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

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 wiresharks. 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 infested 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.

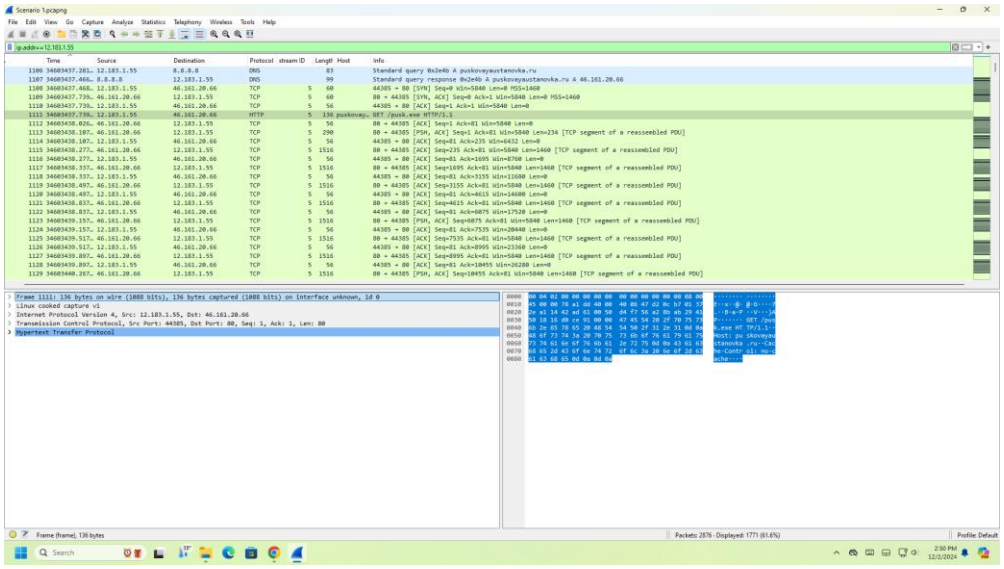


Figure 1: Domain name which is questionable

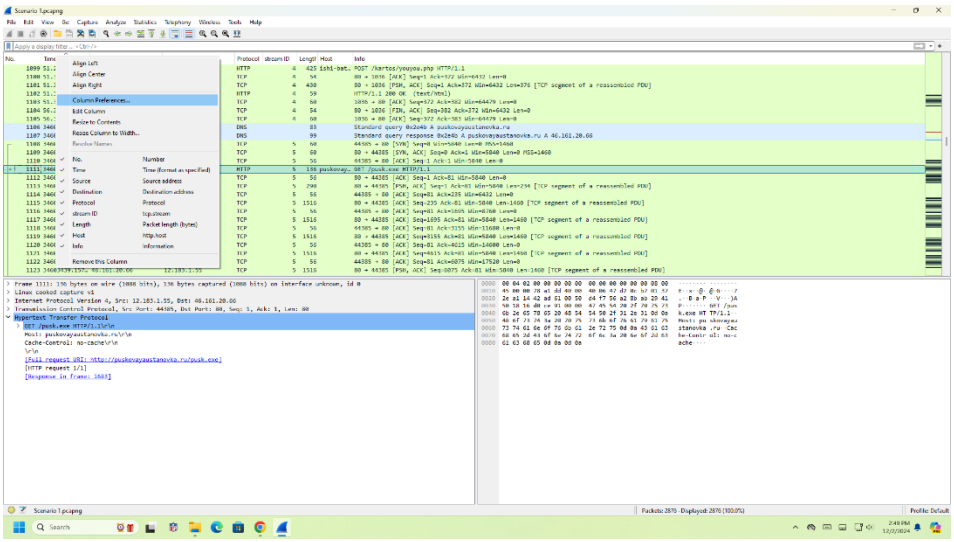


Figure2. Setting the coloumn preferences

