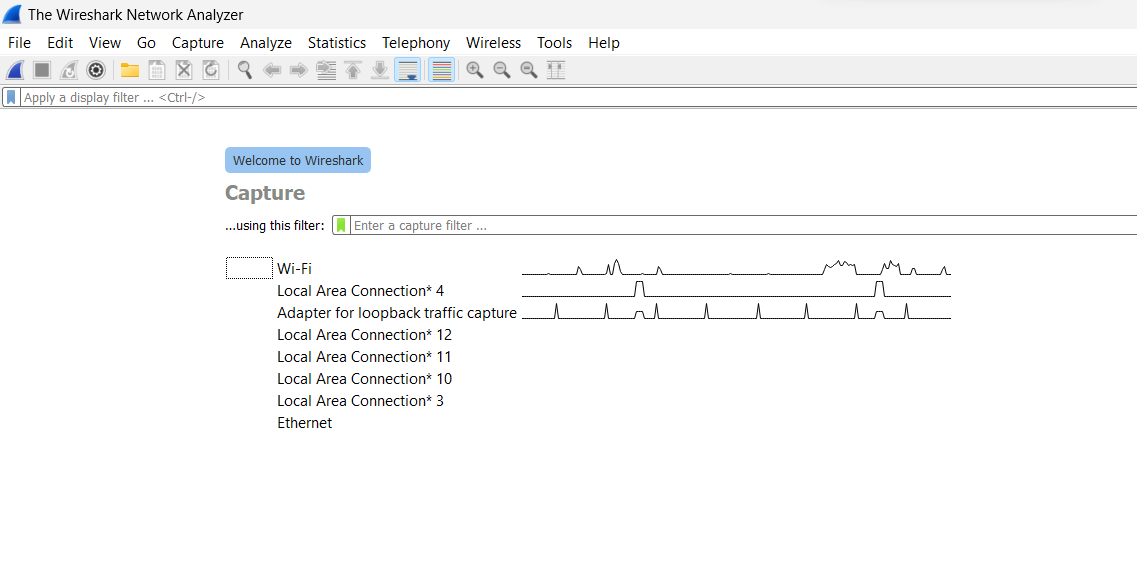


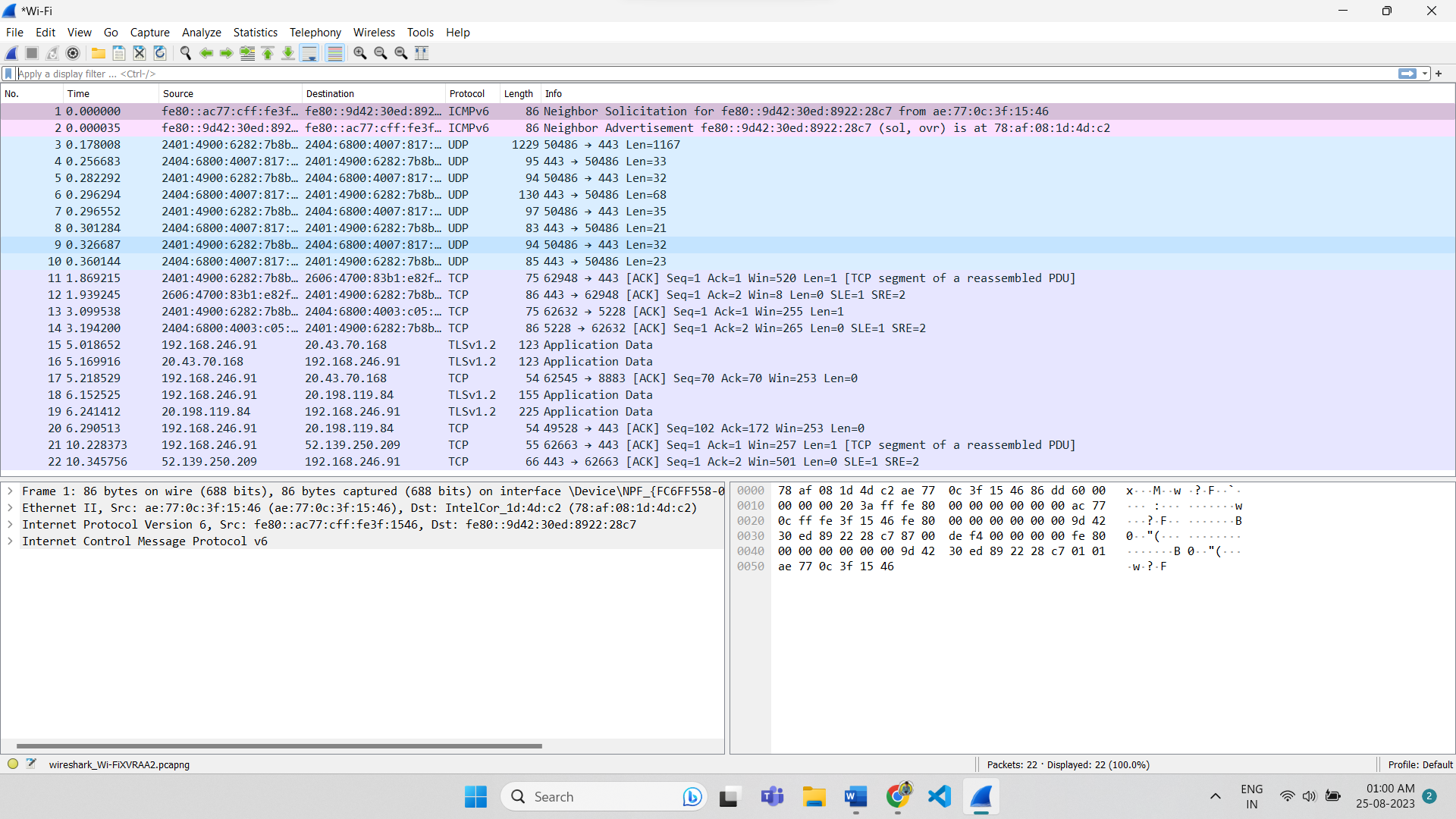
3) Wireshark

**INTERFACE (Home Screen) :**



In the main window, you'll see a list of available network interfaces. These are your network