INT301 PROJECT REPORT

NETWORK MINER TOOL

Submitted By

Anaparthi Sai Dinesh

(Register No : 11905673)

Roll No:17

Section: KE022

Code:- INT301

Under the guidance of

Dr. Manjot Kaur

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Chapter-1

1.1 INTRODUCTION:

In today's fast-paced world, network security is of utmost importance. Organizations and individuals need to be vigilant about the security of their networks, as a single breach could result in a significant loss of sensitive information. Packet sniffing is one of the techniques used to monitor and analyse network traffic. Network Miner is a popular packet sniffing tool that is used to extract useful information from captured network traffic. In this project, we will use Network Miner to detect the operating system, sessions, and open ports through packet sniffing and investigate the network traffic**.**

1.1 Objective of the Project

The objective of this project is to demonstrate the use of Network Miner as a tool to detect the operating system, sessions, and open ports through packet sniffing. We aim to analyse the captured network traffic to identify any potential security threats and vulnerabilities.

Fig: 1.1 - Network Miner Tool

1.2 Description of the Project

In this project, we will use Network Miner to capture network traffic and analyse it to extract valuable information such as operating systems, sessions, and open ports. We will then investigate the network traffic to identify any potential security threats or vulnerabilities.

1.3 Scope of the Project

The scope of this project is to demonstrate the use of Network Miner in detecting the operating system, sessions, and open ports through packet sniffing. We will analyse the captured network traffic and investigate any potential security threats or vulnerabilities. The project does not include any remedial actions for identified vulnerabilities.

Chapter-2

2 System Description

2.1 Target System Description

The target system description for this project is a network that is accessible through a network interface card (NIC). We will use Network Miner to capture and analyse the network traffic and we can use Wireshark to collect the packets as well.

2.2 Assumptions:

1. The target network is accessible through a network interface card (NIC).

2. The user has the necessary permissions to capture and analyse network traffic.

3. The user is familiar with the basic concepts of network traffic analysis, including TCP/IP protocols, network topologies, and network security.

2.3 Dependencies:

1.NetworkMiner requires a computer running Windows, Linux, or macOS operating systems.

2.NetworkMiner requires a network interface card (NIC) to capture network traffic.

3.NetworkMiner depends on the accuracy and completeness of network traffic data for accurate analysis.

4.For advanced analysis and identification of security threats, Network Miner may need to be used in conjunction with other tools such as Wireshark or Snort.

2.4 Data Set Used in Support of Your Project

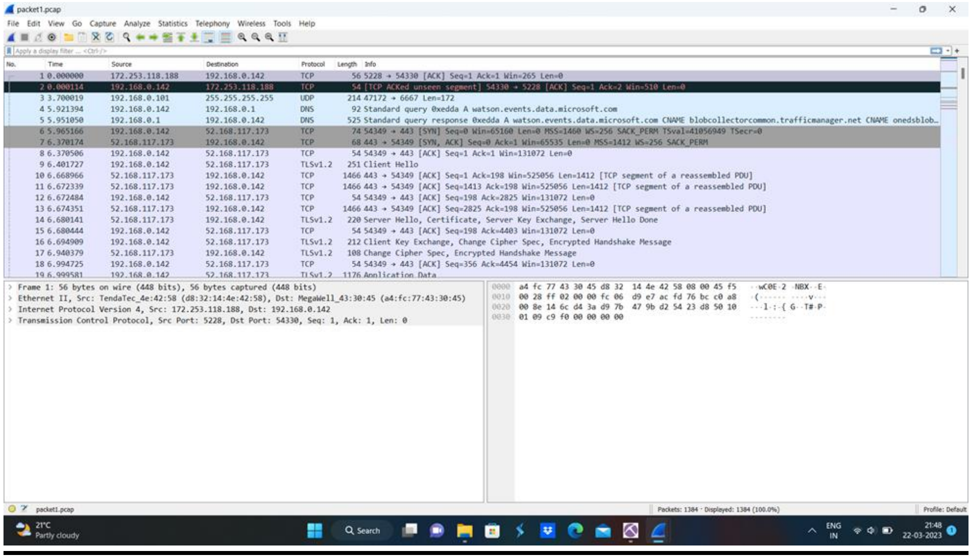
2.4.1 Wireshark:

For getting the open ports through packet sniffing and investigating the network traffic the best to tool use is Wireshark:

Wireshark is a network protocol analyzer or an application that captures packets from a network connection, such as from your computer to your home office or the internet. The packet is the name given to a discrete unit of data in a typical Ethernet network

Steps to use the Wireshark tool is:

1. Install Wireshark.
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark
5. Click on "Capture > Interfaces". A pop-up window will display.
6. You'll want to capture traffic that goes through your ethernet driver. Click on the Start button to capture traffic via this interface.
7. Visit the URL that you wanted to capture the traffic from.
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
9. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.


