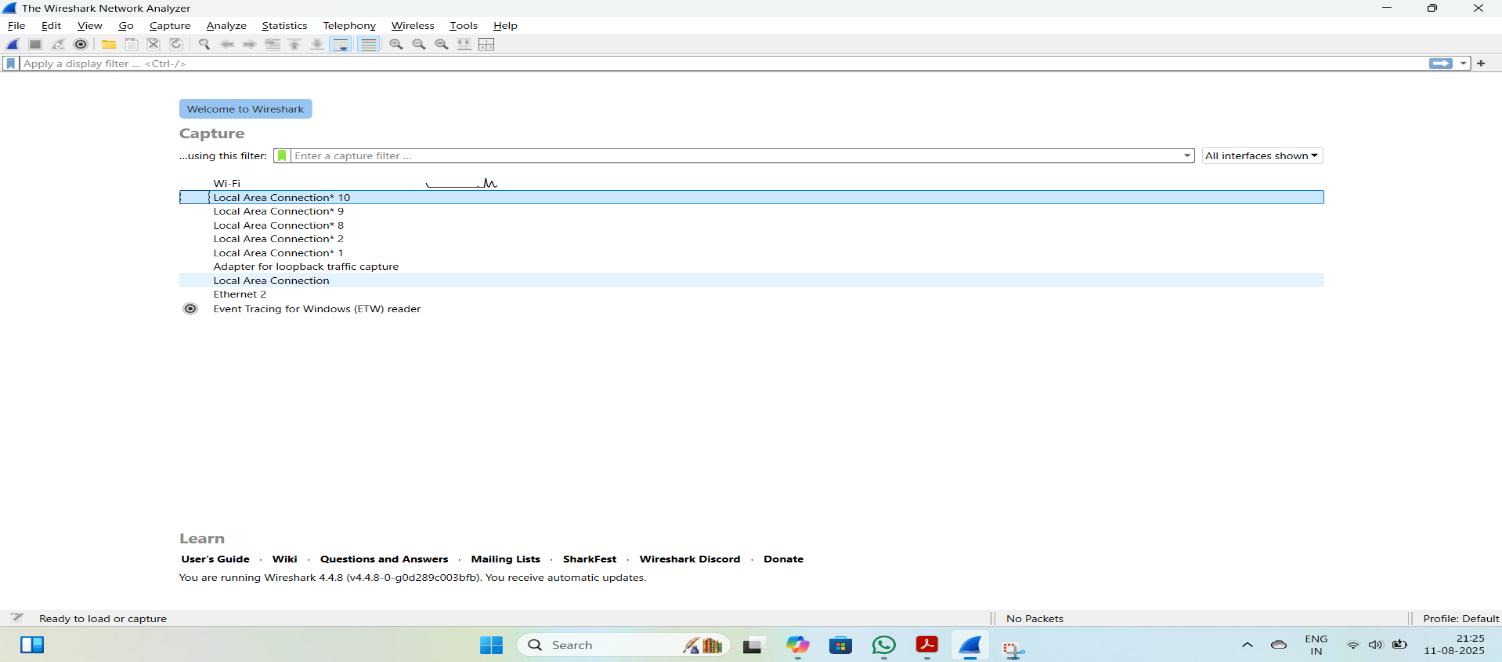
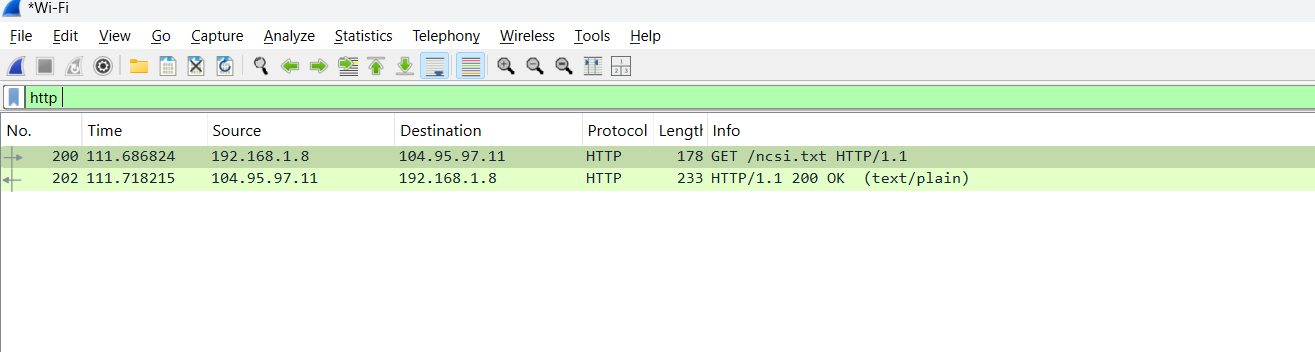
**TASK-5**