adapters through which Wireshark can capture packets. The above screen shows my adapters and the traffic on it.

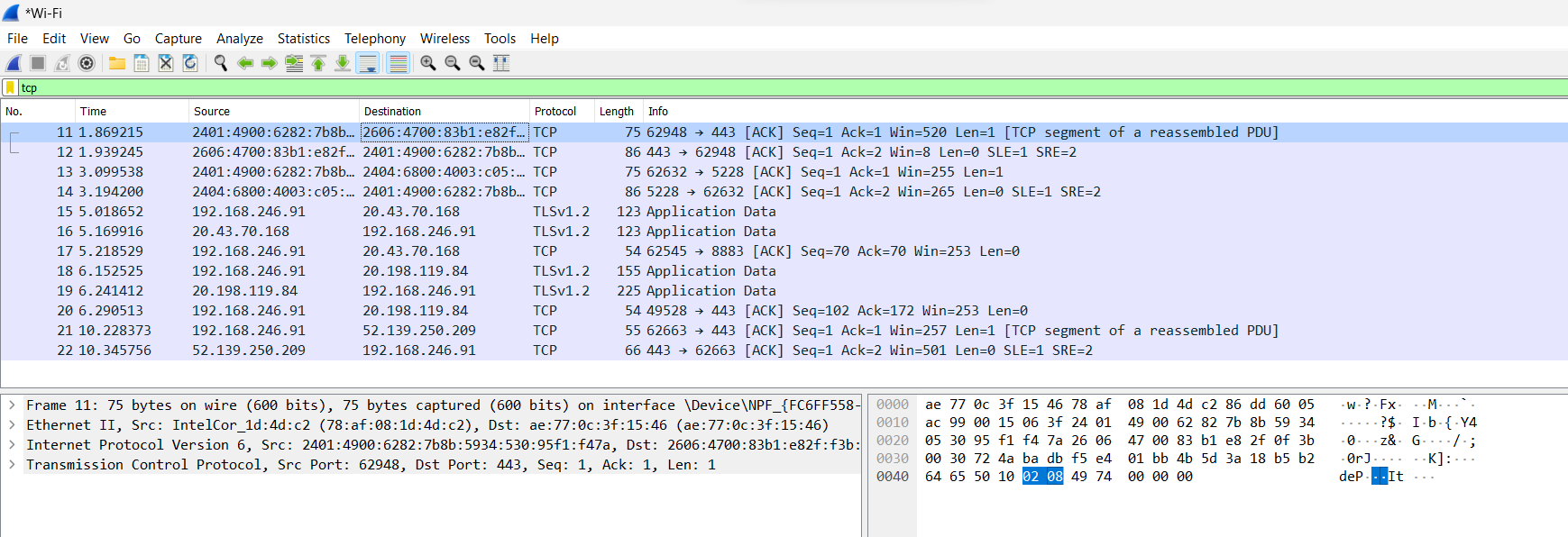
1. Here selecting Wifi adapter and **Capturing the packets for 5 sec.**



