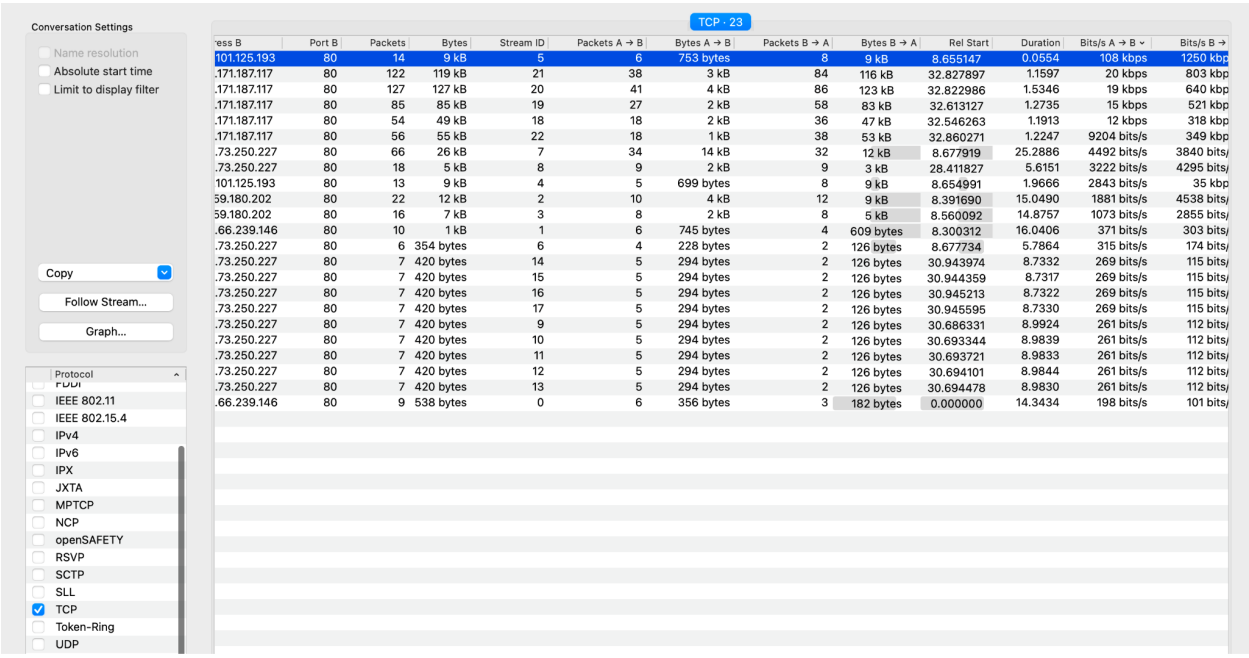
Venkata Naga Dheeraj Pavuluri
N16788493

Part 1

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

Getting the most active by sorting the bits per second column in ascending order



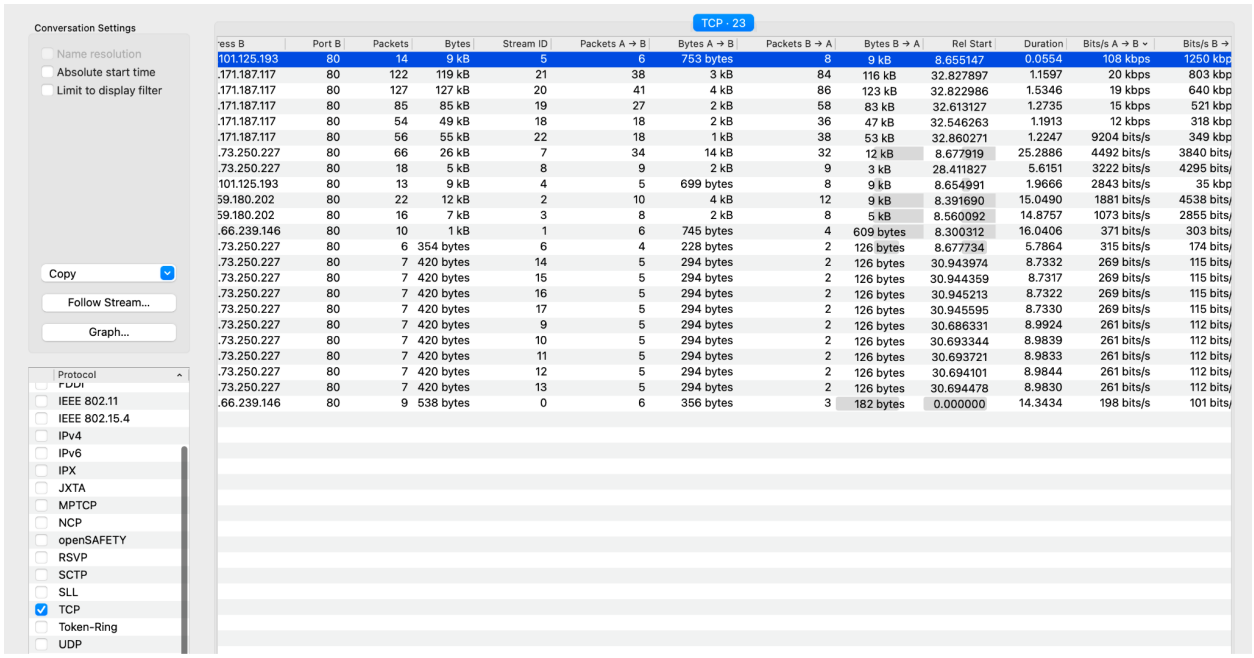
ess B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B →
101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108 kbps	1250 kbp
.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20 kbps	803 kbp
.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822986	1.5346	19 kbps	640 kbp
.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15 kbps	521 kbp
.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12 kbps	318 kbp
.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204 bits/s	349 kbp
.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492 bits/s	3840 bits/
.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.411827	5.6151	3222 bits/s	4295 bits/
101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843 bits/s	35 kbp
59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881 bits/s	4538 bits/
59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073 bits/s	2855 bits/
.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371 bits/s	303 bits/
.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677734	5.7864	315 bits/s	174 bits/
.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261 bits/s	112 bits/
.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198 bits/s	101 bits/

a->b 108k bits/sec

b->a 1250 k bits/sec

2. 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)

The total bytes transferred is **9402** :



ess 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 →
101.125.193	80	14	9 kB	5	6	753 bytes	8	9 kB	8.655147	0.0554	108 kbps	1250 kbp
.171.187.117	80	122	119 kB	21	38	3 kB	84	116 kB	32.827897	1.1597	20 kbps	803 kbp
