



Date 15/09/2025

Lab Practical #10:

Study Packet capture and header analysis by Wireshark (HTTP, ICMP, DNS, TCP, UDP etc.)

Practical Assignment #10:

- 1. Explain usage of Wireshark tool.**
- 2. Packet capture and header analysis by Wireshark (HTTP, ICMP, DNS, TCP, UDP etc.)**

Wireshark

Wireshark is an open-source network protocol analyser.

It captures live packet data from a network interface and allows detailed inspection of protocols.

Supports hundreds of protocols (HTTP, ICMP, DNS, TCP, UDP, etc.).

Protocols Studied

HTTP (Hyper Text Transfer Protocol): Used for web communication.

ICMP (Internet Control Message Protocol): Used for error messages and diagnostics (e.g., ping).

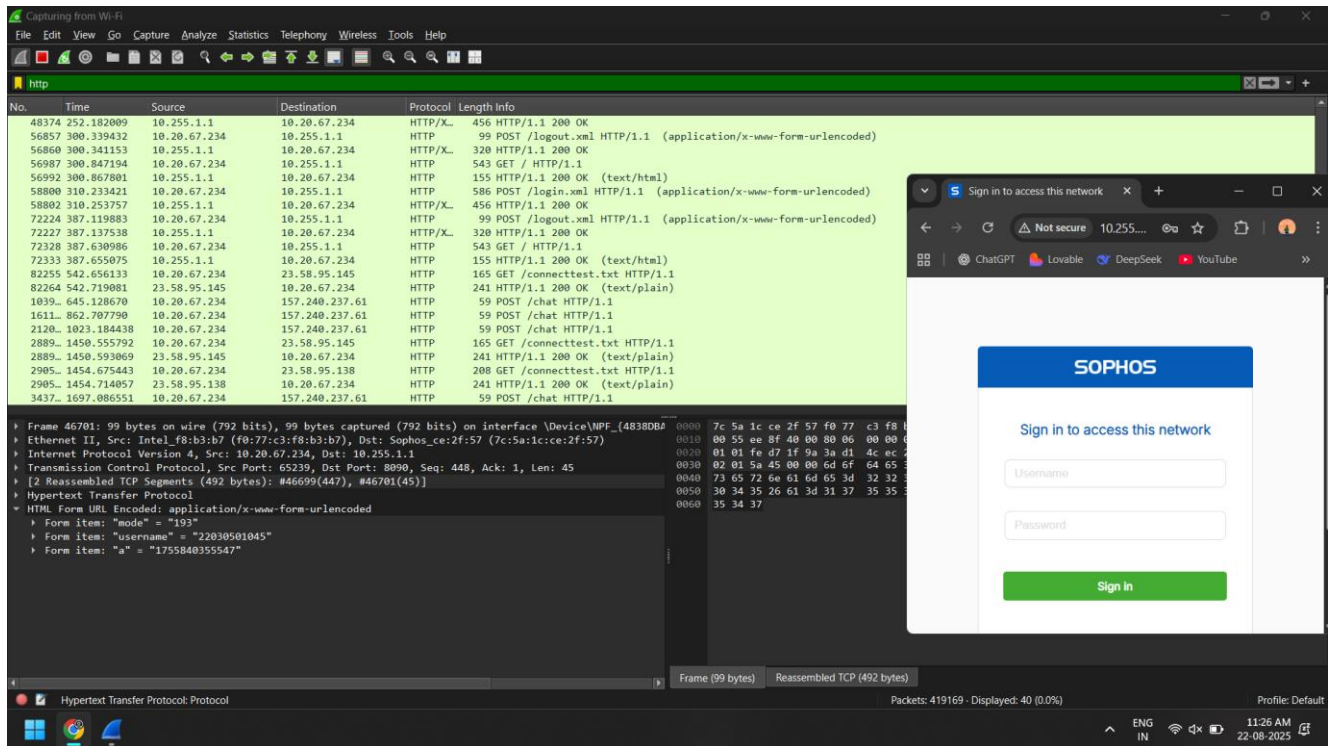
DNS (Domain Name System): Resolves domain names to IP addresses.

TCP (Transmission Control Protocol): Connection-oriented protocol for reliable communication.

UDP (User Datagram Protocol): Connectionless protocol for fast but unreliable communication.

