**Task 5: Capture and Analyze Network Traffic Using Wireshark**

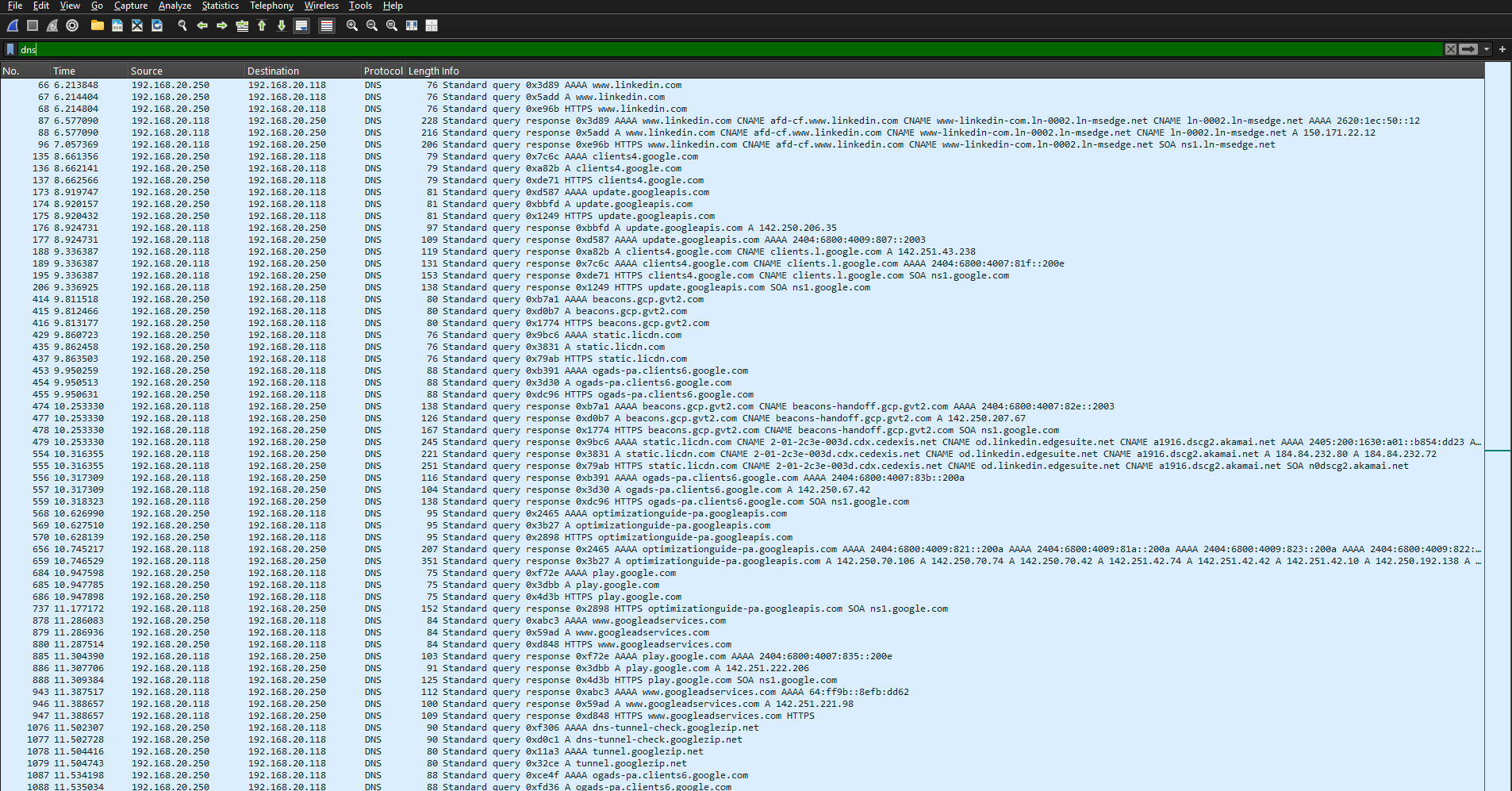
**Objective:**  
To capture live network packets and identify common protocols and traffic types using Wireshark.

