Software and Cybersecurity Lab

CS445 Lab3

Name: Dipean Dasgupta ID: 202151188

Task: Explore Packet sniffing in wireshark and see how it captures and analyzes network traffic.

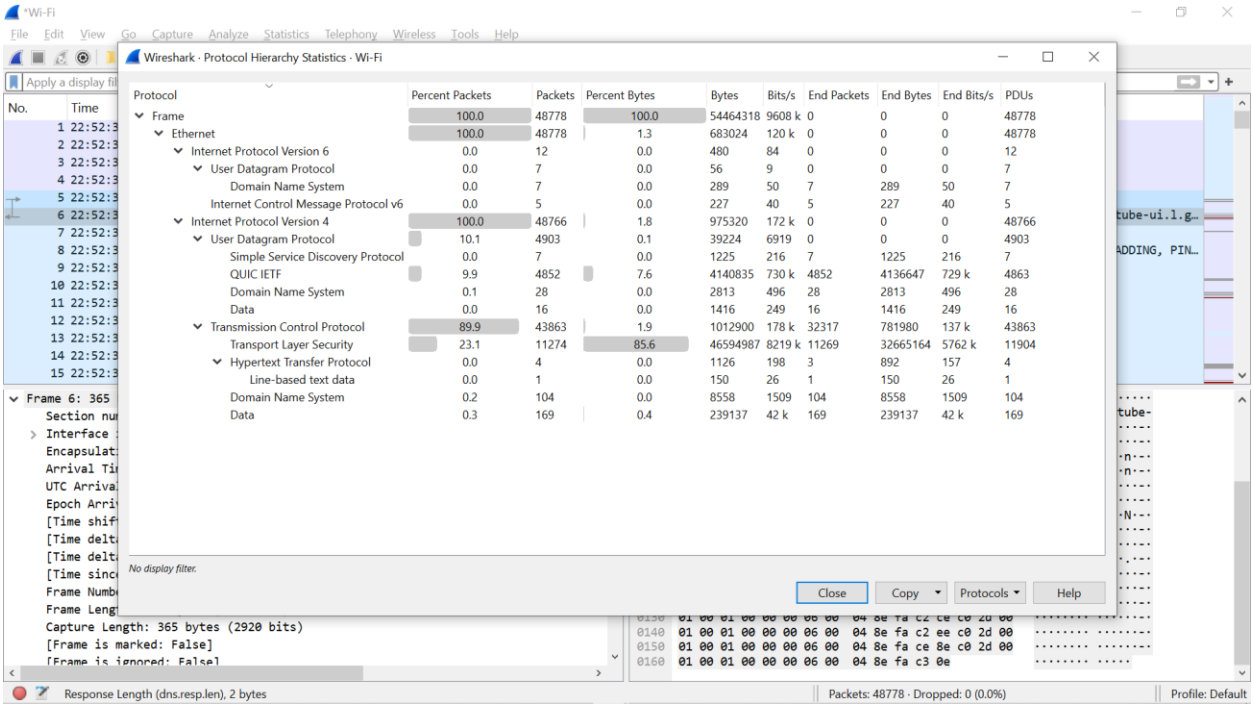
Setup:

- **OS: Windows 10**
- **Software: Wireshark**

Firstly Wireshark software was start up. As Laptop was connected to wifi, so from the capture interfaces options WiFi was selected. On clicking the capture button, for test one website was visited and then capture was halted. In the meantime Wireshark software captured all the packets.

