TASK – 5: Packet Analysis through Wireshark

## 1. Protocols Identified

You captured at least five different protocols in your network traffic:

* TCP (Transmission Control Protocol): Used for reliable communication. Many packets in your capture are TCP.
* UDP (User Datagram Protocol): Connectionless protocol seen with some traffic (likely DNS or other services).
* DNS (Domain Name System): Resolving domain names (e.g., queries for googleapis.com).
* TLSv1.2 (Transport Layer Security): Encrypts HTTP traffic, seen as TLSv1.2 packets.
* ICMPv6 (Internet Control Message Protocol for IPv6): Used for neighbor discovery and error reporting in IPv6 networks.

## 2. Example Packet Details

Here are details of some sample packets from capture:

* TCP Packets
  + Source: 2401:4900:967f:4c7:...
  + Destination: 2a03:2880:...
  + Example Info: TCP Acked Unseen segment, TCP Dup Ack, sequence numbers show possible retransmissions.
* UDP Packets
  + Example: length 93, could be DNS traffic.
* DNS Packets
  + Standard queries for AAAA [www.googleapis.com](https://www.googleapis.com) and HTTPS [www.googleapis.com](https://www.googleapis.com).
* TLSv1.2 Packets
  + Secure connection setup for HTTPS traffic.
* ICMPv6 Packets
  + Neighbor solicitation and advertisement, showing IPv6 activity.

## 3. Observations / Analysis

* The network is using IPv6 addresses for communication.
* We successfully captured traffic for:
  + Web browsing (HTTPS/TLSv1.2, DNS queries).
  + TCP communication including retransmissions and acknowledgements.
  + UDP packets (could correspond to DNS).
  + ICMPv6 neighbor advertisements—this is part of IPv6 address resolution on the local network.
* Sites accessed include googleapis.com (visible in DNS queries).
* Several TCP duplicate ACK packets suggest there may have been packet loss or retransmissions.