

CA-03

INT-301: Open Source and Technologies Report of project

Name of the student: Nikhil soren Registration no: 11910020

Roll no:51.

Section: KE057

Git hub Link: https://github.com/Nikhilsoren12/INT301.git

Name of the faculty: Navjot Kaur

# Introduction:

This report gives us the idea of developing a network miner tool with which we can analyze network traffic and detect OS, sessions, and open ports through packet sniffing, helping organizations to improve their network security.

# 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.

# Description of the project:

The project explains how to set up a network miner tool that uses packet sniffing to find the operating system, open ports, and active sessions. It describes important factors including picking a library for packet sniffing, creating filters, capturing packets, extracting data, displaying findings, and testing and improving the programme. The literature emphasises the value of using the tool ethically and legally, as well as having a solid grasp of networking protocols, operating systems, and programming ideas.

For the project the tool i.e used is NetworkMiner.

The network exploration and security auditing tool NetworkMiner, sometimes known as Network Mapper, is free and open-source software. Network administrators, security experts, and hackers all use it frequently for a variety of tasks, including network inventory, port scanning, and vulnerability identification.

NetworkMiner uses a number of methods, including port scanning, version detection, and OS detection, to produce an in-depth diagram of a network and its services. TCP/IP, UDP, ICMP, and SNMP are just a few of the many operating systems and protocols it supports.

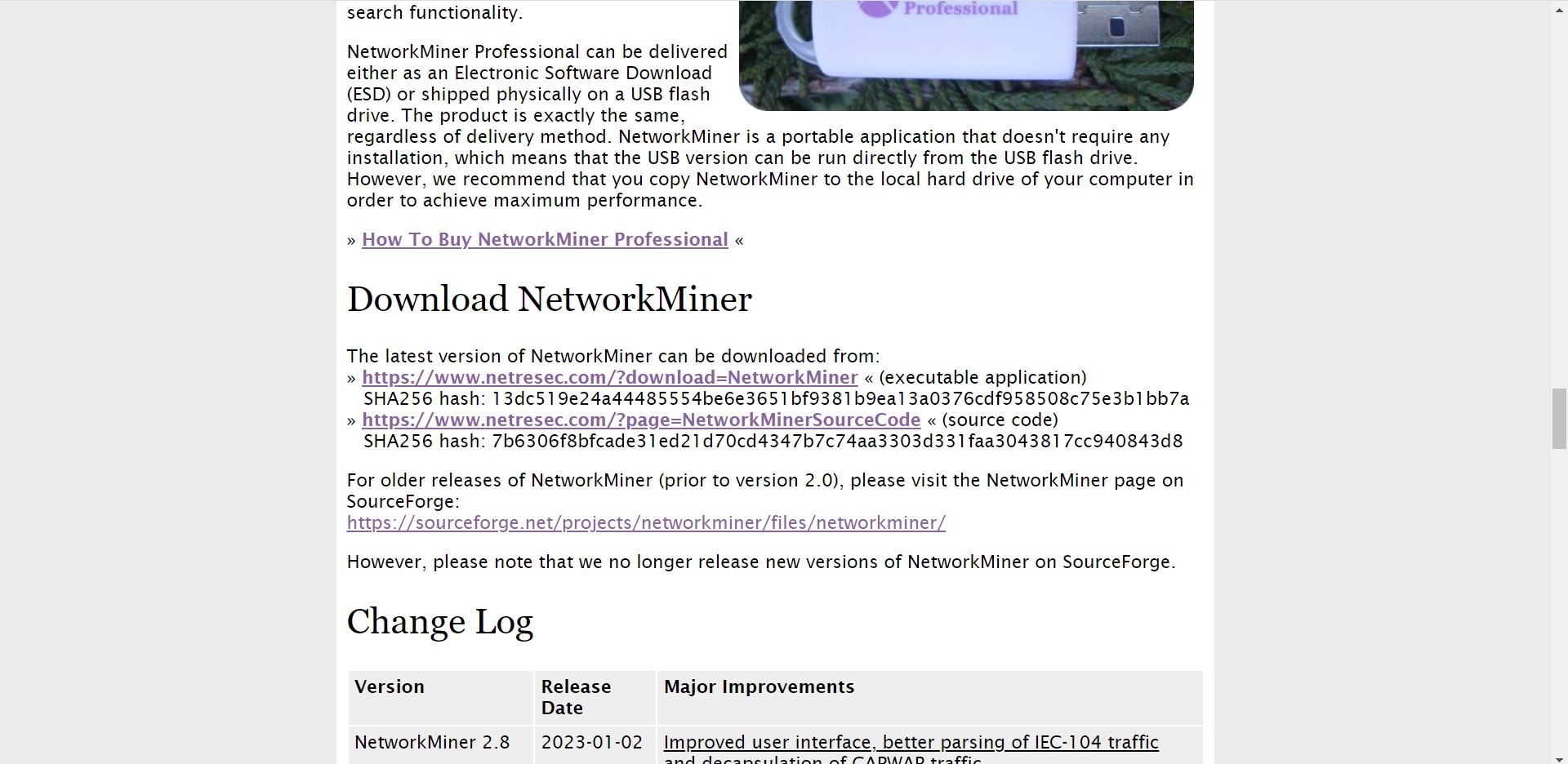
Steps to download and install the NetworkMiner in the sysytem:

Visit the NetworkMiner website's home page: The first step is to go to https://NetworkMiner.org/, the official NetworkMiner website.

Get the installer here: Go to the "Download" section and choose the installation that corresponds to your operating system. Among other platforms, NetworkMiner is accessible for Windows, Linux, and macOS.

Install NetworkMiner: After downloading the installer, run it and cross check all the steps to the prompts on the screen to install NetworkMiner on your computer. Your operating system may have an impact on the installation procedure.

Snapshot of website download page:



# Scope of the project:

The aim is to develop a network mining tool that uses packet sniffing to find open ports, sessions, and operating systems. The scope involves picking a library, creating filters, examining packets, and displaying the outcomes in an approachable manner.

# Objectives:

Create a network miner tool that can record and examine network traffic.

To determine the operating systems of devices on the network, use packet sniffing techniques.

Determine which network connections are active. Determine which networked devices have open ports. Create reports on the tool's findings.

# Tasks:

Using a open source tool ,here NetworkMiner to execute the tasks. Create a network traffic capture and analysis packet sniffing module.

Use techniques to determine the operating systems of networked devices based on the headers and payloads of packets.

Identify active sessions between networked devices by implementing algorithms.

Utilize algorithms to locate open ports on networked devices. Create a reporting module that can produce reports based on the tool's findings.

To confirm the tool's efficacy and correctness, test it on several networks.

Adjust the tool to make it more precise and effective.

# System Description:

NetworkMiner is an open-source programme used for network administration, security audits, and network research. It can detect

hosts, devices, and services on a network using a variety of scanning techniques, and it is compatible with a number of operating systems.

Operating system compatibility:NetworkMiner is a cross-platform utility that works with a number of operating systems, including Windows, Linux, macOS, and BSD.

Identifying hosts, devices, and services on a network is possible with the help of the network discovery tool NetworkMiner. It probes target hosts and finds open ports using a variety of methods, such as ping scanning, TCP scanning, and UDP scanning.

NetworkMiner's port scanning feature enables users to look for open ports on target hosts. It can detect several kinds of firewalls and intrusion prevention systems and can carry out various port scans, including TCP, UDP, SYN, ACK, and FIN scans.

NetworkMiner has a scriptable interface that enables users to create custom scripts to increase the capabilities of the programme. These scripts are employable.

# Target system description:

A network forensic investigation tool called NetworkMiner is made to record and examine network data. It is a Windows operating system-compatible open-source programme. The NetworkMiner target system is described as follows:

Hardware Requirements:

Processor: 2 GHz or higher RAM: 4 GB or higher

Hard Drive: 100 MB of available space Network Interface Card (NIC): Ethernet NIC

Software Requirements:

Operating System: Windows 7 or later NET Framework 4.7.2 or later

# Assumptions:

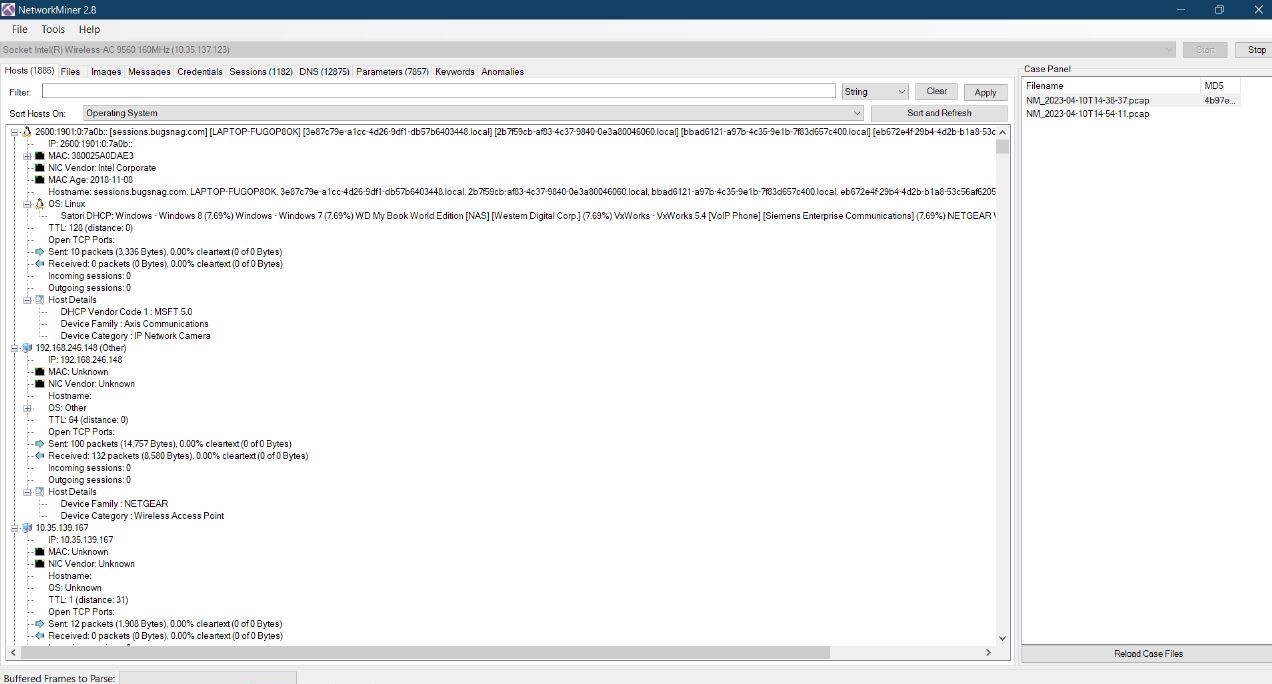
Target system is network-connected: According to NetworkMiner, the target machine is network-connected and has an IP address that can be accessed from the NetworkMiner host. NetworkMiner finds and identifies network hosts and services using IP-based scanning techniques.

The target machine must be connected to a network, not set up to stop NetworkMiner probes, have sufficient rights on the NetworkMiner host, and not be employing evasion methods or encrypted communications. The precision and comprehensiveness of

