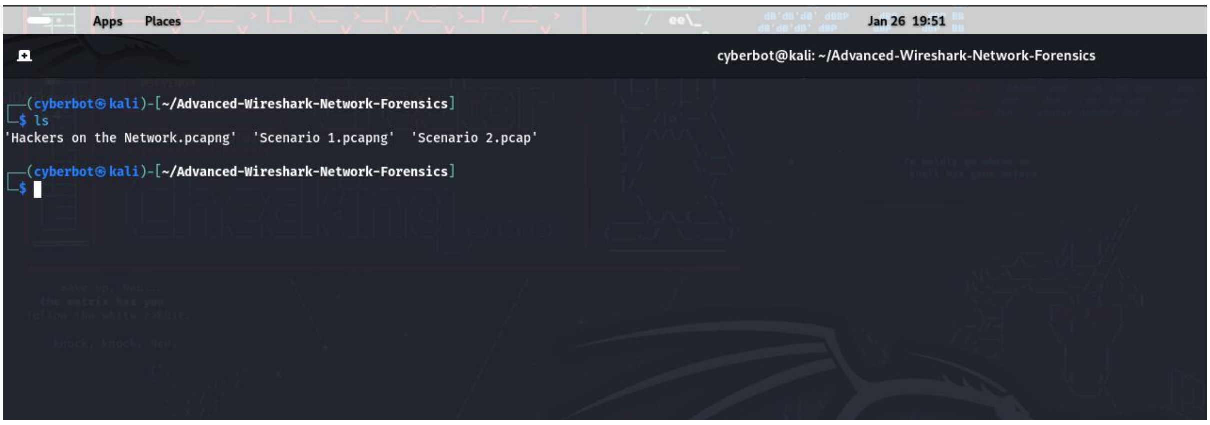
## Prerequisites for lab

## Downloading the scenario files from github screenshot



```
┌──(cyberbot㉿kali)-[~]
└─$ git clone https://github.com/NetsecExplained/Advanced-Wireshark-Network-Forensics
Cloning into 'Advanced-Wireshark-Network-Forensics'...
remote: Enumerating objects: 5, done.
Receiving objects:  20% (1/5), 2.44 MiB | 1.19 MiB/s
```

## List of files under that repo



```
┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ ls
'Hackers on the Network.pcapng'  'Scenario 1.pcapng'  'Scenario 2.pcap'

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ 
```

## Overview

This lab document provides a comprehensive guide to network forensics investigation techniques using Wireshark for analyzing malware and network attacks.

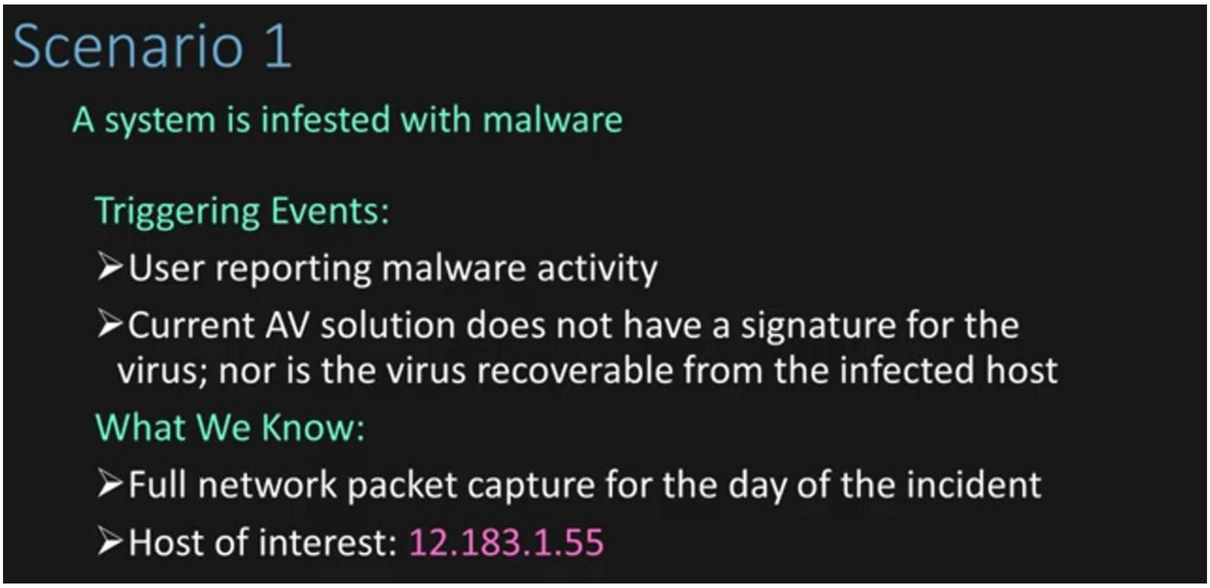
## Required Tools

- Wireshark (latest version)
- Hex Editor (recommended: HxD or010 Editor)
- Virtual Machine for Safe Analysis
- Online Malware Analysis Platform (VirusTotal)

## Safety Precautions

- ALWAYS analyze malware in an isolated, sandboxed environment
- Use snapshots or disposable virtual machines
- Never analyze malware on a production system

## Scenario 1: Malware Infection Investigation



# Scenario 1

A system is infested with malware

Triggering Events:

- User reporting malware activity
- Current AV solution does not have a signature for the virus; nor is the virus recoverable from the infected host

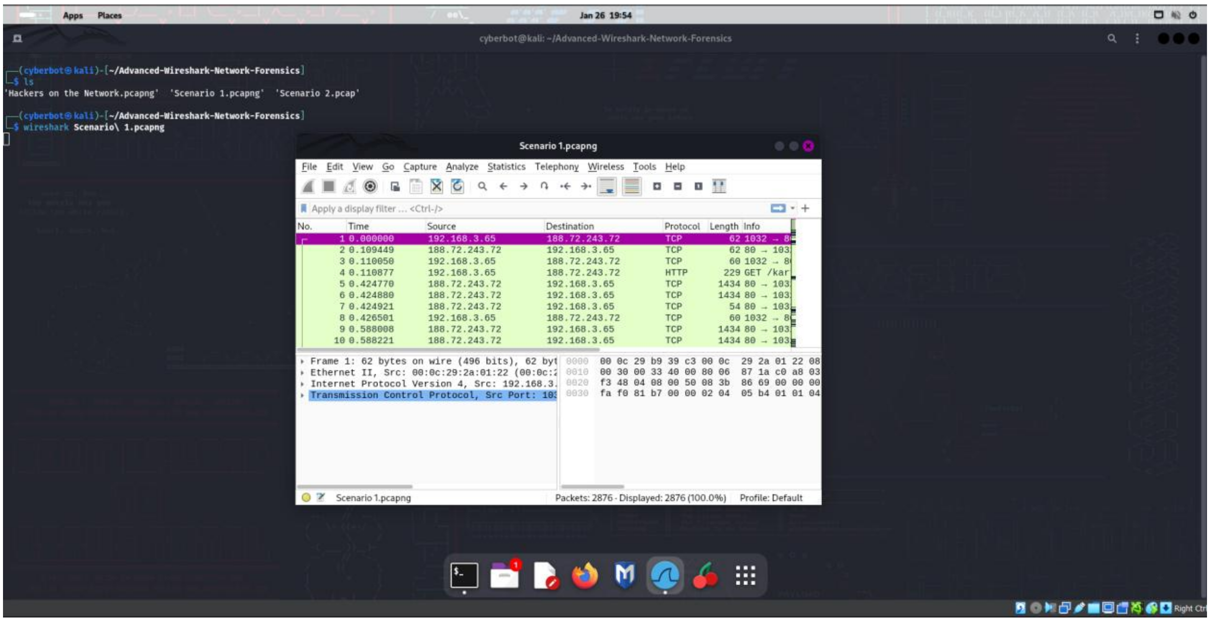
What We Know:

- Full network packet capture for the day of the incident
- Host of interest: 12.183.1.55

Step 1:

Opening the file in wireshark

And starting the investigation



Apps
Places
Jan 26 19:54
cyberbot@kali: ~/Advanced-Wireshark-Network-Forensics

```
┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ ls
'Hackers on the Network.pcapng'  'Scenario 1.pcapng'  'Scenario 2.pcap'

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ wireshark Scenario\ 1.pcapng
```

Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination     Protocol  Length Info
    1 0.000000   192.168.3.65    188.72.243.72   TCP         62 1032 → 8
    2 0.109449   188.72.243.72   192.168.3.65    TCP         62 80 → 103
    3 0.110050   192.168.3.65    188.72.243.72   TCP         60 1032 → 8
    4 0.110877   192.168.3.65    188.72.243.72   HTTP       229 GET /kar
    5 0.424770   188.72.243.72   192.168.3.65    TCP       1434 80 → 103
    6 0.424880   188.72.243.72   192.168.3.65    TCP       1434 80 → 103
    7 0.424921   188.72.243.72   192.168.3.65    TCP         54 80 → 103
    8 0.426501   192.168.3.65    188.72.243.72   TCP         60 1032 → 8
    9 0.588008   188.72.243.72   192.168.3.65    TCP       1434 80 → 103
   10 0.588221   188.72.243.72   192.168.3.65    TCP       1434 80 → 103
```

```
› Frame 1: 62 bytes on wire (496 bits), 62 byt
› Ethernet II, Src: 00:0c:29:2a:01:22 (00:0c:2
› Internet Protocol Version 4, Src: 192.168.3.
› Transmission Control Protocol, Src Port: 103
```

```
0000  00 0c 29 b9 39 c3 00 0c  29 2a 01 22 08
0010  00 30 00 33 40 00 80 06  87 1a c0 a8 03
0020  f3 48 04 08 00 50 08 3b  86 69 00 00 00
0030  fa f0 81 b7 00 00 02 04  05 b4 01 01 04
```

## Preliminary Investigation Steps

1. Initial Packet Capture Examination

- Identifing the infected host IP address

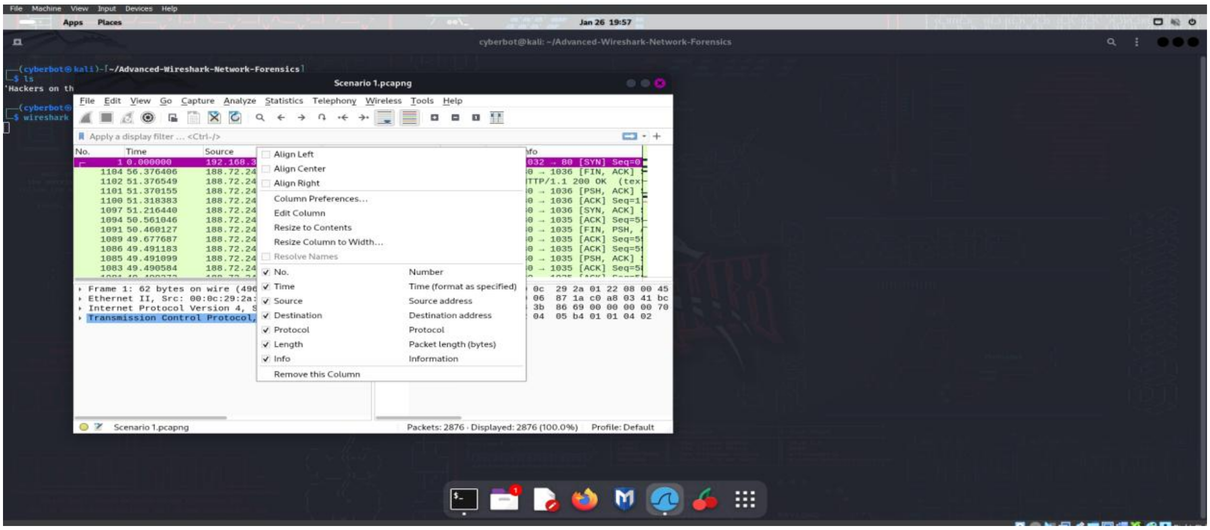
- just configure Wireshark and add two custom columns

- Stream ID and filter is tcp.stream

- Host and filter is http.host

Then save it

## -like below

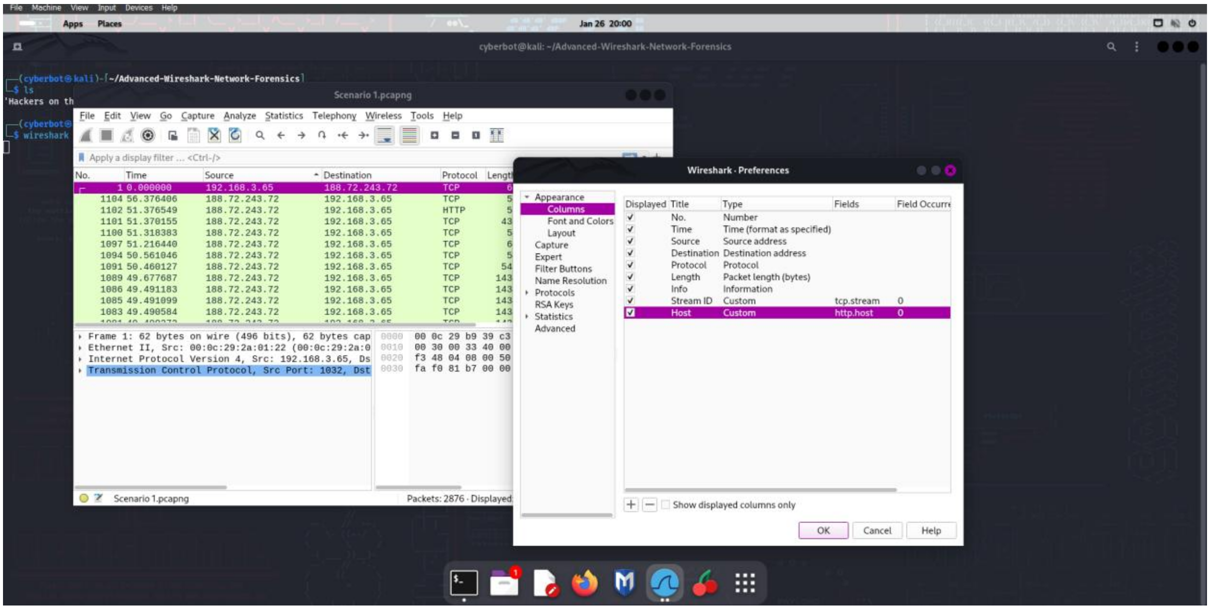


File Machine View Input Devices Help
Apps Places
Jan 26 19:57
cyberbot@kali: ~/Advanced-Wireshark-Network-Forensics
Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
□ Align Left
□ Align Center
□ Align Right
Column Preferences…
Edit Column
Resize to Contents
Resize Column to Width…
□ Resolve Names
Remove this Column
Scenario 1.pcapng
Packets: 2876 · Displayed: 2876 (100.0%)
Profile: Default

```
┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ ls
'Hackers on th

┌──(cyberbot㉿
└─$ wireshark
```

| | |
|---|---|
| ☑ No. | Number |
| ☑ Time | Time (format as specified) |
| ☑ Source | Source address |
| ☑ Destination | Destination address |
| ☑ Protocol | Protocol |
| ☑ Length | Packet length (bytes) |
| ☑ Info | Information |

