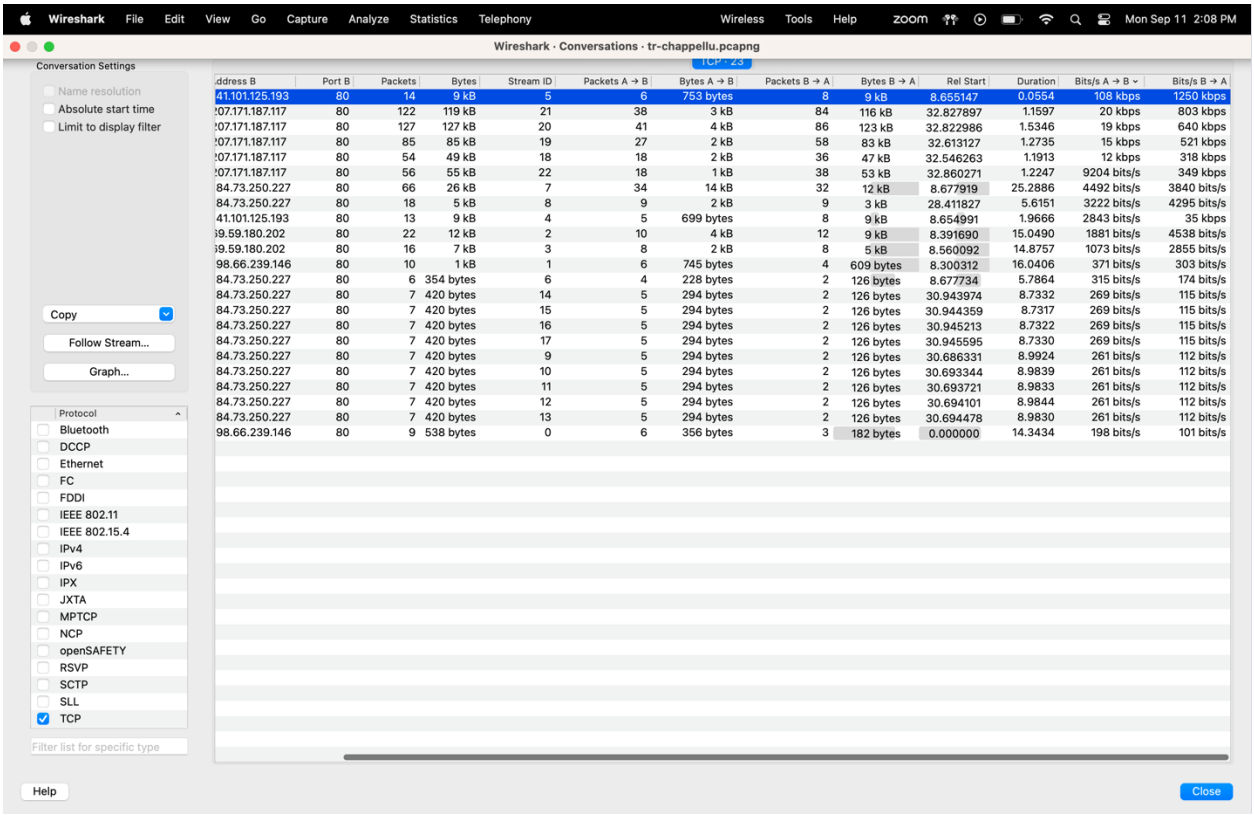
Computer Networks Assignment

Hari Kishan Reddy Abbasani
ha2755

Part 1

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



Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
41.101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108 kbps	1250 kbps
07.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20 kbps	803 kbps
07.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822986	1.5346	19 kbps	640 kbps
07.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15 kbps	521 kbps
07.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12 kbps	318 kbps
07.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204 bits/s	349 kbps
84.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492 bits/s	3840 bits/s
84.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.411827	5.6151	3222 bits/s	4295 bits/s
41.101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843 bits/s	35 kbps
9.59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881 bits/s	4538 bits/s
9.59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073 bits/s	2855 bits/s
98.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371 bits/s	303 bits/s
84.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677734	5.7864	315 bits/s	174 bits/s
84.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261 bits/s	112 bits/s
98.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198 bits/s	101 bits/s

So, the most active TCP conversation in the file (by bits per second) is the packet with Stream id 5 with highest Bits/s A→B is 108kbps and Bits/s B→A is 1250 kbps

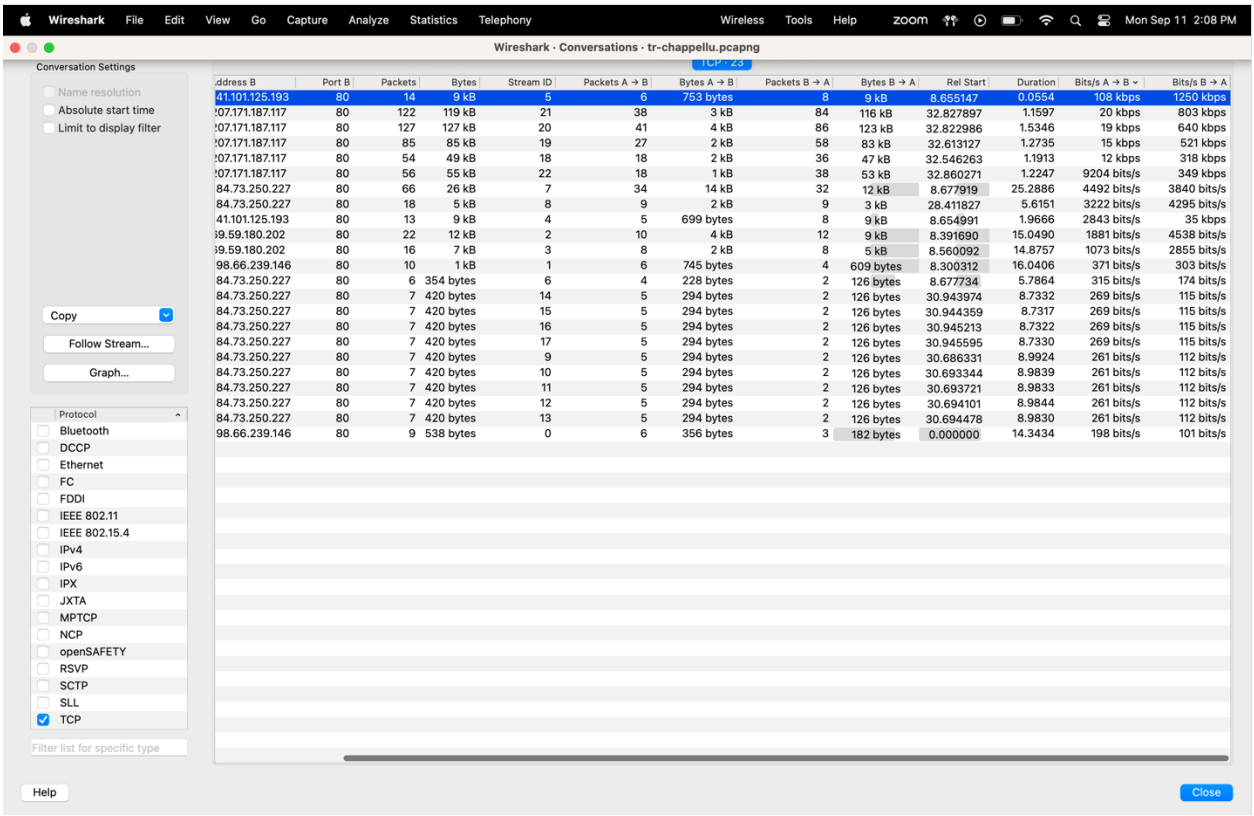
Here's the most TCP conversation data collected in json format:

