

INT301 PROJECT REPORT

NETWORK MINOR 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**



L OVELY
P ROFESSIONAL
U NIVERSITY

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 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.

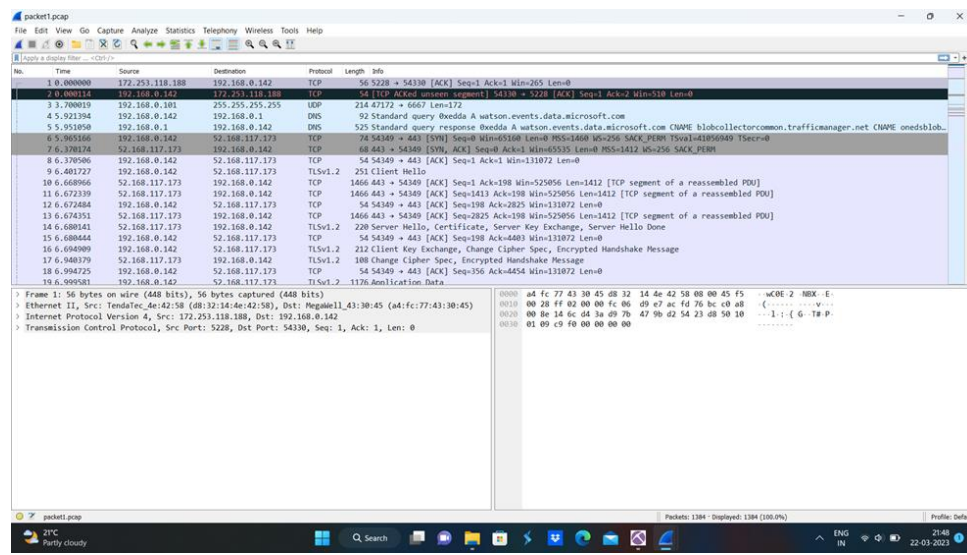


Fig: 2.4 - Wireshark

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

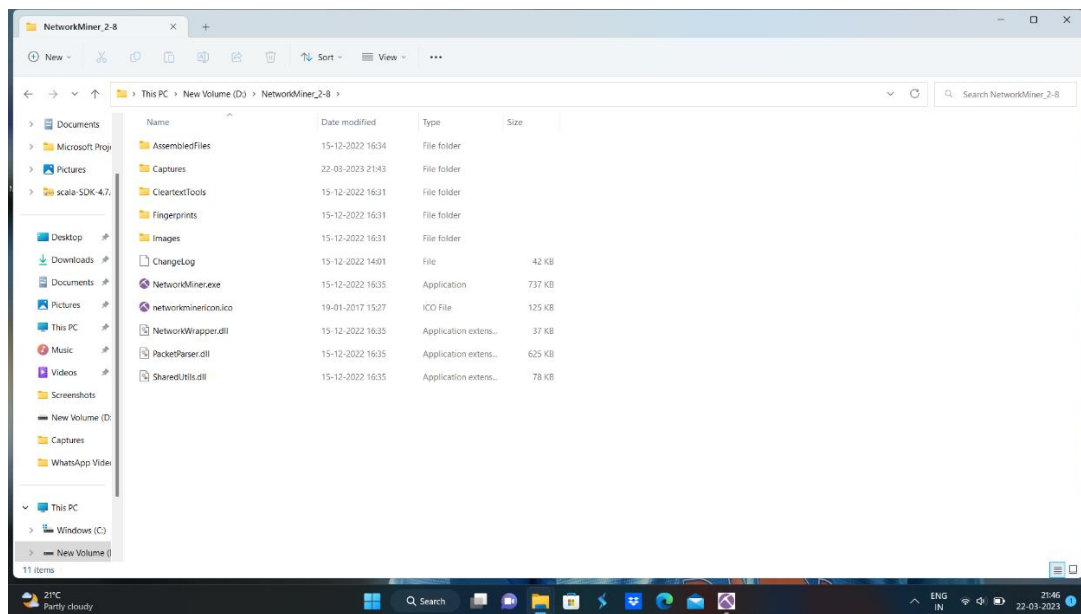


Fig: 3.1- Application

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 miner 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 to click on the start button

