**Task 3: Networking Basics for Cyber Security**

**Tool used:** Wireshark

1.Learn basic networking concepts (IP, MAC, DNS, TCP/UDP).

**IP address**  
Identifies a device on a network (example: 192.168.1.5)

**MAC address**  
Hardware address of a network interface (fixed, physical)

**DNS (Domain Name System)**  
Converts website names into IP addresses  
Example: google.com → 142.250.x.x

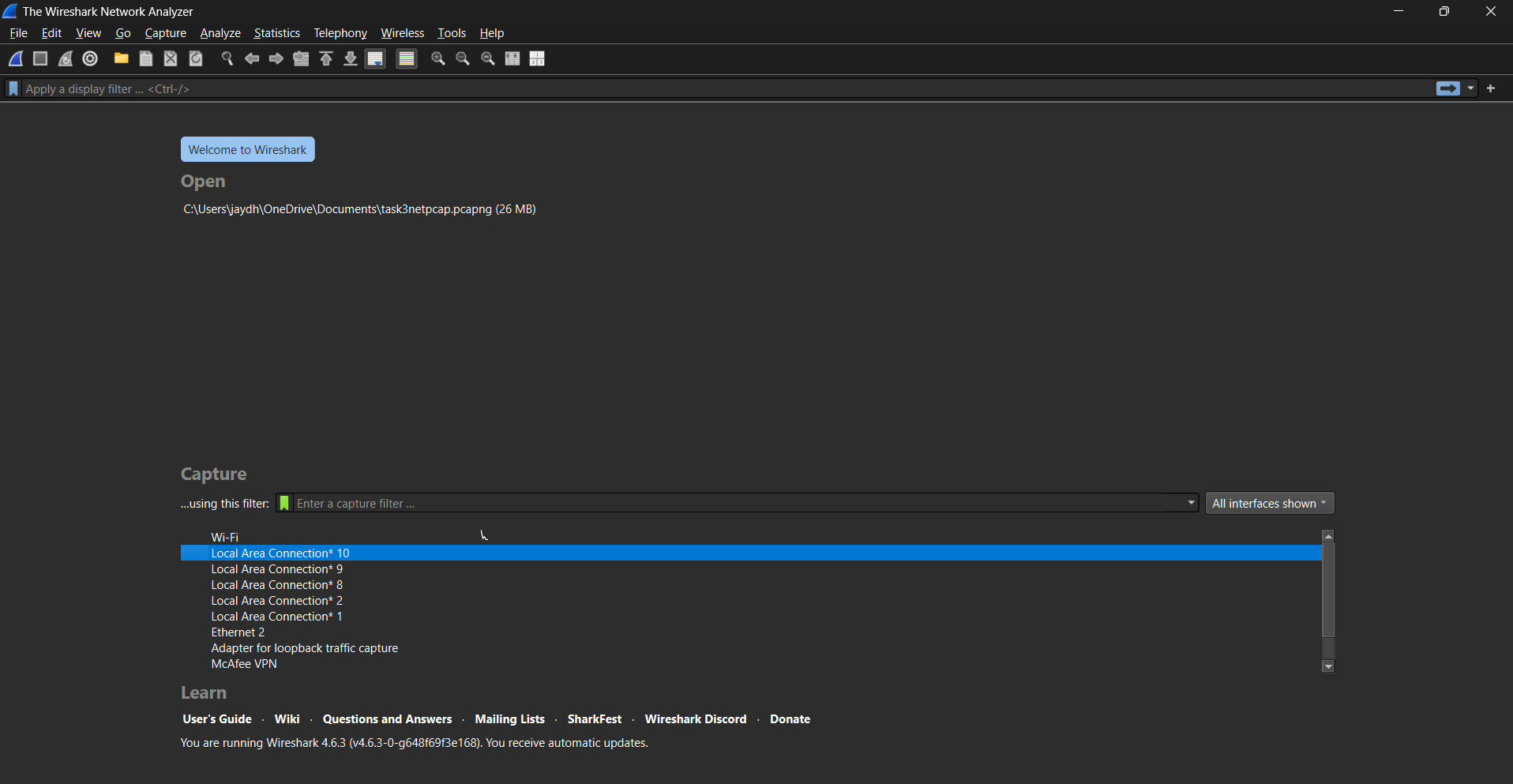
**TCP (Transmission Control Protocol) (3 way handshake)**  
Reliable, connection-based (used for web, email, logins)

