Assignment-1 (Wireshark Fundamentals)

Shravya Vorugallu

Part-1:

a) Find the most active TCP conversation in the file (by bits per second).

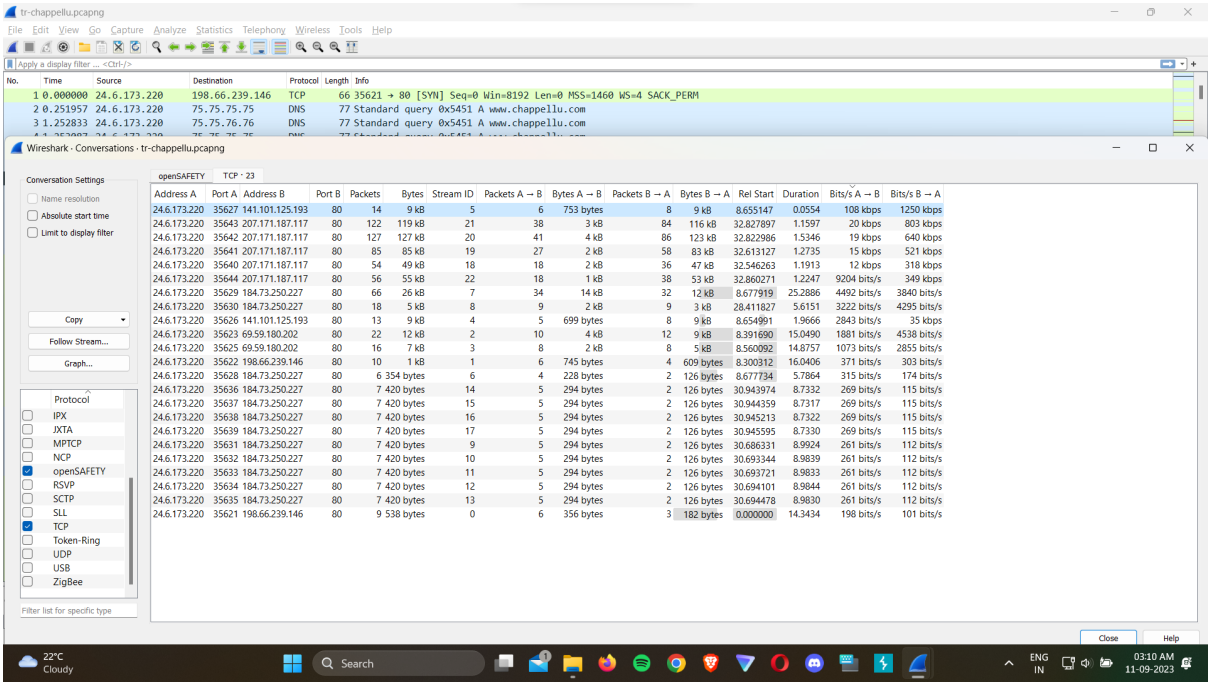
Solution:

When we arrange the Bits/s A->B in the TCP section in descending order, the top most field gives the most active TCP conversation. Here, the conversation between the addresses 24.6.173.220 and 141.101.125.193 which happened on port A 35627 is the most active conversation.

The Value is Bits/s A->B = **108kbps**

Bits/s B->A = **1250kbps**

Total Value - 1250+108 = **1358kbps**



b) What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select Apply as Filter > Selected > A → B. Save the packets once the filter is applied)

Solution:

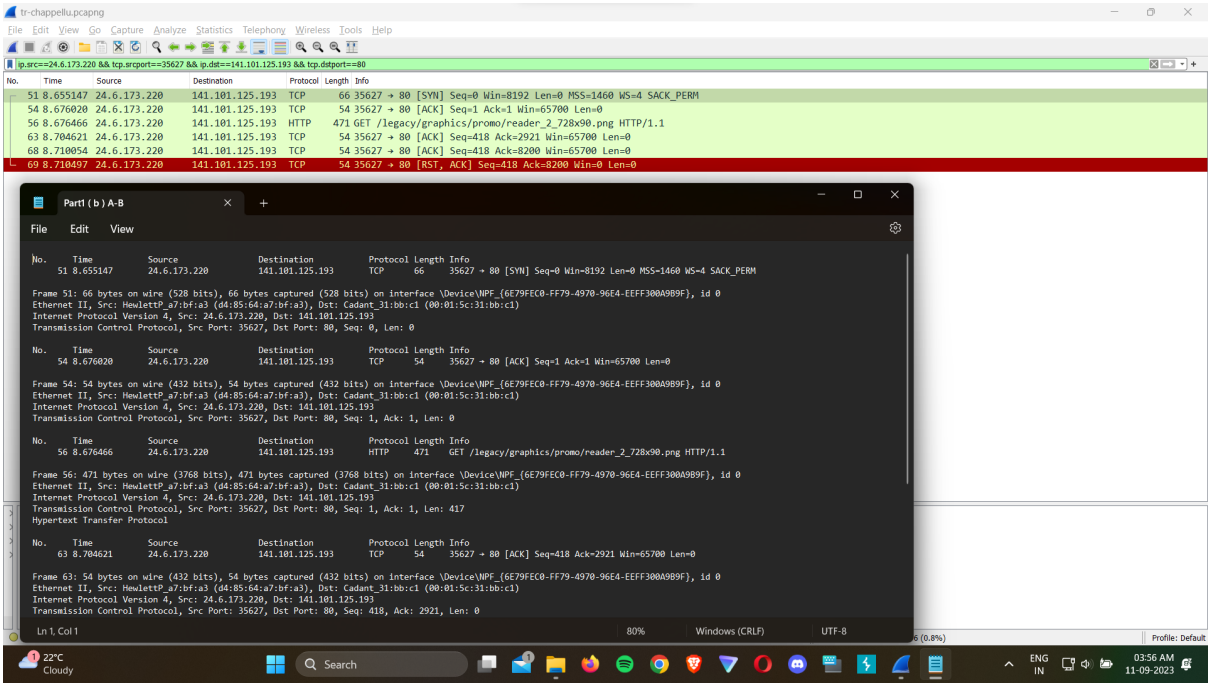
To find the total bytes, filter the most active conversation twice (with A->B and B->A) and export the file in text form. Add the total length fields in these two files to get the total bytes transferred in each file.