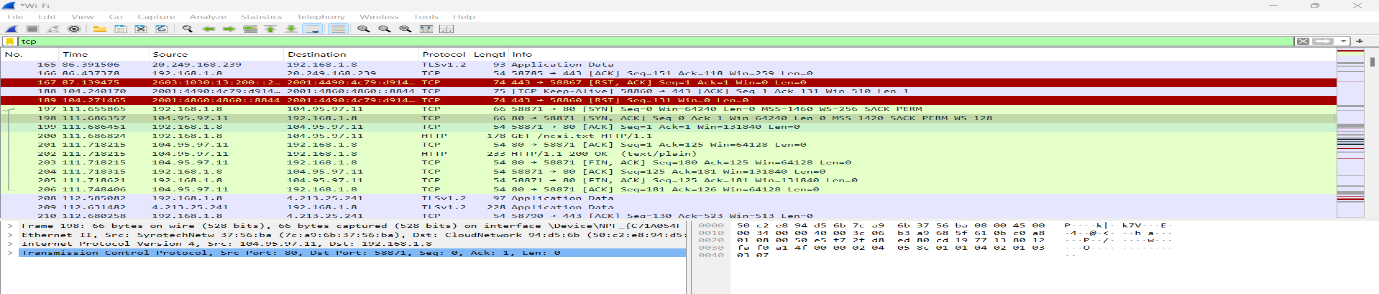
**Filter Captured Packets by Protocol**

