

Homework 1

Part 1: tr-chappelu.pcapng

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

Under Wireshark TCP · 23: the TCP conversation of Address A (24.6.173.220), Port 35627 and Address B (141.101.125.193), Port 80 had the most active conversation.

- Bits/s A → B: 108k
- Bits/s B → A: 1250k

Ethernet · 1		IPv4 · 7	IPv6	TCP · 23	UDP · 16								
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	35621	198.66.239.146	80	9	538	6	356	3	182	0.000000	14.3434	198	101
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	35623	69.59.180.202	80	22	12k	10	3540	12	8538	8.391690	15.0490	1881	4538
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	35626	141.101.125.193	80	13	9348	5	699	8	8649	8.654991	1.9666	2843	35k
24.6.173.220	35627	141.101.125.193	80	14	9402	6	753	8	8649	8.655147	0.0554	108k	1250k
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	35629	184.73.250.227	80	66	26k	34	14k	32	12k	8.677919	25.2886	4492	3840
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	35631	184.73.250.227	80	7	420	5	294	2	126	30.686331	8.9924	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	35633	184.73.250.227	80	7	420	5	294	2	126	30.693721	8.9833	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	35635	184.73.250.227	80	7	420	5	294	2	126	30.694478	8.9830	261	112
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	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	35640	207.171.187.117	80	54	49k	18	1935	36	47k	32.546263	1.1913	12k	318k
24.6.173.220	35641	207.171.187.117	80	85	85k	27	2421	58	82k	32.613127	1.2735	15k	521k
24.6.173.220	35642	207.171.187.117	80	127	126k	41	3703	86	122k	32.822986	1.5346	19k	640k
24.6.173.220	35643	207.171.187.117	80	122	119k	38	3015	84	116k	32.827897	1.1597	20k	803k
24.6.173.220	35644	207.171.187.117	80	56	54k	18	1409	38	53k	32.860271	1.2247	9204	349k

- 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)

No.	Time	Source	Destination	Protocol	Length	Info
51	8.655147	24.6.173.220	141.101.125.193	TCP	66	35627 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	8.676020	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
56	8.676466	24.6.173.220	141.101.125.193	HTTP	471	GET /legacy/graphics/promo/reader_2_728x90.png HTTP/1.1
63	8.704621	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=2921 Win=65700 Len=0
68	8.710054	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=8200 Win=65700 Len=0
69	8.710497	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [RST, ACK] Seq=418 Ack=8200 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
51	8.655147	24.6.173.220	141.101.125.193	TCP	66	35627 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	8.676020	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
56	8.676466	24.6.173.220	141.101.125.193	HTTP	471	GET /legacy/graphics/promo/reader_2_728x90.png HTTP/1.1
63	8.704621	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=2921 Win=65700 Len=0
68	8.710054	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [ACK] Seq=418 Ack=8200 Win=65700 Len=0
69	8.710497	24.6.173.220	141.101.125.193	TCP	54	35627 → 80 [RST, ACK] Seq=418 Ack=8200 Win=0 Len=0