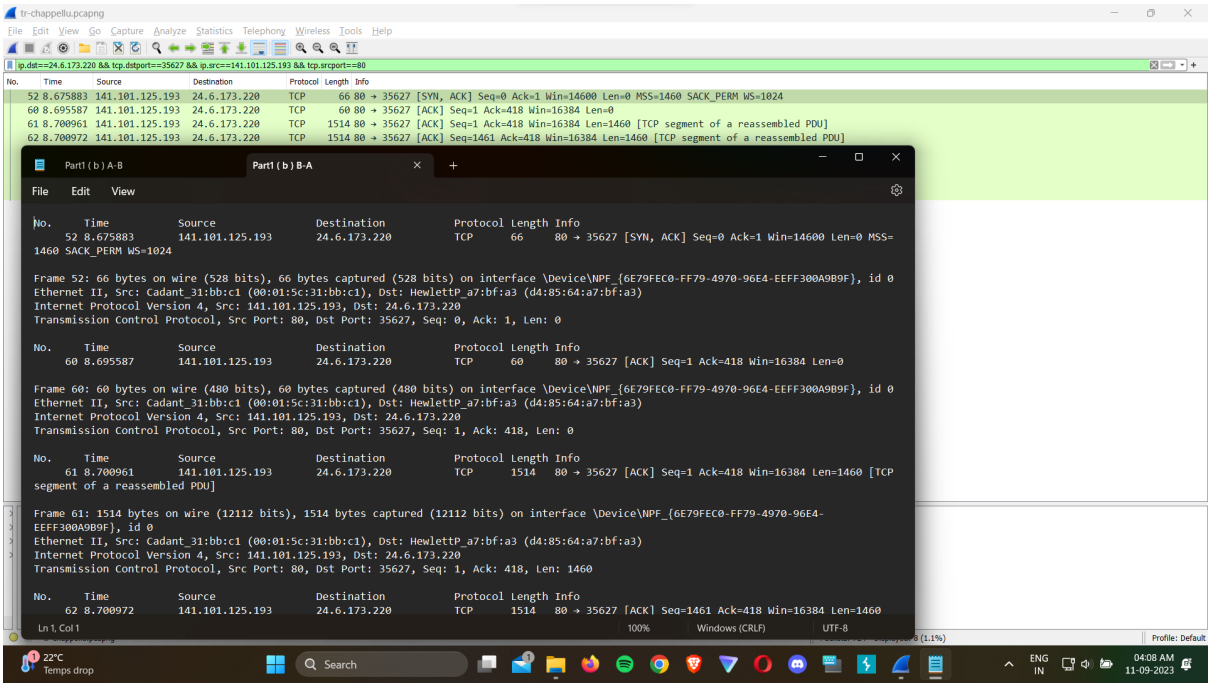
From the screenshots below, when we add the lengths, we get:

A->B = 66+54+471+54+54+54 = **753 bytes**

B->A = 66+60+1514+1514+1514+1514+1514+953 = **8649 bytes**

Total = 753 + 8649 = **9402 Bytes**



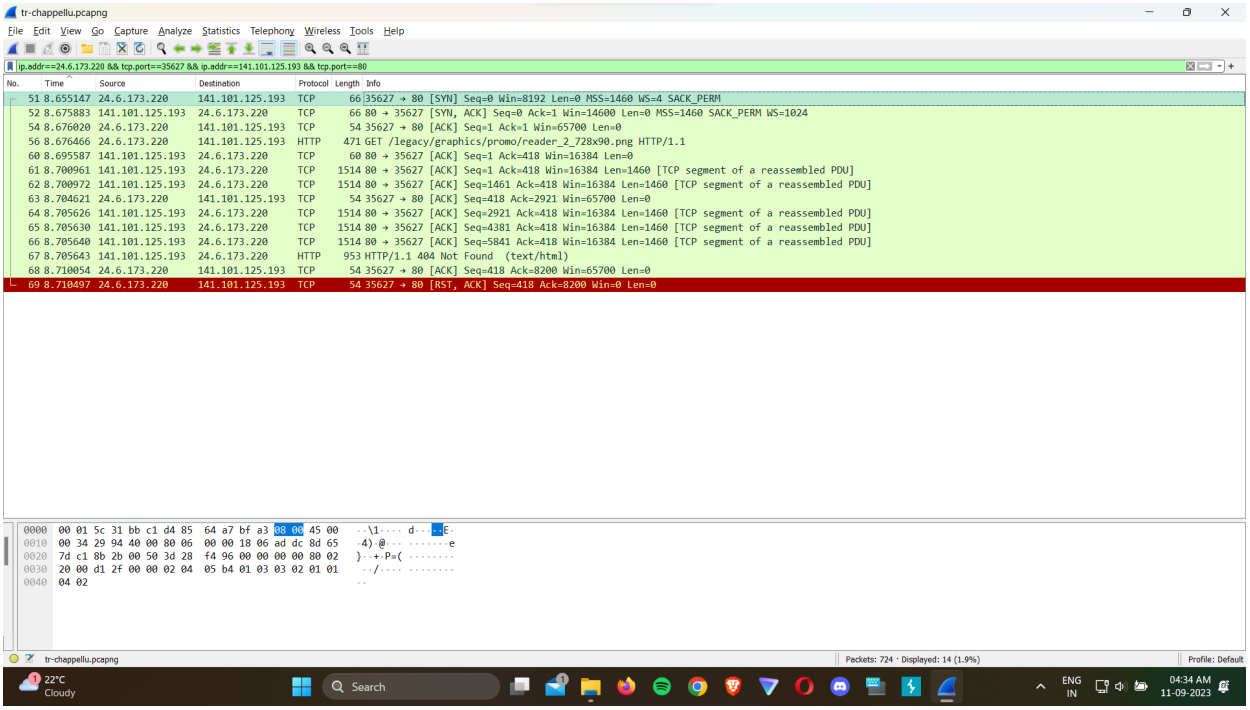


c) Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake.

Solution:

In the screenshot of the output below, the TCP handshake occurred between packets 51-54. To get the Round Trip Time (RTT) we subtract the timestamp of the SYN packet from the timestamp of the ACK packet.

RTT (SYN -> SNY/ACK -> ACK) = 8.676020 - 8.655147 = **0.020873 seconds.**



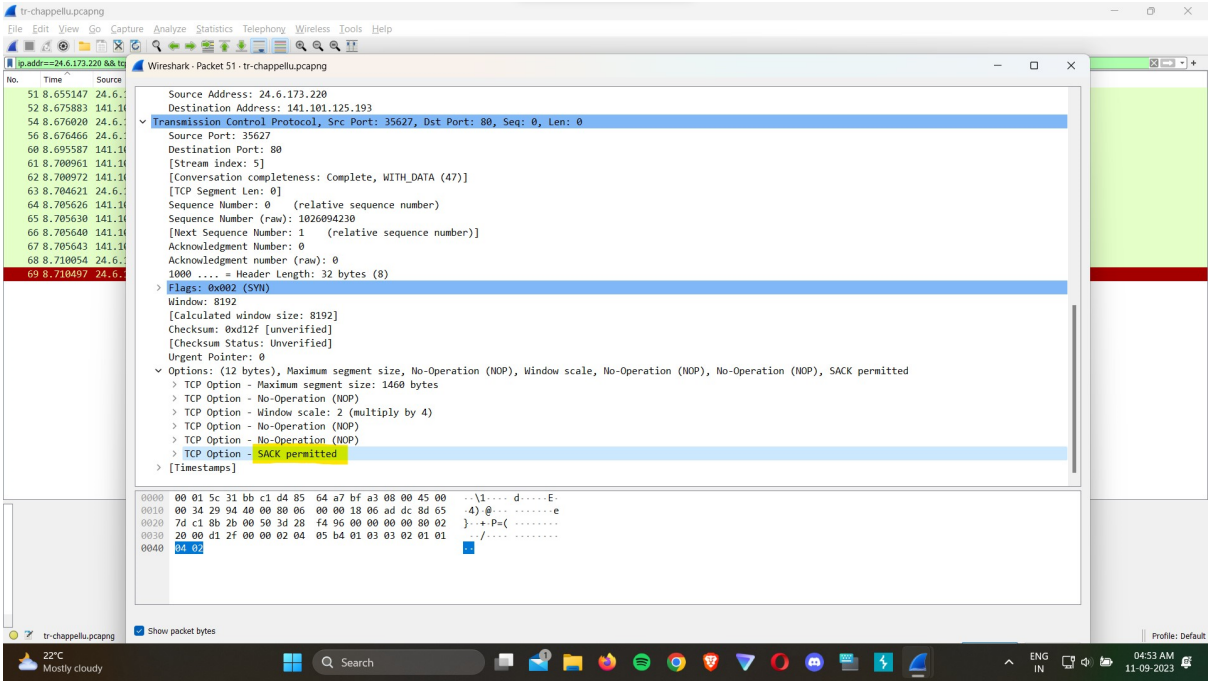
d) What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.