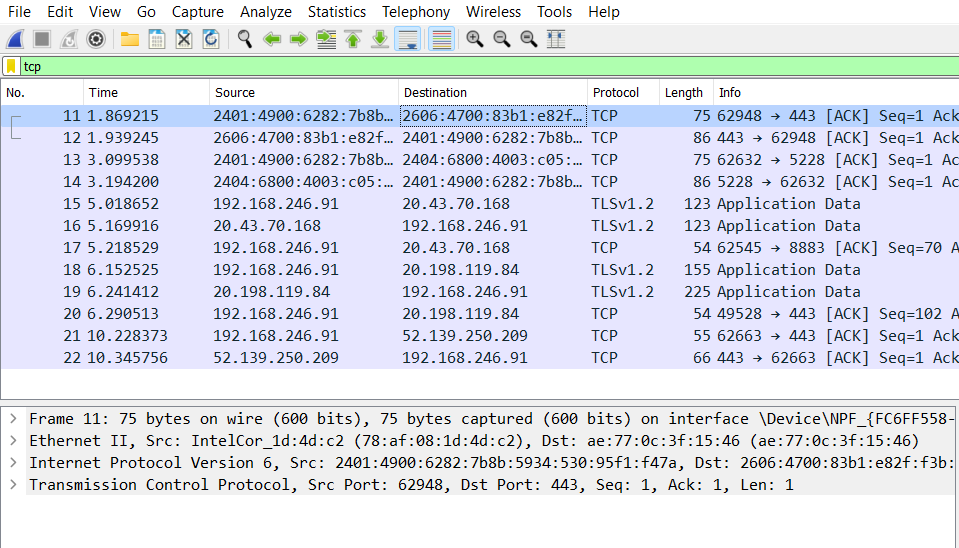
Locating TCP packet – packet no. 11

Locating UDP packet – packet no. 3

1. Applying filter to see only TCP packets.



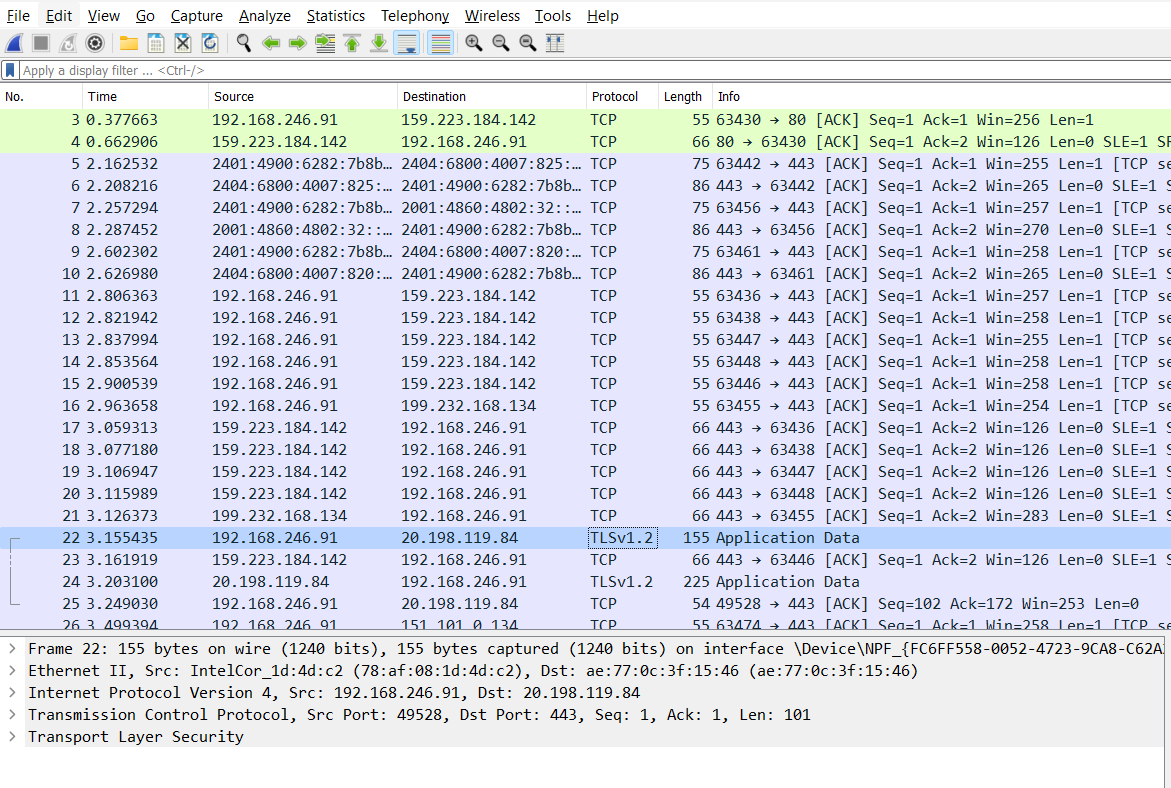
