Task 5: Capture and Analyze Network Traffic Using Wireshark

Objective

Capture live network packets and analyze common protocols used during browsing and ping activity.

Tools Used

- Wireshark

- macOS Terminal

Steps Followed

1. Selected active network interface (Wi-Fi).

2. Captured for 1 minute while:

   - Browsing `example.com` and `wikipedia.org`

   - Pinging `google.com` via terminal

3. Filtered traffic for relevant protocols.

Protocols Identified

Protocol	Description	Example
DNS	Resolves domain names	`A` query for `wikipedia.org`
HTTP	Web traffic (unencrypted)	GET request to `example.com`
ICMP	Ping diagnostic traffic	Echo request/reply from `ping google.com`
TCP	Reliable transport for HTTP	Three-way handshake observed
TLS	Secure HTTP (HTTPS) traffic	TLS handshake to `google.com`

Deliverables

- `task5_network_capture.pcap`

- This short protocol analysis report