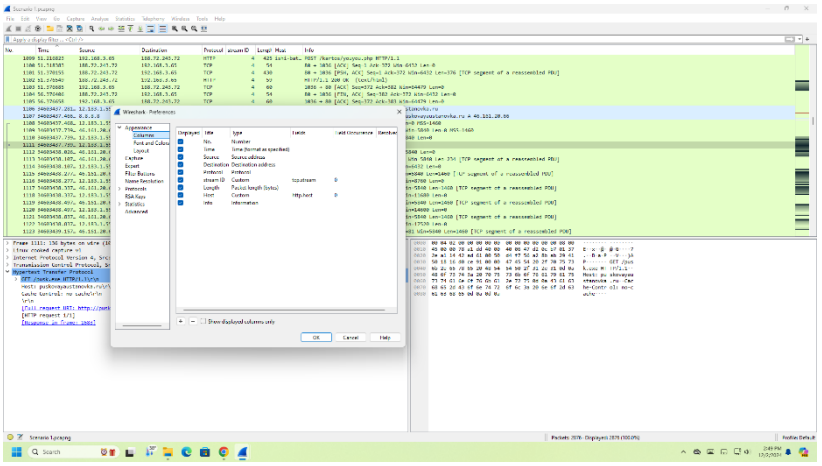


Figure 3. Adding columns Stream Id, host ID & adding Http & TCP Header

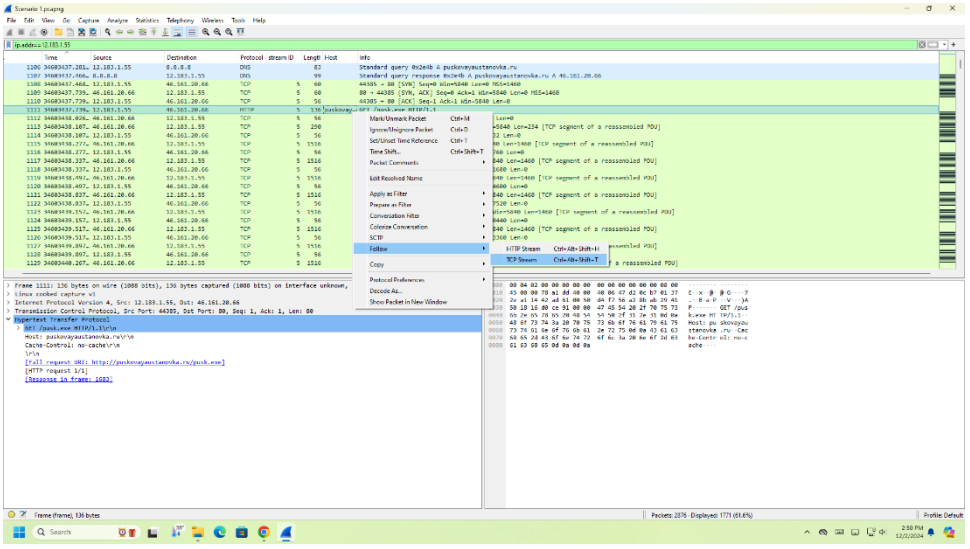


Figure4. Testing the ip with TCp header

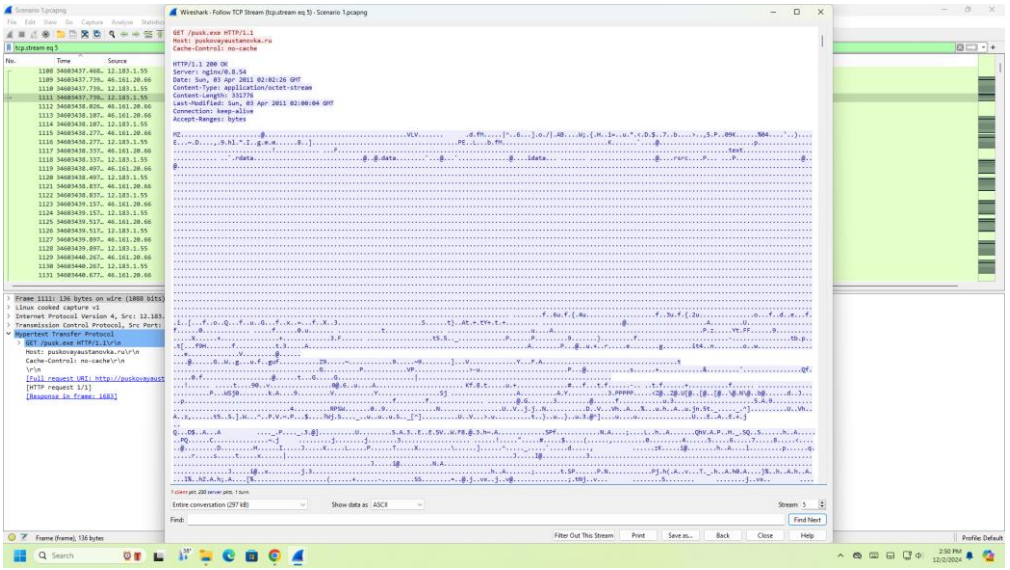


Figure 5: No user agent was detected

Download the Data in a raw format and open it in a hexa data form

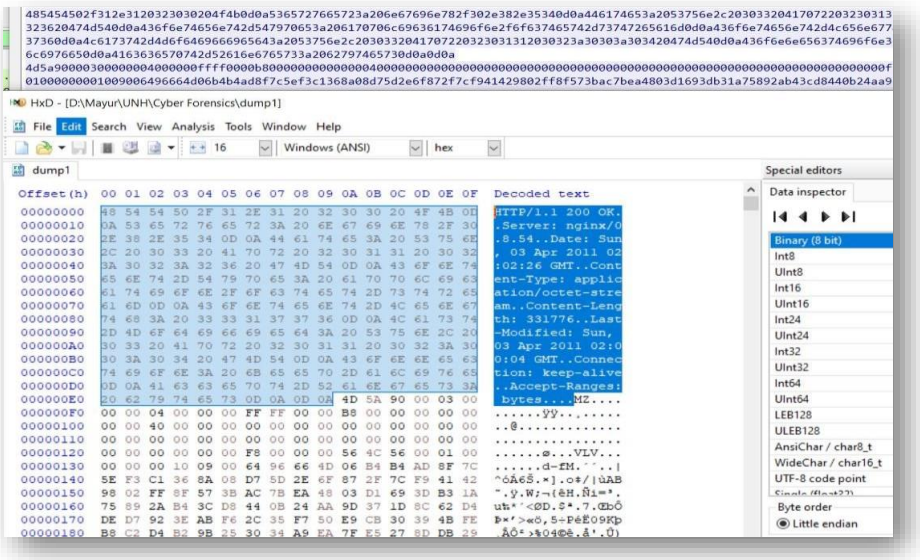
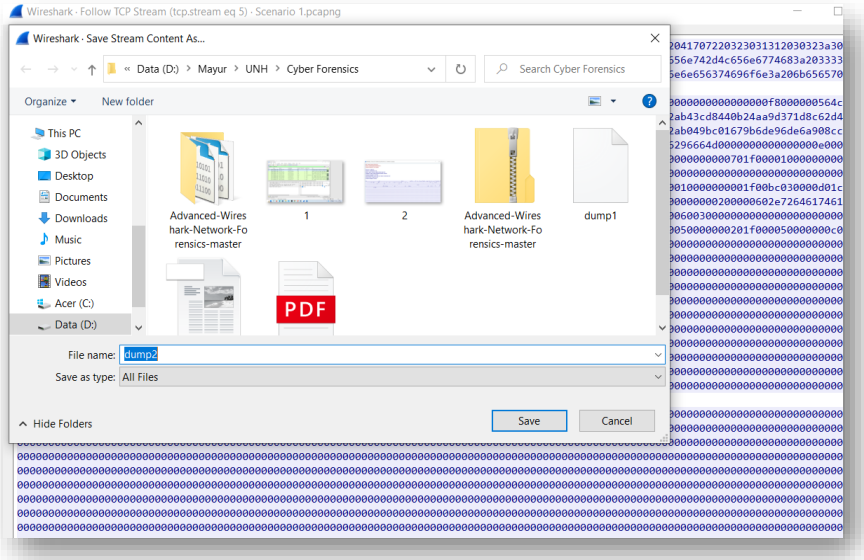


