Project report

INT301: Open Source Technologies

Name: Anaparthi Sai Dinesh

Roll No: 17

Section: RKE022

Git link: https://github.com/ANAPARTHI-SAI-DINESH/Int301ProjectCA3

Topic:

[Q(28)] Implement a network miner tool to detect the operating system, sessions, and open ports through packet sniffing and investigate the network traffic.

Ans) For implementing this question,

We have to discuss Network minor tool:

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. wit,hout putting any traffic on the network.

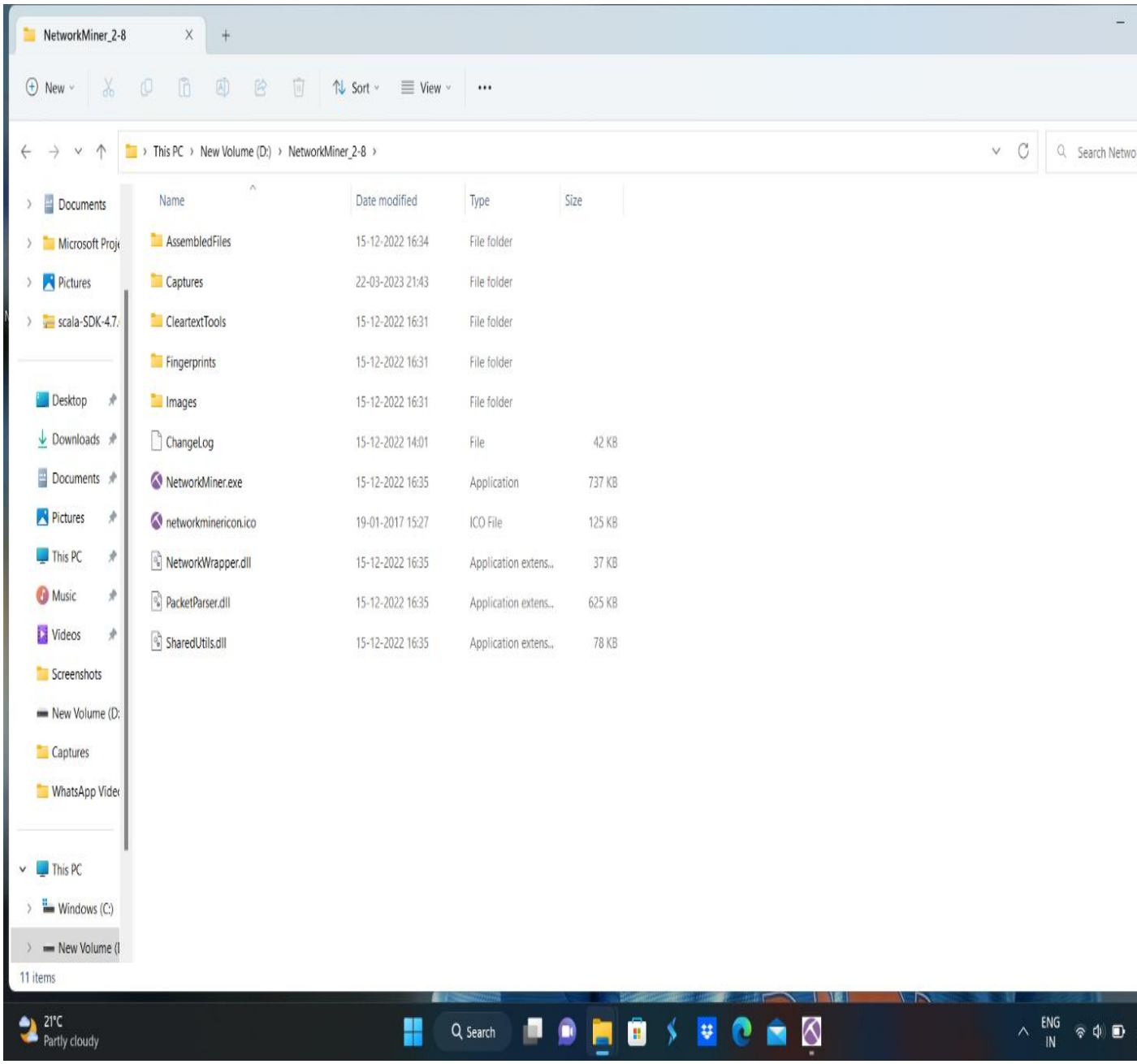
Network monitoring tools are software applications designed to collect and analyze network traffic data to help network administrators identify and troubleshoot issues that may arise. They can be used to monitor network performance, detect security threats, and identify bottlenecks or other issues that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

The secondary thing we have to know about packet sniffing:

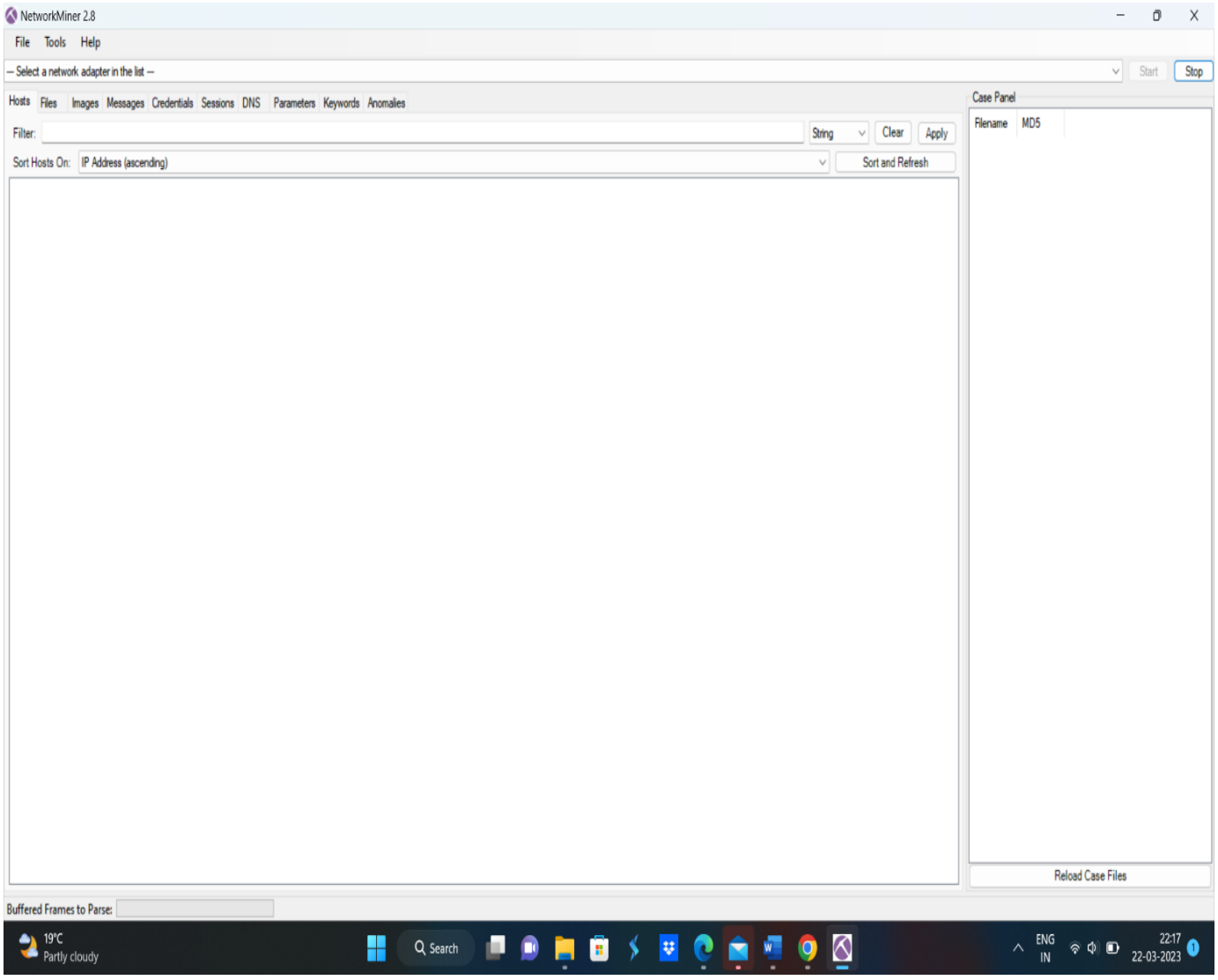
Packet sniffing involves capturing and analyzing network traffic to gain insights into the network. To implement a network miner tool to detect the operating system, sessions, and open ports

These tools capture and analyze packets of data as they pass through the network, providing detailed information about network traffic and helping to identify issues such as network congestion, security threats, or application performance problems.

So now we will download this network minor tool to detect the operating system, sessions, and open ports through packet sniffing and investigate the network traffic



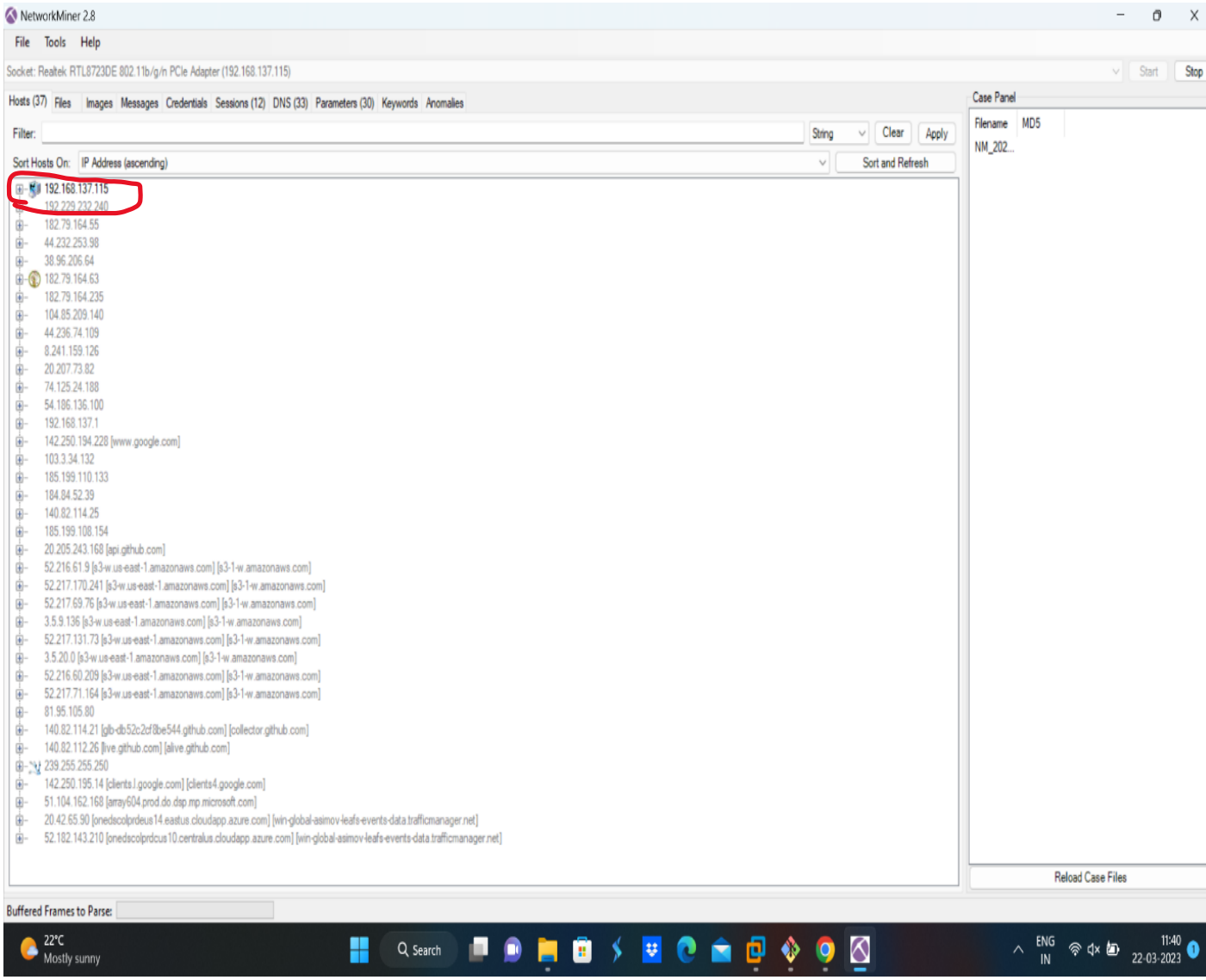
This is what the network minor tool looks like:



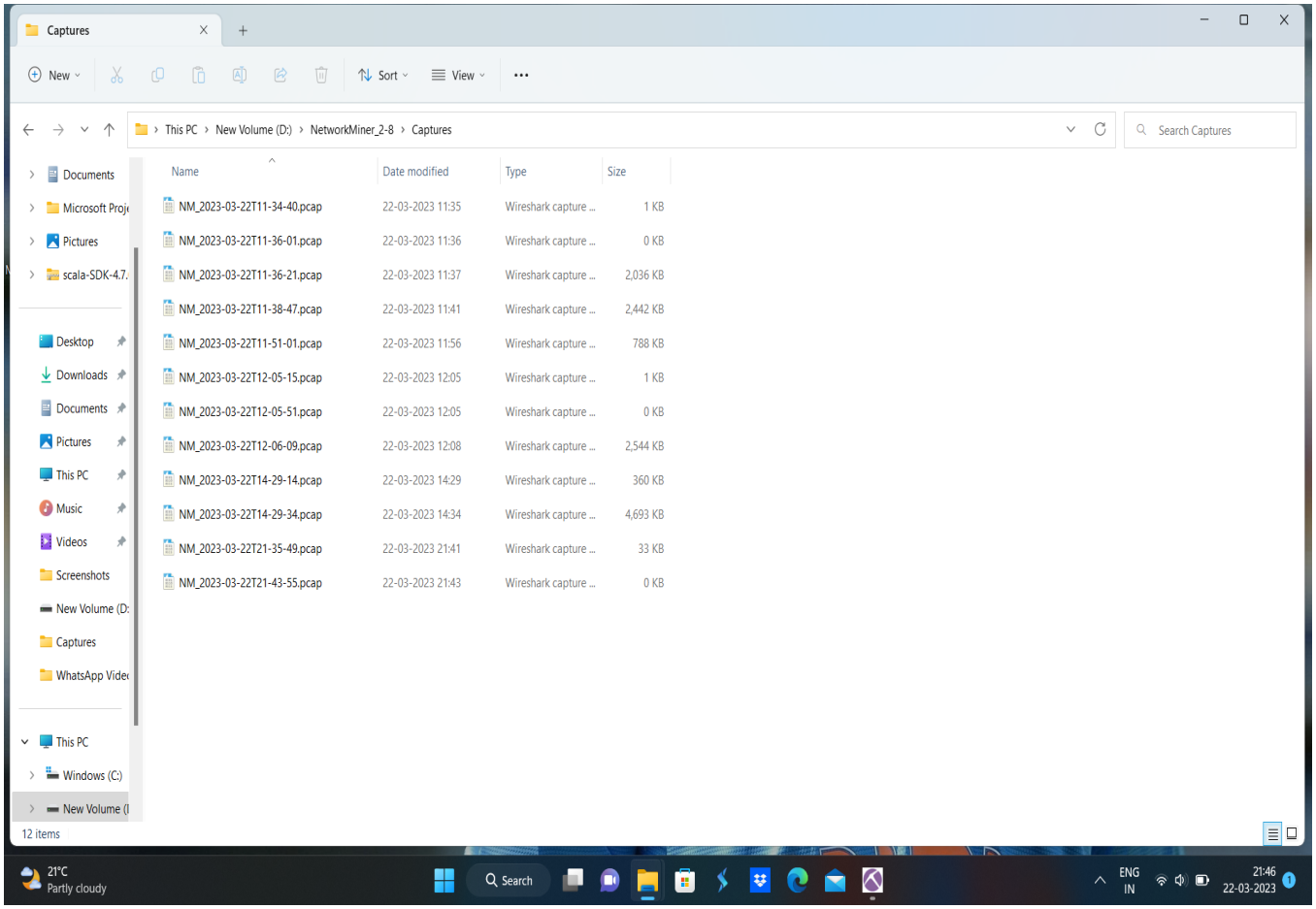
For executing the network minor tool we have to run the app as administrator then we will get the exact info about our device, hosts ports etc…

Then when we entered the application we have select a network adaptor at the top of the page and then we have click on start the button

So that we can find the current running host with the port numbers like in the below picture



By doing like that we will get the packets to collect the info that what was running in our device at that particular time



We can save our packets in .pcap format.

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.

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

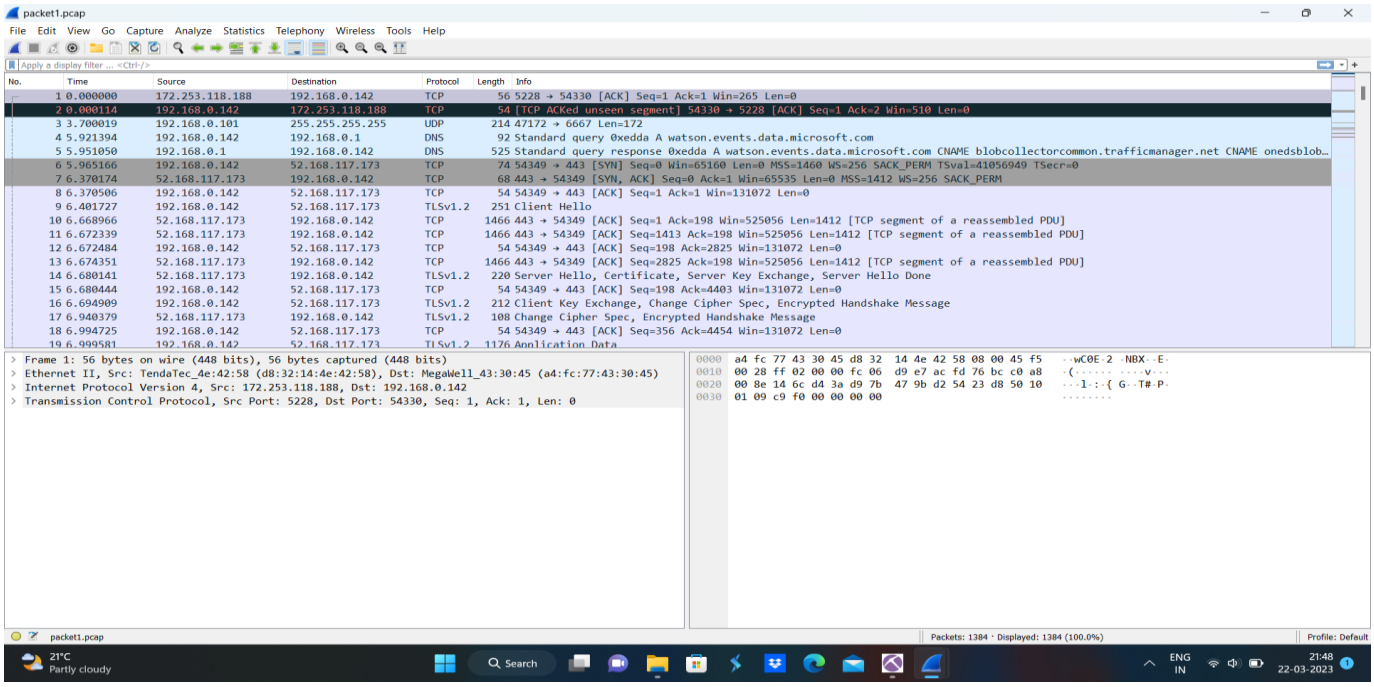
Wireshark is a network protocol analyzer or an application that captures packets from a network connection, such as from your computer to your home office or the internet. PThe packetis the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world.