.171.187.117	80	127	127 kB	20	41	4 kB	86	123 kB	32.822986	1.5346	19 kbps	640 kbp
.171.187.117	80	85	85 kB	19	27	2 kB	58	83 kB	32.613127	1.2735	15 kbps	521 kbp
.171.187.117	80	54	49 kB	18	18	2 kB	36	47 kB	32.546263	1.1913	12 kbps	318 kbp
.171.187.117	80	56	55 kB	22	18	1 kB	38	53 kB	32.860271	1.2247	9204 bits/s	349 kbp
.73.250.227	80	66	26 kB	7	34	14 kB	32	12 kB	8.677919	25.2886	4492 bits/s	3840 bits/
.73.250.227	80	18	5 kB	8	9	2 kB	9	3 kB	28.411827	5.6151	3222 bits/s	4295 bits/
101.125.193	80	13	9 kB	4	5	699 bytes	8	9 kB	8.654991	1.9666	2843 bits/s	35 kbp
59.180.202	80	22	12 kB	2	10	4 kB	12	9 kB	8.391690	15.0490	1881 bits/s	4538 bits/
59.180.202	80	16	7 kB	3	8	2 kB	8	5 kB	8.560092	14.8757	1073 bits/s	2855 bits/
.66.239.146	80	10	1 kB	1	6	745 bytes	4	609 bytes	8.300312	16.0406	371 bits/s	303 bits/
.73.250.227	80	6	354 bytes	6	4	228 bytes	2	126 bytes	8.677734	5.7864	315 bits/s	174 bits/
.73.250.227	80	7	420 bytes	14	5	294 bytes	2	126 bytes	30.943974	8.7332	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	15	5	294 bytes	2	126 bytes	30.944359	8.7317	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	16	5	294 bytes	2	126 bytes	30.945213	8.7322	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	17	5	294 bytes	2	126 bytes	30.945595	8.7330	269 bits/s	115 bits/
.73.250.227	80	7	420 bytes	9	5	294 bytes	2	126 bytes	30.686331	8.9924	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	10	5	294 bytes	2	126 bytes	30.693344	8.9839	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	11	5	294 bytes	2	126 bytes	30.693721	8.9833	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	12	5	294 bytes	2	126 bytes	30.694101	8.9844	261 bits/s	112 bits/
.73.250.227	80	7	420 bytes	13	5	294 bytes	2	126 bytes	30.694478	8.9830	261 bits/s	112 bits/
.66.239.146	80	9	538 bytes	0	6	356 bytes	3	182 bytes	0.000000	14.3434	198 bits/s	101 bits/

3. Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake.
A TCP involves a 3-way handshake, those are SYN, SYN -> ACK, and ACK.

Here the RTT is:

SYN -> ACK 0.020736

ACK. 0.000137

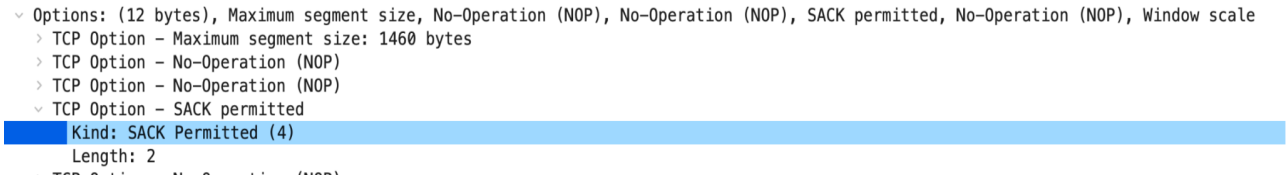
RTT 0.020873

```
[Timestamps]
  [Time since first frame in this TCP stream: 0.020873000 seconds]
  [Time since previous frame in this TCP stream: 0.000137000 seconds]
[SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 52]
  [The RTT to ACK the segment was: 0.000137000 seconds]
  [iRTT: 0.020873000 seconds]
```

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

The Selective Acknowledgment (SACK) technique corrects this behavior when several lost segments occur. The sender only needs to retransmit the segments that were genuinely lost since using selective acknowledgments, the data receiver may tell the sender about all segments that have successfully arrived.

As we can see, the TCP Option is Sack authorized, therefore the Selective acknowledgment is allowed in this session.