**UDP (User Datagram Protocol) (connectionless)**  
Faster but unreliable (used for DNS, streaming)

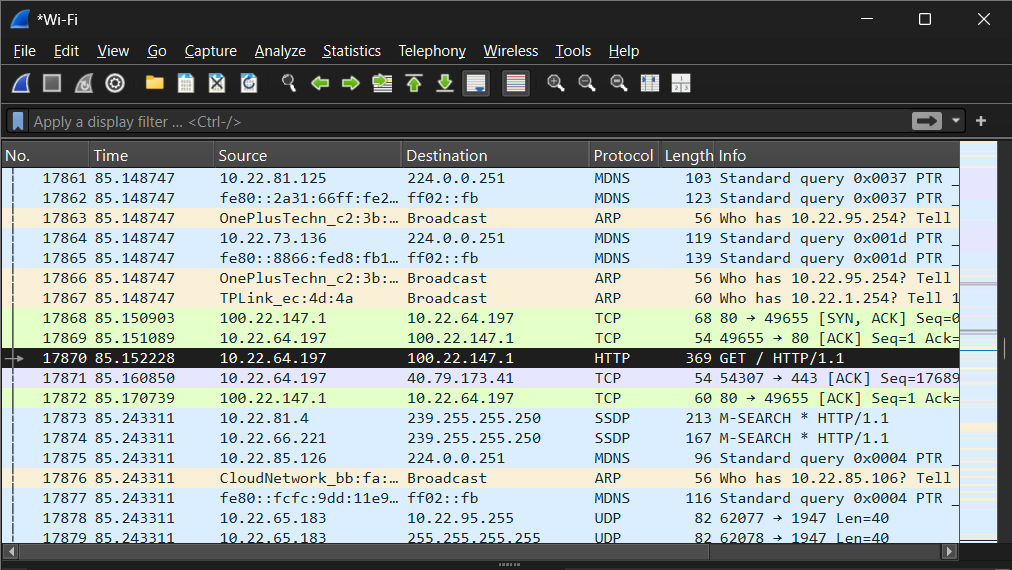
**TCP Three-Way Handshake**

* **SYN (Synchronize)**  
  The client initiates the connection by sending a packet with the SYN flag set to 1.  
  It includes its Initial Sequence Number (ISN).  
  The acknowledgment number is 0 because no data has been received yet.
* **SYN-ACK (Synchronize-Acknowledge)**  
  The server replies with both SYN and ACK flags set to 1.  
  It acknowledges the client’s ISN by setting the acknowledgment number to **ISN + 1**  
  and sends its own ISN.
* **ACK (Acknowledge)**  
  The client sends a final packet with the ACK flag set to 1.  
  It acknowledges the server’s ISN by setting the acknowledgment number to **server ISN + 1**.  
  The connection is now established, enabling full-duplex communication.

