Task 5: Network Traffic Capture and Protocol Analysis

# Objective:

Capture live network packets and identify basic protocols and traffic types using Wireshark.

# Tools Used:

Wireshark (Free Network Protocol Analyzer)

# Steps Performed:

1. Installed and opened Wireshark.

2. Selected the active network interface and started packet capture.

3. Generated network traffic by browsing websites and using ping commands.

4. Stopped the capture after 1 minute.

5. Applied protocol filters such as 'http', 'dns', 'tcp', and 'icmp' to identify specific traffic.

6. Analyzed source/destination IPs, ports, and packet details.

7. Followed a TCP stream to examine an entire session conversation.

8. Exported the capture file as Task\_5\_Capture.pcap.

# Protocols Identified:

- \*\*HTTP\*\*: Web traffic (port 80)

- \*\*DNS\*\*: Domain resolution queries (port 53)

- \*\*TCP\*\*: Transport protocol used by many applications

- \*\*ICMP\*\*: Internet Control Message Protocol (used in ping)

# Summary:

During this task, I used Wireshark to capture real-time network traffic on my system. I successfully filtered and analyzed key internet protocols like HTTP, DNS, TCP, and ICMP. The process helped me understand how data flows between computers and servers. I also learned how to trace sessions using TCP stream analysis. This hands-on experience improved my understanding of protocol layers and live packet structures.