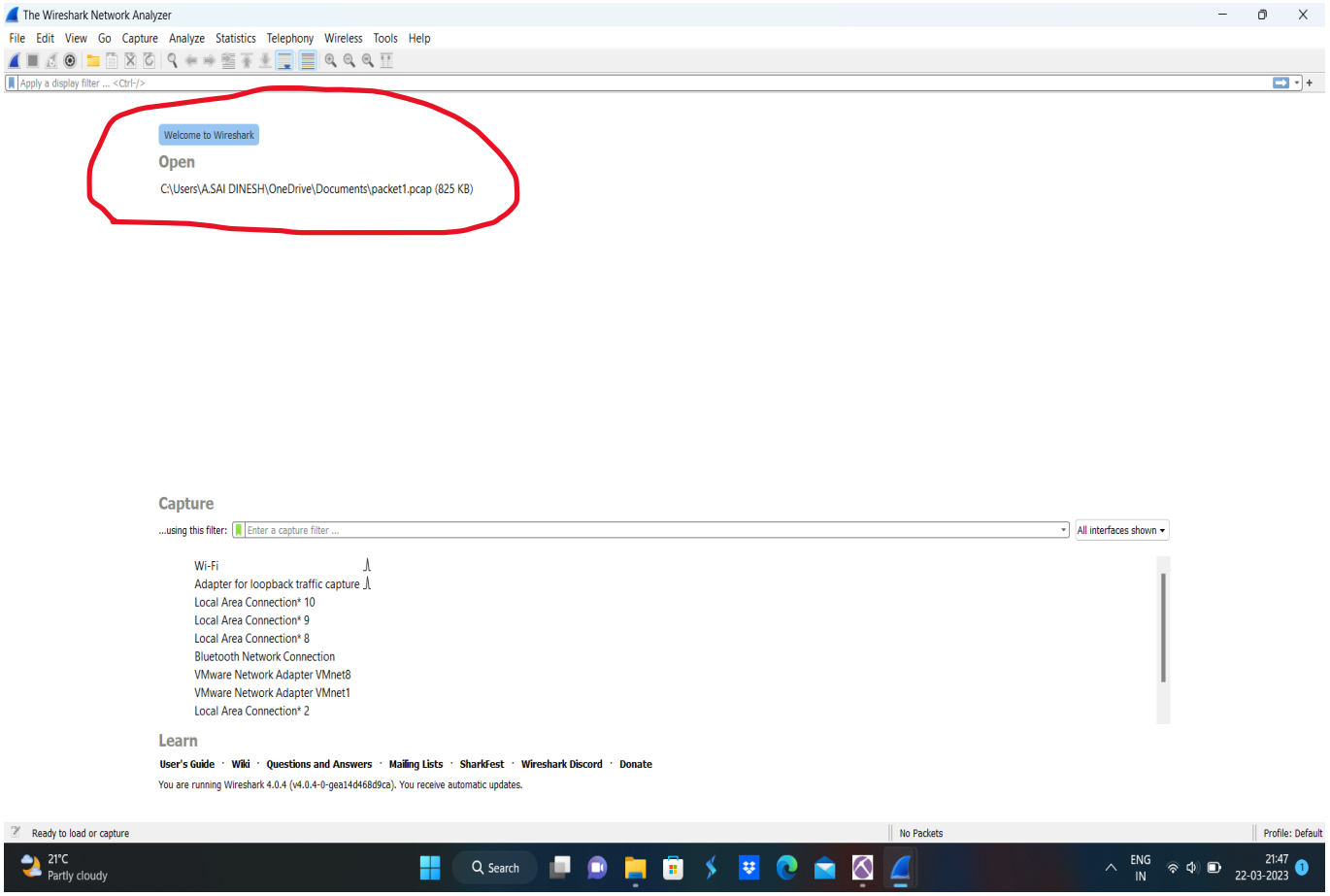
Steps to use the wireshark tool is:

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.

This is what wireshark looks like when we starts capturing the packets information:



After completion of storing the packets its shows here how many packets we saved for using in the network minor tool.