**Tools Used:**

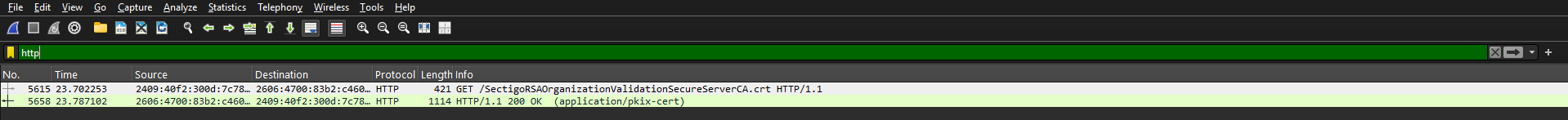
* Wireshark (latest stable version)

**Process Followed:**

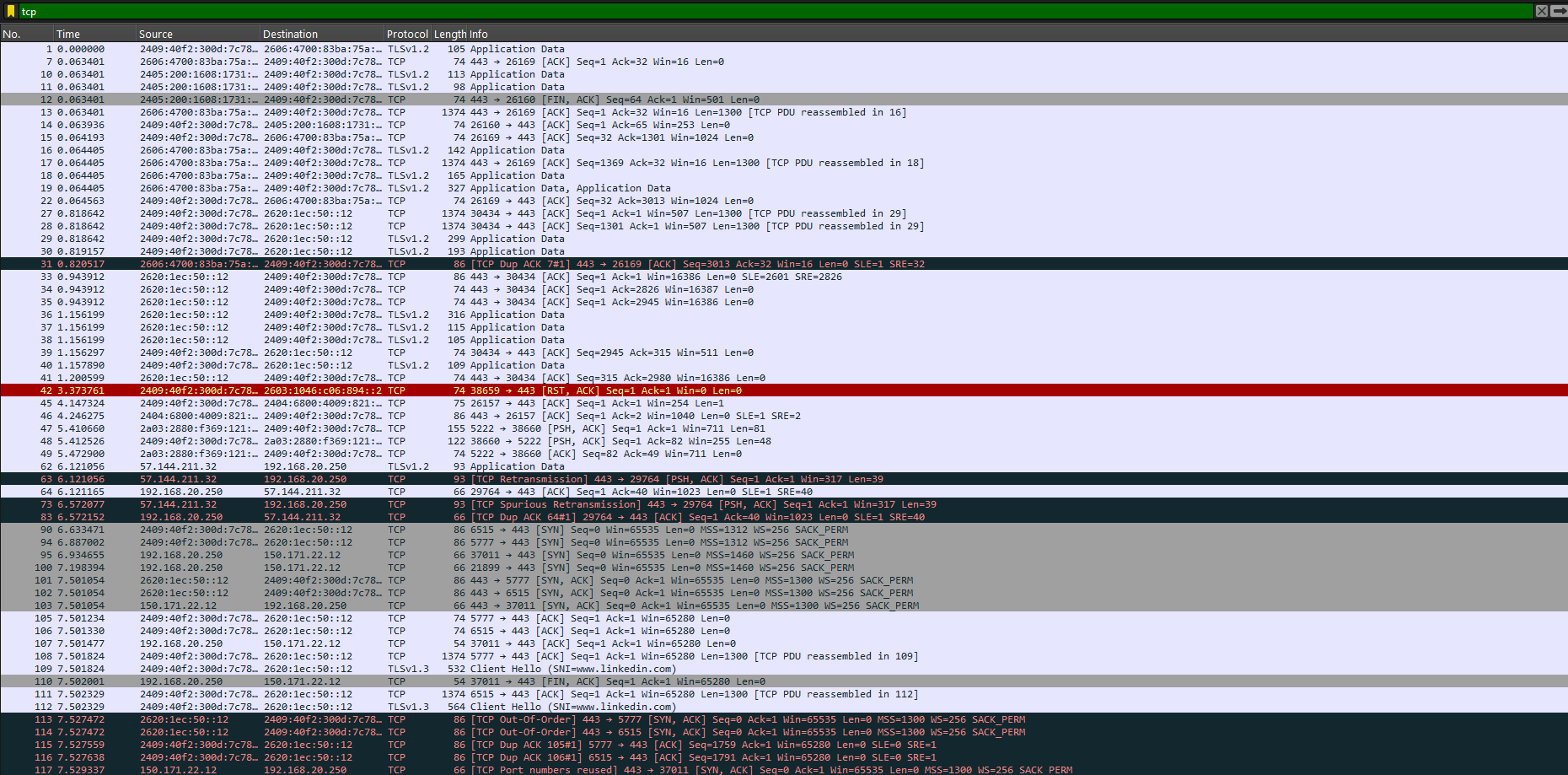
1. Installed Wireshark and selected the active network interface.
2. Started live capture and generated traffic by browsing websites and pinging a server.
3. Stopped capture after ~1 minute.
4. Applied filters (http, dns, tcp, tls, quic) to analyze specific protocol packets.
5. Exported the captured traffic into a .pcap file for documentation.