Solution:

Sack acknowledgements, also known as SACK, are used to let the sender know about the packets received. This helps mitigate any missing packet issues.

To know if SACK is permitted, we need to go to the options section in the SYN packet and see the permission.

In the below screenshot, the TCP option shows **"SACK Permitted"** which indicates that selective acknowledgements are permitted in this conversation.

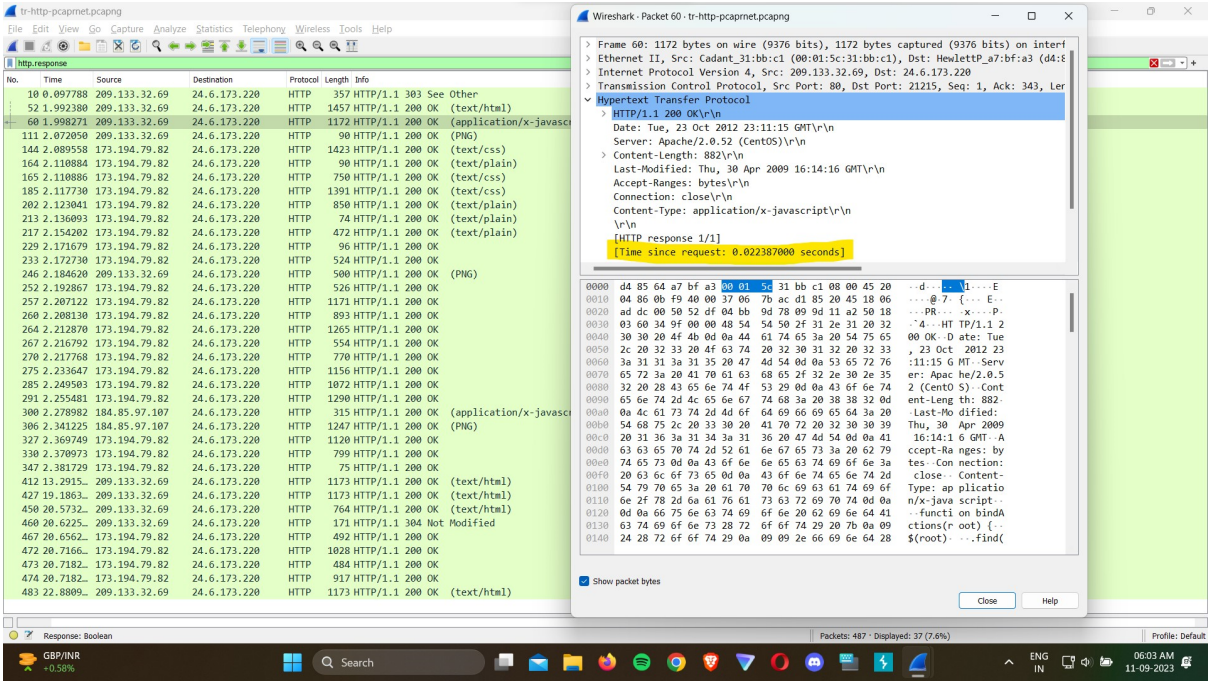


Part-2:

a) **Use a filter to display the HTTP response time for each HTTP request.**
Solution:

The filter used to display each HTTP request is **“http.time”.** This displays all the requests with a parameter for response time.
Now we need to go into the packet details and navigate to the **Hypertext Transfer Protocol** section. In this, we can find the field **[Time Since Request]** which indicates the response time of that specific response.

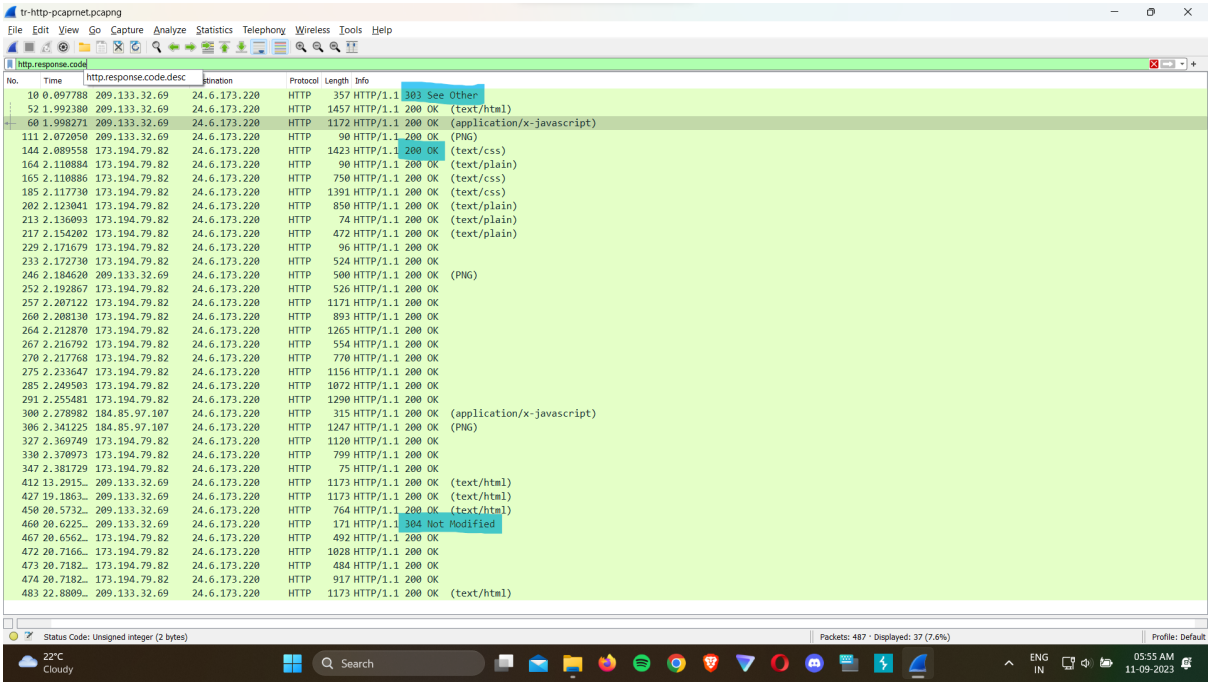
The screenshot below shows an example of this.



b) **Define and explain the significance of each HTTP response status code.**

Solution:
There are 3 HTTP response codes given in the file that are highlighted in the scccreenshot below.

