

NAME: Kadiyala Sri Pavan

UNIVERSITY: Aditya University

EMAIL: pavancc1478@gmail.com

Task-3

Network Traffic Analysis using Wireshark

Objective:

To capture and analyze network traffic using Wireshark and understand basic networking protocols.

1. Basic Networking Concepts :

■ IP Address :

IP addresses serve as unique identifiers for devices on a network, similar to postal addresses for mail delivery. IPv4 uses a 32-bit format like **192.168.1.1**, while IPv6 employs 128 bits for vastly more addresses. Routers use IP to forward packets across networks during transmission.

■ MAC Address :

MAC addresses are hardware-based identifiers burned into network interface cards by manufacturers, operating at the data link layer. Each is 48 bits long, often shown as **00:1A:2B:3C:4D:5E**, and remains fixed unlike changeable IP addresses. Switches use MAC to deliver frames within local networks.

- **DNS Resolution :**

DNS translates human-readable domain names (e.g., **example.com**) into IP addresses through a hierarchical system of servers. Queries typically use UDP port 53 for speed, falling back to TCP for larger responses. Devices rely on DNS servers, often assigned via DHCP, for internet connectivity.

- **TCP Protocol :**

TCP provides reliable, connection-oriented delivery with a three-way handshake (**SYN, SYN-ACK, ACK**) to establish sessions. It guarantees order, error-checking via checksums, and retransmission of lost packets, making it ideal for web browsing and email. Flow control prevents overwhelming receivers.

- **UDP Protocol :**

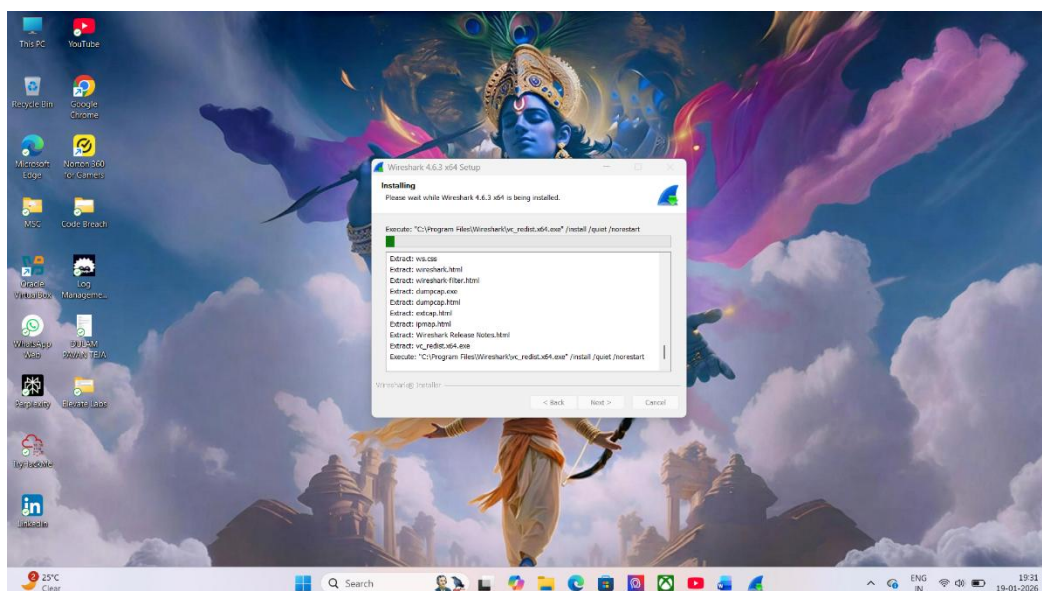
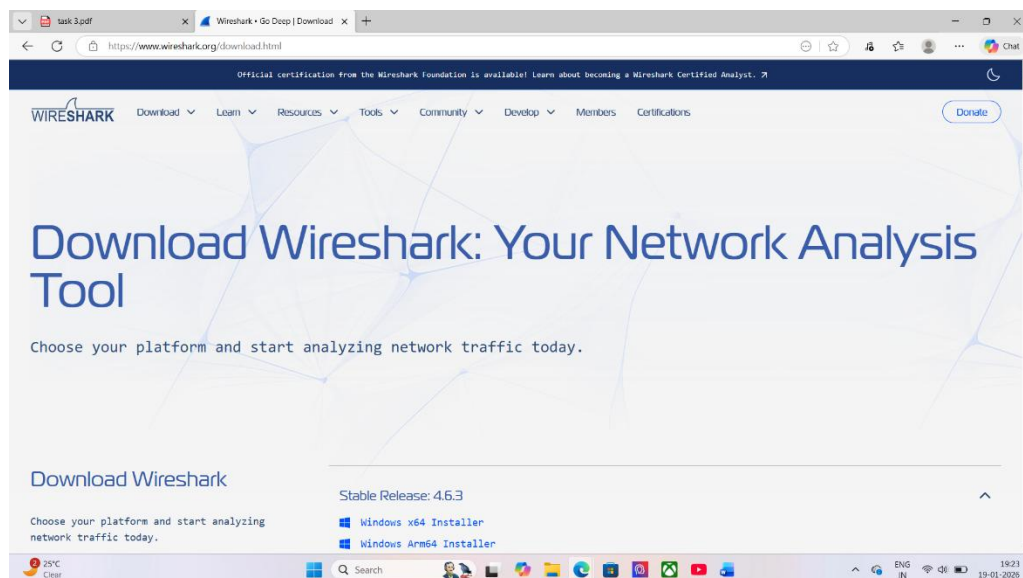
UDP offers connectionless, low-overhead transmission without handshakes or retransmissions, prioritizing speed over reliability. It suits applications like video streaming or DNS queries where occasional packet loss is tolerable. Headers are minimal at 8 bytes versus TCP's larger structure.