Figure 6: Raw images copied as dump 1 and dump 2

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



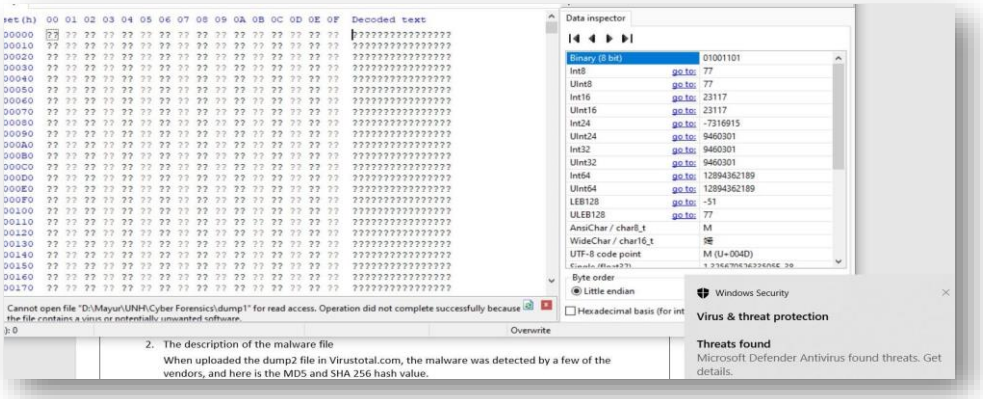


Figure 8: Antivirus detected and quarantined the infected file

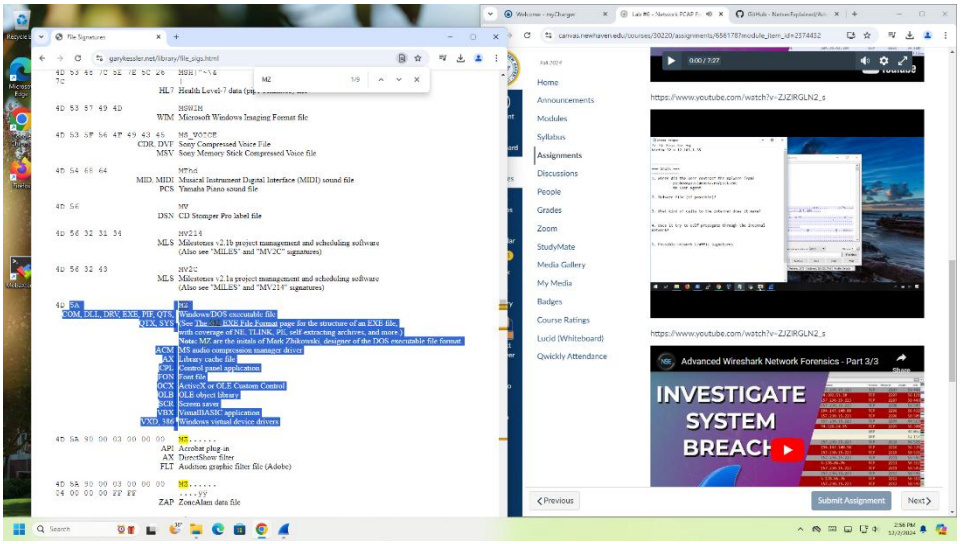
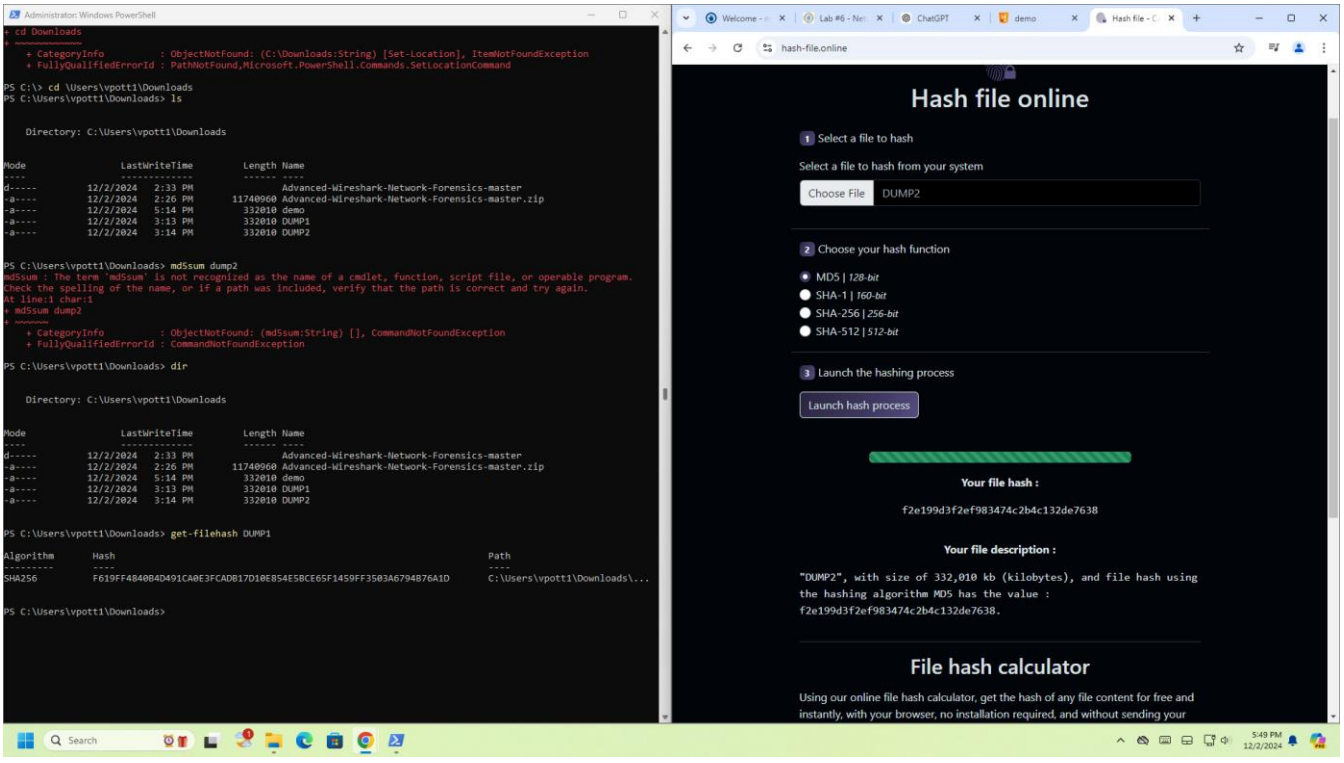
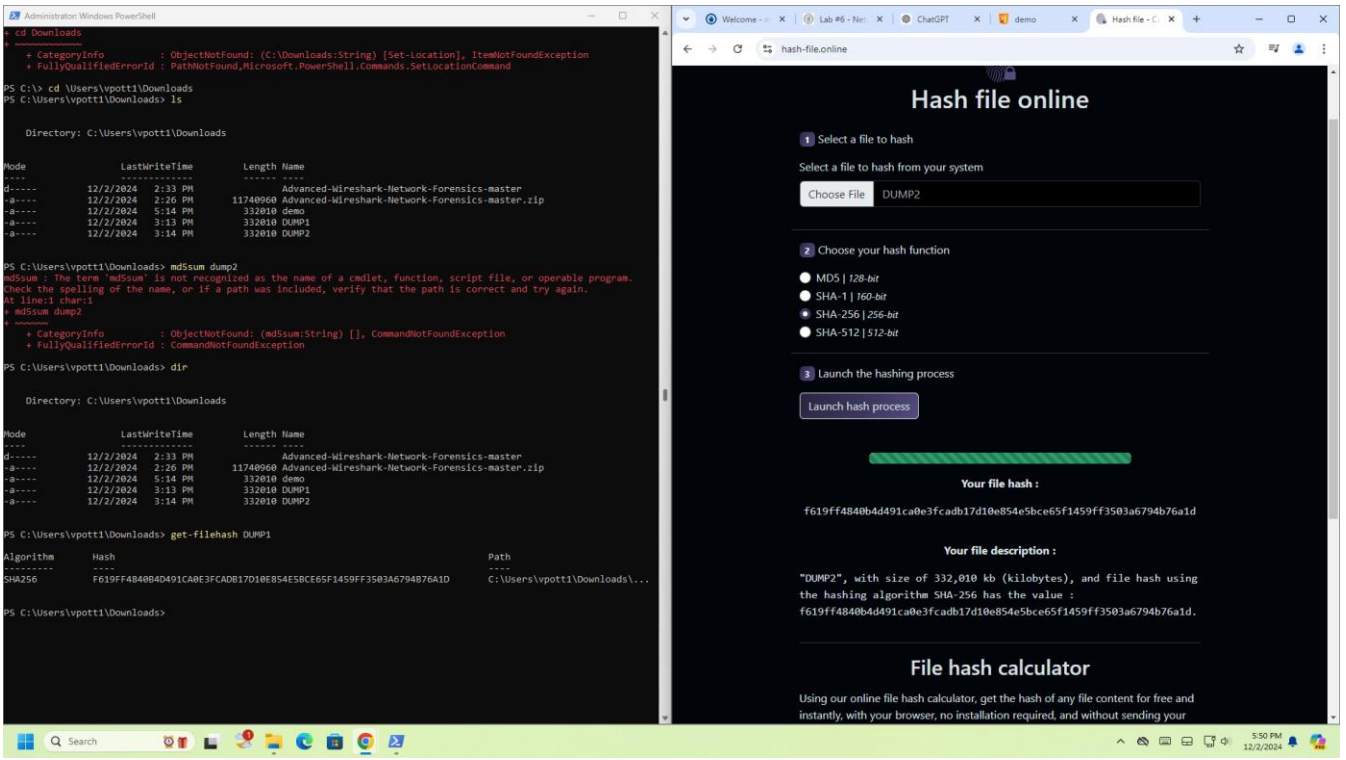