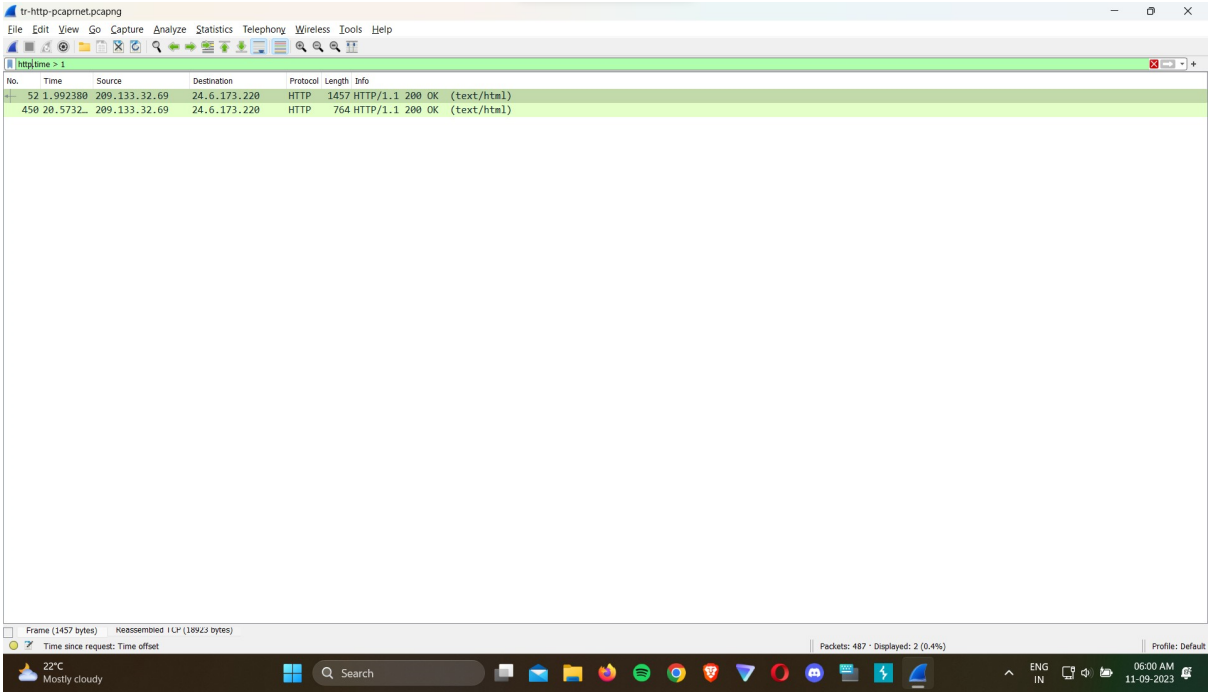
1) ***200 (OK)*** : This code signifies that the server has successfully processed the request made by the client. It helps in confirming the operations and successful responses. It helps browsers in caching these requests.
2) ***303 (See Other)*** : This code indicates that the client should make a new GET request to a different URI. Typically used to redirect clients to other resources or locations, This helps to avoid double form submission, which enhances the user experience.
3) **304 (Not Modified**) : This code shows that the indicated response is notmodified and that it is not necessary to process it again. This helps in cache optimization and increase the efficiency of the server.



c) Apply a filter that lists packets wherein the HTTP response time is greater than one second.

Solution:

To list all packets with response time greater than 1 we need to use the filter **“http.time>1”.** This will list out all the packets with a response time of less than 1 sec. The Screenshot below shows all the packets with the response lime less than 1sec.



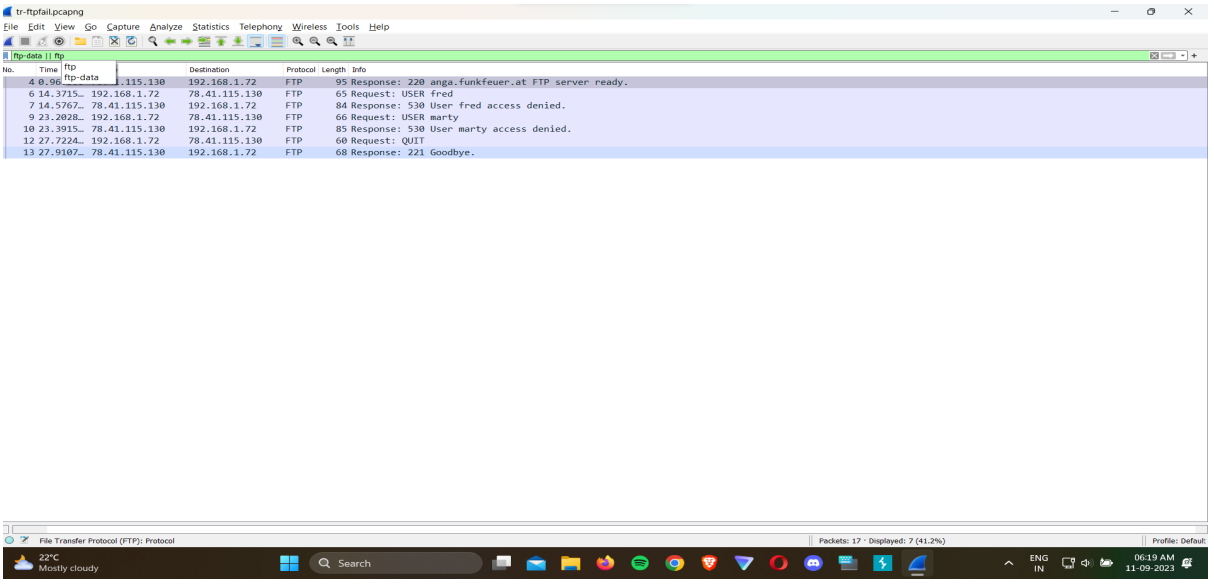
Part-3:

a) **Use a filter to display the FTP request and response packets.**

Solution:

To display the FTP packets, we can use the filter **"ftp-data || ftp"** which shows both ftp and ftp-data packets in the sorted list.

