# THIEF

## Overview

The goal of this project is to analyze network activity that has been recorded in a PCAP file, extract files that have been sent via HTTP, and then analyze those files in further detail using programs like Exiftool, Binwalk, and Steghide. VMware is used for virtualization and Wireshark is used for packet analysis in the project's Kali Linux implementation.

## Features

Analyze PCAP files to identify HTTP traffic.

Extract files transferred over HTTP.

Perform file analysis using Binwalk, Steghide, and Exiftool.

Utilize VMware for virtualization and sandboxing.

## Tools Used:

1)Wireshark

2)Binwalk

3)Steghide

4)VMware

## Usage

Install Dependencies: Ensure that Wireshark, Binwalk, Steghide, and VMware are installed on your system.

Clone Repository: Clone this repository to your local machine using the following command:

https://github.com/Avi191130/GROUP-15

Navigate to Project Directory:

Change directory to the project folder:

cd project

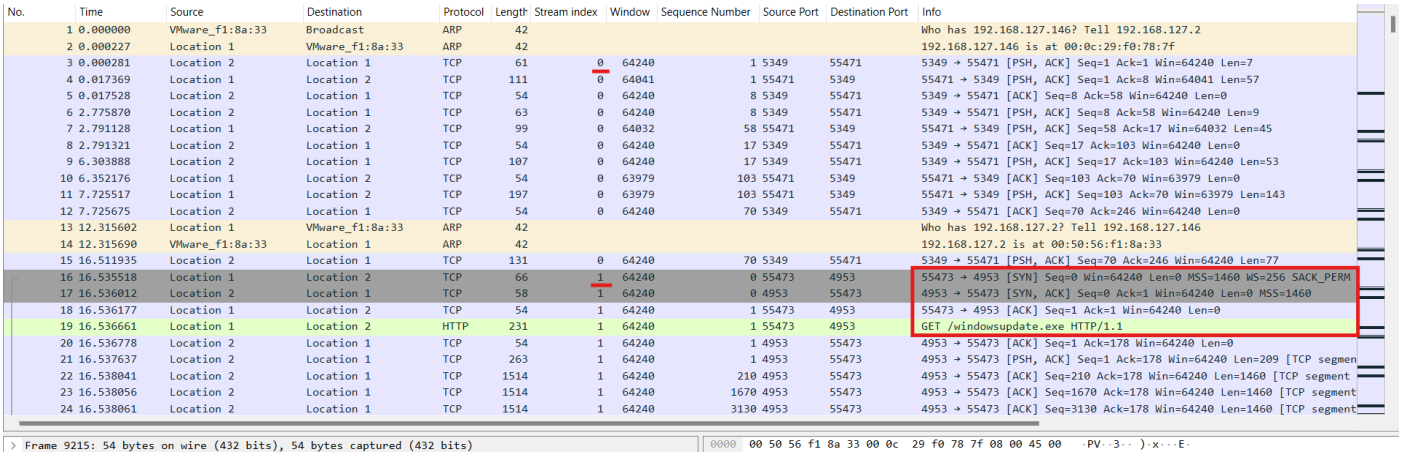
## Run Analysis:

Use Wireshark to open and analyze the PCAP file.

Identify HTTP traffic and extract relevant files.