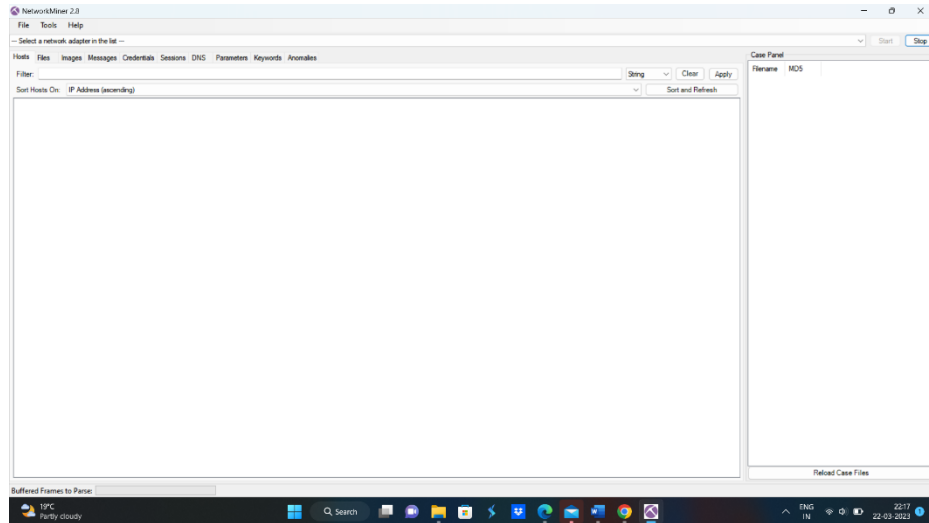


Fig: 3.2 - Network Miner Tool

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.

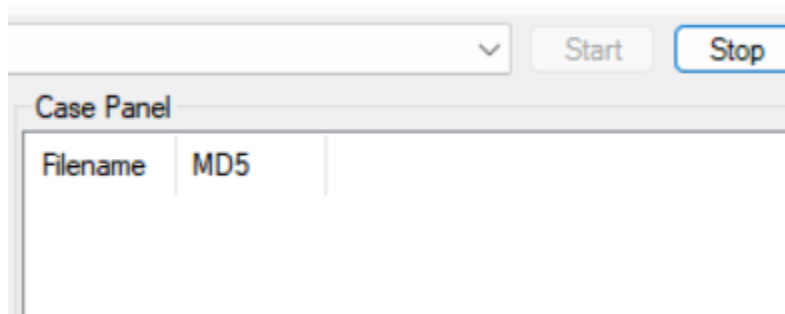


Fig: 3.3 - Start Button

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

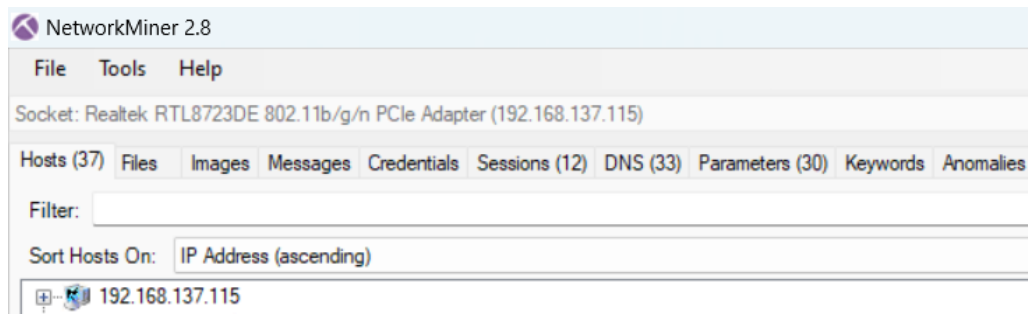


Fig: 3.3.1 - Current Running Host

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.

