**Network Traffic Analysis Report**

**Objective**

To capture live network packets, identify core protocols in use (QUIC, TCP, DNS, HTTP), and summarize their activity using Wireshark.

**Protocols Identified**

| **Protocol** | **Screenshot** | **Description** | **Usage Observed** |
| --- | --- | --- | --- |
| QUIC | Screenshot\_quic.png | Modern transport protocol used for secure and fast web connections, especially by Google and YouTube. | Observed multiple QUIC packets with handshakes and protected payloads indicating secure connections, likely to Google services. |
| TCP | Screenshot\_tcp.png  Screenshot.png | Reliable, connection-oriented protocol commonly used for HTTP, HTTPS, and other web traffic. | SYN/ACK packets detected in web browsing sessions, often establishing or terminating secure web connections. |
| DNS | Screenshot\_dns.png | Domain Name System protocol used for resolving hostnames to IP addresses. | Several DNS standard query and response packets show lookups to Google and static content servers, indicating domain resolution for browsing. |
| HTTP | Screenshot\_http.png | Application layer protocol for web data transfer in plaintext (not encrypted). | Recorded multiple GET and POST requests with data transfer between client and web servers, representing direct web browsing activity. |

**Summary of Packet Details**

* **QUIC** was the predominant protocol for modern web traffic, especially for encrypted and low-latency communication to Google domains.
* **TCP** clearly supported transport-layer reliability for application data transfers, as highlighted by SYN, ACK, and PSH flag sequences.
* **DNS** queries actively resolved service domains, with responses facilitating further web traffic.
* **HTTP** requests and responses were mostly related to web browsing and resource retrieval, such as dynamic content loading and certificate validation.
* Screenshots confirm a diverse mix of secure, encrypted traffic (QUIC, TLS), basic web loading via HTTP, and foundational network resolution via DNS.

**Example Packet Analysis**

* **QUIC handshake info**: As seen in the Info field, QUIC packets showcase connection initializations, payload protection, and cryptographic handshakes.
* **TCP ACK/SYN flags**: TCP connections highlighted standard back-and-forth handshaking for session establishment.
* **DNS standard queries**: DNS packets include domain queries and received IP mappings, confirming successful domain name resolutions.
* **HTTP GET/POST**: Clear evidence of client HTTP requests and server responses, including JSON data and certificate validation events.