**Task**: Task 5 – Capture and Analyze Network Traffic  
**Tool Used**: Wireshark

**Name**: Anshool Naik  
**Operating System**: Kali Linux  
**Capture Duration**: 1 minute  
**Capture File**: network\_capture\_task5.pcapng

**Objective**

To capture live network traffic using Wireshark and identify at least 3 different network protocols observed during typical user activity like browsing or pinging a server.

**Steps Performed**

1. Opened Wireshark and selected the active interface: eth0.
2. Started live packet capture.
3. Generated traffic by:
   * Visiting a website (e.g., example.com).
   * Running ping google.com in the terminal.
4. Stopped the capture after one minute.
5. Filtered and analyzed packets based on protocol.
6. Identified multiple network protocols and saved the capture file as .pcapng.

**Protocols Identified**

| **Protocol** | | **Description** | | **Role in Capture** |
| --- | --- | --- | --- | --- |
| **TCP** | Transmission Control Protocol | | | Used for establishing web connections (port 80/443) |
| **DNS** | Domain Name System | | | Resolved hostnames like google.com to IP |
| **ICMP** | Internet Control Message Protocol | | Seen during ping google.com testing | |