Task 5 – Capture and Analyze Network Traffic Using Wireshark (Anonymized)

Task 5 – Capture and Analyze Network Traffic Using Wireshark (Anonymized)

Objective
Capture live network packets and identify basic protocols and traffic types. All host identifiers and sensitive details are anonymized in this report.

Steps Followed
1. Installed and opened Wireshark, selected the active network interface (name redacted).
2. Started a capture and performed simple network actions: visited a webpage, performed DNS lookups, and pinged a host (all targets anonymized).
3. Stopped the capture after ~1 minute and saved the capture file (anonymized).
4. Used display filters to isolate protocols: HTTP, DNS, TCP, and ICMP.
5. Exported a small sample of packets (anonymized) and reviewed packet details (headers and payloads where visible).

Protocols Identified (examples)
- DNS: Observed standard UDP queries and responses for name resolution.
- HTTP: Observed HTTP GET requests and corresponding responses (no sensitive payload captured).
- TCP: Observed SYN, SYN-ACK, and ACK sequences establishing connections.
- ICMP: Observed echo request/reply packets from ping testing.