

# Intro to Cyber Forensics Lab Grading Sheet

Project: **Lab 6 - Network PCAP Forensics Scenarios**

---

Member Name: **VINUSHA GOUD POTTOLLA**

Member Name: **OLUWATOYOSI KEHINDE**

Member Name: **BOINAPELLY AKSHITH ROA**

Member Name: **AMANI PONMAN**

Member Name: **YADLAPALLI IAKSHMIDAR**

---

## Executive Summary \_\_\_\_\_ / 4 points

+ √ -

- ☐ ☐ ☐ Executive summary is brief and focused to the point of the project
- ☐ ☐ ☐ The summary clearly illustrates the objectives of the laboratory exercise

## Apparatus \_\_\_\_\_ / 4 points

- ☐ ☐ ☐ The apparatus are clearly illustrated and documented

## Procedures \_\_\_\_\_ / 12 points

- ☐ ☐ ☐ Adequate information provided to allow re-creation of work
- ☐ ☐ ☐ Consistent level of coverage throughout the project – nothing overly detailed or omitted

## Problem Solving \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ All problems identified
- ☐ ☐ ☐ Alternative solutions identified
- ☐ ☐ ☐ Solutions attempted listed
- ☐ ☐ ☐ Final solution detailed (what fixed the problem and why?)

## Conclusions & Recommendations \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ Tie back to the learning objectives identified in the executive summary - critical
- ☐ ☐ ☐ Conclusions stated in a logical fashion
- ☐ ☐ ☐ Conclusions are viable based on the procedures and results
- ☐ ☐ ☐ Recommendations practical & relevant

## Format & Grammar \_\_\_\_\_ / 5 points

- ☐ ☐ ☐ Table of Contents present
- ☐ ☐ ☐ Report written in past tense
- ☐ ☐ ☐ Proper voice (no I's, We's, Our's or The group)
- ☐ ☐ ☐ Paper easy to read (fonts, spacing, etc.)
- ☐ ☐ ☐ Proper credit given to sources in bibliography (APA style)
- ☐ ☐ ☐ Paper is cohesive and consistent in tone

\_\_\_\_\_ Spelling & grammar errors: *minus one half point for each, up to a max deduction of 5 points – at that time, paper is returned for correction and re-submission with a one letter grade penalty.*

Final Score \_\_\_\_\_ / 35

## **Contents**

<b>1. Executive Summary .....</b>	<b>3</b>
<b>2. Apparatus .....</b>	<b>4</b>
<b>3. Laboratory Procedures .....</b>	<b>5</b>
<b>3.1. Time-Log .....</b>	<b>6</b>
<b>3.2. Procedure .....</b>	<b>7</b>
<b>4. Problem Solving and Troubleshooting .....</b>	<b>17</b>
<b>5. Conclusion and Recommendations .....</b>	<b>18</b>
<b>6. References .....</b>	<b>19</b>

## **1. Executive Summary**

This lab report provides an overview of the steps taken in the investigative process for lab exercise #6, which is Network PCAP Forensics. Examination of several PCAP files was a step in the inquiry process. It has involved the use of detection techniques such as Wireshark. In addition to details on the resources gathered during an active session, the report focuses on the procedures used to identify URLs and visited sites, together with their login credentials.

With the assistance of lecture notes and videos that were given on Canvas, this laboratory exercise was carried out under the supervision of Professor Matthew Jackson. Introducing the student investigators to the process of analyzing network packets, identifying the system with infected with malware by the given host ID, and also using many protocols for their investigation was the primary goal of this exercise.

## 2. Apparatus

Hardware and software utilized for the lab exercise are listed in Table 1.

ITEM/PART	MODEL NUMBER	VERSION	USAGE
Dell Inspiron	5570	Windows 11	Workstation used for Network Analysis
Macbook Air	7,2	2.27f2	Secondary work station
Wireshark	4.2.0	N/A	Free open-source packet analyser

### 3.Lab Procedure

Sno	DATE	TIME	Action taken/Investigation lead
1	NOV-29	5:10	Started the lab
2	NOV-29	5:30	Accessed the netoworl files and downloaded from githiub throught the provided link
3	NOV-29	6:10	Started working with Scenario-1
4	NOV-29	7:30	Started working with Scenario-2
5	NOV-29	9:00	Results were summarized
6	Dec-3	11:00	Documentation completion

Table-Time log of actions taken during the investigation

## 4.Procedure

### Scenario 1:

A system is infested with malware

Given Host Id-12.183.1.55

Following file inspection, the following information was gathered.

- 192.168.3.65, the host's IP address
- 188.72.243.72 is the suspect IP address.
- 12.183.1.55 is the victim's IP address.

Based on the investigation, it's possible that the system has a dormant malware infection or that the user made a direct call to the executable, indicating their intent to download the malicious file. Nevertheless, no user agent requests were discovered.