packet1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
packet1.pcap
Packets: 1384 · Displayed: 1384 (100.0%)
Profile: Default
21°C
Partly cloudy
Search
ENG
IN
21:48
22-03-2023

```
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    172.253.118.188  192.168.0.142    TCP         56 5228 → 54330 [ACK] Seq=1 Ack=1 Win=265 Len=0
    2 0.000114    192.168.0.142    172.253.118.188  TCP         54 [TCP ACKed unseen segment] 54330 → 5228 [ACK] Seq=1 Ack=2 Win=510 Len=0
    3 3.700019    192.168.0.101    255.255.255.255  UDP        214 47172 → 6667 Len=172
    4 5.921394    192.168.0.142    192.168.0.1      DNS         92 Standard query 0xedda A watson.events.data.microsoft.com
    5 5.951050    192.168.0.1      192.168.0.142    DNS        525 Standard query response 0xedda A watson.events.data.microsoft.com CNAME blobcollectorcommon.trafficmanager.net CNAME onedsblob…
    6 5.965166    192.168.0.142    52.168.117.173   TCP         74 54349 → 443 [SYN] Seq=0 Win=65160 Len=0 MSS=1460 WS=256 SACK_PERM TSval=41056949 TSecr=0
    7 6.370174    52.168.117.173   192.168.0.142    TCP         68 443 → 54349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM
    8 6.370506    192.168.0.142    52.168.117.173   TCP         54 54349 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
    9 6.401727    192.168.0.142    52.168.117.173   TLSv1.2    251 Client Hello
   10 6.668966    52.168.117.173   192.168.0.142    TCP       1466 443 → 54349 [ACK] Seq=1 Ack=198 Win=525056 Len=1412 [TCP segment of a reassembled PDU]
   11 6.672339    52.168.117.173   192.168.0.142    TCP       1466 443 → 54349 [ACK] Seq=1413 Ack=198 Win=525056 Len=1412 [TCP segment of a reassembled PDU]
   12 6.672484    192.168.0.142    52.168.117.173   TCP         54 54349 → 443 [ACK] Seq=198 Ack=2825 Win=131072 Len=0
   13 6.674351    52.168.117.173   192.168.0.142    TCP       1466 443 → 54349 [ACK] Seq=2825 Ack=198 Win=525056 Len=1412 [TCP segment of a reassembled PDU]
   14 6.680141    52.168.117.173   192.168.0.142    TLSv1.2    220 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   15 6.680444    192.168.0.142    52.168.117.173   TCP         54 54349 → 443 [ACK] Seq=198 Ack=4403 Win=131072 Len=0
   16 6.694909    192.168.0.142    52.168.117.173   TLSv1.2    212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   17 6.940379    52.168.117.173   192.168.0.142    TLSv1.2    108 Change Cipher Spec, Encrypted Handshake Message
   18 6.994725    192.168.0.142    52.168.117.173   TCP         54 54349 → 443 [ACK] Seq=356 Ack=4454 Win=131072 Len=0
   19 6.999581    192.168.0.142    52.168.117.173   TLSv1.2   1176 Application Data
```

```
> Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
> Ethernet II, Src: TendaTec_4e:42:58 (d8:32:14:4e:42:58), Dst: MegaWell_43:30:45 (a4:fc:77:43:30:45)
> Internet Protocol Version 4, Src: 172.253.118.188, Dst: 192.168.0.142
> Transmission Control Protocol, Src Port: 5228, Dst Port: 54330, Seq: 1, Ack: 1, Len: 0
```

```
0000  a4 fc 77 43 30 45 d8 32  14 4e 42 58 08 00 45 f5   ··wC0E·2 ·NBX··E·
0010  00 28 ff 02 00 00 fc 06  d9 e7 ac fd 76 bc c0 a8   ·(······ ····v···
0020  00 8e 14 6c d4 3a d9 7b  47 9b d2 54 23 d8 50 10   ···l·:·{ G··T#·P·
0030  01 09 c9 f0 00 00 00 00                            ········
```