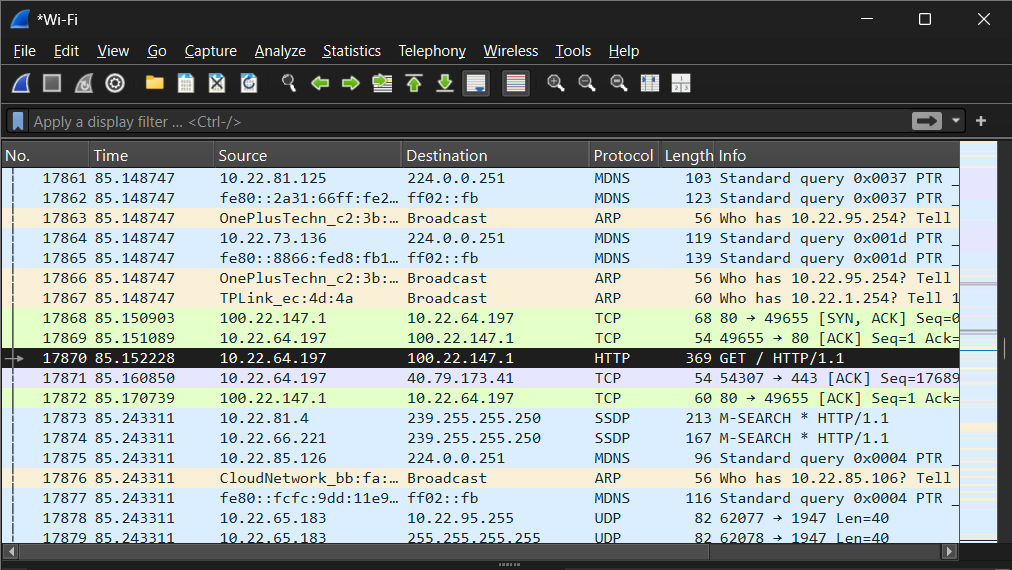
Wireshark was installed successfully on the system.