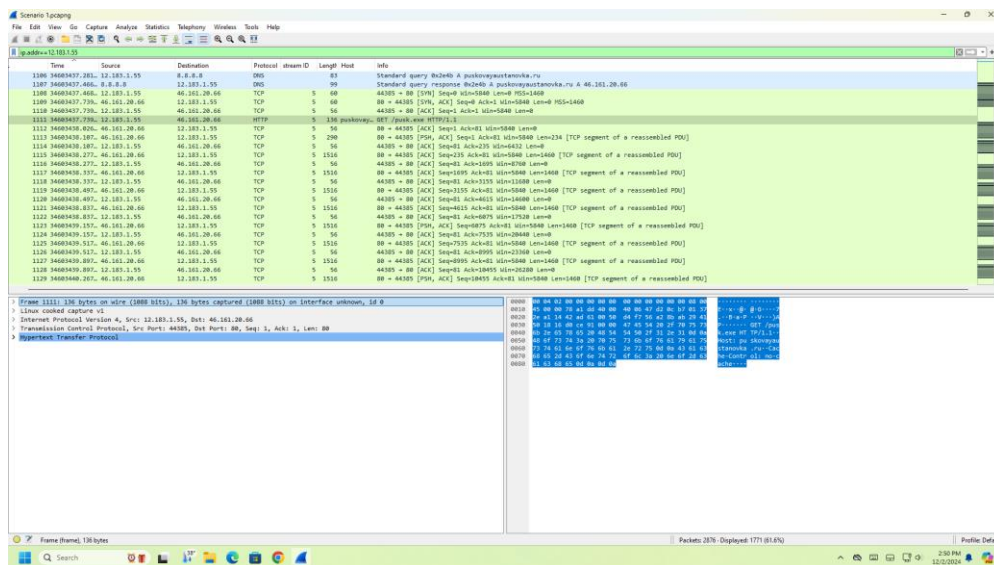


Figure 1: Domain name which is questionable

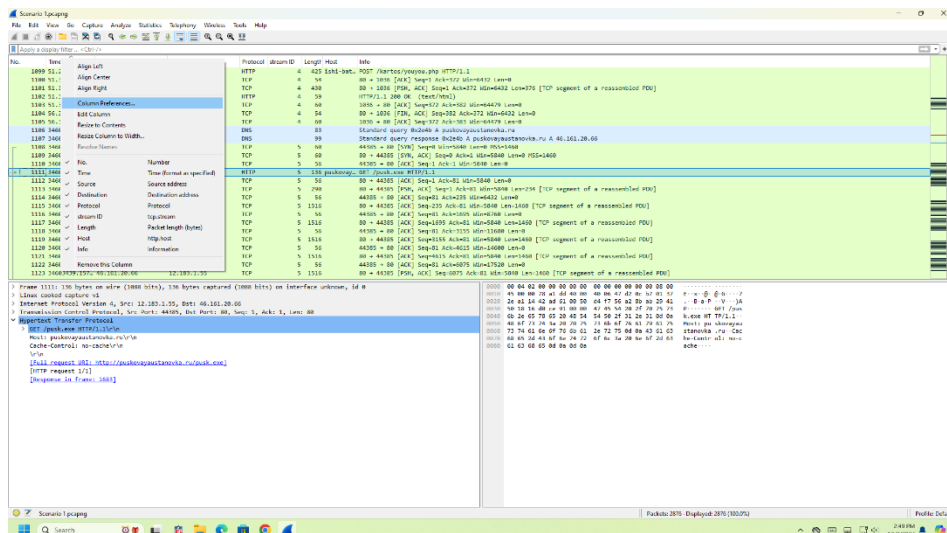


Figure2. Setting the column preferences

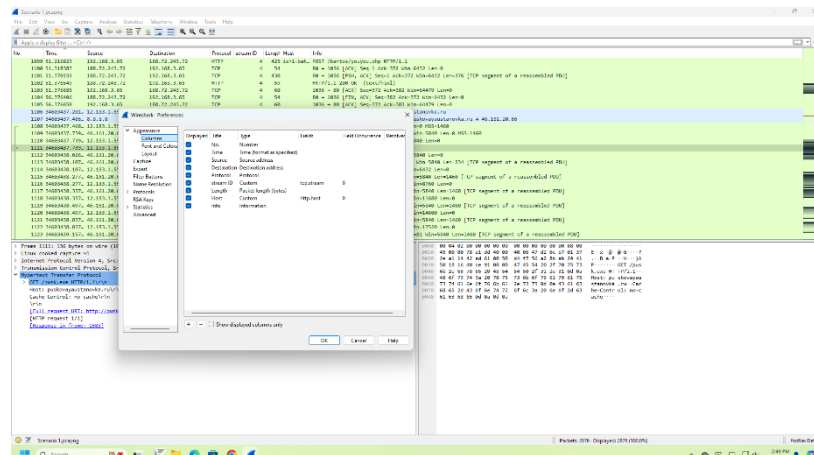


Figure 3. Adding columns Stream Id, host ID & adding Http & TCP Header

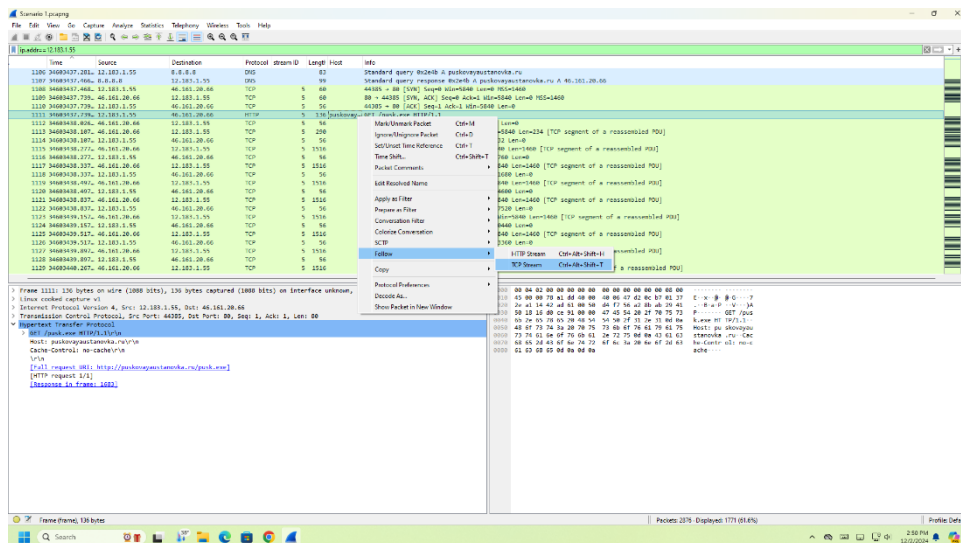


Figure4. Testing the ip with Tcp header



Figure 5: No user agent was detected

The screenshot shows the CyberForensicsDump1 application interface. The main window displays a hex dump of a file. The interface includes a menu bar (File, Edit, Search, View, Analysis, Tools, Window, Help), a toolbar, and a status bar. The main window displays a hex dump with columns for Offset (h), Hex, ASCII, and Decoded text. The decoded text shows an HTTP 1.1 200 OK response from a server named ngxin0k. The right sidebar shows a 'Special editors' panel with a 'Data inspector' tab and a 'Binary (8 bit)' view showing various bit fields like Int8, Int16, Int32, etc.