```
No.   Time          Source          ...nfo
   1 0.000000       192.168.3       032 → 80 [SYN] Seq=0
1104 56.376406      188.72.24       0 → 1036 [FIN, ACK]
1102 51.376549      188.72.24       TTP/1.1 200 OK  (tex
1101 51.370155      188.72.24       0 → 1036 [PSH, ACK]
1100 51.318383      188.72.24       0 → 1036 [ACK] Seq=1
1097 51.216440      188.72.24       0 → 1036 [SYN, ACK]
1094 50.561046      188.72.24       0 → 1035 [ACK] Seq=5
1091 50.460127      188.72.24       0 → 1035 [FIN, PSH,
1089 49.677687      188.72.24       0 → 1035 [ACK] Seq=5
1086 49.491183      188.72.24       0 → 1035 [ACK] Seq=5
1085 49.491099      188.72.24       0 → 1035 [PSH, ACK]
1083 49.490584      188.72.24       0 → 1035 [ACK] Seq=5

› Frame 1: 62 bytes on wire (496
› Ethernet II, Src: 00:0c:29:2a:
› Internet Protocol Version 4, S
› Transmission Control Protocol,

0c  29 2a 01 22 08 00 45
06  87 1a c0 a8 03 41 bc
3b  86 69 00 00 00 00 70
04  05 b4 01 01 04 02
```



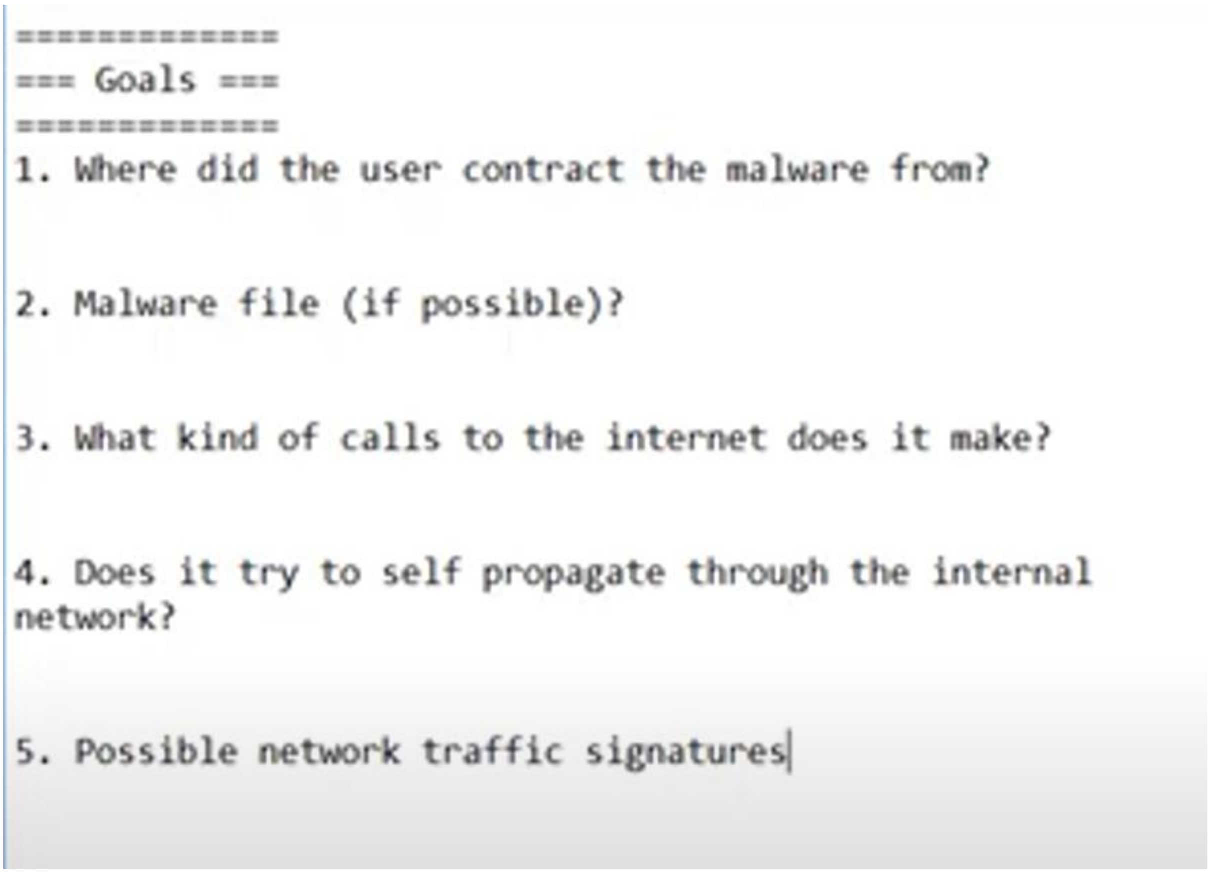
File Machine View Input Devices Help
Apps Places
Jan 26 20:00
cyberbot@kali: ~/Advanced-Wireshark-Network-Forensics
Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Scenario 1.pcapng
Packets: 2876 · Displayed
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Show displayed columns only
OK
Cancel
Help

```
┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ ls
'Hackers on th

┌──(cyberbot㉿
└─$ wireshark
```

```
No.   Time          Source          Destination     Protocol  Lengt
   1 0.000000       192.168.3.65    188.72.243.72   TCP          6
1104 56.376406      188.72.243.72   192.168.3.65    TCP          5
1102 51.376549      188.72.243.72   192.168.3.65    HTTP         5
1101 51.370155      188.72.243.72   192.168.3.65    TCP         43
1100 51.318383      188.72.243.72   192.168.3.65    TCP          5
1097 51.216440      188.72.243.72   192.168.3.65    TCP          6
1094 50.561046      188.72.243.72   192.168.3.65    TCP          5
1091 50.460127      188.72.243.72   192.168.3.65    TCP         54
1089 49.677687      188.72.243.72   192.168.3.65    TCP        143
1086 49.491183      188.72.243.72   192.168.3.65    TCP        143
1085 49.491099      188.72.243.72   192.168.3.65    TCP        143
1083 49.490584      188.72.243.72   192.168.3.65    TCP        143

› Frame 1: 62 bytes on wire (496 bits), 62 bytes cap   0000  00 0c 29 b9 39 c3
› Ethernet II, Src: 00:0c:29:2a:01:22 (00:0c:29:2a:0   0010  00 30 00 33 40 00
› Internet Protocol Version 4, Src: 192.168.3.65, Ds   0020  f3 48 04 08 00 50
› Transmission Control Protocol, Src Port: 1032, Dst   0030  fa f0 81 b7 00 00
```

| Displayed | Title | Type | Fields | Field Occurre |
|---|---|---|---|---|
| ✓ | No. | Number | | |
| ✓ | Time | Time (format as specified) | | |
| ✓ | Source | Source address | | |
| ✓ | Destination | Destination address | | |
| ✓ | Protocol | Protocol | | |
| ✓ | Length | Packet length (bytes) | | |
| ✓ | Info | Information | | |
| ✓ | Stream ID | Custom | tcp.stream | 0 |
| ☑ | Host | Custom | http.host | 0 |

## Goals To find



```
==============
=== Goals ===
==============
1. Where did the user contract the malware from?


2. Malware file (if possible)?


3. What kind of calls to the internet does it make?


4. Does it try to self propagate through the internal
network?


5. Possible network traffic signatures
```

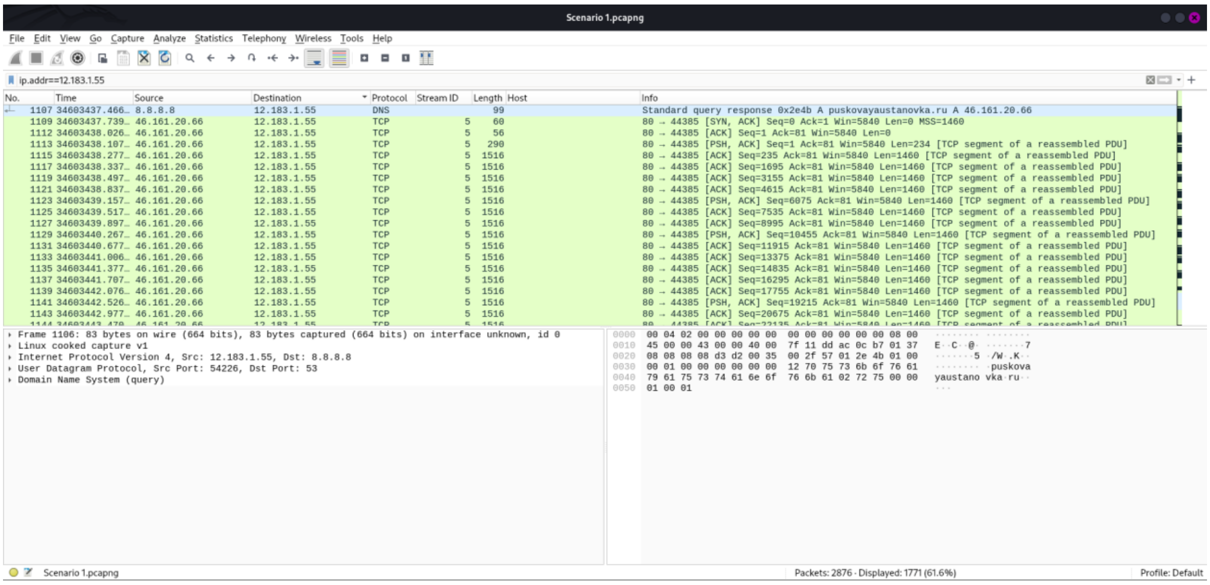
- Document investigation goals and findings

Answer for 1)

Lets start with pattern matching using the victim ip give in scenario description

VICTIM IP:12.183.1.55

Command “ip.addr==12.183.1.55”



Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==12.183.1.55

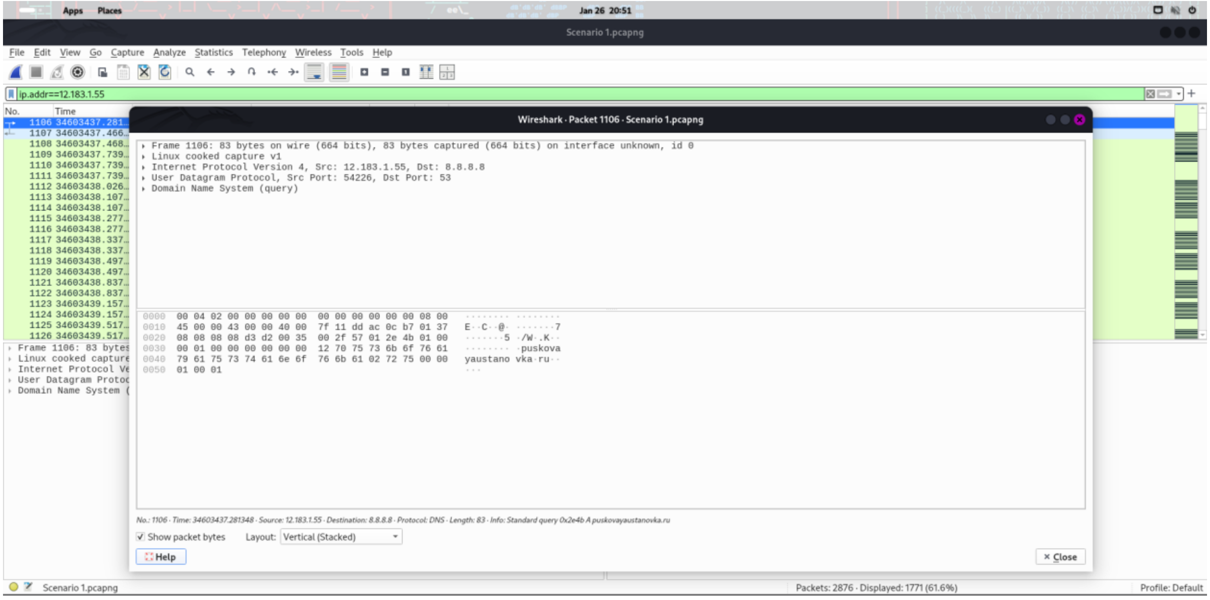
```
No.   Time              Source        Destination   Protocol Stream ID Length Host  Info
 1107 34603437.466… 8.8.8.8       12.183.1.55   DNS                 99        Standard query response 0x2e4b A puskovayaustanovka.ru A 46.161.20.66
 1109 34603437.739… 46.161.20.66  12.183.1.55   TCP          5      60        80 → 44385 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 1112 34603438.026… 46.161.20.66  12.183.1.55   TCP          5      56        80 → 44385 [ACK] Seq=1 Ack=81 Win=5840 Len=0
 1113 34603438.107… 46.161.20.66  12.183.1.55   TCP          5     290        80 → 44385 [PSH, ACK] Seq=1 Ack=81 Win=5840 Len=234 [TCP segment of a reassembled PDU]
 1115 34603438.277… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=235 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1117 34603438.337… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=1695 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1119 34603438.497… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=3155 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1121 34603438.837… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=4615 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1123 34603439.157… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [PSH, ACK] Seq=6075 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1125 34603439.517… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=7535 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1127 34603439.897… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=8995 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1129 34603440.267… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [PSH, ACK] Seq=10455 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1131 34603440.677… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=11915 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1133 34603441.006… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=13375 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1135 34603441.377… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=14835 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1137 34603441.707… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=16295 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1139 34603442.076… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=17755 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1141 34603442.526… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [PSH, ACK] Seq=19215 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1143 34603442.977… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=20675 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
 1144 34603443.470… 46.161.20.66  12.183.1.55   TCP          5    1516        80 → 44385 [ACK] Seq=22135 Ack=81 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
```

```
› Frame 1106: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface unknown, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 12.183.1.55, Dst: 8.8.8.8
› User Datagram Protocol, Src Port: 54226, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 04 02 00 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 43 00 00 40 00  7f 11 dd ac 0c b7 01 37   E··C··@· ·······7
0020  08 08 08 08 d3 d2 00 35  00 2f 57 01 2e 4b 01 00   ·······5 ·/W·.K··
0030  00 01 00 00 00 00 00 00  12 70 75 73 6b 6f 76 61   ········ ·puskova
0040  79 61 75 73 74 61 6e 6f  76 6b 61 02 72 75 00 00   yaustano vka·ru··
0050  01 00 01                                           ···
```

Scenario 1.pcapng   Packets: 2876 · Displayed: 1771 (61.6%)   Profile: Default

# We can find the



Apps Places
Jan 26 20:51
Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 1106 · Scenario 1.pcapng

ip.addr==12.183.1.55

```
No.   Time
 1106 34603437.281…
 1107 34603437.466…
 1108 34603437.468…
 1109 34603437.739…
 1110 34603437.739…
 1111 34603437.739…
 1112 34603438.026…
 1113 34603438.107…
 1114 34603438.107…
 1115 34603438.277…
 1116 34603438.277…
 1117 34603438.337…
 1118 34603438.337…
 1119 34603438.497…
 1120 34603438.497…
 1121 34603438.837…
 1122 34603438.837…
 1123 34603439.157…
 1124 34603439.157…
 1125 34603439.517…
 1126 34603439.517…
```