Figure 9. Understanding about MZ binary code in the hexa data





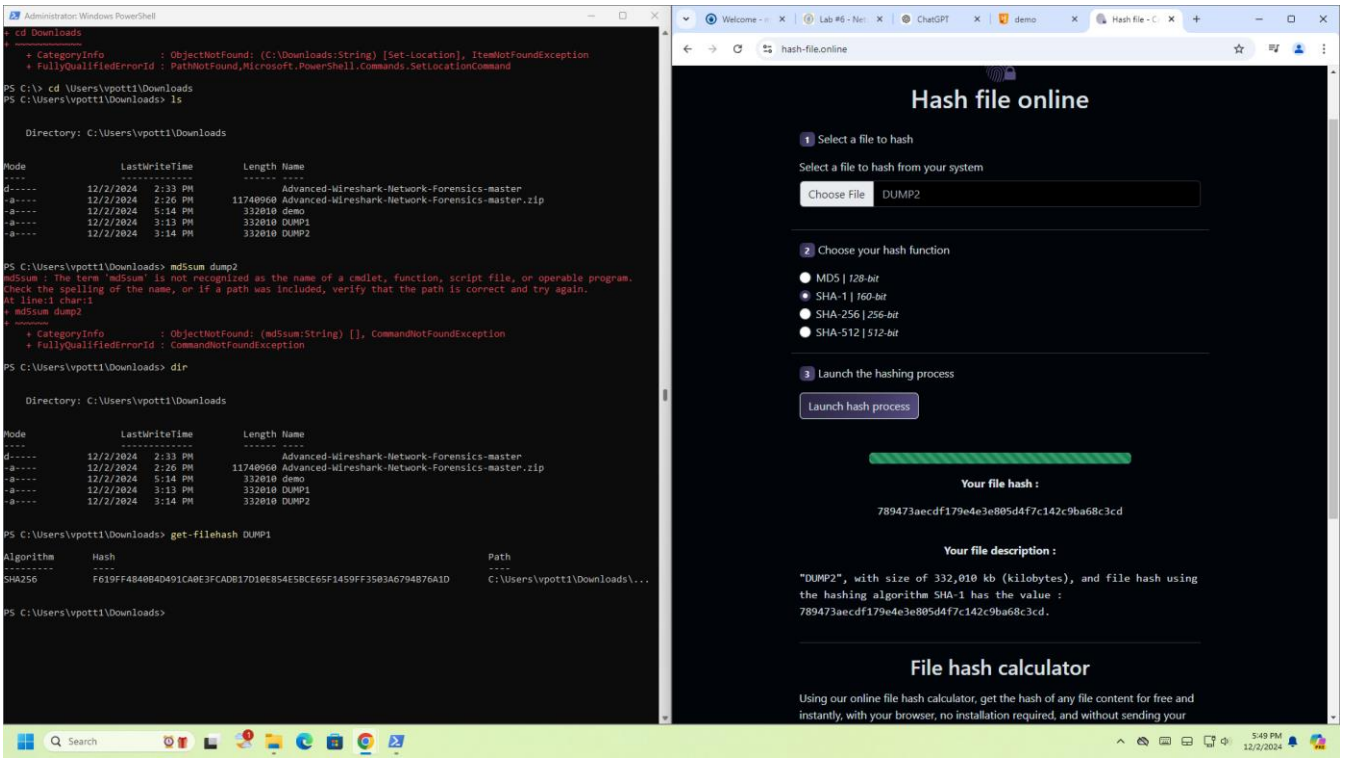
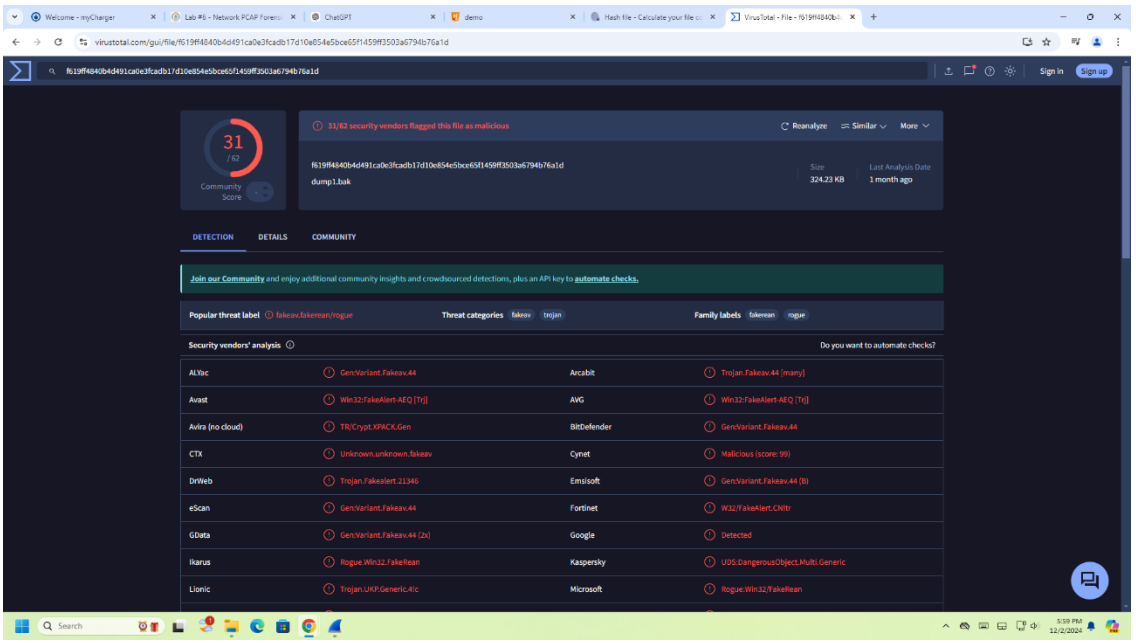


