SWARNAMALA.V **241901116**

EXP:12 Capture, Save, and Analyze Network Traffic using Wireshark DATE: 13/10/25

Aim:
To use Wireshark to capture, save, and analyze network traffic over multiple protocols (TCP, UDP, IP, HTTP, ARP, DHCP, ICMP, DNS).

Introduction:
Wireshark is a packet analyzer used for network troubleshooting and protocol analysis.

Algorithm (Procedure):

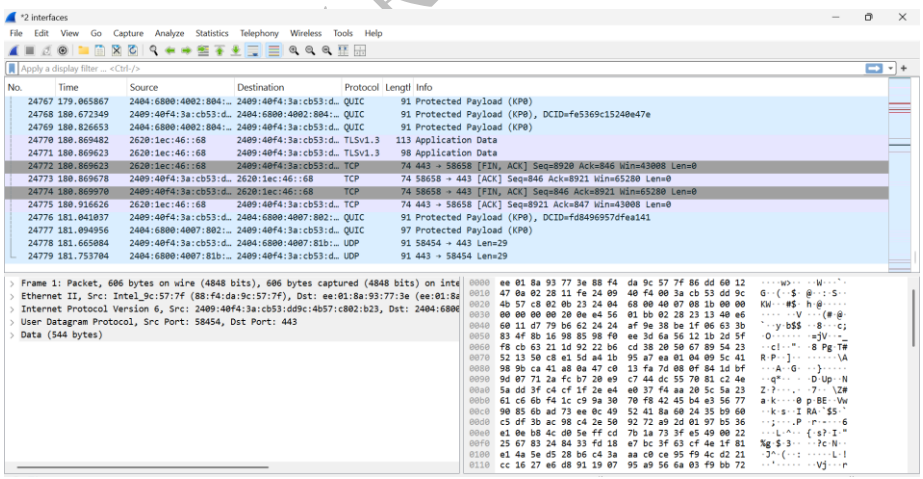
- Launch Wireshark and select the active network interface.
- Start capturing packets.
- Perform network activities (e.g., browsing, ping, DHCP request).
- Stop the capture and save the file.
- Use filters to isolate TCP, UDP, HTTP, ARP, DHCP, ICMP, and DNS traffic.
- Analyze details and packet contents.

Result:
Traffic captured and analyzed; protocol communications are observed for learning or troubleshooting.

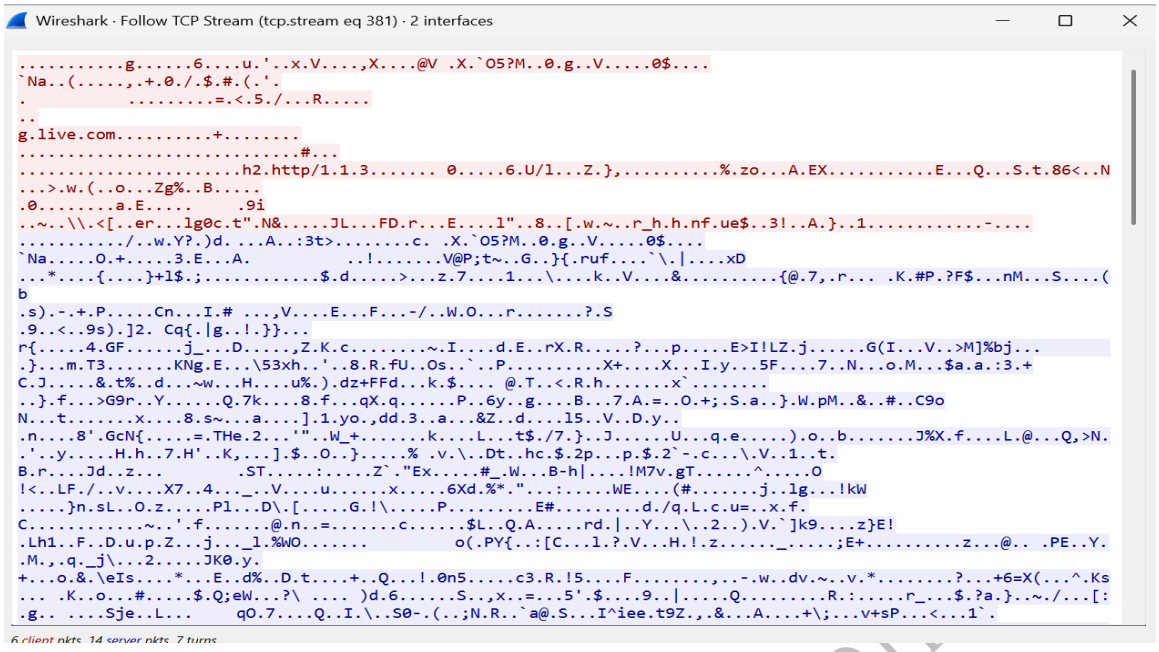
Output:

1. Capture or Open a Packet Capture File

- Start by capturing live traffic via your network interface or open an existing .pcap file.
- Click **File > Open** to load a saved capture file.



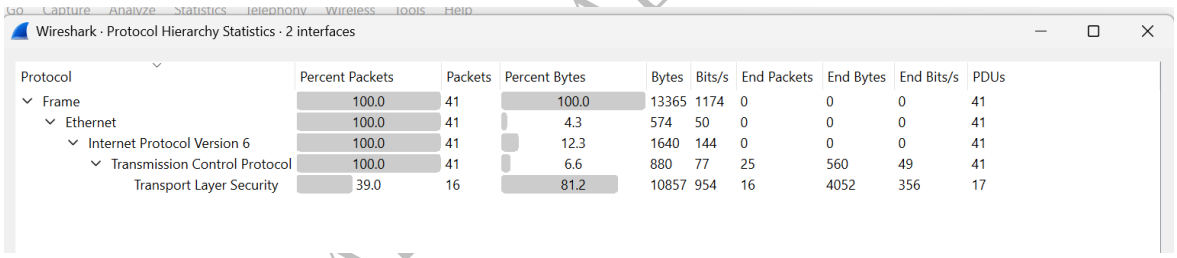
Follow TCP streams



Protocol Hierarchy:

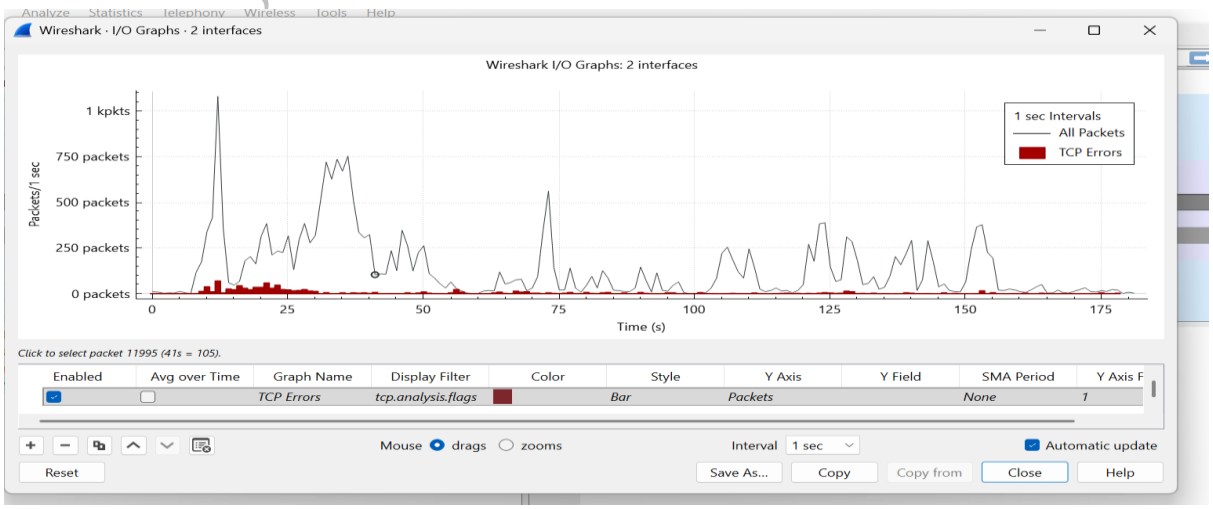
Shows a breakdown of protocols seen in the capture with counts and percentages.