2. Install Wireshark.

Sept-1: Go to the Wireshark official website: [Wireshark • Go Deep | Download](#)

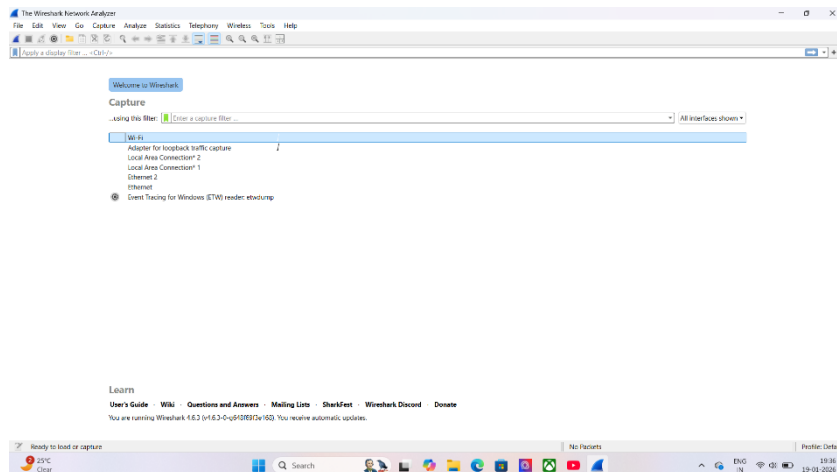
Step-2: Install the Wireshark into the windows.

Select **Npcap** (IMPORTANT)

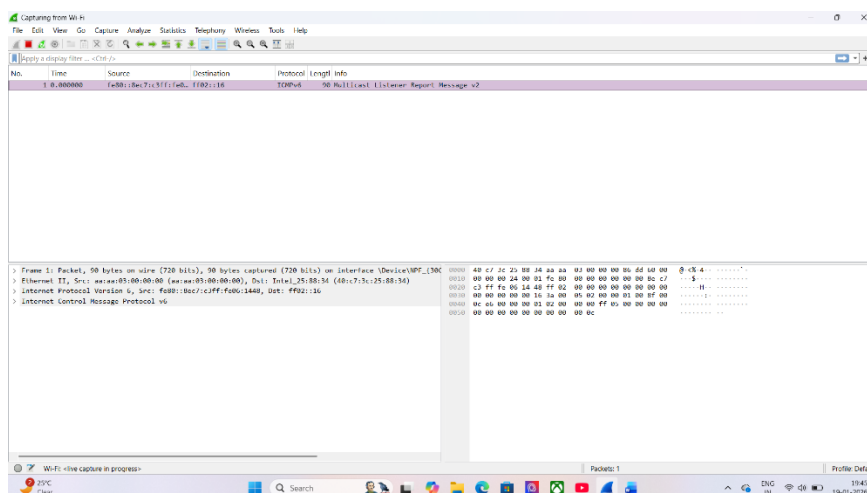


3. Capture Live Network Traffic.

- After Completing the installation of Wireshark open the Wireshark.