Figure.10-12 Analysizing the hash value of the dump files

Figure 13: Results for the detected malware from virustotal site



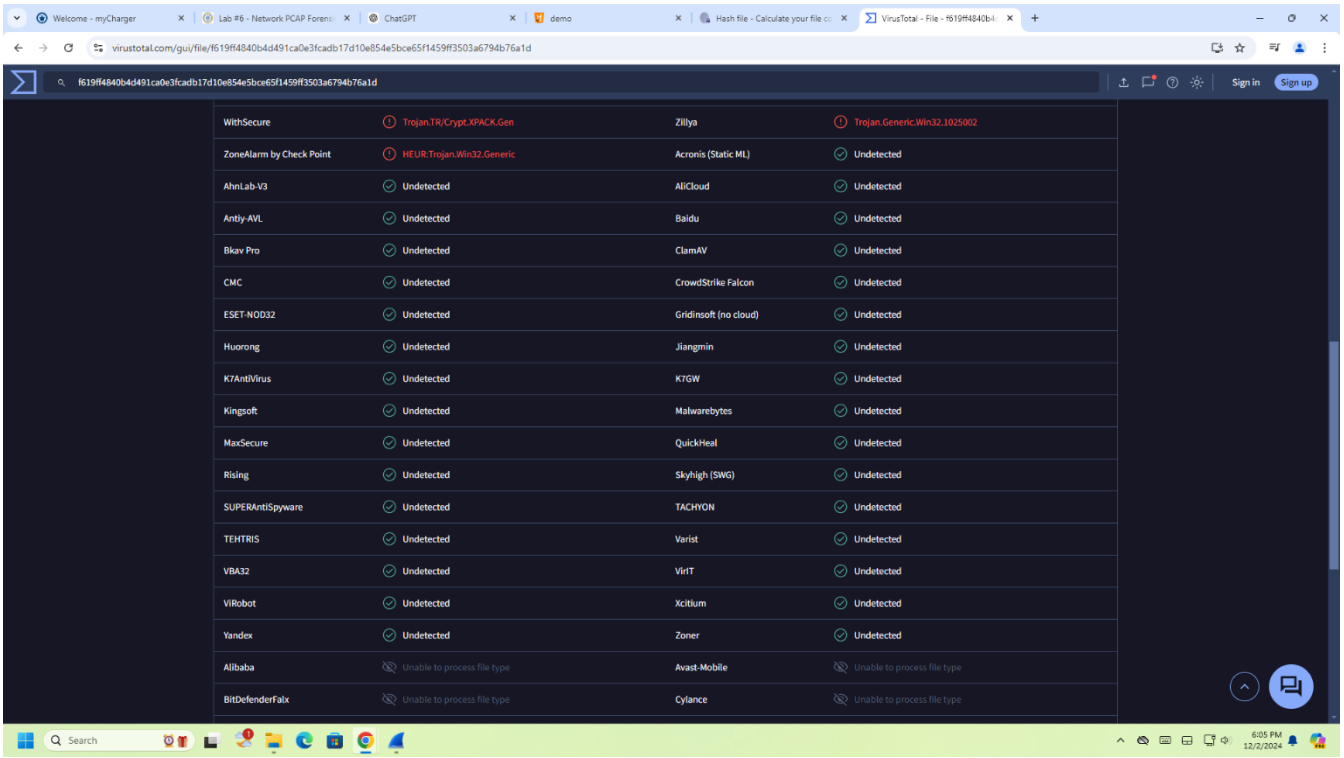


Figure 14: Results of virus as detected by multiple cybersecurity software providers

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.

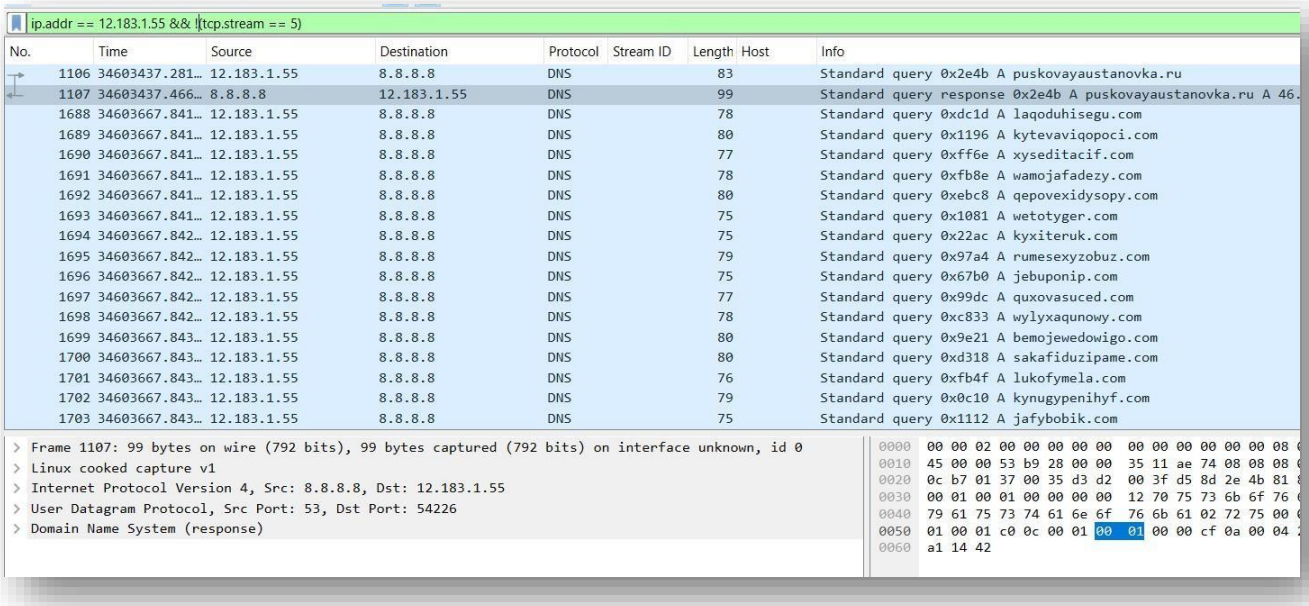
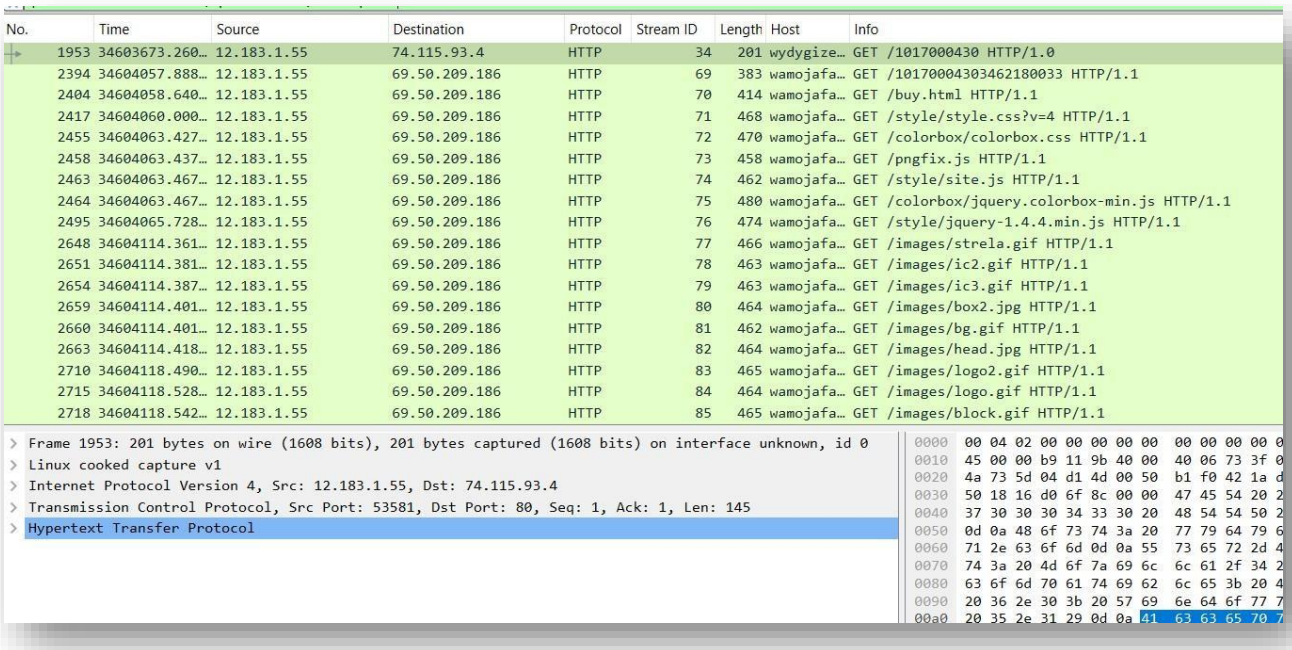