Go to Statistics > Protocol Hierarchy.



I/O GRAPHS;

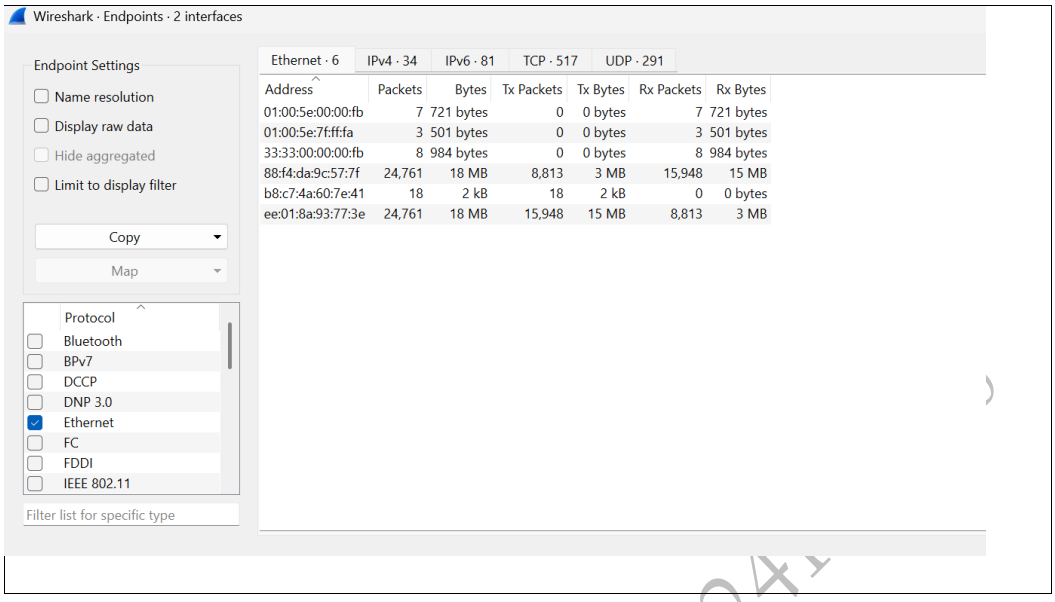
Use statistics > I/O graphs to visualize traffic rate and identify spickes or drops over time



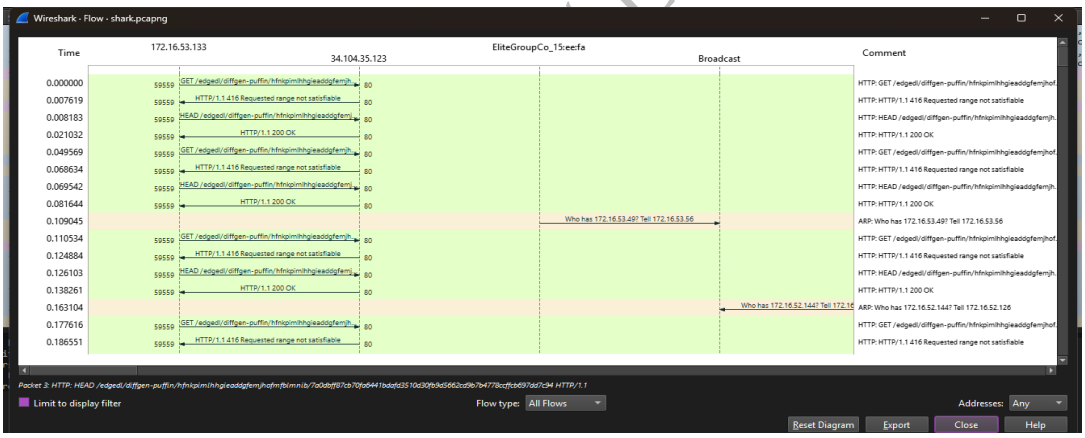
Endpoints:

Lists all endpoints (IPs, MACs) involved in the capture and summarizes traffic per endpoint.

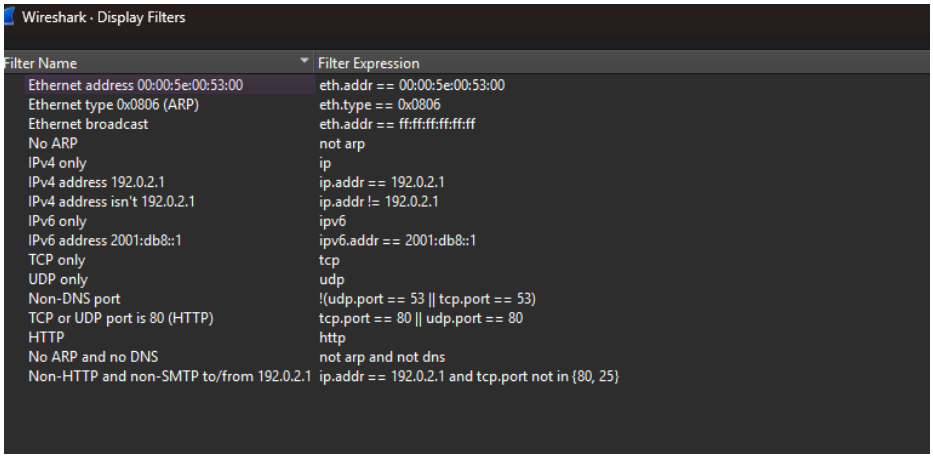
Go to Statistics > Endpoints.



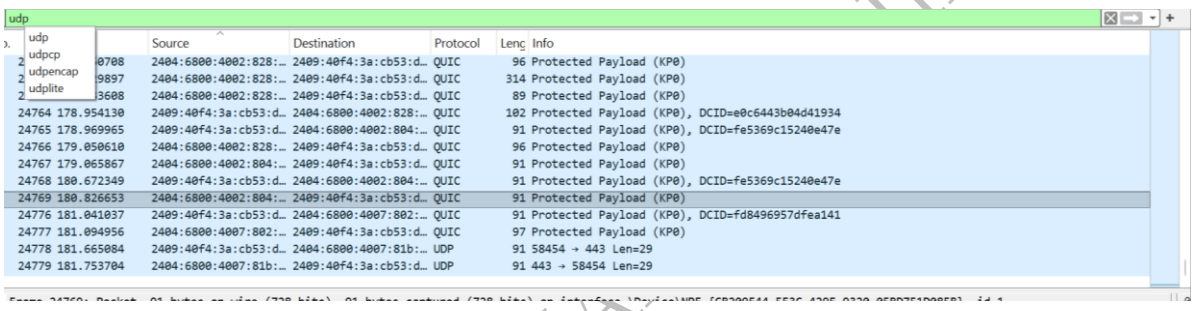
Flow: Depicts directional communication between network hosts, showing data exchanges in sequential context for analysis



