Task 5: Capture and Analyze Network Traffic Using Wireshark

# Objective

The objective of this task was to perform a live capture of network packets using Wireshark, identify commonly used protocols such as HTTP, DNS, and TCP, and analyze them to understand their behavior and significance.

# Tools Used

- Wireshark  
- Windows/Linux OS  
- Web Browser & Ping Command  
- Internet Connection

# Steps Followed

1. Installed Wireshark and launched the application.  
2. Began packet capture on the active network interface.  
3. Generated network traffic by visiting websites and pinging servers.  
4. Stopped capture after approximately one minute.  
5. Applied filters such as 'http', 'dns', and 'tcp' to isolate specific protocols.  
6. Identified and analyzed the structure and behavior of at least three protocols.  
7. Saved the packet capture file as 'network\_capture.pcapng'.

# Protocols Identified

## 1. HTTP (HyperText Transfer Protocol)

HTTP is an application-layer protocol used for transmitting hypermedia documents, such as HTML. It typically operates over TCP port 80. In the captured traffic, HTTP GET requests and server responses were visible in plain text, showing requested URLs and response codes.

## 2. DNS (Domain Name System)

DNS is a protocol used to resolve human-readable domain names into IP addresses. It usually runs on UDP port 53. Captured DNS queries showed domain name lookups and corresponding responses containing resolved IP addresses.

## 3. TCP (Transmission Control Protocol)

TCP is a connection-oriented transport-layer protocol that ensures reliable data transfer. It involves a three-way handshake mechanism (SYN, SYN-ACK, ACK). The capture displayed the connection setup and data transfer between client and server using TCP.

# Additional Observations

During analysis, multiple IP addresses and port numbers were noted, indicating communication between various devices. Interesting packets included DNS queries for domain resolution and HTTP requests for web resources. The presence of TCP handshakes confirmed the establishment of reliable connections.