Subtask1:

From the protocol hierarchy in statistics tab, information on the protocols that the packets were of were displayed. As per this particular capture the protocols are listed in the screenshot below:



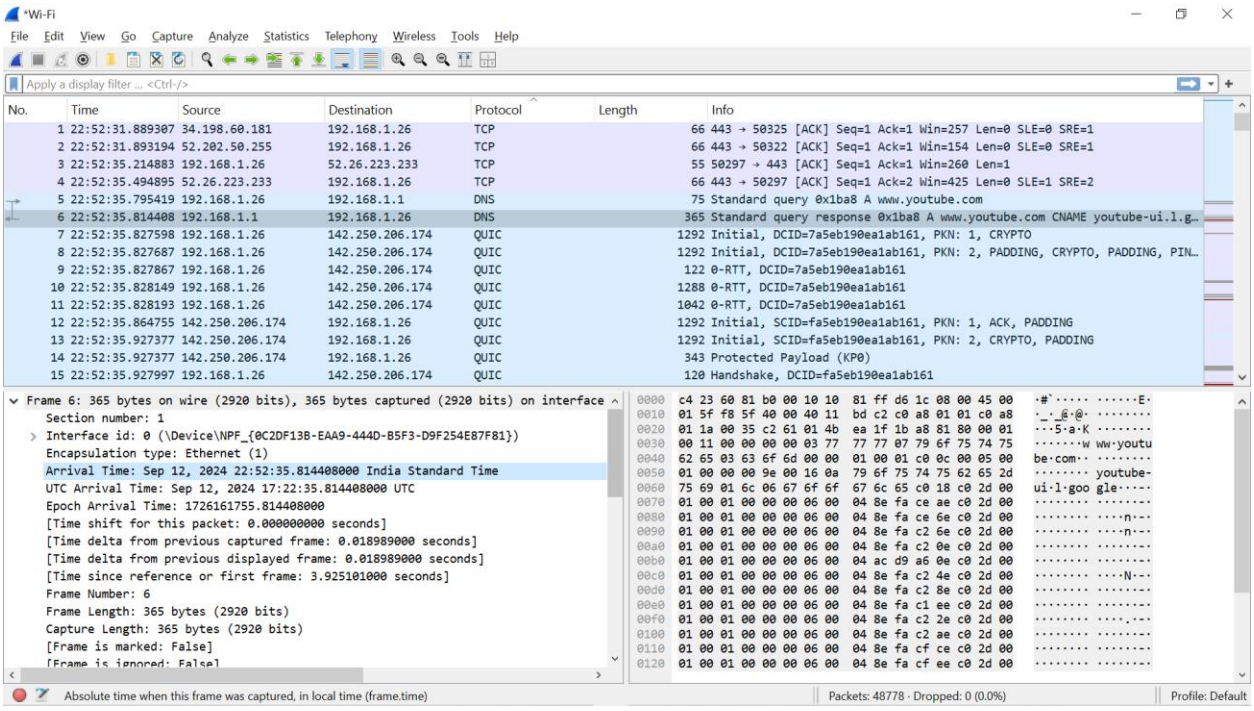
The image depicts that multiple protocols have been captured. List of those protocols as per wireshark is listed below:

1. TCP(43863) 2. QUIC(4852) 3. DNS (140) 4. TLS

5. ICMP(5) 6. HTTP(4) 7. UDP 8.SSDP (7)

Subtask 2:

Here, for a specific site request time elapsed from request to reply message is calculated.



From the screenshot we can see, when site of youtube was requested(5th one in list), query response was the 6th in the list.