1. Locating a TCP packet and analyzing its layers.



Packet number – 11 (selected above)

No. of layers – 4 (layers details in lower window pane)

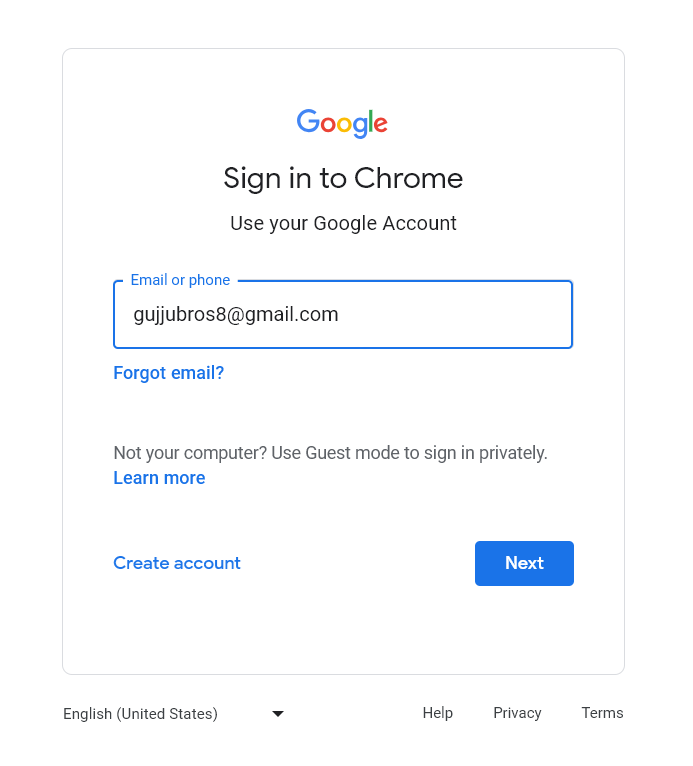
1. Locating a TLS packet and analyzing its layers.