- Select interface:
Ethernet-> LAN
Wi-Fi-> Wireless
Click on the Start (blue shark icon)



4. Packet Filters:

We have different code for packet Filters that is

1. HTTP = http

The screenshot shows a Wireshark packet capture of HTTP traffic. The packet list on the left shows several GET requests to various resources. The selected packet (No. 25463) is a TCP Reset (RST) from 192.168.1.7 to 192.168.1.7, with a sequence number of 23,37,85,99. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data of the packet.

2. DNS = dns

The screenshot shows a Wireshark packet capture of DNS traffic. The packet list on the left shows several DNS queries and responses. The selected packet (No. 6387) is a DNS query from 192.168.1.7 to 192.168.1.1, with a sequence number of 26,439,331. The packet details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System layers. The packet bytes pane shows the raw data of the packet.

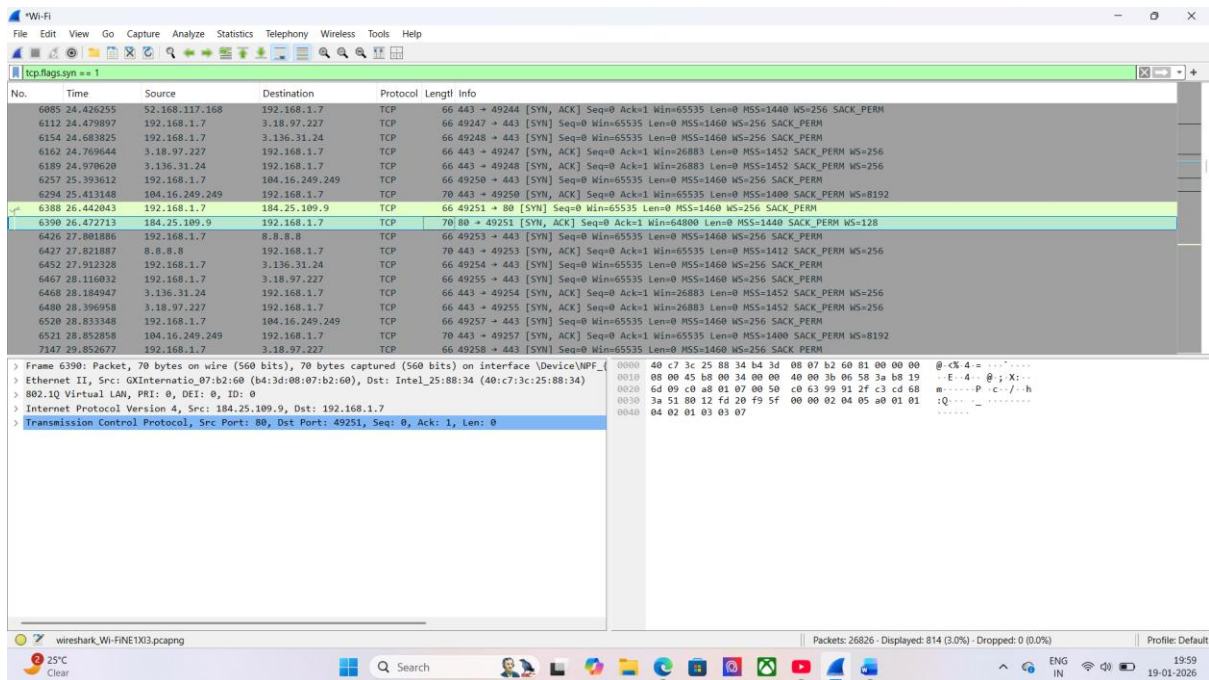
3. TCP = tcp

Wireshark packet capture showing TCP traffic. The packet list shows a SYN packet (No. 6398) from 192.168.1.7 to 192.168.1.7. The packet details show the TCP header with Seq=49251, Win=0, Len=0, and the flag SYN. The packet bytes show the raw TCP segment.

4. UDP = udp

Wireshark packet capture showing UDP traffic. The packet list shows a QUIC packet (No. 6393) from 192.168.1.7 to 192.168.1.7. The packet details show the QUIC header with Version=4, Src Port=443, and Dst Port=52707. The packet bytes show the raw QUIC segment.