Fig: 2.4 - Wireshark

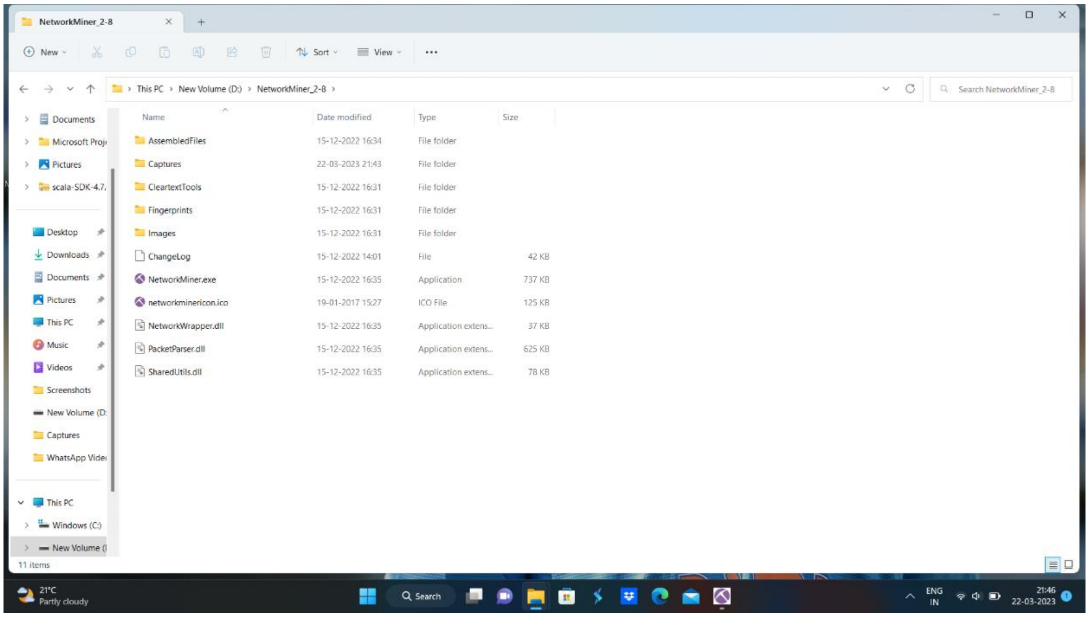
Chapter-3

3 Analysis Report

3.1 Download and install Network Miner on your computer.

3.1.1 Network Miner tool is a Network Forensic Analysis Tool (NFAT) for Windows. Network Miner tool can be used as a passive network sniffer/packet capturing tool to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.

3.1.2 Network monitoring tools are software applications designed to collect and analyse network traffic data to help network administrators identify and troubleshoot issues that may arise. They can be used to monitor network performance, detect security threats, and identify bottlenecks or other issues that may be impacting the performance of the network



Name	Date modified	Type	Size
AssembledFiles	15-12-2022 16:34	File folder	
Captures	22-03-2023 21:43	File folder	
CleartextTools	15-12-2022 16:31	File folder	
Fingerprints	15-12-2022 16:31	File folder	
Images	15-12-2022 16:31	File folder	
ChangeLog	15-12-2022 14:01	File	42 KB
NetworkMiner.exe	15-12-2022 16:35	Application	737 KB
networkminericon.ico	19-01-2017 15:27	ICO File	125 KB
NetworkWrapper.dll	15-12-2022 16:35	Application extens...	37 KB
PacketParser.dll	15-12-2022 16:35	Application extens...	625 KB
SharedUtils.dll	15-12-2022 16:35	Application extens...	78 KB

Fig: 3.1- Application

3.2 Start Network Miner and select the network interface card (NIC) that you want to use to capture network traffic.

3.2.1 For executing the network minor tool we have to run the app as administrator then we will get the exact info about our device, hosts ports etc…Then when we entered the application we have to select a network adaptor at the top of the page and then we have click on start the button

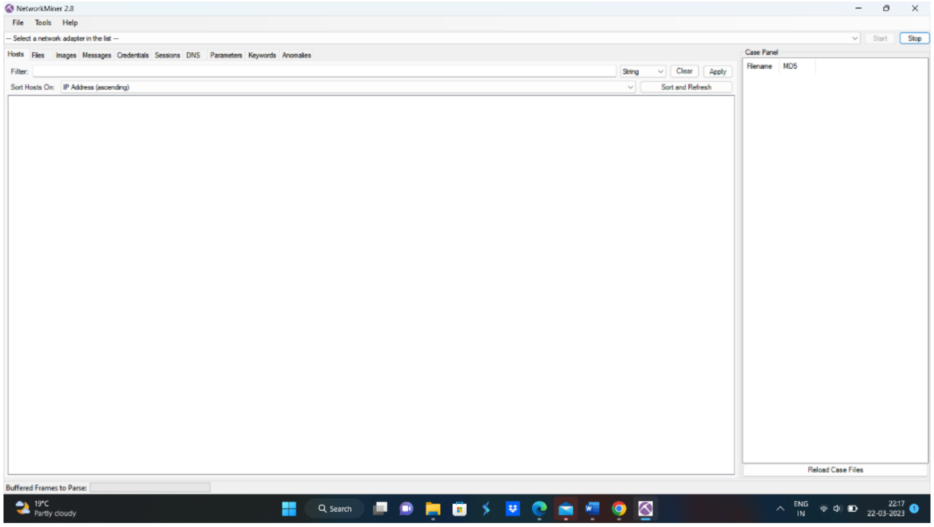


Fig: 3.2 - Network Miner Tool

3.3 Click on the "Start" button to start capturing network traffic

As from above **Fig: 3.2** we can see the option like select a network adaptor at top left side of the page and then we have to click on the start button to proceed.