Packet number – 22 (selected above)

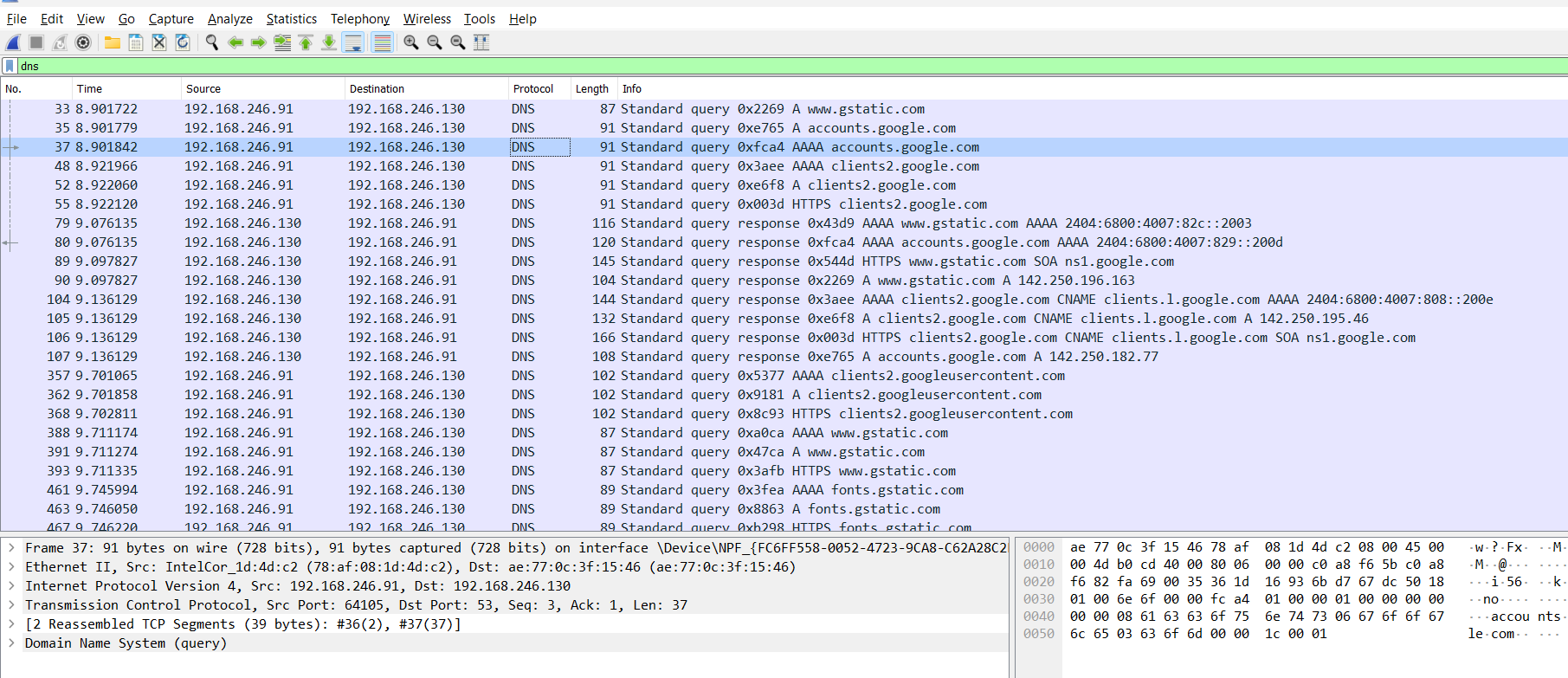
No. of layers – 5 (layers details in lower window pane)

