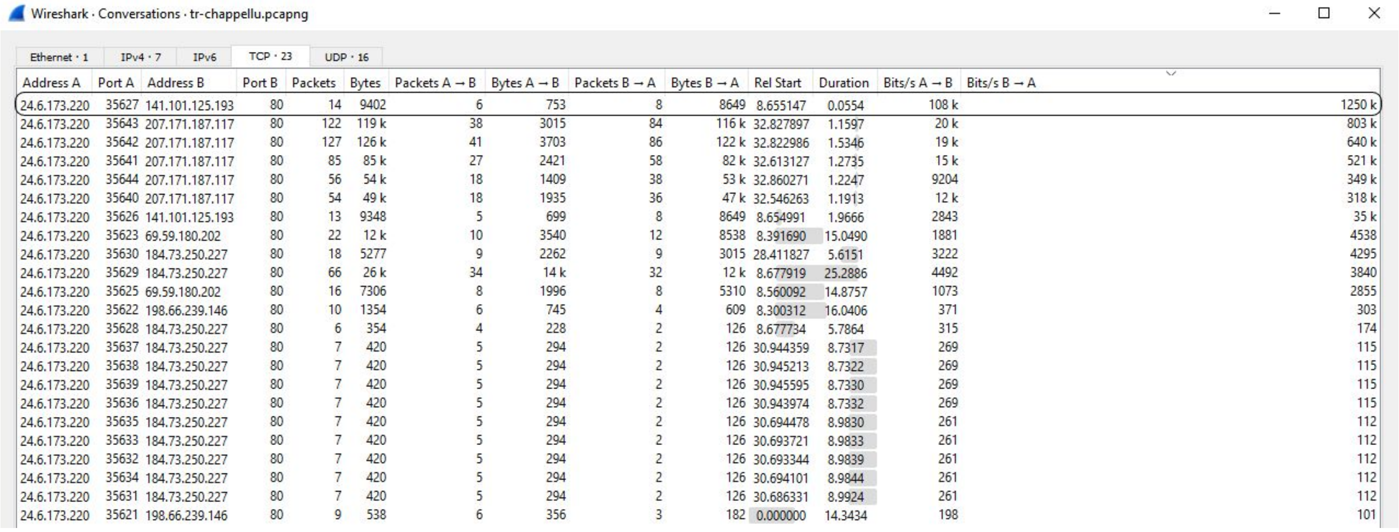
Assignment 2
Tanmay Dureja (td1391)

Part 1 Solutions

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

- The most active TCP conversation in this displayed as follows with Bits Transfer from A->B at 108kbits/s and B->A at 1250 kbits/s.