Analyze extracted files using Binwalk, Steghide

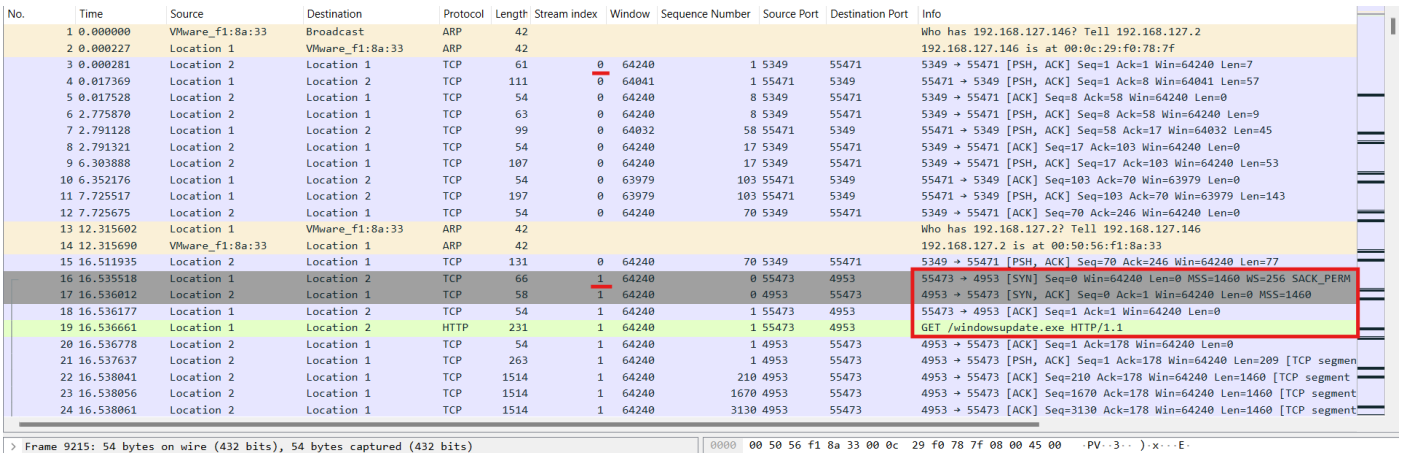
## Used Wireshark to open and analyze the PCAP file.



| No. | Time | Source | Destination | Protocol | Length | Stream index | Window | Sequence Number | Source Port | Destination Port | Info |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | VMware_f1:8a:33 | Broadcast | ARP | 42 | | | | | | Who has 192.168.127.146? Tell 192.168.127.2 |
| 2 | 0.000227 | Location 1 | VMware_f1:8a:33 | ARP | 42 | | | | | | 192.168.127.146 is at 00:0c:29:f0:78:7f |
| 3 | 0.000281 | Location 2 | Location 1 | TCP | 61 | 0 | 64240 | 1 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=7 |
| 4 | 0.017369 | Location 1 | Location 2 | TCP | 111 | 0 | 64041 | 1 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=1 Ack=8 Win=64041 Len=57 |
| 5 | 0.017528 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 8 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=8 Ack=58 Win=64240 Len=0 |
| 6 | 2.775870 | Location 2 | Location 1 | TCP | 63 | 0 | 64240 | 8 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=8 Ack=58 Win=64240 Len=9 |
| 7 | 2.791128 | Location 1 | Location 2 | TCP | 99 | 0 | 64032 | 58 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=58 Ack=17 Win=64032 Len=45 |
| 8 | 2.791321 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 17 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=17 Ack=103 Win=64240 Len=0 |
| 9 | 6.303888 | Location 2 | Location 1 | TCP | 107 | 0 | 64240 | 17 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=17 Ack=103 Win=64240 Len=53 |
| 10 | 6.352176 | Location 1 | Location 2 | TCP | 54 | 0 | 63979 | 103 | 55471 | 5349 | 55471 → 5349 [ACK] Seq=103 Ack=70 Win=63979 Len=0 |
| 11 | 7.725517 | Location 1 | Location 2 | TCP | 197 | 0 | 63979 | 103 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=103 Ack=70 Win=63979 Len=143 |
| 12 | 7.725675 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 70 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=70 Ack=246 Win=64240 Len=0 |
| 13 | 12.315602 | Location 1 | VMware_f1:8a:33 | ARP | 42 | | | | | | Who has 192.168.127.2? Tell 192.168.127.146 |
| 14 | 12.315690 | VMware_f1:8a:33 | Location 1 | ARP | 42 | | | | | | 192.168.127.2 is at 00:50:56:f1:8a:33 |
| 15 | 16.511935 | Location 2 | Location 1 | TCP | 131 | 0 | 64240 | 70 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=70 Ack=246 Win=64240 Len=77 |
| 16 | 16.535518 | Location 1 | Location 2 | TCP | 66 | 1 | 64240 | 0 | 55473 | 4953 | 55473 → 4953 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 17 | 16.536012 | Location 2 | Location 1 | TCP | 58 | 1 | 64240 | 0 | 4953 | 55473 | 4953 → 55473 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 18 | 16.536177 | Location 1 | Location 2 | TCP | 54 | 1 | 64240 | 1 | 55473 | 4953 | 55473 → 4953 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 19 | 16.536661 | Location 1 | Location 2 | HTTP | 231 | 1 | 64240 | 1 | 55473 | 4953 | GET /windowsupdate.exe HTTP/1.1 |
| 20 | 16.536778 | Location 2 | Location 1 | TCP | 54 | 1 | 64240 | 1 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=1 Ack=178 Win=64240 Len=0 |
| 21 | 16.537637 | Location 2 | Location 1 | TCP | 263 | 1 | 64240 | 1 | 4953 | 55473 | 4953 → 55473 [PSH, ACK] Seq=1 Ack=178 Win=64240 Len=209 [TCP segmen |
| 22 | 16.538041 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 210 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=210 Ack=178 Win=64240 Len=1460 [TCP segment |
| 23 | 16.538056 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 1670 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=1670 Ack=178 Win=64240 Len=1460 [TCP segment |
| 24 | 16.538061 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 3130 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=3130 Ack=178 Win=64240 Len=1460 [TCP segment |

```
> Frame 9215: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
0000  00 50 56 f1 8a 33 00 0c  29 f0 78 7f 08 00 45 00   ·PV··3·· )·x···E·
```