Figure 7: Copied the initial bytes in hex editor to determine file type

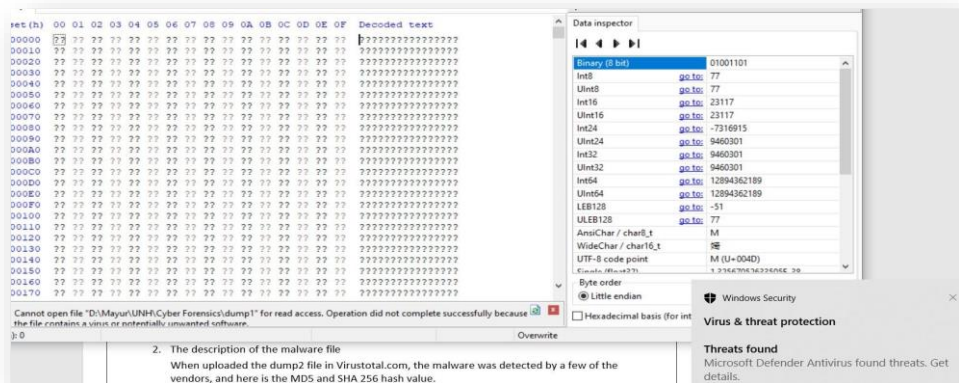
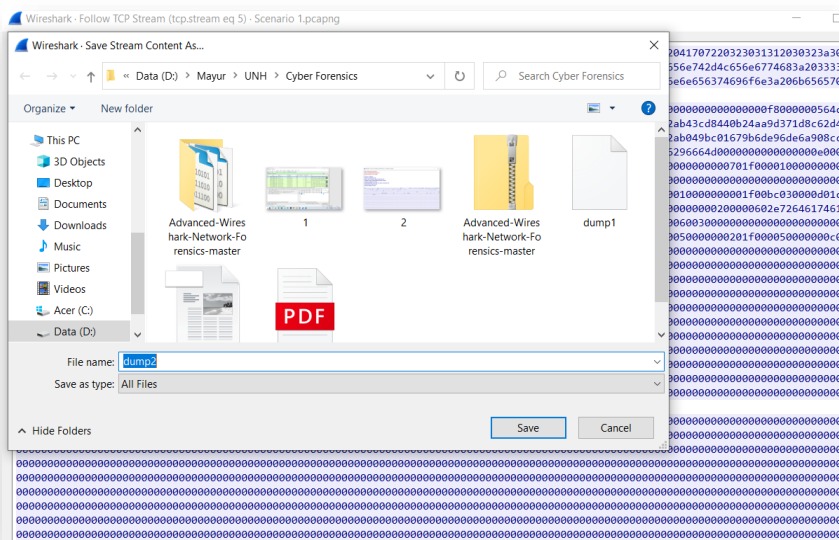




Figure 8: Antivirus detected and quarantined the infected file

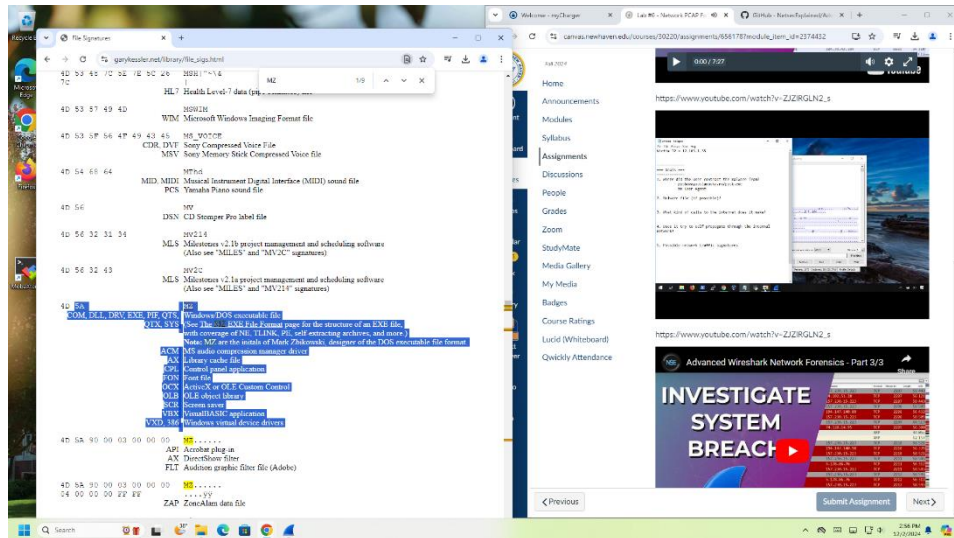
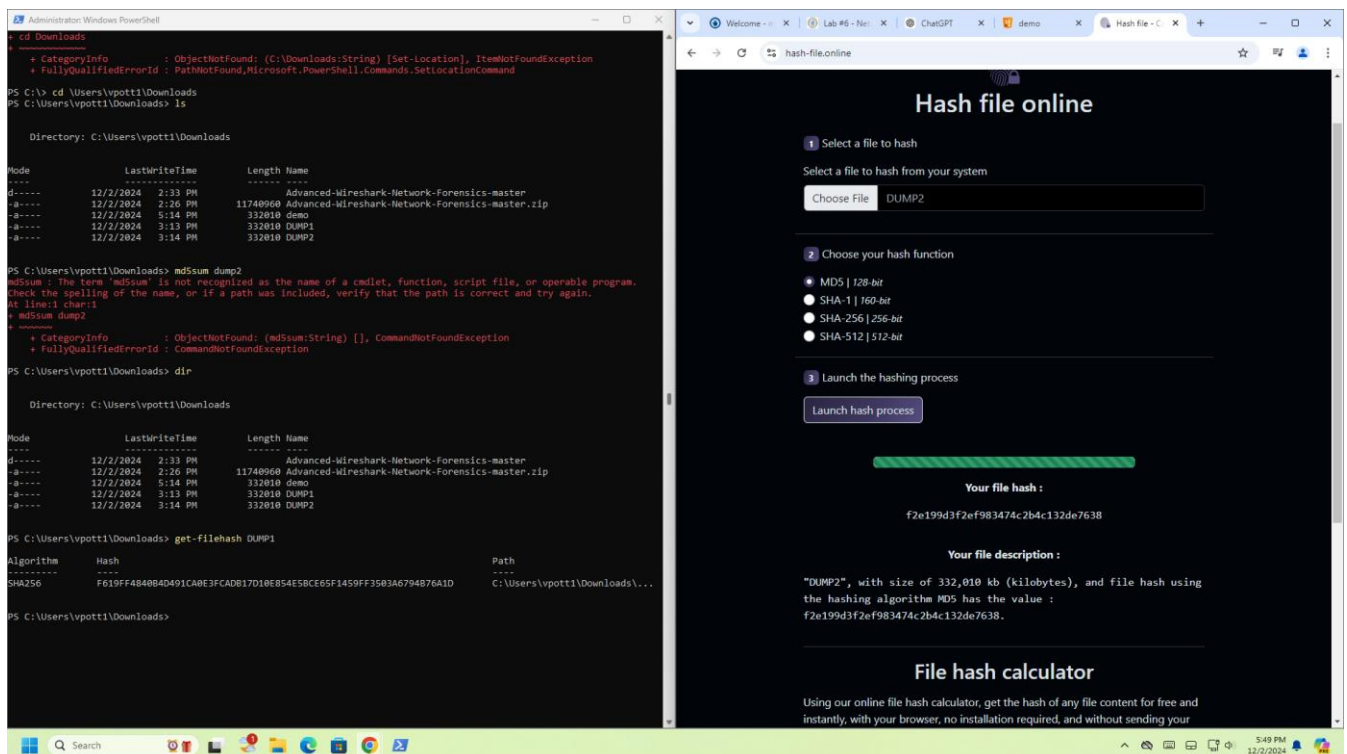