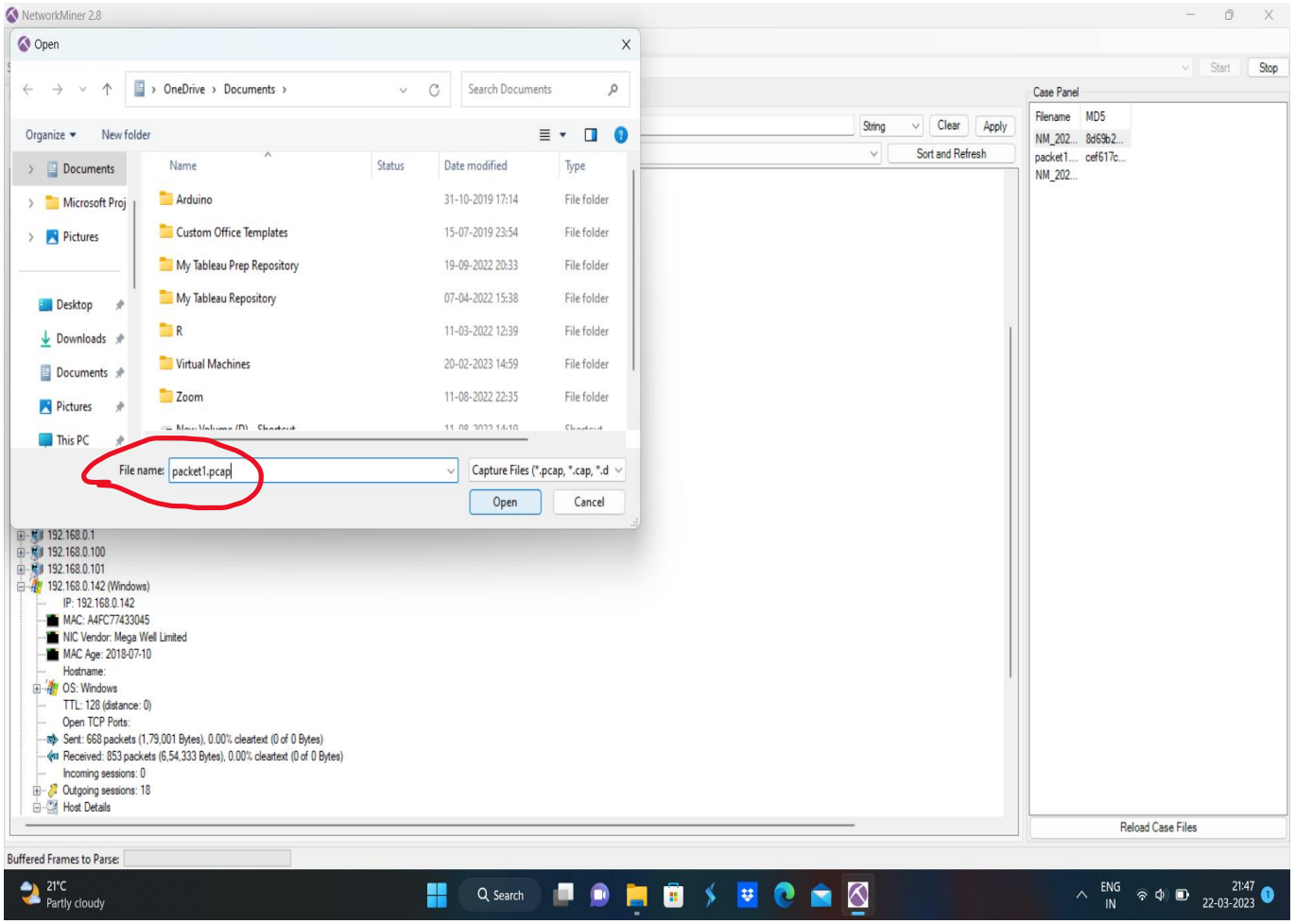


1. Packet capture: Wireshark allows network administrators to capture and analyze network packets in real time, providing a detailed view of network traffic. It can capture packets from a variety of sources, including wired and wireless networks, and can be used to capture packets on specific ports or with specific protocols.

2. Protocol analysis: Wireshark provides detailed protocol analysis for a wide range of network protocols, including TCP/IP, HTTP, DNS, and many others. This makes it a powerful tool for identifying issues with specific protocols, such as slow response times or dropped packets.

3. Troubleshooting: Wireshark can be used to troubleshoot network issues by providing a detailed view of network traffic. For example, if a network is experiencing slow response times, Wireshark can be used to identify the source of the issue, such as a server that is overloaded or a network device that is misconfigured.

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....

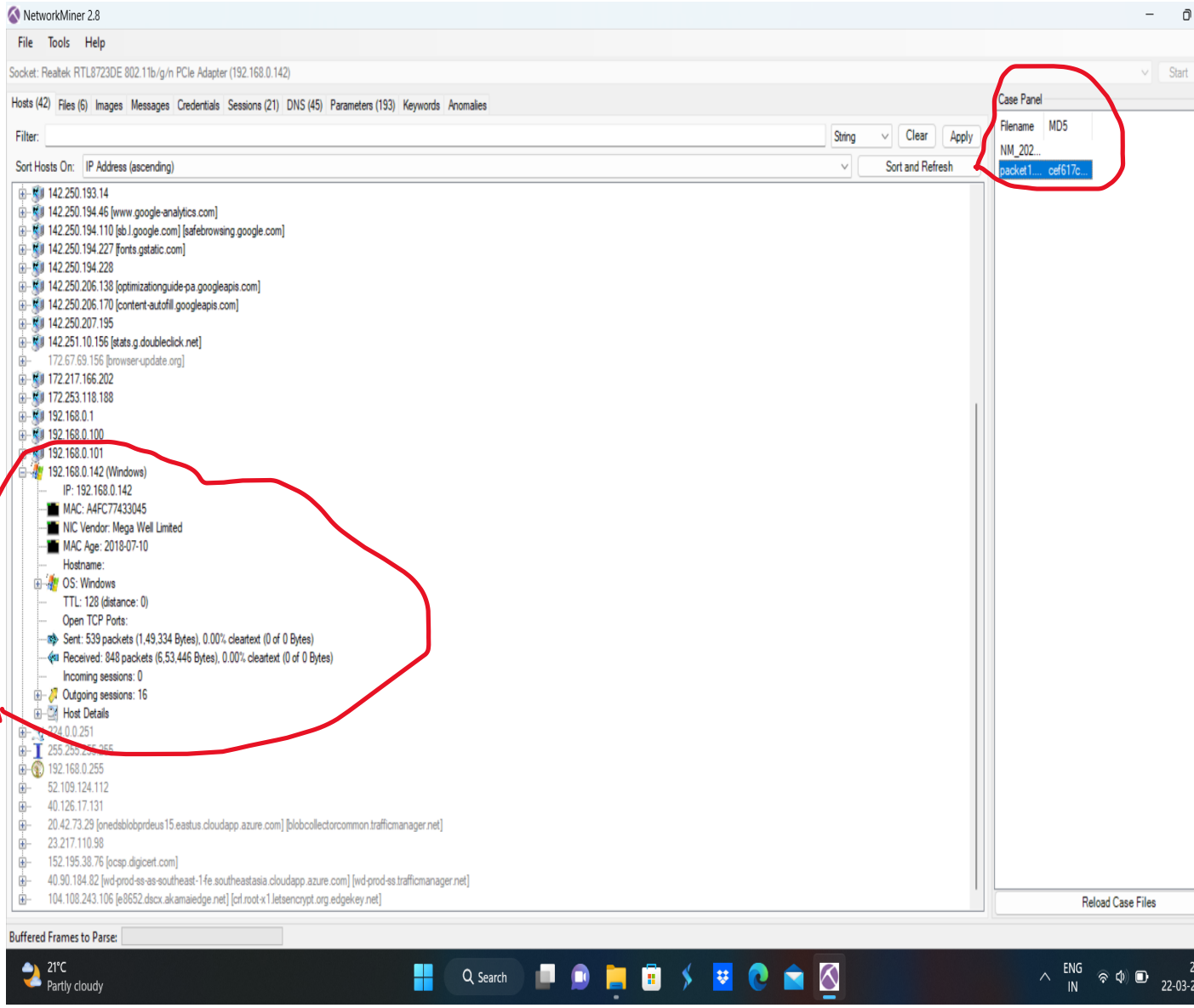


As Network monitoring tools are software applications designed to collect and analyze network traffic data to help network administrators identify and troubleshoot issues that may arise. They can be used to monitor network performance, detect security threats, and identify bottlenecks or other issues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