1. Starting to collect the packets.
2. **Logging in to Google.**

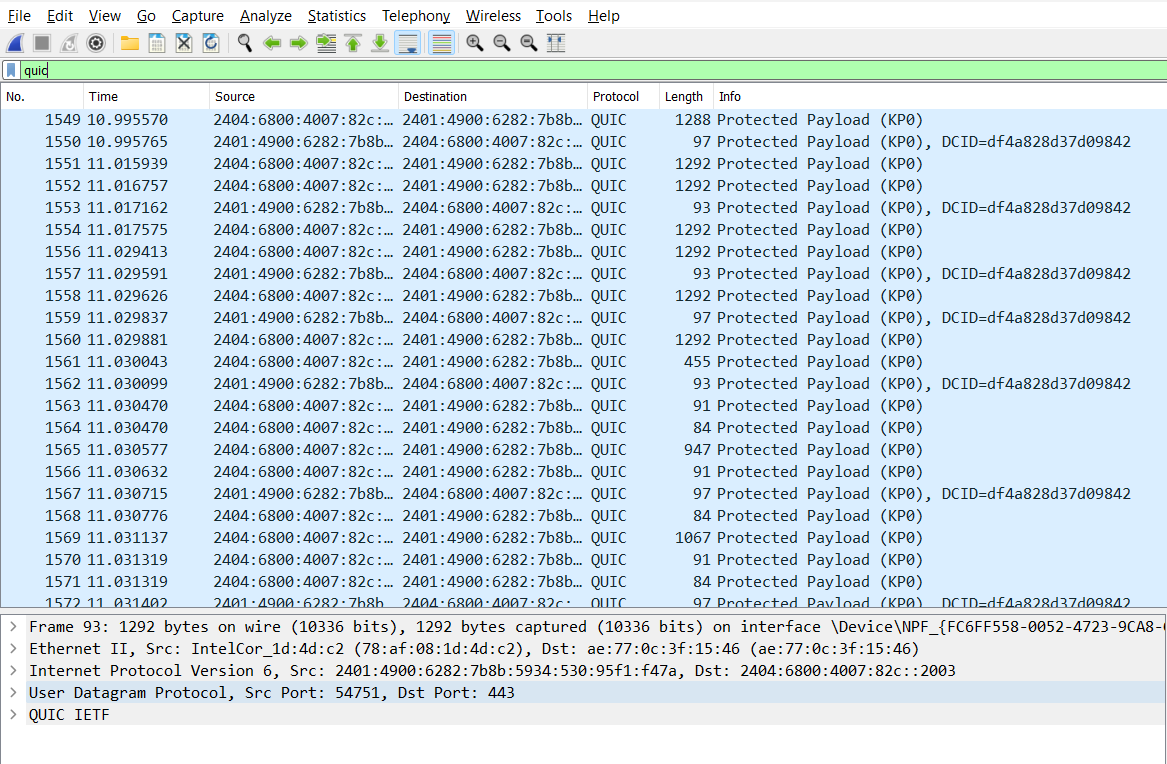


1. Stopping the packets capture.

**Locating Request and Response of Gmail Login.**

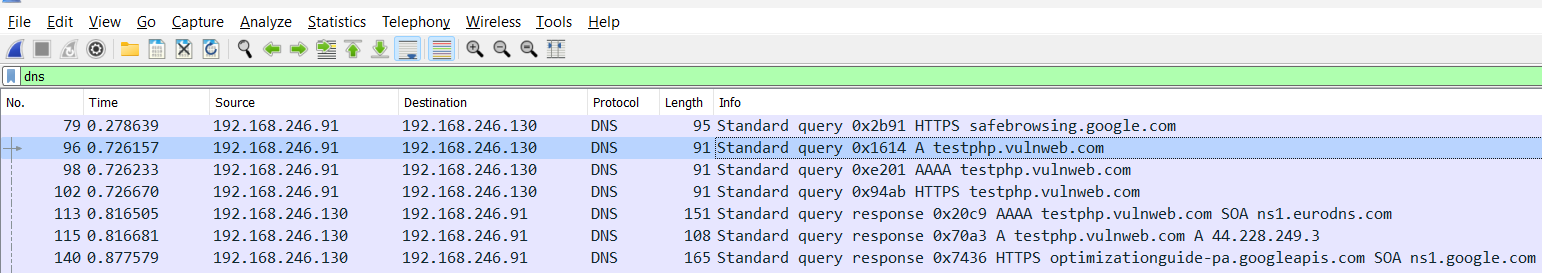


1. Packet 37 asking for **request**, and packet 79 onwards got the **response**.
2. Checking the presence of encrypted content.
3. Packets with description PROTECTED PAYLOAD.