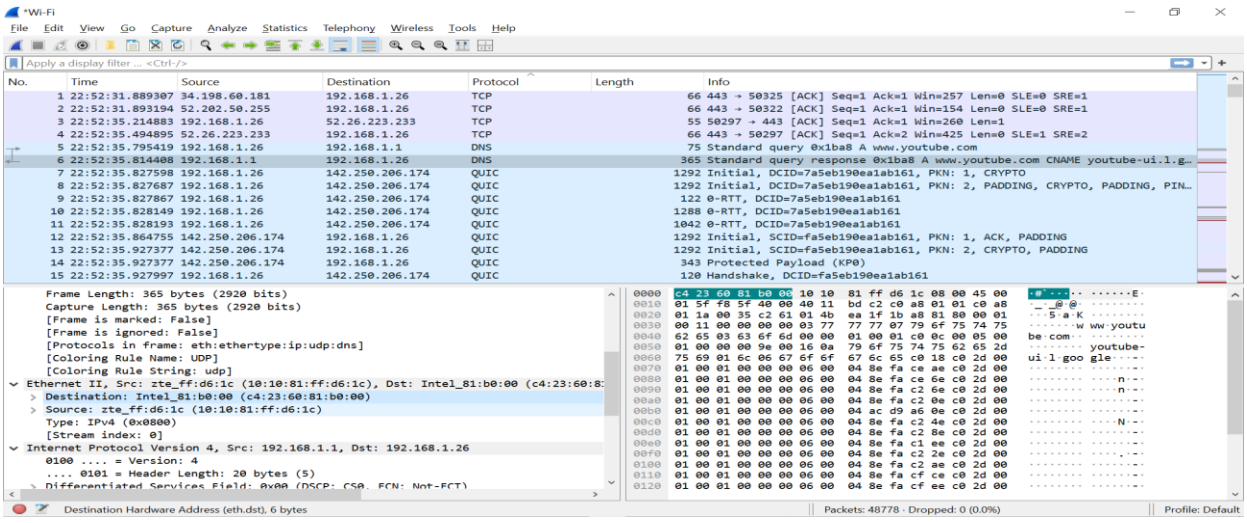
Query Timestamp: 22 : 52 : 35.795419

Query Response Timestamp: 22 : 52 : 35.814408

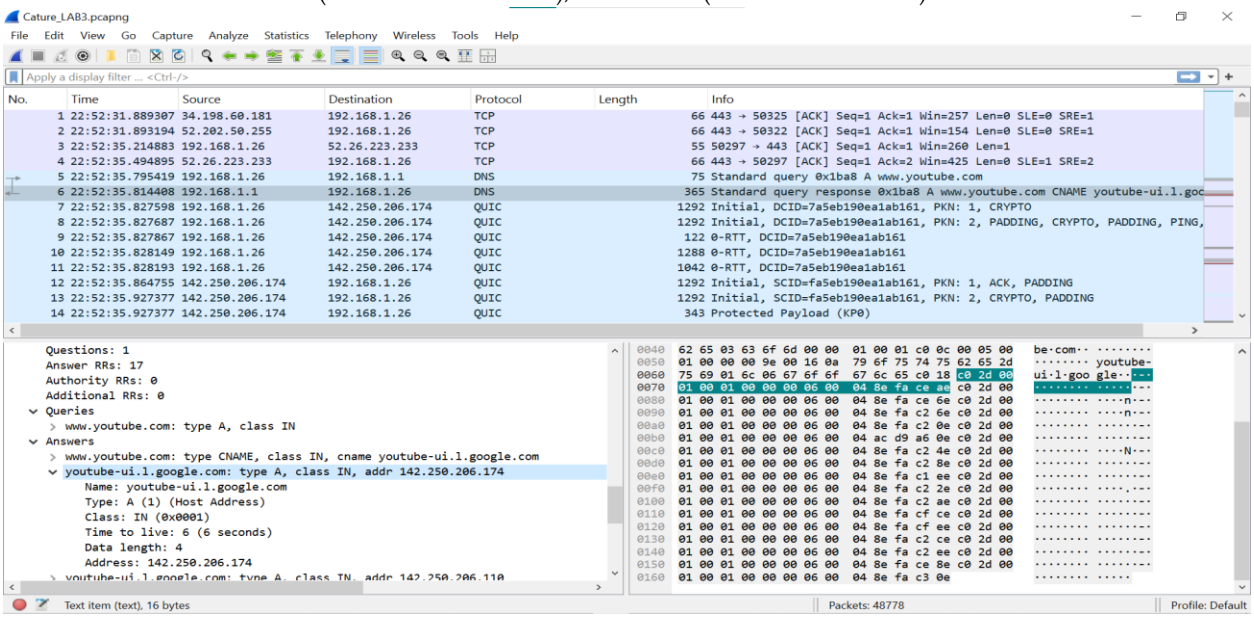
Time Elapsed: 0.018989000 seconds; this can be also verified from the Frame details ; given Time delta from previous captured frame is 0.018989000 seconds.