```
› Frame 1106: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface unknown, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 12.183.1.55, Dst: 8.8.8.8
› User Datagram Protocol, Src Port: 54226, Dst Port: 53
› Domain Name System (query)
```

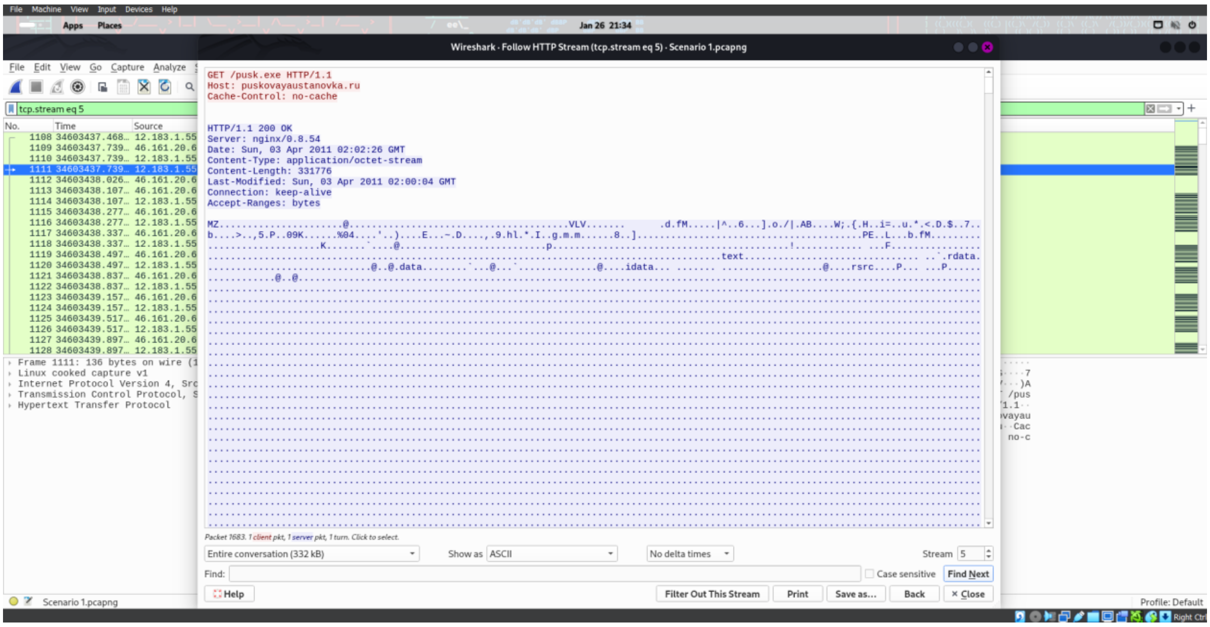
```
0000  00 04 02 00 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 43 00 00 40 00  7f 11 dd ac 0c b7 01 37   E··C··@· ·······7
0020  08 08 08 08 d3 d2 00 35  00 2f 57 01 2e 4b 01 00   ·······5 ·/W·.K··
0030  00 01 00 00 00 00 00 00  12 70 75 73 6b 6f 76 61   ········ ·puskova
0040  79 61 75 73 74 61 6e 6f  76 6b 61 02 72 75 00 00   yaustano vka·ru··
0050  01 00 01                                           ···
```

No.: 1106 · Time: 34603437.281348 · Source: 12.183.1.55 · Destination: 8.8.8.8 · Protocol: DNS · Length: 83 · Info: Standard query 0x2e4b A puskovayaustanovka.ru

☑ Show packet bytes   Layout: Vertical (Stacked)

Scenario 1.pcapng   Packets: 2876 · Displayed: 1771 (61.6%)   Profile: Default

Follow TCP stream for a suspicious website of .ru domain



Wireshark · Follow HTTP Stream (tcp.stream eq 5) · Scenario 1.pcapng

```
GET /pusk.exe HTTP/1.1
Host: puskovayaustanovka.ru
Cache-Control: no-cache


HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Sun, 03 Apr 2011 02:02:26 GMT
Content-Type: application/octet-stream
Content-Length: 331776
Last-Modified: Sun, 03 Apr 2011 02:00:04 GMT
Connection: keep-alive
Accept-Ranges: bytes

MZ.......................@...............................VLV.......
```

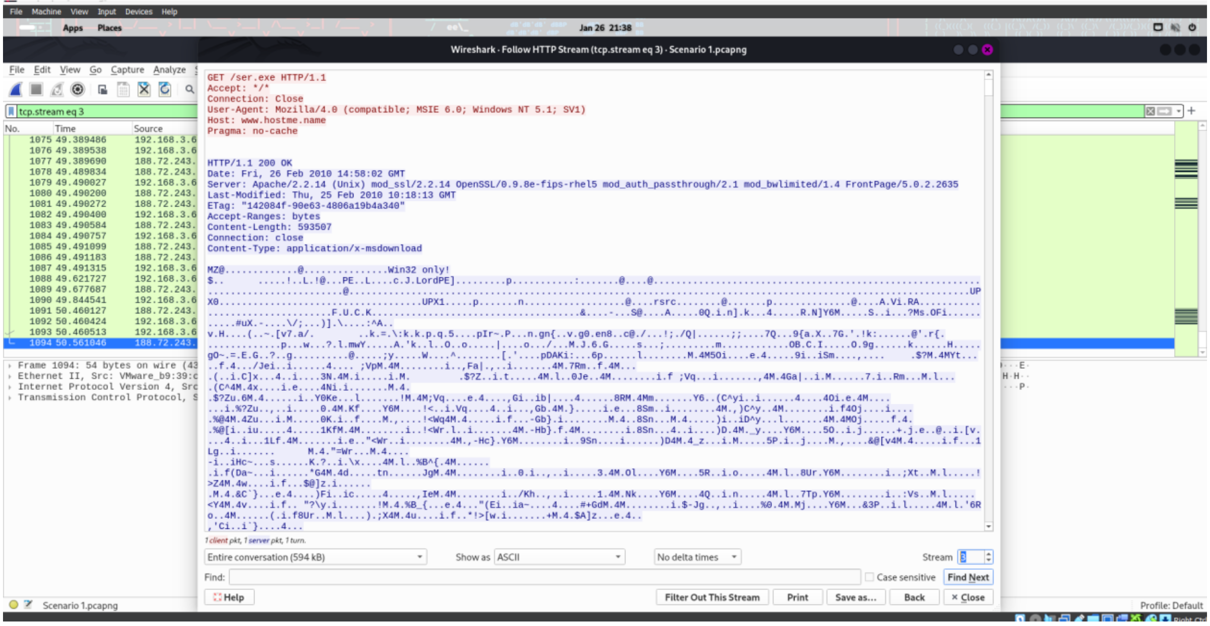
Answer :

The user contracted the malware from puskovayaustanovka.ru/pusk.exe

No USER-AGENT found

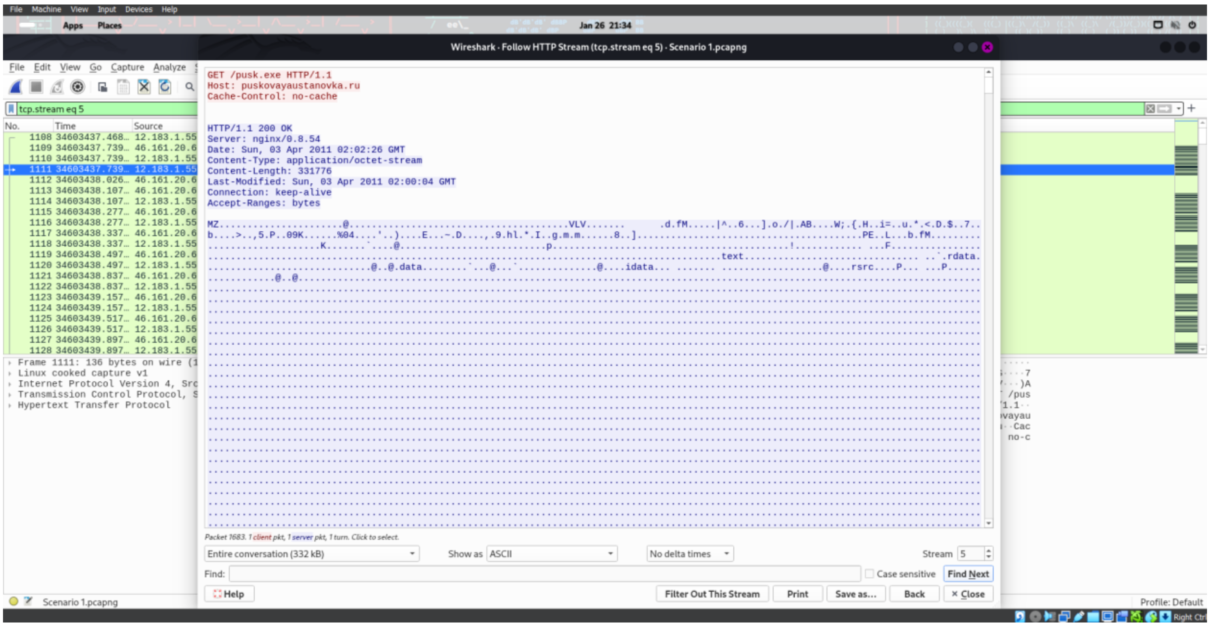
# 2.Malware file if possible ?

## – Analyze download request characteristics



Wireshark · Follow HTTP Stream (tcp.stream eq 3) · Scenario 1.pcapng

```
GET /ser.exe HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.hostme.name
Pragma: no-cache


HTTP/1.1 200 OK
Date: Fri, 26 Feb 2010 14:58:02 GMT
Server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Last-Modified: Thu, 25 Feb 2010 10:18:13 GMT
ETag: "142084f-90e63-4806a19b4a340"
Accept-Ranges: bytes
Content-Length: 593507
Connection: close
Content-Type: application/x-msdownload

MZ@.............@...............Win32 only!
```



File Machine View Input Devices Help
Apps Places
Jan 26 21:34
Wireshark · Follow HTTP Stream (tcp.stream eq 5) · Scenario 1.pcapng
File Edit View Go Capture Analyze

tcp.stream eq 5

```
No.   Time               Source
1108 34603437.468…  12.183.1.55
1109 34603437.739…  46.161.20.6
1110 34603437.739…  12.183.1.55
1111 34603437.739…  12.183.1.55
1112 34603438.026…  46.161.20.6
1113 34603438.107…  46.161.20.6
1114 34603438.107…  12.183.1.55
1115 34603438.277…  46.161.20.6
1116 34603438.277…  12.183.1.55
1117 34603438.337…  46.161.20.6
1118 34603438.337…  12.183.1.55
1119 34603438.497…  46.161.20.6
1120 34603438.497…  12.183.1.55
1121 34603438.837…  46.161.20.6
1122 34603438.837…  12.183.1.55
1123 34603439.157…  46.161.20.6
1124 34603439.157…  12.183.1.55
1125 34603439.517…  46.161.20.6
1126 34603439.517…  12.183.1.55
1127 34603439.897…  46.161.20.6
1128 34603439.897…  12.183.1.55
› Frame 1111: 136 bytes on wire (1
› Linux cooked capture v1
› Internet Protocol Version 4, Src
› Transmission Control Protocol, S
› Hypertext Transfer Protocol
```

```
GET /pusk.exe HTTP/1.1
Host: puskovayaustanovka.ru
Cache-Control: no-cache


HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Sun, 03 Apr 2011 02:02:26 GMT
Content-Type: application/octet-stream
Content-Length: 331776
Last-Modified: Sun, 03 Apr 2011 02:00:04 GMT
Connection: keep-alive
Accept-Ranges: bytes

