

**CA3**

Of

**INT301**

Submitted By :

**Amit Yadav**

Registration No. **11910567**

Section : **KE015**

Roll No : **17**

**School of Computer Science & Engineering**

**Lovely Professional University, Phagwara**

1. Introduction

1.1 Objective of the project

- Implement a network miner tool to detect the operating system, sessions and open ports through packet sniffing and investigate the network traffic.

1.2 Description of the project

- This project involves the implementation of network minor tool which detects operating systems, sessions, and open ports on a network through packet sniffing. The tool captures packets from the network interface and analyse the packets to extract the information about the network, and display the results.

1.3 Scope of the project

- The scope of this project is to display the information the results of network analysis analysed by the network miner tool.

2. System Description

2.1 Target system description

- The experiment is performed on

Operating System: Windows 10 Home Single Language 64-bit.

Processor: AMD Ryzen 7 5800H with Radeon Graphics (16 CPUs), ~3.2GHz

Memory: 16384MB RAM

Available OS Memory: 14188MB RAM

Page File: 14309MB used, 3356MB available

Microsoft Graphics Hybrid: Supported

DirectX Database Version: 1.4.5

2.2 Assumptions and Dependencies

- The network miner tool needs compatibility with certain operating systems, and it may not work on all operating systems without modifications or additional configurations.

- The network miner tool needs to be able to access the network interface to capture packets. It assumes that the network interface is functioning properly and can be accessed by the tool.

- The network miner tool assumes that the network interface gives all permissions required for capturing all packets on the network.

2.3 Functional/Non-Functional Dependencies

- The tool must be able to capture packets from the network interface to analyze network traffic.

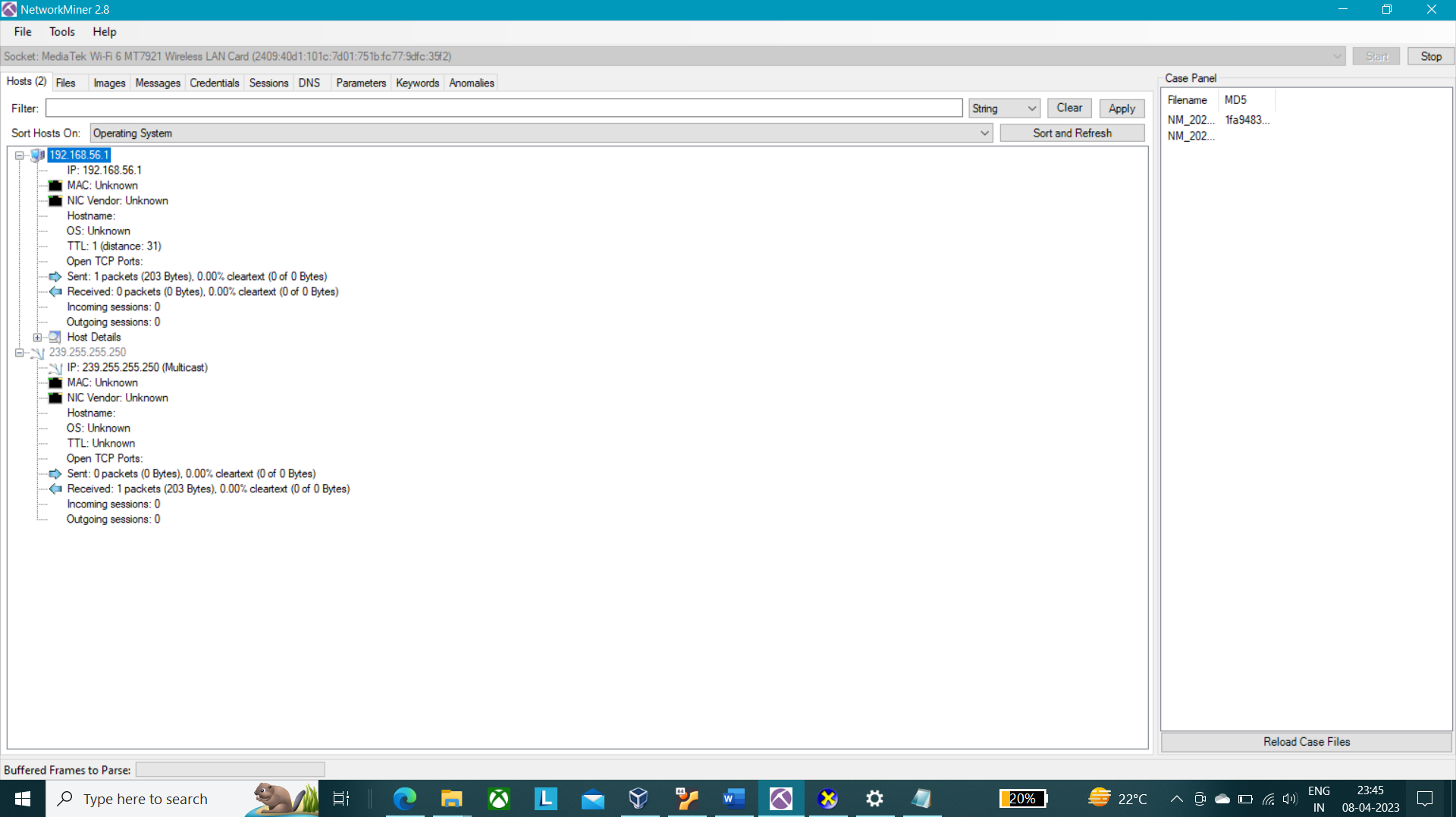
- The tool must be able to decode network protocols such as TCP, UDP, HTTP, and others to analyse the network traffic.