Figure 16: Random requests of DNS to domains



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

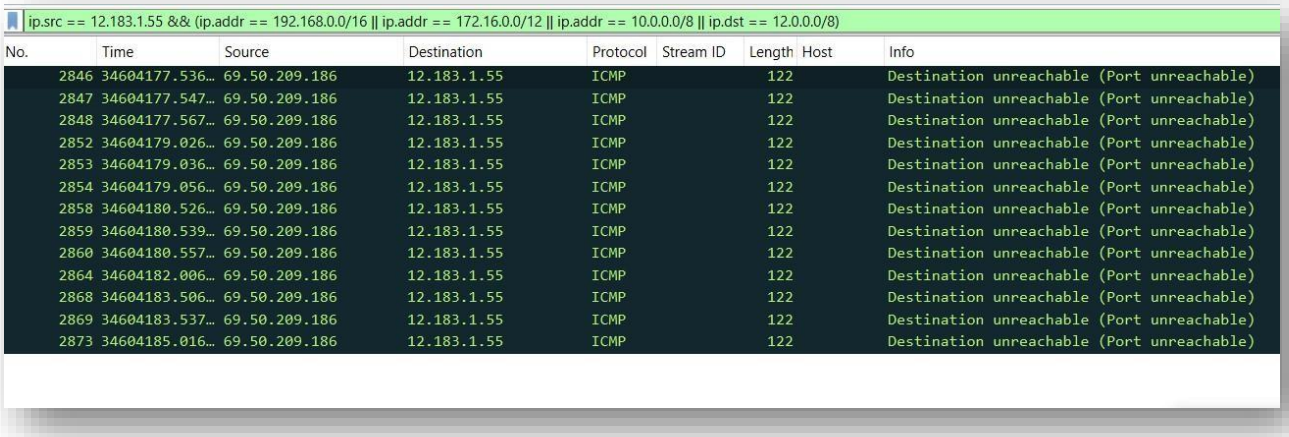
```
> Frame 1953: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface unknown, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 12.183.1.55, Dst: 74.115.93.4
> Transmission Control Protocol, Src Port: 53581, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
> Hypertext Transfer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

```
0000  00 04 02 00 00 00 00 00  00 00 00 00 0
0010  45 00 00 b9 11 9b 40 00  40 06 73 3f 0
0020  4a 73 5d 04 d1 4d 00 50  b1 f0 42 1a d
0030  50 18 16 d0 6f 8c 00 00  47 45 54 20 2
0040  37 30 30 30 34 33 30 20  48 54 54 50 2
0050  0d 0a 48 6f 73 74 3a 20  77 79 64 79 6
0060  71 2e 63 6f 6d 0d 0a 55  73 65 72 2d 4
0070  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 34 2
0080  63 6f 6d 70 61 74 69 62  6c 65 3b 20 4
0090  20 36 2e 30 3b 20 57 69  6e 64 6f 77 7
00a0  20 35 2e 31 29 0d 0a 41  63 63 65 70 7
```

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

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

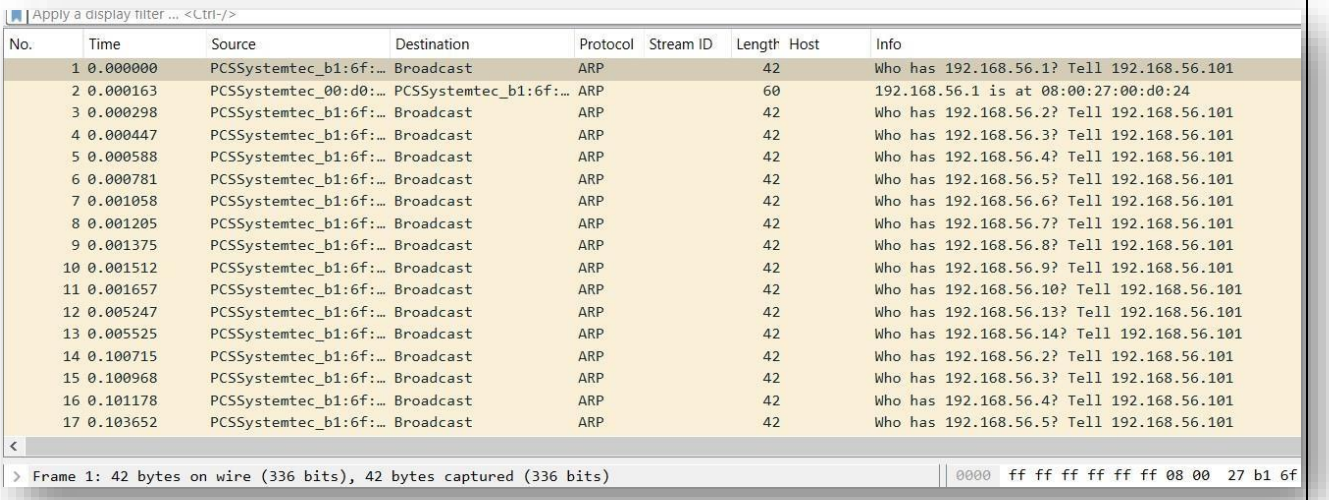
```
GET /buy.html HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727
LR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: wamojafadezy.com
Connection: Keep-Alive
Cookie: 7olnVuVTUHoG=10170004303462180033

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.)



