Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch:___C3__	**Roll No.:___110**
Experiment No. 8	

Title: Working with sample real life cases related to Network security and forensics using tool - Network Miner.

Objective:

Expected Outcome of Experiment:

CO	Outcome
4	Illustrate and Compare network security mechanisms

Books/ Journals/ Websites referred:

Abstract:-

Wireshark and NetworkMiner are two popular tools used for network analysis and packet sniffing. While both tools serve similar purposes, they have some differences in their features and capabilities. In this experiment, we are going to solve a forensics case using the tools.

Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company's prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company's secret recipe.

Security staff have been monitoring Ann's activity for some time, but haven't found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

"We have a packet capture of the activity," said security staff, "but we can't figure out what's going on. Can you help?"

You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence including:

1. What is the name of Ann's IM buddy?
2. What was the first comment in the captured IM conversation?
3. What is the name of the file Ann transferred?
4. What is the magic number of the file you want to extract (first four bytes)?
5. What was the MD5sum of the file?
6. What is the secret recipe?

Related Theory: -

Wireshark:

Wireshark is a free and open-source packet analyzer. It is widely used by network professionals to capture and analyze network traffic in real-time. Wireshark can capture packets from a live network or read packets from a previously saved capture file.

Key features of Wireshark include:

- Packet Capture: Wireshark can capture packets from a wide range of network interfaces.

- Packet Analysis: It provides detailed packet information, including protocols used, packet headers, and payload data.

- Filtering: Wireshark offers powerful filtering capabilities to focus on specific packets or protocols.

- Decoding: It can decode many protocols and display them in a human-readable format.

- Statistics: Wireshark can generate various statistics, such as packet counts, protocol distribution, and conversations.

- Export: Captured packets can be exported in various formats for further analysis or reporting.

NetworkMiner:

NetworkMiner is a network forensic analysis tool that can be used to detect operating systems, sessions, hostnames, open ports, and extract files transferred over the network. It is primarily focused on extracting useful information from captured network traffic.

Key features of NetworkMiner include:

- Automatic Protocol Detection: NetworkMiner can automatically detect protocols used in the captured traffic.

- File Extraction: It can extract files transferred over the network, such as images, documents, and executables.

- Host Information: NetworkMiner can identify hostnames, IP addresses, and operating systems of devices on the network.

- Session Reconstruction: It reconstructs sessions between hosts, showing the data exchanged during the session.

- Export: Extracted files and other information can be exported for further analysis.

Differences:

- Focus: Wireshark is primarily focused on packet analysis and provides detailed information about each packet. NetworkMiner, on the other hand, focuses on extracting useful information from the captured traffic.

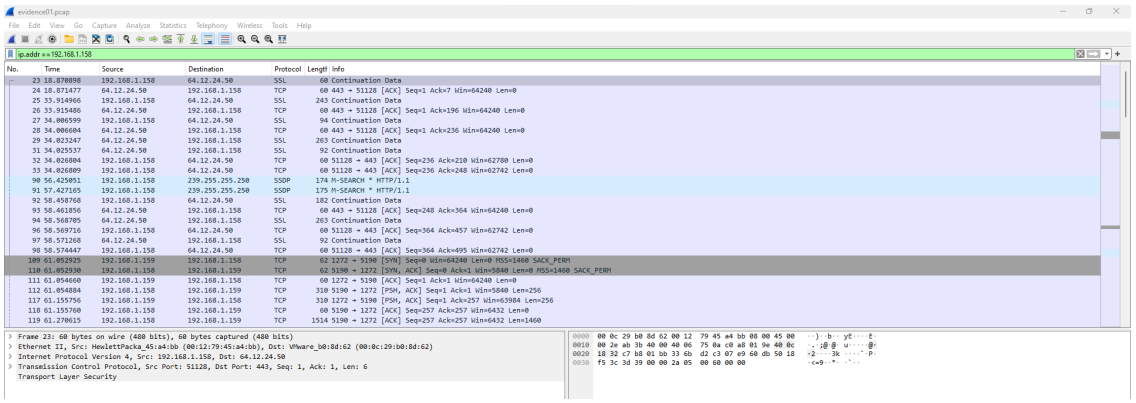
- Features: Wireshark offers more advanced features for packet analysis, filtering, and decoding, while NetworkMiner is more specialized in extracting files and host information.

