Assignment 8

Title: Configure and Demonstrate Use of Vulnerability Assessment Tool like Wireshark

Name: Shubhankar jakate
PRN : 22310371
Roll No = 382019

Aim:

To configure and demonstrate the use of a vulnerability assessment and network analysis tool such as **Wireshark**.

Objectives:

1. To understand how network packets are captured and analyzed.
2. To identify vulnerabilities and suspicious network behavior.
3. To learn how to use Wireshark for real-time traffic monitoring and protocol analysis.

Tools / Software Required:

- Wireshark (Latest version)
- Operating System: Windows
- Network Connection: Wi-Fi

Theory:

Wireshark is an open-source network protocol analyzer used for capturing and inspecting data packets flowing through a network.
It helps in identifying vulnerabilities, diagnosing network issues, and monitoring real-time traffic.

Wireshark captures packets at the network interface and displays detailed information such as source and destination IP addresses, protocols, ports, and payload data.
It supports various protocols like **TCP, UDP, HTTP, HTTPS, DNS, ARP, and ICMP**.

Key Features:

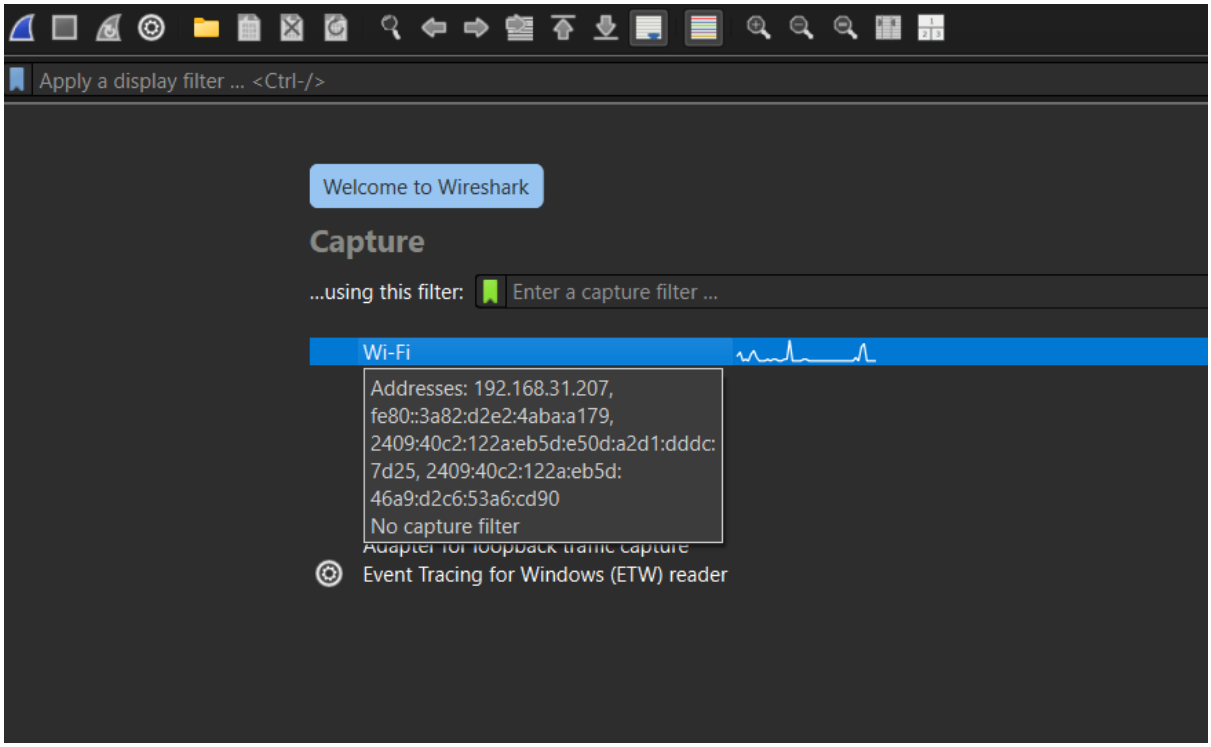
- Real-time packet capture and offline analysis
- Deep inspection of hundreds of protocols
- Filtering tools for specific traffic
- Color-coding for better packet visualization
- Export data for further analysis