MZ......................@.......................................VLV.......      .d.fM.....|^..6...].o./|.AB....W;.{.H..i=..u.*.<.D.$..7..
b....>..,5.P..09K......%04....'..)....E...~.D....,.9.hl.*.I..g.m.m......8..]..................................PE..L...b.fM.........
....................K.......`....@..........................p....................................!............ ...F................
..............................................................................text...........................................`.rdata.
.............................@..@.data........`...@...`.............@....idata...  .......  ..................@....rsrc....P...  ...P......
...........@..@.............................................................................................................................
```

Packet 1683. 1 client pkt, 1 server pkt, 1 turn. Click to select.

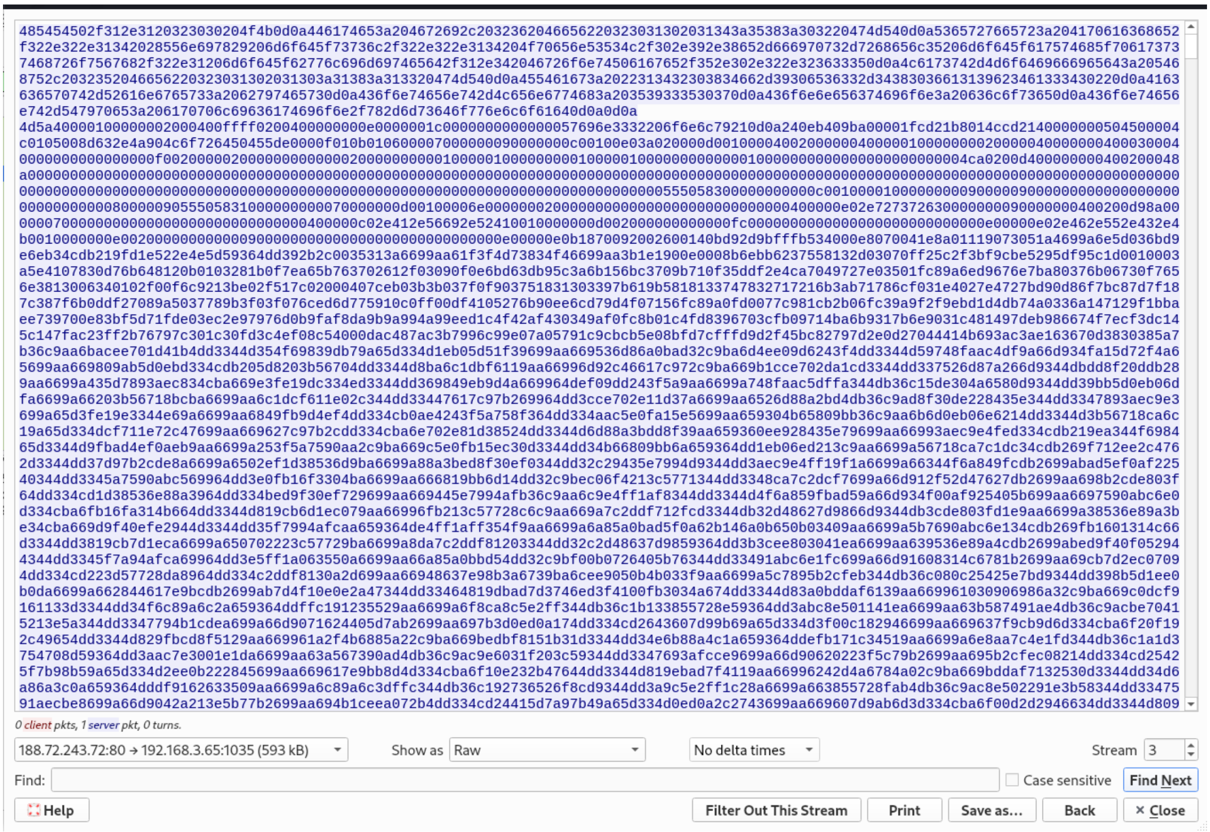
Entire conversation (332 kB) Show as ASCII No delta times Stream 5

Find: □ Case sensitive Find Next

Two malware files FOUND PUSK.EXE AND SER.EXE

- Check for unusual request patterns

MZ patterns



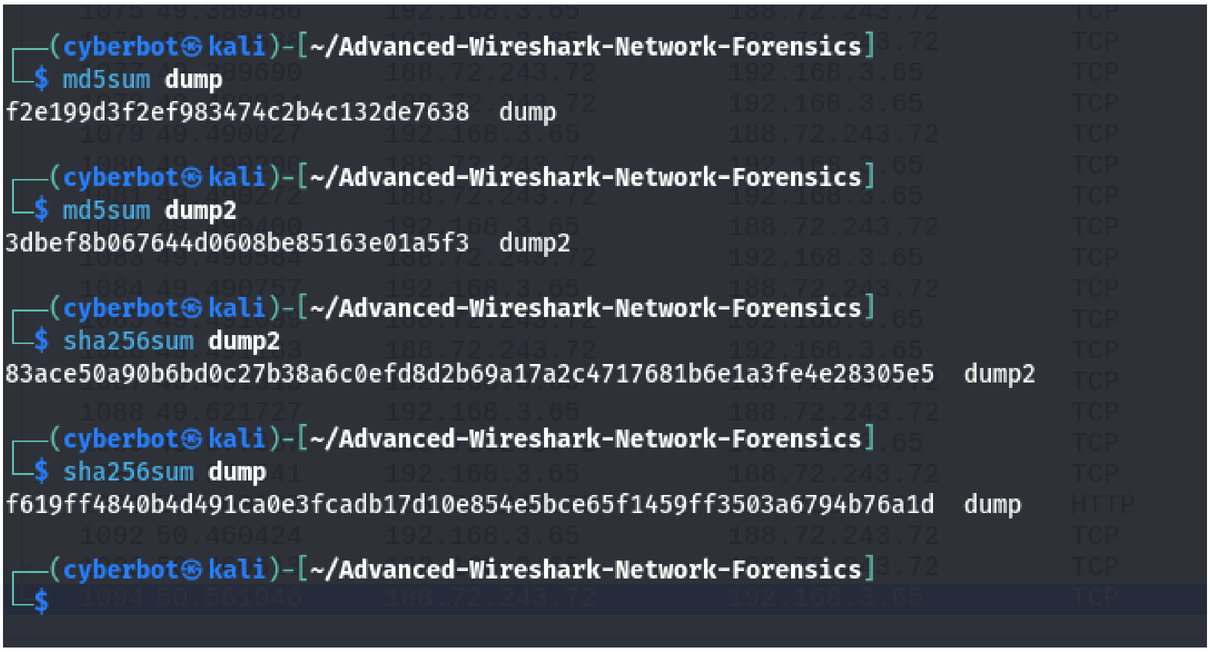
```
485454502f312e3120323030204f4b0d0a446174653a204672692c2032362046656220323031302031343a35383a303220474d540d0a5365727665723a204170616368652
f322e322e31342028556e697829206d6f645f73736c2f322e322e3134204f70656e53534c2f302e392e38652d666970732d7268656c35206d6f645f617574685f70617373
7468726f7567682f322e31206d6f645f62776c696d697465642f312e342046726f6e74506167652f352e302e322e323633350d0a4c6173742d4d6f6469666965643a20546
8752c2032352046656220323031302031303a31383a313320474d540d0a455461673a2022313432303834662d39306536332d343830366131396234613334302220d0a4163
636570742d52616e6765733a2062797465730d0a436f6e74656e742d4c656e6774683a203539333530370d0a436f6e6e656374696f6e3a20636c6f73650d0a436f6e74656
e742d547970653a206170706c69636174696f6e2f782d6d73646f776e6c6f61640d0a0d0a
4d5a40000100000002000400ffff0200400000000000e0000001c000000000000000057696e3332206f6e6c79210d0a240eb409ba00001fcd21b8014ccd21400000000504500004
c0105008d632e4a904c6f726450455de0000f010b01060000700000009000000c00100e03a020000d00100004002000000400000100000000200000400000000400030004
000000000000000f00200000200000000000000200000000001000001000000000100000100000000000000100000000000000000000000004ca0200d400000000400200048
a000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000555058300000000000c001000010000000009000009000000000000000000
000000000008000009055505831000000000007000000d00100006e00000002000000000000000000000000000000400000e02e72737263000000009000000400200d98a00
00007000000000000000000000000000400000c02e412e56692e524100100000000d002000000000000fc000000000000000000000000000e00000e02e462e552e432e4
b0010000000e002000000000000090000000000000000000000000000000e00000e0b1870092002600140bd92d9bfffb534000e8070041e8a01119073051a4699a6e5d036bd9
e6eb34cdb219fd1e522e4e5d59364dd392b2c0035313a6699aa61f3f4d73834f46699aa3b1e1900e0008b6ebb6237558132d03070ff25c2f3bf9cbe5295df95c1d0010003
a5e4107830d76b648120b0103281b0f7ea65b763702612f03090f0e6bd63db95c3a6b156bc3709b710f35ddf2e4ca7049727e03501fc89a6ed9676e7ba80376b06730f765
6e3813006340102f00f6c9213be02f517c02000407ceb03b3b037f0f903751831303397b619b5818133747832717216b3ab71786cf031e4027e4727bd90d86f7bc87d7f18
7c387f6b0ddf27089a5037789b3f03f076ced6d775910c0ff00df4105276b90ee6cd79d4f07156fc89a0fd0077c981cb2b06fc39a9f2f9ebd1d4db74a0336a147129f1bba
ee739700e83bf5d71fde03ec2e97976d0b9faf8da9b9a994a99eed1c4f42af430349af0fc8b01c4fd8396703cfb09714ba6b9317b6e9031c481497deb986674f7ecf3dc14
5c147fac23ff2b76797c301c30fd3c4ef08c54000dac487ac3b7996c99e07a05791c9cbcb5e08bfd7cfffd9d2f45bc82797d2e0d27044414b693ac3ae163670d3830385a7
b36c9aa6bacee701d41b4dd3344d354f69839db79a65d334d1eb05d51f39699aa669536d86a0bad32c9ba6d4ee09d6243f4dd3344d59748faac4df9a66d934fa15d72f4a6
5699aa669809ab5d0ebd334cdb205d8203b56704dd3344d8ba6c1dbf6119aa66996d92c46617c972c9ba669b1cce702da1cd3344dd337526d87a266d9344dbdd8f20ddb28
9aa6699a435d7893aec834cba669e3fe19dc334ed3344dd369849eb9d4a669964def09dd243f5a9aa6699a748faac5dffa344db36c15de304a6580d9344dd39bb5d0eb06d
fa6699a66203b56718bcba6699aa6c1dcf611e02c344dd33447617c97b269964dd3cce702e11d37a6699aa6526d88a2bd4db36c9ad8f30de228435e344dd3347893aec9e3
699a65d3fe19e3344e69a6699aa6849fb9d4ef4dd334cb0ae4243f5a758f364dd334aac5e0fa15e5699aa659304b65809bb36c9aa6b6d0eb06e6214dd3344d3b56718ca6c
19a65d334dcf711e72c47699aa669627c97b2cdd334cba6e702e81d38524dd3344d6d88a3bdd8f39aa659360ee928435e79699aa66993aec9e4fed334cdb219ea344f6984
65d3344d9fbad4ef0aeb9aa6699a253f5a7590aa2c9ba669c5e0fb15ec30d3344dd34b66809bb6a659364dd1eb06ed213c9aa6699a56718ca7c1dc34cdb269f712ee2c476
2d3344dd37d97b2cde8a6699a6502ef1d38536d9ba6699a88a3bed8f30ef0344dd32c29435e7994d9344dd3aec9e4ff19f1a6699a66344f6a849fcdb2699abad5ef0af225
40344dd3345a7590abc569964dd3e0fb16f3304ba6699aa666819bb6d14dd32c9bec06f4213c5771344dd3348ca7c2dcf7699a66d912f52d47627db2699aa698b2cde803f
64dd334cd1d38536e88a3964dd334bed9f30ef729699aa669445e7994afb36c9aa6c9e4ff1af8344dd3344d4f6a859fbad59a66d934f00af925405b699aa6697590abc6e0
d334cba6fb16fa314b664dd3344d819cb6d1ec079aa66996fb213c57728c6c9aa669a7c2ddf712fcd3344db32d48627d9866d9344db3cde803fd1e9aa6699a38536e89a3b
e34cba669d9f40efe2944d3344dd35f7994afcaa659364de4ff1aff354f9aa6699a6a85a0bad5f0a62b146a0b650b03409aa6699a5b7690abc6e134cdb269fb1601314c66
d3344dd3819cb7d1eca6699a650702223c57729ba6699a8da7c2ddf81203344dd32c2d48637d9859364dd3b3cee803041ea6699aa639536e89a4cdb2699abed9f40f05294
4344dd3345f7a94afca69964dd3e5ff1a063550a6699aa66a85a0bbd54dd32c9bf00b0726405b76344dd33491abc6e1fc699a66d91608314c6781b2699aa69cb7d2ec0709
4dd334cd223d57728da8964dd334c2ddf8130a2d699aa66948637e98b3a6739ba6cee9050b4b033f9aa6699a5c7895b2cfeb344db36c080c25425e7bd9344dd398b5d1ee0
b0da6699a662844617e9bcdb2699ab7d4f10e0e2a47344dd33464819dbad7d3746ed3f4100fb3034a674dd3344d83a0bddaf6139aa669961030906986a32c9ba669c0dcf9
161133d3344dd34f6c89a6c2a659364ddffc191235529aa6699a6f8ca8c5e2ff344db36c1b133855728e59364dd3abc8e501141ea6699aa63b587491ae4db36c9acbe7041
5213e5a344dd3347794b1cdea699a66d9071624405d7ab2699aa697b3d0ed0a174dd334cd2643607d99b69a65d334d3f00c182946699aa669637f9cb9d6d334cba6f20f19
2c49654dd3344d829fbcd8f5129aa669961a2f4b6885a22c9ba669bedbf8151b31d3344dd34e6b88a4c1a659364ddefb171c34519aa6699a6e8aa7c4e1fd344db36c1a1d3
754708d59364dd3aac7e3001e1da6699aa63a567390ad4db36c9ac9e6031f203c59344dd3347693afcce9699a66d90620223f5c79b2699aa695b2cfec08214dd334cd2542
5f7b98b59a65d334d2ee0b222845699aa669617e9bb8d4d334cba6f10e232b47644dd3344d819ebad7f4119aa66996242d4a6784a02c9ba669bddaf7132530d3344dd34d6
a86a3c0a659364dddf9162633509aa6699a6c89a6c3dffc344db36c192736526f8cd9344dd3a9c5e2ff1c28a6699a663855728fab4db36c9ac8e502291e3b58344dd33475
91aecbe8699a66d9042a213e5b77b2699aa694b1ceea072b4dd334cd24415d7a97b49a65d334d0ed0a2c2743699aa669607d9ab6d3d334cba6f00d2d2946634dd3344d809
```

0 client pkts, 1 server pkt, 0 turns.

188.72.243.72:80 → 192.168.3.65:1035 (593 kB) Show as Raw No delta times Stream 3

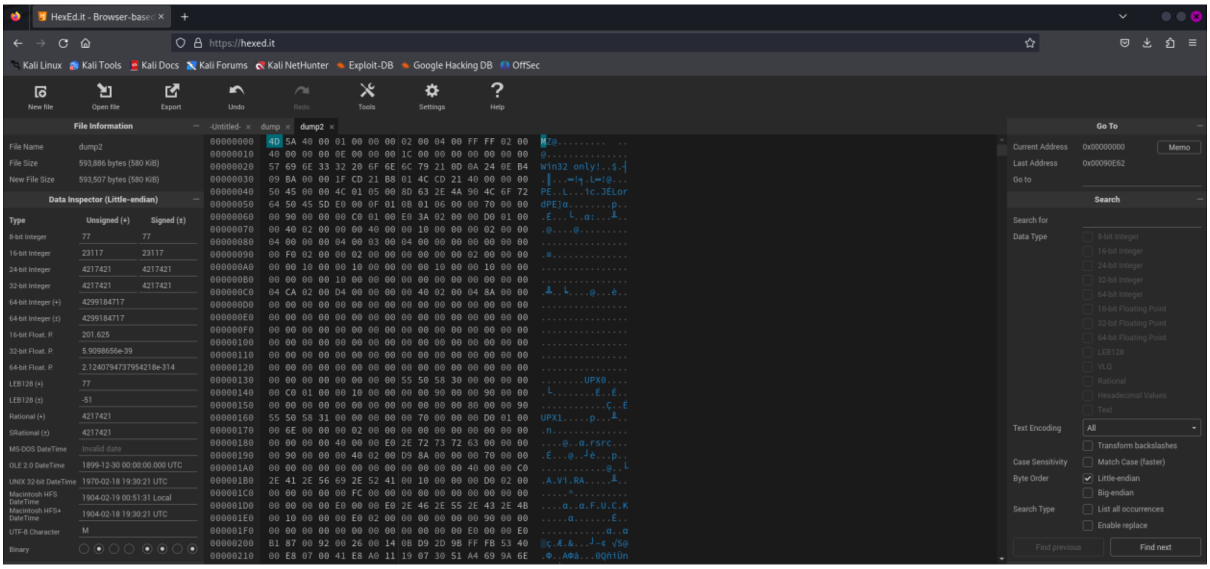
Find: □ Case sensitive Find Next

## - Verify file signature



```
┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ md5sum dump
f2e199d3f2ef983474c2b4c132de7638  dump

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ md5sum dump2
3dbef8b067644d0608be85163e01a5f3  dump2

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ sha256sum dump2
83ace50a90b6bd0c27b38a6c0efd8d2b69a17a2c4717681b6e1a3fe4e28305e5  dump2

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$ sha256sum dump
f619ff4840b4d491ca0e3fcadb17d10e854e5bce65f1459ff3503a6794b76a1d  dump

┌──(cyberbot㉿kali)-[~/Advanced-Wireshark-Network-Forensics]
└─$
```

## - Extract executable file



File Information

| | |
|---|---|
| File Name | dump2 |
| File Size | 593,886 bytes (580 KiB) |
| New File Size | 593,507 bytes (580 KiB) |

Data Inspector (Little-endian)

| Type | Unsigned (+) | Signed (±) |
|---|---|---|
| 8-bit Integer | 77 | 77 |
| 16-bit Integer | 23117 | 23117 |
| 24-bit Integer | 4217421 | 4217421 |
| 32-bit Integer | 4217421 | 4217421 |
| 64-bit Integer (+) | 4299184717 | |
| 64-bit Integer (±) | 4299184717 | |
| 16-bit Float. P. | 201.625 | |
| 32-bit Float. P. | 5.9098656e-39 | |
| 64-bit Float. P. | 2.1240794737954218e-314 | |
| LEB128 (+) | 77 | |
| LEB128 (±) | -51 | |
| Rational (+) | 4217421 | |
| SRational (±) | 4217421 | |
| MS-DOS DateTime | Invalid date | |
| OLE 2.0 DateTime | 1899-12-30 00:00:00.000 UTC | |
| UNIX 32-bit DateTime | 1970-02-18 19:30:21 UTC | |
| Macintosh HFS DateTime | 1904-02-19 00:51:31 Local | |
| Macintosh HFS+ DateTime | 1904-02-18 19:30:21 UTC | |
| UTF-8 Character | M | |
| Binary | ○ ● ○ ○ ● ● ○ ● | |