Wireshark · Conversations · tr-chappellu.pcapng

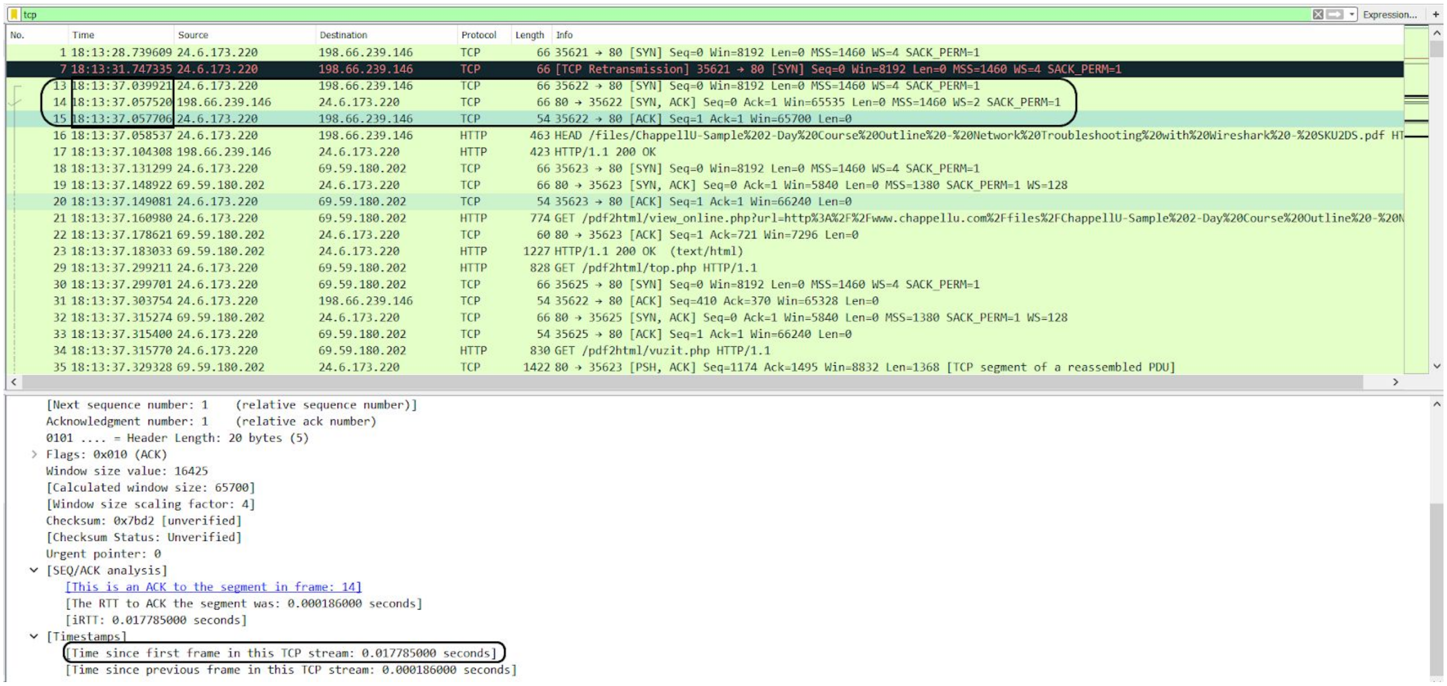
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.173.220	35627	141.101.125.193	80	14	9402	6	753	8	8649	8.655147	0.0554	108 k	1250 k
24.6.173.220	35643	207.171.187.117	80	122	119 k	38	3015	84	116 k	32.827897	1.1597	20 k	803 k
24.6.173.220	35642	207.171.187.117	80	127	126 k	41	3703	86	122 k	32.822986	1.5346	19 k	640 k
24.6.173.220	35641	207.171.187.117	80	85	85 k	27	2421	58	82 k	32.613127	1.2735	15 k	521 k
24.6.173.220	35644	207.171.187.117	80	56	54 k	18	1409	38	53 k	32.860271	1.2247	9204	349 k
24.6.173.220	35640	207.171.187.117	80	54	49 k	18	1935	36	47 k	32.546263	1.1913	12 k	318 k
24.6.173.220	35626	141.101.125.193	80	13	9348	5	699	8	8649	8.654991	1.9666	2843	35 k
24.6.173.220	35623	69.59.180.202	80	22	12 k	10	3540	12	8538	8.391690	15.0490	1881	4538
24.6.173.220	35630	184.73.250.227	80	18	5277	9	2262	9	3015	28.411827	5.6151	3222	4295
24.6.173.220	35629	184.73.250.227	80	66	26 k	34	14 k	32	12 k	8.677919	25.2886	4492	3840
24.6.173.220	35625	69.59.180.202	80	16	7306	8	1996	8	5310	8.560092	14.8757	1073	2855
24.6.173.220	35622	198.66.239.146	80	10	1354	6	745	4	609	8.300312	16.0406	371	303
24.6.173.220	35628	184.73.250.227	80	6	354	4	228	2	126	8.677734	5.7864	315	174
24.6.173.220	35637	184.73.250.227	80	7	420	5	294	2	126	30.944359	8.7317	269	115
24.6.173.220	35638	184.73.250.227	80	7	420	5	294	2	126	30.945213	8.7322	269	115
24.6.173.220	35639	184.73.250.227	80	7	420	5	294	2	126	30.945595	8.7330	269	115
24.6.173.220	35636	184.73.250.227	80	7	420	5	294	2	126	30.943974	8.7332	269	115
24.6.173.220	35635	184.73.250.227	80	7	420	5	294	2	126	30.694478	8.9830	261	112
24.6.173.220	35633	184.73.250.227	80	7	420	5	294	2	126	30.693721	8.9833	261	112
24.6.173.220	35632	184.73.250.227	80	7	420	5	294	2	126	30.693344	8.9839	261	112
24.6.173.220	35634	184.73.250.227	80	7	420	5	294	2	126	30.694101	8.9844	261	112
24.6.173.220	35631	184.73.250.227	80	7	420	5	294	2	126	30.686331	8.9924	261	112
24.6.173.220	35621	198.66.239.146	80	9	538	6	356	3	182	0.000000	14.3434	198	101

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)

A->B 753 bytes
B->A 8649 bytes
for a total of 9402 bytes.

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

The Round Trip Time or RTT 0.017785 seconds by analysing the packets.