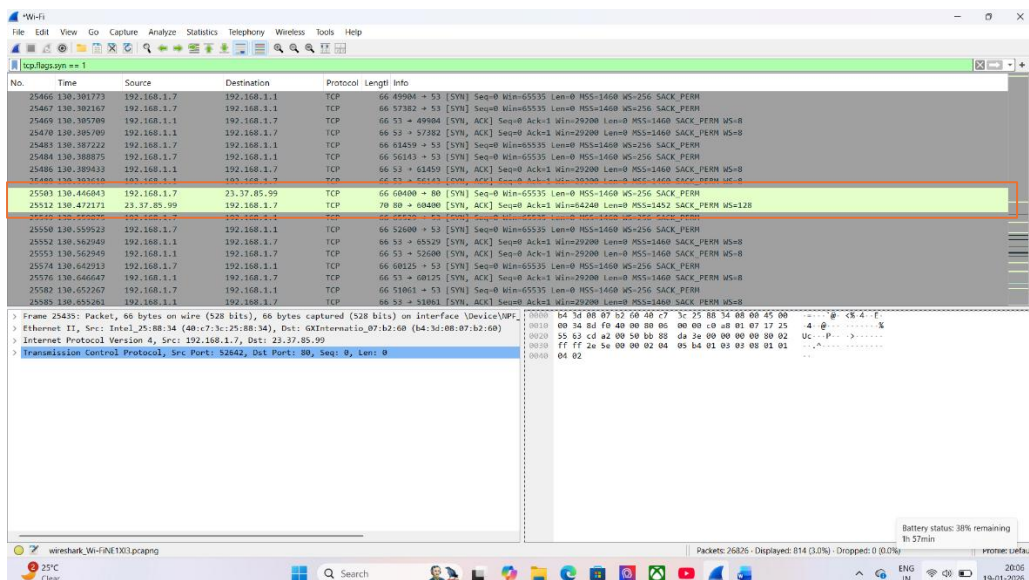
5. TCP Handshake = tcp.flags.syn == 1



5. TCP Three-Way Handshake.

In Wireshark we can observe how three-Way Handshake is work

When we use the “`tcp.flags.syn == 1`” we can observe the working of **SYN, SYN-ACK, & ACK**



Here,

SYN means Clint → Server

SYN, ACK Means Server → Clint

ACK Means Clint → Server

These Three Packets together = TCP Three-Way Handshake

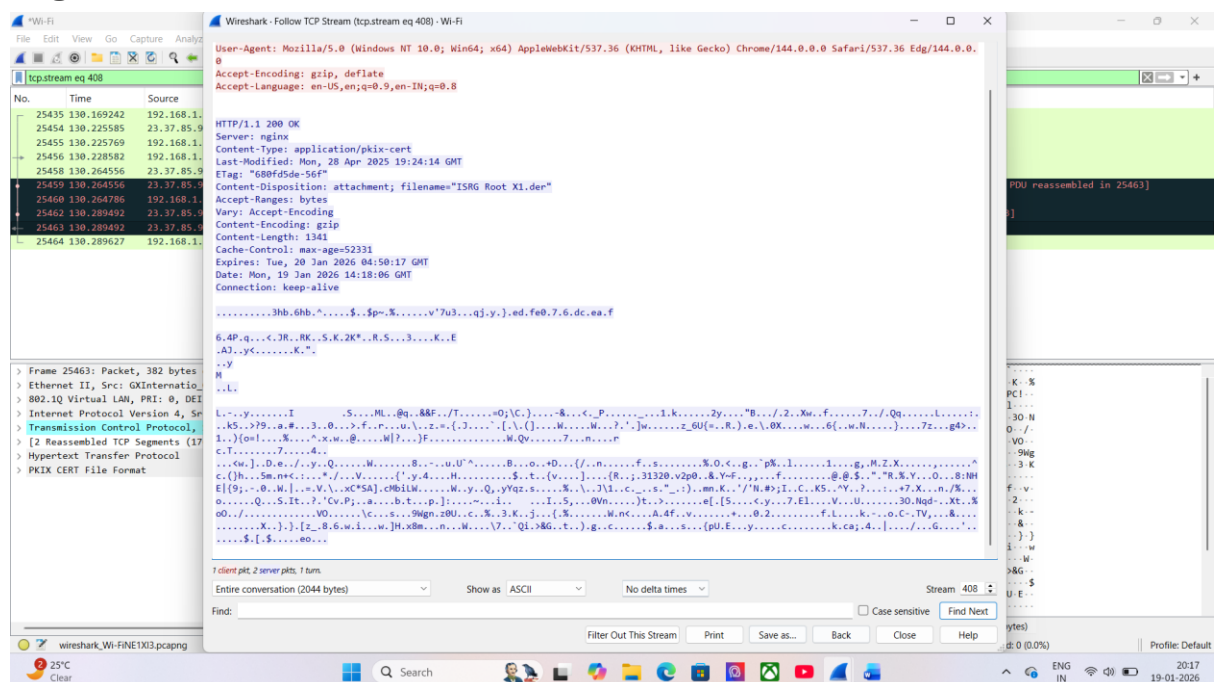
6.Plain Text vs Encrypted Traffic.