```
00000000  4D 5A 40 00 01 00 00 00  02 00 04 00 FF FF 02 00  MZ@.........  ..
00000010  40 00 00 00 0E 00 00 00  1C 00 00 00 00 00 00 00  @...............
00000020  57 69 6E 33 32 20 6F 6E  6C 79 21 0D 0A 24 0E B4  Win32 only!..$.┤
00000030  09 BA 00 00 1F CD 21 B8  01 4C CD 21 40 00 00 00  .║...═!╕.L═!@...
00000040  50 45 00 00 4C 01 05 00  8D 63 2E 4A 90 4C 6F 72  PE..L...ìc.JÉLor
00000050  64 50 45 5D E0 00 0F 01  0B 01 06 00 00 70 00 00  dPE]α........p..
00000060  00 90 00 00 00 C0 01 00  E0 3A 02 00 00 D0 01 00  .É...└..α:...╨..
00000070  00 40 02 00 00 00 40 00  00 10 00 00 00 02 00 00  .@....@.........
00000080  04 00 00 00 04 00 03 00  04 00 00 00 00 00 00 00  ................
00000090  00 F0 02 00 00 02 00 00  00 00 00 00 02 00 00 00  .≡..............
000000A0  00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  ................
000000B0  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0  04 CA 02 00 D4 00 00 00  00 40 02 00 04 8A 00 00  .╩..╘....@...è..
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00  55 50 58 30 00 00 00 00  ........UPX0....
00000140  00 C0 01 00 00 10 00 00  00 00 90 00 00 90 00 00  .└........É..É..
00000150  00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 90  ............Ç..É
00000160  55 50 58 31 00 00 00 00  00 70 00 00 00 D0 01 00  UPX1.....p...╨..
00000170  00 6E 00 00 00 02 00 00  00 00 00 00 00 00 00 00  .n..............
00000180  00 00 00 00 40 00 00 E0  2E 72 73 72 63 00 00 00  ....@..α.rsrc...
00000190  00 90 00 00 00 40 02 00  D9 8A 00 00 00 70 00 00  .É...@..┘è...p..
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 C0  ............@..└
000001B0  2E 41 2E 56 69 2E 52 41  00 10 00 00 00 D0 02 00  .A.Vi.RA.....╨..
000001C0  00 00 00 00 00 FC 00 00  00 00 00 00 00 00 00 00  .....ⁿ..........
000001D0  00 00 00 00 E0 00 00 E0  2E 46 2E 55 2E 43 2E 4B  ....α..α.F.U.C.K
000001E0  00 10 00 00 00 E0 02 00  00 00 00 00 00 90 00 00  .....α.......É..
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 E0 00 00 E0  ............α..α
00000200  B1 87 00 92 00 26 00 14  0B D9 2D 9B FF FB 53 40  ▒ç.Æ.&...┘-¢ √S@
00000210  00 E8 07 00 41 E8 A0 11  19 07 30 51 A4 69 9A 6E  .Φ..AΦá...0QñiÜn
```

Go To

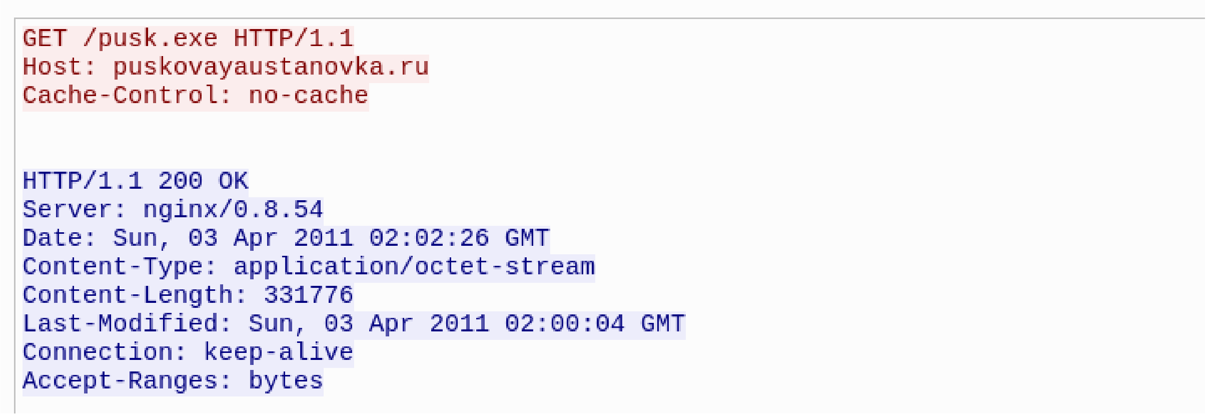
| | |
|---|---|
| Current Address | 0x00000000 |
| Last Address | 0x00090E62 |
| Go to | |

Search

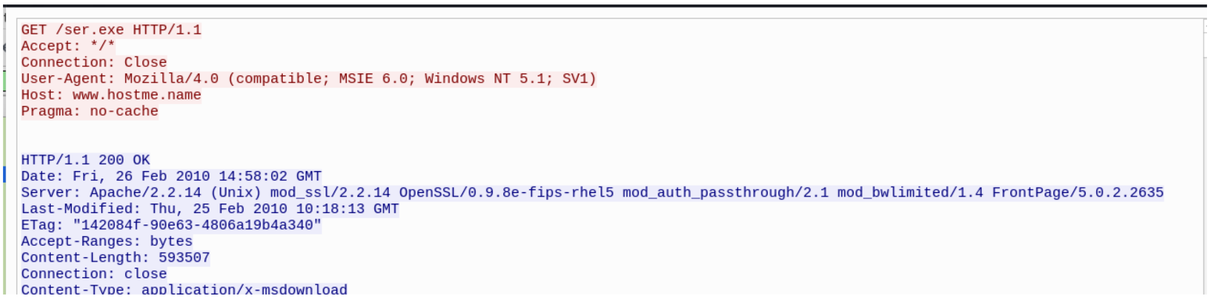
| | |
|---|---|
| Search for | |
| Data Type | □ 8-bit Integer<br>□ 16-bit Integer<br>□ 24-bit Integer<br>□ 32-bit Integer<br>□ 64-bit Integer<br>□ 16-bit Floating Point<br>□ 32-bit Floating Point<br>□ 64-bit Floating Point<br>□ LEB128<br>□ VLQ<br>□ Rational<br>□ Hexadecimal Values<br>□ Text |
| Text Encoding | All<br>□ Transform backslashes |
| Case Sensitivity | □ Match Case (faster) |
| Byte Order | ☑ Little-endian<br>□ Big-endian |
| Search Type | □ List all occurrences<br>□ Enable replace |

FOUND THE EXE MALWARE FILE

## 3) What kind of calls to the internet does it take?



```
GET /pusk.exe HTTP/1.1
Host: puskovayaustanovka.ru
Cache-Control: no-cache


HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Sun, 03 Apr 2011 02:02:26 GMT
Content-Type: application/octet-stream
Content-Length: 331776
Last-Modified: Sun, 03 Apr 2011 02:00:04 GMT
Connection: keep-alive
Accept-Ranges: bytes
```

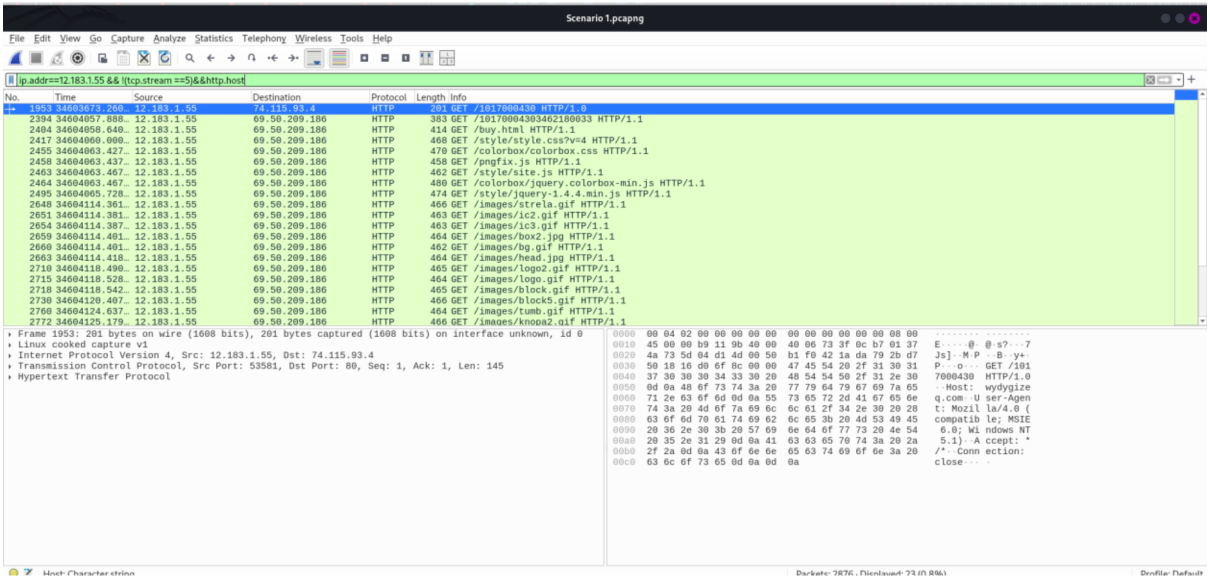


```
GET /ser.exe HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.hostme.name
Pragma: no-cache


HTTP/1.1 200 OK
Date: Fri, 26 Feb 2010 14:58:02 GMT
Server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Last-Modified: Thu, 25 Feb 2010 10:18:13 GMT
ETag: "142084f-90e63-4806a19b4a340"
Accept-Ranges: bytes
Content-Length: 593507
Connection: close
Content-Type: application/x-msdownload
```

## 4) Does it try to self propagate through the internal network ?

## Answer : No

## 5) Possible Traffic signatures



Scenario 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

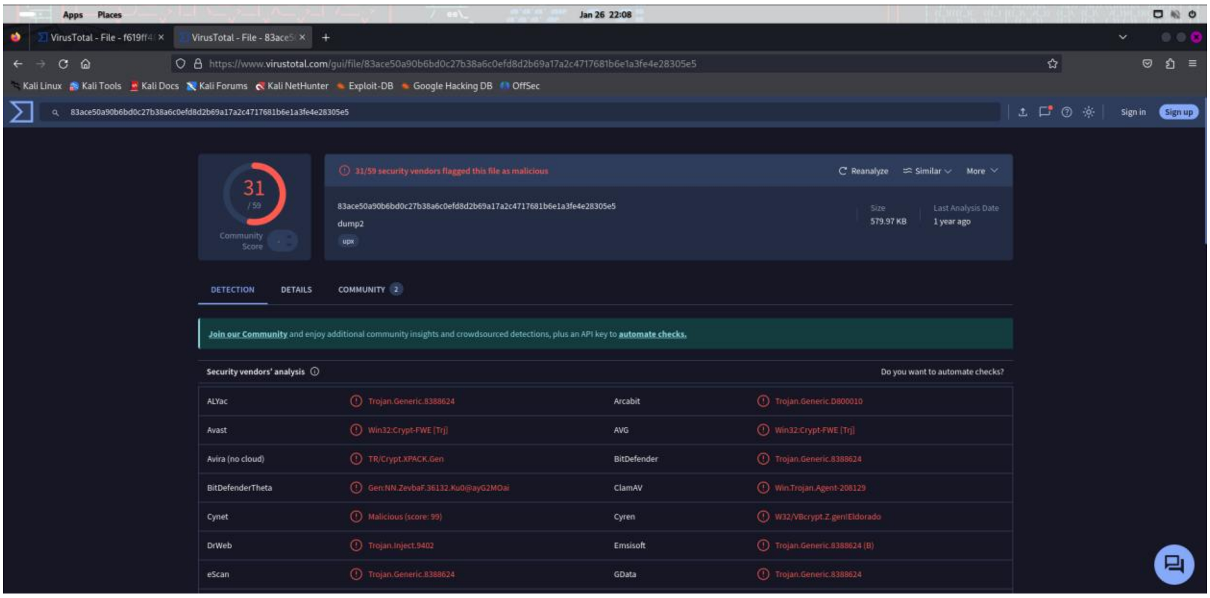
ip.addr==12.183.1.55 && !(tcp.stream ==5)&&http.host

```
No.   Time             Source       Destination    Protocol Length Info
 1953 34603673.260…  12.183.1.55  74.115.93.4    HTTP     201 GET /1017000430 HTTP/1.0
 2394 34604057.888…  12.183.1.55  69.50.209.186  HTTP     383 GET /10170004303462180033 HTTP/1.1
 2404 34604058.640…  12.183.1.55  69.50.209.186  HTTP     414 GET /buy.html HTTP/1.1
 2417 34604060.000…  12.183.1.55  69.50.209.186  HTTP     468 GET /style/style.css?v=4 HTTP/1.1
 2455 34604063.427…  12.183.1.55  69.50.209.186  HTTP     470 GET /colorbox/colorbox.css HTTP/1.1
 2458 34604063.437…  12.183.1.55  69.50.209.186  HTTP     458 GET /pngfix.js HTTP/1.1
 2463 34604063.467…  12.183.1.55  69.50.209.186  HTTP     462 GET /style/site.js HTTP/1.1
 2464 34604063.467…  12.183.1.55  69.50.209.186  HTTP     480 GET /colorbox/jquery.colorbox-min.js HTTP/1.1
 2495 34604065.728…  12.183.1.55  69.50.209.186  HTTP     474 GET /style/jquery-1.4.4.min.js HTTP/1.1
 2648 34604114.361…  12.183.1.55  69.50.209.186  HTTP     466 GET /images/strela.gif HTTP/1.1
 2651 34604114.381…  12.183.1.55  69.50.209.186  HTTP     463 GET /images/ic2.gif HTTP/1.1
 2654 34604114.387…  12.183.1.55  69.50.209.186  HTTP     463 GET /images/ic3.gif HTTP/1.1
 2659 34604114.401…  12.183.1.55  69.50.209.186  HTTP     464 GET /images/box2.jpg HTTP/1.1
 2660 34604114.401…  12.183.1.55  69.50.209.186  HTTP     462 GET /images/bg.gif HTTP/1.1
 2663 34604114.418…  12.183.1.55  69.50.209.186  HTTP     464 GET /images/head.jpg HTTP/1.1
 2710 34604118.490…  12.183.1.55  69.50.209.186  HTTP     465 GET /images/logo2.gif HTTP/1.1
 2715 34604118.528…  12.183.1.55  69.50.209.186  HTTP     464 GET /images/logo.gif HTTP/1.1
 2718 34604118.542…  12.183.1.55  69.50.209.186  HTTP     465 GET /images/block.gif HTTP/1.1
 2730 34604120.407…  12.183.1.55  69.50.209.186  HTTP     466 GET /images/block5.gif HTTP/1.1
 2760 34604124.637…  12.183.1.55  69.50.209.186  HTTP     464 GET /images/tumb.gif HTTP/1.1
 2772 34604125.179…  12.183.1.55  69.50.209.186  HTTP     466 GET /images/knopa2.gif HTTP/1.1
```