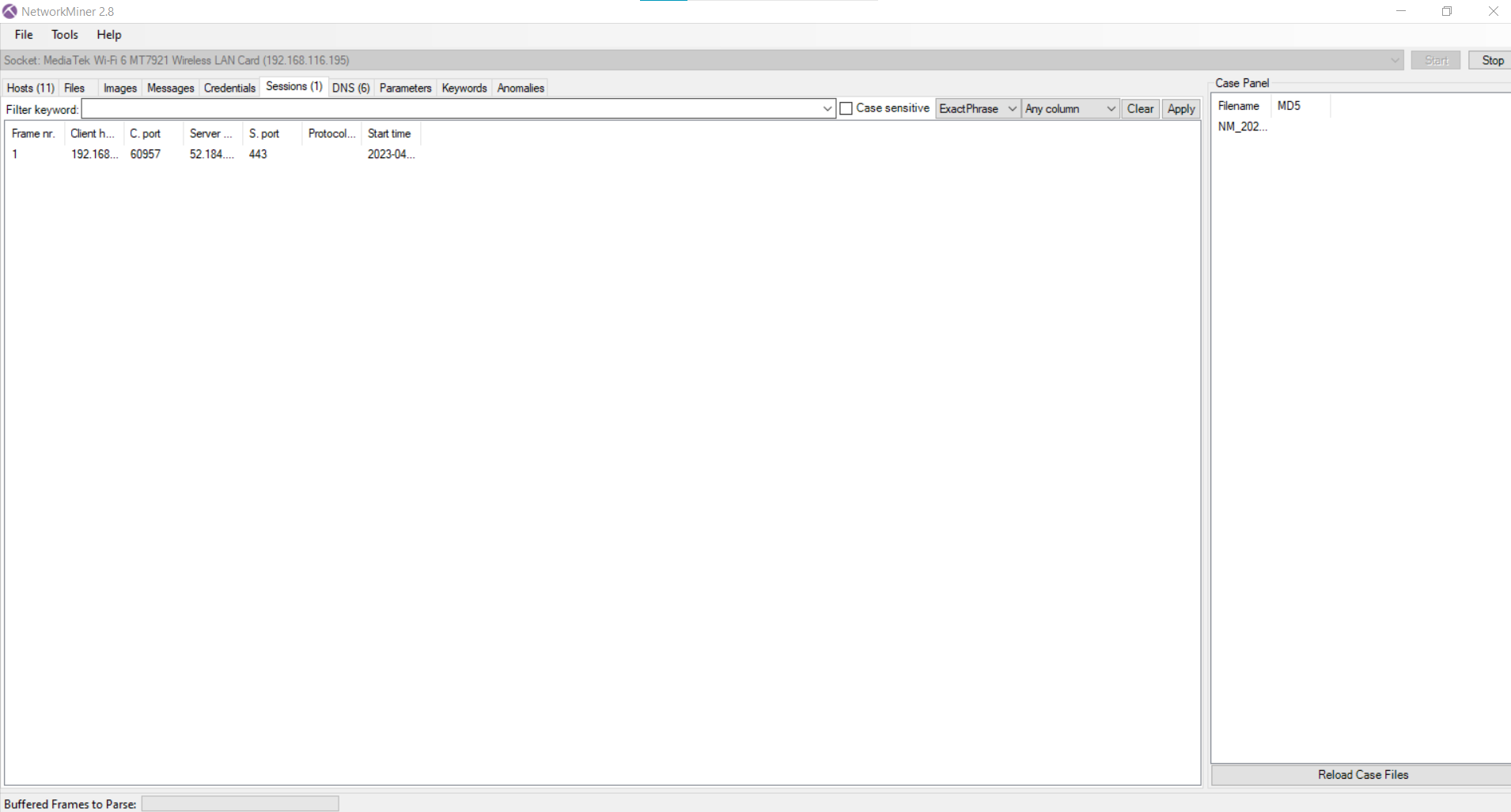
- The tool must be able to identify the operating system of devices on the network.