The Screenshot below shows all the FTP request and response packets in the pcap file.



b) **List the server and client IP addresses and port numbers.**

Solution:

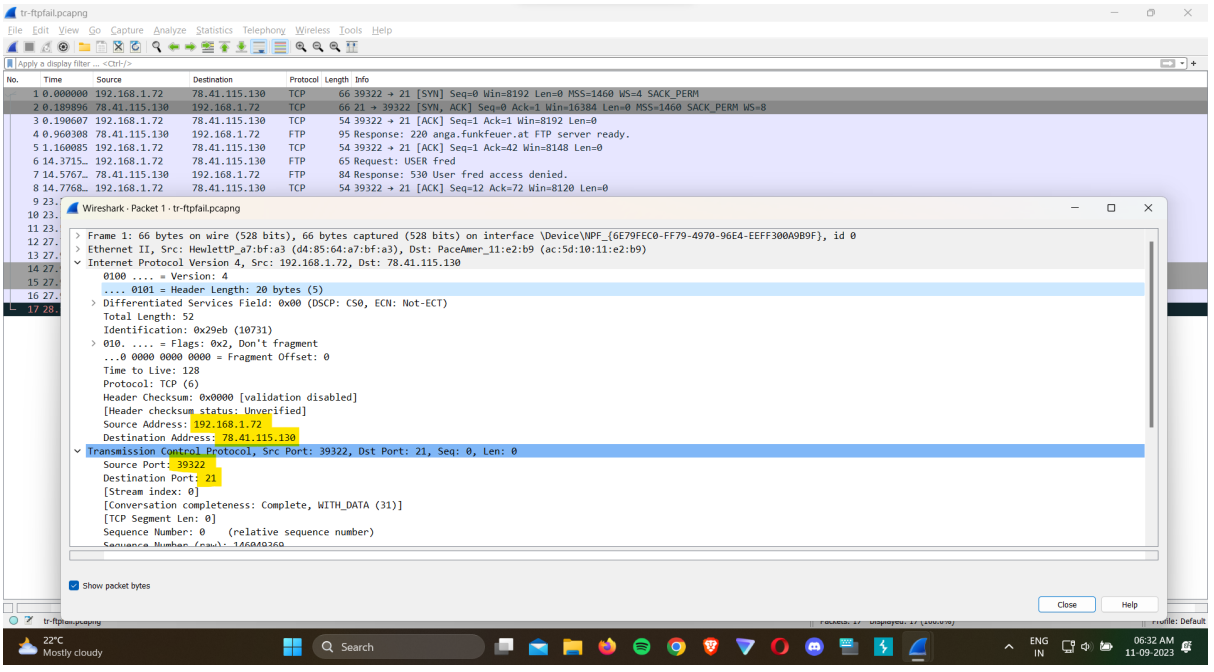
Client IP address : **192.168.1.72**

Server IP address : **78.41.155.130**

Client Port : **39322**

Server Port : **21**

In the screenshot below, I have highlighted the IP addresses and the port numbers.



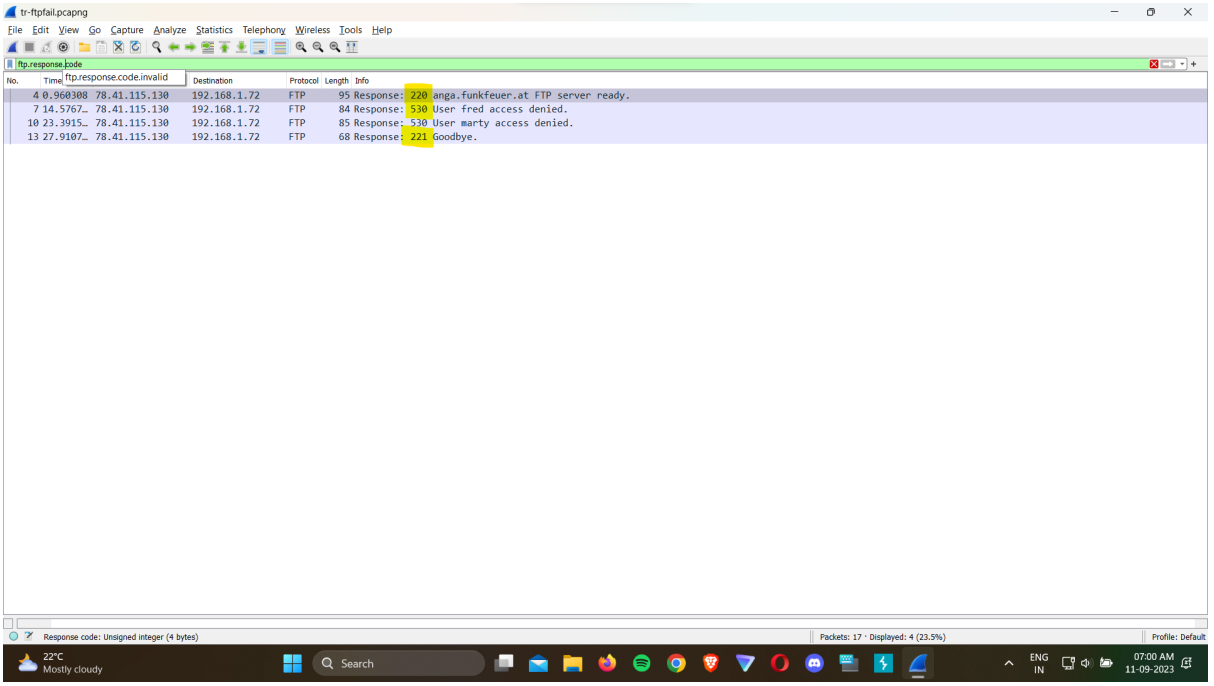
c) **Use another filter to display only the FTP response codes for the packets. Define and explain the significance of the response codes.**
Solution:
There are three FTP response codes shown in this file which are 220, 530 and 221.

220 (Service Ready): This code is given when the FTP server is ready to take orders from the client. This usually happens after the first connection is made.

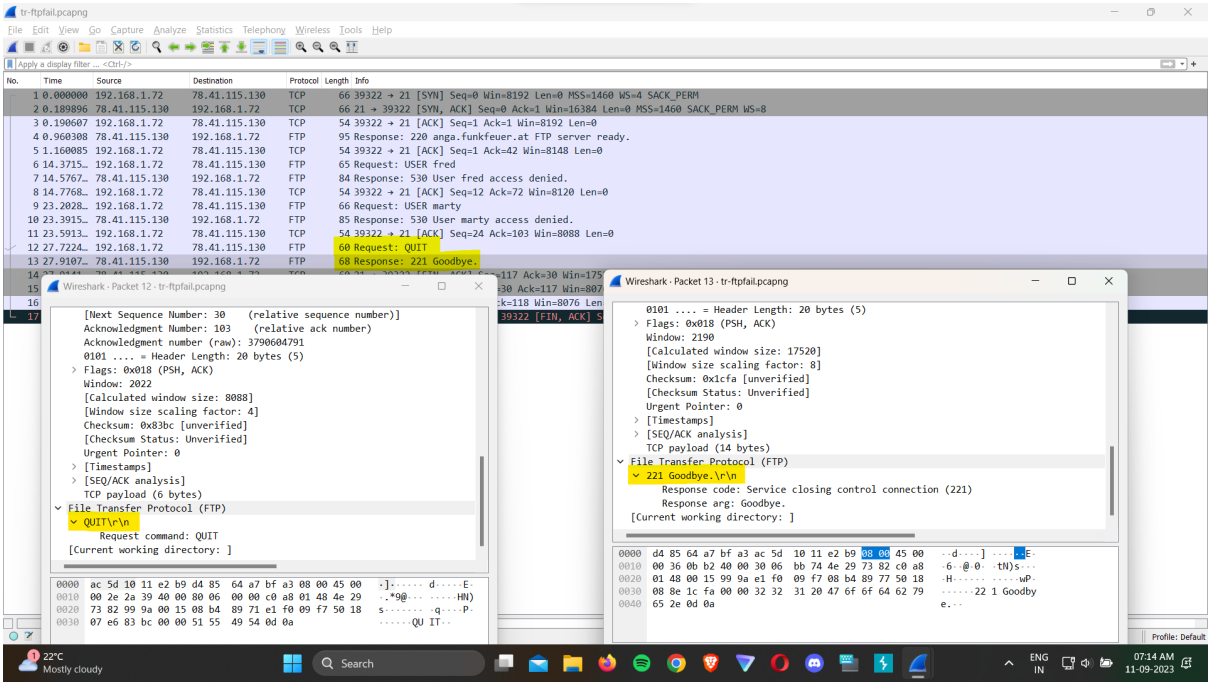
530 (Login Authentication Failed): It is given in scenarios when the authentication has failed while logging in. This helps prevent access to the files it was meant to access.