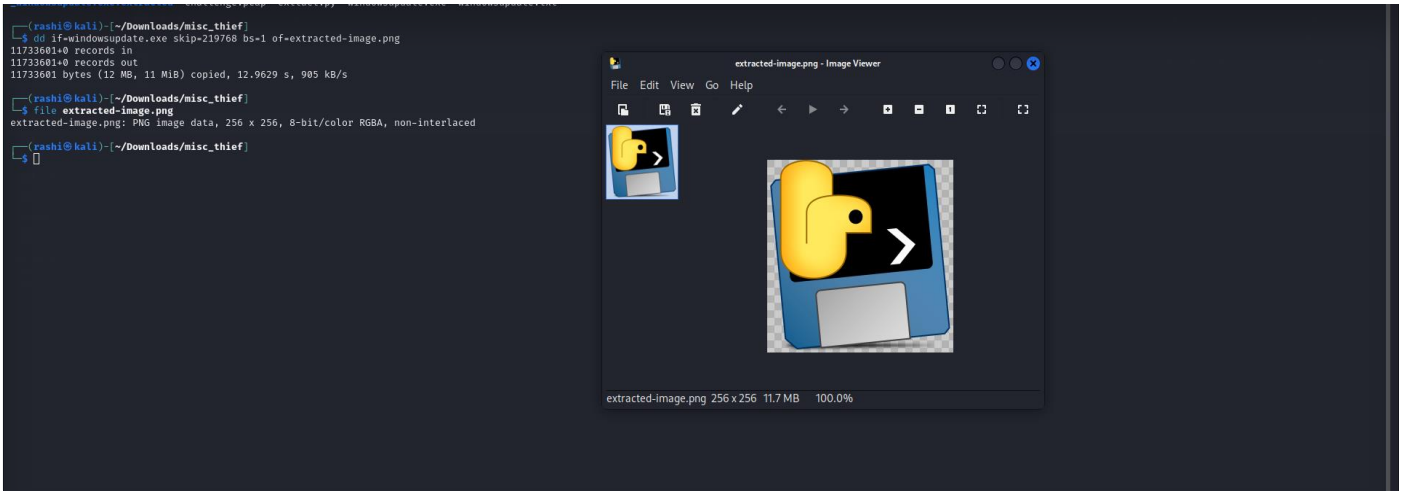
Identifing  HTTP traffic and extract relevant files.