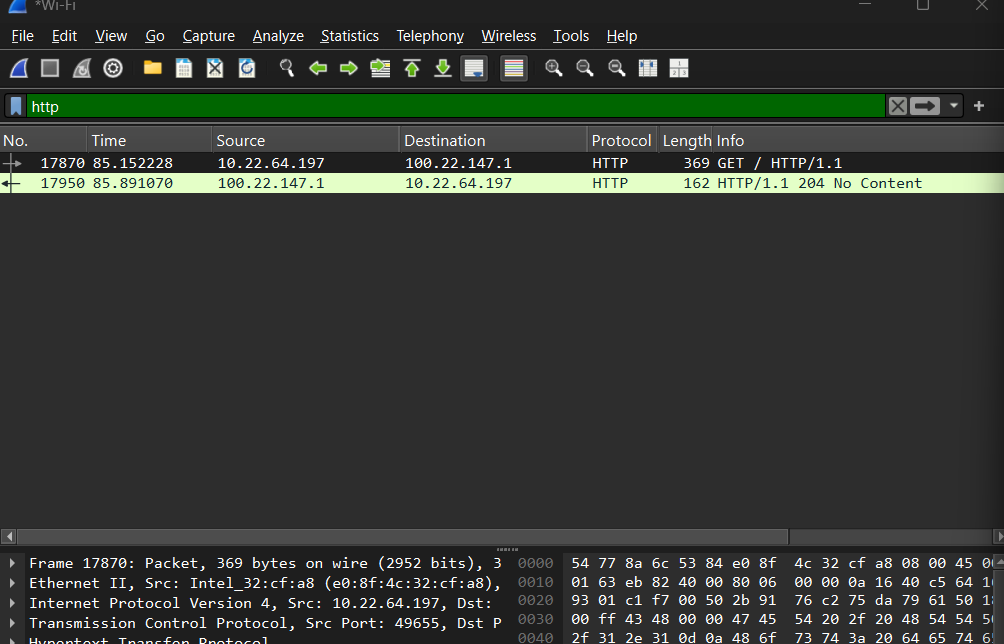


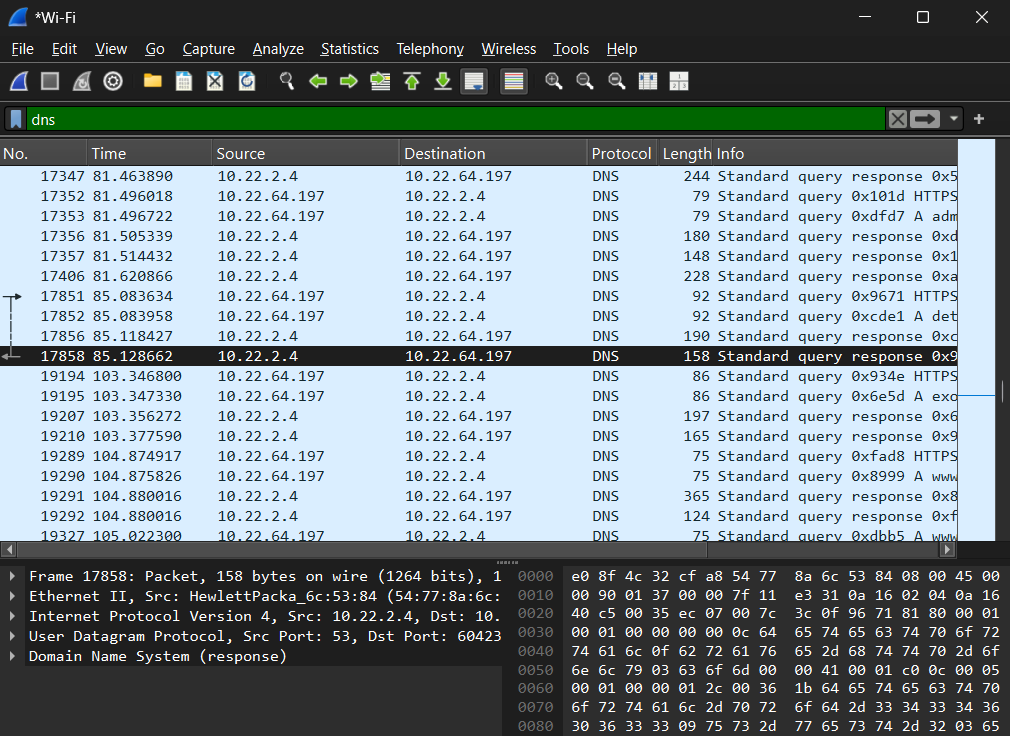
The active network interface (Wi-Fi) was selected.