221 (Service Closing Control Connection): This is given to show that the FTP session is over and the client and server has ended their connection.

The screenshot below shows the FTP codes used in the pcap file.



d) **Is the FTP termination initiated by server or client? Please justify your answer.**
Solution:
The termination of FTP is initiated by the client. In the screenshot below the client sends the command **“QUIT”** to which the server responds back with a “**221 Goodbye**”. Hence, it shows that the client is the one to initiate the termination of the FTP request.



e) **How secure is FTP?**

Solution: It is not a secure protocol by itself, as it does not provide any kind of encryption, which means that any kind of data that is transferred over this protocol can easily be sniffed. Sending login credentials over this is very dangerous, which shows the weak authentication capabilities of the protocol. It also lacks a way to provide data integrity. Thus, it is not a safe protocol by itself, and it is better to use other alternative protocols like FTPS or HTTPS.

Part-4:

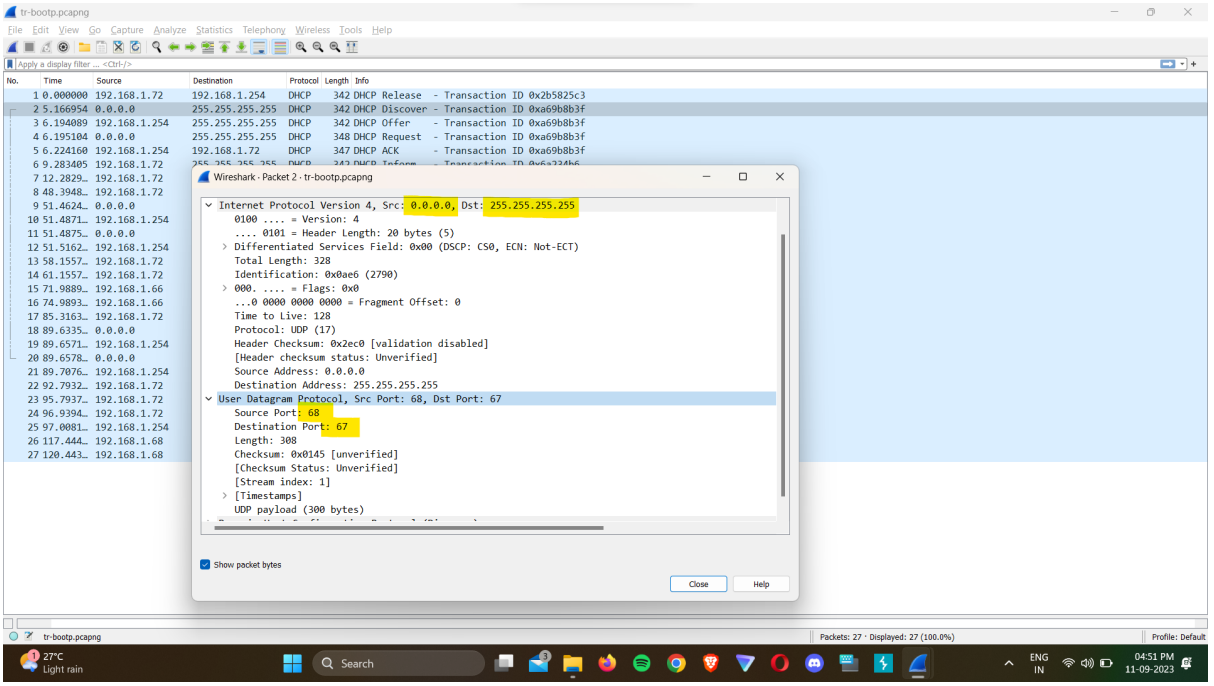
a) **What layer of the OSI model can DHCP Discover packets be found? What type of packet is DHCP Discover? List the source and destination IP addresses and port numbers.**

Solution:

DHCP Discover packets are found in the **Second Layer** of the of the OSI model, which is the **Data Link Layer**. They are part of the first step of DHCP, in which a client looks for a DHCP server on the network.

DHC Discover is a type of **Broadcast Packet.** It is the packet that the DHCP client uses to ask for any DHCP server on the network's setup information.

Source IP - **0.0.0.0**
Destination IP - **225.225.225.225**
Source Port - **68** (UDP port)
Destination Port - **67** (UDP port)



b) How many DHCP packets are exchanged between the client and server before the client receives an IP address? Define and explain the commands used in the DHCP handshake.

Solution:

There are four major steps in the DHCP handshake: DHCP Discover, DHCP Offer, DHCP Request, and DHCP Acknowledgement. In the DHCP Acknowledgement packet the client receives an IP address with a lease duration, which is the duration of the IP address that can be used by the client. **There are 3 packets exchanged before the IP address is received in the fourth packet** between the client and the server.

DHCP Commands.