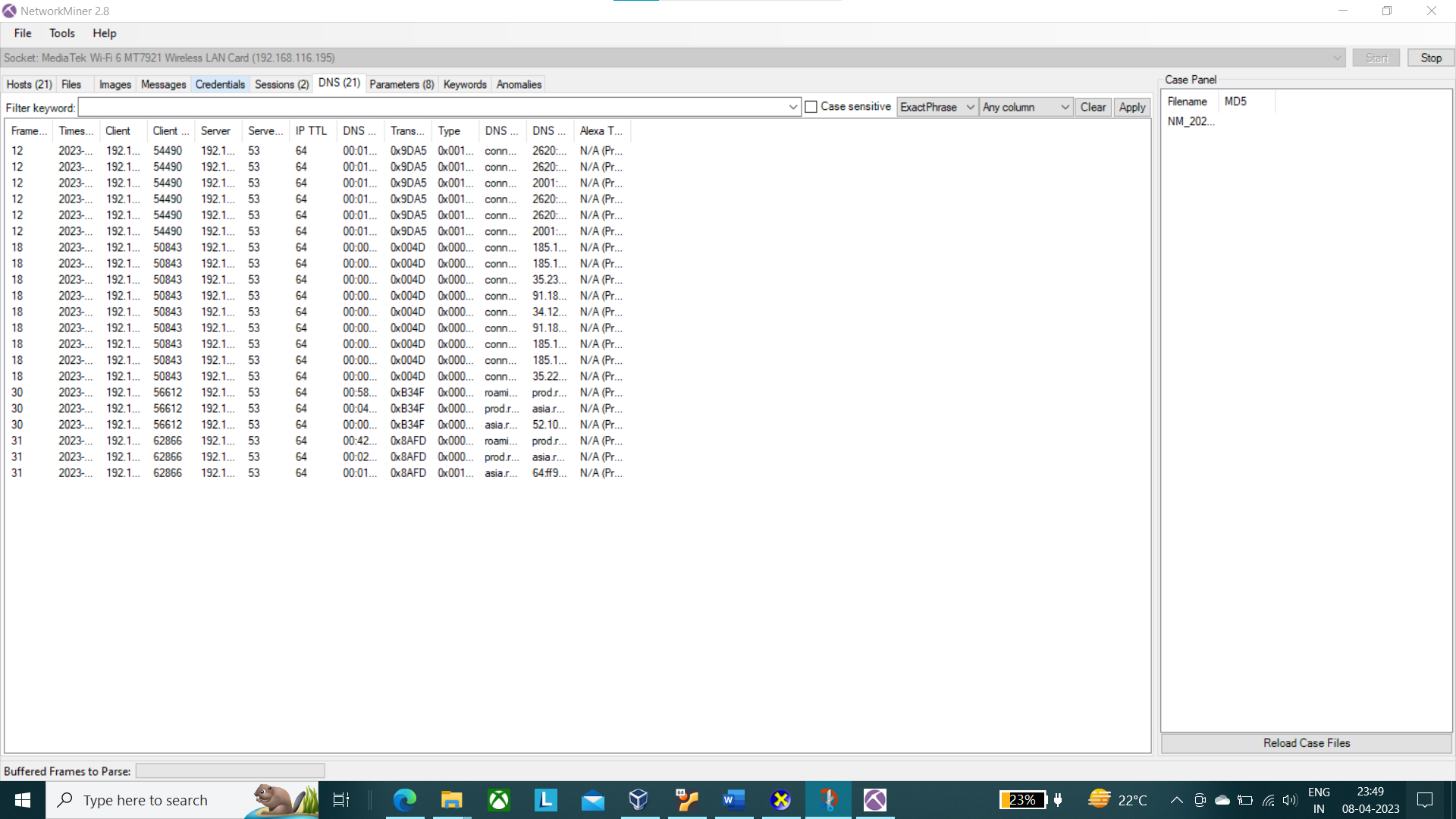
- The tool must be able to track and identify sessions between devices on the network.