Figure 9. Understanding about MZ binary code in the hexa data



Administrator: Windows PowerShell

```

cd Downloads
+ CategoryInfo          : ObjectNotFound: (C:\Downloads:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\> cd \Users\vpott1\Downloads
PS C:\Users\vpott1\Downloads> ls

Directory: C:\Users\vpott1\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          12/2/2024  2:33 PM             Advanced-Wireshark-Network-Forensics-master
-a-----          12/2/2024  2:26 PM    11740960 Advanced-Wireshark-Network-Forensics-master.zip
-a-----          12/2/2024  5:14 PM         332810 demo
-a-----          12/2/2024  3:13 PM         332810 DUMP1
-a-----          12/2/2024  3:14 PM         332810 DUMP2

PS C:\Users\vpott1\Downloads> md5sum dump2
md5sum : The term 'md5sum' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (md5sum:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\vpott1\Downloads> dir

Directory: C:\Users\vpott1\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          12/2/2024  2:33 PM             Advanced-Wireshark-Network-Forensics-master
-a-----          12/2/2024  2:26 PM    11740960 Advanced-Wireshark-Network-Forensics-master.zip
-a-----          12/2/2024  5:14 PM         332810 demo
-a-----          12/2/2024  3:13 PM         332810 DUMP1
-a-----          12/2/2024  3:14 PM         332810 DUMP2

PS C:\Users\vpott1\Downloads> get-filehash DUMP1

Algorithm      Hash
-----
SHA256         F619FF4840B4D491CABE3FCADB17D10E854E5BCE65F1459FF3503A6794B76A1D
Path
-----
C:\Users\vpott1\Downloads\...

PS C:\Users\vpott1\Downloads>

```

hash-file.online

## Hash file online

- Select a file to hash
 

Select a file to hash from your system

Choose File DUMP2
- Choose your hash function
 

☐ MD5 | 128-bit
 ☒ SHA-1 | 160-bit
 ☐ SHA-256 | 256-bit
 ☐ SHA-512 | 512-bit
- Launch the hashing process
 

Launch hash process

**Your file hash :**

f619ff4840b4d491cae3fcadb17d10e854e5bce65f1459ff3503a6794b76a1d

**Your file description :**

"DUMP2", with size of 332,010 kb (kilobytes), and file hash using the hashing algorithm SHA-256 has the value : f619ff4840b4d491cae3fcadb17d10e854e5bce65f1459ff3503a6794b76a1d.

### File hash calculator

Using our online file hash calculator, get the hash of any file content for free and instantly, with your browser, no installation required, and without sending your

Administrator: Windows PowerShell

```

cd Downloads
+ CategoryInfo          : ObjectNotFound: (C:\Downloads:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\> cd \Users\vpott1\Downloads
PS C:\Users\vpott1\Downloads> ls

Directory: C:\Users\vpott1\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          12/2/2024  2:33 PM             Advanced-Wireshark-Network-Forensics-master
-a-----          12/2/2024  2:26 PM    11740960 Advanced-Wireshark-Network-Forensics-master.zip
-a-----          12/2/2024  5:14 PM         332810 demo
-a-----          12/2/2024  3:13 PM         332810 DUMP1
-a-----          12/2/2024  3:14 PM         332810 DUMP2

PS C:\Users\vpott1\Downloads> md5sum dump2
md5sum : The term 'md5sum' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (md5sum:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\vpott1\Downloads> dir

Directory: C:\Users\vpott1\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          12/2/2024  2:33 PM             Advanced-Wireshark-Network-Forensics-master
-a-----          12/2/2024  2:26 PM    11740960 Advanced-Wireshark-Network-Forensics-master.zip
-a-----          12/2/2024  5:14 PM         332810 demo
-a-----          12/2/2024  3:13 PM         332810 DUMP1
-a-----          12/2/2024  3:14 PM         332810 DUMP2

PS C:\Users\vpott1\Downloads> get-filehash DUMP1

Algorithm      Hash
-----
SHA256         F619FF4840B4D491CABE3FCADB17D10E854E5BCE65F1459FF3503A6794B76A1D
Path
-----
C:\Users\vpott1\Downloads\...

PS C:\Users\vpott1\Downloads>

```

hash-file.online

## Hash file online

- Select a file to hash
 

Select a file to hash from your system

Choose File DUMP2
- Choose your hash function
 

☐ MD5 | 128-bit
 ☒ SHA-1 | 160-bit
 ☐ SHA-256 | 256-bit
 ☐ SHA-512 | 512-bit
- Launch the hashing process
 

Launch hash process

**Your file hash :**

789473aecdf179e4e3e805d4f7c142c9ba68c3cd

**Your file description :**

"DUMP2", with size of 332,010 kb (kilobytes), and file hash using the hashing algorithm SHA-1 has the value : 789473aecdf179e4e3e805d4f7c142c9ba68c3cd.

### File hash calculator

Using our online file hash calculator, get the hash of any file content for free and instantly, with your browser, no installation required, and without sending your