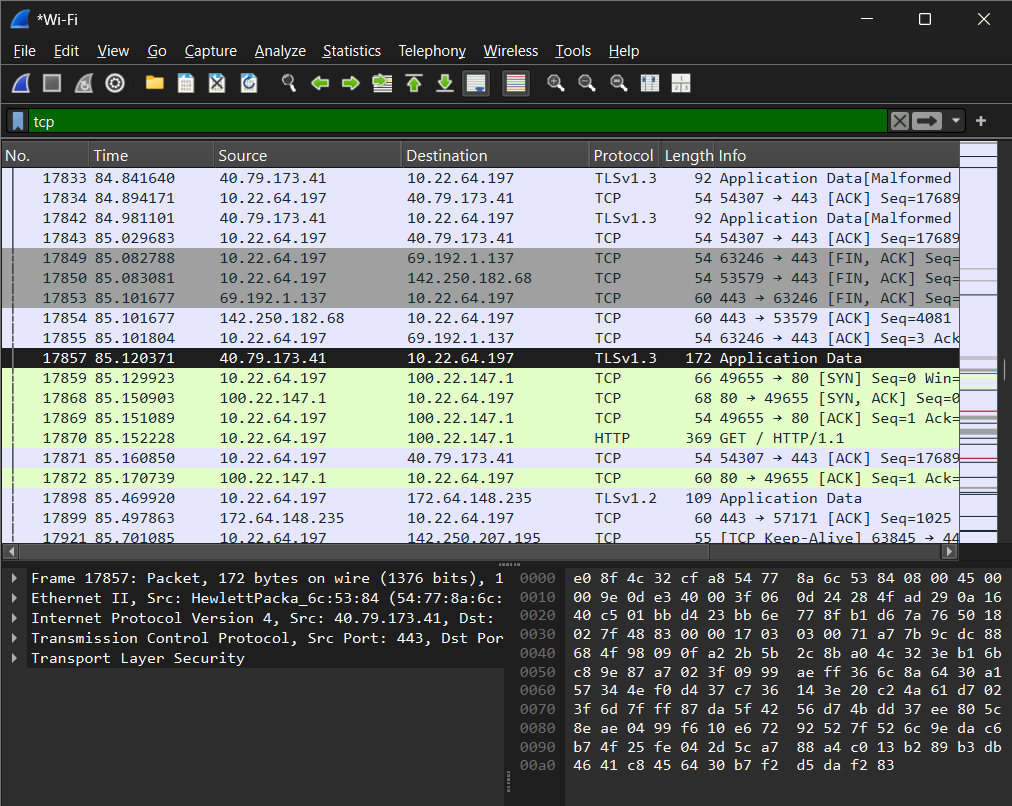


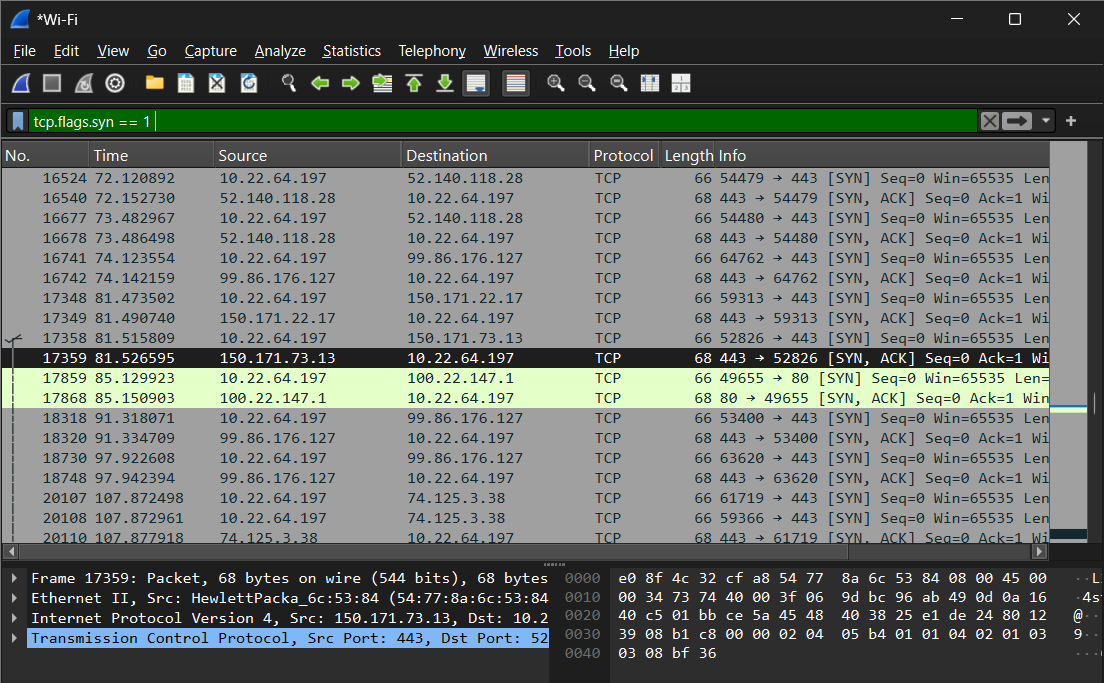
Live network traffic was captured while browsing common websites.

