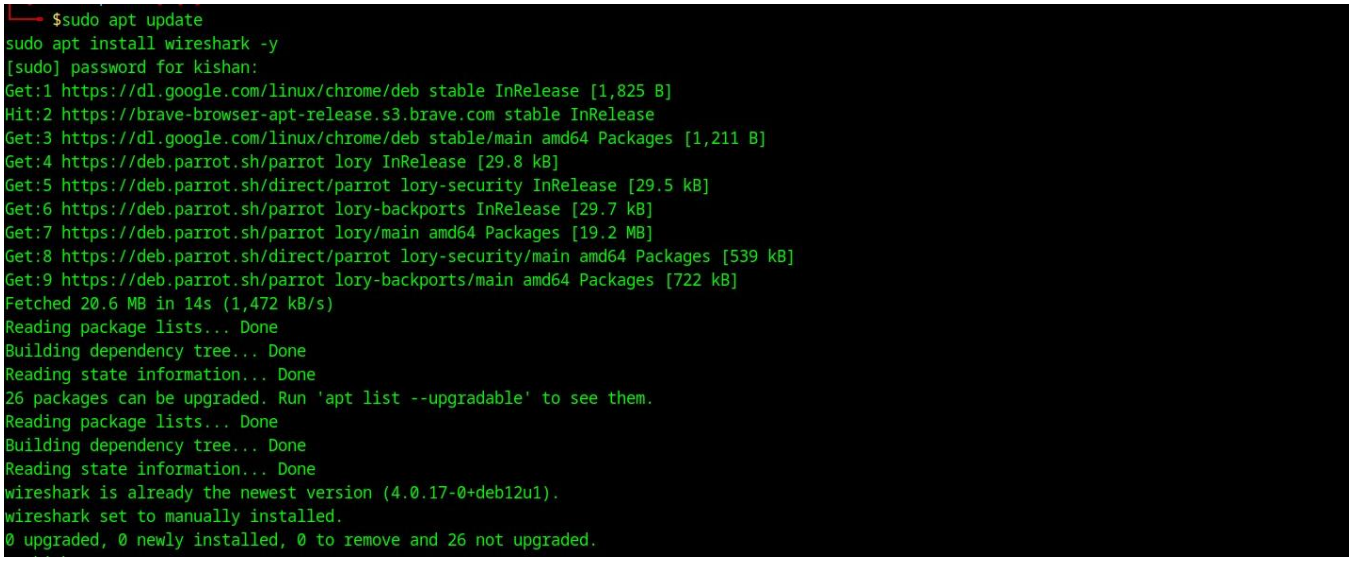
Task 5: Capture and Analyze Network Traffic Using Wireshark

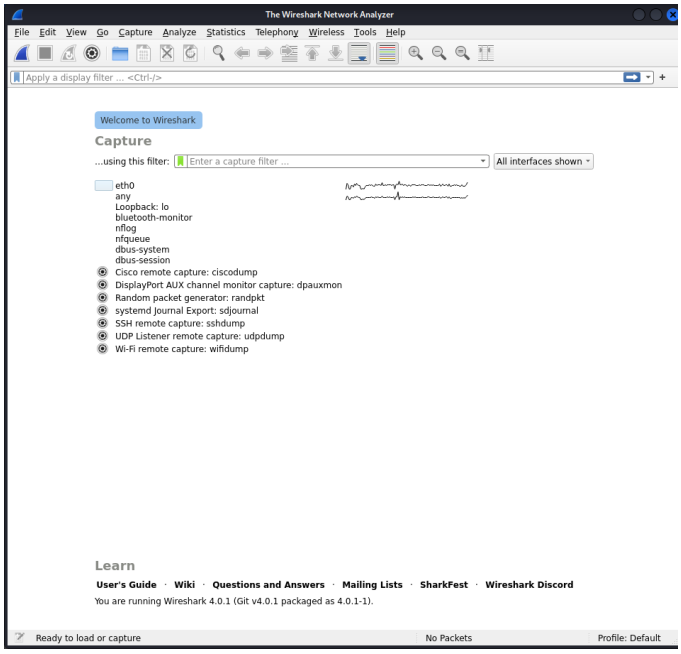
Task Objective : To capture live network packets on a Linux system using Wireshark and analyze the traffic to identify common protocols like HTTP, DNS, TCP, and ICMP.