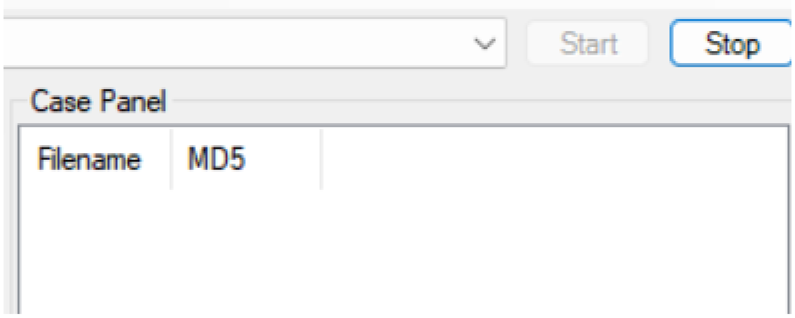
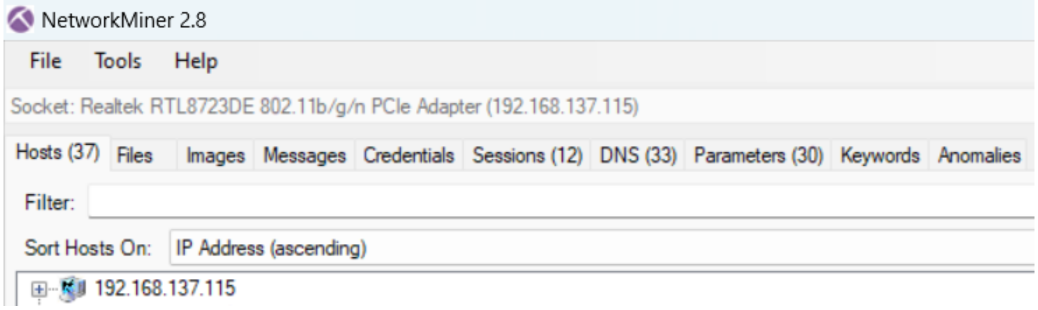


Fig: 3.3 - Start Button

3.3.1 After we selected our current active network adaptor we can find the current running host with the port numbers like in the below picture



Socket: Realtek RTL8723DE 802.11b/g/n PCIe Adapter (192.168.137.115)

Filter:

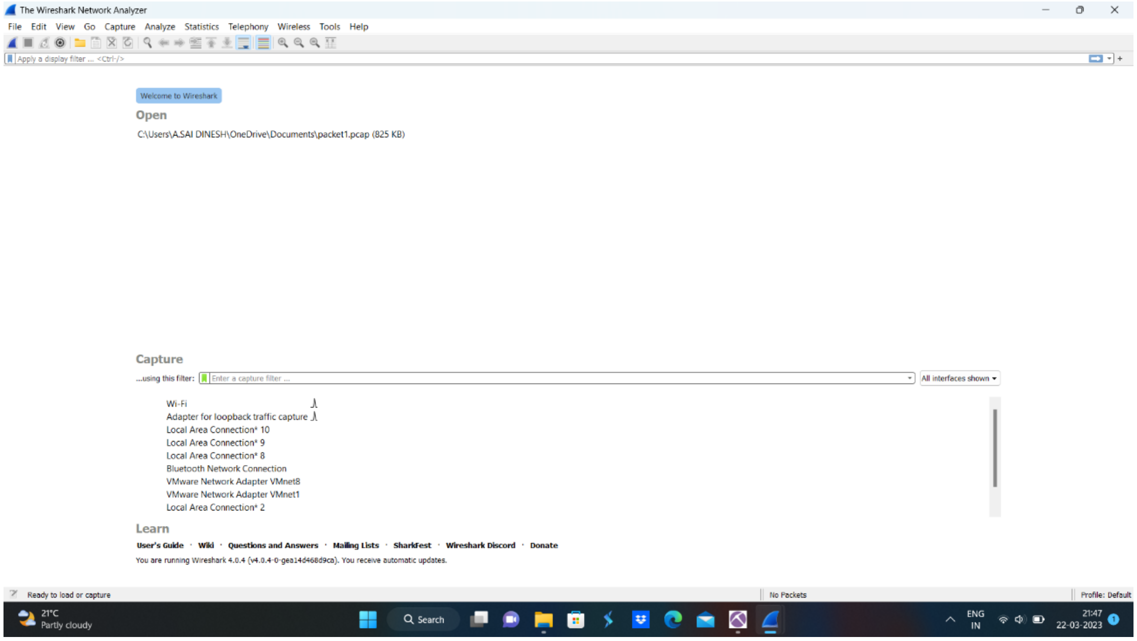
Sort Hosts On: IP Address (ascending)

192.168.137.115

Fig: 3.3.1 - Current Running Host

3.3.2 From **Fig:2.4,** After completion of storing the packets its shows here how many packets we saved for use in the network minor tool.