- Plain Text (Insecure)

Plain text means it is a insecure protocol Like **HTTP** it show the user details and the data will readable

Filter: http

Right click → Follow → TCP Stream



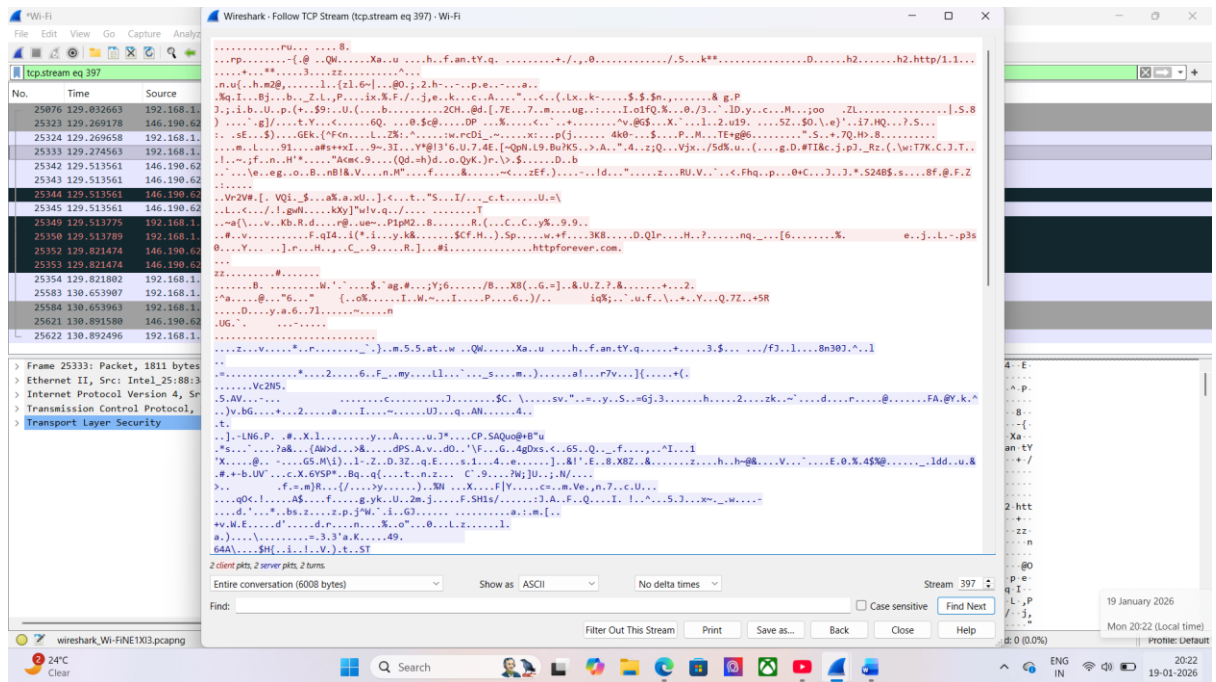
Here, we can observe how the http protocol will shoes the user details without secure.

- Encrypted(Secure)

Encrypted means it is secure protocol Like **HTTPS/TLS** it can't show the user details and data not readable

We can observe by using

Filter: tls



Here, We can Observe the **HTTPS** how the user details are store to the secure.

