Wireshark Report

Objective

To perform a live packet capture using Wireshark, apply filters to analyze specific protocols, save the results as a .pcap file, and summarize findings on commonly observed protocols including UDP, DNS, TCP, TLS, and ICMP.

Steps Performed:

1. Opened Wireshark and Selected Interface

- Wi-Fi interface was selected
- Live capture started using the main capture button

2. Generated Network Activity

- Visited websites (e.g., Google, YouTube)
- Used ping google.com to generate ICMP
- DNS queries were triggered automatically during browsing

3. Stopped and Saved the Capture

- Saved as:

  wireshark_packet_capture.pcapng

4. Applied Protocol Filters and Analyzed Packets

Summary of Findings:

The capture revealed active DNS queries over UDP, secure web traffic using TLS over TCP, and ICMP echo requests via ping. All DNS queries succeeded with no errors or retransmissions. Packets showed standard headers and flags (e.g., SYN, ACK, Echo Request), indicating a healthy and correctly functioning network environment.