{"Address A"(source): "24.6.173.220",
"Address B"(destination): "141.101.125.193",
"Bits/s A → B": "108834",
"Bits/s B → A": "1250081",
"Bytes": "9402",
"Bytes A → B": "753",
"Bytes B → A": "8649",

```
  "Duration": "0.055350000000000676",
  "Packets": "14",
  "Packets A → B": "6",
  "Packets B → A": "8",
  "Percent Filtered": "0",
  "Port A": "35627",
  "Port B": "80",
  "Rel Start": "8.655147",
  "Stream ID": "5",
 },
```


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)

Answer:



ddress B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
41.101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108 kbps	1250 kbps
07.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20 kbps	803 kbps
07.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822986	1.5346	19 kbps	640 kbps
07.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15 kbps	521 kbps
07.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12 kbps	318 kbps
07.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204 bits/s	349 kbps
84.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492 bits/s	3840 bits/s
84.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.411827	5.6151	3222 bits/s	4295 bits/s
41.101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843 bits/s	35 kbps
9.59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881 bits/s	4538 bits/s
9.59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073 bits/s	2855 bits/s
98.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371 bits/s	303 bits/s
84.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677734	5.7864	315 bits/s	174 bits/s
84.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269 bits/s	115 bits/s
84.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261 bits/s	112 bits/s
84.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261 bits/s	112 bits/s
98.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198 bits/s	101 bits/s

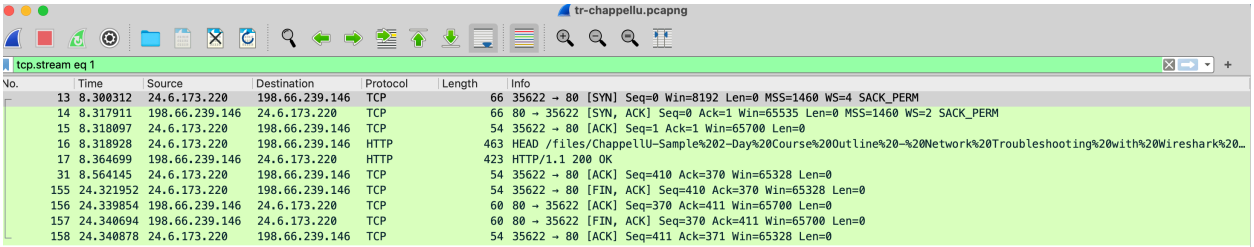
From the data collected in json format


```
 {
  "Address A": "24.6.173.220",
  "Address B": "141.101.125.193",
  "Bits/s A → B": "108834",
  "Bits/s B → A": "1250081",
  "Bytes": "9402",
  "Bytes A → B": "753",
  "Bytes B → A": "8649",
  "Duration": "0.055350000000000676",
  "Packets": "14",
  "Packets A → B": "6",
  "Packets B → A": "8",
```

```
    "Percent Filtered": "0",
    "Port A": "35627",
    "Port B": "80",
    "Rel Start": "8.655147",
    "Stream ID": "5",
    "Total Packets": "0"
  },
```

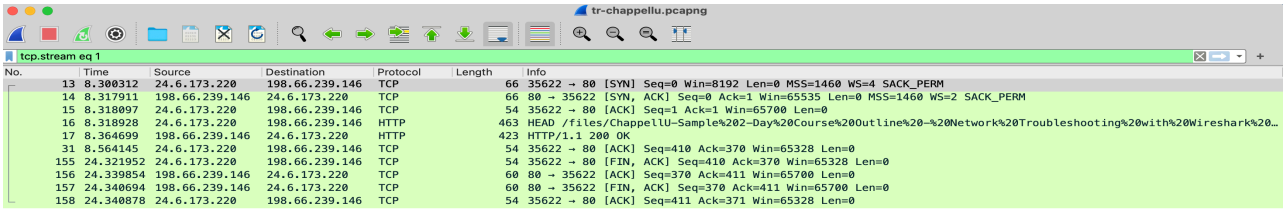

From the above json data collected:
753 bytes were transferred from A to B.
8649 bytes were transferred from B to A.
Total Bytes Transferred = 753 bytes (A to B) + 8649 bytes (B to A)
Total Bytes Transferred = 9402 bytes
So, the total amount of data transferred in the most active TCP conversation is 9,402 bytes.

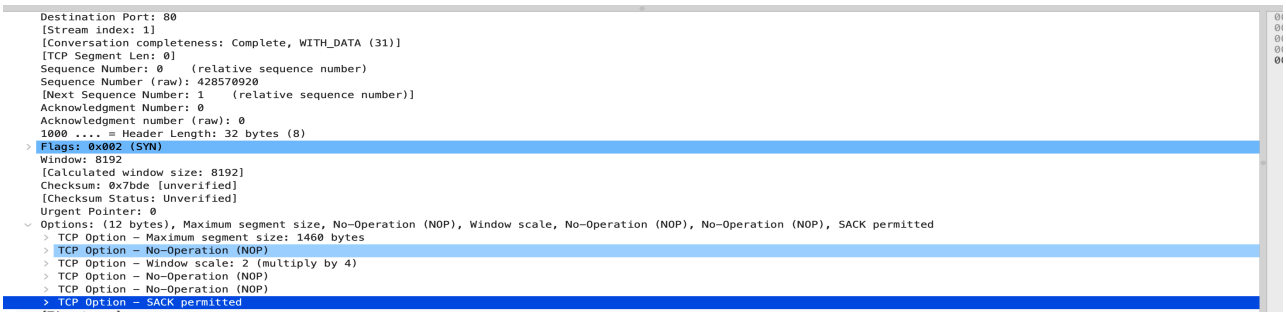
c)Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake:



Round Trip time b/w A and B = ((Timestamp of SYN-ACK - Timestamp of SYN) + (Timestamp of ACK – Timestamp of SYN-ACK))
RTT = (8.317911 – 8.300312) + (8.318097 – 8.317911) = 0.017599 seconds
Which approximately equal to 17.5 milli seconds
RTT = 17.5 milli seconds

d. **Understand selective acknowledgments and check if they are permitted**:

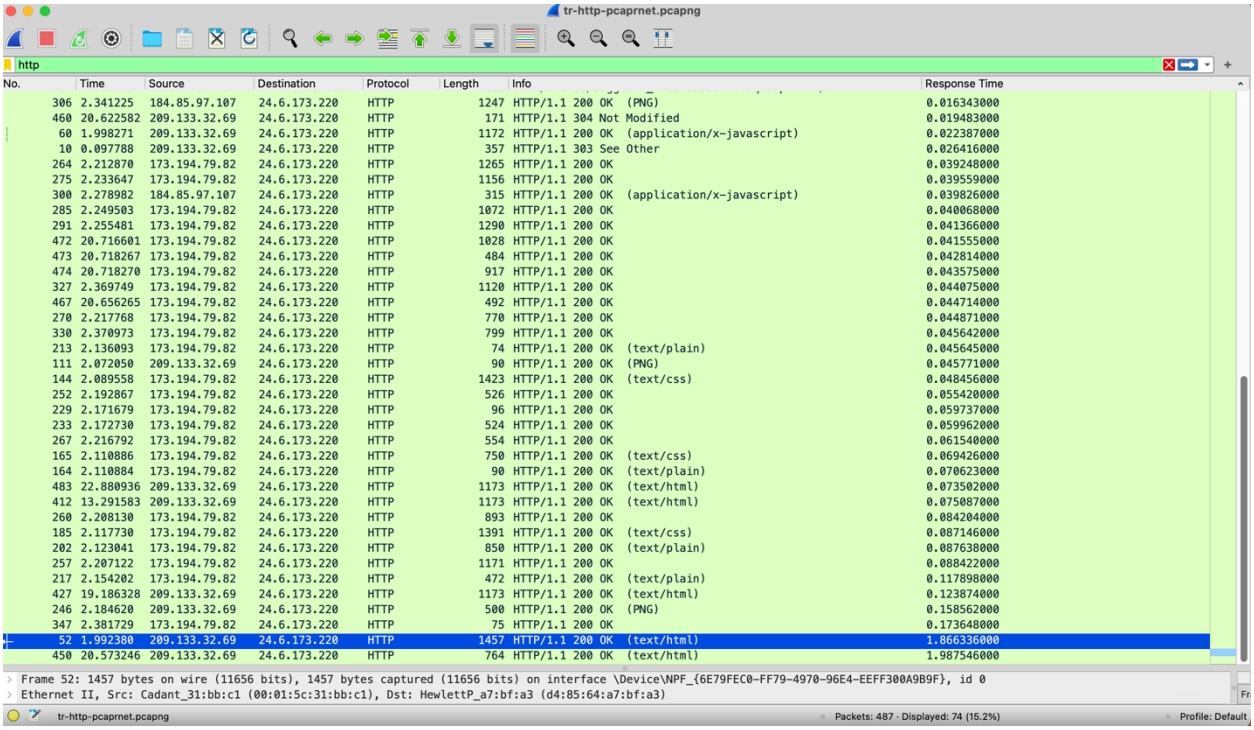




As shown in the picture, SACK is permitted, and I have highlighted it with a blue colour. From the wire shark I have understood that Selective acknowledgments (SACK) are a feature of TCP that allows a receiver to inform the sender about which packets it has received successfully, and which packets are missing in a more detailed manner than traditional TCP acknowledgments.

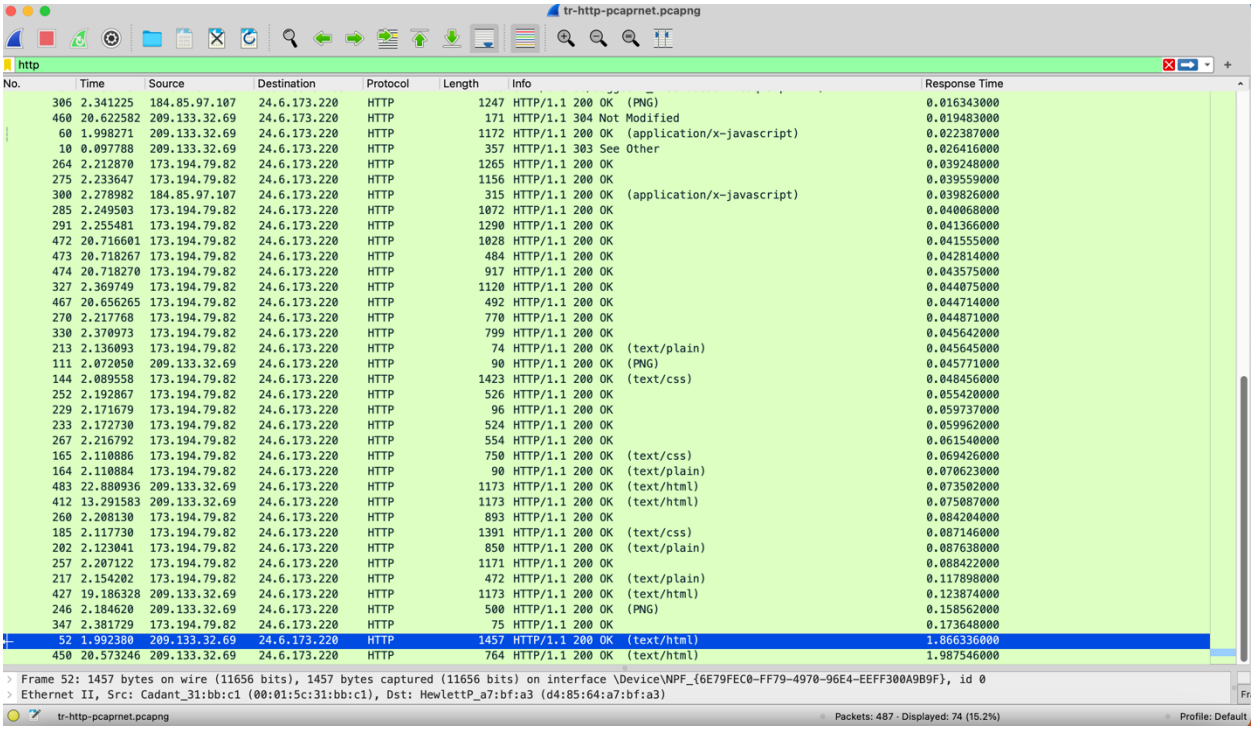
Part 2: Analyzing tr-http-pcaprnet.pcapng

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



As shown in the above picture,
I have added a new column with
Column name: **Response time**
Field: custom
Field content: **http.time** to get the response time of each http request

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



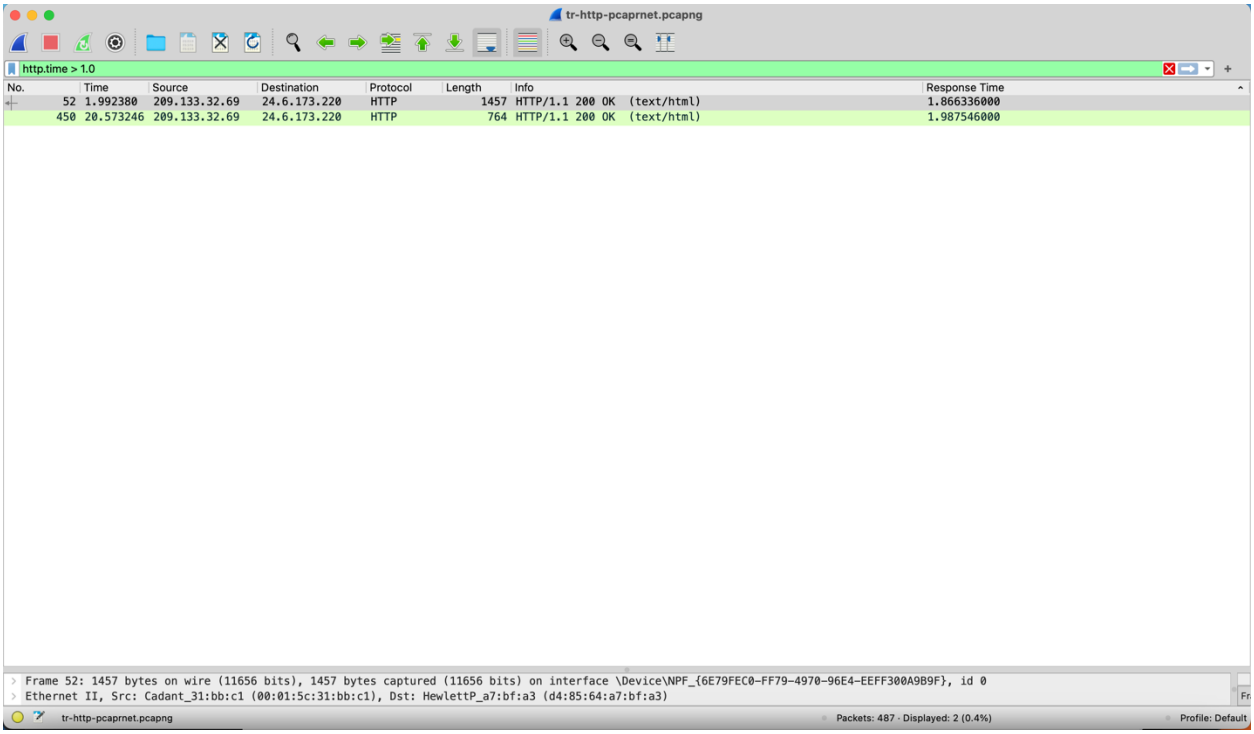
HTTP response status codes indicate the result of an HTTP request. Here in the Screenshot, we can see HTTP response status code as 200,303,304.