```
› Frame 1953: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface unknown, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 12.183.1.55, Dst: 74.115.93.4
› Transmission Control Protocol, Src Port: 53581, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
› Hypertext Transfer Protocol
```

```
0000  00 04 02 00 00 00 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 b9 11 9b 40 00  40 06 73 3f 0c b7 01 37   E·····@· @·s?···7
0020  4a 73 5d 04 d1 4d 00 50  b1 f0 42 1a da 79 2b d7   Js]··M·P ··B··y+·
0030  50 18 16 d0 6f 8c 00 00  47 45 54 20 2f 31 30 31   P···o··· GET /101
0040  37 30 30 30 34 33 30 20  48 54 54 50 2f 31 2e 30   7000430  HTTP/1.0
0050  0d 0a 48 6f 73 74 3a 20  77 79 64 79 67 69 7a 65   ··Host:  wydygize
0060  71 2e 63 6f 6d 0d 0a 55  73 65 72 2d 41 67 65 6e   q.com··U ser-Agen
0070  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 34 2e 30 20 28   t: Mozil la/4.0 (
0080  63 6f 6d 70 61 74 69 62  6c 65 3b 20 4d 53 49 45   compatib le; MSIE
0090  20 36 2e 30 3b 20 57 69  6e 64 6f 77 73 20 4e 54    6.0; Wi ndows NT
00a0  20 35 2e 31 29 0d 0a 41  63 63 65 70 74 3a 20 2a    5.1)··A ccept: *
00b0  2f 2a 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   /*··Conn ection: 
00c0  63 6c 6f 73 65 0d 0a 0d  0a                        close··· ·
```

# VIRUS TOTAL REPORT ABOUT MALWARE



https://www.virustotal.com/gui/file/83ace50a90b6bd0c27b38a6c0efd8d2b69a17a2c4717681b6e1a3fe4e28305e5

83ace50a90b6bd0c27b38a6c0efd8d2b69a17a2c4717681b6e1a3fe4e28305e5

31 / 59 Community Score

31/59 security vendors flagged this file as malicious

83ace50a90b6bd0c27b38a6c0efd8d2b69a17a2c4717681b6e1a3fe4e28305e5

dump2

upx

Size 579.97 KB

Last Analysis Date 1 year ago

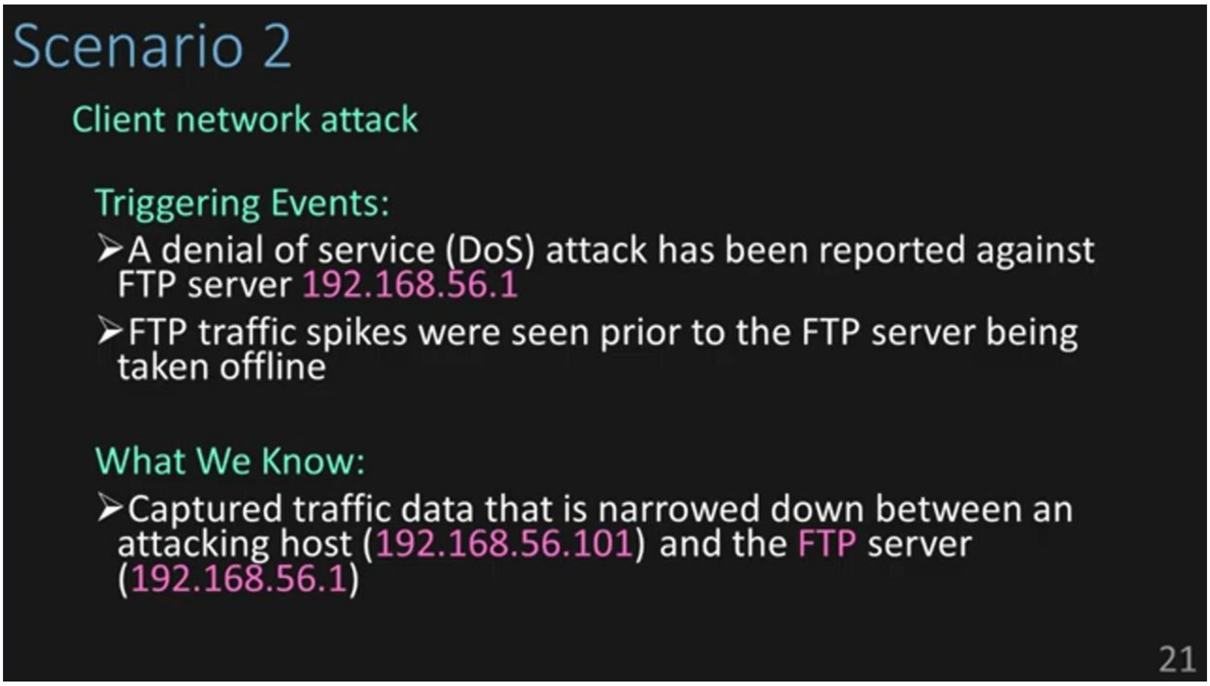
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| ALYac | Trojan.Generic.8388624 | Arcabit | Trojan.Generic.D800010 |
| Avast | Win32:Crypt-FWE [Trj] | AVG | Win32:Crypt-FWE [Trj] |
| Avira (no cloud) | TR/Crypt.XPACK.Gen | BitDefender | Trojan.Generic.8388624 |
| BitDefenderTheta | Gen:NN.ZevbaF.36132.Ku0@ayG2MOai | ClamAV | Win.Trojan.Agent-208129 |
| Cynet | Malicious (score: 99) | Cyren | W32/VBcrypt.Z.gen!Eldorado |
| DrWeb | Trojan.Inject.9402 | Emsisoft | Trojan.Generic.8388624 (B) |
| eScan | Trojan.Generic.8388624 | GData | Trojan.Generic.8388624 |

## Scenario 2: FTP Server Attack Investigation



Scenario 2

Client network attack

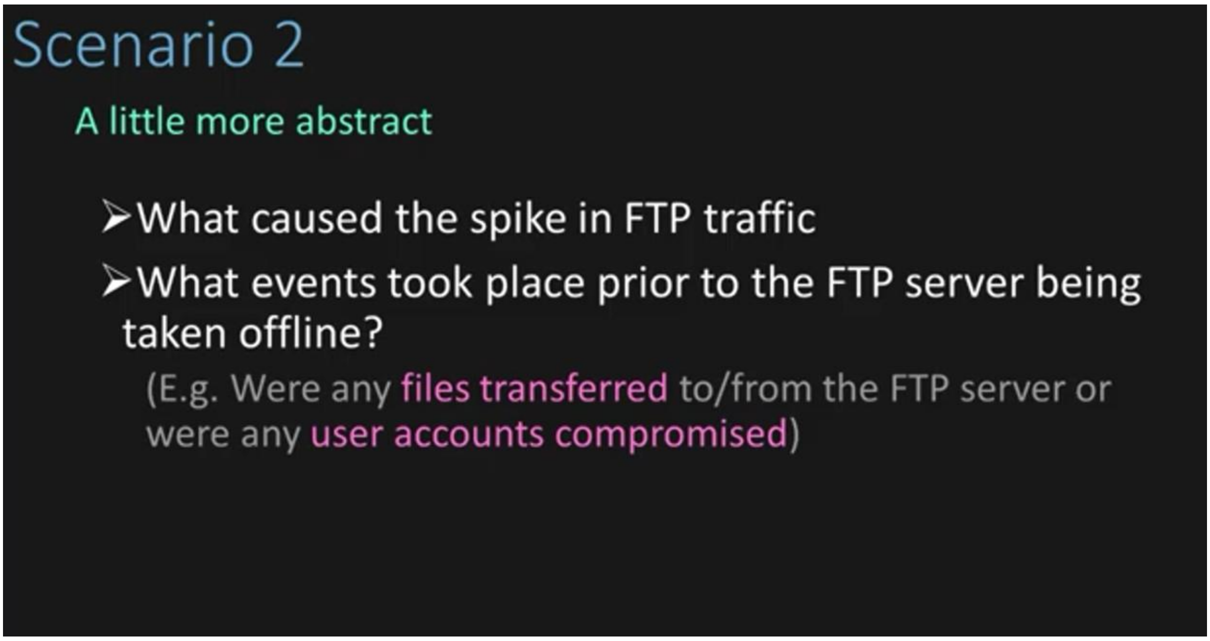
Triggering Events:

- A denial of service (DoS) attack has been reported against FTP server 192.168.56.1
- FTP traffic spikes were seen prior to the FTP server being taken offline

What We Know:

- Captured traffic data that is narrowed down between an attacking host (192.168.56.101) and the FTP server (192.168.56.1)

21



Scenario 2

A little more abstract

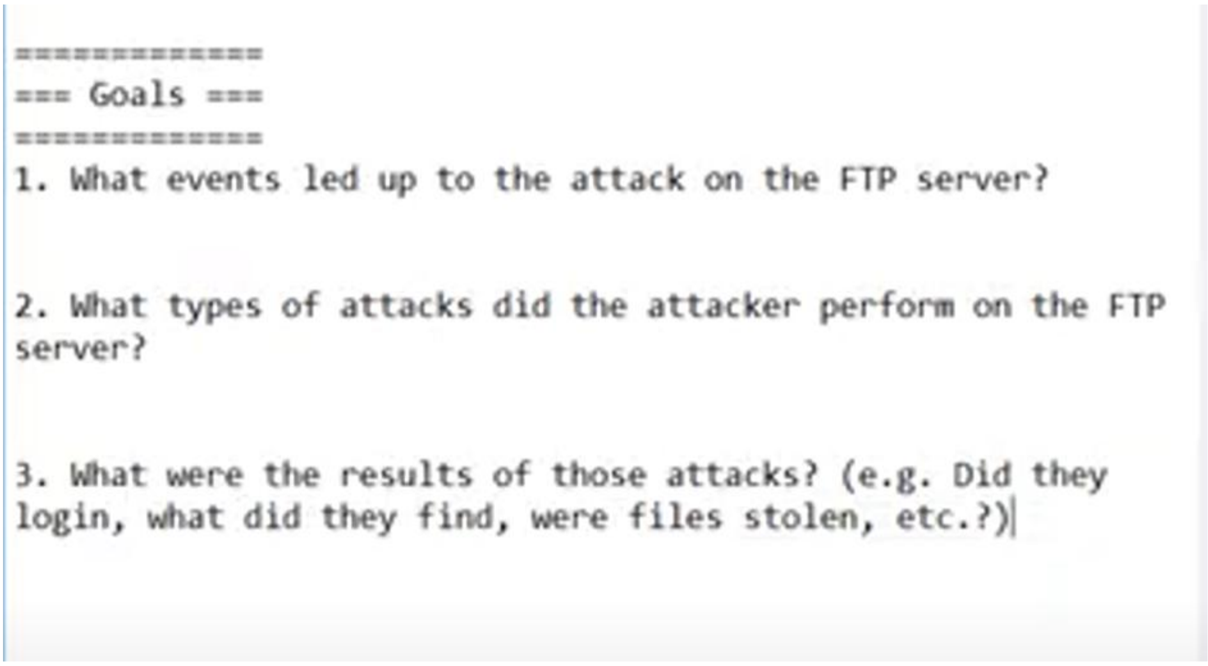
- What caused the spike in FTP traffic
- What events took place prior to the FTP server being taken offline?

  (E.g. Were any files transferred to/from the FTP server or were any user accounts compromised)

Objective

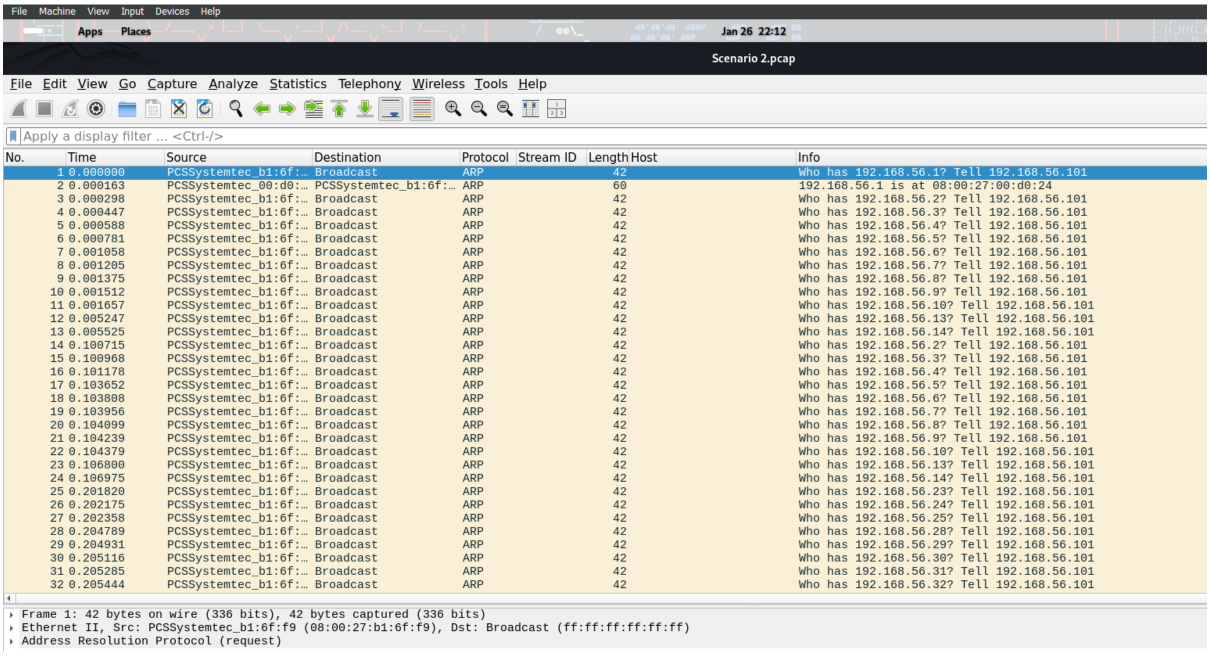
Investigate a potential Denial of Service (DoS) attack targeting an FTP server.

GOALS



```
=============
=== Goals ===
=============
1. What events led up to the attack on the FTP server?