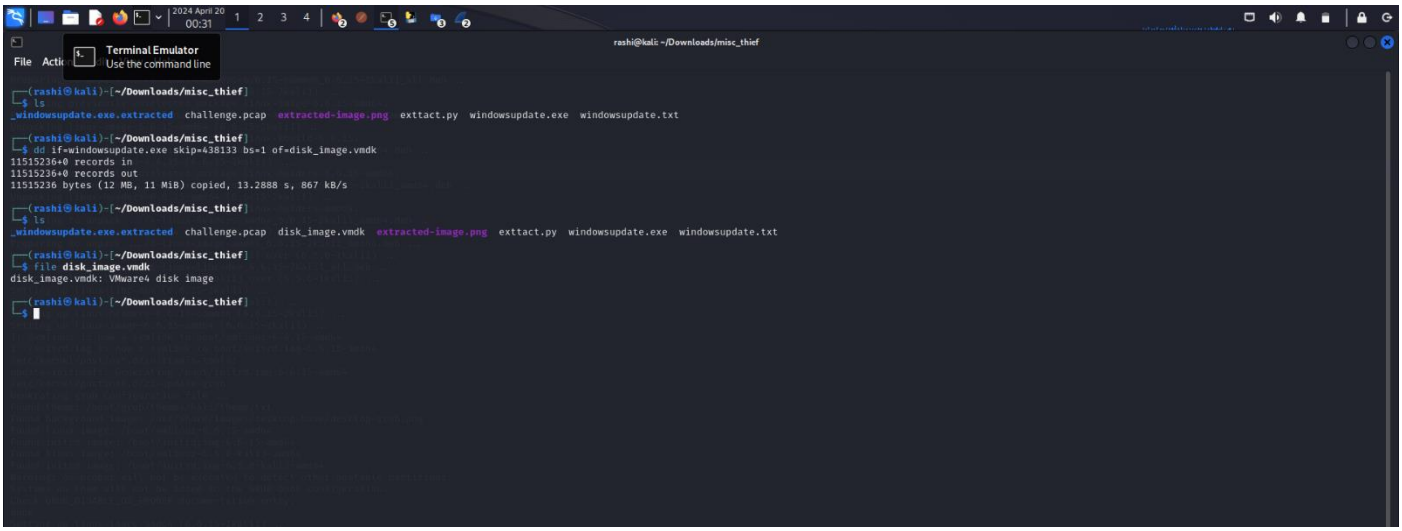
| No. | Time | Source | Destination | Protocol | Length | Stream index | Window | Sequence Number | Source Port | Destination Port | Info |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | VMware_f1:8a:33 | Broadcast | ARP | 42 | | | | | | Who has 192.168.127.146? Tell 192.168.127.2 |
| 2 | 0.000227 | Location 1 | VMware_f1:8a:33 | ARP | 42 | | | | | | 192.168.127.146 is at 00:0c:29:f0:78:7f |
| 3 | 0.000281 | Location 2 | Location 1 | TCP | 61 | 0 | 64240 | 1 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=7 |
| 4 | 0.017369 | Location 1 | Location 2 | TCP | 111 | 0 | 64041 | 1 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=1 Ack=8 Win=64041 Len=57 |
| 5 | 0.017528 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 8 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=8 Ack=58 Win=64240 Len=0 |
| 6 | 2.775870 | Location 2 | Location 1 | TCP | 63 | 0 | 64240 | 8 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=8 Ack=58 Win=64240 Len=9 |
| 7 | 2.791128 | Location 1 | Location 2 | TCP | 99 | 0 | 64032 | 58 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=58 Ack=17 Win=64032 Len=45 |
| 8 | 2.791321 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 17 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=17 Ack=103 Win=64240 Len=0 |
| 9 | 6.303888 | Location 2 | Location 1 | TCP | 107 | 0 | 64240 | 17 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=17 Ack=103 Win=64240 Len=53 |
| 10 | 6.352176 | Location 1 | Location 2 | TCP | 54 | 0 | 63979 | 103 | 55471 | 5349 | 55471 → 5349 [ACK] Seq=103 Ack=70 Win=63979 Len=0 |
| 11 | 7.725517 | Location 1 | Location 2 | TCP | 197 | 0 | 63979 | 103 | 55471 | 5349 | 55471 → 5349 [PSH, ACK] Seq=103 Ack=70 Win=63979 Len=143 |
| 12 | 7.725675 | Location 2 | Location 1 | TCP | 54 | 0 | 64240 | 70 | 5349 | 55471 | 5349 → 55471 [ACK] Seq=70 Ack=246 Win=64240 Len=0 |
| 13 | 12.315602 | Location 1 | VMware_f1:8a:33 | ARP | 42 | | | | | | Who has 192.168.127.2? Tell 192.168.127.146 |
| 14 | 12.315690 | VMware_f1:8a:33 | Location 1 | ARP | 42 | | | | | | 192.168.127.2 is at 00:50:56:f1:8a:33 |