1. Install Wireshark.



2. Start capturing on your active network interface.

The GUI of wireshark will be like this. Now I will select eth0. This is a wired (Wi-Fi) interface connected on PCI bus 1, slot 0.



3. Browse a website or ping a server to generate traffic.

After starting the capture, a new terminal window was opened and the following command was run to ping Google, which generates ICMP packets.

ping google.com -c 5

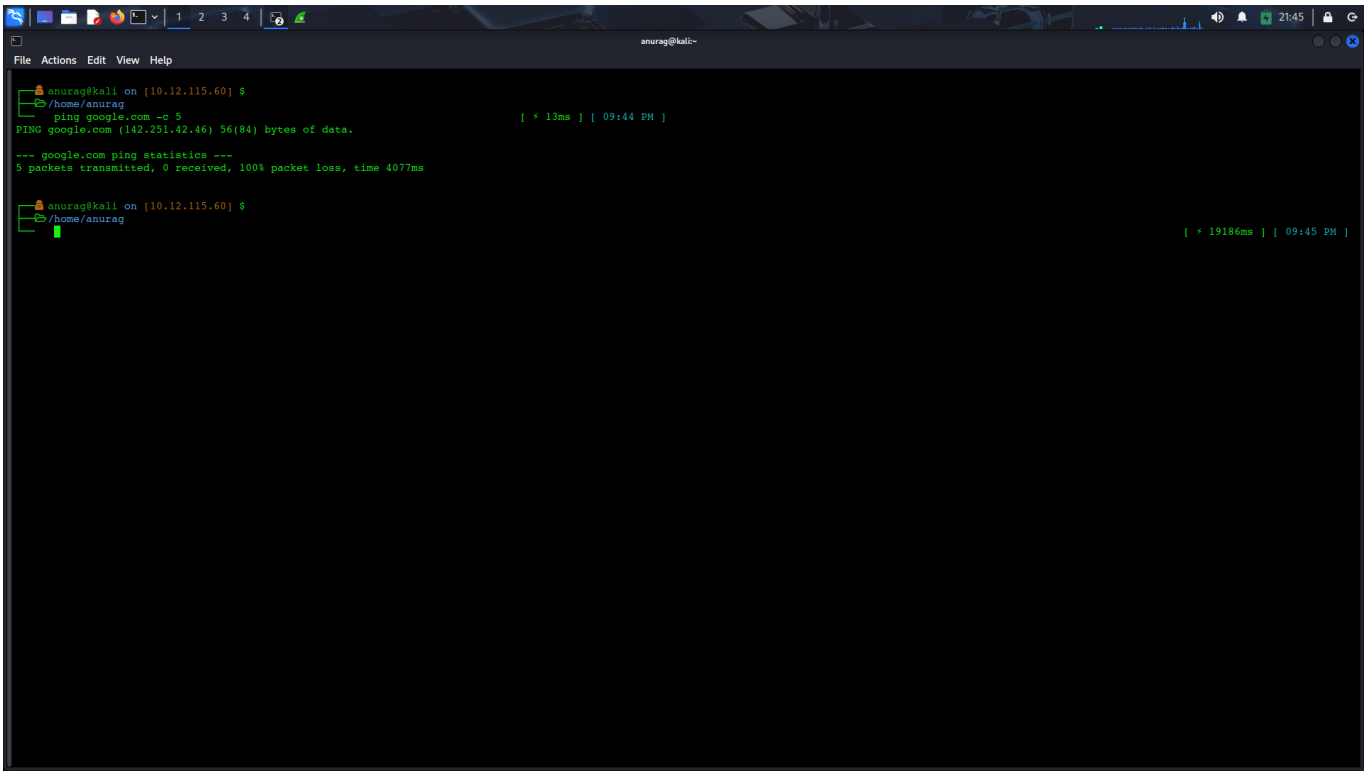
Then, to generate HTTP, HTTPS, and DNS traffic, a website was accessed using