Packets are a fundamental concept in network monitoring tools, and they are used extensively in the analysis of network traffic. A packet is a unit of data that is transmitted over a network, and it typically consists of a header and a payload.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Search
ENG
IN

C:\Users\A.SAI DINESH\OneDrive\Documents\packet1.pcap (825 KB)

Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2

You are running Wireshark 4.0.4 (v4.0.4-0-gea14d468d9ca). You receive automatic updates.

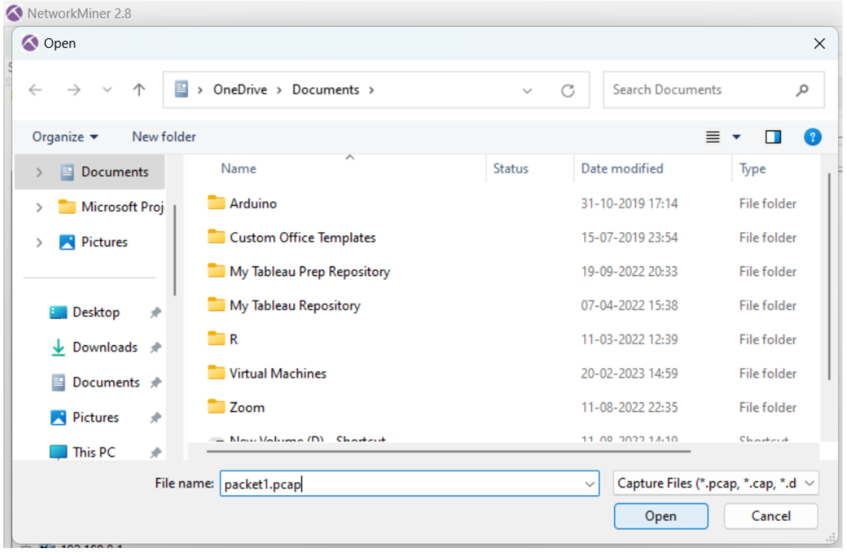
Ready to load or capture | No Packets | Profile: Default

21°C Partly cloudy

21:47 22-03-2023

Fig: 3.3.2 - Wireshark Packet Loader

3.3.3 After collecting packets we have to open the network minor tool and then click on the **file option** at the top and then **open** the packets that we saved from Wireshark to get the output for getting operating systems ,sessions, ports, parameters, etc.…



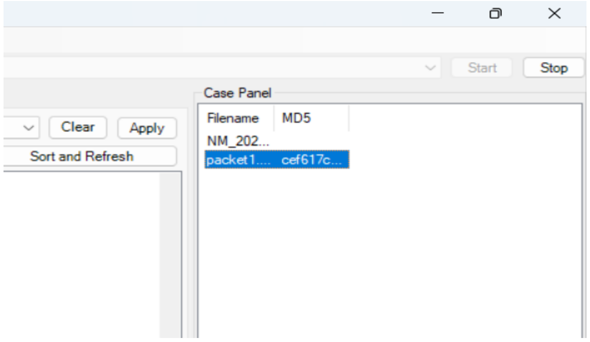
Name	Status	Date modified	Type
Arduino		31-10-2019 17:14	File folder
Custom Office Templates		15-07-2019 23:54	File folder
My Tableau Prep Repository		19-09-2022 20:33	File folder
My Tableau Repository		07-04-2022 15:38	File folder
R		11-03-2022 12:39	File folder
Virtual Machines		20-02-2023 14:59	File folder
Zoom		11-08-2022 22:35	File folder

File name: packet1.pcap

Capture Files (*.pcap, *.cap, *.d

Fig: 3.3.3 - Packet Loading

3.3.4 Here at the top right, we see the filename as packet1 so this is the packet we got from Wireshark software**.**



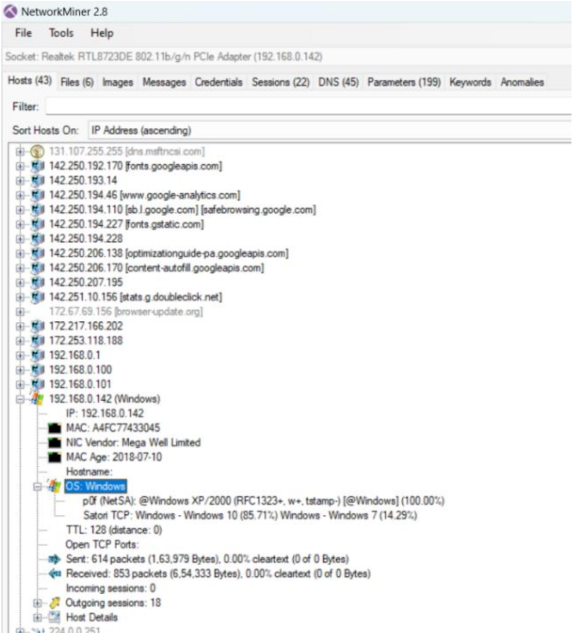
Filename	MD5
NM_202...	
packet1....	cef617c...