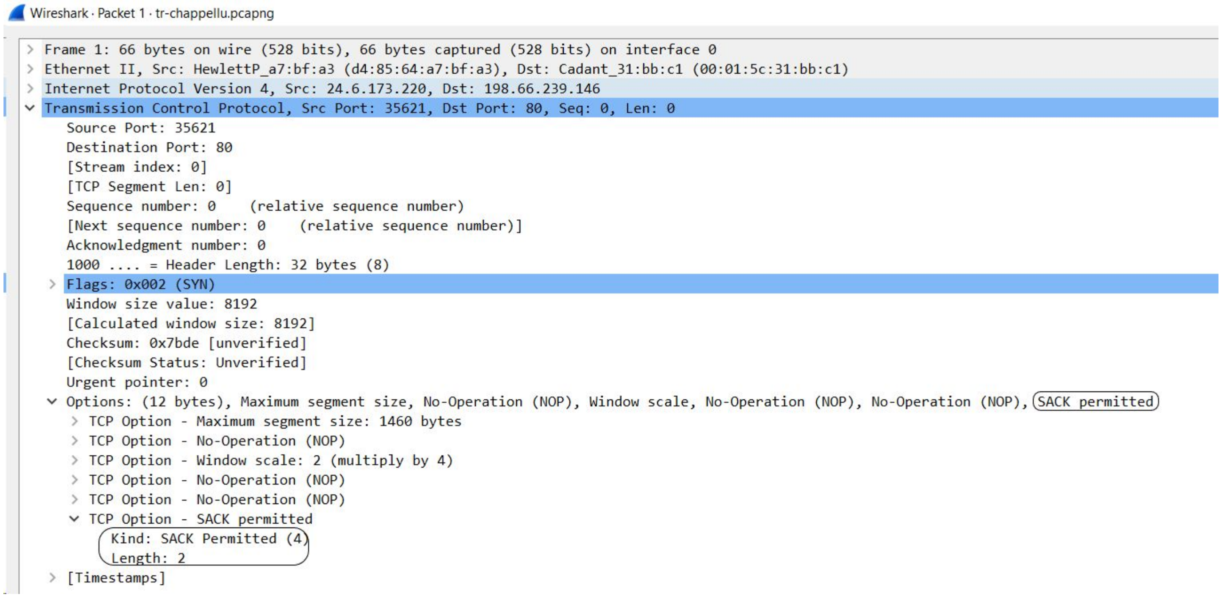


No.	Time	Source	Destination	Protocol	Length	Info
1	18:13:28.739609	24.6.173.220	198.66.239.146	TCP	66	35621 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	18:13:31.747335	24.6.173.220	198.66.239.146	TCP	66	[TCP Retransmission] 35621 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	18:13:37.039921	24.6.173.220	198.66.239.146	TCP	66	35622 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
14	18:13:37.057520	198.66.239.146	24.6.173.220	TCP	66	80 → 35622 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
15	18:13:37.057706	24.6.173.220	198.66.239.146	TCP	54	35622 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
16	18:13:37.058537	24.6.173.220	198.66.239.146	HTTP	463	HEAD /files/ChappellU-Sample%202-Day%20Course%20Outline%20-%20Network%20Troubleshooting%20with%20Wireshark%20-%20SKU2DS.pdf HT
17	18:13:37.104308	198.66.239.146	24.6.173.220	HTTP	423	HTTP/1.1 200 OK
18	18:13:37.131299	24.6.173.220	69.59.180.202	TCP	66	35623 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19	18:13:37.148922	69.59.180.202	24.6.173.220	TCP	66	80 → 35623 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1 WS=128
20	18:13:37.149081	24.6.173.220	69.59.180.202	TCP	54	35623 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
21	18:13:37.160980	24.6.173.220	69.59.180.202	HTTP	774	GET /pdf2html/view_online.php?url=http%3A%2F%2Fwww.chappellu.com%2Ffiles%2FChappellU-Sample%202-Day%20Course%20Outline%20-%20N
22	18:13:37.178621	69.59.180.202	24.6.173.220	TCP	60	80 → 35623 [ACK] Seq=1 Ack=721 Win=7296 Len=0
23	18:13:37.183033	69.59.180.202	24.6.173.220	HTTP	1227	HTTP/1.1 200 OK (text/html)
29	18:13:37.299211	24.6.173.220	69.59.180.202	HTTP	828	GET /pdf2html/top.php HTTP/1.1
30	18:13:37.299701	24.6.173.220	69.59.180.202	TCP	66	35625 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
31	18:13:37.303754	24.6.173.220	198.66.239.146	TCP	54	35622 → 80 [ACK] Seq=410 Ack=370 Win=65328 Len=0
32	18:13:37.315274	69.59.180.202	24.6.173.220	TCP	66	80 → 35625 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1 WS=128
33	18:13:37.315400	24.6.173.220	69.59.180.202	TCP	54	35625 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
34	18:13:37.315770	24.6.173.220	69.59.180.202	HTTP	830	GET /pdf2html/vuzit.php HTTP/1.1
35	18:13:37.329328	69.59.180.202	24.6.173.220	TCP	1422	80 → 35623 [PSH, ACK] Seq=1174 Ack=1495 Win=8832 Len=1368 [TCP segment of a reassembled PDU]

```
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0x7bd2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 14]
      [The RTT to ACK the segment was: 0.000186000 seconds]
      [iRTT: 0.017785000 seconds]
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.017785000 seconds]
      [Time since previous frame in this TCP stream: 0.000186000 seconds]
```

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

Selective acknowledgements or SACK is a strategy used to correct the behaviour of multiple packet drops in a transmission. They help the receiver inform the sender of all the packets that arrived successfully so the sender needs to retransmit only the packets that were lost.
Yes, they are permitted in our conversation, it can be seen as follows in the packet information :-