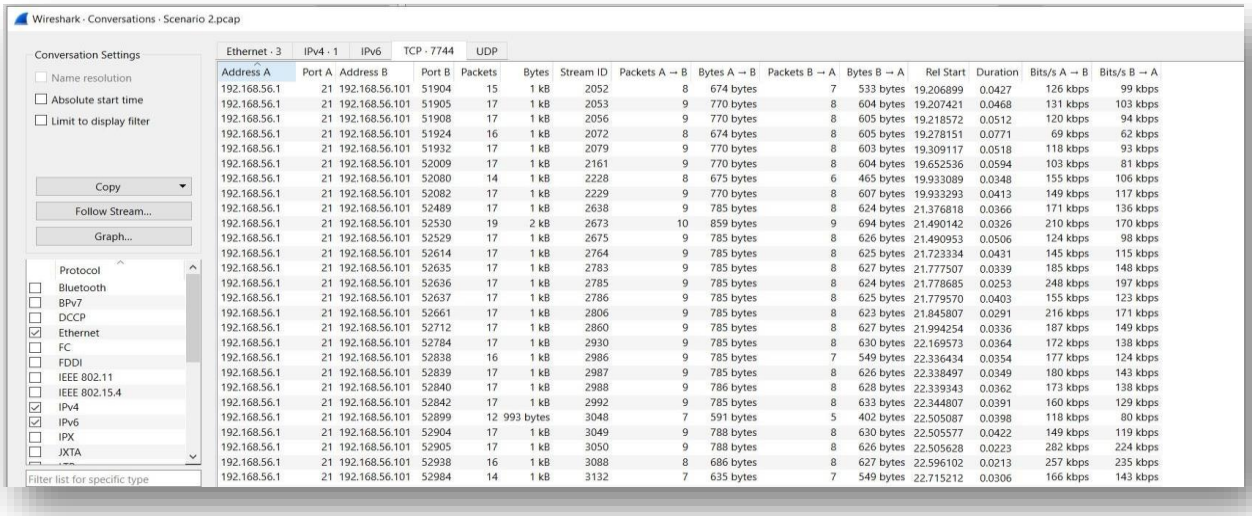
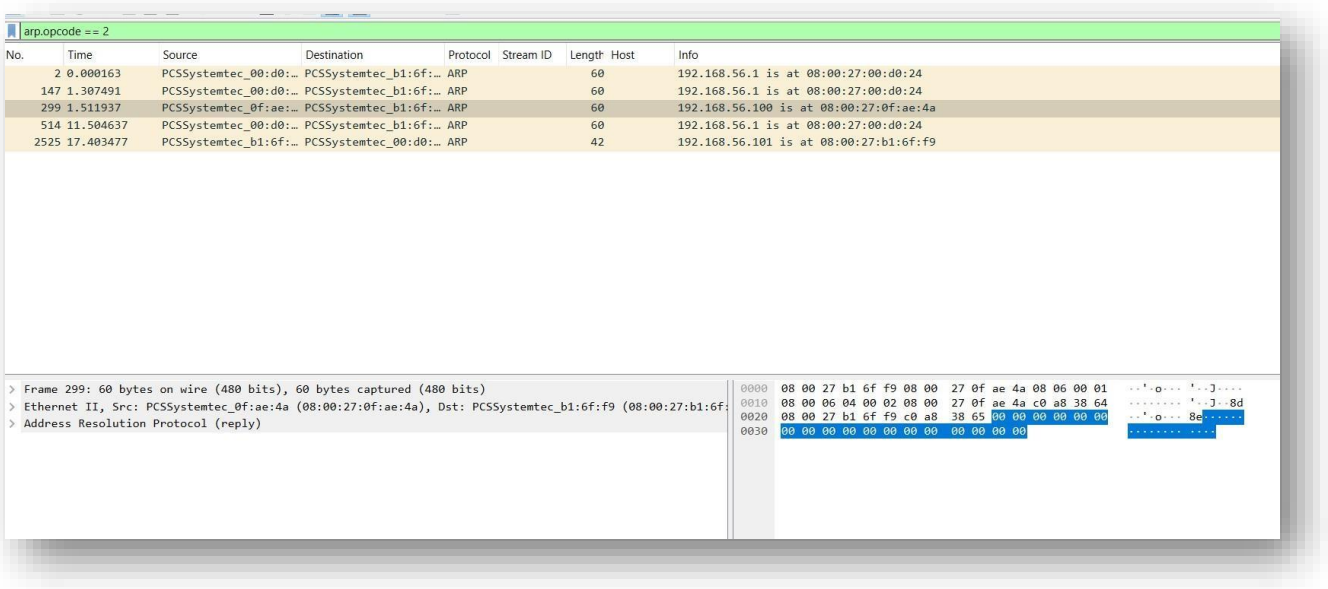


Figure 2: Huge number of TCP connections were identified

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



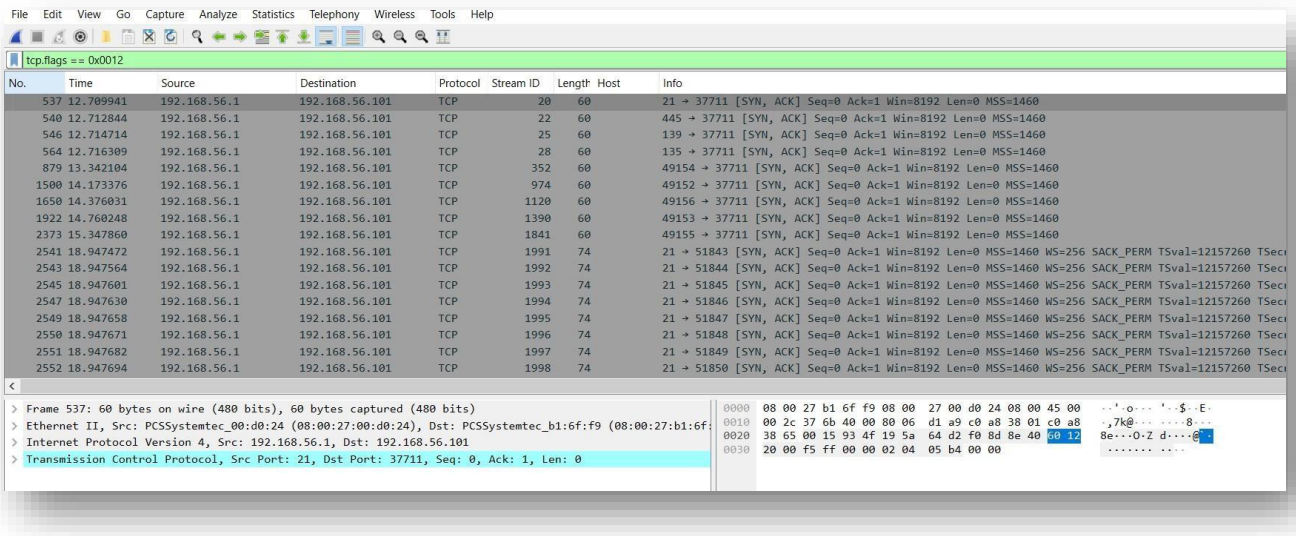


Figure 4: These ports were identified as open

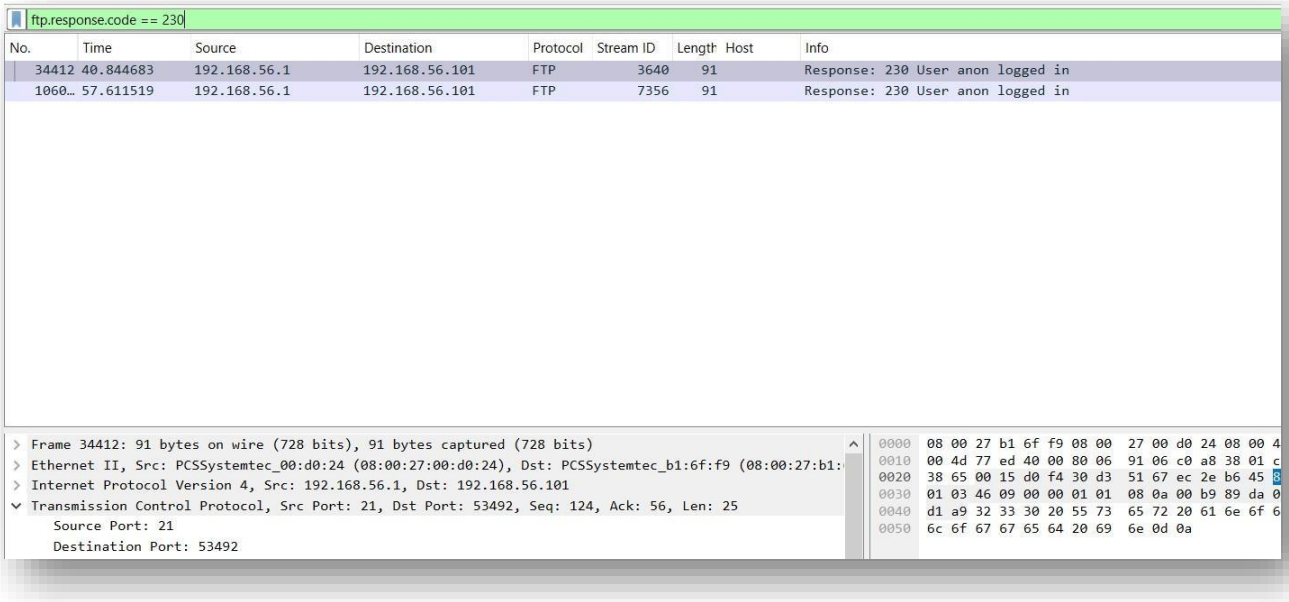


Figure 5.: The user's logged-in ports (the attacker used a brute force assault to obtain unauthorized access)