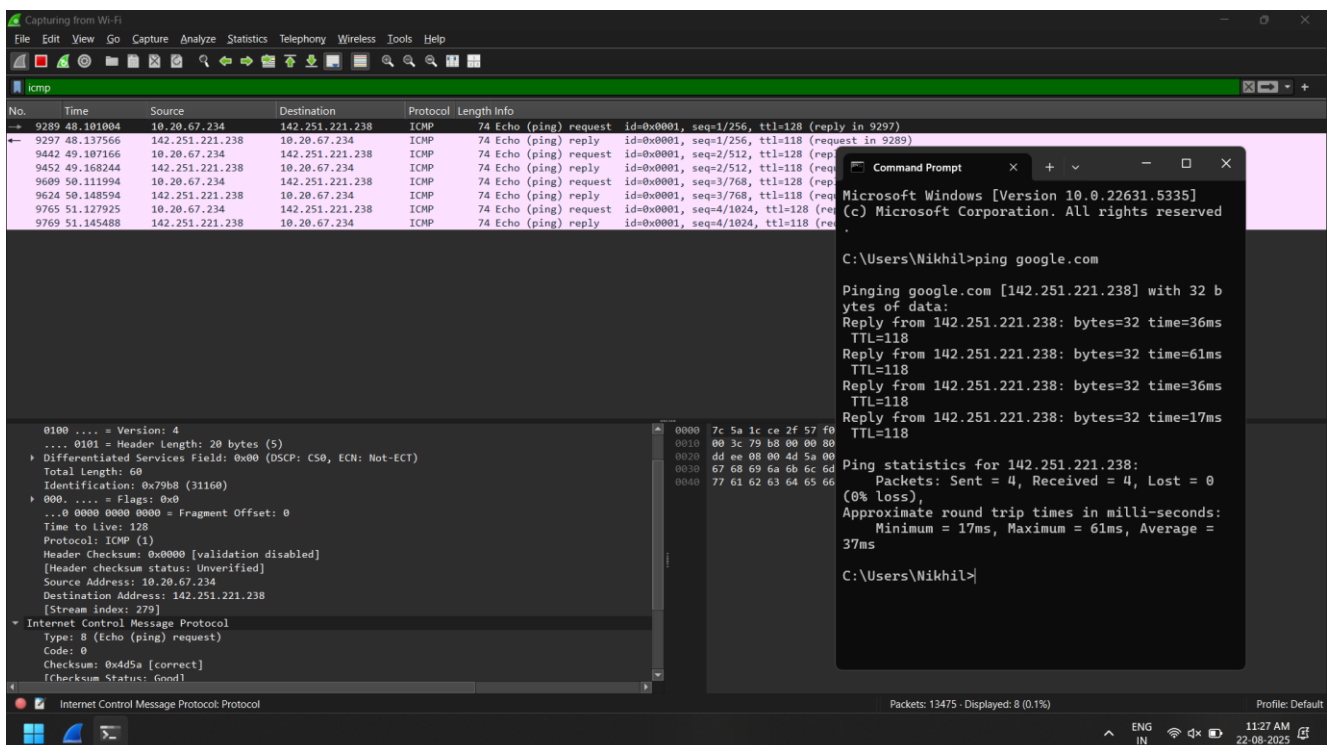
Date 15/09/2025

1. HTTP



The screenshot shows a Wireshark packet capture of HTTP traffic. The packet list on the left shows several HTTP requests and responses. The packet details pane on the right shows the structure of an HTTP GET request for '/connecttest.txt'. The packet bytes pane at the bottom shows the raw data of the request. In the background, a web browser window displays a Sophos login page with fields for Username and Password, and a Sign In button.

2. ICMP



The screenshot shows a Wireshark packet capture of ICMP traffic. The packet list on the left shows several ICMP Echo (ping) requests and replies. The packet details pane on the right shows the structure of an ICMP Echo request. The packet bytes pane at the bottom shows the raw data of the request. In the background, a Command Prompt window shows the results of a ping command to google.com, displaying the IP address 142.251.221.238 and various statistics including round trip times and packet loss.



Date 15/09/2025

3. DNS

The image shows a Wireshark packet capture of a DNS transaction. The packet list shows a standard query (No. 2512) and a standard query response (No. 2514). The packet details pane for the response shows the domain name system protocol and the response data. A Windows Command Prompt window is open, showing the command 'nslookup' and its output: 'Default Server: UnKnown Address: 10.20.1.1'.

4. TCP

The image shows a Wireshark packet capture of a TCP connection. The packet list shows a three-way handshake (SYN, SYN-ACK, ACK) and subsequent data transfer. The packet details pane for the first data packet (No. 6331) shows the transmission control protocol details, including the sequence number, acknowledgment number, and window size. The packet bytes pane shows the raw data of the packet.