# Task 5: Capture and Analyze Network Traffic Using Wireshark

## Objective:

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

## Tools:

Wireshark (Free)

## Steps Performed:

- Installed Wireshark on the system.

- Started capturing packets on the active network interface.

- Browsed websites and pinged a server to generate network traffic.

- Stopped the capture after approximately 1 minute.

- Applied filters in Wireshark to view specific protocols such as HTTP, DNS, and TCP.

- Identified at least three different protocols from the captured traffic.

- Exported the capture as a .pcap file for submission.

## Protocols Identified:

- HTTP – Used for web browsing and transmitting web content.

- DNS – Used to resolve domain names to IP addresses.

- TCP – Transmission Control Protocol, ensuring reliable data transfer between devices.

## Findings and Packet Details:

The captured network traffic revealed multiple protocols in action. HTTP packets were observed during web browsing, showing GET and POST requests. DNS queries and responses were identified while resolving domain names. TCP connections were established for reliable communication between the client and servers.

## Outcome:

This task provided hands-on experience in network traffic capturing and analysis. It enhanced understanding of how different protocols function and interact on a network.