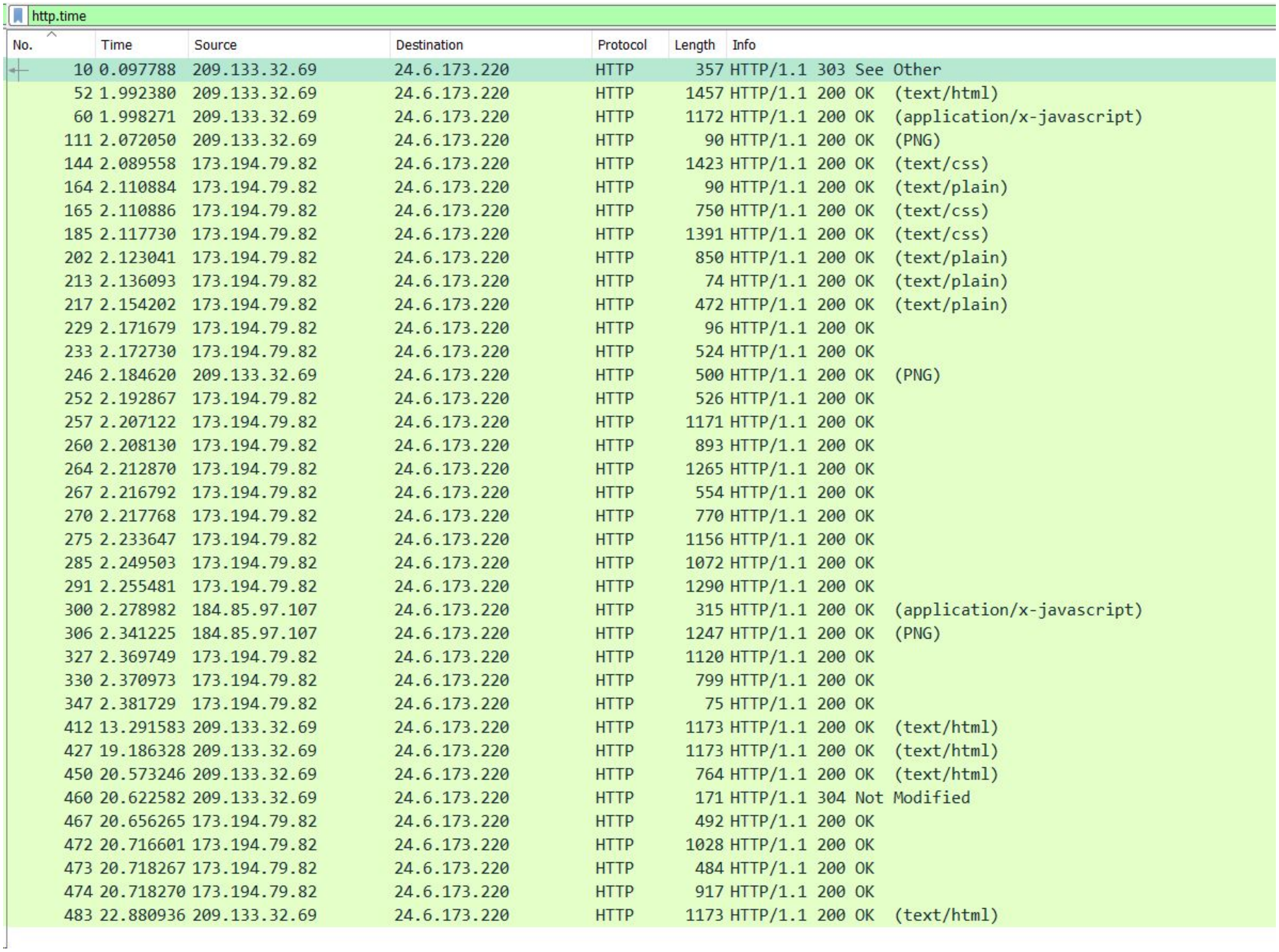
```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 198.66.239.146
v Transmission Control Protocol, Src Port: 35621, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 35621
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x7bde [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > TCP Option - Maximum segment size: 1460 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 2 (multiply by 4)
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    v TCP Option - SACK permitted
        Kind: SACK Permitted (4)
        Length: 2
  > [Timestamps]
```

Assignment 2
Tanmay Dureja (td1391)

Part 2 Solutions

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

The filter used would be ‘http.time’.