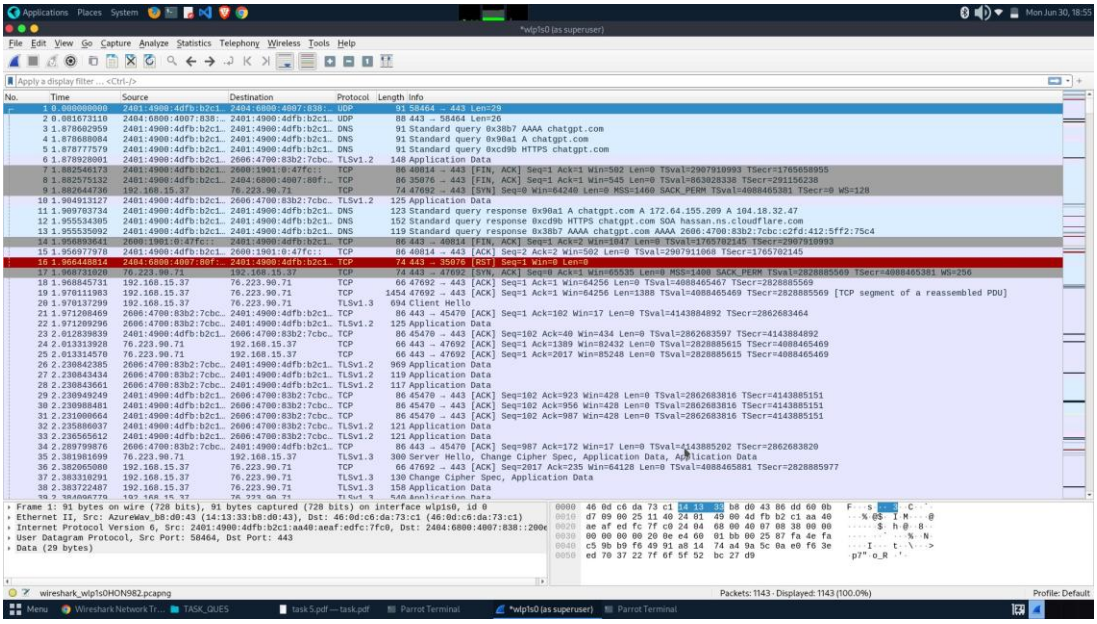
curl https://example.com

This simulates real-world browsing activity and helps capture various protocol packets like DNS (for name resolution), TCP (for reliable transport), and HTTP/HTTPS (for web content).