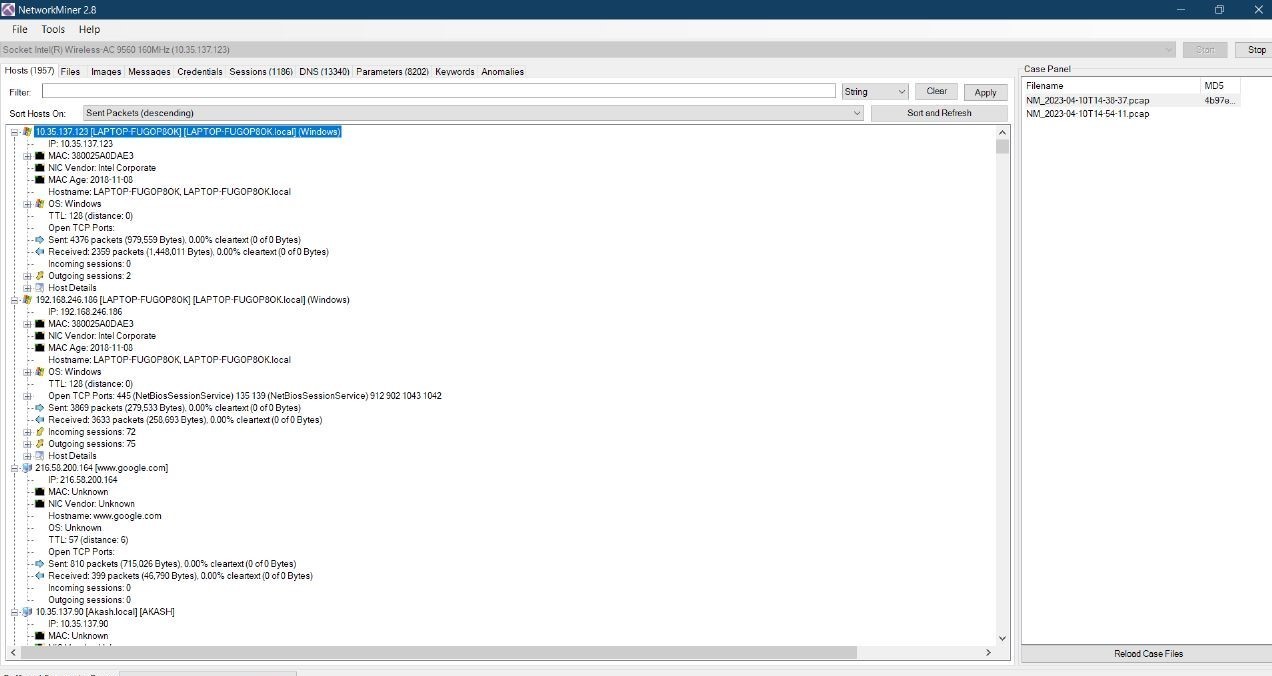
NetworkMiner's findings may be impacted by these presumptions. When using NetworkMiner for network investigation and security audits, it's critical to comprehend these presumptions.