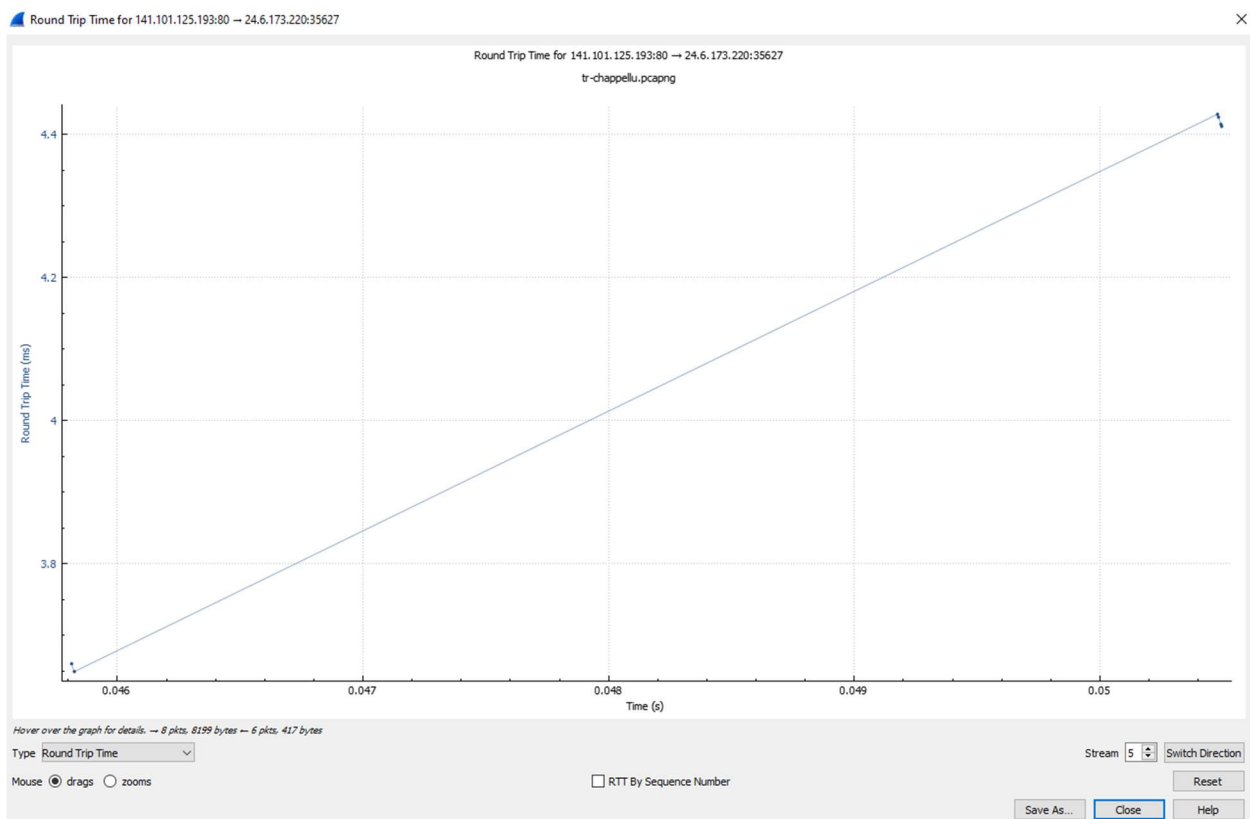
24.6.173.220	35627	141.101.125.193	80	14	9402	6	753	8	8649	8.655147	0.0554	108k	1250k
--------------	-------	-----------------	----	----	------	---	-----	---	------	----------	--------	------	-------

- Packets A → B: 753 bytes, 6 packets
- Packets B → A: 8649 bytes, 8 packets

In the filtered conversation:

No.	Bytes captured
51	66 bytes
54	54 bytes
56	471 bytes
63	54 bytes
68	54 bytes
69	54 bytes
Total	753 bytes captured

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



No.	Time since first frame	Time since previous frame	RTT calculated	RTT to ACK the segment
51	0	0 s	0 s	Not an ACK packet
54	0.020873 s	0.000137 s	0.020736 s	0.000137 seconds
56	0.021319 s	0.000446 s	0.020873 s	0.020873 seconds
63	0.049474 s	0.003649 s	0.045825 s	0.003649 seconds

68	0.054907 s	0.004411 s	0.050496 s	0.004411 seconds
69	0.05535000 s	0.000443 s	0.054907 s	0.054907 seconds

- Packet No. 51 does not have any RTT info as it is not an ACK packet sent.
- d) What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.

```
51 8.655147 24.6.173.220 141.101.125.1... TCP 66 35627 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
```

Frame 51 shows SACK_PERMS=1, meaning that selective acknowledgements are permitted in this conversation of kind 4 and length 2. The client has sent out packet no. 51 with the setting of SACK_PERMITTED = 1 to the server, informing the server that the client has Selective Acknowledgement options turned on¹.

When inspecting other TCP conversations with SACK permitted, the client would send out retransmissions for packets of different frames, showing cases of Selective Acknowledgements.

```

    TCP Option - SACK permitted
      Kind: SACK Permitted (4)
      Length: 2

```

Selective Acknowledgements are a modification to the TCP protocol where the TCP receiver will selectively choose what packet segments to acknowledge in the event that packets sent are out of order or in the event of packet lost². The TCP receiver will send duplicate acknowledgements for the packet segments they have received to the TCP sender. The TCP sender will deduce from the acknowledgements that there is a missing packet and send the missing packet to the receiver until the acknowledgement is received for that particular packet³. This is to reduce the number of redundant packets being sent to the TCP receiver during the event of packet loss or out-of-order packets being received⁴.