Figure.10-12 Analyzing the hash value of the dump files

Figure 13: Results for the detected malware from virustotal site

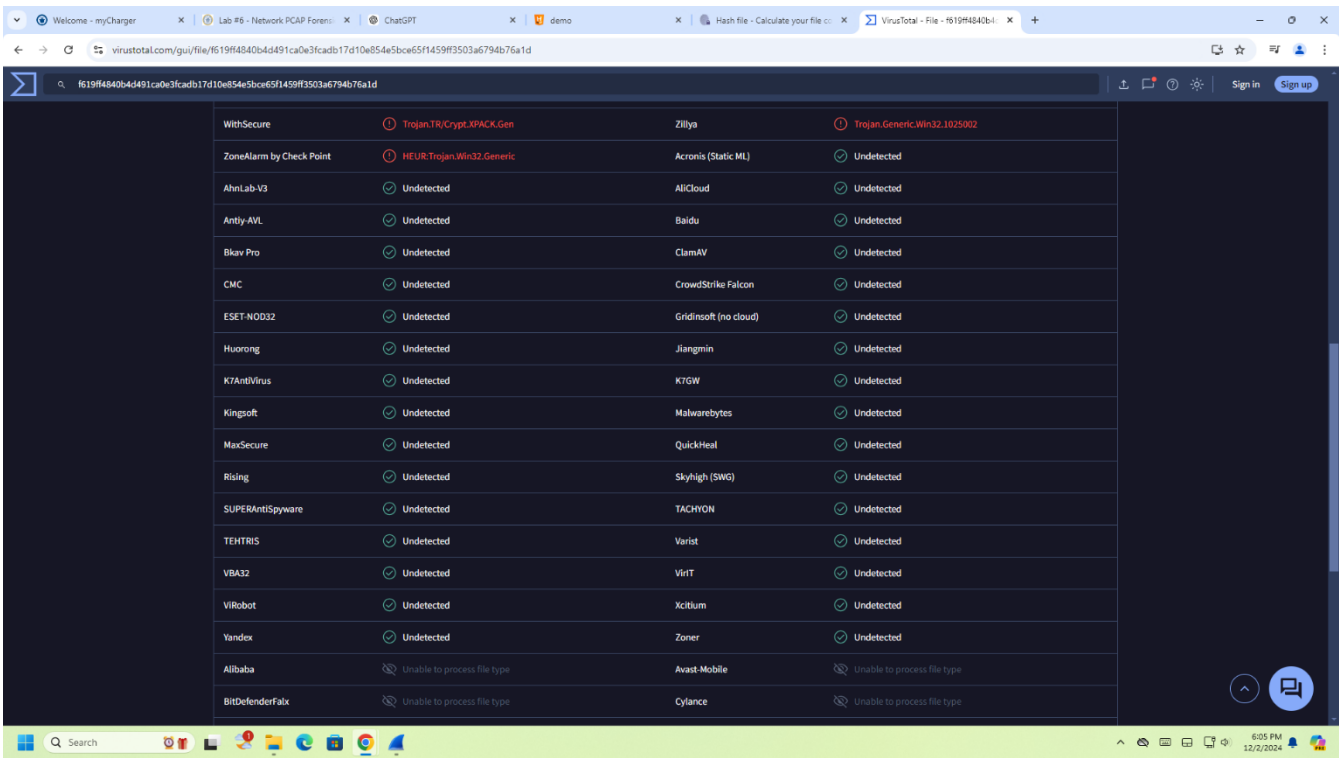
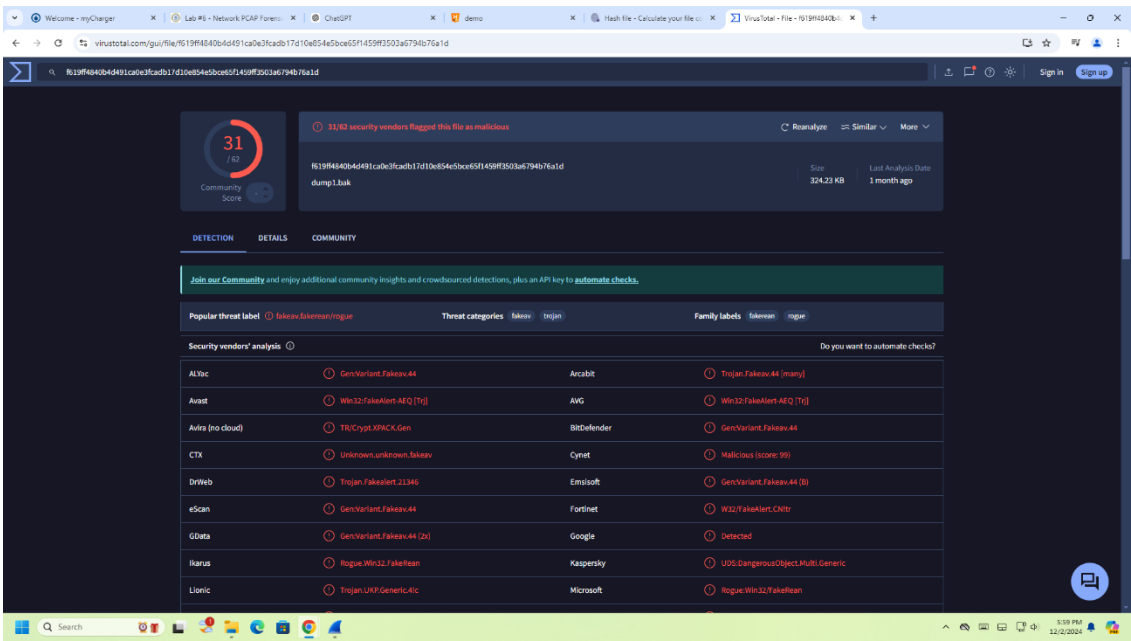


Figure 14: Results of virus as detected by multiple cybersecurity software providers

Zillya	! Trojan.Generic.Win32.1025002	ZoneAlarm by Check Point	! UDS:DangerousObject.Multi.Ge
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Antiy-AVL	✓ Undetected	Baidu	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	ESET-NOD32	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected	Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected	K7GW	✓ Undetected
Kingsoft	✓ Undetected	Malwarebytes	✓ Undetected
MaxSecure	✓ Undetected	QuickHeal	✓ Undetected
Rising	✓ Undetected	Sangfor Engine Zero	✓ Undetected

Figure 15: Some of the undetected viruses

## Calls to the internet:

Random DNS queries are sent to other domains in addition to the many connections to DNS. These domains had HTTP communications, and a connection to the server's website was made using port 80.