Subtask 3:

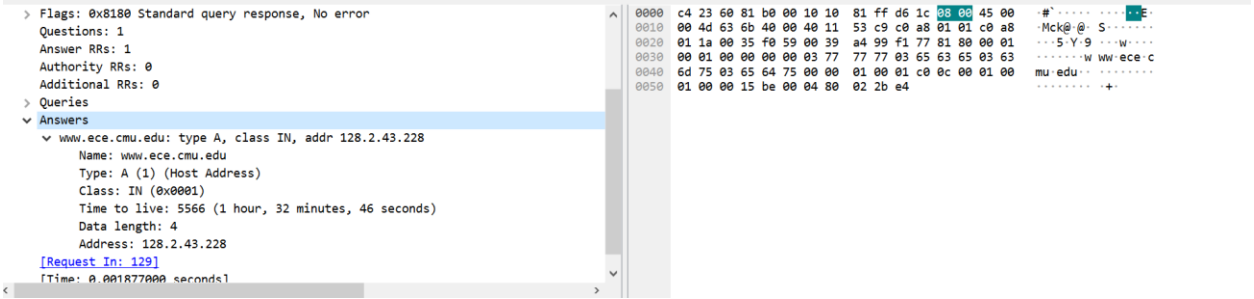
For my laptop, IPv4 Address: 192.168.1.26 MAC Address: C4-23-60-81-B0-00



From the screenshot, in the bottom left section under Ethernet II,
Destination: C4:23:60:81:b0:00(mac address matched), 192.168.1.26(IP address matched)



Here, since site query was of youtube , from the screenshot shared below; the ip address for youtube is: 142.250.206.174



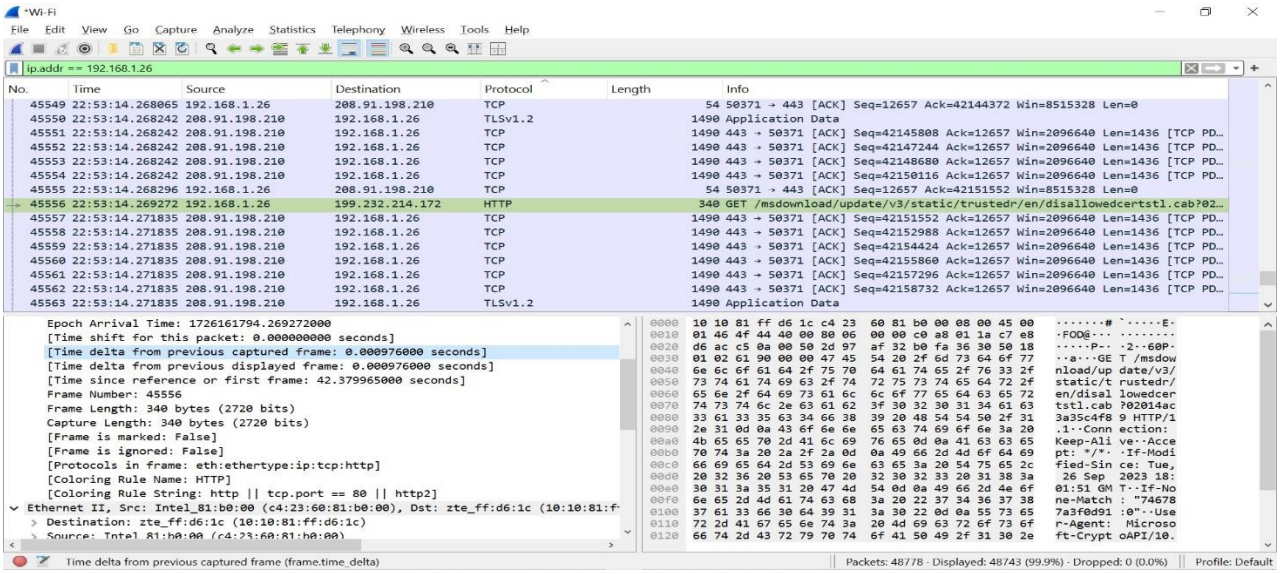
Ip address of www.ece.cmu.edu: 128.2.43.228

Subtask 4:

So, total number of packets captured by wireshark was 48778.