| 15 | 16.511935 | Location 2 | Location 1 | TCP | 131 | 0 | 64240 | 70 | 5349 | 55471 | 5349 → 55471 [PSH, ACK] Seq=70 Ack=246 Win=64240 Len=77 |
| 16 | 16.535518 | Location 1 | Location 2 | TCP | 66 | 1 | 64240 | 0 | 55473 | 4953 | 55473 → 4953 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 17 | 16.536012 | Location 2 | Location 1 | TCP | 58 | 1 | 64240 | 0 | 4953 | 55473 | 4953 → 55473 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 18 | 16.536177 | Location 1 | Location 2 | TCP | 54 | 1 | 64240 | 1 | 55473 | 4953 | 55473 → 4953 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 19 | 16.536661 | Location 1 | Location 2 | HTTP | 231 | 1 | 64240 | 1 | 55473 | 4953 | GET /windowsupdate.exe HTTP/1.1 |
| 20 | 16.536778 | Location 2 | Location 1 | TCP | 54 | 1 | 64240 | 1 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=1 Ack=178 Win=64240 Len=0 |
| 21 | 16.537637 | Location 2 | Location 1 | TCP | 263 | 1 | 64240 | 1 | 4953 | 55473 | 4953 → 55473 [PSH, ACK] Seq=1 Ack=178 Win=64240 Len=209 [TCP segmen |
| 22 | 16.538041 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 210 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=210 Ack=178 Win=64240 Len=1460 [TCP segment |
| 23 | 16.538056 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 1670 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=1670 Ack=178 Win=64240 Len=1460 [TCP segment |
| 24 | 16.538061 | Location 2 | Location 1 | TCP | 1514 | 1 | 64240 | 3130 | 4953 | 55473 | 4953 → 55473 [ACK] Seq=3130 Ack=178 Win=64240 Len=1460 [TCP segment |

```
> Frame 9215: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
0000  00 50 56 f1 8a 33 00 0c  29 f0 78 7f 08 00 45 00   ·PV··3·· )·x···E·
```

Analyze extracted files using Binwalk, Steghide




If necessary, utilize VMware for virtualization and sandboxing of extracted files.




## Acknowledgments

we would especially want to thank the creators of vmware binwalk steghide exiftool and wireshark for their invaluable contributions to the open-source community thank the people or organizations whose efforts or contributions were included into the project