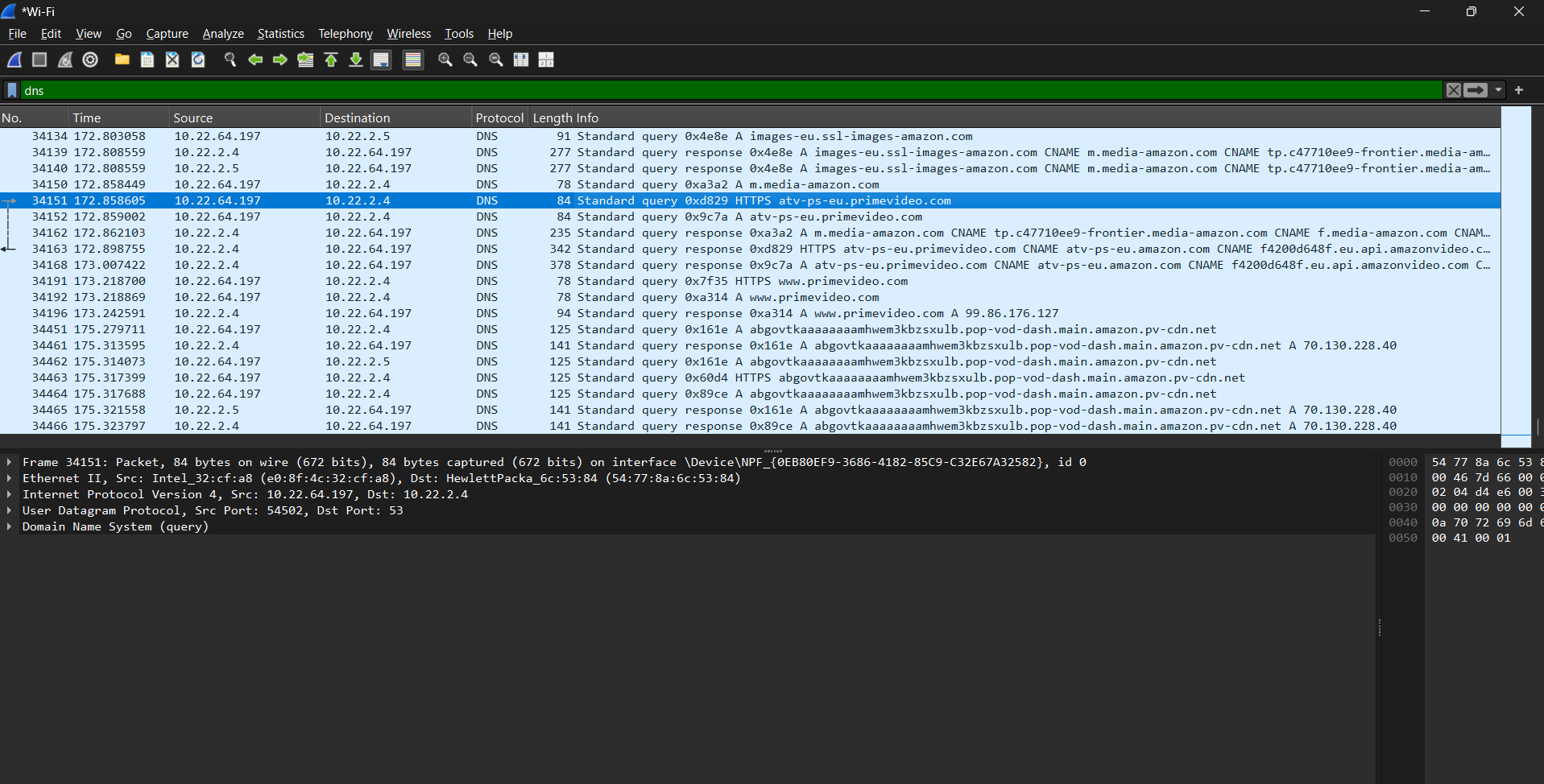


Display filters such as HTTP, DNS, and TCP were applied. 