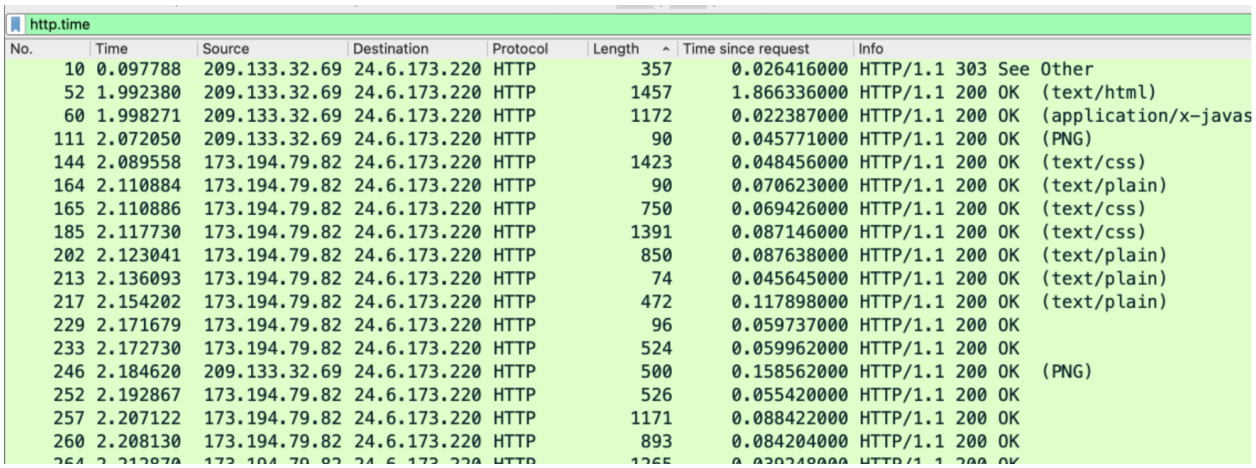
Part 2

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

Filter the used to display http response time here is

http.time

displaying Time since the request



No.	Time	Source	Destination	Protocol	Length	Time since request	Info
10	0.097788	209.133.32.69	24.6.173.220	HTTP	357	0.026416000	HTTP/1.1 303 See Other
52	1.992380	209.133.32.69	24.6.173.220	HTTP	1457	1.866336000	HTTP/1.1 200 OK (text/html)
60	1.998271	209.133.32.69	24.6.173.220	HTTP	1172	0.022387000	HTTP/1.1 200 OK (application/x-javas
111	2.072050	209.133.32.69	24.6.173.220	HTTP	90	0.045771000	HTTP/1.1 200 OK (PNG)
144	2.089558	173.194.79.82	24.6.173.220	HTTP	1423	0.048456000	HTTP/1.1 200 OK (text/css)
164	2.110884	173.194.79.82	24.6.173.220	HTTP	90	0.070623000	HTTP/1.1 200 OK (text/plain)
165	2.110886	173.194.79.82	24.6.173.220	HTTP	750	0.069426000	HTTP/1.1 200 OK (text/css)
185	2.117730	173.194.79.82	24.6.173.220	HTTP	1391	0.087146000	HTTP/1.1 200 OK (text/css)
202	2.123041	173.194.79.82	24.6.173.220	HTTP	850	0.087638000	HTTP/1.1 200 OK (text/plain)
213	2.136093	173.194.79.82	24.6.173.220	HTTP	74	0.045645000	HTTP/1.1 200 OK (text/plain)
217	2.154202	173.194.79.82	24.6.173.220	HTTP	472	0.117898000	HTTP/1.1 200 OK (text/plain)
229	2.171679	173.194.79.82	24.6.173.220	HTTP	96	0.059737000	HTTP/1.1 200 OK
233	2.172730	173.194.79.82	24.6.173.220	HTTP	524	0.059962000	HTTP/1.1 200 OK
246	2.184620	209.133.32.69	24.6.173.220	HTTP	500	0.158562000	HTTP/1.1 200 OK (PNG)
252	2.192867	173.194.79.82	24.6.173.220	HTTP	526	0.055420000	HTTP/1.1 200 OK
257	2.207122	173.194.79.82	24.6.173.220	HTTP	1171	0.088422000	HTTP/1.1 200 OK
260	2.208130	173.194.79.82	24.6.173.220	HTTP	893	0.084204000	HTTP/1.1 200 OK

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

200	The HTTP 200 OK success status response code indicates that the request has succeeded
303	See Other redirect status response codes show that the redirects point to another website rather than the requested resource directly.

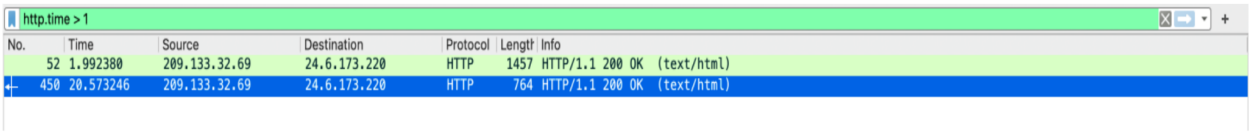
304	The 304 Not Modified status code indicates that since you last viewed the website, it has not been updated.