200 OK: This status code means the server has successfully processed the HTTP request.

304 Not Modified: This status code states that the website you're requesting hasn't been updated (not modified) since the last time you accessed it.

303 See other: This status code says that a page has been temporarily moved.

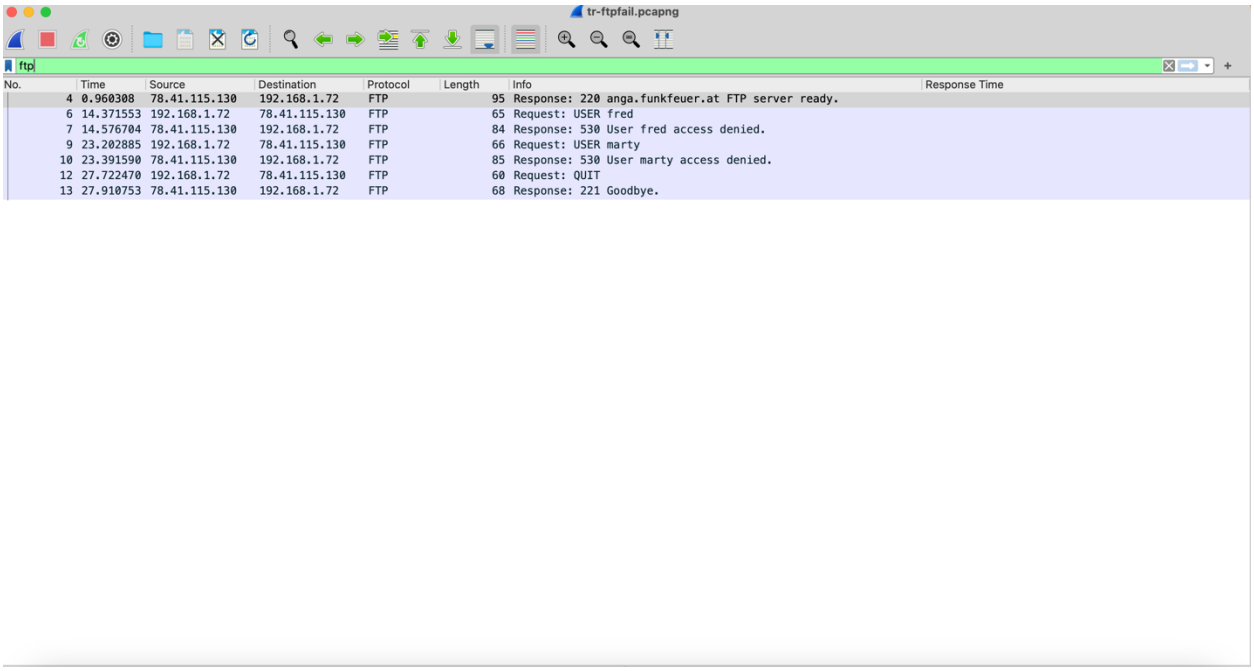
c) Apply a filter that lists packets wherein the HTTP response time is greater than one second.



I have used **http.time > 1.0** to get the packets with response time greater than 1 as shown in the above screenshot.

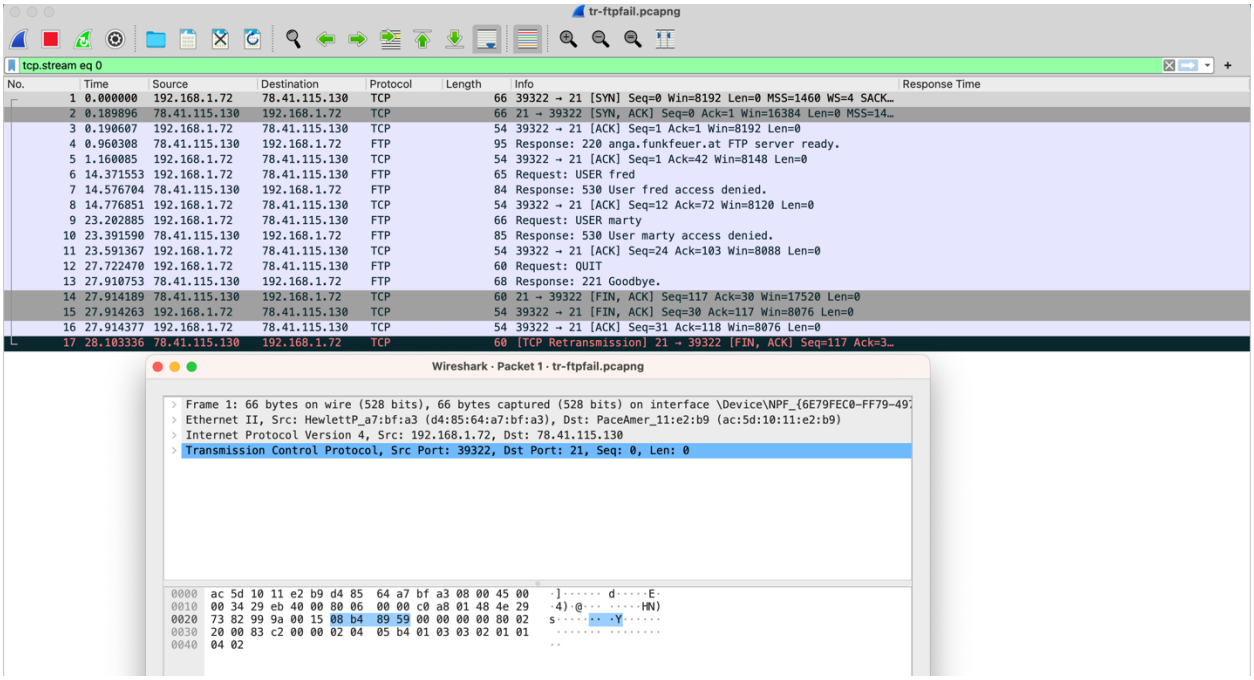
Part 3: tr-ftpfail.pcapng

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



As shown in the above figure, these are the FTP request and response packets by applying FTP filter.

- **List the server and client IP addresses and port numbers.**



From the above screenshot,

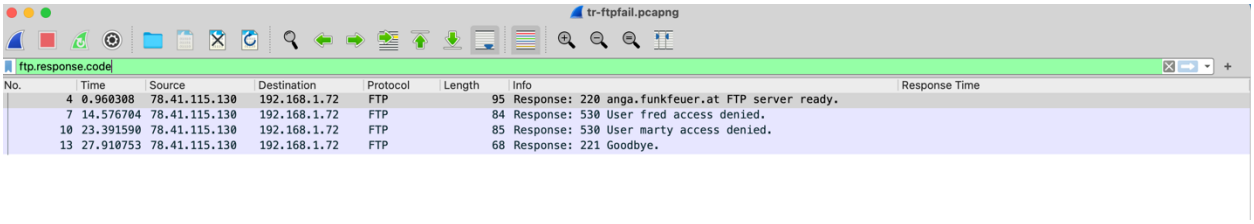
Source/Client Ip address: 192.168.1.72

Source Port: 39322

Destination/Server Ip address: 78.41.115.130

Destination Port: 21

- **Use another filter to display only the FTP response codes for the packets. Define and explain the significance of the response codes.**



FTP response codes are three-digit numbers that indicate the status of FTP commands.