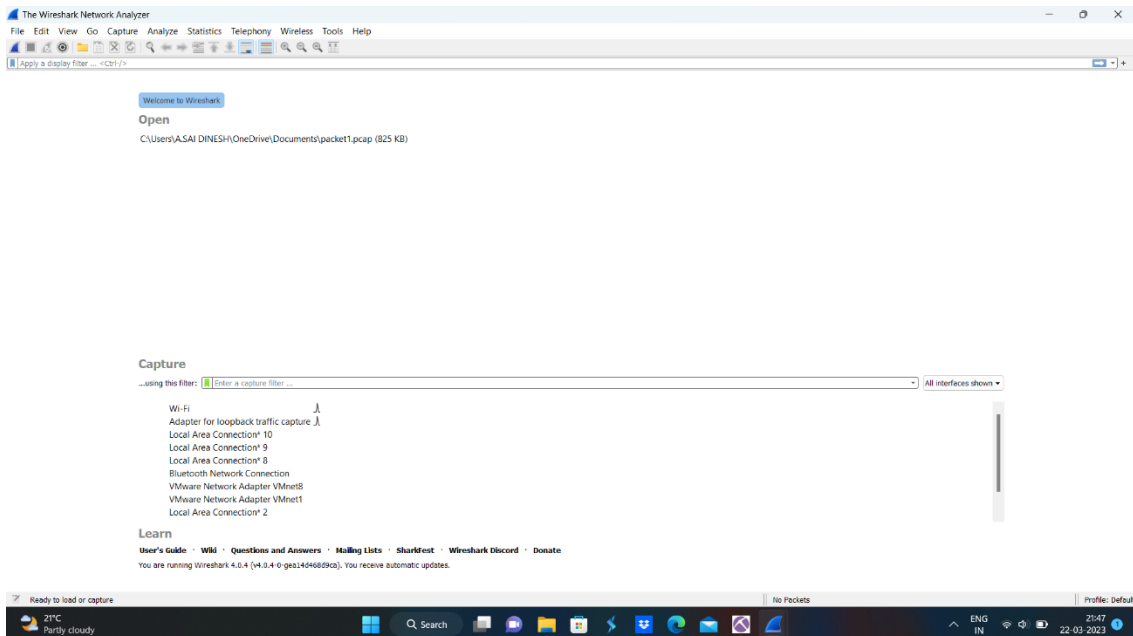


Fig: 3.3.2 - Wireshark Packet Loader

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....