Other Common HTTP Responses

404	Please specify if the missing page or resource is gone permanently or just temporarily.
500	Indicates a problem with the server
503	signifies that the server is down as a result of temporary server overload or server maintenance.

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

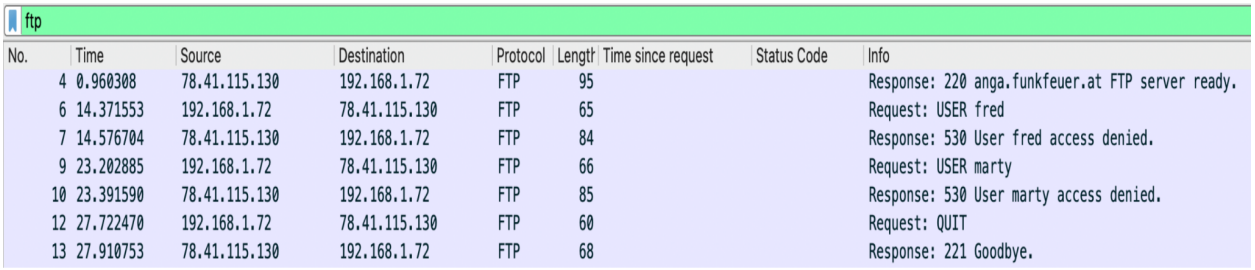
Filter http.time > 1



Part 3

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

Using filter: ftp



2. List the server and client IP addresses and port numbers.

Source	Destination	Source Port	Destination Port
78.41.115.130	192.168.1.72	21	39322
192.168.1.72	78.41.115.130	39322	21
78.41.115.130	192.168.1.72	21	39322
192.168.1.72	78.41.115.130	39322	21
78.41.115.130	192.168.1.72	21	39322
192.168.1.72	78.41.115.130	39322	21
78.41.115.130	192.168.1.72	21	39322

Source Address - 192.168.1.72
Source Port - 39322
Destination Address - 78.41.115.130
Destination Port - 21

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

Filter: ftp.response.code.

Response code	Info
Service ready for new user	Response: 220 anga.funkfeuer.at FTP server re
	Request: USER fred
Not logged in	Response: 530 User fred access denied.
	Request: USER marty
Not logged in	Response: 530 User marty access denied.
	Request: QUIT
Service closing control connection	Response: 221 Goodbye.

220: Service ready for new user.

530: Not logged in.

221: Service closing control connection.

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

The termination of an FTP session requires the FTP client to send a QUIT message to the FTP server as shown in the figure below.

Here the client sends a QUIT request and the server sends a Goodbye response

12	27.722470	192.168.1.72	78.41.115.130	FTP	60	Request: QUIT
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.

5. How secure is FTP?

Due to its reliance on unencrypted credentials for authentication and sensitivity to sniffing, spoofing, and other common attack techniques, FTP is not constructed securely (is insecure).

PART - 4:

1. 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.

