Task 5: Capture and Analyze Network Traffic Using Wireshark

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools Used: Wireshark (Free, Open Source)

Method (Steps Taken):

1. Installed Wireshark and launched the tool.
2. Selected the active network interface (Wi-Fi).
3. Started capturing live packets.
4. Generated traffic by browsing a website (HTTP/HTTPS) and running ping to google.com.
5. Stopped the capture after approximately 1 minute.
6. Applied protocol filters (DNS, TCP, ICMP).
7. Identified and analyzed at least 3 protocols.
8. Saved the capture file as .pcap.

Findings:

Protocol	Description	Example Packet Detail
DNS	Resolves domain names into IP addresses	Client requested 'google.com' → DNS server responded with IP
TCP	Provides reliable communication (connection-oriented)	Observed 3-way handshake: SYN → SYN-ACK → ACK
ICMP	Used for network diagnostics like ping	Ping request (Echo) and response (Reply) recorded

Outcome: Gained hands-on experience in capturing and analyzing network traffic, identified common protocols (DNS, TCP, ICMP), and learned filtering techniques.