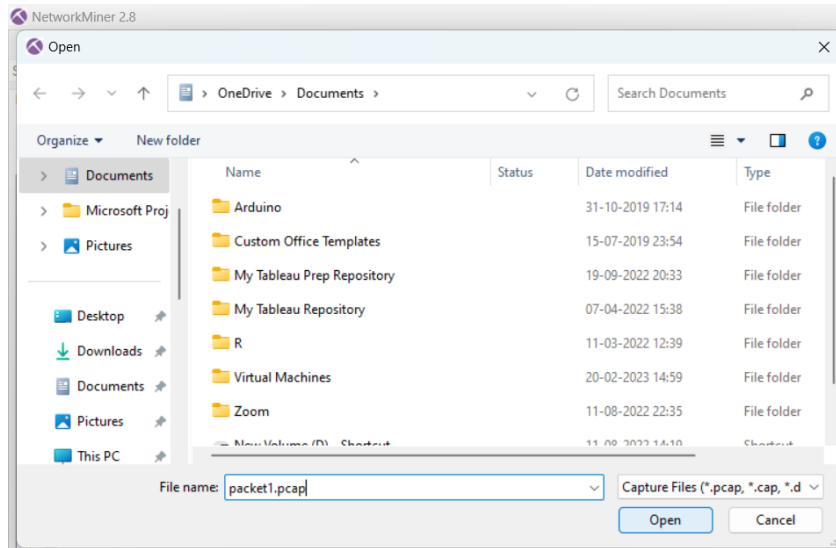


Fig: 3.3.3 - Packet Loading

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

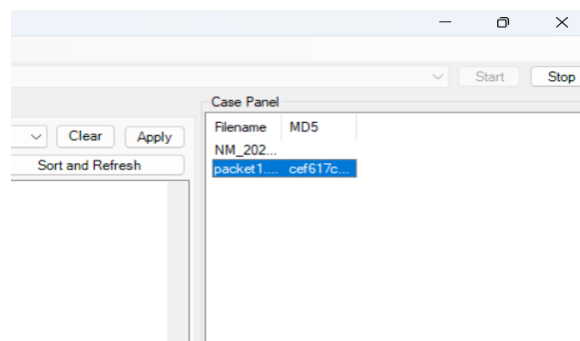


Fig: 3.3.4 - Packet

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

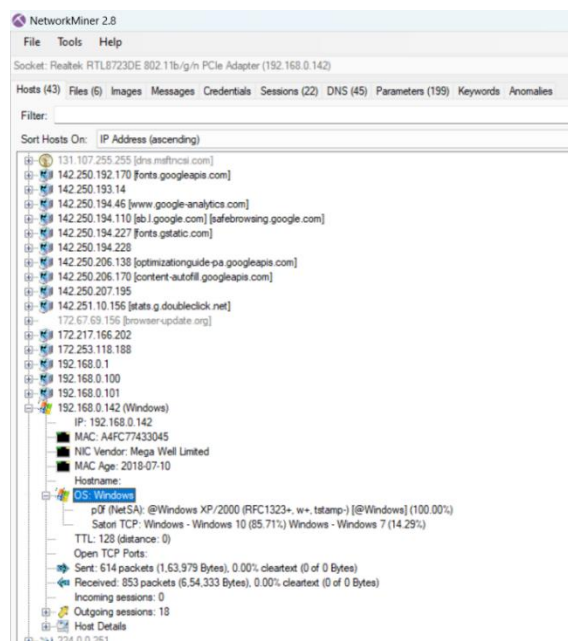


Fig: 3.4.1- Ip add, Mac add, Hosts



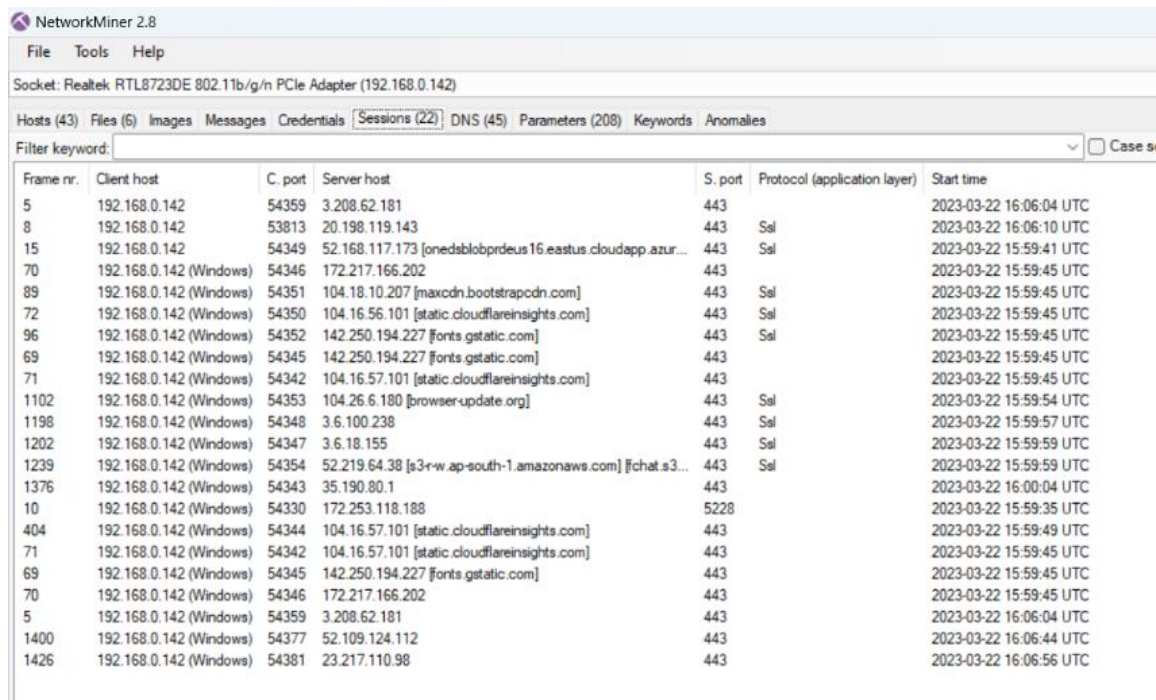
Fig: 3.4.1 Host Details

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.