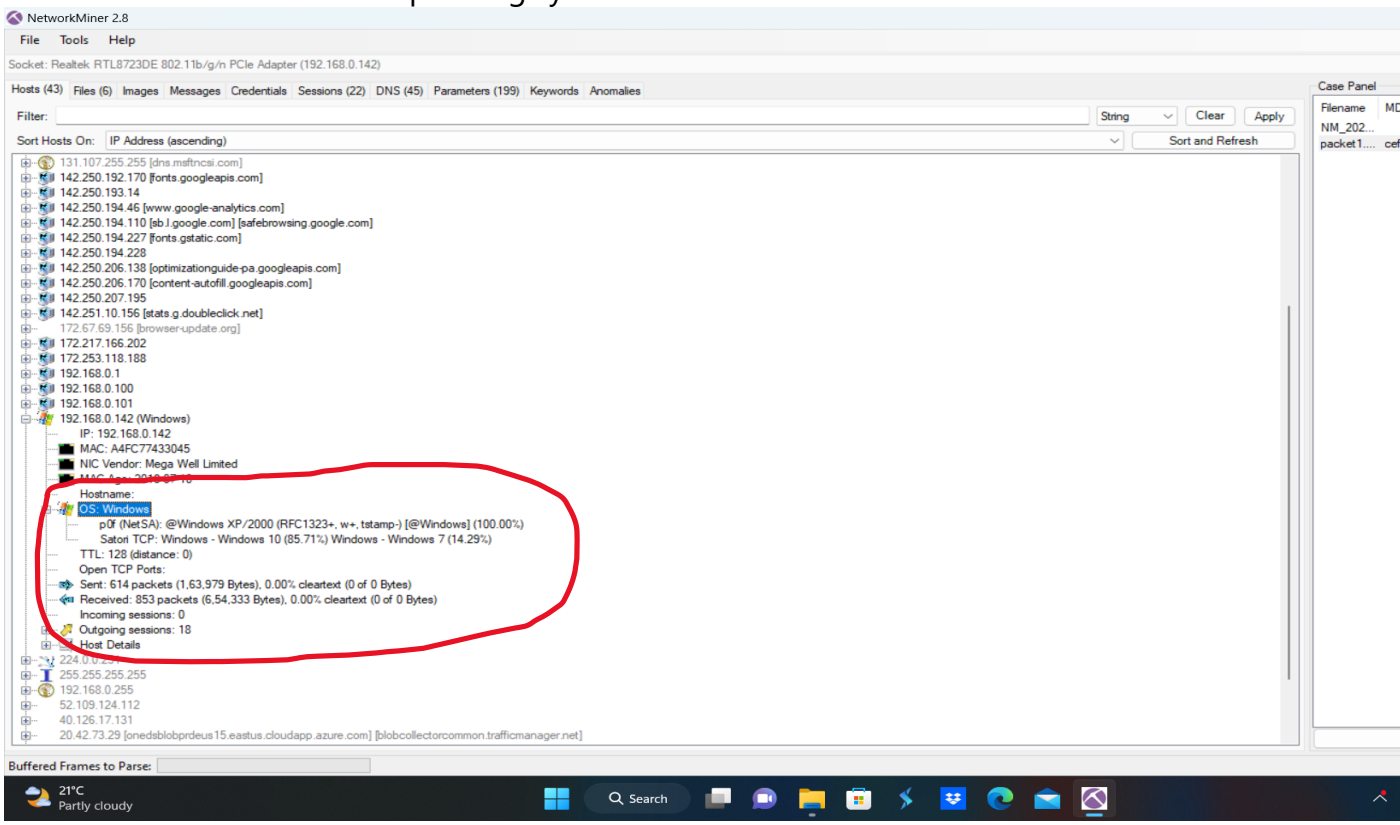
This is how we can find the operating system and hosts and port numbers of our device:

Here at the top right, we see the filename as packet1 so this the packet we got from wireshark software.

