**Capture and Analyze Network Traffic Using Wireshark**

**OBJECTIVE:** **Capture live network packets and identify basic protocols and traffic types.**

**METHOD:**

1. **Installed Wireshark on Windows (version 4.4.8).**
2. **Selected the active network interface – Wi-Fi, since the system was connected to the internet via mobile hotspot.**
3. **Started packet capture by double-clicking the Wi-Fi interface.**
4. **Generated network traffic by browsing various websites and performing a ping google.com command in Command Prompt.**
5. **Captured packets for approximately one minute to ensure a variety of protocols appeared in the results.**
6. **Stopped the capture using the red square button in Wireshark.**
7. **Applied protocol filters (e.g., tcp, quic, icmpv6) in the filter bar to isolate and analyze specific packet types.**
8. **Identified at least three protocols based on the filtered views.**
9. **Saved the capture as a .pcap file for documentation and future reference.**
10. **Took screenshots of the filtered protocol views for inclusion in the report and GitHub repository.**

**FINDINGS: During the analysis of the captured network traffic, the following protocols were identified:**

1. **TCP (Transmission Control Protocol)**
   * **Description: A connection-oriented protocol that ensures reliable data transmission between devices. It uses acknowledgments (ACK) and retransmissions to maintain data integrity.**
   * **Example from Capture: Source: 64:ff9b::d6b:69e → Destination: 2409:408c:2e9d:4211... with flags [ACK].**
2. **QUIC (Quick UDP Internet Connections)**
   * **Description: A modern transport protocol developed by Google, built on top of UDP, designed for fast and secure connections (commonly used by Chrome, YouTube, and Google services).**
   * **Example from Capture: Multiple Protected Payload (KPQ) packets exchanged between client and server over UDP port 443.**
3. **ICMPv6 (Internet Control Message Protocol for IPv6)**
   * **Description: Used for diagnostic and error-reporting functions in IPv6 networks. It is commonly seen in ping tests and neighbor discovery operations.**
   * **Example from Capture: Neighbor Solicitation and Neighbor Advertisement messages between local IPv6 addresses.**

**CONCLUSION:**

**This task provided practical experience in using Wireshark to capture and analyze live network traffic. By applying protocol filters, it was possible to identify and study TCP, QUIC, and ICMPv6 traffic patterns. The exercise improved understanding of how different protocols function, how they appear in packet captures, and how such analysis can be applied for network troubleshooting and cybersecurity investigations.**