REPORT

OPEN-SOURCE TECHNOLOGIES (INT 301)

**NAME : Karthik. M**

**REG NO :** 11908893

**ROLL NO :** 51

**SECTION :** KEO58



**SUBMITTED TO :** Navjot Kaur

**Lovely Professional University Phagwara, Punjab, India**

**TOPIC:**

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

**Objectives:**

**Improve network security**: One of the main objectives of a network miner tool is to improve network security. By monitoring network traffic, the tool can detect potential security threats such as malware, unauthorized access attempts, or data exfiltration. This can help organizations take appropriate measures to prevent or mitigate security incidents.

**Troubleshoot network issues:** Another objective of a network miner tool is to troubleshoot network issues. By monitoring network traffic, the tool can identify the root cause of network problems such as connectivity issues or application performance problems. This can help organizations take appropriate measures to resolve network issues and maintain network availability and reliability.

**Optimize network performance:** A network miner tool can also be used to optimize network performance. By monitoring network traffic, the tool can identify bottlenecks, latency issues, or other performance problems that may impact the user experience. This can help organizations optimize network infrastructure and improve user satisfaction.

**Monitor compliance:** In some cases, a network miner tool may be used to monitor compliance with regulatory or legal requirements. For example, the tool may be used to ensure that sensitive data is not being transmitted over the network in violation of data privacy regulations.

**Gain insight into network usage:** Finally, a network miner tool can be used to gain insight into network usage. By monitoring network traffic, the tool can identify which applications and services are being used most frequently, which users are consuming the most bandwidth, and other usage patterns that can inform network planning and optimization.

Overall, the objective of a network miner tool is to provide organizations with visibility into network activity and enable them to make informed decisions regarding network security, performance, and optimization.

# Description:

# A network miner tool is a software application designed to capture, analyze, and interpret network traffic data. This type of tool is commonly used by IT security professionals, network administrators, and system analysts to monitor and manage network performance, security, and compliance.

# To detect the operating system of a device on a network, a network miner tool typically employs a technique called "passive OS fingerprinting". This involves capturing network traffic data and analyzing the unique characteristics of packets sent by different operating systems. For example, different operating systems may have different default values for various TCP/IP parameters such as Time to Live (TTL), Window Size, or Initial Sequence Number (ISN). By analyzing these parameters, a network miner tool can make an educated guess about the operating system that is generating the network traffic.

# Passive OS fingerprinting can be performed using a variety of techniques, such as statistical analysis, pattern matching, or machine learning algorithms. Some network miner tools may use a combination of these techniques to improve accuracy and reliability.

# Once the network miner tool has identified the operating system of a device on the network, this information can be used to inform network security, troubleshooting, or optimization activities. For example, if a network miner tool detects an outdated or vulnerable operating system, security measures can be implemented to mitigate the risk of cyber-attacks. Similarly, if a network miner tool detects performance issues caused by a specific operating system, network administrators can take steps to optimize the network infrastructure to improve performance. Overall, a network miner tool that can detect the operating system of devices on a network is an asset for any organization that wants to monitor and manage network activity effectively.

# scope:

# Network traffic analysis: A network miner tool can analyze network traffic to detect patterns and trends in data usage. This information can help organizations optimize network performance by identifying which applications and services are using the most bandwidth.

# Network security: A network miner tool can identify the OS running on a device, which can help organizations determine the appropriate security measures to protect against OS-specific vulnerabilities or threats. For example, if the tool detects a device running an outdated OS that is no longer supported by the vendor, the organization may need to take steps to mitigate the risks associated with running an unsupported OS.

# Troubleshooting: A network miner tool can help troubleshoot network issues by identifying the OS running on a particular device. This information can help support personnel identify potential compatibility issues or conflicts with other devices or software running on the network.

# Application performance: A network miner tool can monitor the performance of applications and services running on the network by analyzing packet data. The tool can identify latency issues, bottlenecks, and other problems that may be affecting application performance.

# Compliance: In some cases, a network miner tool may be used to monitor compliance with regulatory or legal requirements. For example, the tool may be used to ensure that sensitive data is not being transmitted over the network in violation of data privacy regulations.