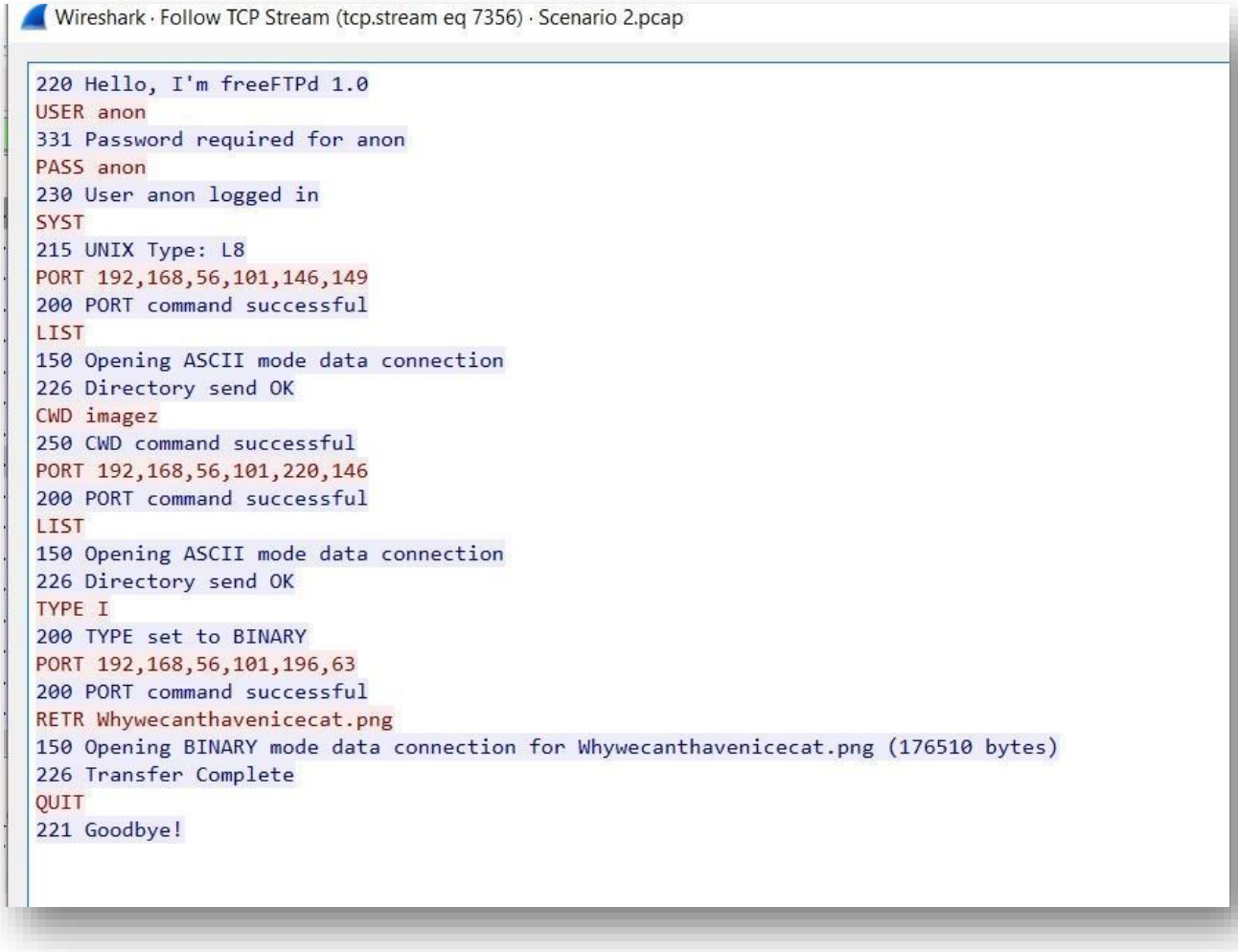


Figure 6: successfully logged in using the "anon/anon" credentials. After using the credentials to log in, the attacker searched the directories and downloaded an image.

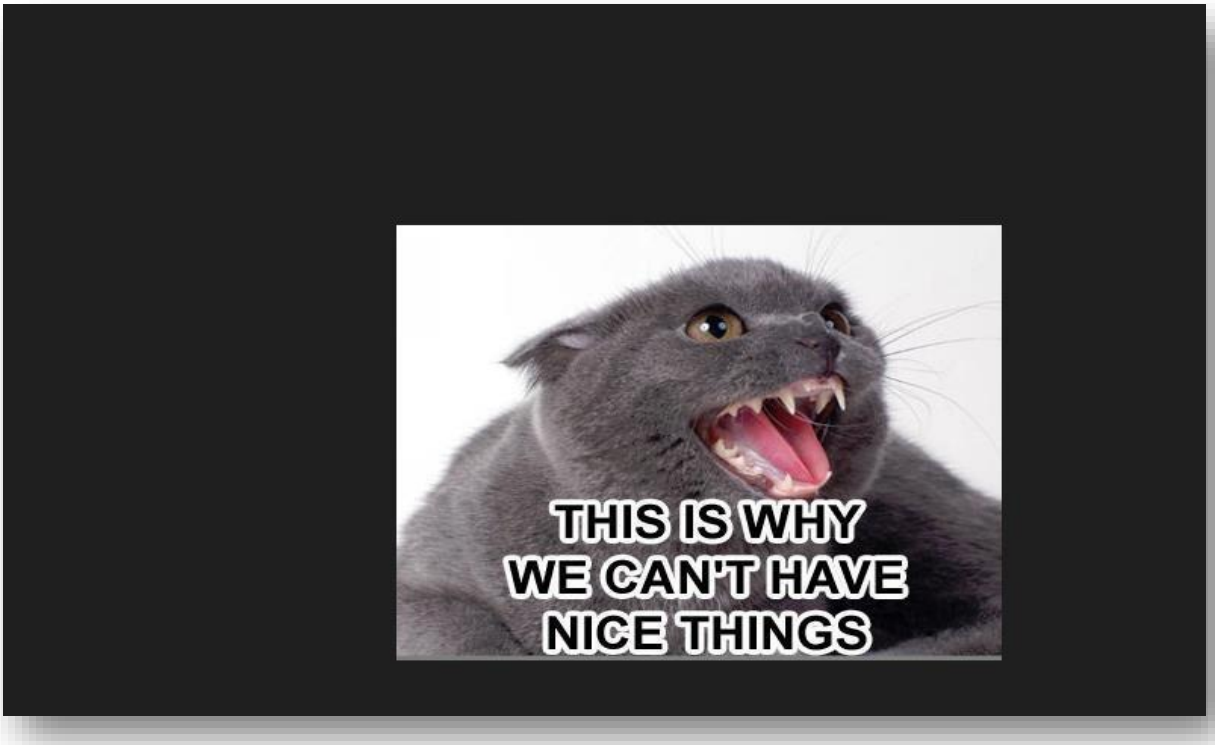


Figure 7: whywecanthavenicecat.png

When the encoded text is file is opened we got the above eveidemce 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
- Video Lectures - https://canvas.newhaven.edu/courses/26502/pages/watch-network-forensics-dns?module_item_id=2054452