Fig: 3.3.4 - Packet

3.4 Once network traffic has been captured, you can view the extracted information on the "Hosts," "Sessions," tabs. These tabs provide information on the operating system, sessions, and open ports.

3.4.1 Hosts: When network traffic is captured and analysed using Network Miner Tool, the "Hosts" tab displays information about each host that is communicating on the network, including IP addresses, MAC addresses, and the operating system running on the host.

By analyzing the information in the "Hosts" tab, network administrators can gain insights into the devices that are communicating on the network and identify potential security threats or vulnerabilities, such as unauthorized devices or unusual network activity



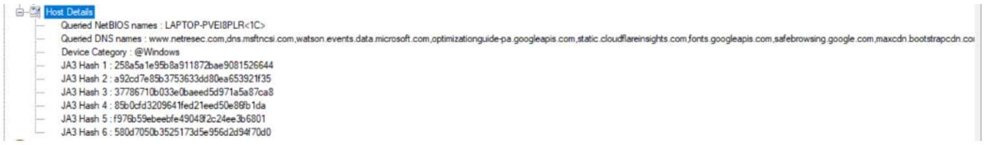
Socket: Realtek RTL8723DE 802.11b/g/n PCIe Adapter (192.168.0.142)

Filter:

Sort Hosts On: IP Address (ascending)

```
131.107.255.255 [dns.msftncsi.com]
142.250.192.170 [fonts.googleapis.com]
142.250.193.14
142.250.194.46 [www.google-analytics.com]
142.250.194.110 [sb.l.google.com] [safebrowsing.google.com]
142.250.194.227 [fonts.gstatic.com]
142.250.194.228
142.250.206.138 [optimizationguide-pa.googleapis.com]
142.250.206.170 [content-autofill.googleapis.com]
142.250.207.195
142.251.10.156 [stats.g.doubleclick.net]
172.67.69.156 [browser-update.org]
172.217.166.202
172.253.118.188
192.168.0.1
192.168.0.100
192.168.0.101
192.168.0.142 (Windows)
    IP: 192.168.0.142
    MAC: A4FC77433045
    NIC Vendor: Mega Well Limited
    MAC Age: 2018-07-10
    Hostname:
    OS: Windows
        p0f (NetSA): @Windows XP/2000 (RFC1323+, w+, tstamp-) [@Windows] (100.00%)
        Satori TCP: Windows - Windows 10 (85.71%) Windows - Windows 7 (14.29%)
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 614 packets (1,63,979 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 853 packets (6,54,333 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 18
    Host Details
224.0.0.251
```

Fig: 3.4.1- Ip add, Mac add, Hosts



```
Host Details
    Queried NetBIOS names : LAPTOP-PVEI8PLR<1C>
    Queried DNS names : www.netresec.com,dns.msftncsi.com,watson.events.data.microsoft.com,optimizationguide-pa.googleapis.com,static.cloudflareinsights.com,fonts.googleapis.com,safebrowsing.google.com,maxcdn.bootstrapcdn.co
    Device Category : @Windows
    JA3 Hash 1 : 258a5a1e95b8a911872bae9081526644
    JA3 Hash 2 : a92cd7e85b3753633dd80ea653921f35
    JA3 Hash 3 : 37786710b033e0baeed5d971a5a87ca8
    JA3 Hash 4 : 85b0cfd3209641fed21eed50e86fb1da
    JA3 Hash 5 : f976b59ebeebfe49048f2c24ee3b6801
    JA3 Hash 6 : 580d7050b3525173d5e956d2d94f70d0
```