2. What types of attacks did the attacker perform on the FTP
server?


3. What were the results of those attacks? (e.g. Did they
login, what did they find, were files stolen, etc.?)
```

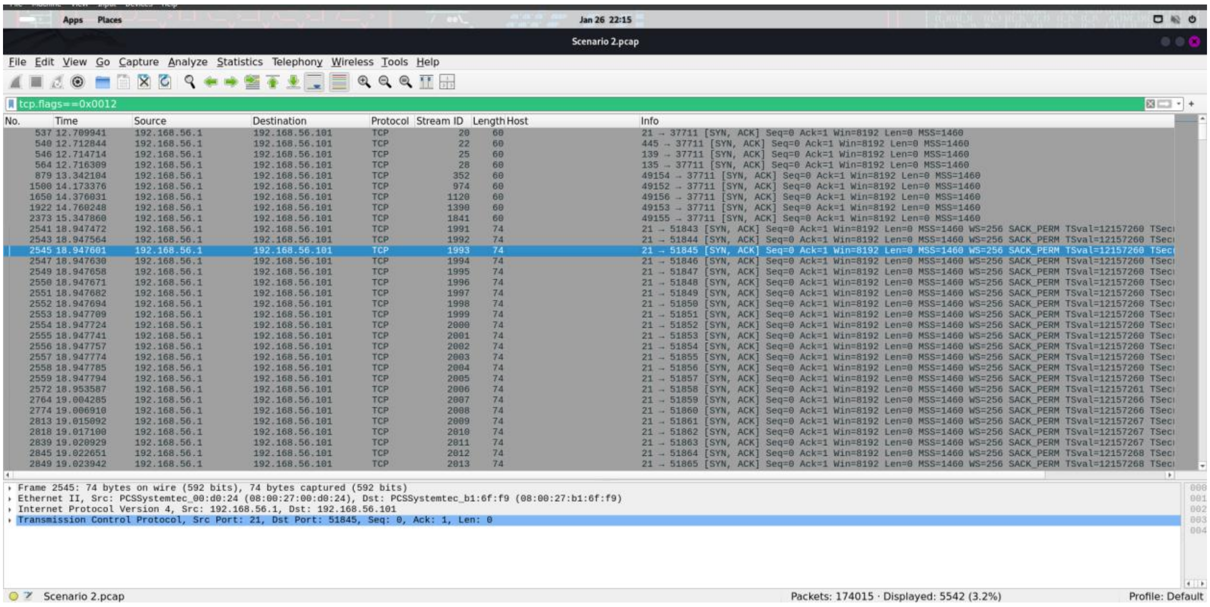
# 1. What events led to the attack on the FTP server?



File Machine View Input Devices Help
Apps Places
Jan 26 22:12
Scenario 2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source                Destination           Protocol Stream ID Length Host  Info
   1 0.000000   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.1? Tell 192.168.56.101
   2 0.000163   PCSSystemtec_00:d0:… PCSSystemtec_b1:6f:… ARP                60           192.168.56.1 is at 08:00:27:00:d0:24
   3 0.000298   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.2? Tell 192.168.56.101
   4 0.000447   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.3? Tell 192.168.56.101
   5 0.000588   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.4? Tell 192.168.56.101
   6 0.000781   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.5? Tell 192.168.56.101
   7 0.001058   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.6? Tell 192.168.56.101
   8 0.001205   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.7? Tell 192.168.56.101
   9 0.001375   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.8? Tell 192.168.56.101
  10 0.001512   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.9? Tell 192.168.56.101
  11 0.001657   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.10? Tell 192.168.56.101
  12 0.005247   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.13? Tell 192.168.56.101
  13 0.005525   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.14? Tell 192.168.56.101
  14 0.100715   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.2? Tell 192.168.56.101
  15 0.100968   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.3? Tell 192.168.56.101
  16 0.101178   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.4? Tell 192.168.56.101
  17 0.103652   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.5? Tell 192.168.56.101
  18 0.103808   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.6? Tell 192.168.56.101
  19 0.103956   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.7? Tell 192.168.56.101
  20 0.104099   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.8? Tell 192.168.56.101
  21 0.104239   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.9? Tell 192.168.56.101
  22 0.104379   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.10? Tell 192.168.56.101
  23 0.106800   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.13? Tell 192.168.56.101
  24 0.106975   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.14? Tell 192.168.56.101
  25 0.201820   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.23? Tell 192.168.56.101
  26 0.202175   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.24? Tell 192.168.56.101
  27 0.202358   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.25? Tell 192.168.56.101
  28 0.204789   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.28? Tell 192.168.56.101
  29 0.204931   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.29? Tell 192.168.56.101
  30 0.205116   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.30? Tell 192.168.56.101
  31 0.205285   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.31? Tell 192.168.56.101
  32 0.205444   PCSSystemtec_b1:6f:… Broadcast             ARP                42           Who has 192.168.56.32? Tell 192.168.56.101
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
› Ethernet II, Src: PCSSystemtec_b1:6f:f9 (08:00:27:b1:6f:f9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```



Apps Places
Jan 26 22:15
Scenario 2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

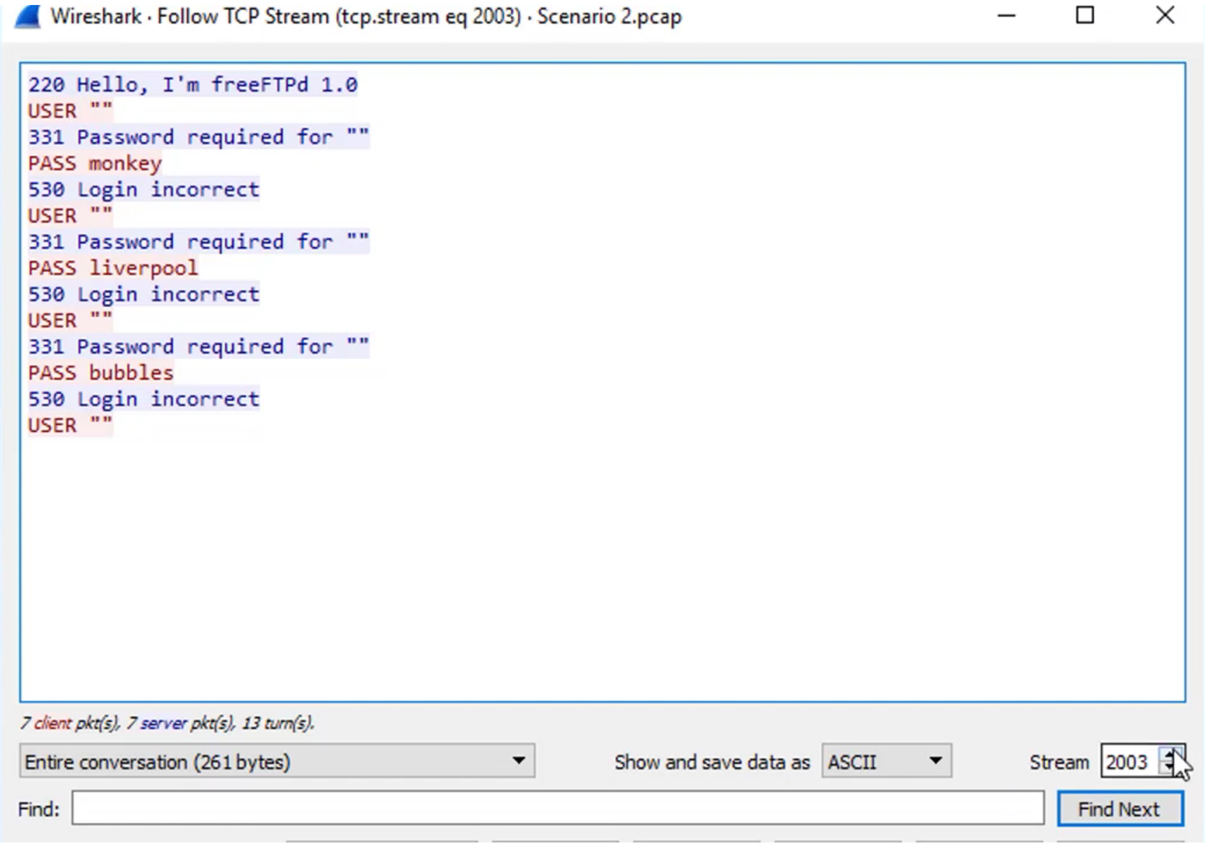
```
tcp.flags==0x0012
```

```
No.  Time       Source          Destination       Protocol Stream ID Length Host  Info
 537 12.709941  192.168.56.1    192.168.56.101    TCP          20     60          21 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 540 12.712844  192.168.56.1    192.168.56.101    TCP          22     60          445 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 546 12.714714  192.168.56.1    192.168.56.101    TCP          25     60          139 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 564 12.716309  192.168.56.1    192.168.56.101    TCP          28     60          135 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 879 13.342104  192.168.56.1    192.168.56.101    TCP         352     60          49154 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1500 14.173376  192.168.56.1    192.168.56.101    TCP         974     60          49152 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1650 14.376031  192.168.56.1    192.168.56.101    TCP        1120     60          49156 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1922 14.760248  192.168.56.1    192.168.56.101    TCP        1390     60          49153 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
2373 15.347860  192.168.56.1    192.168.56.101    TCP        1841     60          49155 → 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
2541 18.947472  192.168.56.1    192.168.56.101    TCP        1991     74          21 → 51843 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2543 18.947564  192.168.56.1    192.168.56.101    TCP        1992     74          21 → 51844 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2545 18.947601  192.168.56.1    192.168.56.101    TCP        1993     74          21 → 51845 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2547 18.947630  192.168.56.1    192.168.56.101    TCP        1994     74          21 → 51846 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2549 18.947658  192.168.56.1    192.168.56.101    TCP        1995     74          21 → 51847 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2550 18.947671  192.168.56.1    192.168.56.101    TCP        1996     74          21 → 51848 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2551 18.947682  192.168.56.1    192.168.56.101    TCP        1997     74          21 → 51849 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2552 18.947694  192.168.56.1    192.168.56.101    TCP        1998     74          21 → 51850 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2553 18.947709  192.168.56.1    192.168.56.101    TCP        1999     74          21 → 51851 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2554 18.947724  192.168.56.1    192.168.56.101    TCP        2000     74          21 → 51852 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2555 18.947741  192.168.56.1    192.168.56.101    TCP        2001     74          21 → 51853 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2556 18.947757  192.168.56.1    192.168.56.101    TCP        2002     74          21 → 51854 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2557 18.947774  192.168.56.1    192.168.56.101    TCP        2003     74          21 → 51855 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2558 18.947785  192.168.56.1    192.168.56.101    TCP        2004     74          21 → 51856 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2559 18.947794  192.168.56.1    192.168.56.101    TCP        2005     74          21 → 51857 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSec
2572 18.953587  192.168.56.1    192.168.56.101    TCP        2006     74          21 → 51858 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157261 TSec
2764 19.004285  192.168.56.1    192.168.56.101    TCP        2007     74          21 → 51859 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157266 TSec
2774 19.006910  192.168.56.1    192.168.56.101    TCP        2008     74          21 → 51860 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157266 TSec
2813 19.015092  192.168.56.1    192.168.56.101    TCP        2009     74          21 → 51861 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157267 TSec
2818 19.017100  192.168.56.1    192.168.56.101    TCP        2010     74          21 → 51862 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157267 TSec
2839 19.020929  192.168.56.1    192.168.56.101    TCP        2011     74          21 → 51863 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157267 TSec
2845 19.022651  192.168.56.1    192.168.56.101    TCP        2012     74          21 → 51864 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157268 TSec
2849 19.023942  192.168.56.1    192.168.56.101    TCP        2013     74          21 → 51865 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157268 TSec
```

```
› Frame 2545: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
› Ethernet II, Src: PCSSystemtec_00:d0:24 (08:00:27:00:d0:24), Dst: PCSSystemtec_b1:6f:f9 (08:00:27:b1:6f:f9)
› Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
› Transmission Control Protocol, Src Port: 21, Dst Port: 51845, Seq: 0, Ack: 1, Len: 0
```

```
Scenario 2.pcap                    Packets: 174015 · Displayed: 5542 (3.2%)                    Profile: Default
```

## 2. What types of attacks did the attacker perform the FTP server?

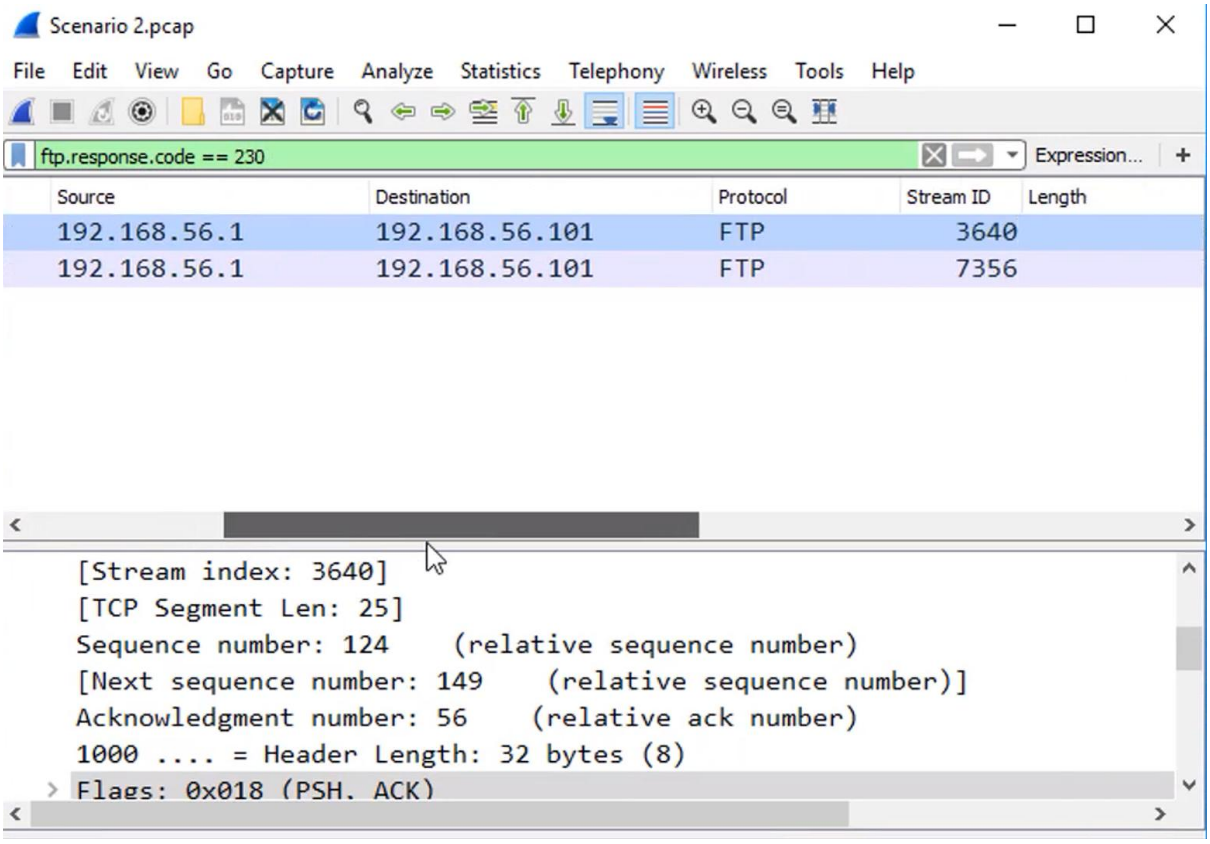


Wireshark · Follow TCP Stream (tcp.stream eq 2003) · Scenario 2.pcap