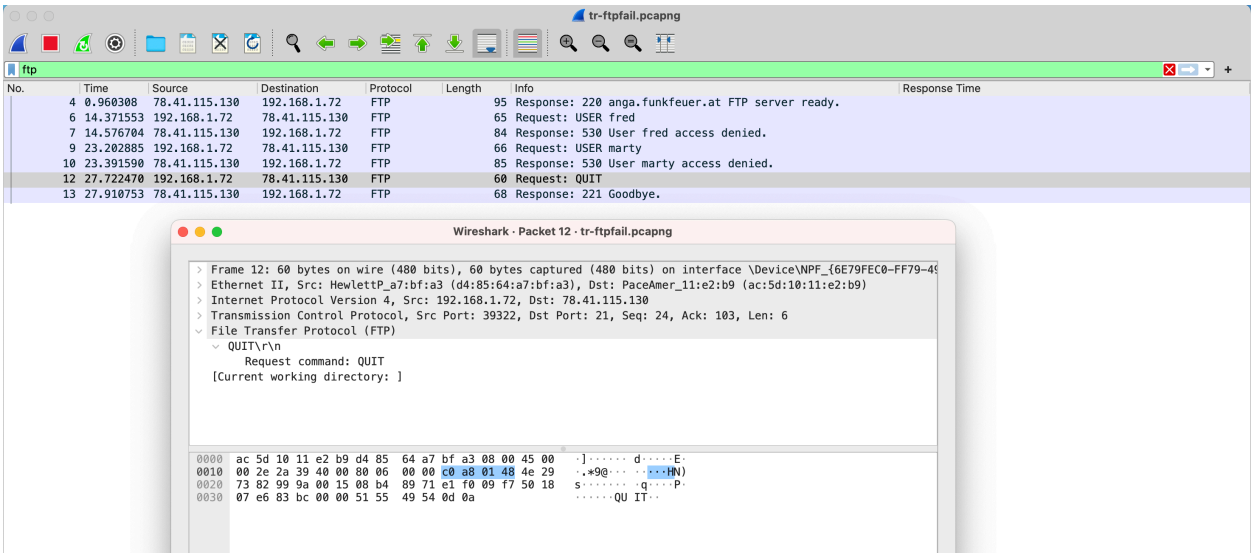
Let’s analyze the FTP response code we got in the wireshark from the file given: **220, 530, 221.**

FTP 220: This code is sent in response to a new user connecting to the FTP server to indicate that the server is ready for the new client.

FTP 530: From the screenshot, Both User fred and Mary account access is denied which states that they are using an incorrect username or password.

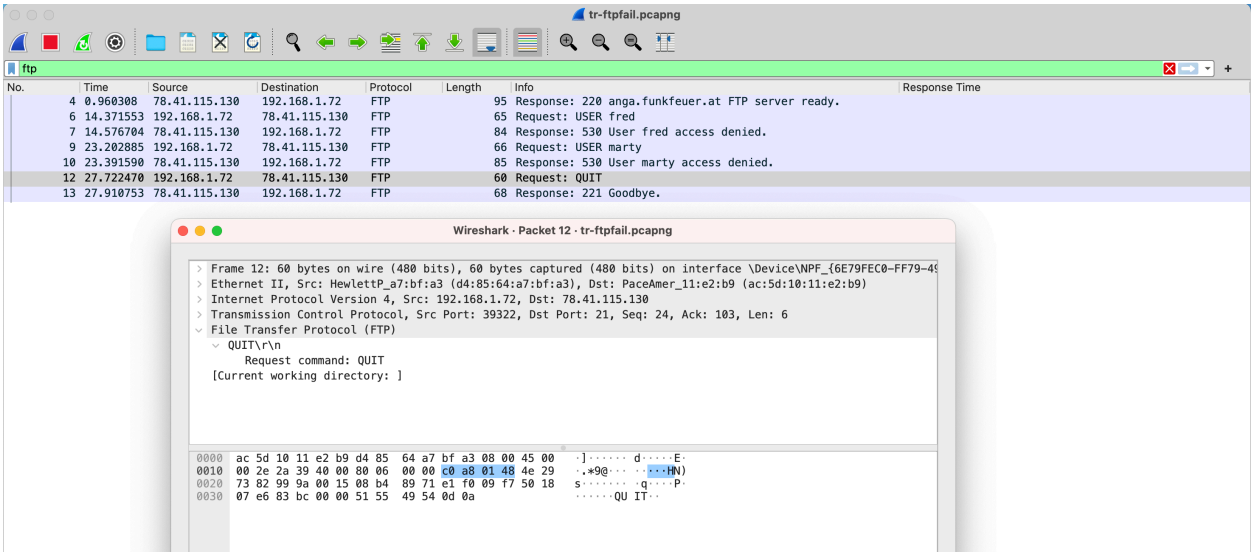
FTP 221: This code is used to send over the control connection in response to the client's QUIT command.

- **Is the FTP termination initiated by server or client? Please justify your answer.**



Source/Client with IP address 192.168.1.72 has initiated the FTP Termination by requesting the command: **QUIT** from the above screenshot and thereby Server responded with a message GoodBye.

- **How secure is FTP?**



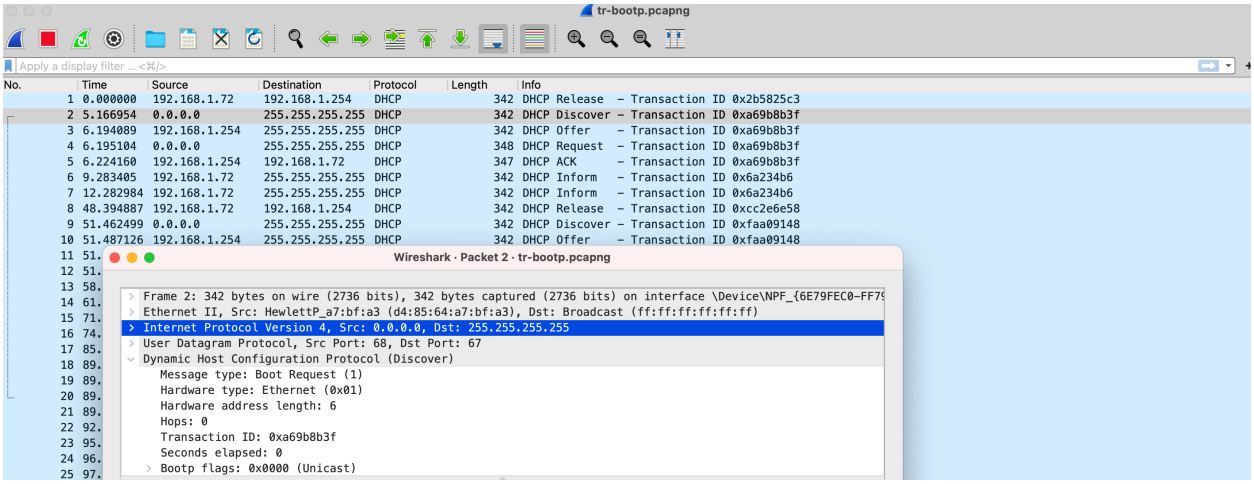
I consider FTP (File Transfer Protocol) is not secure because as per my observation, Standard FTP transmits data, including login credentials, in plain text without any encryption, I can see usernames **Fred and Mary** are directly exposed and states their access status as denied. This makes it vulnerable to eavesdropping and data interception.

I also feel that it doesn't provide strong user authentication and the other reason is it requires multiple ports to be open, which can be problematic for firewall configurations.

To enhance FTP security, we can use secure alternatives like FTPS (FTP Secure) or SFTP (SSH File Transfer Protocol), which provide encryption, strong authentication, and data integrity checks.

Part 4: tr-bootp.pcapng

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.