http.time

No.	Time	Source	Destination	Protocol	Length	Info
10	0.097788	209.133.32.69	24.6.173.220	HTTP	357	HTTP/1.1 303 See Other
52	1.992380	209.133.32.69	24.6.173.220	HTTP	1457	HTTP/1.1 200 OK (text/html)
60	1.998271	209.133.32.69	24.6.173.220	HTTP	1172	HTTP/1.1 200 OK (application/x-javascript)
111	2.072050	209.133.32.69	24.6.173.220	HTTP	90	HTTP/1.1 200 OK (PNG)
144	2.089558	173.194.79.82	24.6.173.220	HTTP	1423	HTTP/1.1 200 OK (text/css)
164	2.110884	173.194.79.82	24.6.173.220	HTTP	90	HTTP/1.1 200 OK (text/plain)
165	2.110886	173.194.79.82	24.6.173.220	HTTP	750	HTTP/1.1 200 OK (text/css)
185	2.117730	173.194.79.82	24.6.173.220	HTTP	1391	HTTP/1.1 200 OK (text/css)
202	2.123041	173.194.79.82	24.6.173.220	HTTP	850	HTTP/1.1 200 OK (text/plain)
213	2.136093	173.194.79.82	24.6.173.220	HTTP	74	HTTP/1.1 200 OK (text/plain)
217	2.154202	173.194.79.82	24.6.173.220	HTTP	472	HTTP/1.1 200 OK (text/plain)
229	2.171679	173.194.79.82	24.6.173.220	HTTP	96	HTTP/1.1 200 OK
233	2.172730	173.194.79.82	24.6.173.220	HTTP	524	HTTP/1.1 200 OK
246	2.184620	209.133.32.69	24.6.173.220	HTTP	500	HTTP/1.1 200 OK (PNG)
252	2.192867	173.194.79.82	24.6.173.220	HTTP	526	HTTP/1.1 200 OK
257	2.207122	173.194.79.82	24.6.173.220	HTTP	1171	HTTP/1.1 200 OK
260	2.208130	173.194.79.82	24.6.173.220	HTTP	893	HTTP/1.1 200 OK
264	2.212870	173.194.79.82	24.6.173.220	HTTP	1265	HTTP/1.1 200 OK
267	2.216792	173.194.79.82	24.6.173.220	HTTP	554	HTTP/1.1 200 OK
270	2.217768	173.194.79.82	24.6.173.220	HTTP	770	HTTP/1.1 200 OK
275	2.233647	173.194.79.82	24.6.173.220	HTTP	1156	HTTP/1.1 200 OK
285	2.249503	173.194.79.82	24.6.173.220	HTTP	1072	HTTP/1.1 200 OK
291	2.255481	173.194.79.82	24.6.173.220	HTTP	1290	HTTP/1.1 200 OK
300	2.278982	184.85.97.107	24.6.173.220	HTTP	315	HTTP/1.1 200 OK (application/x-javascript)
306	2.341225	184.85.97.107	24.6.173.220	HTTP	1247	HTTP/1.1 200 OK (PNG)
327	2.369749	173.194.79.82	24.6.173.220	HTTP	1120	HTTP/1.1 200 OK
330	2.370973	173.194.79.82	24.6.173.220	HTTP	799	HTTP/1.1 200 OK
347	2.381729	173.194.79.82	24.6.173.220	HTTP	75	HTTP/1.1 200 OK
412	13.291583	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)
427	19.186328	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)
450	20.573246	209.133.32.69	24.6.173.220	HTTP	764	HTTP/1.1 200 OK (text/html)
460	20.622582	209.133.32.69	24.6.173.220	HTTP	171	HTTP/1.1 304 Not Modified
467	20.656265	173.194.79.82	24.6.173.220	HTTP	492	HTTP/1.1 200 OK
472	20.716601	173.194.79.82	24.6.173.220	HTTP	1028	HTTP/1.1 200 OK
473	20.718267	173.194.79.82	24.6.173.220	HTTP	484	HTTP/1.1 200 OK
474	20.718270	173.194.79.82	24.6.173.220	HTTP	917	HTTP/1.1 200 OK
483	22.880936	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)

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

200 OK is the response for a successful HTTP request and it depends on the type of HTTP request method used.

For a GET request it means that the resource was transmitted in the response message body.

For a HEAD request it means that only the HTTP header fields were sent in the response and no data/payload is sent with it.

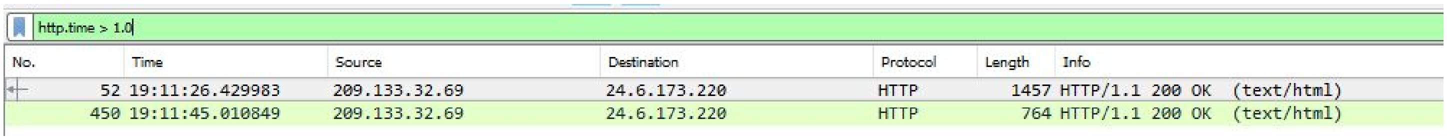
For a POST request it means that a resource containing/describing the result of the action is sent.

303 See Other is the response code for a redirect status, which means that the requested resource can be found at a different Uniform Resource Identifier.

304 Not Modified is the response when there is no need to retransmit the requested resource. It redirects to a cached resource.

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

The packets where HTTP response time is greater than one second are listed below :-

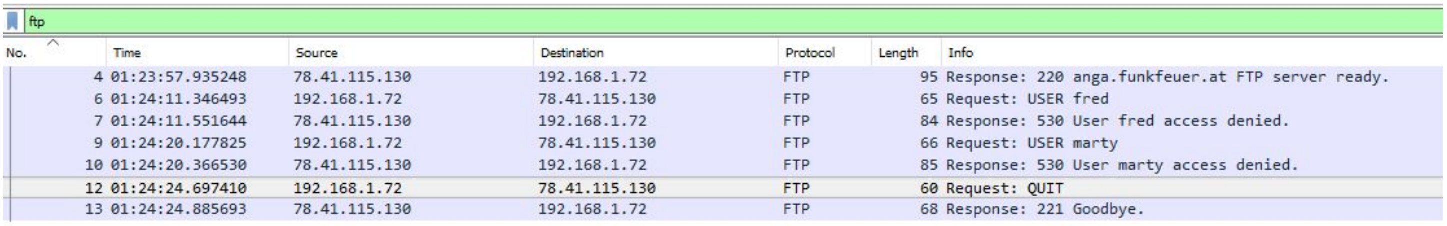


```
http.time > 1.0
No.    Time              Source          Destination     Protocol  Length Info
    52 19:11:26.429983   209.133.32.69   24.6.173.220    HTTP        1457 HTTP/1.1 200 OK  (text/html)
   450 19:11:45.010849   209.133.32.69   24.6.173.220    HTTP         764 HTTP/1.1 200 OK  (text/html)
```

Part 3 Solutions

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

'ftp' filter displays the request and response packages.