```
220 Hello, I'm freeFTPd 1.0
USER ""
331 Password required for ""
PASS monkey
530 Login incorrect
USER ""
331 Password required for ""
PASS liverpool
530 Login incorrect
USER ""
331 Password required for ""
PASS bubbles
530 Login incorrect
USER ""
```

7 client pkt(s), 7 server pkt(s), 13 turn(s).

Entire conversation (261 bytes) · Show and save data as: ASCII · Stream: 2003

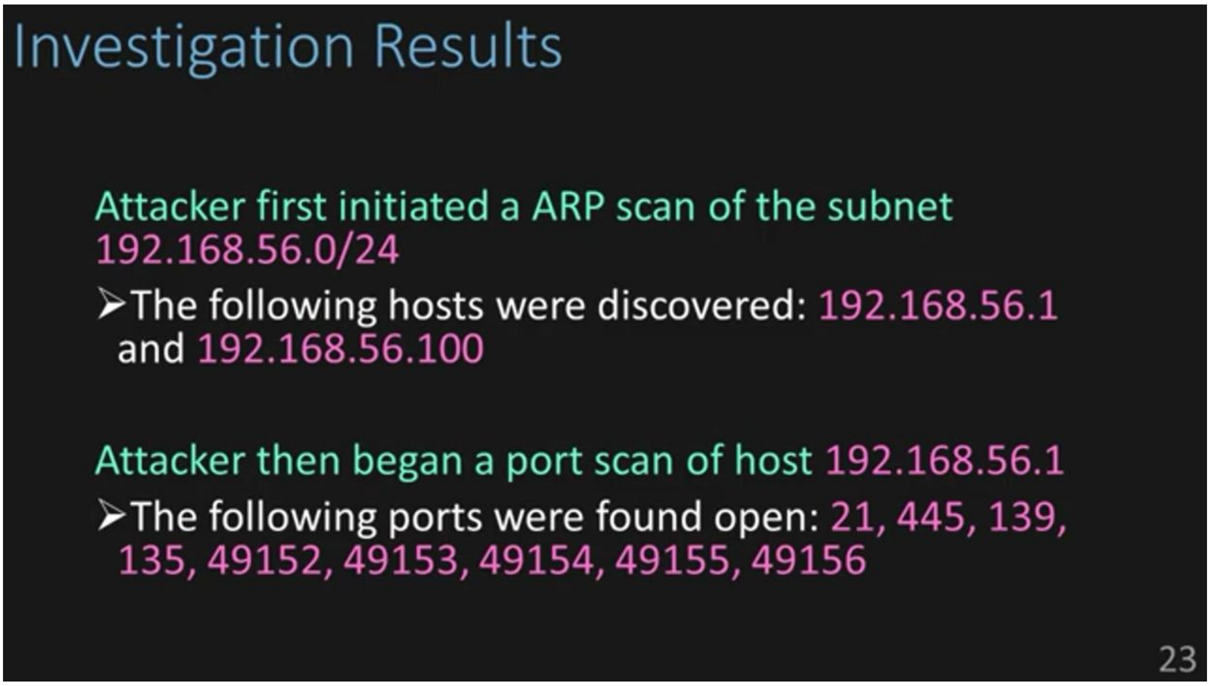


Scenario 2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

Filter: ftp.response.code == 230

```
Source            Destination        Protocol   Stream ID   Length
192.168.56.1      192.168.56.101     FTP             3640
192.168.56.1      192.168.56.101     FTP             7356
```

```
[Stream index: 3640]
[TCP Segment Len: 25]
Sequence number: 124    (relative sequence number)
[Next sequence number: 149    (relative sequence number)]
Acknowledgment number: 56    (relative ack number)
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
```



## Investigation Results

Attacker first initiated a ARP scan of the subnet 192.168.56.0/24

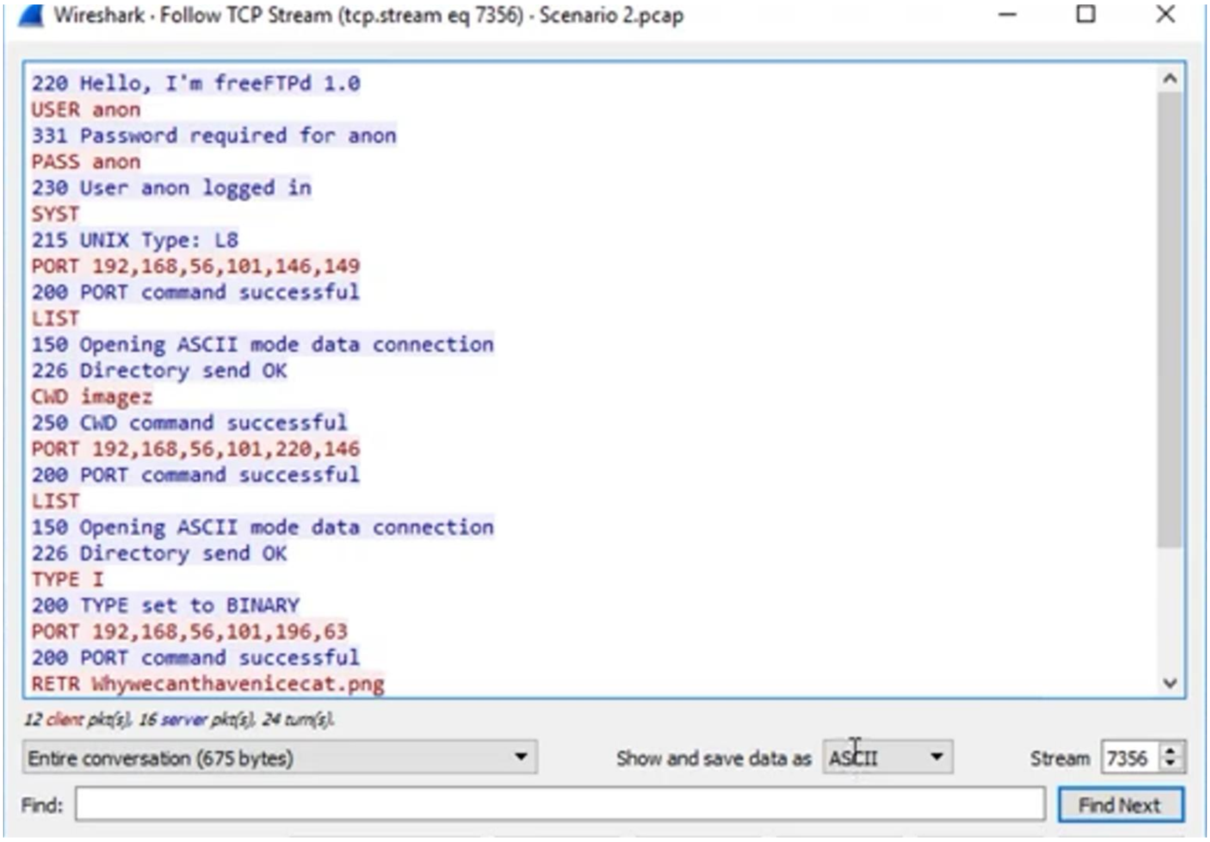
- The following hosts were discovered: 192.168.56.1 and 192.168.56.100

Attacker then began a port scan of host 192.168.56.1

- The following ports were found open: 21, 445, 139, 135, 49152, 49153, 49154, 49155, 49156

3. were the results of those attacks? (e.g. Did they

login, did they find, files stolen, etc.



Wireshark · Follow TCP Stream (tcp.stream eq 7356) · Scenario 2.pcap

```
220 Hello, I'm freeFTPd 1.0
USER anon
331 Password required for anon
PASS anon
230 User anon logged in
SYST
215 UNIX Type: L8
PORT 192,168,56,101,146,149
200 PORT command successful
LIST
150 Opening ASCII mode data connection
226 Directory send OK
CWD imagez
250 CWD command successful
PORT 192,168,56,101,220,146
200 PORT command successful
LIST
150 Opening ASCII mode data connection
226 Directory send OK
TYPE I
200 TYPE set to BINARY
PORT 192,168,56,101,196,63
200 PORT command successful
RETR Whywecanthavenicecat.png
```

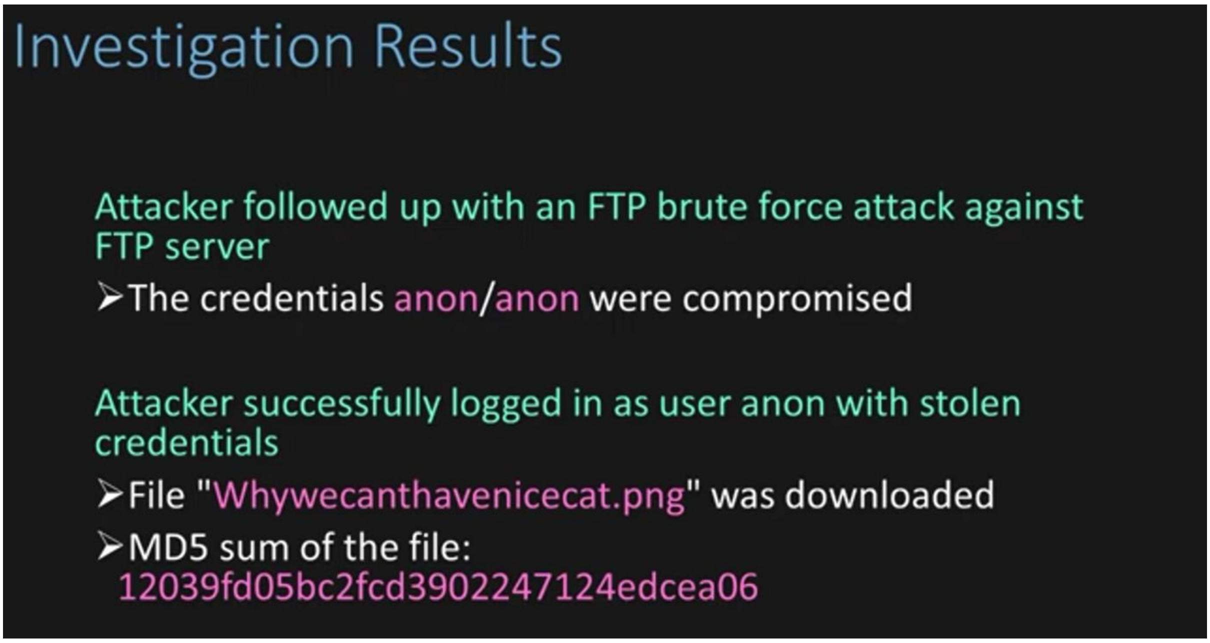
12 client pkt(s), 16 server pkt(s), 24 turn(s).

Entire conversation (675 bytes)

Show and save data as ASCII

Stream 7356

Find:



# Investigation Results

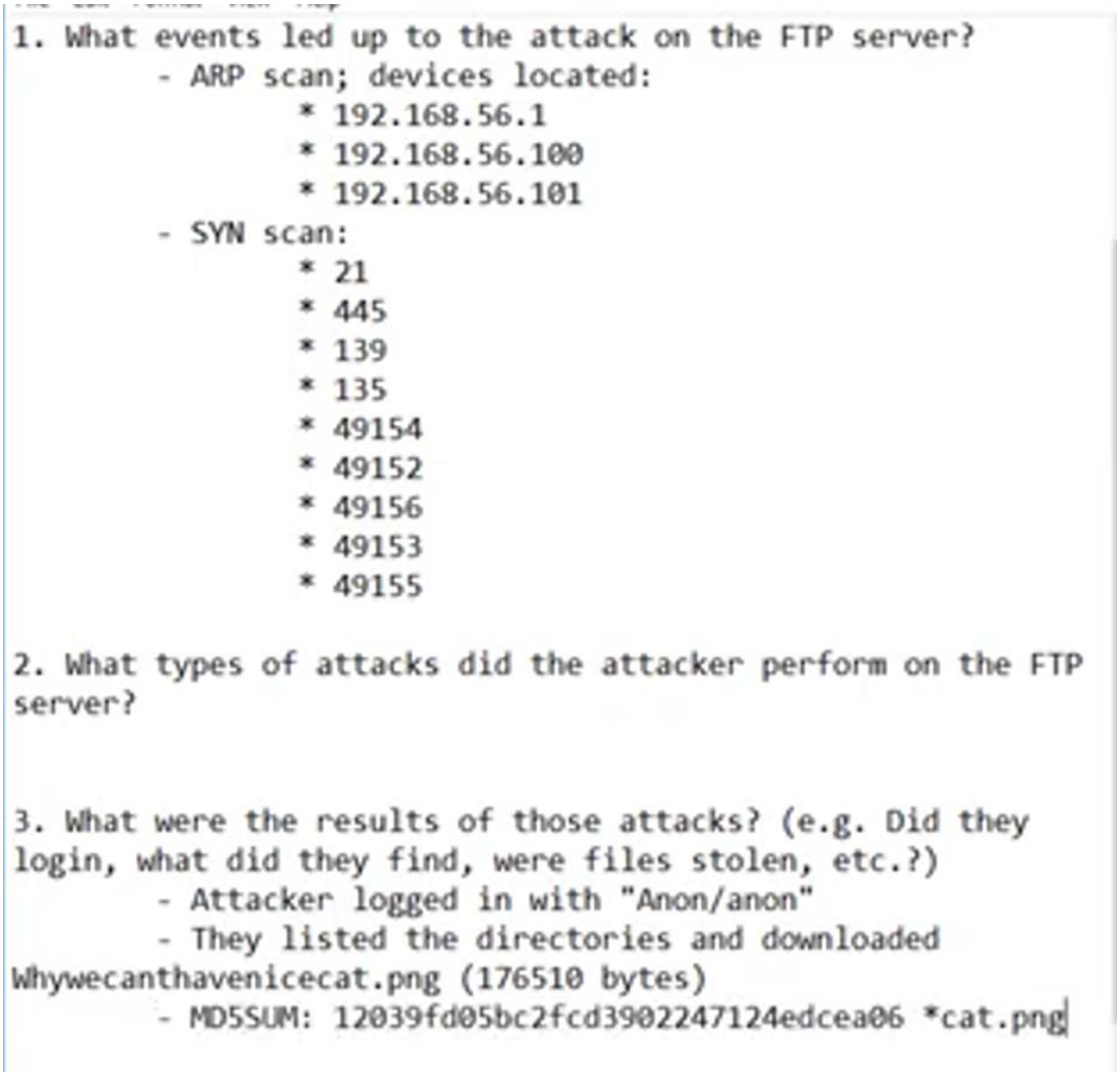
Attacker followed up with an FTP brute force attack against FTP server

- The credentials anon/anon were compromised

Attacker successfully logged in as user anon with stolen credentials

- File "Whywecanthavenicecat.png" was downloaded
- MD5 sum of the file: 12039fd05bc2fcd3902247124edcea06

CAT.PNG FOUND



```
1. What events led up to the attack on the FTP server?
        - ARP scan; devices located:
                * 192.168.56.1
                * 192.168.56.100
                * 192.168.56.101
        - SYN scan:
                * 21
                * 445
                * 139
                * 135
                * 49154
                * 49152
                * 49156
                * 49153
                * 49155

2. What types of attacks did the attacker perform on the FTP
server?


3. What were the results of those attacks? (e.g. Did they
login, what did they find, were files stolen, etc.?)
        - Attacker logged in with "Anon/anon"
        - They listed the directories and downloaded
Whywecanthavenicecat.png (176510 bytes)
        - MD5SUM: 12039fd05bc2fcd3902247124edcea06 *cat.png
```

## Conclusion

Network forensics requires systematic, methodical investigation combining technical skills, analytical thinking, and comprehensive documentation.