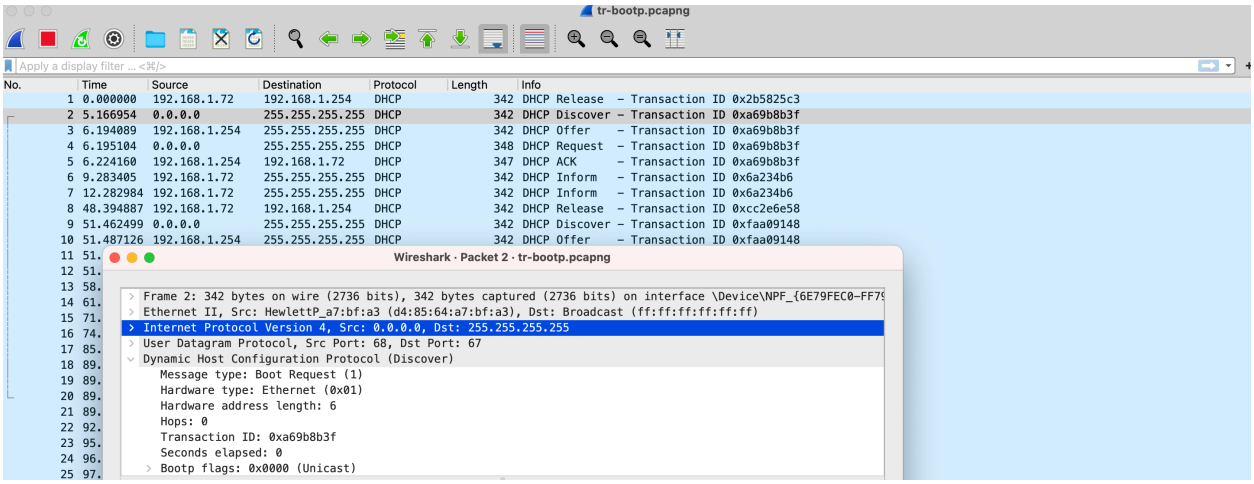
- As per the above screenshot, DHCP (Dynamic Host Configuration Protocol) Discover packets are found at the Data Link Layer, specifically within the Ethernet frame. The Data Link Layer is Layer 2 of the OSI model. DHCP Discover packets are broadcast messages that are sent as Ethernet frames with a destination MAC address of all ones **(FF:FF:FF:FF:FF:FF)** as we can see it in the above figure (Dst: Broadcast) to discover DHCP servers on the local network segment. These packets are used by DHCP clients to request IP address.

- DHCP Discover is a **broadcast packet** type that the DHCP client uses to discover DHCP servers on the network.

- DHCP Discover Packet:
  - Source IP Address: 0.0.0.0
  - Destination IP Address: 255.255.255.255
  - Source Port: 68
  - Destination Port: 67

- DHCP Release Packet:
  - Source IP Address: 192.168.1.72
  - Destination IP Address: 192.168.1.254
  - Source Port: 68
  - Destination Port: 67

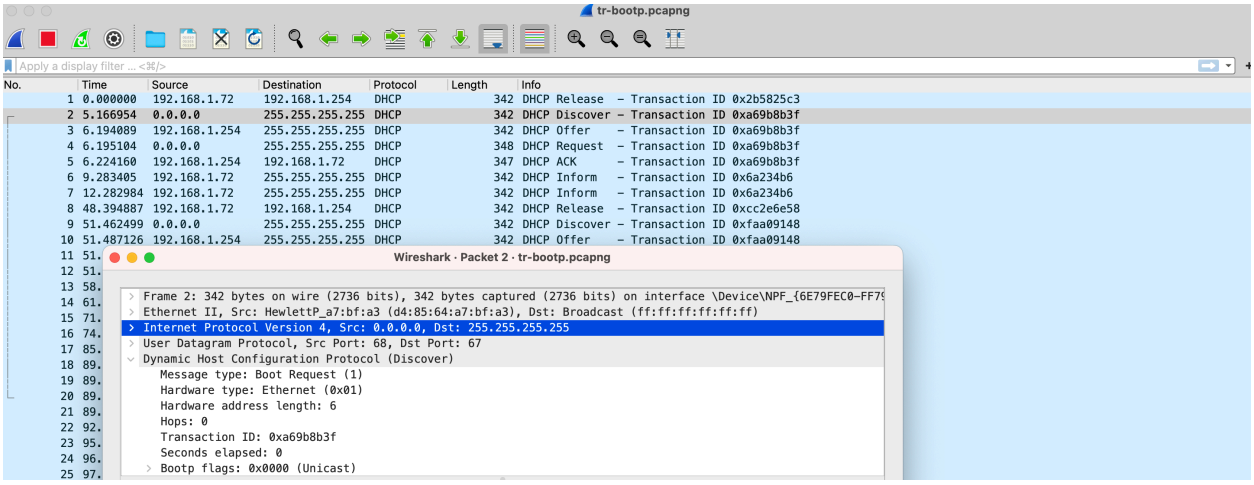
b) How many DHCP packets are exchanged between the client and server before the client receives an IP address? Define and explain the commands used in the DHCP handshake.



Four DHCP (2,3,4,5) packets are exchanged between the client and server before the Client received an Ip address:

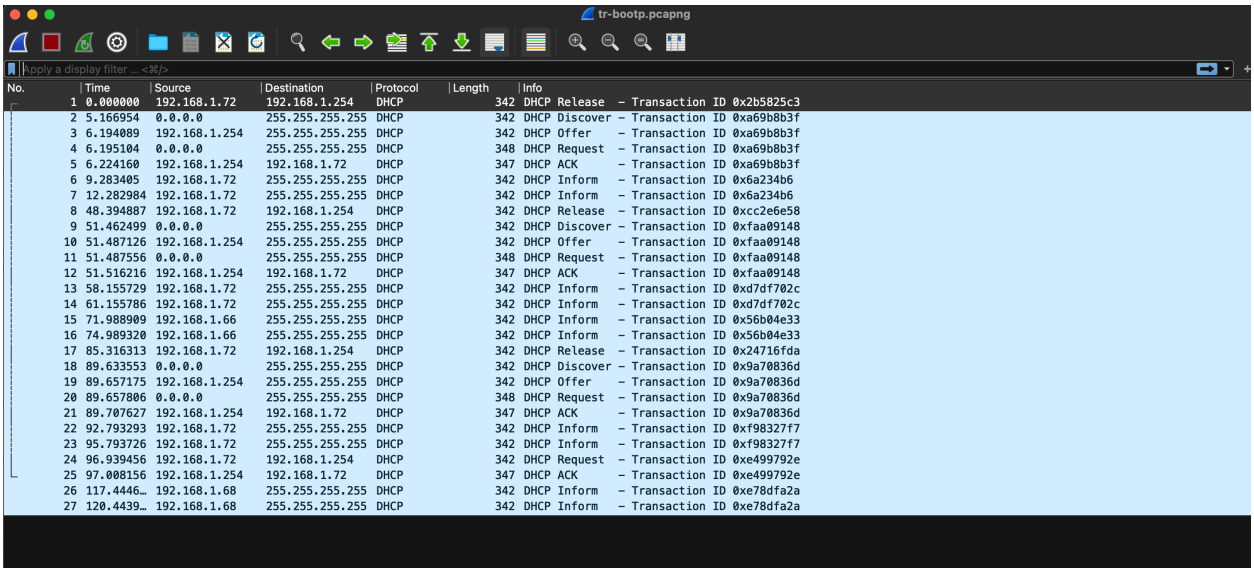
- **DHCP Discover (Client to Server – 0.0.0.0 to 255.255.255.255)**: The client broadcasted a DHCP Discover packet to discover available DHCP servers. This packet includes the client's MAC address and a randomly generated transaction ID as seen in the picture.
- **DHCP Offer (192.168.1.254 to 255.255.255.255)**: When a DHCP server receives a Discover packet, it has responded with a DHCP Offer packet.
- **DHCP Request (0.0.0.0 to 255.255.255.255)**: The client has sent a DHCP Request packet to the server. This packet requests the offered IP address.
- **DHCP Acknowledgment (192.168.1.254 to 192.168.1.72)**: The DHCP server has acknowledged the client's request by sending a DHCP Acknowledgment packet, which includes the IP address lease and other configuration parameters. The client can now use the IP address: **192.168.1.72**.

c)What is the significance of DHCP Release packet?