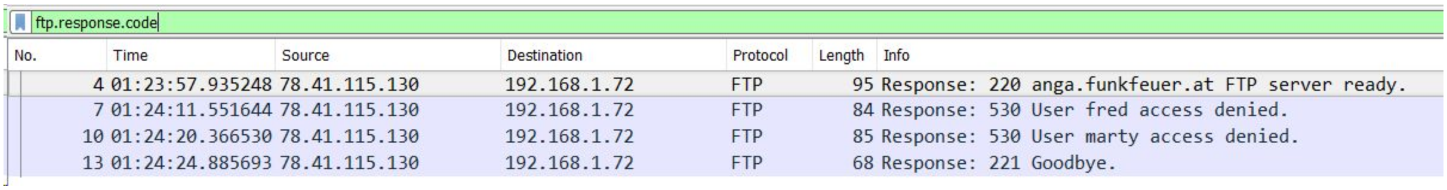
```
ftp
No.     Time              Source          Destination     Protocol  Length Info
      4 01:23:57.935248   78.41.115.130   192.168.1.72    FTP           95 Response: 220 anga.funkfeuer.at FTP server ready.
      6 01:24:11.346493   192.168.1.72    78.41.115.130   FTP           65 Request: USER fred
      7 01:24:11.551644   78.41.115.130   192.168.1.72    FTP           84 Response: 530 User fred access denied.
      9 01:24:20.177825   192.168.1.72    78.41.115.130   FTP           66 Request: USER marty
     10 01:24:20.366530   78.41.115.130   192.168.1.72    FTP           85 Response: 530 User marty access denied.
     12 01:24:24.697410   192.168.1.72    78.41.115.130   FTP           60 Request: QUIT
     13 01:24:24.885693   78.41.115.130   192.168.1.72    FTP           68 Response: 221 Goodbye.
```

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

Client – 192.168.1.72 , 39322
Server – 78.41.115.130, 21

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

'ftp.response.code' is the filter used.

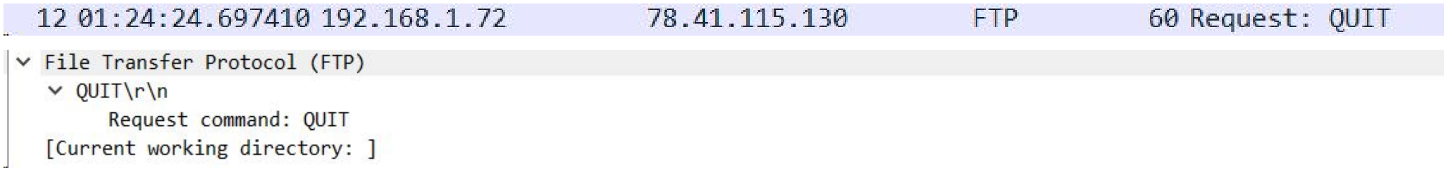


```
ftp.response.code
No.    Time            Source          Destination    Protocol  Length Info
     4 01:23:57.935248 78.41.115.130   192.168.1.72   FTP           95 Response: 220 anga.funkfeuer.at FTP server ready.
     7 01:24:11.551644 78.41.115.130   192.168.1.72   FTP           84 Response: 530 User fred access denied.
    10 01:24:20.366530 78.41.115.130   192.168.1.72   FTP           85 Response: 530 User marty access denied.
    13 01:24:24.885693 78.41.115.130   192.168.1.72   FTP           68 Response: 221 Goodbye.
```

Response Codes
220 Server Ready- This code is sent to respond to a new user who is connecting to the FTP Server that the server is ready to accept new clients.
530 Not Logged In - This code is sent to respond to any requests/commands from the user to log-in before the command is processed.

221 Goodbye- This code is sent over to respond to the client's QUIT request and is sent immediately before the control connection is closed by the server.

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



```
12 01:24:24.697410 192.168.1.72         78.41.115.130        FTP        60 Request: QUIT
```

```
v File Transfer Protocol (FTP)
  v QUIT\r\n
      Request command: QUIT
  [Current working directory: ]
```

FTP termination is initiated by Client as seen in the capture above, when a client sends a QUIT request. When the server accepts a QUIT request, it closes the connection and does not read any further requests, stops listening for data connections and drops any accepted connections.

e. How secure is FTP?

FTP is not secure independently as it is a plain text based protocol and un-encrypted.
, FTP + TLS/SSL (FTPS) is an extension to FTP that adds transport layer security and provides reasonable security if the server encrypts control and data streams. FTP can also be secured as SFTP(SSH FTP) and is an extension to Secure Shell protocol to provide secure file transfer.

Part 4 Solutions

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.

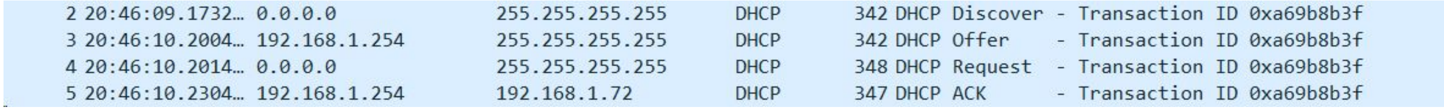
DHCP Discover packets can be found in the Application Layer in the OSI Model.
DHCP Discover is a UDP Packet.