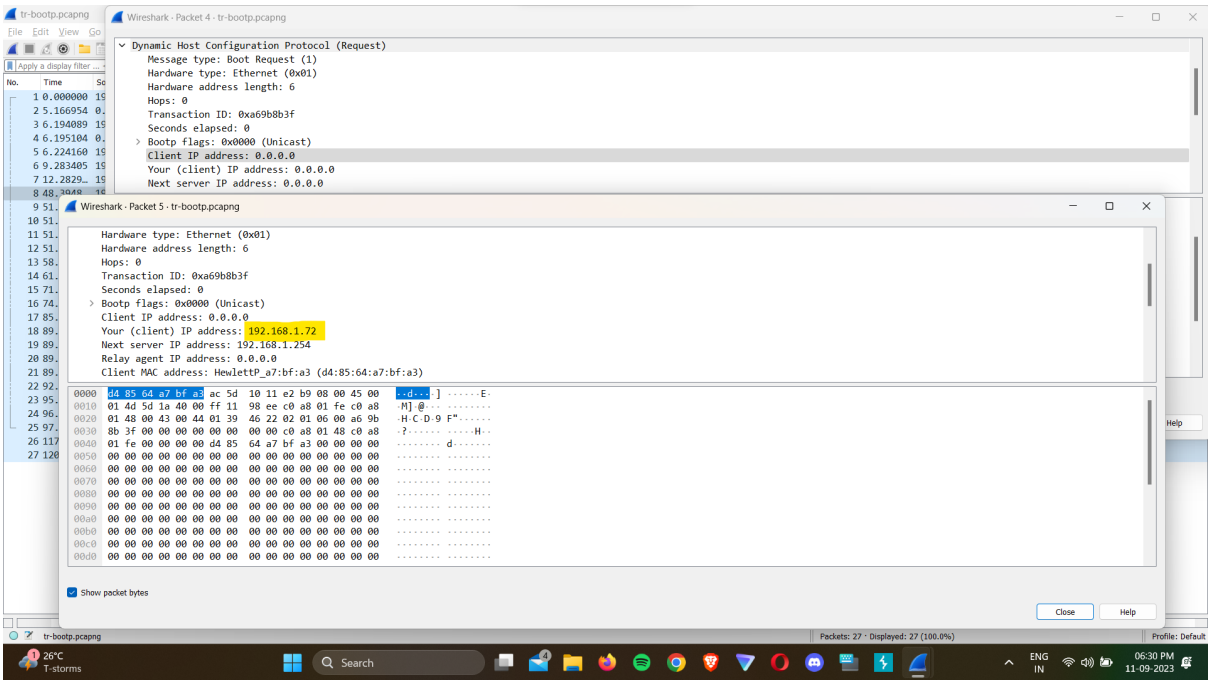
DHCP Discover: This packet is broadcast by the client on the network, requesting information about the IP configuration. The IP addresses used are 0.0.0.0 by the client or source and 225.225.225.225 for the destination.

DHCP Offer: When the DHC server receives the discover packet, it sends a DHCP Offer packet, which has information about the available IP addresses and information about the configuration. The source is the IP of the DHCP server, and the destination is the broadcast channel, which is 225.225.225.225.

DHCP Request: When the client receives the Offer packet, it chooses an IP address from the list and checks if any other systems are using the same IP address. Once it finds that the IP is free to use, it selects that IP and sends a DHCP request packet into the broadcast channel, requesting the IP.

DHCP Acknowledgement: When the DHCP server receives the request from the client, it verifies again if the IP address is still available and sends a DHCP ACK packet to the client with details, configuration, and the lease agreement of the IP.

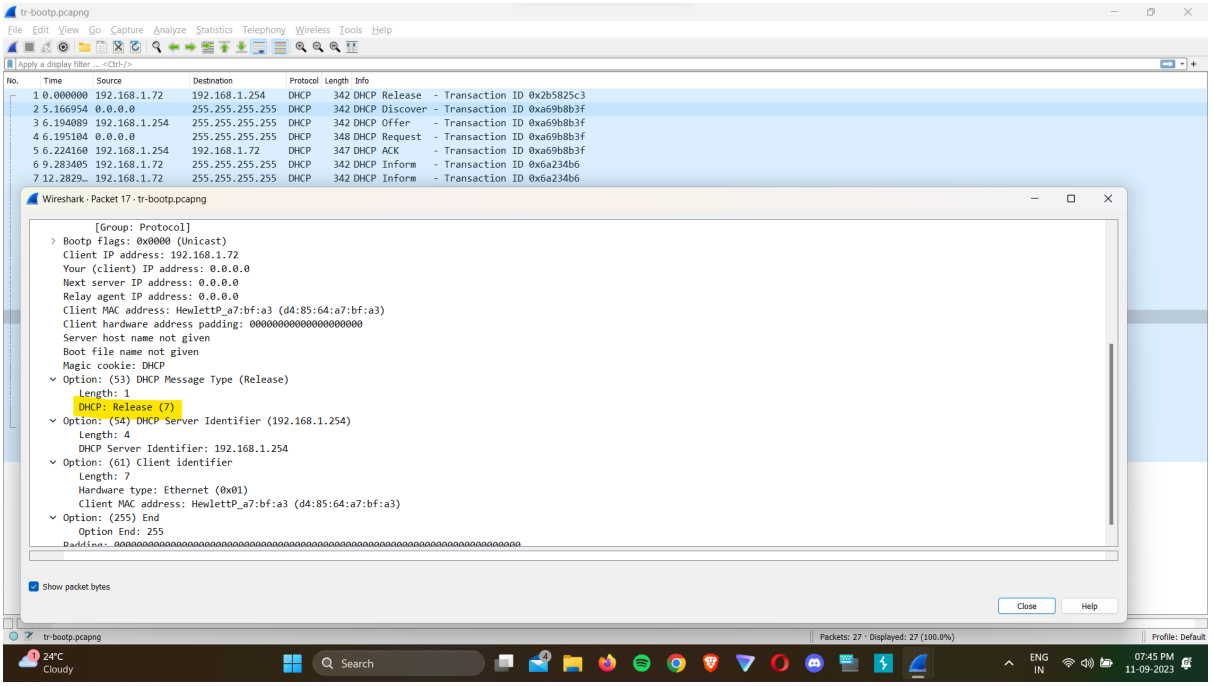
The screenshot below shows the ACK packet and the IP that is assigned to the client by the DHCP server.



c) What is the significance of DHCP Release packet?

Solution: When the client no longer needs the IP address provided by the DHCP server anymore, The client sends a DHCP release packet to the server indicating that it does not require the IP address any further and cancels any of the remaining lease amount.

The screenshot below shows the DHCP release command provided by the client.



d) Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.

Solution:

When the network has two DHCP servers, communication follows these steps:

DHCP Discover: The client broadcasts the discover packet into the network, requesting an IP address. This is received by both DHCP servers.

DHCP Offer: Now both servers offer their set of available IP addresses to the client.

DHCP Request: Now the client selects any one of the offers received. It chooses based on the order in which it received the offer. It then sends a request to the selected DHCP server and broadcasts it into the network.

DHCP Acknowledgement: The DHCP server to which the request was meant to be sent accepts it and sends an ACK to the client with IP and configuration details, along with lease duration. While the other DHCP server does not respond as the client didn't choose this server.

These are the steps in which the client is assigned the IP address, and once the lease tenure ends, the same process repeats.