As we can see that the first packet in the above ss is DHCP Release and it is used when a DHCP client wants to relinquish its leased IP address before the lease expires and it allows the DHCP server to reclaim the IP address and make it available for other clients.

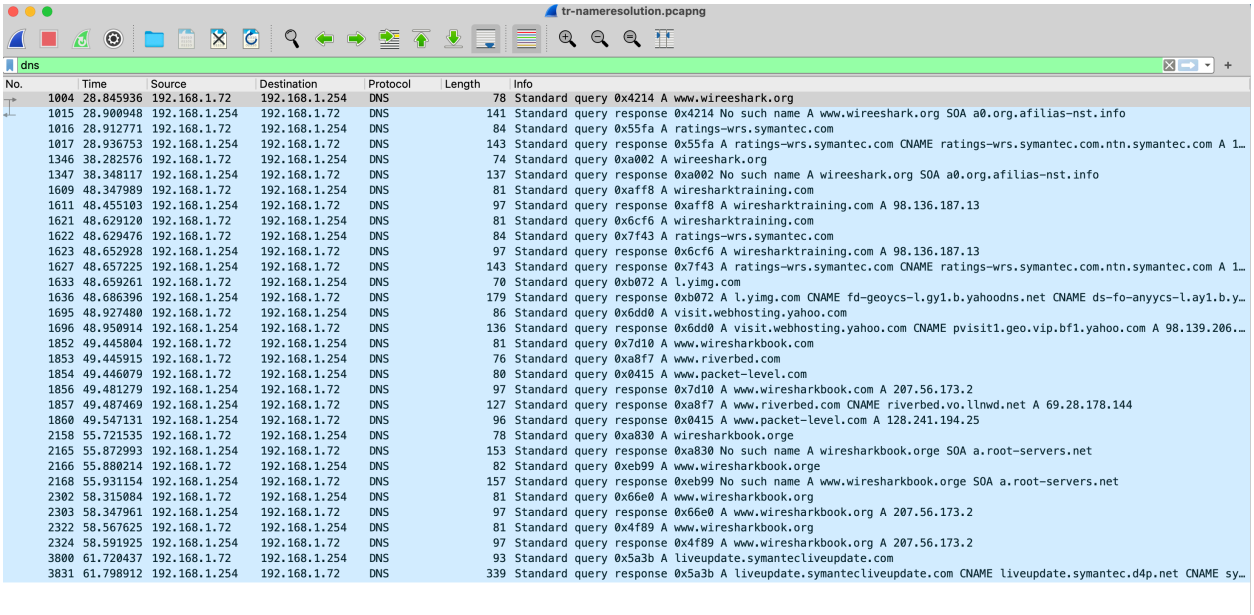
d)Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.



The client will effectively chose only one DHCP server's and the communication with the other DHCP server will be ignored.In the above figure, even though DHCP server with IP 192.168.1.66 has offered/informed the client. The client has chosen only one DHCP server's offer with ip address 192.168.1.72 to avoid conflicts and ensure that only one server's lease is accepted by the client.

Part 5: tr-nameresolution.pcapng

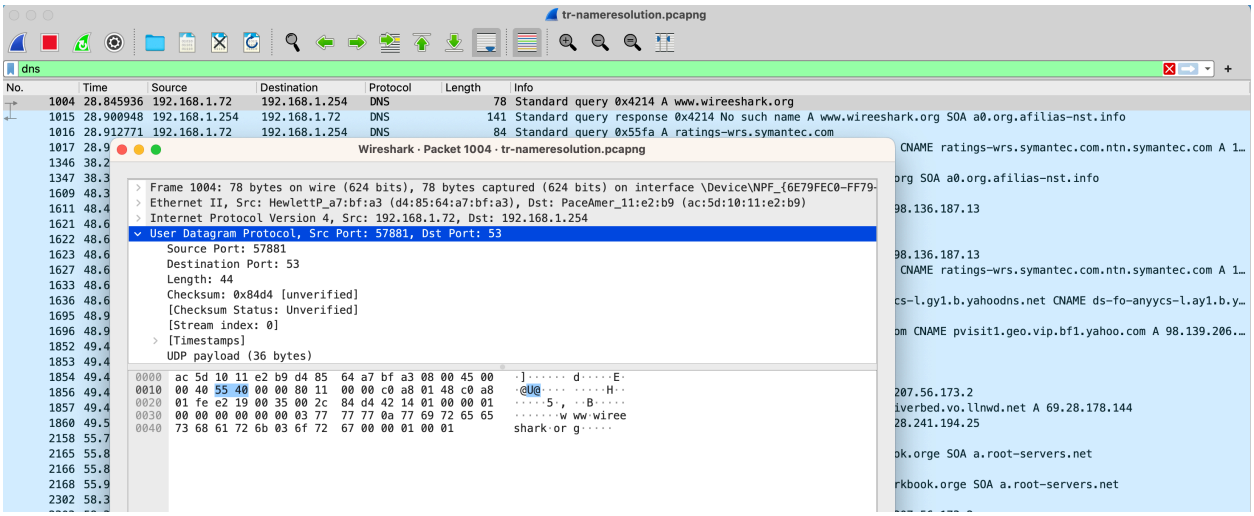
1. Use a filter to display DNS traffic only.



No.	Time	Source	Destination	Protocol	Length	Info
1004	28.845936	192.168.1.72	192.168.1.254	DNS	78	Standard query 0x4214 A www.wireeshark.org
1015	28.900948	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
1016	28.912771	192.168.1.72	192.168.1.254	DNS	84	Standard query 0x55fa A ratings-wrs.symantec.com
1017	28.936753	192.168.1.254	192.168.1.72	DNS	143	Standard query response 0x55fa A ratings-wrs.symantec.com CNAME ratings-wrs.symantec.com.ntn.symantec.com A 1…
1346	38.282576	192.168.1.72	192.168.1.254	DNS	74	Standard query 0xa002 A wireeshark.org
1347	38.348117	192.168.1.254	192.168.1.72	DNS	137	Standard query response 0xa002 No such name A wireeshark.org SOA a0.org.afilias-nst.info
1609	48.347989	192.168.1.72	192.168.1.254	DNS	81	Standard query 0xaff8 A wiresharktraining.com
1611	48.455103	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0xaff8 A wiresharktraining.com A 98.136.187.13
1621	48.629120	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x6cf6 A wiresharktraining.com
1622	48.629476	192.168.1.72	192.168.1.254	DNS	84	Standard query 0x7f43 A ratings-wrs.symantec.com
1623	48.652928	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x6cf6 A wiresharktraining.com A 98.136.187.13
1627	48.657225	192.168.1.254	192.168.1.72	DNS	143	Standard query response 0x7f43 A ratings-wrs.symantec.com CNAME ratings-wrs.symantec.com.ntn.symantec.com A 1…
1633	48.659261	192.168.1.72	192.168.1.254	DNS	70	Standard query 0xb072 A l.yimg.com
1636	48.686396	192.168.1.254	192.168.1.72	DNS	179	Standard query response 0xb072 A l.yimg.com CNAME fd-geoycs-l.gy1.b.yahoodns.net CNAME ds-fo-anyycs-l.ay1.b.y…
1695	48.927480	192.168.1.72	192.168.1.254	DNS	86	Standard query 0x6dd0 A visit.webhosting.yahoo.com
1696	48.950914	192.168.1.254	192.168.1.72	DNS	136	Standard query response 0x6dd0 A visit.webhosting.yahoo.com CNAME pvisit1.geo.vip.bf1.yahoo.com A 98.139.206.…
1852	49.445804	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x7d10 A www.wiresharkbook.com
1853	49.445915	192.168.1.72	192.168.1.254	DNS	76	Standard query 0xa8f7 A www.riverbed.com
1854	49.446079	192.168.1.72	192.168.1.254	DNS	80	Standard query 0x0415 A www.packet-level.com
1856	49.481279	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x7d10 A www.wiresharkbook.com A 207.56.173.2
1857	49.487469	192.168.1.254	192.168.1.72	DNS	127	Standard query response 0xa8f7 A www.riverbed.com CNAME riverbed.vo.llnwd.net A 69.28.178.144
1860	49.547131	192.168.1.254	192.168.1.72	DNS	96	Standard query response 0x0415 A www.packet-level.com A 128.241.194.25
2158	55.721535	192.168.1.72	192.168.1.254	DNS	78	Standard query 0xa830 A wiresharkbook.orge
2165	55.872993	192.168.1.254	192.168.1.72	DNS	153	Standard query response 0xa830 No such name A wiresharkbook.orge SOA a.root-servers.net
2166	55.880214	192.168.1.72	192.168.1.254	DNS	82	Standard query 0xeb99 A www.wiresharkbook.orge
2168	55.931154	192.168.1.254	192.168.1.72	DNS	157	Standard query response 0xeb99 No such name A www.wiresharkbook.orge SOA a.root-servers.net
2302	58.315084	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x66e0 A www.wiresharkbook.org
2303	58.347961	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x66e0 A www.wiresharkbook.org A 207.56.173.2
2322	58.567625	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x4f89 A www.wiresharkbook.org
2324	58.591925	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x4f89 A www.wiresharkbook.org A 207.56.173.2
3800	61.720437	192.168.1.72	192.168.1.254	DNS	93	Standard query 0x5a3b A liveupdate.symantecliveupdate.com
3831	61.798912	192.168.1.254	192.168.1.72	DNS	339	Standard query response 0x5a3b A liveupdate.symantecliveupdate.com CNAME liveupdate.symantec.d4p.net CNAME sy…

