Task – 5

**Capture and Analyze Network Traffic Using Wireshark**

Objective:  
Capture live network packets using Wireshark, identify basic protocols, and analyse traffic types.

Step 1: **Install and Lunch the Wireshark**

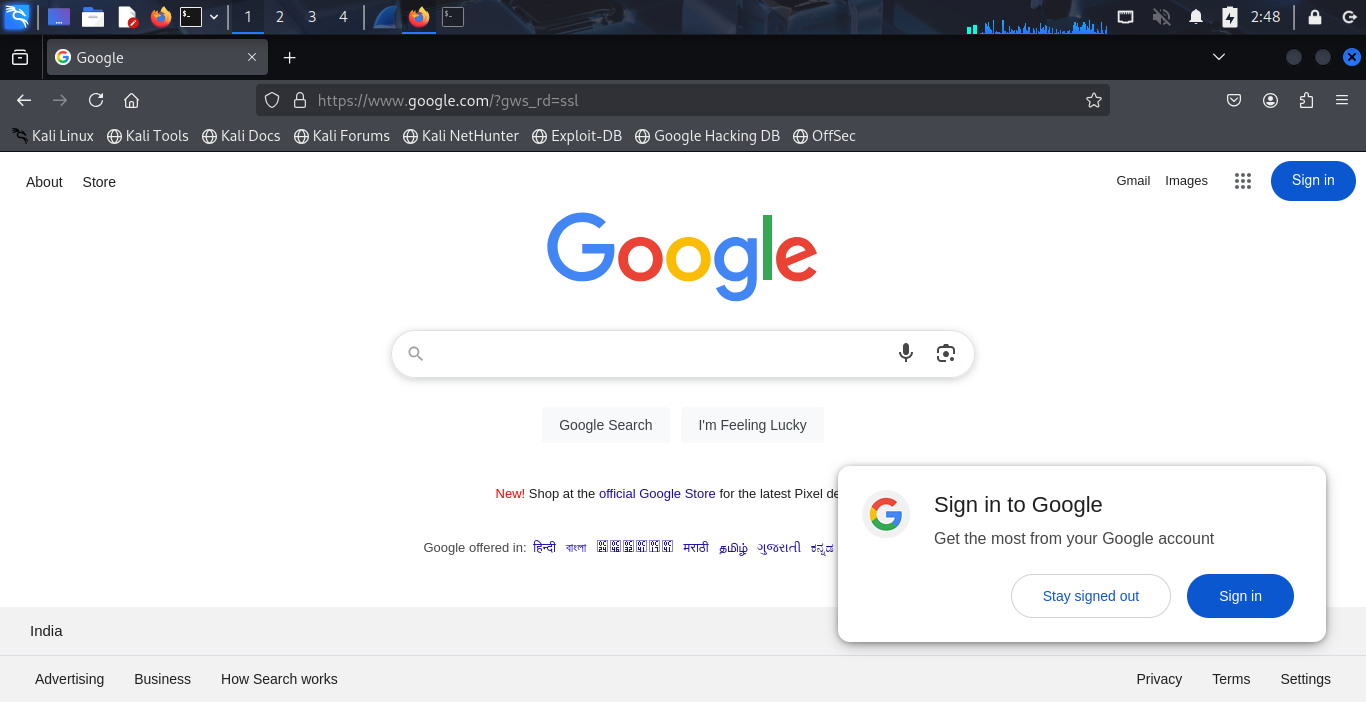
* Install Wireshark, In kali Linux we have default Wireshark tool.
* Launch the Wireshark tool.