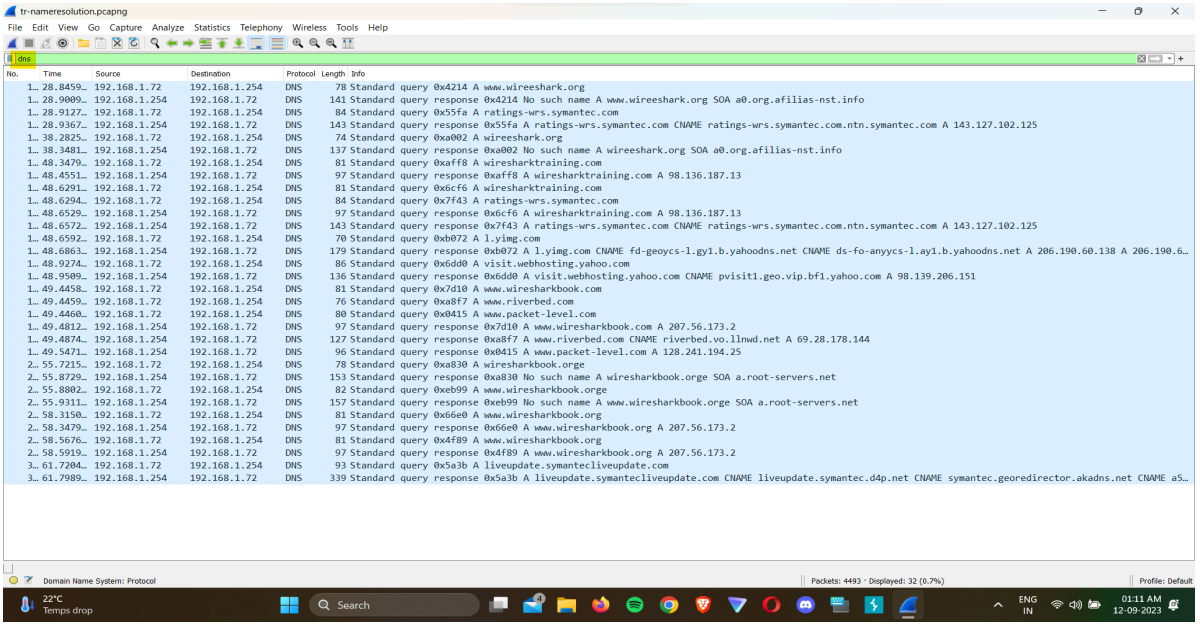
Part-5:

a) Use a filter to display DNS traffic only.

Solution:

To display the DNS traffic, we need to use the filter “**dns**”.

The screenshot shows the filtered DNS traffic.



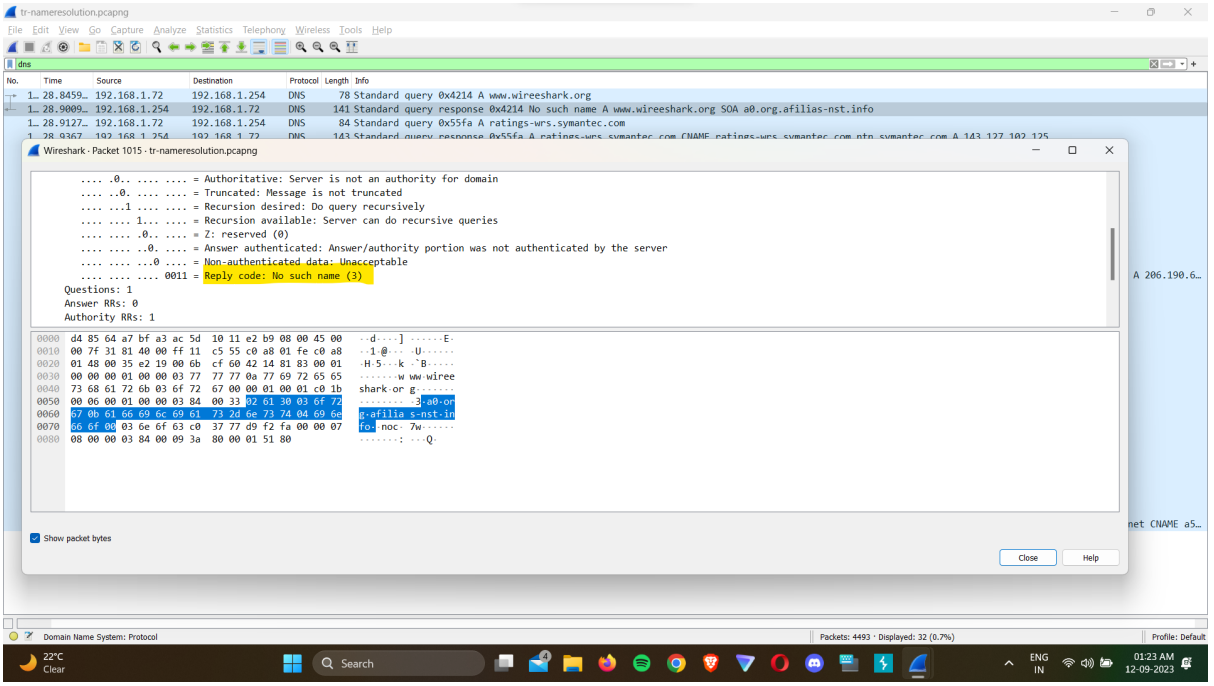
b) Which transport layer protocol is used for DNS queries?

Solution:
It uses UDP (User Datagram Protocol) for DNS queries. The reason is that it is fast and has a very low overhead.

c) What is the response for the DNS query of packet number 1004? What is the reason for this response?

Solution:
The Packet 1004 requested DNS for the domain www.wireeshark.com.
The packet is given a response with "**No such name**". This means that there was no record of the domain name that was requested in the DNS.

The screenshot shows the response of the requested domain name.


tr-nameresolution.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1… 28.8459… 192.168.1.72 192.168.1.254 DNS 78 Standard query 0x4214 A www.wireeshark.org
1… 28.9009… 192.168.1.254 192.168.1.72 DNS 141 Standard query response 0x4214 No such name A www.wireeshark.org SOA a0.org.afilias-nst.info
1… 28.9127… 192.168.1.72 192.168.1.254 DNS 84 Standard query 0x55fa A ratings-wrs.symantec.com
Wireshark · Packet 1015 · tr-nameresolution.pcapng
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0011 = Reply code: No such name (3)
Questions: 1
Answer RRs: 0
Authority RRs: 1
0000 d4 85 64 a7 bf a3 ac 5d 10 11 e2 b9 08 00 45 00
0010 00 7f 31 81 40 00 ff 11 c5 55 c0 a8 01 fe c0 a8
0020 01 48 00 35 e2 19 00 6b cf 60 42 14 81 83 00 01
0030 00 00 00 01 00 00 03 77 77 77 0a 77 69 72 65 65
0040 73 68 61 72 6b 03 6f 72 67 00 00 01 00 01 c0 1b
0050 00 06 00 01 00 00 03 84 00 33 02 61 30 03 6f 72
0060 67 0b 61 66 69 6c 69 61 73 2d 6e 73 74 04 69 6e
0070 66 6f 00 03 6e 6f 63 c0 37 77 d9 f2 fa 00 00 07
0080 08 00 00 03 84 00 09 3a 80 00 01 51 80
Show packet bytes
Close
Help
A 206.190.6…
net CNAME a5…
Domain Name System: Protocol
Packets: 4493 · Displayed: 32 (0.7%)
Profile: Default
22°C
Clear
Search
ENG
IN
01:23 AM
12-09-2023