ip.addr == 12.183.155 && !tcp.stream == 5)								
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
1106	34603437.281...	12.183.1.55	8.8.8.8	DNS		83		Standard query 0x2e4b A puskovayaustanovka.ru
1107	34603437.466...	8.8.8.8	12.183.1.55	DNS		99		Standard query response 0x2e4b A puskovayaustanovka.ru A 46
1688	34603667.841...	12.183.1.55	8.8.8.8	DNS		78		Standard query 0xdc1d A laqoduhisegu.com
1689	34603667.841...	12.183.1.55	8.8.8.8	DNS		80		Standard query 0x1196 A kytevaviqopoci.com
1690	34603667.841...	12.183.1.55	8.8.8.8	DNS		77		Standard query 0xff6e A xyseditacif.com
1691	34603667.841...	12.183.1.55	8.8.8.8	DNS		78		Standard query 0xfb8e A wamojafadezy.com
1692	34603667.841...	12.183.1.55	8.8.8.8	DNS		80		Standard query 0xebc8 A qepovexidysoy.com
1693	34603667.841...	12.183.1.55	8.8.8.8	DNS		75		Standard query 0x1081 A wetotyger.com
1694	34603667.842...	12.183.1.55	8.8.8.8	DNS		75		Standard query 0x22ac A kyxiteruk.com
1695	34603667.842...	12.183.1.55	8.8.8.8	DNS		79		Standard query 0x97a4 A rumesexyzobuz.com
1696	34603667.842...	12.183.1.55	8.8.8.8	DNS		75		Standard query 0x67b0 A jebuponip.com
1697	34603667.842...	12.183.1.55	8.8.8.8	DNS		77		Standard query 0x99dc A quxovasuced.com
1698	34603667.842...	12.183.1.55	8.8.8.8	DNS		78		Standard query 0xc833 A wylyxaqunowy.com
1699	34603667.843...	12.183.1.55	8.8.8.8	DNS		80		Standard query 0x9e21 A bemojewedowigo.com
1700	34603667.843...	12.183.1.55	8.8.8.8	DNS		80		Standard query 0xd318 A sakafiduzipame.com
1701	34603667.843...	12.183.1.55	8.8.8.8	DNS		76		Standard query 0xfb4f A lukofymela.com
1702	34603667.843...	12.183.1.55	8.8.8.8	DNS		79		Standard query 0xc10 A kynugypenihyf.com
1703	34603667.843...	12.183.1.55	8.8.8.8	DNS		75		Standard query 0x1112 A jafybobik.com

> Frame 1107: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface unknown, id 0	0000	00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
> Linux cooked capture v1	0010	45 00 00 53 b9 28 00 00 35 11 ae 74 08 08 08 08 08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 12.183.1.55	0020	0c b7 01 37 00 35 d3 d2 00 3f d5 8d 2e 4b 81 81	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
> User Datagram Protocol, Src Port: 53, Dst Port: 54226	0030	00 01 00 01 00 00 00 00 12 70 75 73 6b 6f 76 6f	76 6f 76 6f 76 6f 76 6f 76 6f 76 6f 76 6f 76 6f
> Domain Name System (response)	0040	79 61 75 73 74 61 6e 6f 76 6b 61 02 72 75 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0050	01 00 01 c0 0c 00 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
	0060	a1 14 42	

Figure 16: Random requests of DNS to domains



No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
1953	34603673.260...	12.183.1.55	74.115.93.4	HTTP	34	201	wydygize...	GET /1017000430 HTTP/1.0
2394	34604057.888...	12.183.1.55	69.50.209.186	HTTP	69	383	wamojafa...	GET /10170004303462180033 HTTP/1.1
2404	34604058.640...	12.183.1.55	69.50.209.186	HTTP	70	414	wamojafa...	GET /buy.html HTTP/1.1
2417	34604060.000...	12.183.1.55	69.50.209.186	HTTP	71	468	wamojafa...	GET /style/style.css?v=4 HTTP/1.1
2455	34604063.427...	12.183.1.55	69.50.209.186	HTTP	72	470	wamojafa...	GET /colorbox/colorbox.css HTTP/1.1
2458	34604063.437...	12.183.1.55	69.50.209.186	HTTP	73	458	wamojafa...	GET /pngfix.js HTTP/1.1
2463	34604063.467...	12.183.1.55	69.50.209.186	HTTP	74	462	wamojafa...	GET /style/site.js HTTP/1.1
2464	34604063.467...	12.183.1.55	69.50.209.186	HTTP	75	480	wamojafa...	GET /colorbox/jquery.colorbox-min.js HTTP/1.1
2495	34604065.728...	12.183.1.55	69.50.209.186	HTTP	76	474	wamojafa...	GET /style/jquery-1.4.4.min.js HTTP/1.1
2648	34604114.361...	12.183.1.55	69.50.209.186	HTTP	77	466	wamojafa...	GET /images/strela.gif HTTP/1.1
2651	34604114.381...	12.183.1.55	69.50.209.186	HTTP	78	463	wamojafa...	GET /images/ic2.gif HTTP/1.1
2654	34604114.387...	12.183.1.55	69.50.209.186	HTTP	79	463	wamojafa...	GET /images/ic3.gif HTTP/1.1
2659	34604114.401...	12.183.1.55	69.50.209.186	HTTP	80	464	wamojafa...	GET /images/box2.jpg HTTP/1.1
2660	34604114.401...	12.183.1.55	69.50.209.186	HTTP	81	462	wamojafa...	GET /images/bg.gif HTTP/1.1
2663	34604114.418...	12.183.1.55	69.50.209.186	HTTP	82	464	wamojafa...	GET /images/head.jpg HTTP/1.1
2710	34604118.490...	12.183.1.55	69.50.209.186	HTTP	83	465	wamojafa...	GET /images/logo2.gif HTTP/1.1
2715	34604118.528...	12.183.1.55	69.50.209.186	HTTP	84	464	wamojafa...	GET /images/logo.gif HTTP/1.1
2718	34604118.542...	12.183.1.55	69.50.209.186	HTTP	85	465	wamojafa...	GET /images/block.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 00
0010 45 00 00 b9 11 9b 40 00 40 06 73 3f 00 00 00
0020 4a 73 5d 04 d1 4d 00 50 b1 f0 42 1a d0 00 00
0030 50 18 16 d0 6f 8c 00 00 47 45 54 20 2d 00 00
0040 37 30 30 30 34 33 30 20 48 54 54 50 2d 00 00
0050 0d 0a 48 6f 73 74 3a 20 77 79 64 79 6c 00 00
0060 71 2e 63 6f 6d 0d 0a 55 73 65 72 2d 4a 00 00
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2d 00 00
0080 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4a 00 00
0090 20 36 2e 30 3b 20 57 69 6e 64 6f 77 7d 00 00
00a0 20 35 2e 31 29 0d 0a 41 63 63 65 70 7d 00 00

```

Figure 17: HTTP connections initiated by the host

## Propagation through internal network:

No evidence to connect with RF1918 or 12.x.x.x addresses

ip.src == 12.183.1.55 && (ip.addr == 192.168.0.0/16    ip.addr == 172.16.0.0/12    ip.addr == 10.0.0.0/8    ip.dst == 12.0.0.0/8)								
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
2846	34604177.536...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2847	34604177.547...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2848	34604177.567...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2852	34604179.026...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2853	34604179.036...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2854	34604179.056...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2858	34604180.526...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2859	34604180.539...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2860	34604180.557...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2864	34604182.006...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2868	34604183.506...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2869	34604183.537...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)
2873	34604185.016...	69.50.209.186	12.183.1.55	ICMP		122		Destination unreachable (Port unreachable)

Figure 11: Destination unreachable with ICMP protocol

ip.src == 12.183.1.25 && (ip.addr == 192.168.0.0/16    ip.addr == 172.16.0.0/12    ip.addr == 10.0.0.0/8    ip.dst == 12.0.0.0/8) && (icmp)								
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info

Figure 12: When ICMP wasn't used, it shows that virus didn't attempt to connect internal network