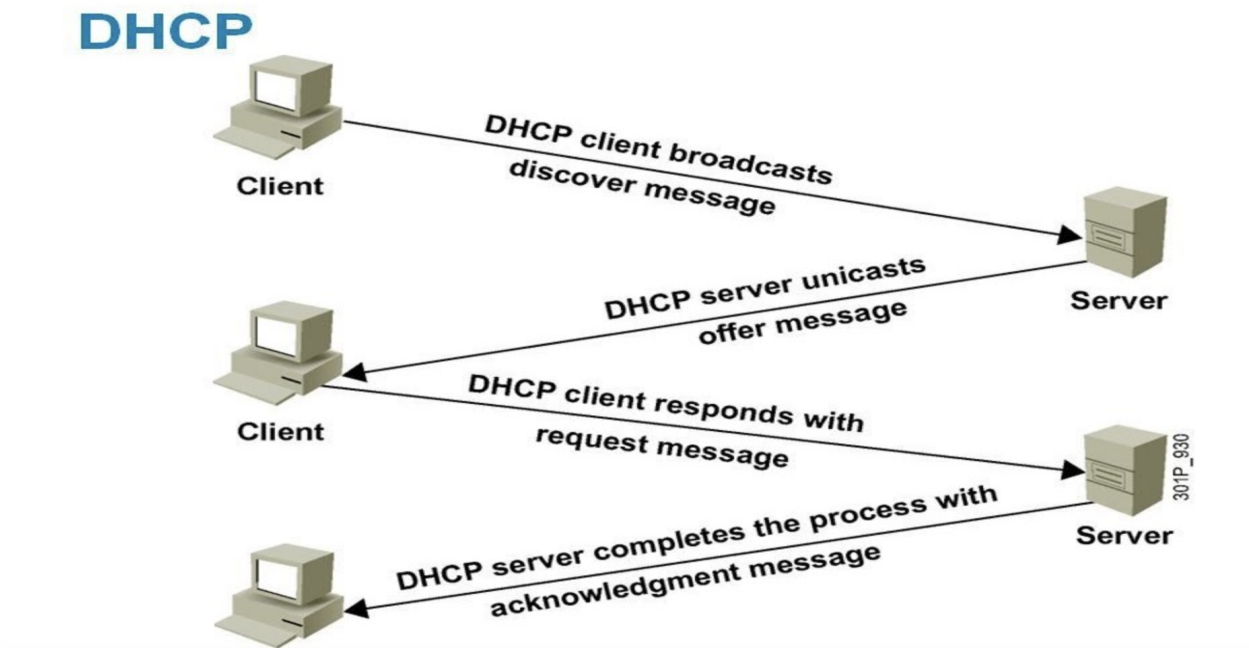
DHCP packets can be found in Layer 2 (data link layer).

DHCP discover is a broadcast packet.

Type	Source	Destination
IP	0.0.0.0	255.255.255.255
Port	68	67

2. 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.

When a machine starts up using DHCP, it has an Ethernet or other link layer address built-in, but no IP address. The machine transmits an IP address request throughout the network, just as ARP. Utilizing a DHCP DISCOVER packet does this. The DHCP server must receive this packet. A free IP address is assigned when the server gets the request, and it then delivers it to the host in a DHCP OFFER packet. The server recognizes a host by its Ethernet address (contained in the DHCP DISCOVER packet) in order to perform this function even when hosts lack IP addresses.



Figure

```
2 5.166954    0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0xa69b8b3f
3 6.194089    192.168.1.254    255.255.255.255    DHCP     342 DHCP Offer    - Transaction ID 0xa69b8b3f
4 6.195104    0.0.0.0          255.255.255.255    DHCP     348 DHCP Request  - Transaction ID 0xa69b8b3f
5 6.224160    192.168.1.254    192.168.1.72       DHCP     347 DHCP ACK      - Transaction ID 0xa69b8b3f
```

These 4 packets involved from discover to acknowledge in client to DHCP communication.

3. What is the significance of DHCP Release packet?

A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

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

The client will get many offers if there are multiple DHCP servers on the same network. Then, it will choose and react to just one. The issue is that there isn't a defined method for one server to communicate its state to other servers. The same addresses can therefore be provided to many hosts if they are present in the DHCP server pools. There are various methods we might use to lessen these hazards as a result.