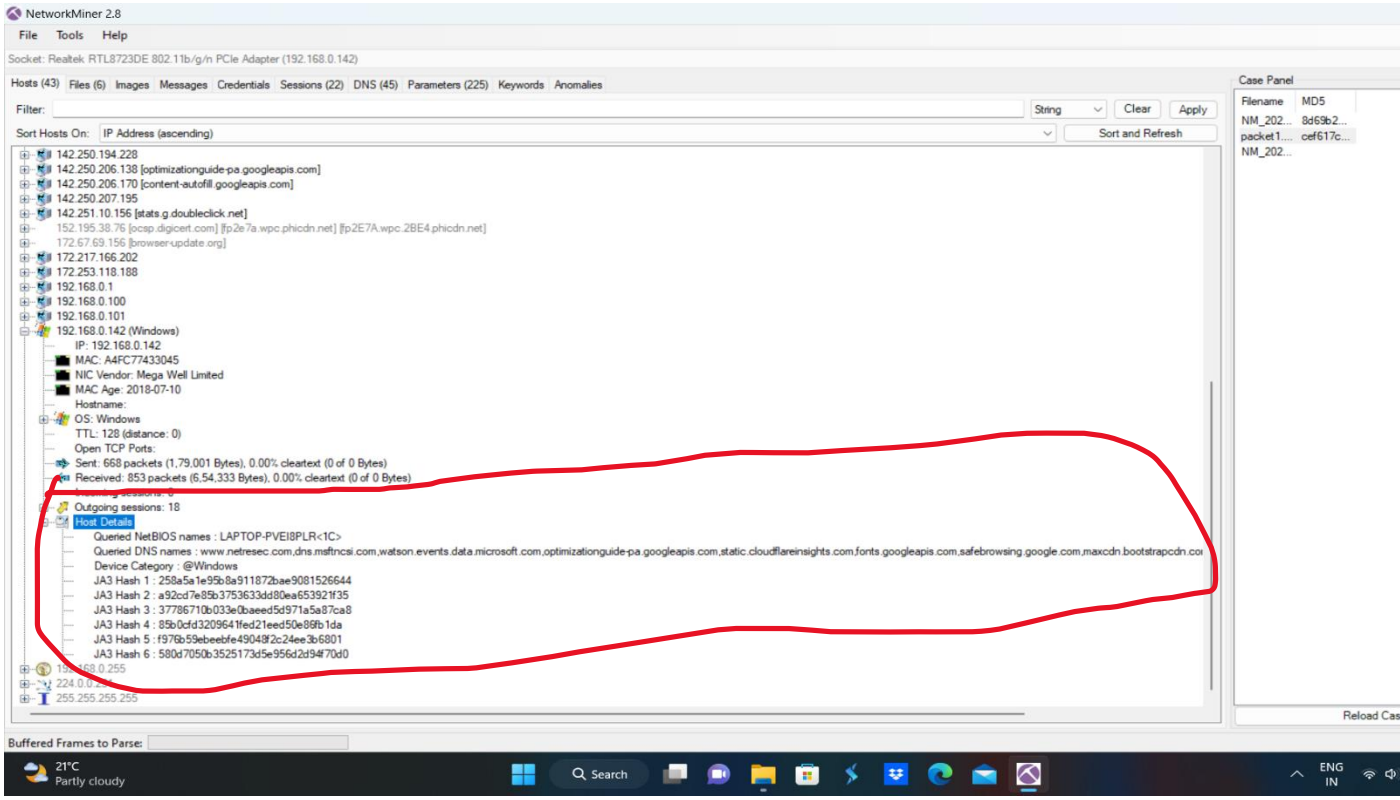
As my device is windows it's showing in the below picture and we can see the ip address.



In details of we can see the operating system here :



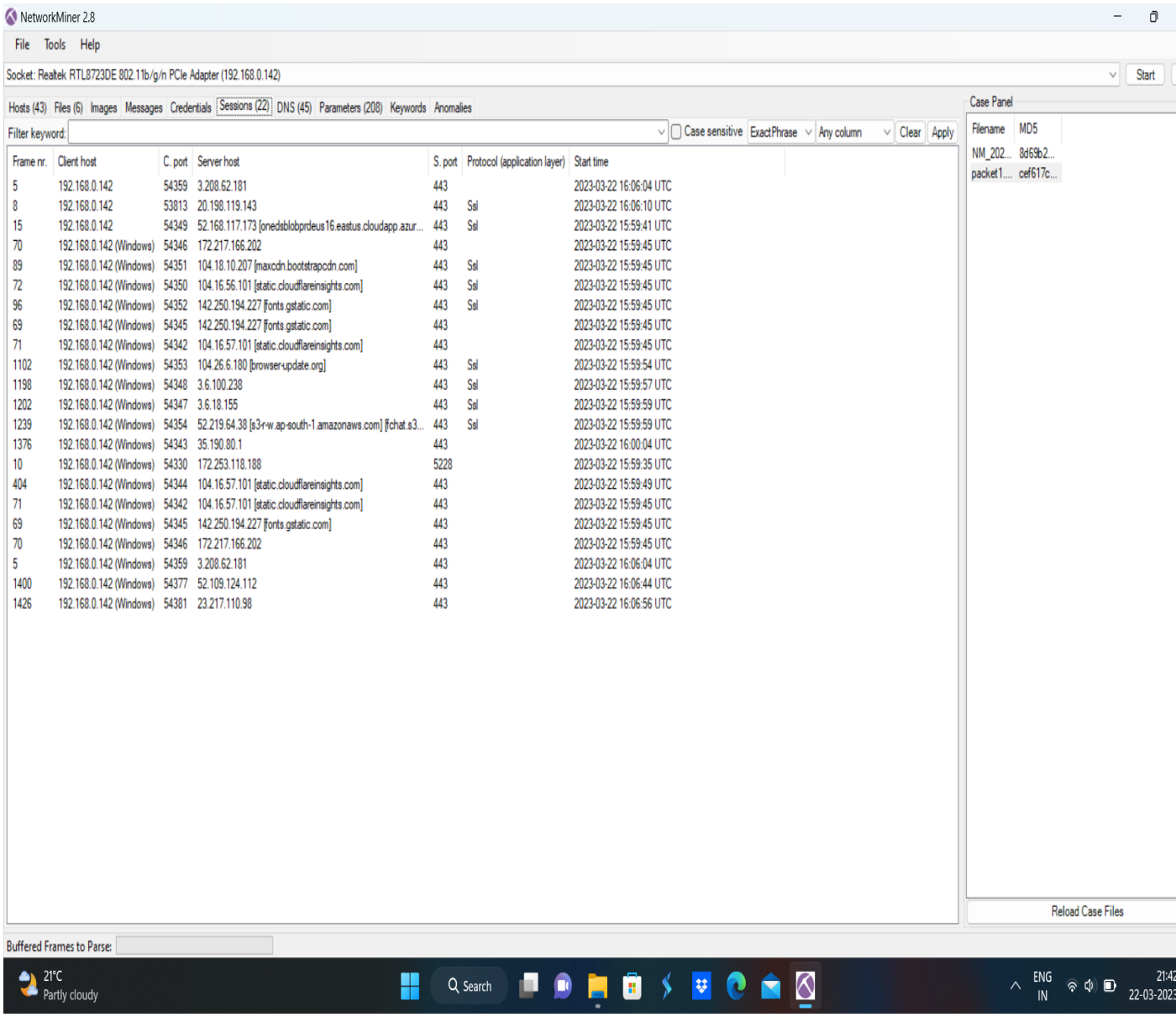
We can see the information of the local host (my lappy name)



As per the ques, we can see the sessions of our packet we have collected:

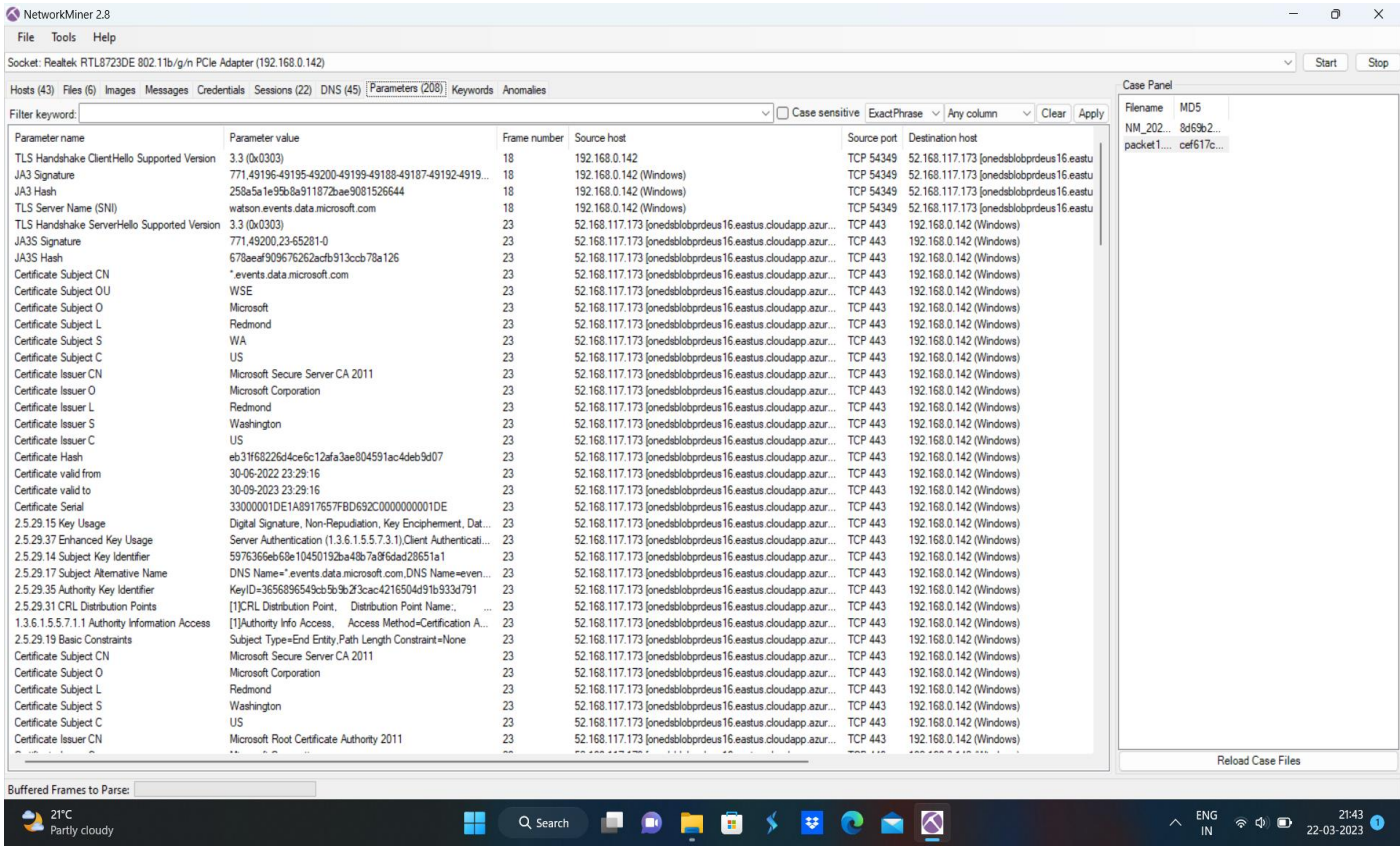
In network monitoring tools, a session refers to a sequence of packets that are transmitted between two endpoints over a network connection. A session can include multiple packets and can be used to analyze the behavior of network connections between devices.

as they provide a way to analyze and understand network behavior at a granular level. By monitoring and analyzing sessions, network administrators can identify issues and optimize network performance, ensuring the security and reliability of the network.



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

and we can see some parameters as well.



Parameter name	Parameter value	Frame number	Source host	Source port	Destination host
TLS Handshake ClientHello Supported Version	3.3 (0x0303)	18	192.168.0.142	TCP 54349	52.168.117.173 [onedsblobprdeus16.eastu
JA3 Signature	771,49196-49195-49200-49199-49188-49187-49192-4919...	18	192.168.0.142 (Windows)	TCP 54349	52.168.117.173 [onedsblobprdeus16.eastu
JA3 Hash	258a5a1e95b8a911872bae9081526644	18	192.168.0.142 (Windows)	TCP 54349	52.168.117.173 [onedsblobprdeus16.eastu
TLS Server Name (SNI)	watson.events.data.microsoft.com	18	192.168.0.142 (Windows)	TCP 54349	52.168.117.173 [onedsblobprdeus16.eastu
TLS Handshake ServerHello Supported Version	3.3 (0x0303)	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
JA3S Signature	771,49200,23-65281-0	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
JA3S Hash	678aeaf909676262acfb913ccb78a126	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject CN	*.events.data.microsoft.com	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject OU	WSE	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject O	Microsoft	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject L	Redmond	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject S	WA	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject C	US	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer CN	Microsoft Secure Server CA 2011	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer O	Microsoft Corporation	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer L	Redmond	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer S	Washington	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer C	US	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Hash	eb31f68226d4ce6c12afa3ae804591ac4deb9d07	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate valid from	30-06-2022 23:29:16	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate valid to	30-09-2023 23:29:16	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Serial	33000001DE1A8917657FBD692C0000000001DE	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.15 Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Dat...	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.37 Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1),Client Authenticati...	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.14 Subject Key Identifier	5976366eb68e10450192ba48b7a8f6dad28651a1	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.17 Subject Alternative Name	DNS Name=*.events.data.microsoft.com,DNS Name=even...	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.35 Authority Key Identifier	KeyID=3656896549cb5b9b2f3cac4216504d91b933d791	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.31 CRL Distribution Points	[1]CRL Distribution Point, Distribution Point Name:, ...	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
1.3.6.1.5.5.7.1.1 Authority Information Access	[1]Authority Info Access, Access Method=Certification A...	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
2.5.29.19 Basic Constraints	Subject Type=End Entity,Path Length Constraint=None	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject CN	Microsoft Secure Server CA 2011	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject O	Microsoft Corporation	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject L	Redmond	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject S	Washington	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Subject C	US	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)
Certificate Issuer CN	Microsoft Root Certificate Authority 2011	23	52.168.117.173 [onedsblobprdeus16.eastus.cloudapp.azur...	TCP 443	192.168.0.142 (Windows)

Thank You MAM