Step 2: **Start Capturing Network Traffic**

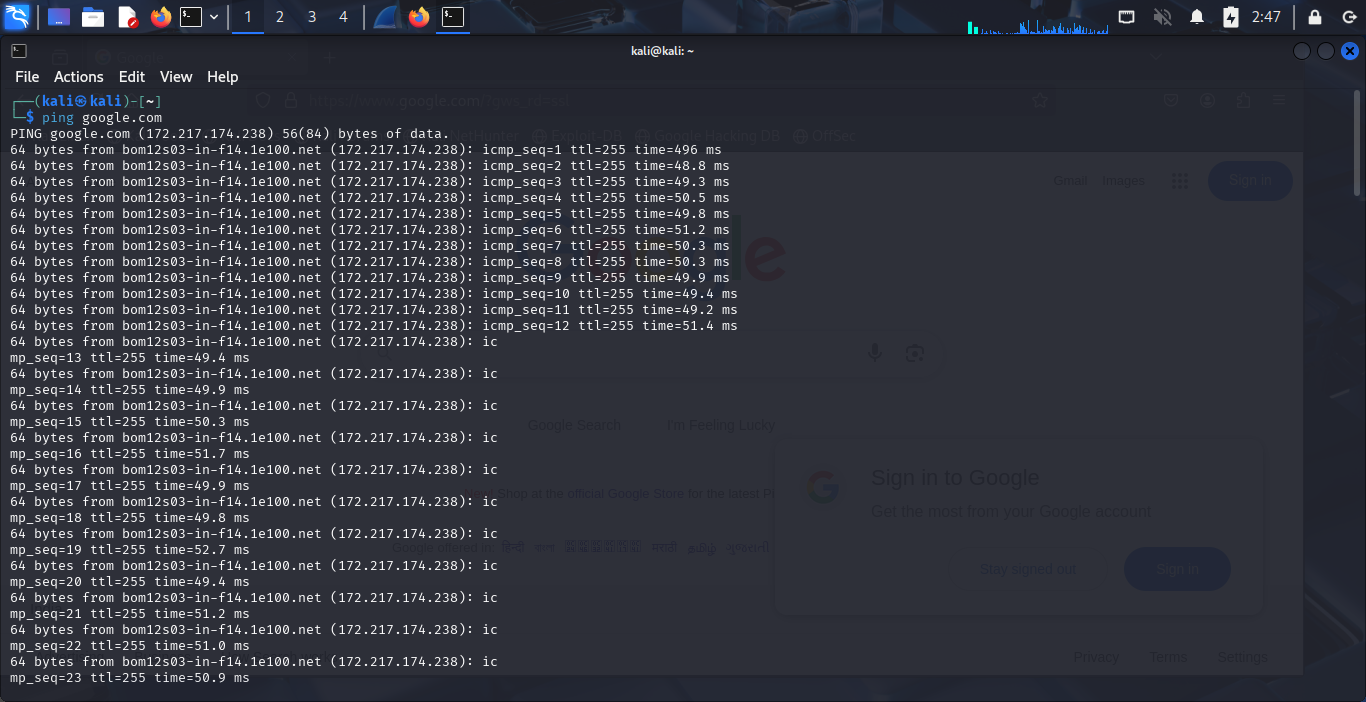
* Open Wireshark.
* Select the active interface (Wi-Fi or Ethernet) from the list.
* Click start button to begin capture the packets.

Step 3: **Generate Network Traffic**

* Open a web browser and visit website we want to capture packet in whireshark (e.g., [https://www.google.com](https://www.google.com/)).
* Alternatively, open a terminal and ping a server.