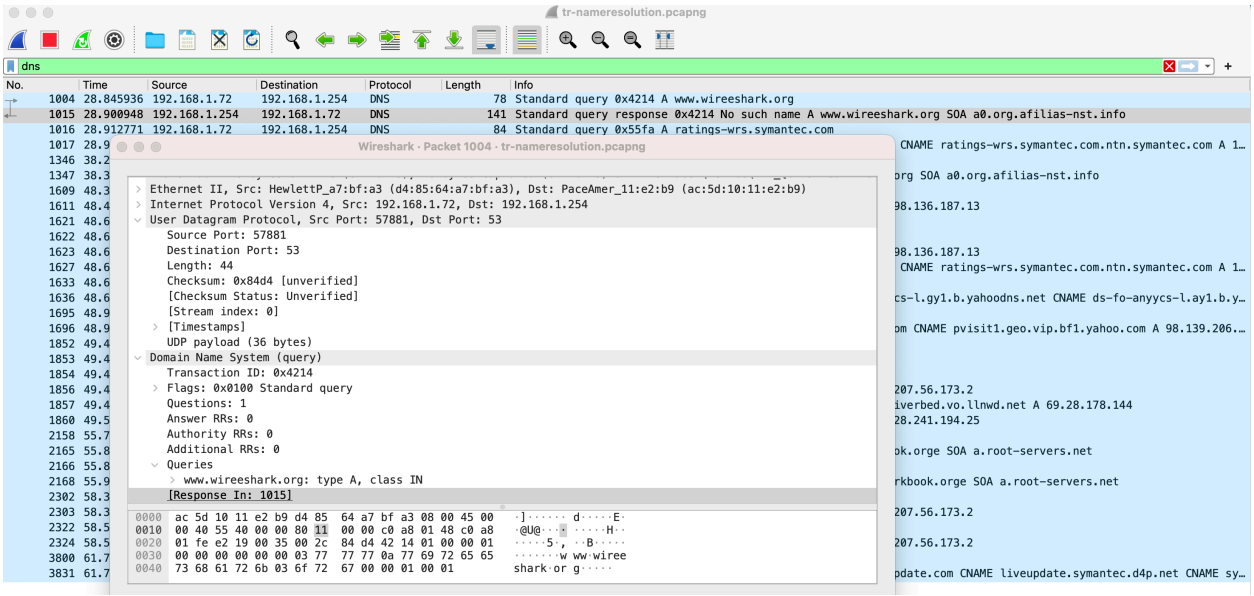
I have used dns to filter only DNS traffic packets.

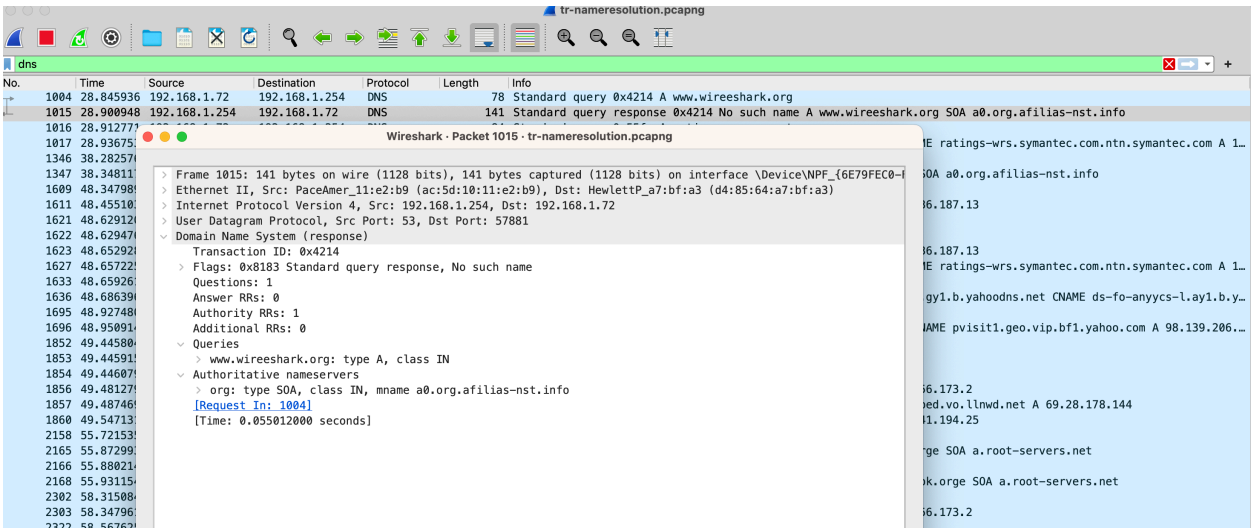
2. Which transport layer protocol is used for DNS queries?



DNS queries use **UDP (User Datagram Protocol)** as we can see in the above screenshot and I have highlighted it in blue colour.

3. What is the response for the DNS query of packet number 1004? What is the reason for this response?





The DNS response for packet number 1015 indicates the following:

- **Packet Number**: 1015
- **Timestamp**: 28.900948
- **Source IP Address**: 192.168.1.254 (DNS Server)
- **Destination IP Address**: 192.168.1.72 (DNS Client)

- **Protocol**: DNS
- **Length**: 141 bytes
- **DNS Message Type**: Standard query response
- **DNS Response Code**: 0x4214
- **DNS Response**: The response code **0x14** corresponds to "No such name," indicating that the DNS server could not find a DNS record for the queried hostname.
- **DNS Query Type**: A (IPv4 address)
- **Queried Hostname**: www.wireeshark.org
- **Start of Authority (SOA)**: a0.org.afilias-nst.info

In summary, this DNS response (packet number 1015) is telling the DNS client (192.168.1.72) that there is no DNS record (A record) associated with the hostname "www.wireeshark.org." The response code **0x14** specifically indicates that the name does not exist in the DNS records.
And from the observation I can see that there is a typo in the hostname "wireeshark.org" in the description. It should likely be "wireshark.org."