# Analysis Report:

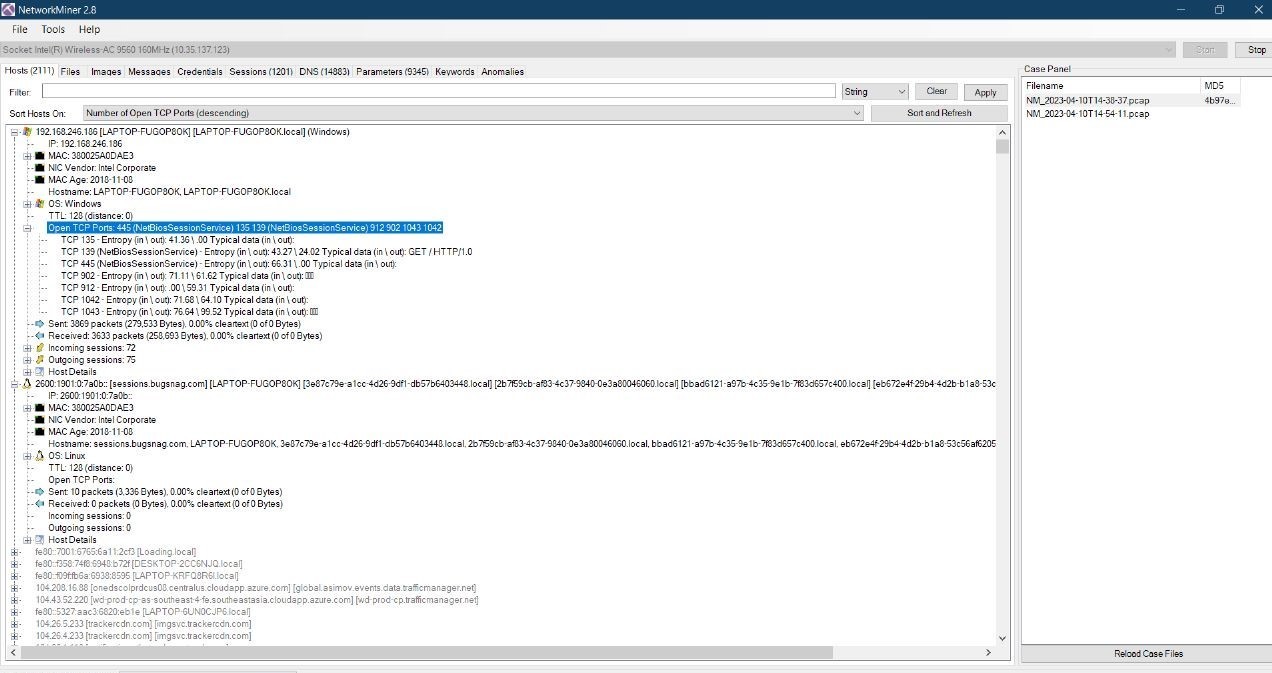
**Snapshots of the scans: scan of Os:**



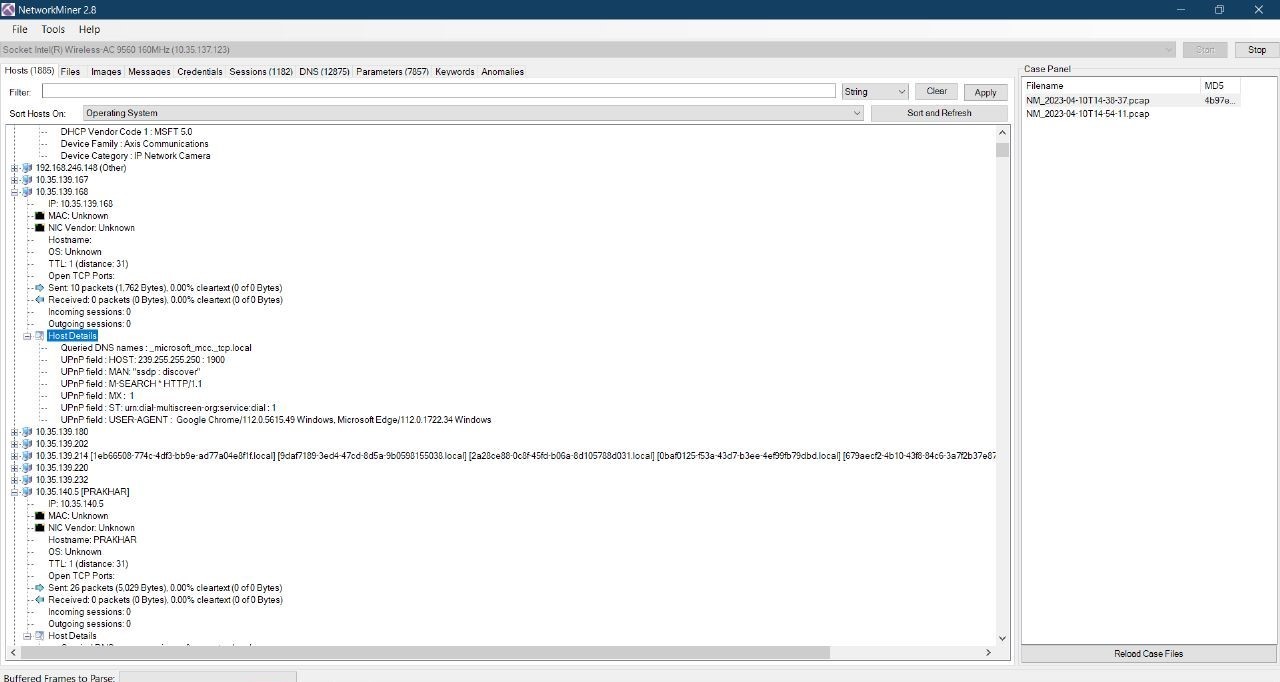
# scan of sent packets:



**Number of open ports:**



# Number of Hosts:



Reference :

1. [https://www.socinvestigation.com/networkminer-tool-dynamic-](https://www.socinvestigation.com/networkminer-tool-dynamic-malware-analysis-with-minimum-dwell-time/) [malware-analysis-with-minimum-dwell-time/](https://www.socinvestigation.com/networkminer-tool-dynamic-malware-analysis-with-minimum-dwell-time/)
2. [https://ww](http://www.netresec.com/?page=NetworkMiner)w[.netresec.com/?page=NetworkMiner](http://www.netresec.com/?page=NetworkMiner)