Procedure:

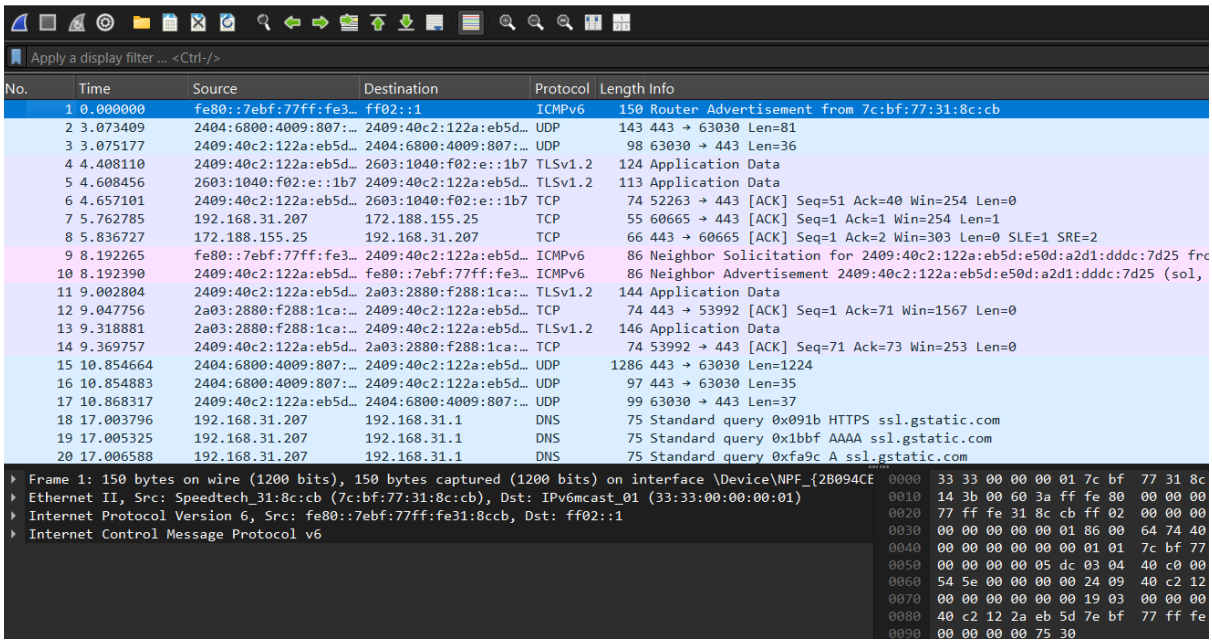
1. Install Wireshark from https://www.wireshark.org/.
2. Launch Wireshark and select the Wi-Fi network interface.
3. Click on **Start Capturing Packets** (blue shark fin icon).
4. Observe packets being captured in real-time.
5. Apply filters like ip, http, or tcp.port == 80 to focus on specific packets.
6. Select a packet to view details such as source, destination, and protocol information.
7. Identify potential vulnerabilities like unencrypted HTTP traffic or unknown connections.
8. Stop capture and save the session as .pcap file for later analysis.

Screenshots:

Screenshot shows network interface selection



Screenshot shows live packet capture



Observations:

Sr. No.	Source IP	Destination IP	Protocol	Info / Observation
1	192.168.31.207	172.188.155.25	TCP	Normal HTTP request

2	192.168.31.207	8.8.8.8	ICMP	Ping request detected
3	192.168.31.207	192.168.31.1	DNS	DNS query for domain resolution

Result:

Successfully configured and used **Wireshark** to capture and analyze network packets.
Observed different protocols and identified potential vulnerabilities in unencrypted network traffic.

Conclusion:

Wireshark is a powerful tool for monitoring, analyzing, and identifying vulnerabilities within network traffic.
It provides detailed insights into network communication, which is essential for cybersecurity and performance troubleshooting.