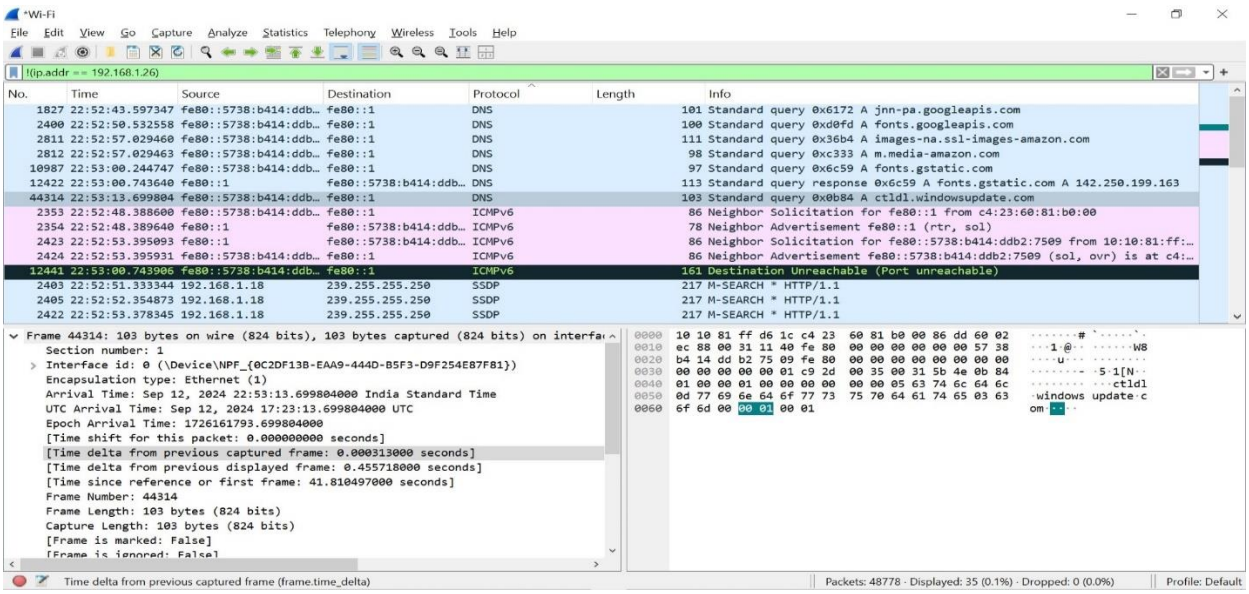
In order to find the packets out of these total packets contain IP address of my device, the filter was used below:

ip.addr == 192.168.1.26



Total 48743 out of 48778 contained IP address of my device.

Now, for finding number of packets not having IP address of my device, the following filter was applied:
!(ip.addr == 192.168.1.26)