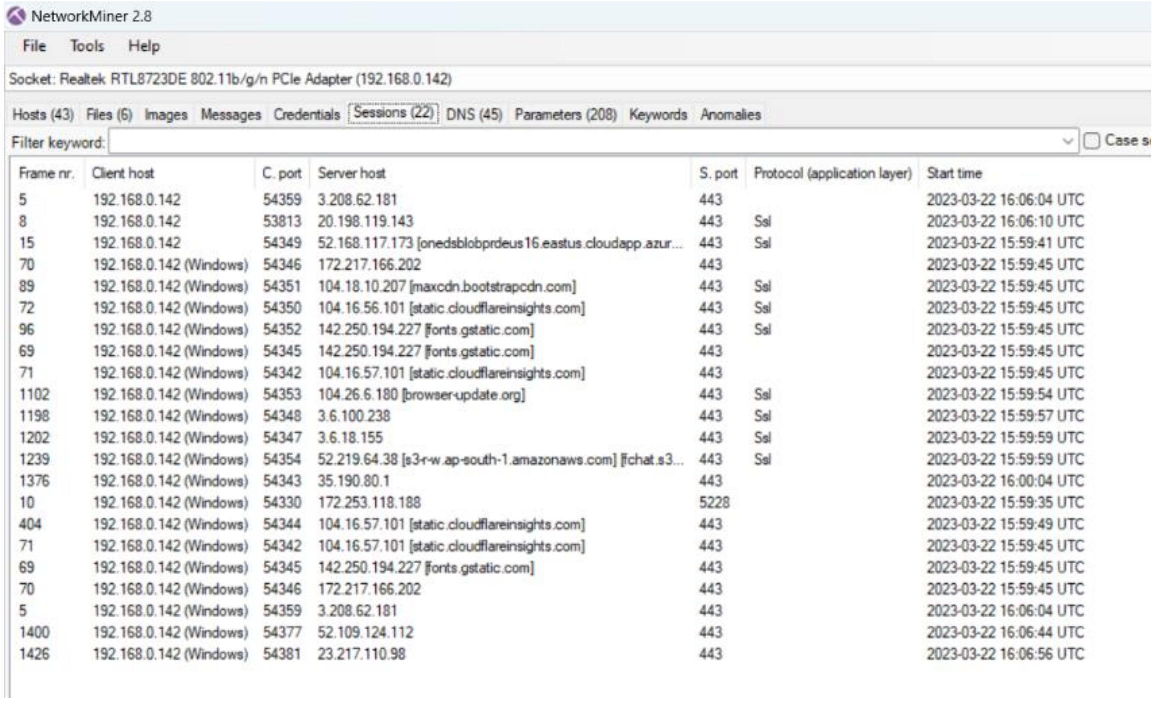
Fig: 3.4.1 Host Details

3.4.2 Sessions:

The "Sessions" tab in Network Miner tool displays information about network sessions that have been captured by the tool. A network session is a sequence of data exchanged between two endpoints over a network connection, such as a TCP connection.

The "Sessions" tab in the above Network Miner tool provides information about each network session that has been captured, such as the source and destination IP addresses and ports, the protocol used for the session, and the duration of the session.

By analysing the information in the "Sessions" tab, network administrators can gain insights into the types of sessions that are occurring on the network, and identify any potential security threats or vulnerabilities that may need to be addressed.



Socket: Realtek RTL8723DE 802.11b/g/n PCIe Adapter (192.168.0.142)

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
5	192.168.0.142	54359	3.208.62.181	443		2023-03-22 16:06:04 UTC
8	192.168.0.142	53813	20.198.119.143	443	Ssl	2023-03-22 16:06:10 UTC
15	192.168.0.142	54349	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	443	Ssl	2023-03-22 15:59:41 UTC
70	192.168.0.142 (Windows)	54346	172.217.166.202	443		2023-03-22 15:59:45 UTC
89	192.168.0.142 (Windows)	54351	104.18.10.207 [maxcdn.bootstrapcdn.com]	443	Ssl	2023-03-22 15:59:45 UTC
72	192.168.0.142 (Windows)	54350	104.16.56.101 [static.cloudflareinsights.com]	443	Ssl	2023-03-22 15:59:45 UTC
96	192.168.0.142 (Windows)	54352	142.250.194.227 [fonts.gstatic.com]	443	Ssl	2023-03-22 15:59:45 UTC
69	192.168.0.142 (Windows)	54345	142.250.194.227 [fonts.gstatic.com]	443		2023-03-22 15:59:45 UTC
71	192.168.0.142 (Windows)	54342	104.16.57.101 [static.cloudflareinsights.com]	443		2023-03-22 15:59:45 UTC
1102	192.168.0.142 (Windows)	54353	104.26.6.180 [browser-update.org]	443	Ssl	2023-03-22 15:59:54 UTC
1198	192.168.0.142 (Windows)	54348	3.6.100.238	443	Ssl	2023-03-22 15:59:57 UTC
1202	192.168.0.142 (Windows)	54347	3.6.18.155	443	Ssl	2023-03-22 15:59:59 UTC
1239	192.168.0.142 (Windows)	54354	52.219.64.38 [s3-r-w.ap-south-1.amazonaws.com] [fchat.s3...	443	Ssl	2023-03-22 15:59:59 UTC
1376	192.168.0.142 (Windows)	54343	35.190.80.1	443		2023-03-22 16:00:04 UTC
10	192.168.0.142 (Windows)	54330	172.253.118.188	5228		2023-03-22 15:59:35 UTC
404	192.168.0.142 (Windows)	54344	104.16.57.101 [static.cloudflareinsights.com]	443		2023-03-22 15:59:49 UTC
71	192.168.0.142 (Windows)	54342	104.16.57.101 [static.cloudflareinsights.com]	443		2023-03-22 15:59:45 UTC
69	192.168.0.142 (Windows)	54345	142.250.194.227 [fonts.gstatic.com]	443		2023-03-22 15:59:45 UTC
70	192.168.0.142 (Windows)	54346	172.217.166.202	443		2023-03-22 15:59:45 UTC
5	192.168.0.142 (Windows)	54359	3.208.62.181	443		2023-03-22 16:06:04 UTC
1400	192.168.0.142 (Windows)	54377	52.109.124.112	443		2023-03-22 16:06:44 UTC
1426	192.168.0.142 (Windows)	54381	23.217.110.98	443		2023-03-22 16:06:56 UTC

