TASK 5: CAPTURE AND ANALYZE NETWORK TRAFFIC USING WIRESHARK.

Objective:

The objective of this task is to use Wireshark to capture live network traffic, identify various communication protocols in use, and analyze the packet details.

Tools Used:

- Wireshark.
- Web Browser (Google Chrome).

Procedure:

Step 1. Install Wireshark

- Download and install Wireshark from the official website: https://www.wireshark.org.

Step 2. Start Packet Capture

- Launch Wireshark.
- Select your active network interface (e.g., Wi-Fi or Ethernet).
- Click Start Capturing Packets (the blue shark fin icon).

Step 3. Generate Network Traffic

- While capturing, open a web browser and visit a website (e.g., https://example.com) or use the terminal/command prompt to run ping google.com.

Step 4. Stop the Capture

- After about 1 minute of activity, click the Stop button (red square icon).

Step 5. Filter by Protocol

- Use the filter bar to type protocols such as http, dns, or tcp and hit Enter to view specific packets.

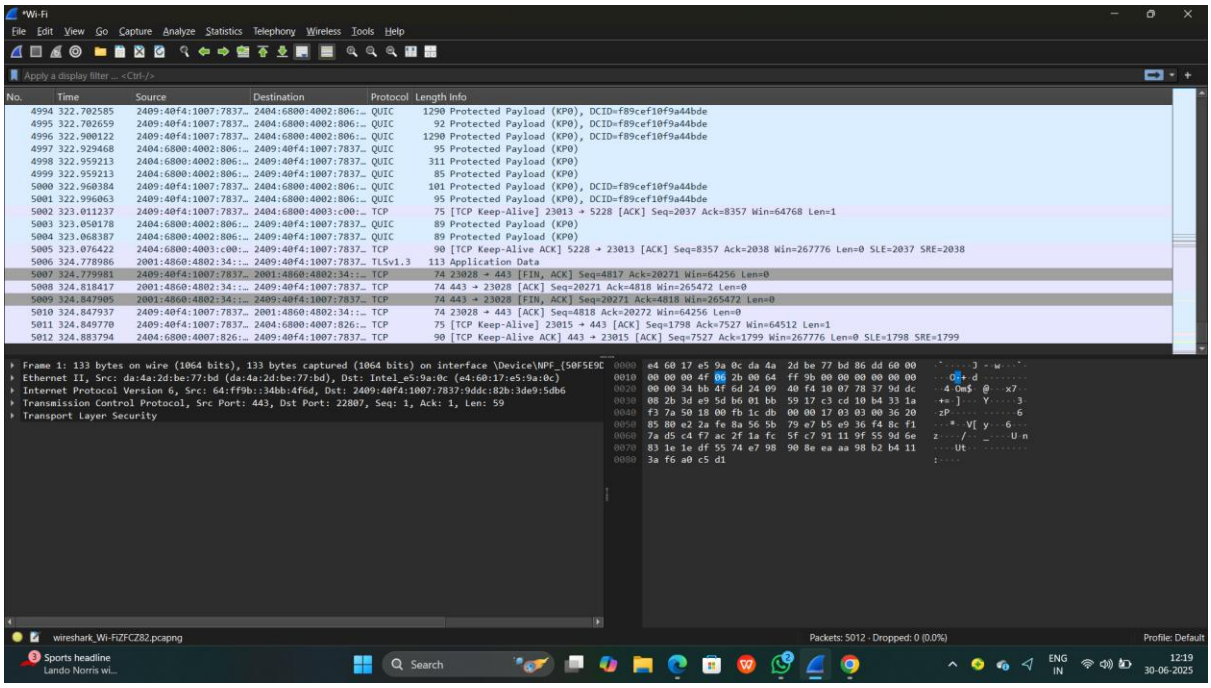
Step 6. Identify Protocols

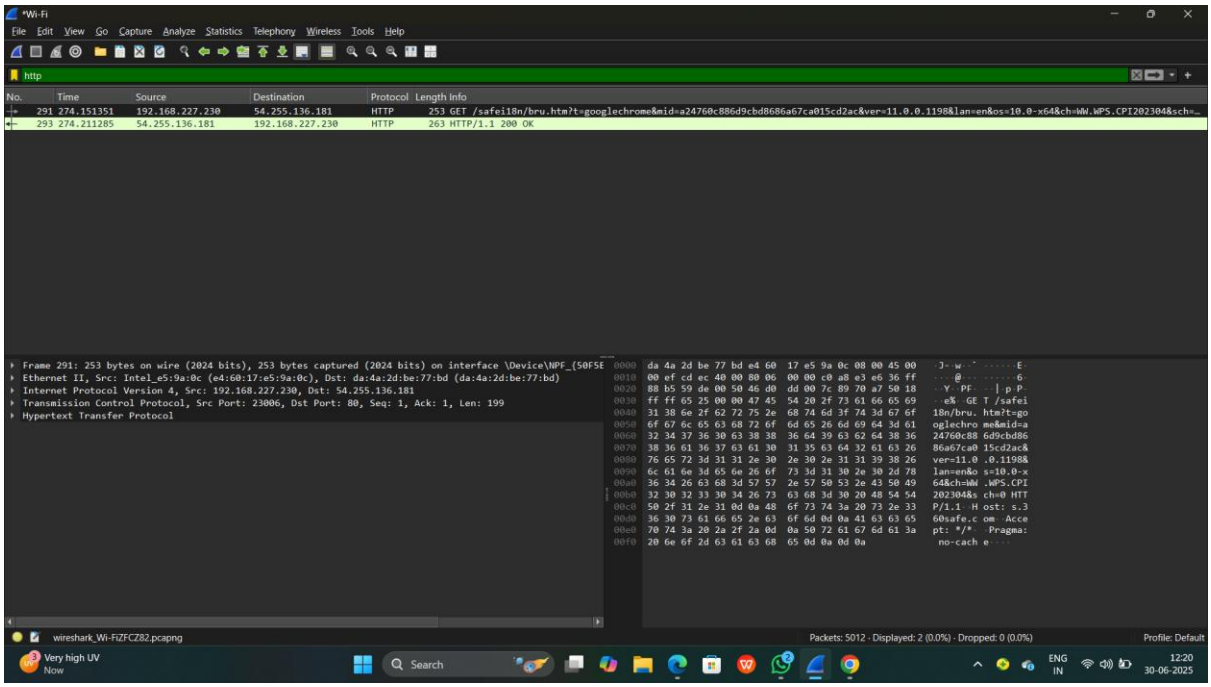
- Examine the captured packets and identify at least three different protocols (e.g., HTTP, DNS, TCP, UDP, ICMP).