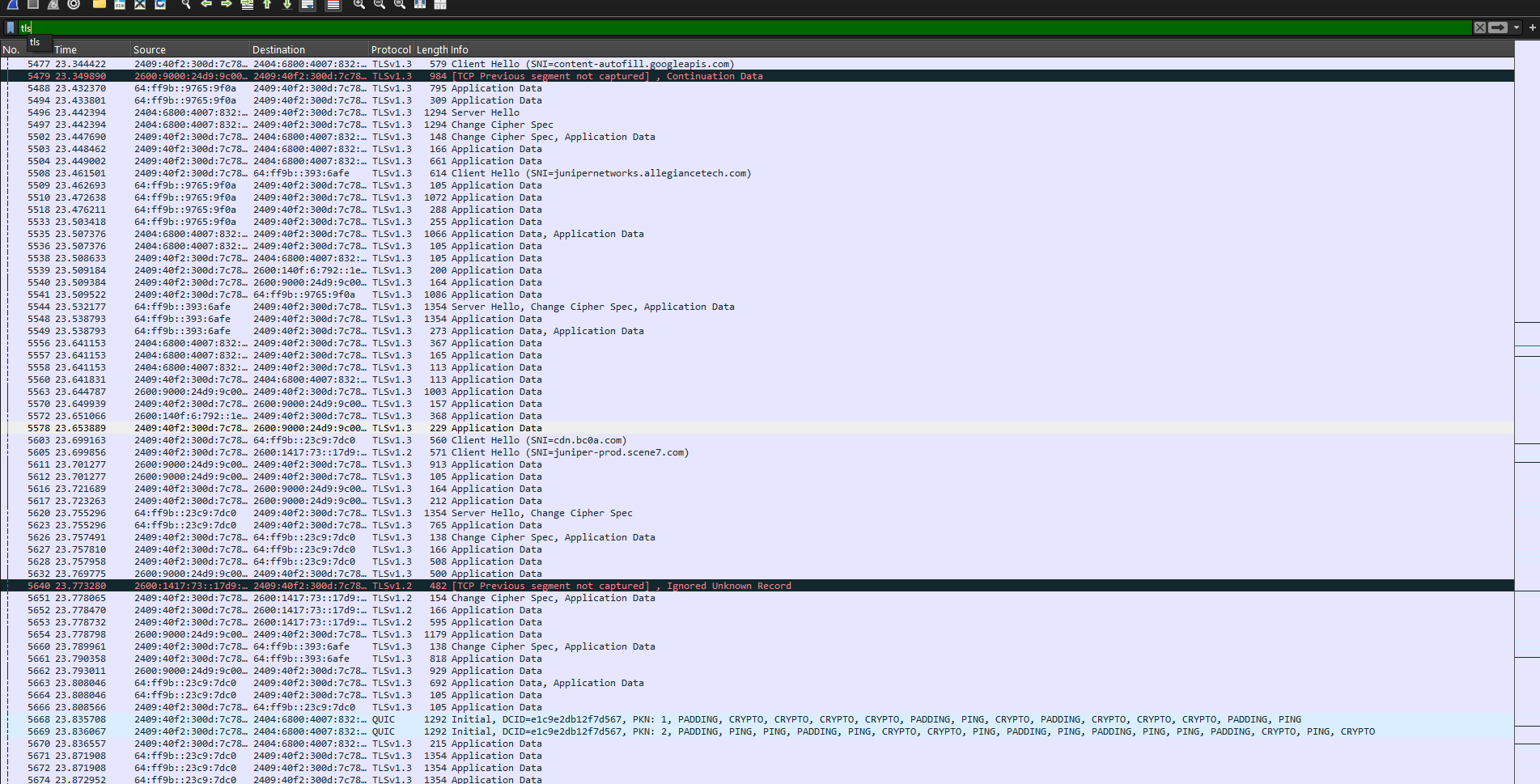
**DNS**



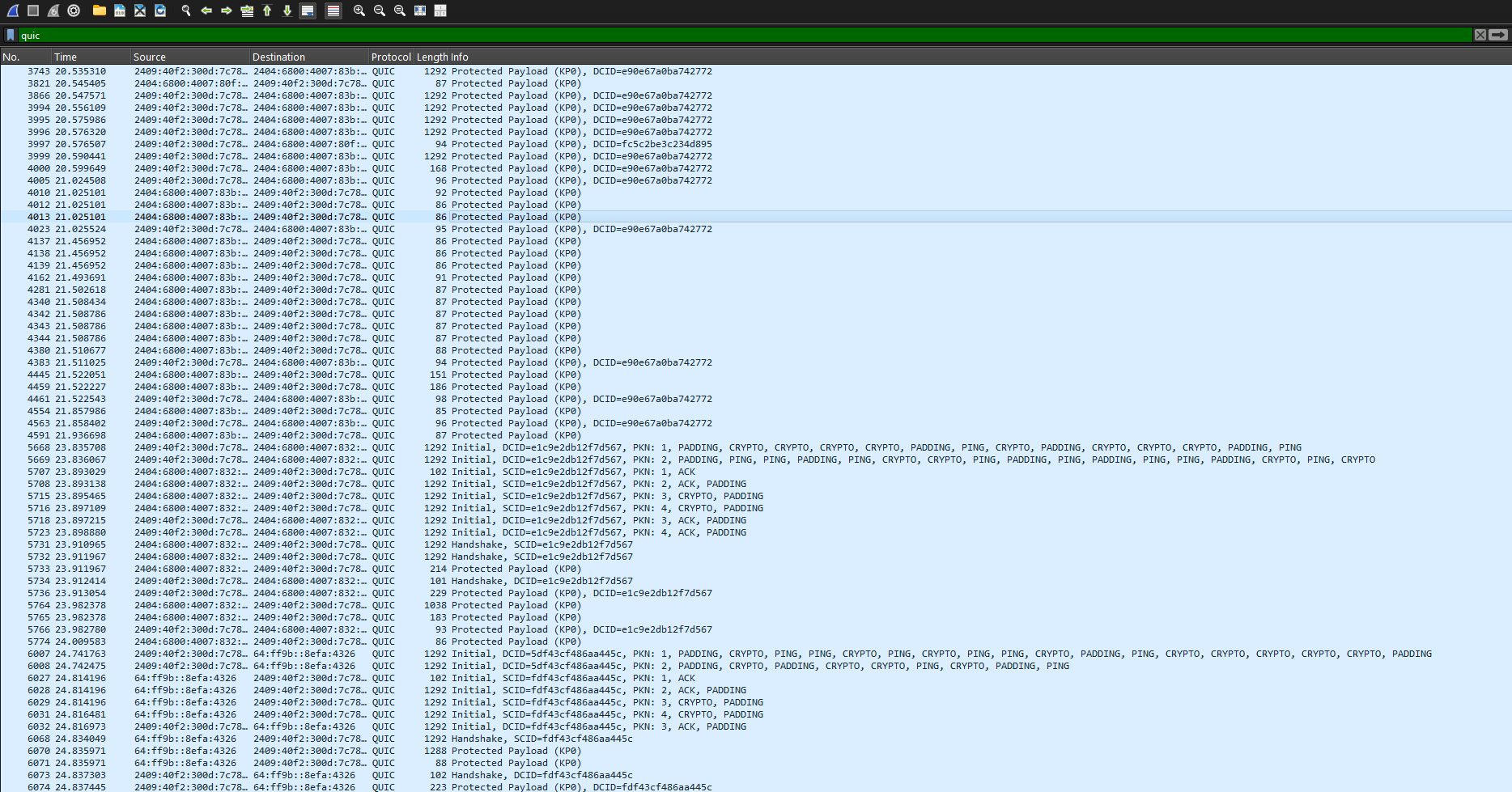
**TCP**



**HTTP**

****

**TLS**

****

**QUIC**

**Protocols Identified**

1. **HTTP (Hypertext Transfer Protocol):**
   * Used for web communication between browser and web server.
   * Packets showed requests (GET, POST) and responses with status codes.
   * Works over port **80** (unencrypted).
2. **DNS (Domain Name System):**
   * Resolves domain names (e.g., google.com) into IP addresses.
   * Packets contained queries and responses.
   * Uses **UDP port 53** by default.
3. **TCP (Transmission Control Protocol):**
   * Provides reliable, connection-oriented communication.
   * Used as the transport protocol for HTTP, TLS, and many others.
   * Packets showed **SYN, ACK, FIN** flags for connection setup/teardown.
4. **TLS (Transport Layer Security):**
   * Provides encryption for secure communication (e.g., HTTPS).
   * Ensures confidentiality, integrity, and authentication.
   * Runs over TCP (commonly on port **443**).
5. **QUIC (Quick UDP Internet Connections):**
   * A modern transport protocol built on UDP.
   * Provides faster and secure connections compared to TCP+TLS.
   * Commonly used by **Google Chrome** and **YouTube** traffic.

**Summary of Findings**

* Successfully captured and analyzed live network traffic.
* Identified **5 protocols: HTTP, DNS, TCP, TLS, and QUIC**.
* Each protocol serves a distinct purpose: DNS for name resolution, TCP/TLS/QUIC for reliable and secure transport, and HTTP for application-level web traffic.
* Learned how to filter packets, interpret protocol details, and export captures as .pcap.

**Deliverables:**

* .pcap file with recorded packets.
* This short report summarizing captured protocols and their roles.

**Outcome:**  
Developed hands-on packet analysis skills and improved awareness of core network protocols.