```
GET /buy.html HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727
LR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: wamojafadezy.com
Connection: Keep-Alive
Cookie: 7oInVuVUHoG=10170004303462180033

HTTP/1.1 200 OK
Date: Sun, 03 Apr 2011 02:12:34 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

2ec2
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Win 7 Total Security</title>
<link rel="stylesheet" type="text/css" href="style/style.css?v=4" />
<!--[if IE 6]><link rel="stylesheet" href="style/ie6.css" type="text/css" /><![endif]-->
<!--[if IE 7]><link rel="stylesheet" href="style/ie7.css" type="text/css" /><![endif]-->
<!--[if IE]><script src="pngfix.js" type="text/javascript"></script><![endif]-->
<link media="screen" rel="stylesheet" href="/colorbox/colorbox.css" />

<script src="/style/jquery-1.4.4.min.js" type="text/javascript" charset="utf-8"></script>
<script src="/style/site.js" type="text/javascript" charset="utf-8"></script>
<script src="/colorbox/jquery.colorbox-min.js"></script>

</head>
<body>
```

Figure 13: Website influencing users to buy antivirus software

## Scenario 2:

The following information was found after reviewing the files. An FTP server with the IP address 192.168.56.1 was discovered to be the target of the denial-of-service attack. Traffic had risen sharply just before the tragedy. The IP address from which the attacker was located was 192.168.56.101.

Figure 1: The attacker's IP address (192.168.56.)

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

< Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) 0000 ff ff ff ff ff ff 08 00 27 b1 6f

Wireshark - Conversations - Scenario 2.pcap

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ BPV7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☐ IPv4

☒ IPv6

☐ IPX

☐ JXTA

Filter list for specific type

Ethernet - 3	IPv4 - 1	IPv6	TCP - 7744	UDP											
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
192.168.56.1	21	192.168.56.101	51904	15	1 kB	2052	8	674 bytes	7	533 bytes	19.206899	0.0427	126 kbps	99 kbps	
192.168.56.1	21	192.168.56.101	51905	17	1 kB	2053	9	770 bytes	8	604 bytes	19.207421	0.0468	131 kbps	103 kbps	
192.168.56.1	21	192.168.56.101	51908	17	1 kB	2056	9	770 bytes	8	605 bytes	19.218572	0.0512	120 kbps	94 kbps	
192.168.56.1	21	192.168.56.101	51924	16	1 kB	2072	8	674 bytes	8	605 bytes	19.278151	0.0771	69 kbps	62 kbps	
192.168.56.1	21	192.168.56.101	51932	17	1 kB	2079	9	770 bytes	8	603 bytes	19.309117	0.0518	118 kbps	93 kbps	
192.168.56.1	21	192.168.56.101	52009	17	1 kB	2161	9	770 bytes	8	604 bytes	19.652536	0.0594	103 kbps	81 kbps	
192.168.56.1	21	192.168.56.101	52080	14	1 kB	2228	8	675 bytes	6	465 bytes	19.933089	0.0348	155 kbps	106 kbps	
192.168.56.1	21	192.168.56.101	52082	17	1 kB	2229	9	770 bytes	8	607 bytes	19.933293	0.0413	149 kbps	117 kbps	
192.168.56.1	21	192.168.56.101	52489	17	1 kB	2638	9	785 bytes	8	624 bytes	21.376818	0.0366	171 kbps	136 kbps	
192.168.56.1	21	192.168.56.101	52530	19	2 kB	2673	10	859 bytes	9	694 bytes	21.490142	0.0326	210 kbps	170 kbps	
192.168.56.1	21	192.168.56.101	52529	17	1 kB	2675	9	785 bytes	8	626 bytes	21.490953	0.0506	124 kbps	98 kbps	
192.168.56.1	21	192.168.56.101	52614	17	1 kB	2764	9	785 bytes	8	625 bytes	21.723334	0.0431	145 kbps	115 kbps	
192.168.56.1	21	192.168.56.101	52635	17	1 kB	2783	9	785 bytes	8	627 bytes	21.777507	0.0339	185 kbps	148 kbps	
192.168.56.1	21	192.168.56.101	52636	17	1 kB	2785	9	785 bytes	8	624 bytes	21.778685	0.0253	248 kbps	197 kbps	
192.168.56.1	21	192.168.56.101	52637	17	1 kB	2786	9	785 bytes	8	625 bytes	21.779570	0.0403	155 kbps	123 kbps	
192.168.56.1	21	192.168.56.101	52661	17	1 kB	2806	9	785 bytes	8	623 bytes	21.845807	0.0291	216 kbps	171 kbps	
192.168.56.1	21	192.168.56.101	52712	17	1 kB	2860	9	785 bytes	8	627 bytes	21.994254	0.0336	187 kbps	149 kbps	
192.168.56.1	21	192.168.56.101	52784	17	1 kB	2930	9	785 bytes	8	630 bytes	22.169573	0.0364	172 kbps	138 kbps	
192.168.56.1	21	192.168.56.101	52838	16	1 kB	2986	9	785 bytes	7	549 bytes	22.336434	0.0354	177 kbps	124 kbps	
192.168.56.1	21	192.168.56.101	52839	17	1 kB	2987	9	785 bytes	8	626 bytes	22.338497	0.0349	180 kbps	143 kbps	
192.168.56.1	21	192.168.56.101	52840	17	1 kB	2988	9	786 bytes	8	628 bytes	22.339343	0.0362	173 kbps	138 kbps	
192.168.56.1	21	192.168.56.101	52842	17	1 kB	2992	9	785 bytes	8	633 bytes	22.344807	0.0391	160 kbps	129 kbps	
192.168.56.1	21	192.168.56.101	52899	12	993 bytes	3048	7	591 bytes	5	402 bytes	22.505087	0.0398	118 kbps	80 kbps	
192.168.56.1	21	192.168.56.101	52904	17	1 kB	3049	9	788 bytes	8	630 bytes	22.505577	0.0422	149 kbps	119 kbps	
192.168.56.1	21	192.168.56.101	52905	17	1 kB	3050	9	788 bytes	8	626 bytes	22.505628	0.0223	282 kbps	224 kbps	
192.168.56.1	21	192.168.56.101	52938	16	1 kB	3088	8	686 bytes	8	627 bytes	22.596102	0.0213	257 kbps	235 kbps	
192.168.56.1	21	192.168.56.101	52984	14	1 kB	3132	7	635 bytes	7	549 bytes	22.715212	0.0306	166 kbps	143 kbps	

Figure 2: Huge number of TCP connections were identified

### Summary of attack:

The network 192.168.56.0/24 was the target of the initial attack. A peek of the hosts was provided by the ARP scan

Figure 3: ARP scan

No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
2	0.000163	PCSSystemtec_00:d0::	PCSSystemtec_b1:6f::	ARP		60		192.168.56.1 is at 08:00:27:00:d0:24
147	1.307491	PCSSystemtec_00:d0::	PCSSystemtec_b1:6f::	ARP		60		192.168.56.1 is at 08:00:27:00:d0:24
299	1.511937	PCSSystemtec_0f:ae::	PCSSystemtec_b1:6f::	ARP		60		192.168.56.100 is at 08:00:27:0f:ae:4a
514	11.504637	PCSSystemtec_00:d0::	PCSSystemtec_b1:6f::	ARP		60		192.168.56.1 is at 08:00:27:00:d0:24
2525	17.403477	PCSSystemtec_b1:6f::	PCSSystemtec_00:d0::	ARP		42		192.168.56.101 is at 08:00:27:b1:6f:f9

> Frame 299: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

> Ethernet II, Src: PCSSystemtec\_0f:ae:4a (08:00:27:0f:ae:4a), Dst: PCSSystemtec\_b1:6f:f9 (08:00:27:b1:6f:f9)

> Address Resolution Protocol (reply)