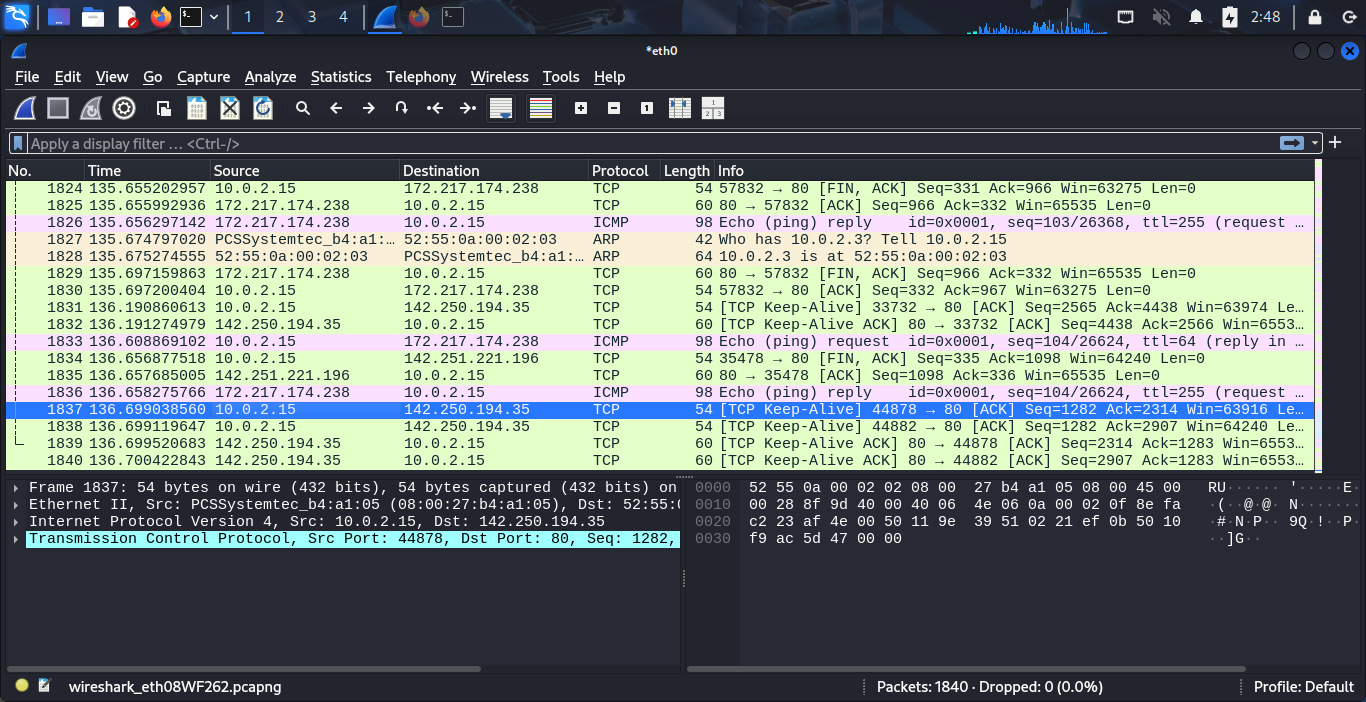
Web browser Screenshot



Terminal Screenshot

Step 4: **Stop the Capture**

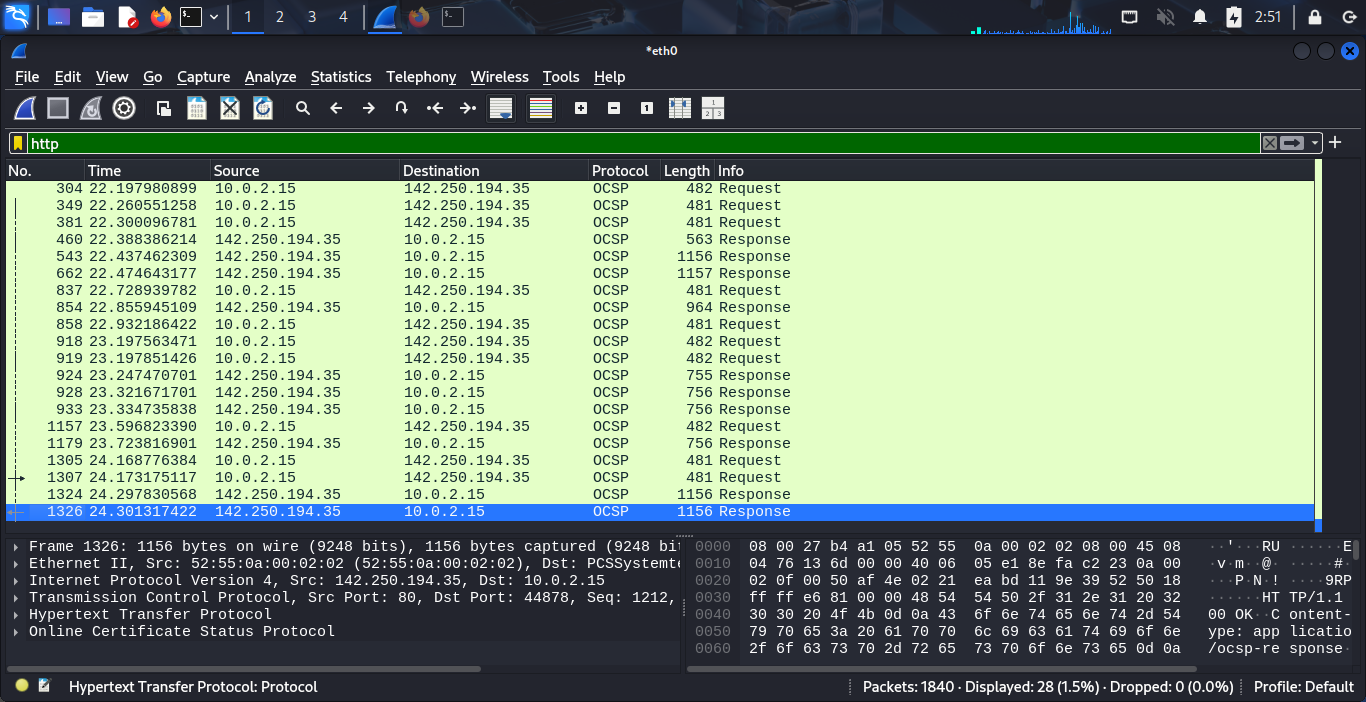
* After about a minute, click the **Stop** button in Wireshark to halt the capture.



