Network Traffic Analysis with Wireshark

The primary objective of this task was to capture live network packets using Wireshark on Kali Linux, analyze the captured traffic, and identify at least three different network protocols.

Tools Used

- **Operating System:** Kali Linux
- **Software:** Wireshark

Procedure

The entire task was performed within the Kali Linux environment. The following steps detail the process from launching Wireshark to saving the final capture file.

1. **Launched Wireshark:** Wireshark was started from the Kali Linux terminal with root privileges to ensure access to network interfaces. The command used was:

```
sudo wireshark
```

2. **Started Packet Capture:** From the Wireshark interface, the eth0 network interface was selected as the active connection for packet sniffing. The capture was then initiated.
3. **Generated Network Traffic:** To create a diverse set of network packets for analysis, two actions were performed:
   a. **Ping Command:** The ping command was used in the terminal to generate ICMP traffic by sending packets to Google's public DNS server.

```
ping 8.8.8.8
```

   b. **Web Browse:** A web browser was used to visit a website to generate DNS, TCP, and HTTP/HTTPS traffic.
4. **Stopped and Saved Capture:** After approximately one minute, the packet capture was stopped. The captured data was then saved as

task5_capture.pcapng for analysis and submission.

Analysis and Protocols Identified

The captured packets were analyzed by applying filters within Wireshark to isolate specific protocols. The following three protocols were successfully identified:

- **TCP (Transmission Control Protocol):** A significant portion of the traffic consisted of TCP packets, which are connection-oriented and ensure reliable data delivery. These packets were primarily generated by Browse a website, showing the three-way handshake process (SYN, SYN-ACK, ACK) used to establish a connection.
- **DNS (Domain Name System):** DNS query packets were observed when the web browser translated the website's domain name into an IP address. These packets are fundamental for navigating the internet, and both UDP and TCP were seen as transport protocols for these queries.
- **ICMP (Internet Control Message Protocol):** This protocol was generated by the ping command. ICMP is used by network devices to send error messages and operational information. The capture clearly showed the "Echo request" and "Echo reply" packets exchanged between my system and the target server (8.8.8.8).