¹ <https://blog.catchpoint.com/2014/06/17/sack-transmissions-improve-web-performance/>

² Kurose & Ross, chapter 3, page 250

³ <https://packetlife.net/blog/2010/jun/17/tcp-selective-acknowledgments-sack/>

⁴ <https://blog.catchpoint.com/2014/06/17/sack-transmissions-improve-web-performance/>

Part 2: tr-http-pcaprnet.pcapng

a) Use a filter to display the HTTP response time for each HTTP 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-javascript)
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

```

Connection: close\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.026416000 seconds]
[Request in frame: 8]
[Request URI: http://www.pcapr.net/]

```

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-javascript)
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
264	2.212870	173.194.79.82	24.6.173.220	HTTP	1265	0.039248000	HTTP/1.1 200 OK
267	2.216792	173.194.79.82	24.6.173.220	HTTP	554	0.061540000	HTTP/1.1 200 OK
270	2.217768	173.194.79.82	24.6.173.220	HTTP	770	0.044871000	HTTP/1.1 200 OK
275	2.233647	173.194.79.82	24.6.173.220	HTTP	1156	0.039559000	HTTP/1.1 200 OK
285	2.249503	173.194.79.82	24.6.173.220	HTTP	1072	0.040068000	HTTP/1.1 200 OK
291	2.255481	173.194.79.82	24.6.173.220	HTTP	1290	0.041366000	HTTP/1.1 200 OK
300	2.278982	184.85.97.107	24.6.173.220	HTTP	315	0.039826000	HTTP/1.1 200 OK (application/x-javascript)
306	2.341225	184.85.97.107	24.6.173.220	HTTP	1247	0.016343000	HTTP/1.1 200 OK (PNG)
327	2.369749	173.194.79.82	24.6.173.220	HTTP	1120	0.044075000	HTTP/1.1 200 OK
330	2.370973	173.194.79.82	24.6.173.220	HTTP	799	0.045642000	HTTP/1.1 200 OK
347	2.381729	173.194.79.82	24.6.173.220	HTTP	75	0.173648000	HTTP/1.1 200 OK
412	13.291583	209.133.32.69	24.6.173.220	HTTP	1173	0.075087000	HTTP/1.1 200 OK (text/html)
427	19.186328	209.133.32.69	24.6.173.220	HTTP	1173	0.123874000	HTTP/1.1 200 OK (text/html)
450	20.573246	209.133.32.69	24.6.173.220	HTTP	764	1.987546000	HTTP/1.1 200 OK (text/html)
460	20.622582	209.133.32.69	24.6.173.220	HTTP	171	0.019483000	HTTP/1.1 304 Not Modified
467	20.656265	173.194.79.82	24.6.173.220	HTTP	492	0.044714000	HTTP/1.1 200 OK
472	20.716601	173.194.79.82	24.6.173.220	HTTP	1028	0.041555000	HTTP/1.1 200 OK
473	20.718267	173.194.79.82	24.6.173.220	HTTP	484	0.042814000	HTTP/1.1 200 OK
474	20.718270	173.194.79.82	24.6.173.220	HTTP	917	0.043575000	HTTP/1.1 200 OK
483	22.880936	209.133.32.69	24.6.173.220	HTTP	1173	0.073502000	HTTP/1.1 200 OK (text/html)

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

- 200 OK: The information was successfully fetched and has been sent.
- 303 See Other: The server has provided the client with another URL GET request for the client to redirect to.
- 304 Not Modified: Informs the client to use a cached version of the response as the message has not been modified.

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

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
52	1.992380	209.133.32.69	24.6.173.220	HTTP	1457	1.866336000	HTTP/1.1 200 OK (text/html)
450	20.573246	209.133.32.69	24.6.173.220	HTTP	764	1.987546000	HTTP/1.1 200 OK (text/html)