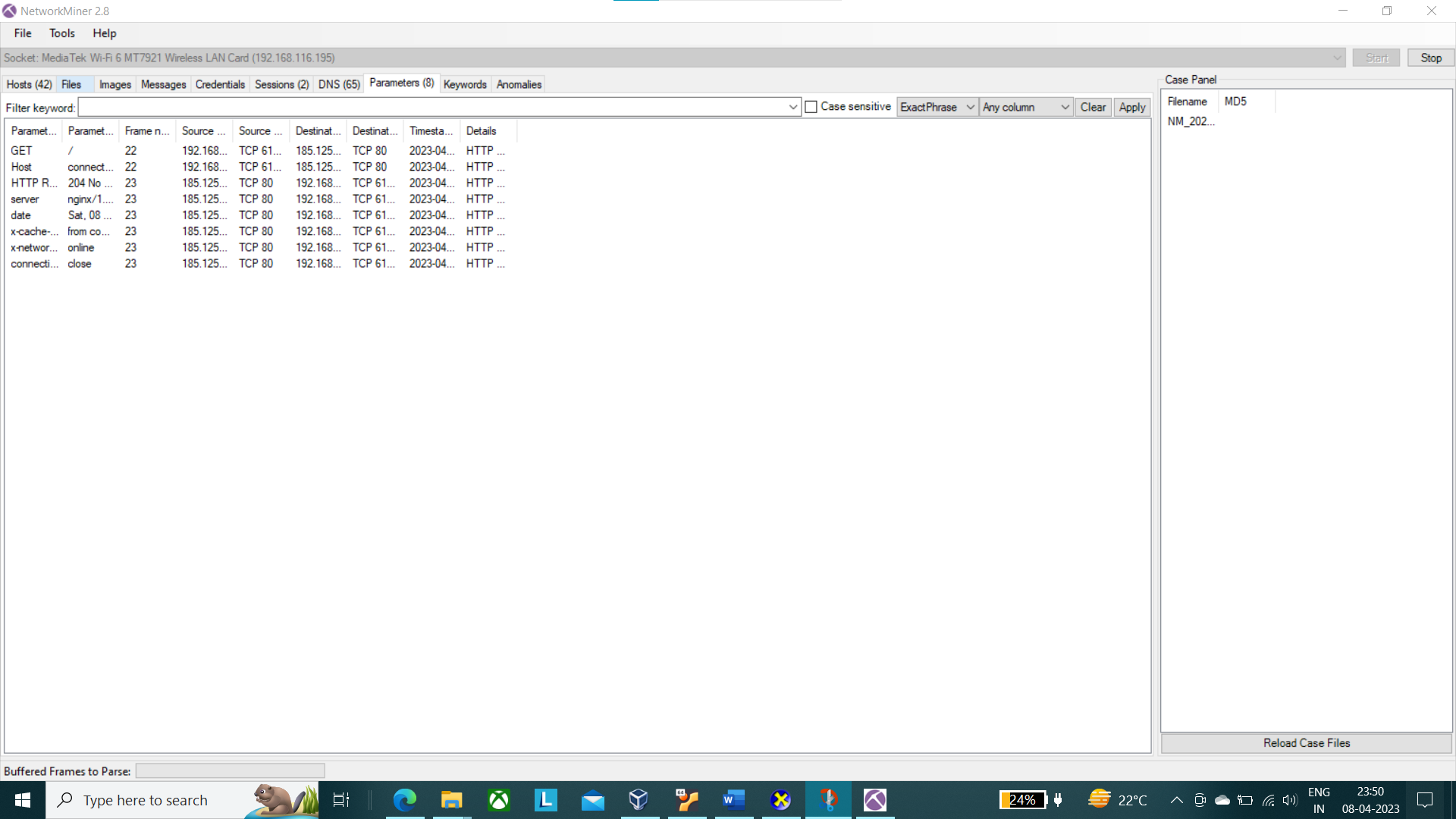
3. Analysis Report

3.1 System snapshots and full analysis report









4. Reference/ Bibliograph

1. google

2. Open AI

3. [Wireshark User’s Guide](https://www.wireshark.org/docs/wsug_html_chunked/)

GITHUB LINK:

[amityadav6612/INT301 (github.com)](https://github.com/amityadav6612/INT301)