This is the interface where i have pressed the commands

This is the traffic captured



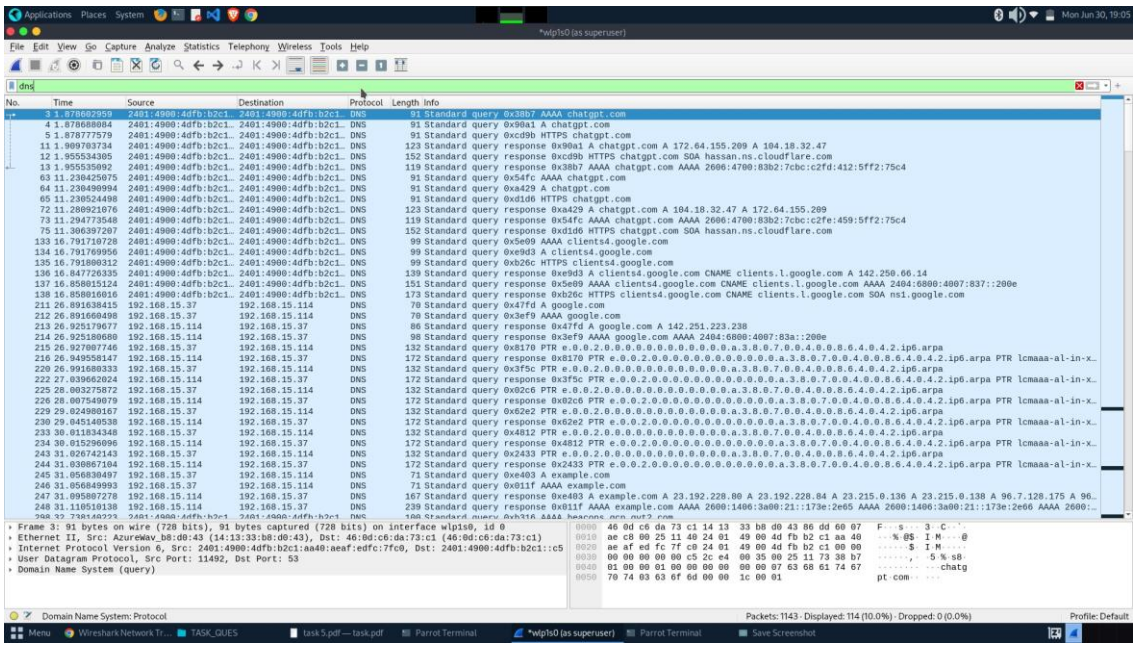


4. Stop capture after a minute.

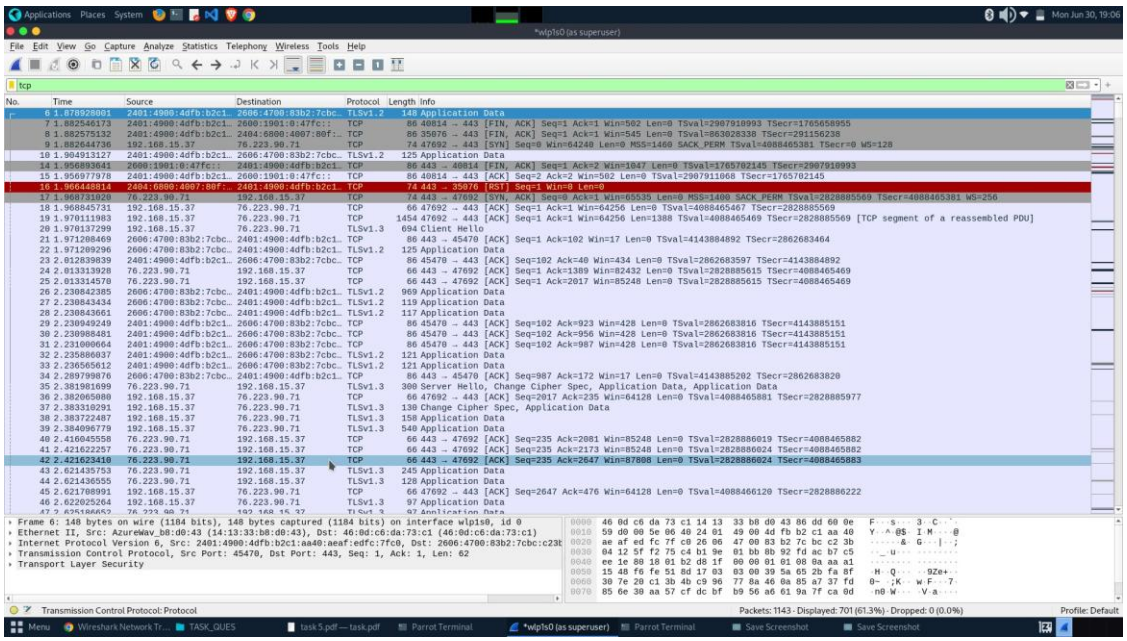
I have stopped it after a min

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

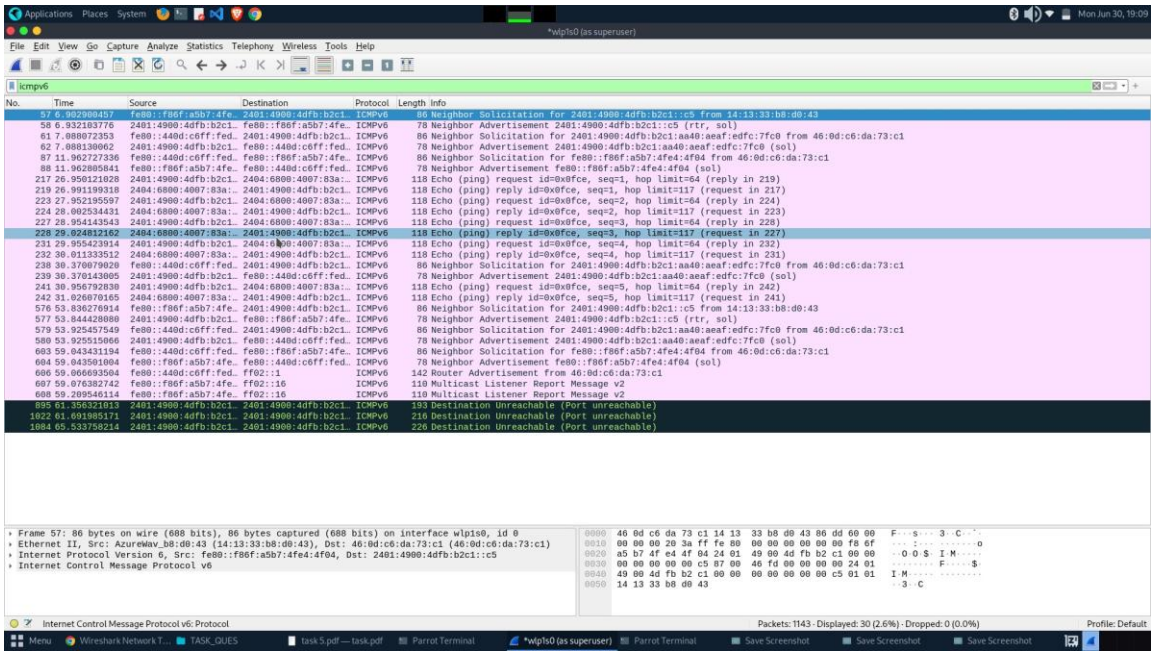
Used the Display Filter bar at the top of Wireshark to isolate specific types of packets.



dns → filters DNS queries and responses



tcp → shows only TCP traffic



icmp → shows ping request/reply

No Http traffic was captured

6. Identify at least 3 different protocols in the capture.

I have ICMP , TCP and DNS packets that were captured on my wire shark i will say what are those and what will they do shortly

1. ICMP (Internet Control Message Protocol)

- **Purpose:** Used for network diagnostics.
- **Example:** ping google.com sends ICMP Echo Requests and receives Echo Replies.
- **Use Case:** Helps check if a host is reachable and measures round-trip time.

2. TCP (Transmission Control Protocol)

- **Purpose:** Ensures reliable and ordered data delivery between devices.
- **Example:** Used in protocols like HTTP, HTTPS, FTP.
- **Use Case:** Establishes a connection (3-way handshake), ensures all data reaches correctly.

3. DNS (Domain Name System)

- **Purpose:** Resolves human-readable domain names into IP addresses.
- **Example:** When accessing example.com, your system sends a DNS query to find its IP.
- **Use Case:** First step in web browsing — without DNS, the browser can't find the server.

7. Export the capture as a .pcap file.

I have exported the capture

8. Summarize your findings and packet details.

During the network capture, three main types of packets were identified: ICMP, TCP, and DNS. Each of these serves a distinct role in network communication:

ICMP (Internet Control Message Protocol)

- Used for diagnostic and error-reporting functions.
- Commonly seen in tools like ping.
- Helps determine if a host is reachable and measures latency.

TCP (Transmission Control Protocol)

- A connection-oriented protocol that ensures reliable data transfer.
- Used in web browsing (HTTP/HTTPS), file transfers (FTP), emails, etc.
- Establishes a connection using a 3-way handshake before transmitting data.

DNS (Domain Name System)

- Resolves domain names (like google.com) to their respective IP addresses.
- Works before any website or online service can be accessed.