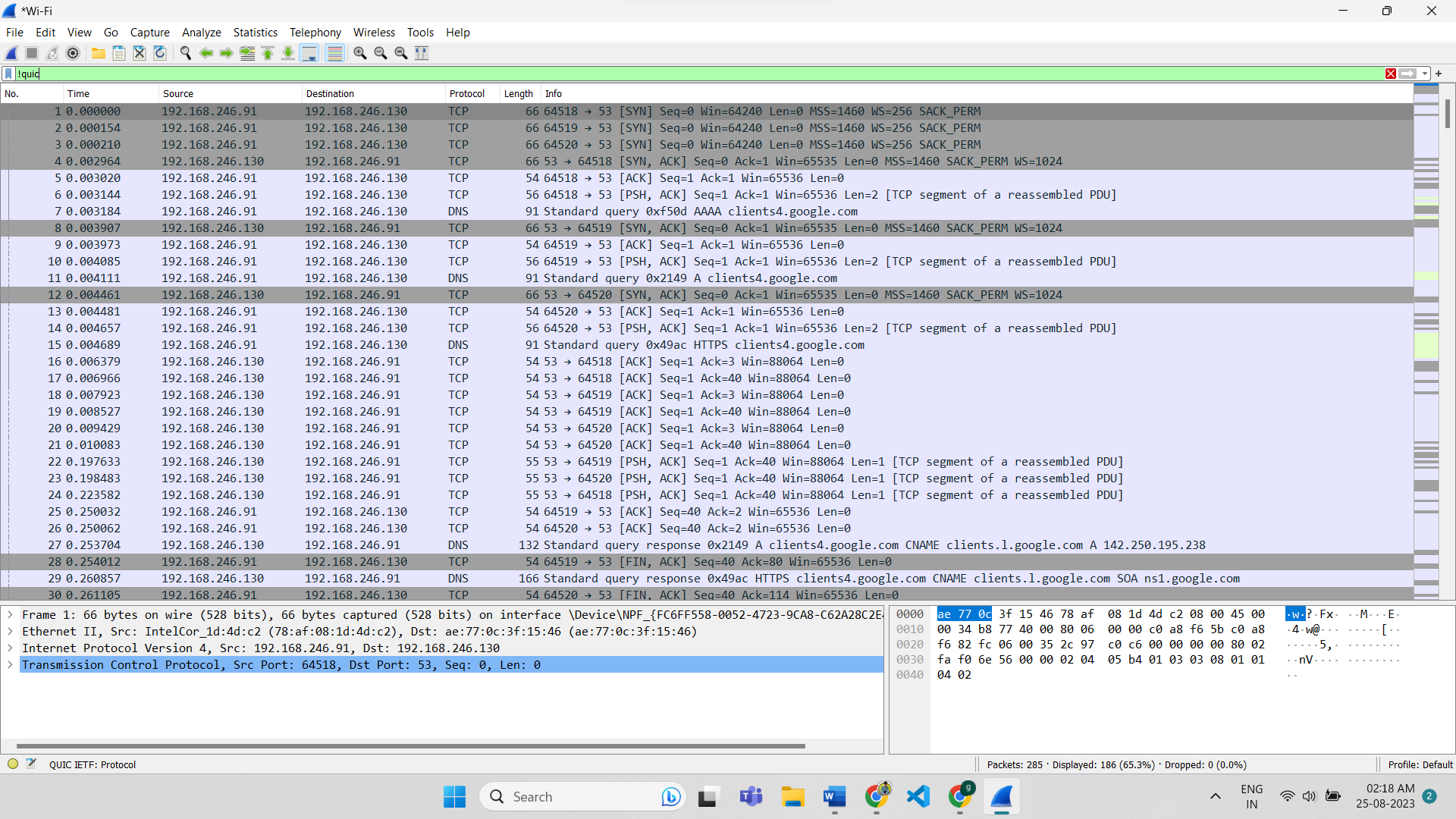
**Protected content**

1. Define Interface & Start collecting packets again
2. login with **guest account** in the webpage <http://testphp.vulnweb.com/login.php>



* Packet 102 asking for **request**, and Packet 113 **response** in above image.

1. Checking the presence of **unencrypted content.**
2. Type “!QUIC” under filters and click on apply.



**Unprotected content**

OVER

------X-----X-----X-----X-----X-----X-----X-----X-----X-----X-----X------X-----X-----X-----X-----X----

**!! . THANK YOU . !!**