# Target system description:

# The target system for a network miner tool can vary depending on the specific use case and objectives of the tool. Generally, the tool is designed to monitor and analyze network traffic to identify specific information about the devices and traffic passing through the network. In the case of detecting the operating system or open ports, the target system would be any device connected to the network. This includes servers, workstations, laptops, mobile devices, and any other devices that are connected to the network. The tool can be configured to scan the network for specific IP addresses or ranges, which can help identify all devices connected to the network.

# To monitor network traffic, the network miner tool typically uses packet sniffing techniques to capture packets as they pass through the network. The tool can then analyze these packets to identify specific information such as the operating system, open ports, or other network traffic characteristics.

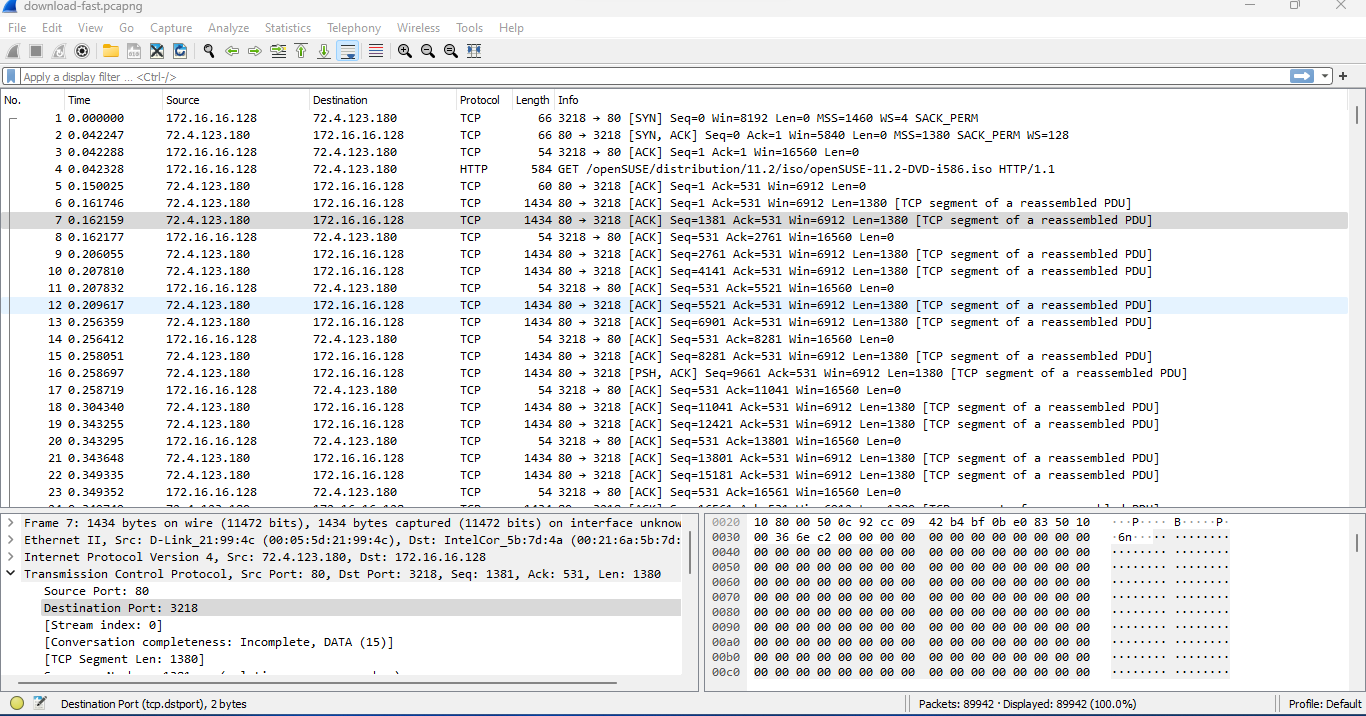
# It is important to note that the use of a network miner tool to monitor network traffic must comply with relevant laws, regulations, and organizational policies. Organizations should establish clear policies and procedures for the use of network monitoring tools and ensure that employees are trained on these policies and procedures. Additionally, the tool should be used only for authorized purposes and in a manner that respects the privacy and security of network users.

**DATA SET:** <https://github.com/chrissanders/packets>

**Snapshots of the project:**

1) First, I downloaded “**Wireshark**”.

2) Then I took dataset from Chris Sanders GitHub.



Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application, table

Description automatically generated

Graphical user interface, application, table

Description automatically generated

**Reference:**

1. [**https://www.youtube.com/@hak5**](https://www.youtube.com/@hak5)