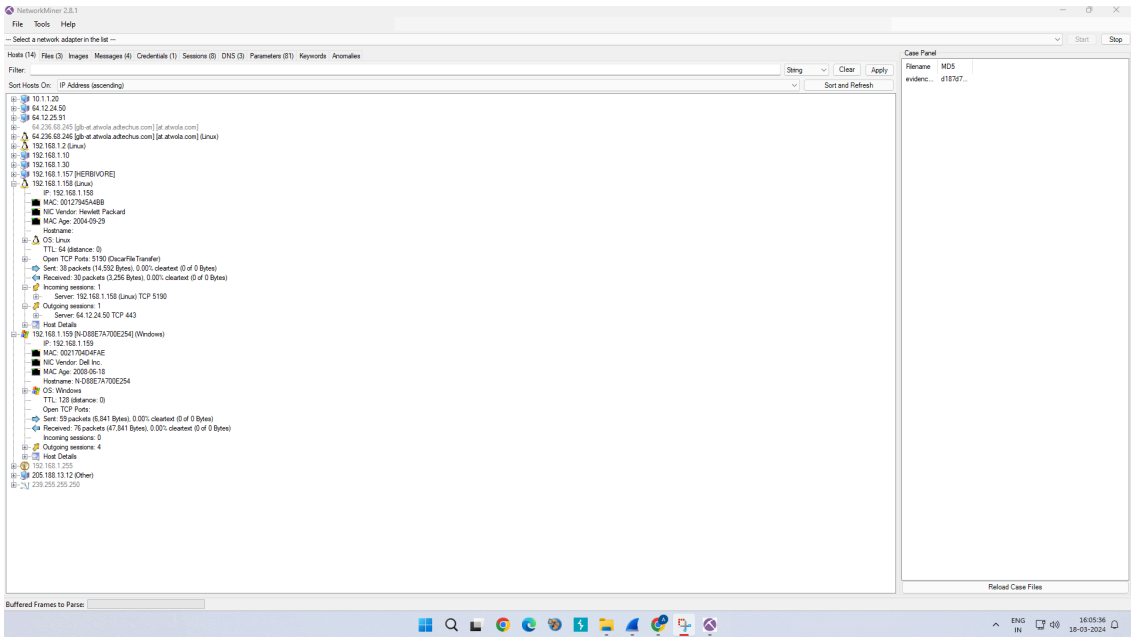
- User Interface: Wireshark has a complex user interface with many options and features, while NetworkMiner has a simpler interface focused on the most commonly used features.

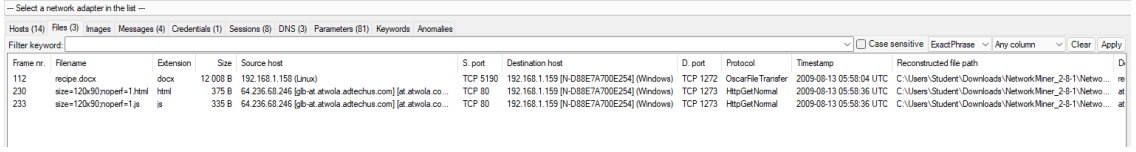
Implementation Details:

1. Enlist all the Steps followed and various options explored

1. Check for outgoing traffic from Ann's IP
2. Check for file details
3. Put the pcap file into network miner and analyze the transmission.







1. What is the name of Ann's IM buddy? 64.12.24.50

2. What was the first comment in the captured IM conversation? Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)

3. What is the name of the file Ann transferred? recipe.docx

4. What is the magic number of the file you want to extract (first four bytes)? 50 4B 03 04

5. What was the MD5sum of the file?
8350582774e1d4dbe1d61d64c89e0ea1

6. What is the secret recipe?
Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Conclusion:- Thus we have performed digital forensics through the use of tools like Wireshark and Network miner. Wireshark is a comprehensive packet analyzer used for detailed packet analysis, while NetworkMiner is more focused on extracting useful information from network traffic, such as files and host information. Both tools are valuable in different scenarios depending on the specific requirements of the network analysis task.