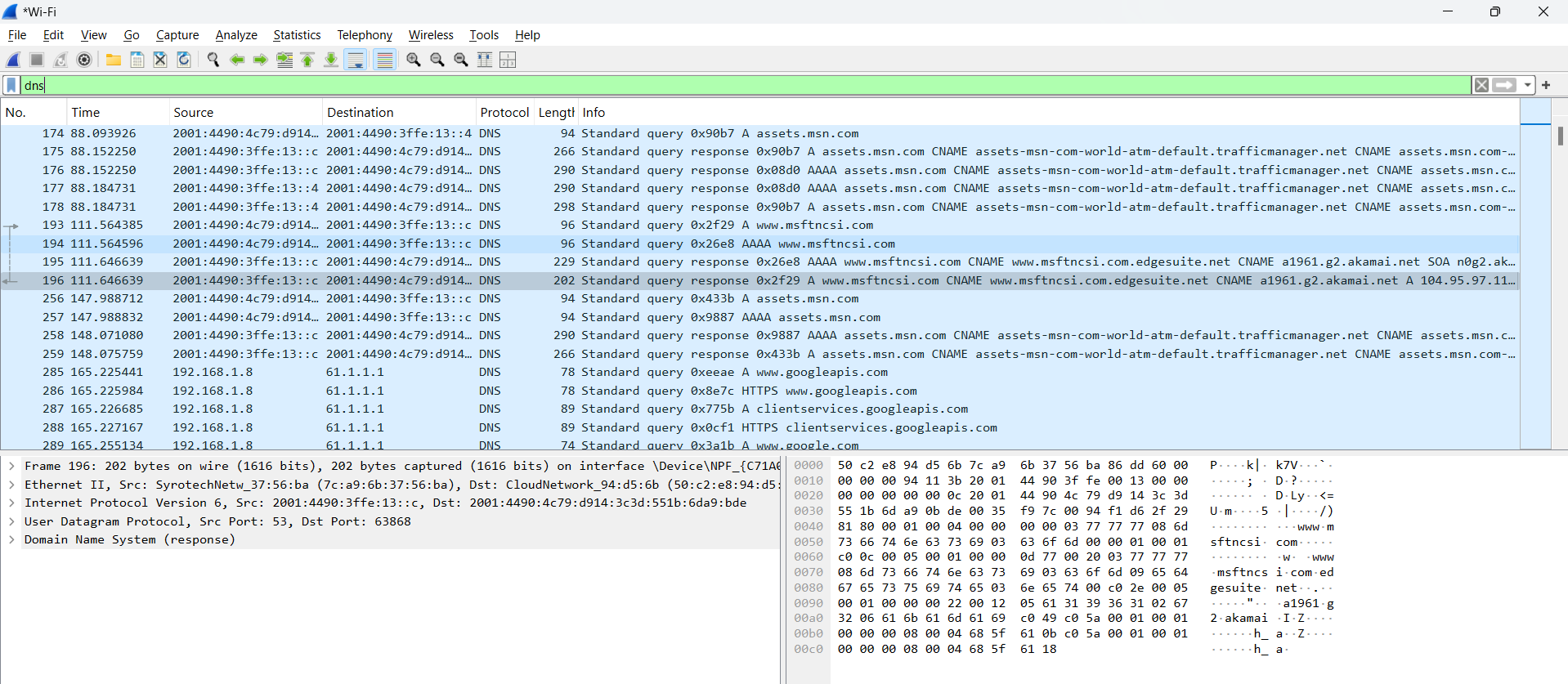
Wireshark interface:



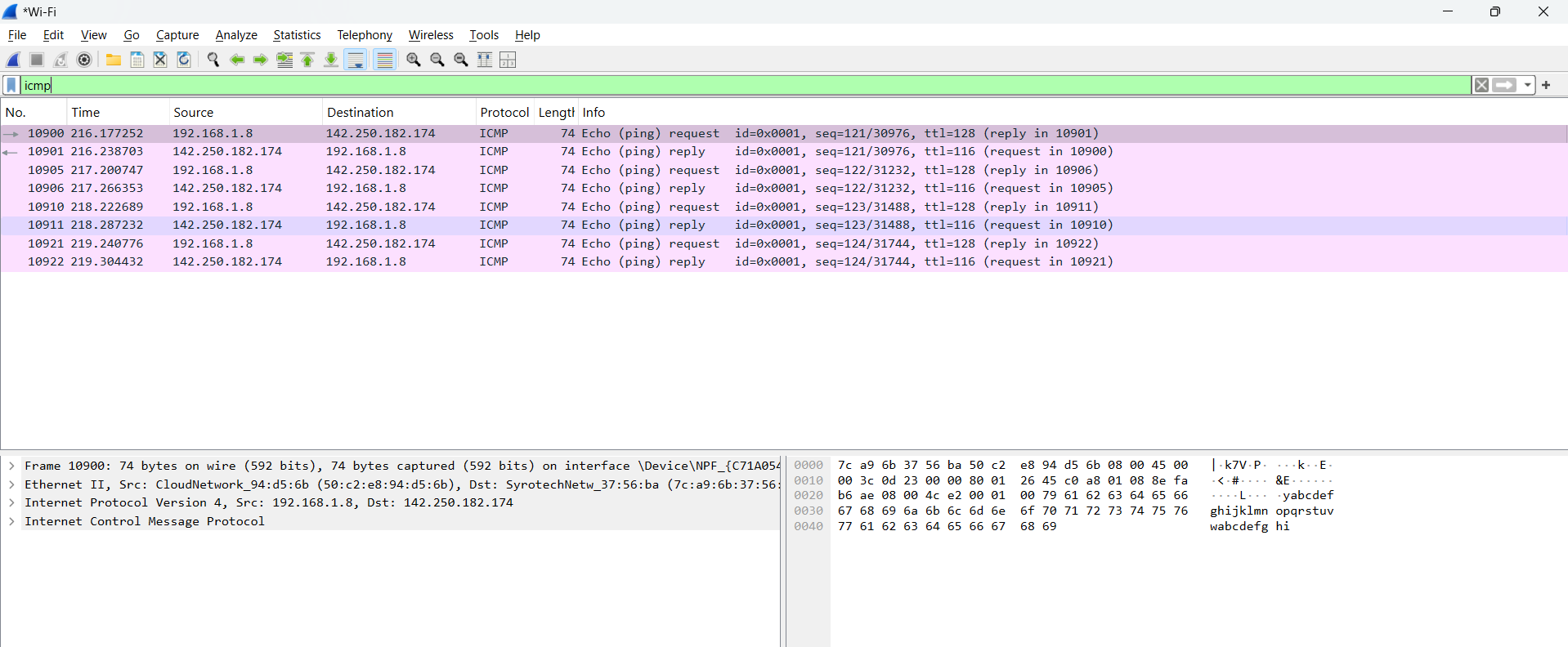
HTTP:



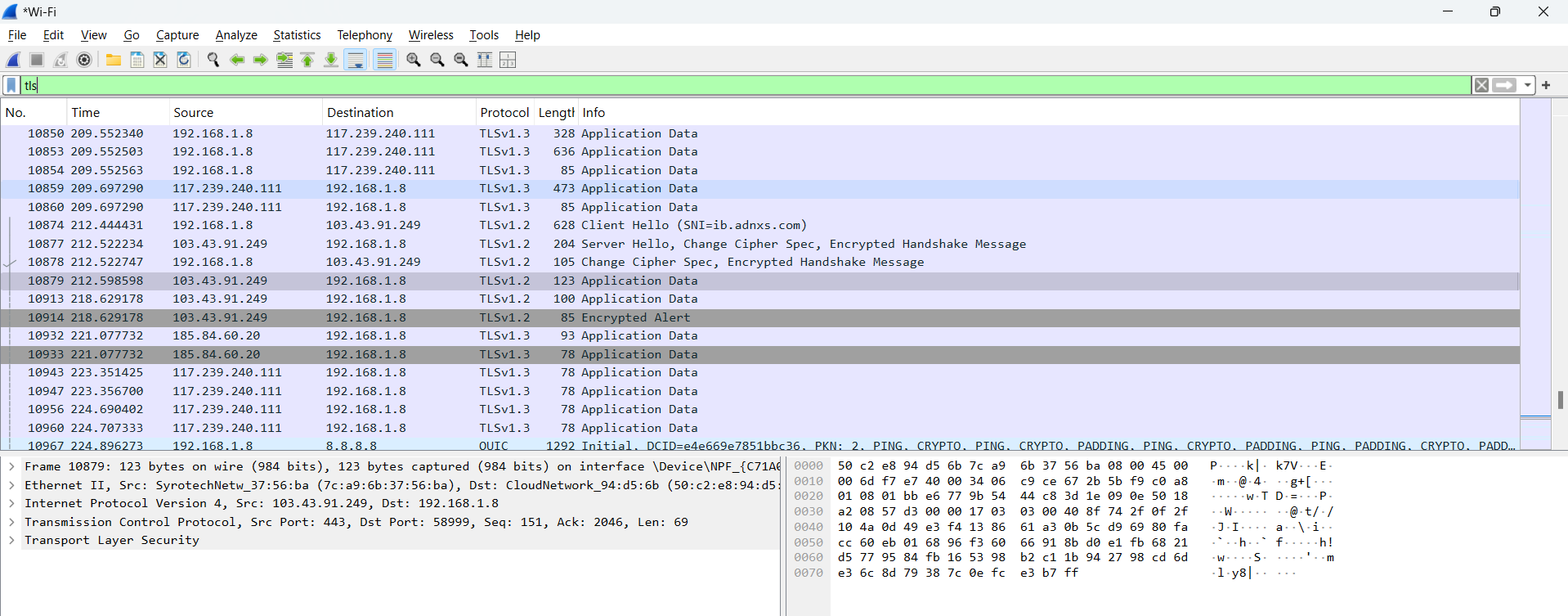
TCP: 