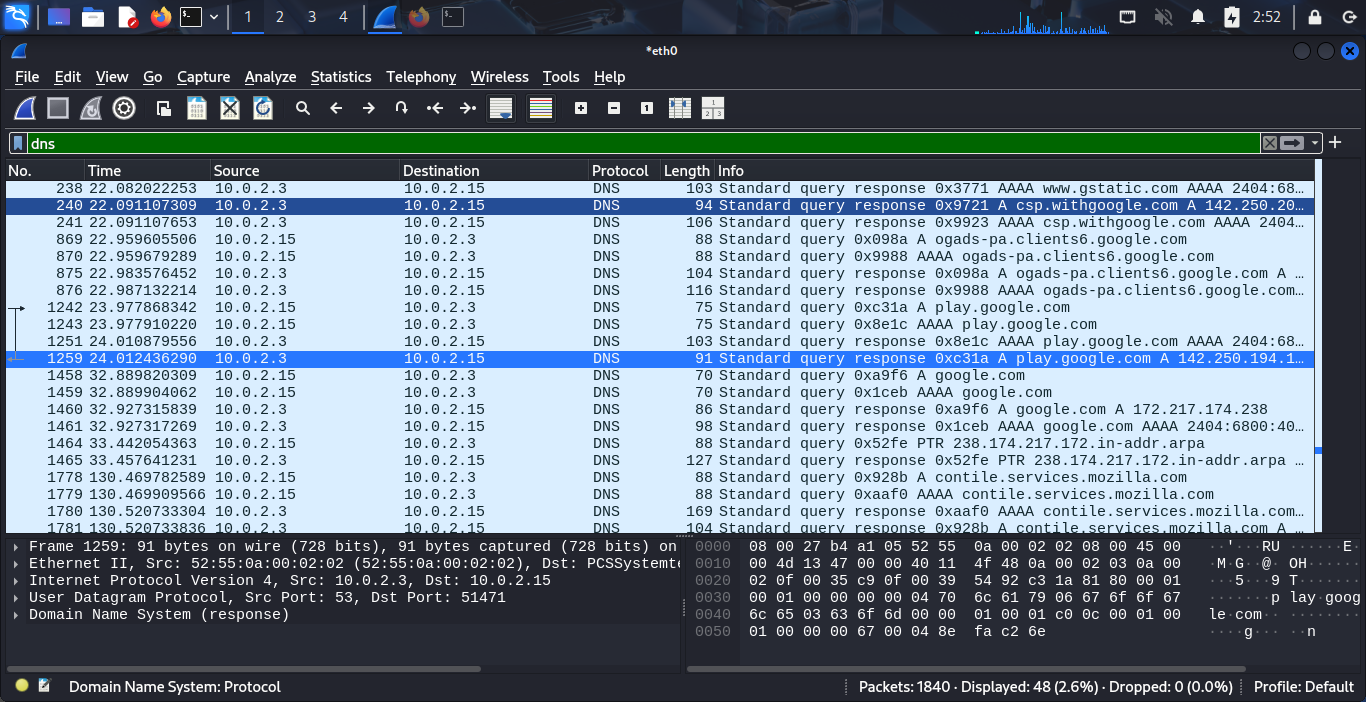
Whireshark Screenshot

Step 5: **Analyze Captured Packets**

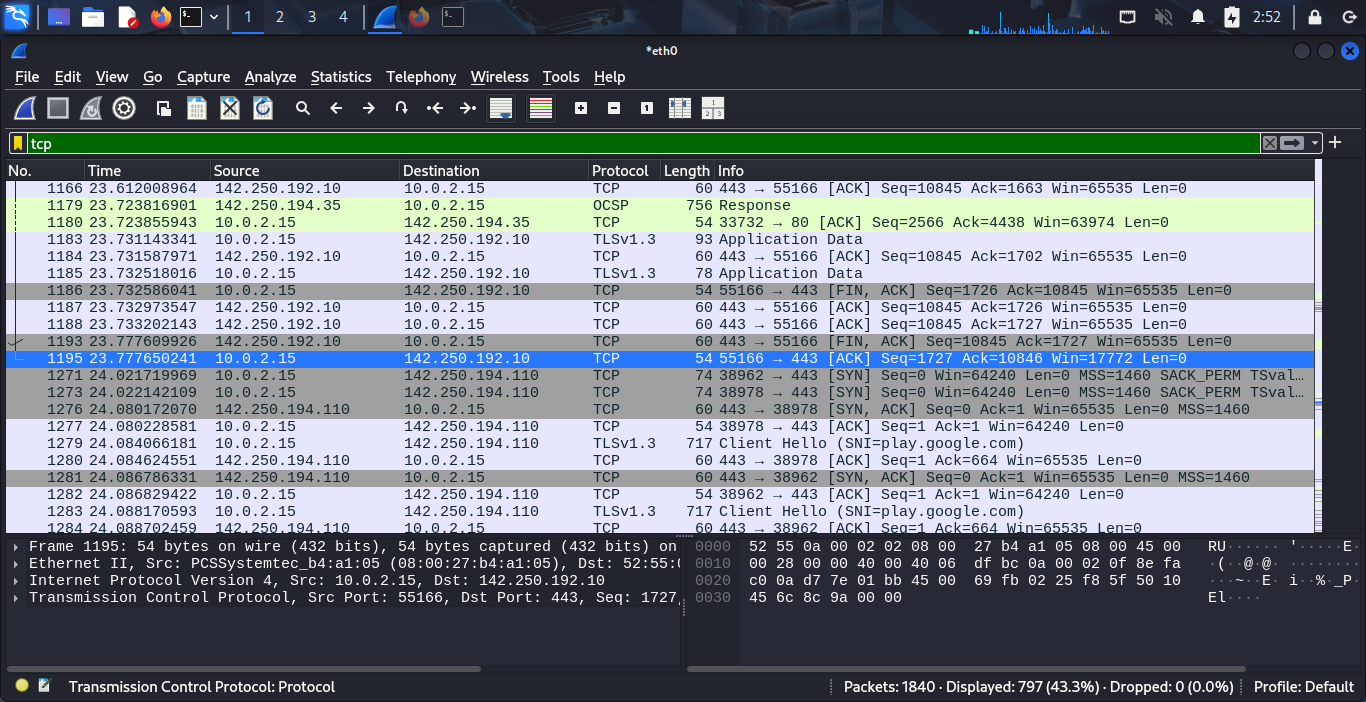
* Observe the list of captured packets in the main window.
* Use Wireshark’s filter bar to isolate specific protocols:
* http for HTTP traffic.
* dns for DNS queries.
* tcp for TCP packets.
* udp for UDP packets.