No.	Time since request
52	1.866336000 seconds
450	1.987546 seconds

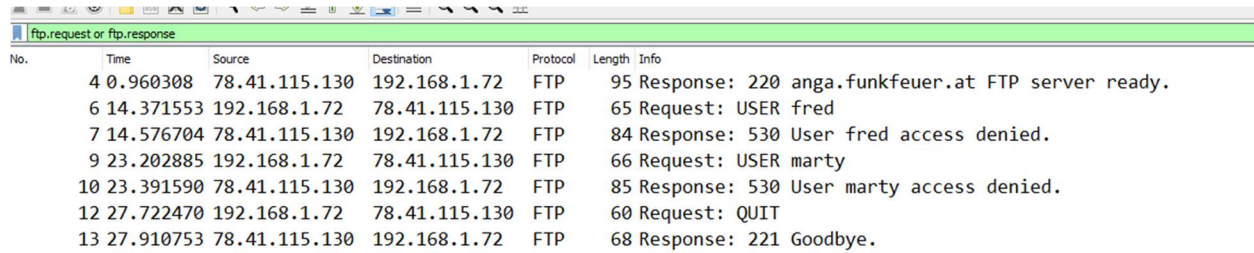
```

No.      Time      Source      Destination      Protocol Length Info
 52 1.992380 209.133.32.69 24.6.173.220 HTTP 1457 HTTP/1.1 200 OK (text/html)
Frame 52: 1457 bytes on wire (11656 bits), 1457 bytes captured (11656 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 209.133.32.69, Dst: 24.6.173.220
Transmission Control Protocol, Src Port: 80, Dst Port: 21214, Seq: 17521, Ack: 334, Len: 1403
[13 Reassembled TCP Segments (18923 bytes): #20(1460), #21(1460), #26(1460), #27(1460), #28(1460), #35(1460), #36(1460), #37(1460), #39(1460), #47(1460), #49(1460), #50(1460), #52(1403)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 23 Oct 2012 23:11:13 GMT\r\n
  Server: Apache/2.0.52 (CentOS)\r\n
  Cache-Control: no-cache, no-store, max-age=0, must-revalidate\r\n
  ETag: "WZht10zCvKZwnyZVKbxKA=="\r\n
  Content-Length: 18651\r\n
  Connection: close\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 1.866336000 seconds]
[Request in frame: 18]
[Request URI: http://www.pcapr.net/home]
File Data: 18651 bytes
Line-based text data: text/html (445 lines)
No.      Time      Source      Destination      Protocol Length Info
 450 20.573246 209.133.32.69 24.6.173.220 HTTP 764 HTTP/1.1 200 OK (text/html)
Frame 450: 764 bytes on wire (6112 bits), 764 bytes captured (6112 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 209.133.32.69, Dst: 24.6.173.220
Transmission Control Protocol, Src Port: 80, Dst Port: 21237, Seq: 20441, Ack: 571, Len: 710
[15 Reassembled TCP Segments (21150 bytes): #432(1460), #433(1460), #435(1460), #436(1460), #437(1460), #439(1460), #440(1460), #441(1460), #442(1460), #444(1460), #445(1460), #446(1460), #448(1460), #449(1460), #450(710)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 23 Oct 2012 23:11:31 GMT\r\n
  Server: Apache/2.0.52 (CentOS)\r\n
  ETag: "szajxVtWroFWIENz+k8Etg=="\r\n
  Content-Length: 20941\r\n
  Connection: close\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 1.987546000 seconds]
[Request in frame: 420]
[Request URI: http://www.pcapr.net/browse?q=sip]
File Data: 20941 bytes
Line-based text data: text/html (528 lines)

```

Part 3: tr-ftpfail.pcapng

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

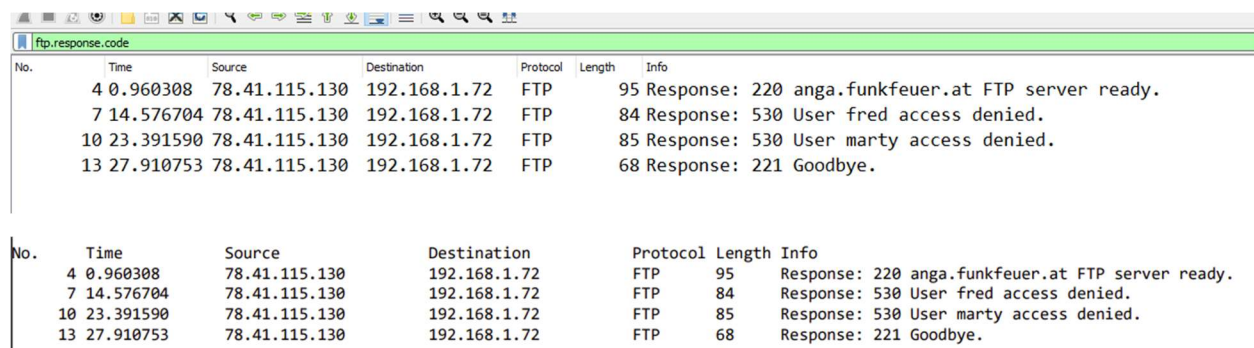


No.	Time	Source	Destination	Protocol	Length	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
6	14.371553	192.168.1.72	78.41.115.130	FTP	65	Request: USER fred
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
9	23.202885	192.168.1.72	78.41.115.130	FTP	66	Request: USER marty
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
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.