```

0000 08 00 27 b1 6f f9 08 00 27 0f ae 4a 08 06 00 01 .....J...
0010 08 00 06 04 00 02 08 00 27 0f ae 4a c0 a8 38 64 .....J--8d
0020 08 00 27 b1 6f f9 c0 a8 38 65 00 00 00 00 00 00 .....8e.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```



tcp.flags == 0x0012								
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
537	12.789941	192.168.56.1	192.168.56.101	TCP	28	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 TSecr=
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 TSecr=
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 TSecr=
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 TSecr=
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 TSecr=
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 TSecr=
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 TSecr=
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 TSecr=

> Frame 537: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)	0000	08 00 27 b1 6f f9 08 00	27 00 d0 24 08 00 45 00	..'.o...'.\$.E..
> Ethernet II, Src: PCSSystemtec_00:d0:24 (08:00:27:00:d0:24), Dst: PCSSystemtec_b1:6f:f9 (08:00:27:b1:6f:f9)	0010	00 2c 37 6b 40 00 00 06	d1 a9 c0 a8 38 01 c0 a8	..7k@...8...
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101	0020	38 65 00 15 93 4f 19 5a	64 d2 f0 8d 8e 40 50 12	8e...O.Z d....E..
> Transmission Control Protocol, Src Port: 21, Dst Port: 37711, Seq: 0, Ack: 1, Len: 0	0030	20 00 f5 ff 00 00 02 04	05 b4 00 00	.....

Figure 4: These ports were identified as open

ftp.response.code == 230								
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
34412	40.844683	192.168.56.1	192.168.56.101	FTP	3640	91		Response: 230 User anon logged in
1060...	57.611519	192.168.56.1	192.168.56.101	FTP	7356	91		Response: 230 User anon logged in

> Frame 34412: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)	0000	08 00 27 b1 6f f9 08 00	27 00 d0 24 08 00 45 00	..'.o...'.\$.E..
> Ethernet II, Src: PCSSystemtec_00:d0:24 (08:00:27:00:d0:24), Dst: PCSSystemtec_b1:6f:f9 (08:00:27:b1:6f:f9)	0010	00 4d 77 ed 40 00 80 06	91 06 c0 a8 38 01 c0 a8	..7k@...8...
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101	0020	38 65 00 15 d0 f4 30 d3	51 67 ec 2e b6 45 30 12	8e...O.Z d....E..
> Transmission Control Protocol, Src Port: 21, Dst Port: 53492, Seq: 124, Ack: 56, Len: 25	0030	01 03 46 09 00 00 01 01	08 0a 00 b9 89 da 00 00	.....
Source Port: 21	0040	d1 a9 32 33 30 20 55 73	65 72 20 61 6e 6f 6e 6f	.....
Destination Port: 53492	0050	6c 6f 67 67 65 64 20 69	6e 0d 0a	.....

Figure 5.: The user's logged-in ports (the attacker used a brute force assault to obtain unauthorized access)

```
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
150 Opening BINARY mode data connection for Whywecanthavenicecat.png (176510 bytes)
226 Transfer Complete
QUIT
221 Goodbye!
```

Figure 6: successfully logged in using the "anon/anon" credentials.

After using the credentials to log in, the attacker searched the directories and downloaded an image.



Figure 7: whywecanthavenicecat.png

When the encoded text is file is opened we got the above eveidence picture.

## **2. Problem Solving and Troubleshooting**

**Problem 1:** Identifying the appropriate tool for analyzing the packet's data.

**Solution 1:** Following a thorough Google search, the most appropriate tool was identified by comparing the available sources and trustworthy sources.

## **3. Conclusion and Recommendations**

In a criminal investigation, network forensics is just as important as any other type of forensics. Essential details, like traffic and illegal access, are provided to the investigator through network data analysis. A thorough examination is necessary to determine whether a particular situation is suspicious, even though some can be quickly determined to be unapproved.

The detectives will be able to recognize and evaluate network servers after finishing this lab assignment. But, while accessing any network that might be an attempt to put the victim in danger, it's crucial to exercise caution.

## **4. References**

- Lecture notes - [https://canvas.newhaven.edu/courses/26502/files/4678895?module\\_item\\_id=2054453](https://canvas.newhaven.edu/courses/26502/files/4678895?module_item_id=2054453)
- Video Lectures - [https://canvas.newhaven.edu/courses/26502/pages/watch-network-forensics-dns?module\\_item\\_id=2054452](https://canvas.newhaven.edu/courses/26502/pages/watch-network-forensics-dns?module_item_id=2054452)