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 [onedblobprdeus16.eastus.cloudapp.azure...]	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] [chat.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

Reference/Bibliography:

[1] NetworkMinerTool: <https://www.netresec.com/index.ashx?page=NetworkMiner>

[2] Wireshark: <https://www.wireshark.org/download.html>

[3] 4.1 GitHub: <https://github.com/ANAPARTHI-SAI-DINESH/Int301ProjectCA3>

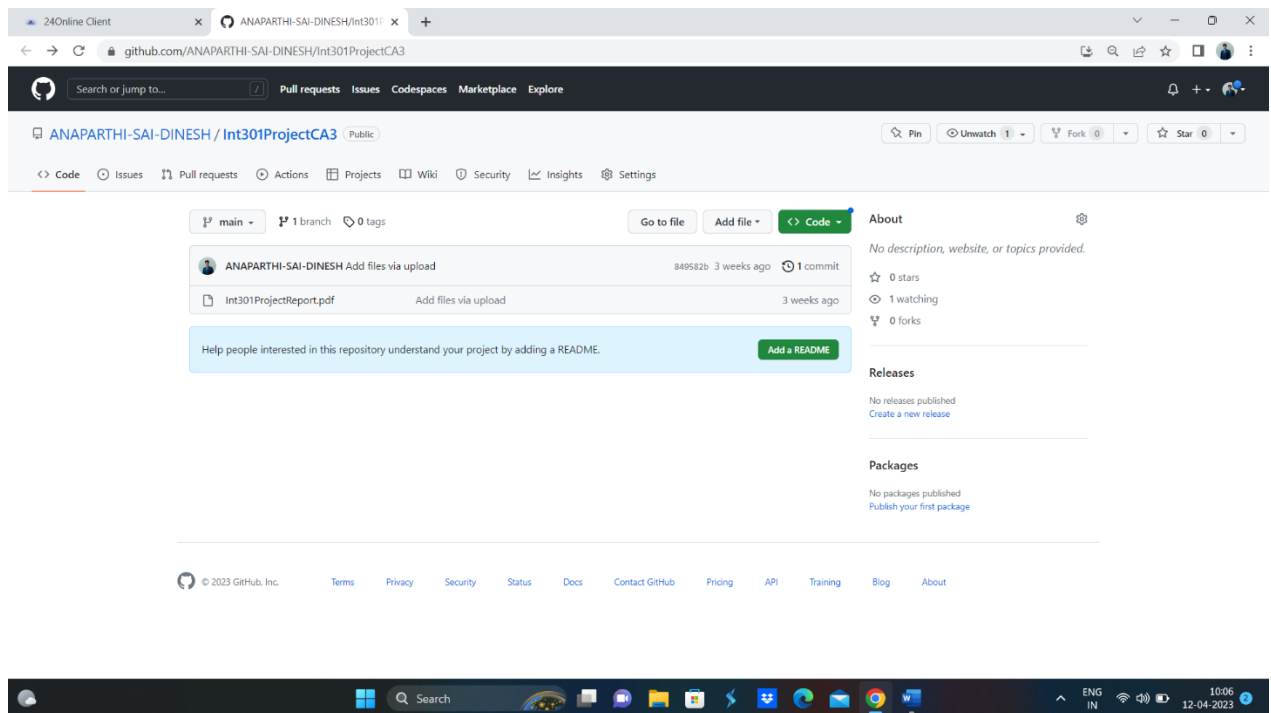


Fig: 4.1 - GitHub