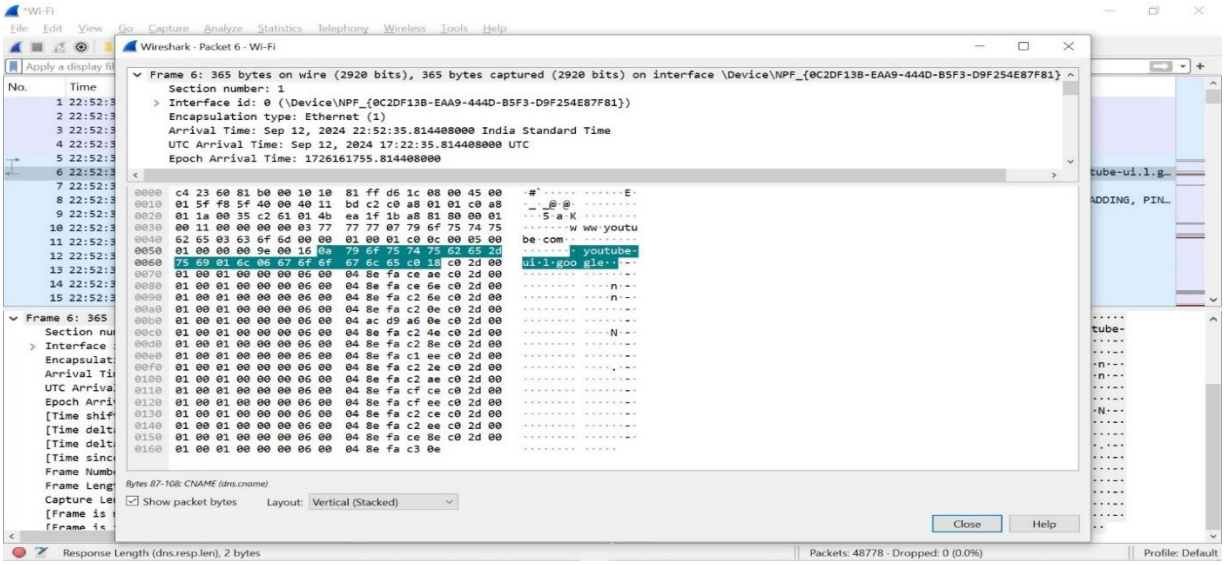


Total of 35 packets did not have my IP address. It justifies [48778-48743=35].

So here:

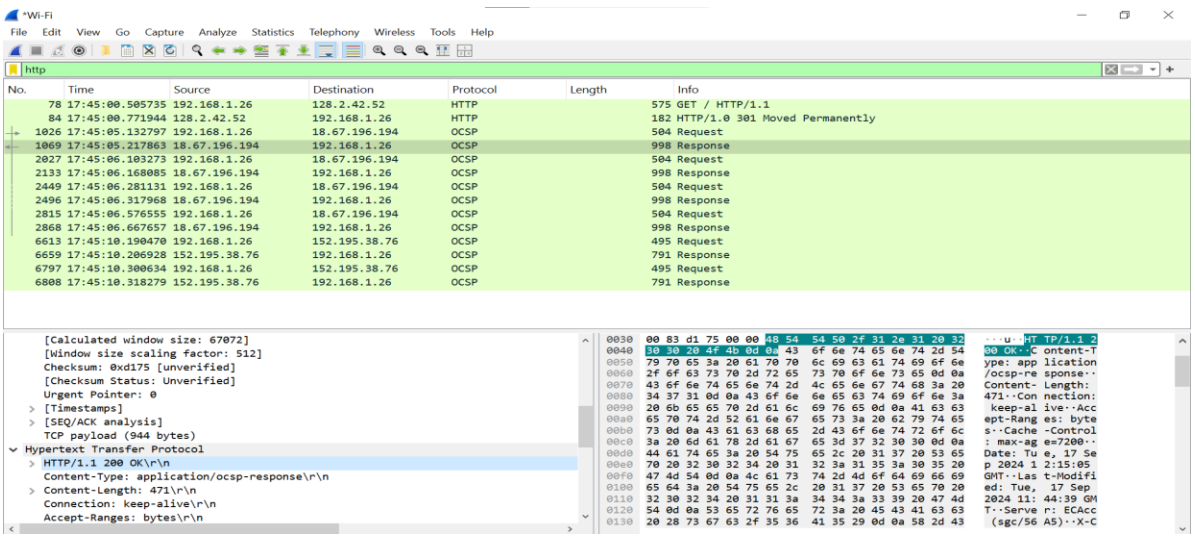
- **No Issues Detected:** Since the sum matches the total number of packets, there is no discrepancy or problem with how Wireshark is applying the filters.
- **Wireshark Behavior:** Wireshark handles the ip.addr filter correctly by including all packets that match the IP in either the source or destination fields and excludes them accurately when using the ! (NOT) operator.

Below screenshot of details of a packet is shared below:



Details of Packet 6 has been shared. Packet 6 was the response to query of a requested site.

Subtask 5:



Ip address of www.ini.cmu.edu: 128.2.42.52

1st packet : HTTP GET message

After that all the responses showed HTTP/1.1 200 OK message.

----------End of Assignment----------