Fig: 3.4.2 - Sessions

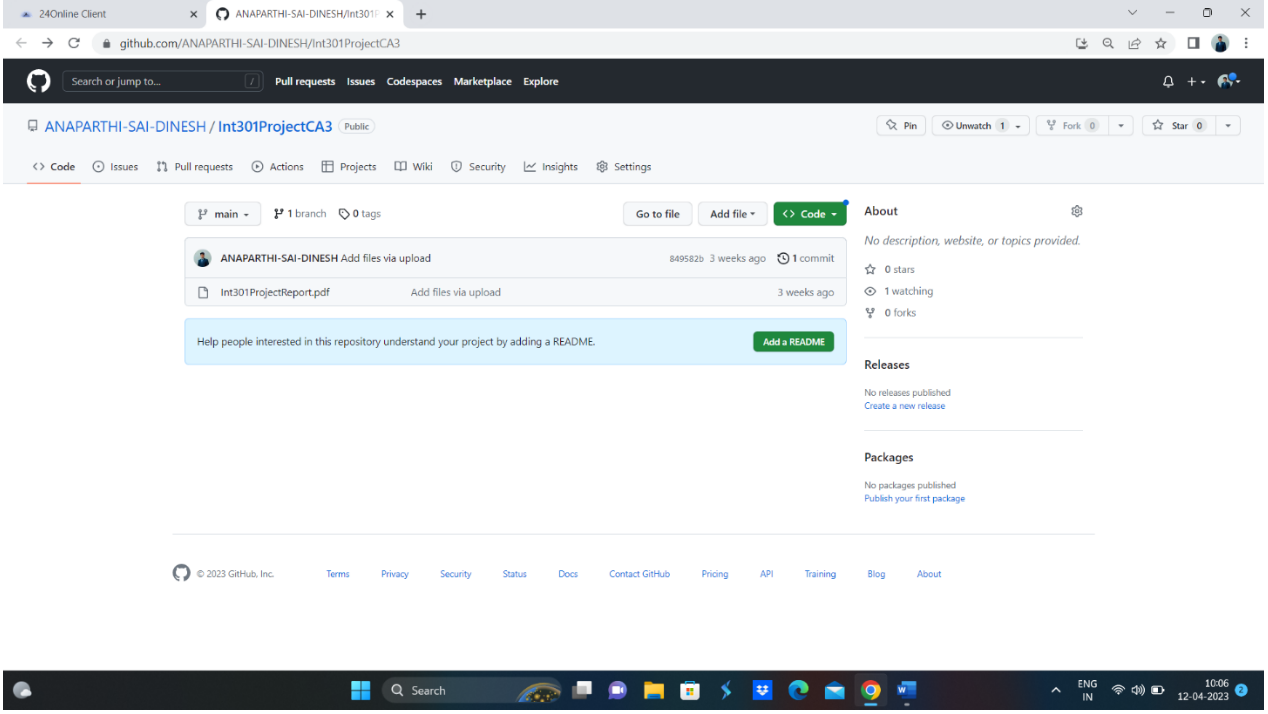
Chapter-4

4 Reference/Bibliography:

- NetworkMinerTool:**https://www.netresec.com/index.ashx?page=NetworkMiner**

- Wireshark: **https://www.wireshark.org/download.html**

- **4.1** GitHub: **https://github.com/ANAPARTHI-SAI-DINESH/Int301ProjectCA3**



github.com/ANAPARTHI-SAI-DINESH/Int301ProjectCA3

ANAPARTHI-SAI-DINESH / Int301ProjectCA3 Public

main · 1 branch · 0 tags

ANAPARTHI-SAI-DINESH Add files via upload 849582b 3 weeks ago 1 commit

Int301ProjectReport.pdf Add files via upload 3 weeks ago

Help people interested in this repository understand your project by adding a README.

About

No description, website, or topics provided.

0 stars

1 watching

0 forks

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

© 2023 GitHub, Inc.

Fig: 4.1 - GitHub