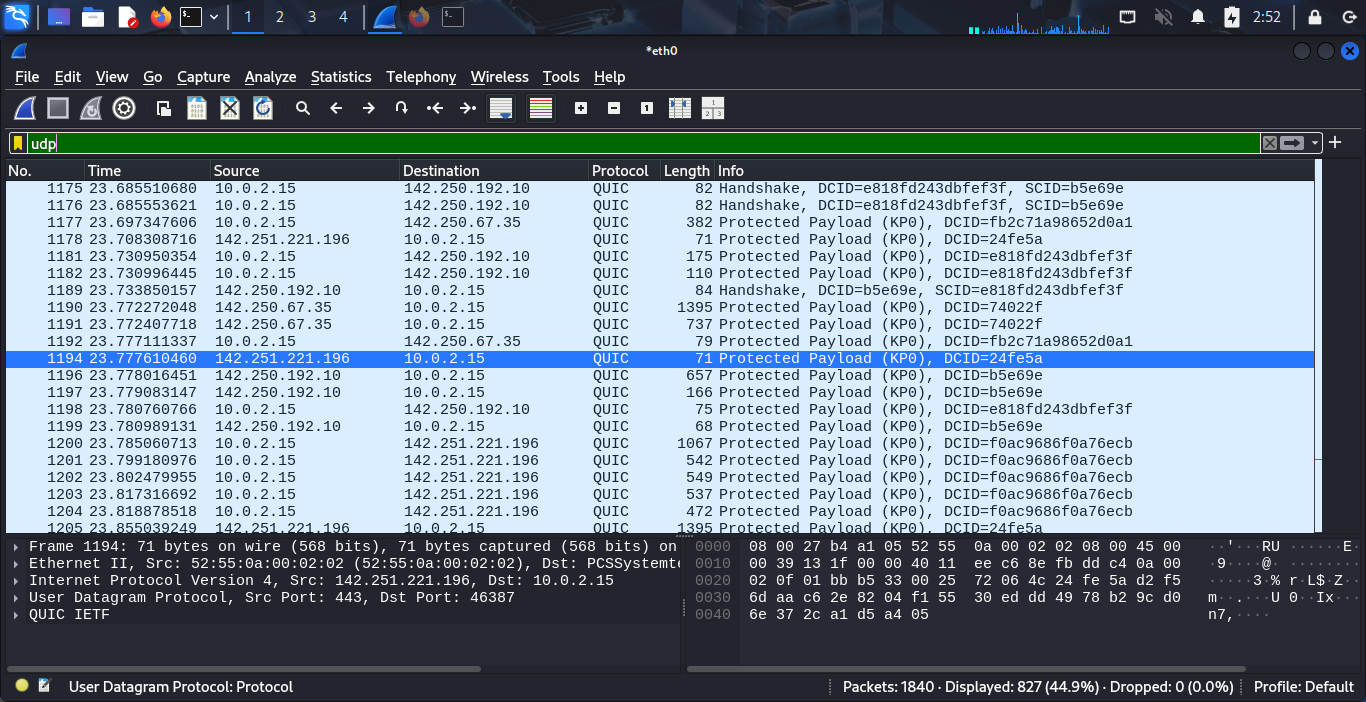
HTTP Capture Screenshot



DNS Capture Screenshot



TCP capture Screenshot



UDP Capture Screenshot

Step 6: **Export the Capture**

* Go to **File > Export Packet Dissections > As PCAP**.
* Save the file.

Step 7: **Summarize Findings**

* Protocols identified (e.g., HTTP, DNS, TCP).
* Observations (e.g., source/destination IPs, packet sizes).
* Screenshots of filtered packets.