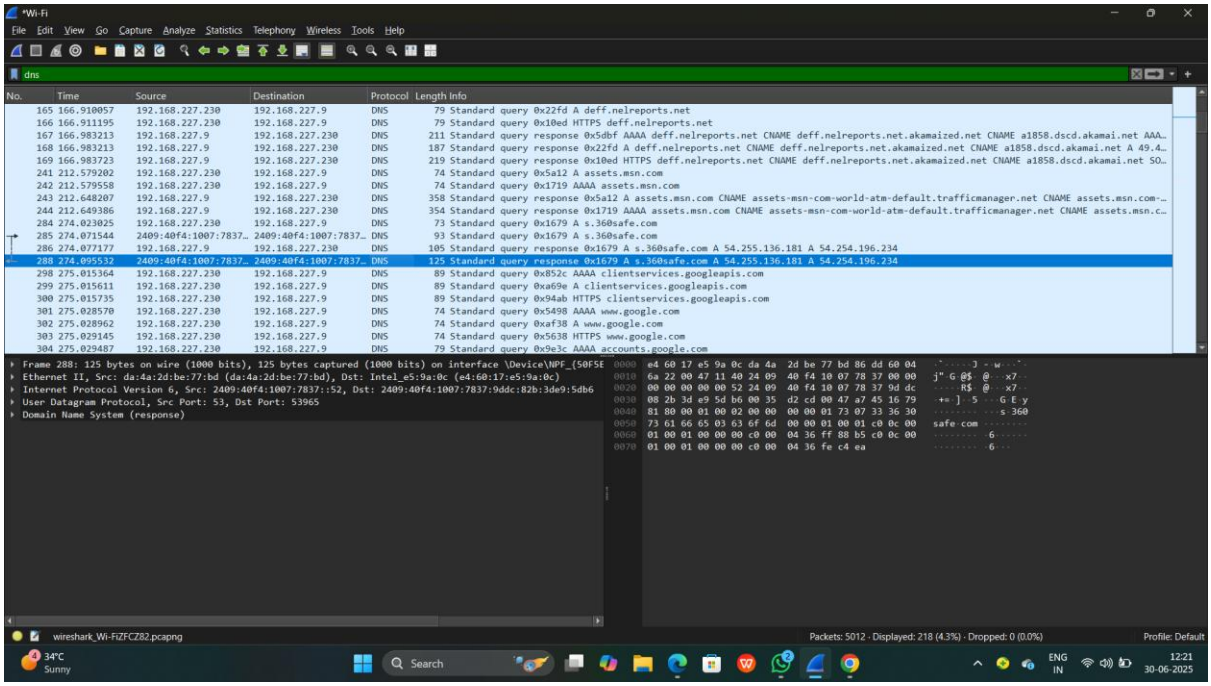
Step 7. Export the Capture

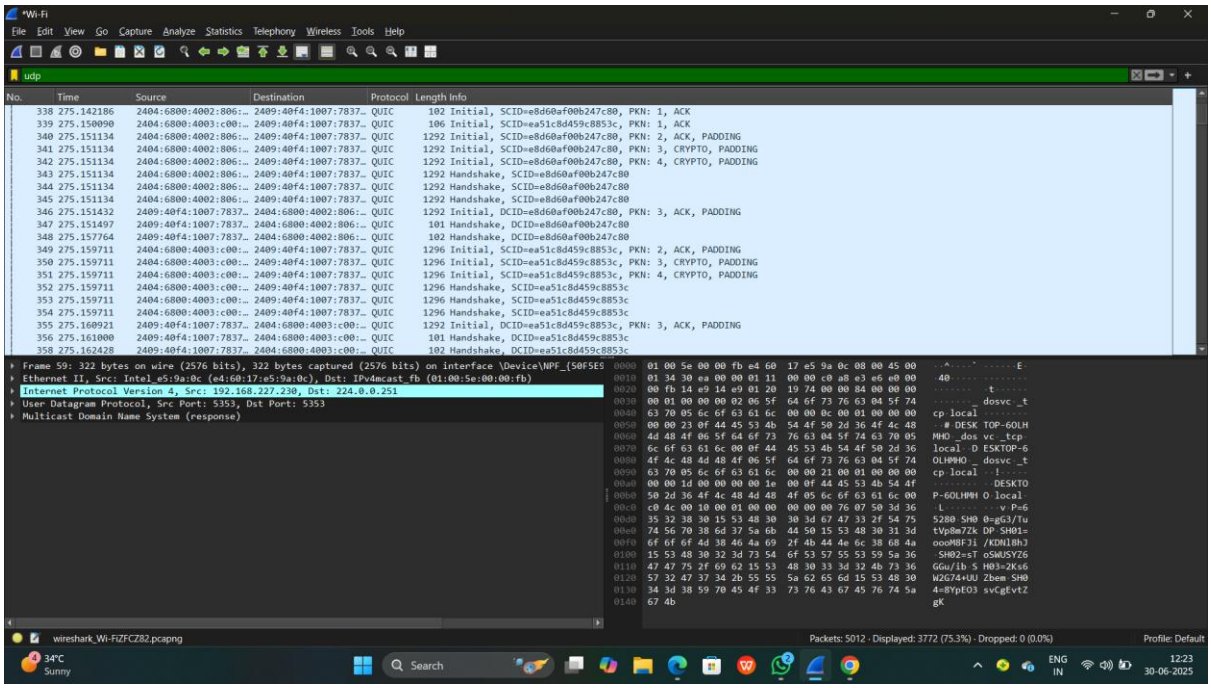
- Go to File > Export Specified Packets.
- Save the capture as a .pcap file

Screenshots:









Conclusion:

The experiment successfully demonstrated the ability of Wireshark to capture and filter live network traffic. Key protocols such as DNS, HTTP, and ICMP were identified, and packet details were analyzed. This task provided a clear understanding of how different protocols work in real-time communication.