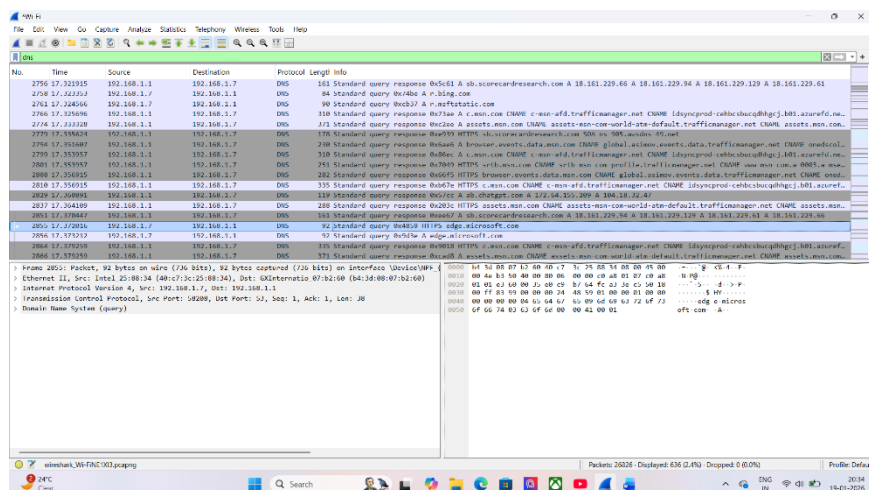
HTTP means not secure protocol it can't store the user details.

HTTPS means secure protocol to store the user details.

7. Capture DNS queries and analyse.

By using the Filter "**dns**" we can see the Query with particular response.

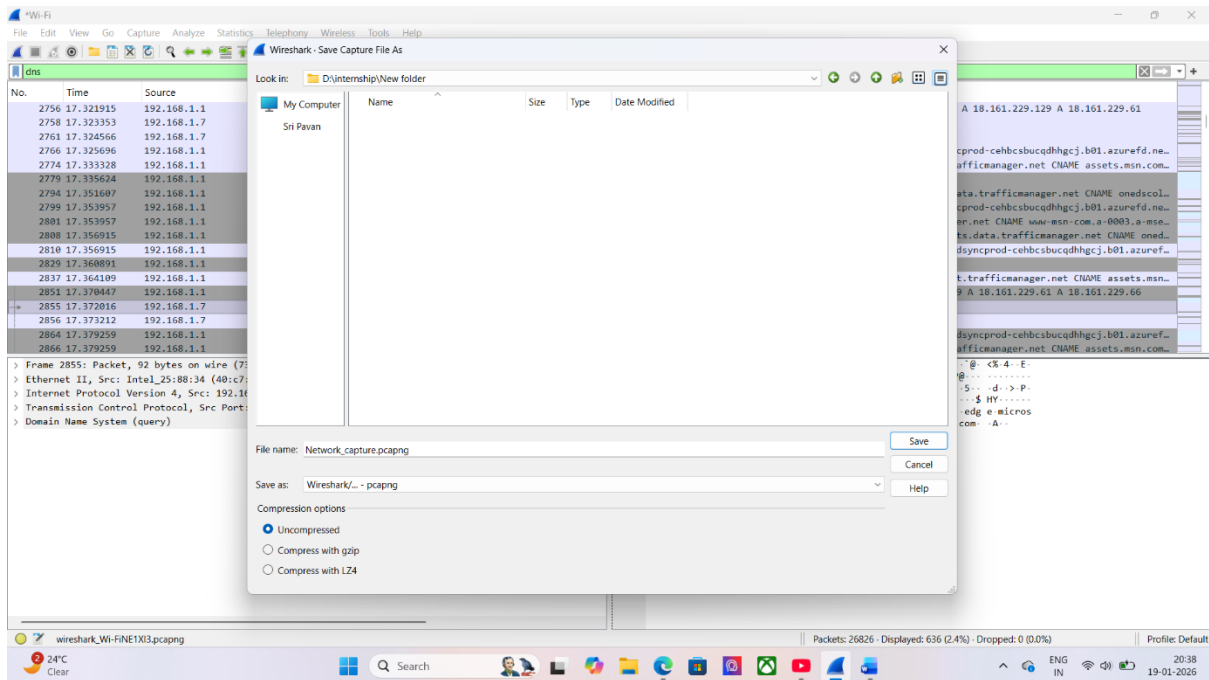
It is used in Website tracking, Malware investigation, Network Forensics



8. Save Packet Capture File.

File → Save As

Filename: Network_capture.pcapng.



Observation:

- i. **TCP** three-way handshake was observed (**SYN**, **SYN-ACK**, **ACK**).
- ii. **DNS** queries resolved domain names to IP addresses.
- iii. **HTTP** traffic was visible in plain text.
- iv. **HTTPS** traffic was encrypted and unreadable.

Conclusion:

Wireshark is an effective tool for analyzing network traffic and identifying insecure communications. It is useful in cybersecurity monitoring and investigations.