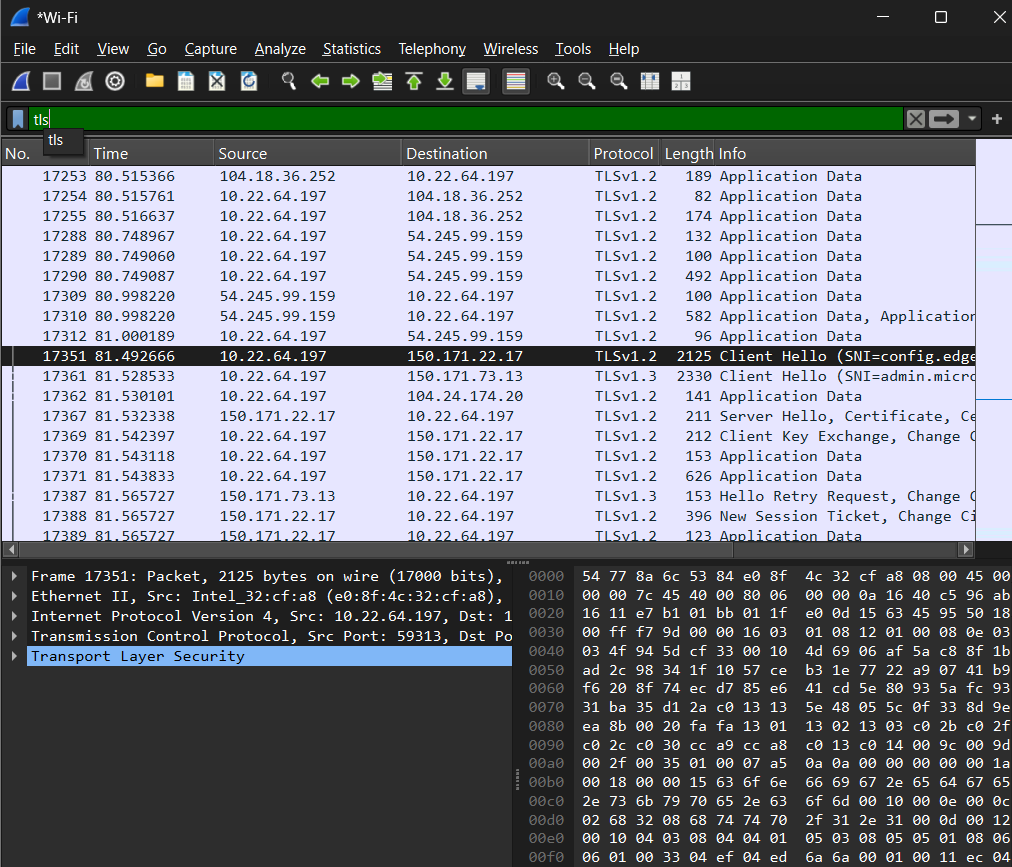




TCP three-way handshake was observed using SYN, SYN-ACK, and ACK packets. 

DNS queries were captured and analysed. 

Plain-text and encrypted traffic were identified.



The packet capture was saved in (. **pcapng**) format for further analysis.

**PCAP FILE**



**Observation**

Live network traffic was successfully captured using Wireshark on the active network interface.

* Multiple packets related to **DNS, TCP, and encrypted web traffic** were observed during the capture.
* DNS query packets were visible, showing that the system was requesting IP addresses for different domain names before accessing websites.
* TCP packets confirmed that connections followed the **three-way handshake process** (SYN, SYN-ACK, ACK) before data transmission started.
* Most of the web traffic was observed as **encrypted traffic (HTTPS/TLS)**, and the actual content of the communication was not readable.
* Very little or no **plain-text HTTP traffic** was observed, indicating secure browsing behaviour.
* The packet capture showed continuous background network activity even when no major applications were running.

Overall, the packet capture demonstrated how normal network communication takes place and how encryption helps protect data from being easily read by attackers.