**Task 5 – Network Traffic Analysis Report**

**Objective:**  
 Capture live network packets using Wireshark and identify at least three different protocols in the captured data.

**Procedure:**

1. Installed and opened **Wireshark** on the active Wi-Fi interface.
2. Started packet capture.
3. Generated traffic by:
   * Browsing multiple websites (HTTPS connections).
   * Running the command:

nginx

CopyEdit

ping google.com

1. Stopped capture after approximately 60 seconds.
2. Applied protocol filters (icmp, tcp, tls, quic) to inspect specific traffic types.
3. Saved capture as task5\_network\_capture.pcap.

**Protocols Identified & Observations:**

1. **TCP (Transmission Control Protocol)**
   * Purpose: Reliable transport layer protocol for establishing connections and ensuring data delivery.
   * Observation: Seen between my local IP 192.168.0.140 and external servers such as 52.104.144.41.
   * Commonly used for HTTPS, HTTP, and other application protocols.
2. **TLSv1.3 (Transport Layer Security)**
   * Purpose: Encrypts communication over the internet for security and privacy.
   * Observation: Detected on TCP port 443, securing HTTPS traffic during web browsing sessions.
   * Included “Server Hello” and encrypted application data.
3. **ICMP (Internet Control Message Protocol)**
   * Purpose: Used for diagnostics and network testing (ping).
   * Observation: Echo requests sent to Google’s IP 142.250.77.110 and replies received.
   * Packet Details: ID 0x0001, Sequence numbers 256–1024, TTL values 128 (request) and 58 (reply).
   * Ping statistics showed **0% packet loss**.
4. **QUIC (Quick UDP Internet Connections)**
   * Purpose: Modern transport protocol designed by Google, running over UDP, optimizing HTTPS performance.
   * Observation: Seen in connections to domains supporting QUIC, with handshake and encrypted payload packets.
   * Improves latency and reliability for web apps.

**Conclusion:**  
 This exercise successfully demonstrated live packet capture and filtering in Wireshark. Multiple protocols were identified, including TCP, TLSv1.3, ICMP, and QUIC, each serving a unique role in network communication. This hands-on analysis improved understanding of protocol behavior, packet structures, and their use in real-world traffic.