DNS: 

ICMP:



TLS:



| **Protocol** | **Filter Expression** |
| --- | --- |
| HTTP | http |
| DNS | dns |
| TCP | tcp |
| ICMP | icmp |
| TLS | tls |

* Type a filter (e.g., http) into the top filter bar and press Enter.
* You’ll see only packets matching that protocol.

**Summary:**

Start capture – open wire shark and start packet capture

Generate traffic - search for any website to create traffic

Stop after 1 min – stop after one min to see the exact results

Filter by protocol – filter protocols by using filter option wire shark

Identify 3+ protocols- identified 5 protocols like HTTP,TCP,ICMP, DNS and TLS

Export as .pcap- finally export file in pcap form

**Interview Questions:**

**1.What is Wireshark used for?**

Wireshark is a **network protocol analyzer** used to:

* Capture and inspect data packets in real time
* Diagnose network issues and performance problems
* Analyze security breaches or suspicious activity
* Learn how protocols work by examining traffic

**2.What is a packet?**

A **packet** is a small unit of data transmitted over a network. It typically contains:

* **Header**: Metadata like source/destination IP, protocol info
* **Payload**: The actual data being sent (e.g., part of a webpage, email, etc.)

**3.How to filter packets in Wireshark?**

You can filter packets using **Display Filters** in the top bar. Examples:

* ip.addr == 192.168.1.1 → packets to/from a specific IP
* http → only HTTP traffic
* tcp.port == 443 → traffic on TCP port 443 (HTTPS)

Wireshark also offers **Capture Filters** before starting a capture, like:

* port 80 → capture only traffic on port 80

4.**What is the difference between TCP and UDP?**

| **Feature** | **TCP (Transmission Control Protocol)** | **UDP (User Datagram Protocol)** |
| --- | --- | --- |
| Connection-based | Yes | No |
| Reliability | High (error checking, retransmission) | Low (no guarantees) |
| Speed | Slower | Faster |
| Use Cases | Web browsing, email, file transfer | Streaming, gaming, VoIP |

TCP ensures data arrives correctly; UDP prioritizes speed over reliability.

**5.What is a DNS query packet?**

A **DNS query packet** is a request sent from a client to a DNS server to resolve a domain name (like example.com) into an IP address. It includes:

* Query type (e.g., A for IPv4, AAAA for IPv6)
* Domain name being queried
* Transaction ID to match responses

6.**How can packet capture help in troubleshooting?**

Packet capture helps by:

* Revealing delays, dropped packets, or retransmissions
* Identifying misconfigured devices or protocols
* Detecting unauthorized access or malware
* Verifying if data is reaching its destination

It’s like an X-ray for your network.

7.**What is a protocol?**

A **protocol** is a set of rules that define how data is transmitted and received over a network. Examples include:

* **HTTP**: for web traffic
* **TCP/IP**: for basic internet communication
* **DNS**: for domain name resolution
* **FTP**: for file transfers

8.**Can Wireshark decrypt encrypted traffic?**

Wireshark **can decrypt some encrypted traffic**, but only under certain conditions:

* For **HTTPS (TLS)**: You need access to the server’s private key or use **SSL key logging** from the client
* For **WPA2 Wi-Fi**: You need the network’s passphrase and capture the full handshake

.