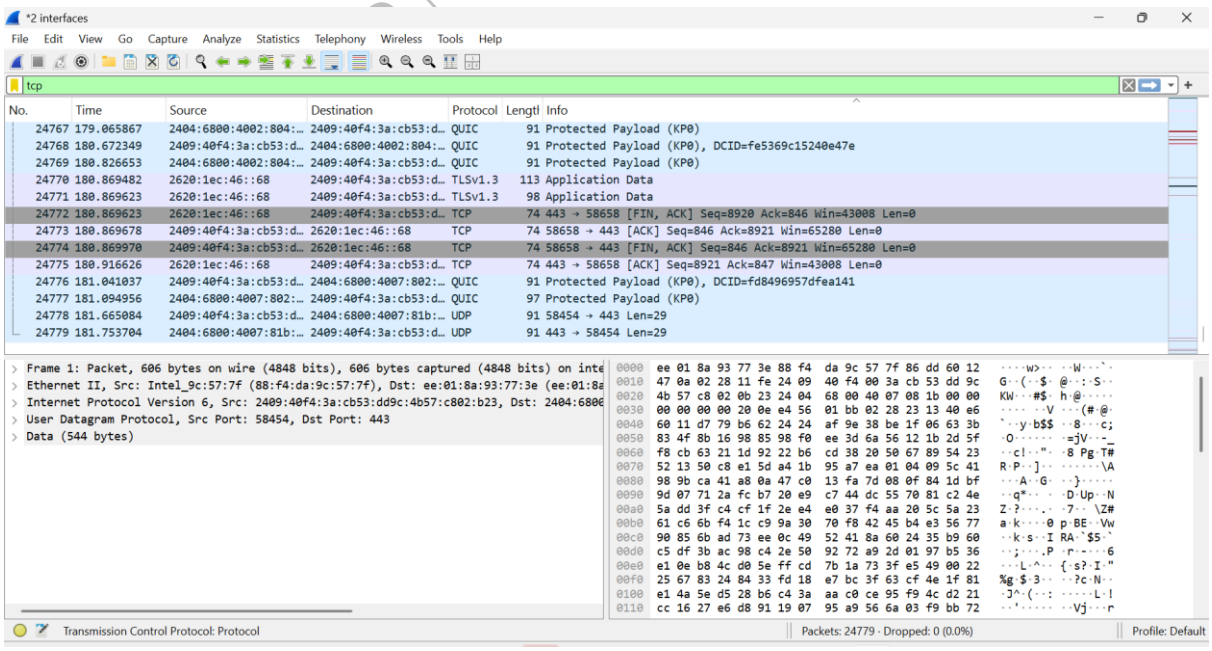
Display Filters: Enable precise viewing of packets by protocol fields, source/destination, or conditions (e.g., tcp.port == 80 or frame.len > 500).



UDP: A connectionless transport protocol providing fast but unreliable message delivery, ideal for real-time or broadcast communications.



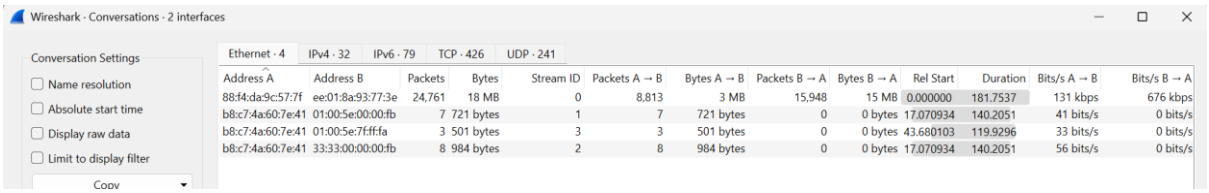
TCP: A connection-oriented transport protocol that ensures reliable data delivery through mechanisms like acknowledgments and retransmissions.