We can even use more than one strategy according to our needs:

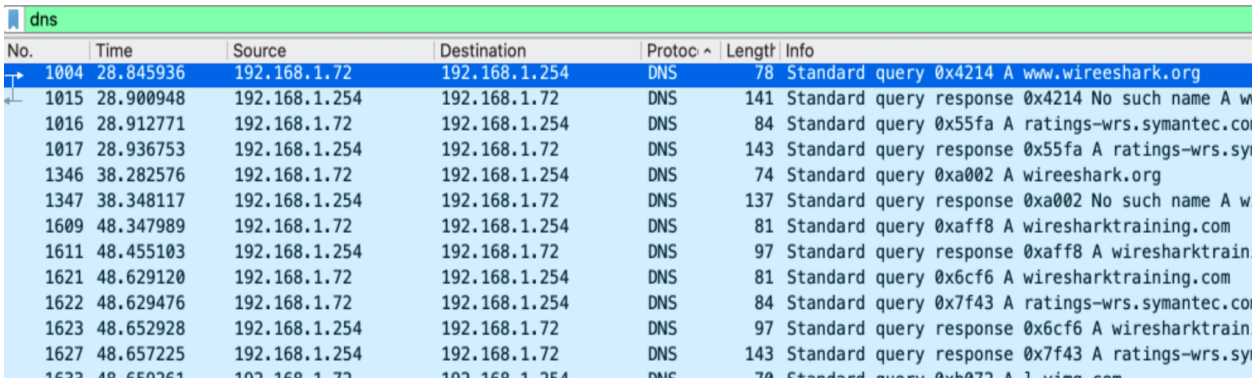
Create subnetworks: DHCP servers are separate for each subnetwork. In the event of a DHCP service failure, this can assist in decreasing broadcast overhead, lessen collision risks, and, of course, limit the universe of impacted customers.

Create a failover configuration: In the event of the primary DHCP server failing, a standby server will take over.

Split the address pools between multiple DHCP servers: The DHCP offers have non-overlapping address pools since everyone is online. When one fails, the other maintains service. We don't require a complex clustering configuration, nor do we need to change the network in any way. The disadvantage is that if only one server is up, its address pool needs to be sufficiently big to handle all users.

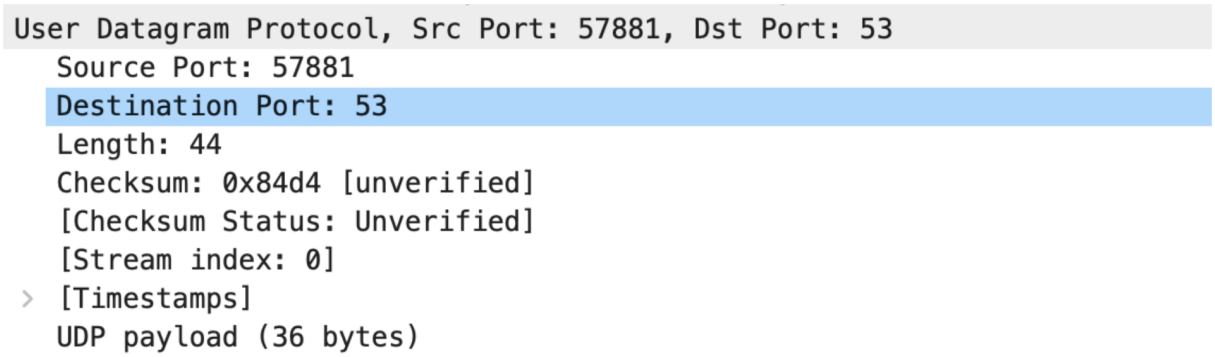
Part 5:

1. Use a filter to display DNS traffic only.



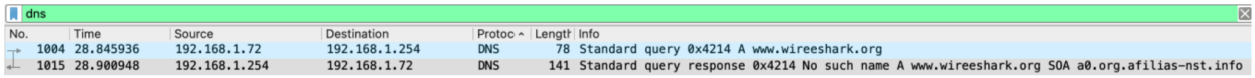
2. Which transport layer protocol is used for DNS queries?

UDP is being used on the transport layer for DNS



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

Packet number 1015 is the response for the packet 1004



The response is **No such name** as we are searching for a value that does not exist “wireshark.org”

```
Flags: 0x8183 Standard query response, No such name
   1... .... .... .... = Response: Message is a response
   .000 0... .... .... = Opcode: Standard query (0)
   .... .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)
```