Source, Port		Destination, Port
0.0.0.0, 68	--->	255.255.255.255, 67
192.168.1.66, 68	--->	255.255.255.255, 67
192.168.1.68, 68	--->	255.255.255.255, 67
192.168.1.72, 68	--->	255.255.255.255, 67
192.168.1.254, 67	--->	255.255.255.255, 68
192.168.1.254, 67	--->	192.168.1.72, 68
192.168.1.72, 68	--->	192.168.1.254, 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 packets are exchanged between the client and server before the client receives an IP address namely
Discover - the client broadcasts a message on the network to discover available DHCP Servers.
Offer - a DHCP server receives the client's request and offers an address from its pool of addresses.
Request - the client replies to the offer requesting the address received in Offer.

Ack - the server acknowledges the request, and provides the client with the address along with other information such as address validity.

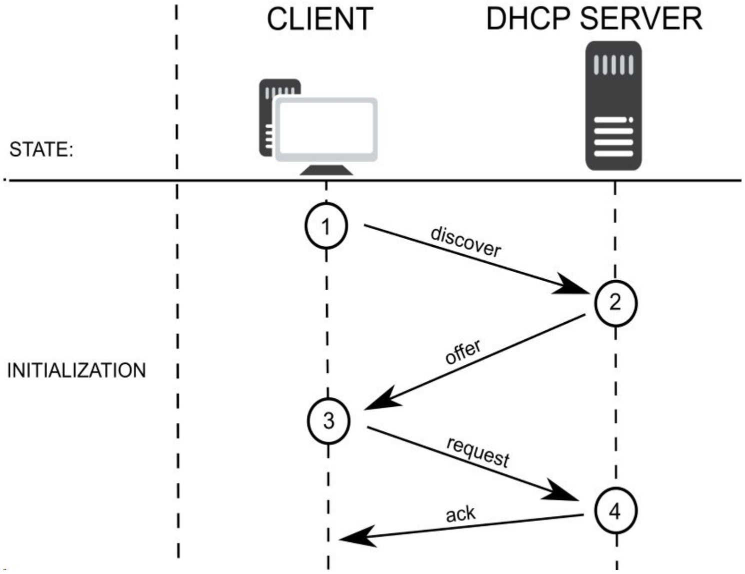


```
    2 20:46:09.1732… 0.0.0.0            255.255.255.255     DHCP      342 DHCP Discover - Transaction ID 0xa69b8b3f
    3 20:46:10.2004… 192.168.1.254      255.255.255.255     DHCP      342 DHCP Offer    - Transaction ID 0xa69b8b3f
    4 20:46:10.2014… 0.0.0.0            255.255.255.255     DHCP      348 DHCP Request  - Transaction ID 0xa69b8b3f
    5 20:46:10.2304… 192.168.1.254      192.168.1.72        DHCP      347 DHCP ACK      - Transaction ID 0xa69b8b3f
```

c. What is the significance of DHCP Release packet?

If the client does not need the allocated IP address any longer, it unicasts a DHCP Release message to the DHCP server. The server then releases the client IP address listed in the client IP field of the received message. Client devices usually do not know when they may be unplugged from the network by the user, the protocol does not mandate the sending of DHCP Release.

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



DHCP client broadcasts a request DHCP Discover message on the network subnet for necessary network information of the the DHCP Server, then the server offers IP parameters in a DHCP Offer message. The client again sends a DHCP Request message to get the offered IP address, which are acknowledged by the server by a DHCP Ack message.

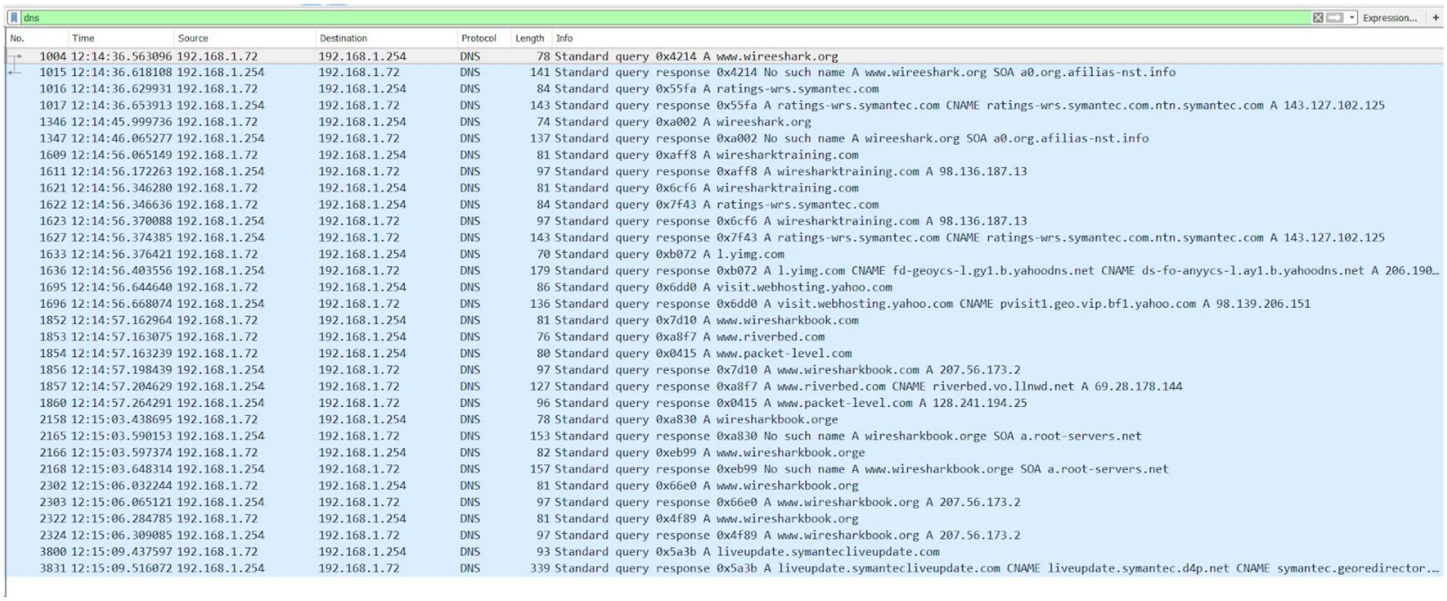
For the condition where two DHCP Servers occur on the same network, the client would would broadcast a Discover request and the first DHCP server to respond with the network information would be the 'winning' server in our case. But if two servers occur on the same subnet, they should have an appropriate distribution of the subnet addresses.