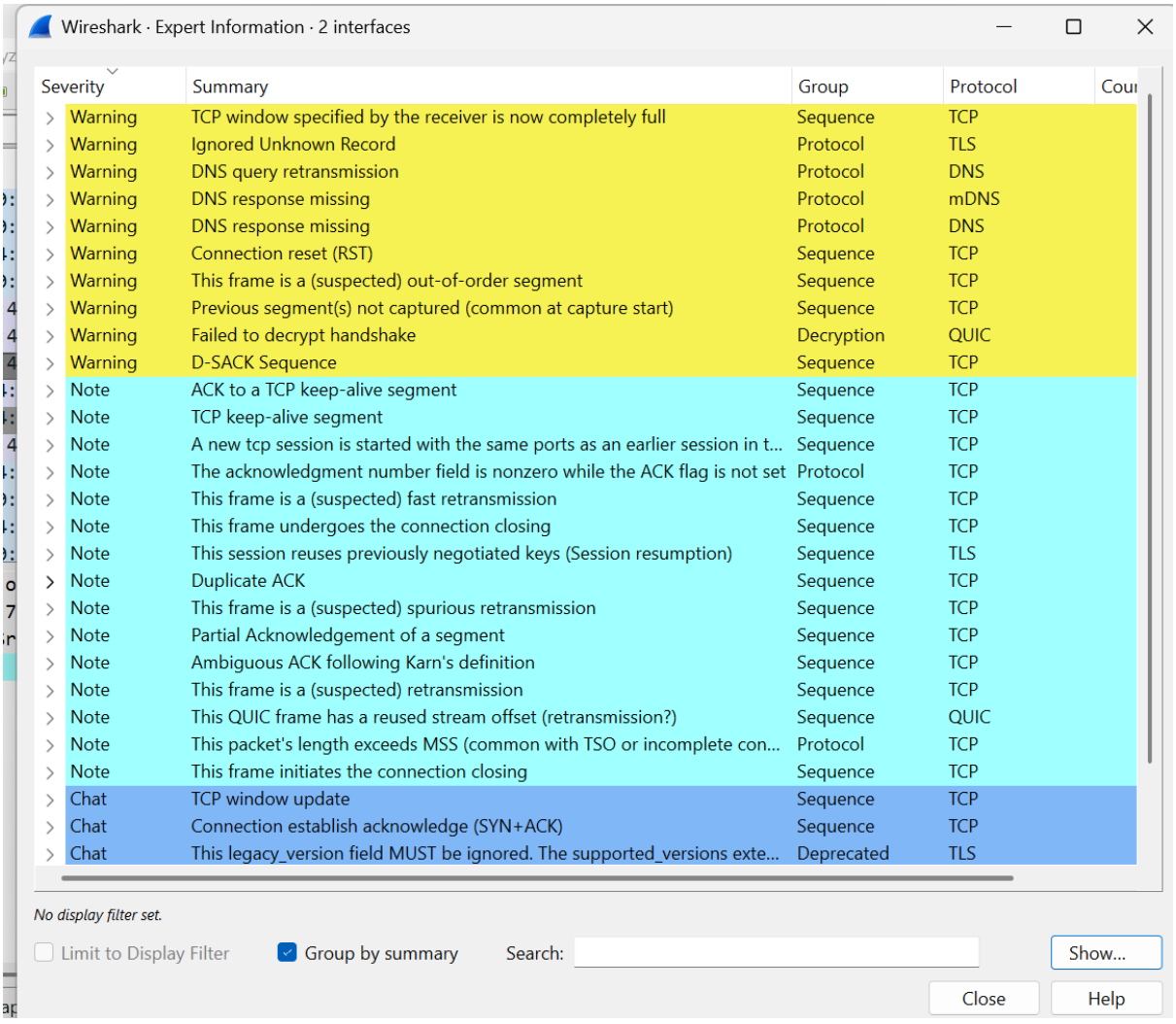
Conversations:

Displays all conversations between IP addresses or MAC addresses. Useful for identifying

communication pairs.
Go to Statistics > Conversations.



Expert Information: Displays protocol anomalies, warnings, and potential issues detected during packet capture for network troubleshooting.



Result

Hence using windows Wireshark,we captured the packets and executed the functions.