Assignment 2
Tanmay Dureja (td1391)

Part 5 Solutions

a. Use a filter to display DNS traffic only.

Filter used is ‘dns’.



dns

No.	Time	Source	Destination	Protocol	Length	Info
1004	12:14:36.563096	192.168.1.72	192.168.1.254	DNS	78	Standard query 0x4214 A www.wireeshark.org
1015	12:14:36.618108	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	12:14:36.629931	192.168.1.72	192.168.1.254	DNS	84	Standard query 0x55fa A ratings-wrs.symantec.com
1017	12:14:36.653913	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 143.127.102.125
1346	12:14:45.999736	192.168.1.72	192.168.1.254	DNS	74	Standard query 0xa002 A wireeshark.org
1347	12:14:46.065277	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	12:14:56.065149	192.168.1.72	192.168.1.254	DNS	81	Standard query 0xaff8 A wiresharktraining.com
1611	12:14:56.172263	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0xaff8 A wiresharktraining.com A 98.136.187.13
1621	12:14:56.346280	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x6cf6 A wiresharktraining.com
1622	12:14:56.346636	192.168.1.72	192.168.1.254	DNS	84	Standard query 0x7f43 A ratings-wrs.symantec.com
1623	12:14:56.370088	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x6cf6 A wiresharktraining.com A 98.136.187.13
1627	12:14:56.374385	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 143.127.102.125
1633	12:14:56.376421	192.168.1.72	192.168.1.254	DNS	70	Standard query 0xb072 A l.yimg.com
1636	12:14:56.403556	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.yahoodns.net A 206.190…
1695	12:14:56.644640	192.168.1.72	192.168.1.254	DNS	86	Standard query 0x6dd0 A visit.webhosting.yahoo.com
1696	12:14:56.668074	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 98.139.206.151
1852	12:14:57.162964	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x7d10 A www.wiresharkbook.com
1853	12:14:57.163075	192.168.1.72	192.168.1.254	DNS	76	Standard query 0xa8f7 A www.riverbed.com
1854	12:14:57.163239	192.168.1.72	192.168.1.254	DNS	80	Standard query 0x0415 A www.packet-level.com
1856	12:14:57.198439	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x7d10 A www.wiresharkbook.com A 207.56.173.2
1857	12:14:57.204629	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	12:14:57.264291	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	12:15:03.438695	192.168.1.72	192.168.1.254	DNS	78	Standard query 0xa830 A wiresharkbook.orge
2165	12:15:03.590153	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	12:15:03.597374	192.168.1.72	192.168.1.254	DNS	82	Standard query 0xeb99 A www.wiresharkbook.orge
2168	12:15:03.648314	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	12:15:06.032244	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x66e0 A www.wiresharkbook.org
2303	12:15:06.065121	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x66e0 A www.wiresharkbook.org A 207.56.173.2
2322	12:15:06.284785	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x4f89 A www.wiresharkbook.org
2324	12:15:06.309085	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x4f89 A www.wiresharkbook.org A 207.56.173.2
3800	12:15:09.437597	192.168.1.72	192.168.1.254	DNS	93	Standard query 0x5a3b A liveupdate.symantecliveupdate.com
3831	12:15:09.516072	192.168.1.254	192.168.1.72	DNS	339	Standard query response 0x5a3b A liveupdate.symantecliveupdate.com CNAME liveupdate.symantec.d4p.net CNAME symantec.georedirector.…

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

DNS is an application protocol which typically uses UDP. It constructs a DNS query message and passes the message to UDP.

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

The response to the DNS query of packet number 1004 at packet 1015 is No Such Name, meaning that the domain name referenced in the query does not exist.

<u>Response from packet capture -</u> Standard query response 0x4214 No such name A www.wireeshark.org SOA a0.org.afilias-nst.info