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

Server IP Address	Server Port Number	Client IP Address	Client Port Number
78.41.115.130	21	192.168.1.72	39322

c) Use another filter to display only the FTP response codes for the packets. Define and explain the significance of the response codes⁵.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.

- FTP 220: The FTP server is ready
- FTP 530: User access denied due to lack of password
- FTP 221: Server has closed the connection; informs the user that they have been logged out⁶.

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

While the request is sent by the client, the FTP connection has to be terminated by the server. This is due to the nature of TCP handshake where the FTP server maintains the user's state. It performs similarly to a TCP connection where the server and the client have to acknowledge each other's actions before proceeding. As such, the server has to send the termination command to the client and then receive an acknowledgement from the client in order to know that the client will also terminate its connection to the server⁷.

⁵ <https://www.wireshark.org/docs/dfref/f/ftp.html>

⁶ https://help.globalscape.com/help/cuteftpmacro3/Numbered_FTP_status_and_error_codes.htm

⁷ Kurose and Ross, page 117

As shown in the Wireshark capture, response code 221, the code to terminate the session was sent by the host server to the client to inform the client that of the termination process.

e) How secure is FTP?

FTP is not very secure. Similarly, to a standard TCP connection, there is no encryption as passwords and usernames are sent as cleartext during authentication⁸. It requires additional protocols such as Secure File Transfer Protocol (SFTP) in order to add another layer of encryption and security for during authentication⁹.

The capture shows usernames in cleartext which can be easily extracted from the connection. It would most likely show passwords as well if they were inputted into the FTP request packet.

⁸ <https://digitalguardian.com/blog/what-ftp-security-securing-ftp-usage>

⁹ <https://www.ssh.com/ssh/ftp/server>

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

DHCP packets are located in the IP protocol where it operates using the link-layer addresses¹⁰. The IP protocol is located in the Network Layer (Layer 3)¹¹. DHCP, itself, is an application layer (Layer 7) protocol. The DHCP Discover Packet is a UDP packet.

```
> Frame 4: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

- Source:
 - IP address: 0.0.0.0
 - Port Number: 68
 - Destination:
 - IP address: 255.255.255.255
 - Port Number: 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 packets are exchanged between the client and server for an IP address.

1. DHCP Discover: A client broadcasts a UDP packet with the IP address of 255.255.255.255 to all nodes on a subnet.
2. DHCP Offer: A DHCP server received the Discover packet and responds with an offer message to the client. Because the client has an IP address of 0.0.0.0, the DHCP Offer message is broadcasted through IP address 255.255.255.255. This message contains an offer of an IP address, a network mask, and a lease time for the IP address.
3. DHCP Request: The client will accept the offer from the DHCP server by echoing the configuration parameters back to the DHCP server.
4. DHCP Ack: The server responds to the DHCP request message with an acknowledgement of the parameters specified by the DHCP Ack, allowing the client to lease the IP address for the duration specified¹².

- c) What is the significance of DHCP Release packet?

It lets the client release their IP address along with the allotted time given to the client¹³.

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

¹⁰ <https://tools.ietf.org/html/rfc2131>

¹¹ Kurose & Ross, page 344

¹² Kurose & Ross, page 346

¹³ <https://tools.ietf.org/html/rfc2131>

Because the client and server have to broadcast the DHCP Discover and DHCP Offer messages to all nodes within a network, this can inform multiple servers about the DHCP client's request. Every DHCP server that receives the request will transmit their own DHCP offer messages via broadcast, allowing the client to receive multiple offers from different host servers. The client will choose from one of the offers by echoing the parameters of that DHCP offer message so that only the DHCP host server that sent out the parameters of that message will be able to recognize and lease out the IP address through a DHCP ACK message. The servers that don't match the parameters of the client will not respond.

Part 5: tr-nameresolution.pcapng

- a. Use a filter to display DNS traffic only.

DNS traffic can be seen by checking for port 53 on a UDP protocol. This is because port 53 is open to all systems.

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.afiliias-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 143.127.102.125
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.afiliias-nst.info
1609	48.347989	192.168.1.72	192.168.1.254	DNS	81	Standard query 0xa002 A wireesharktraining.com
1611	48.455103	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0xa002 A wireesharktraining.com A 98.136.187.13
1621	48.629120	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x6cf6 A wireesharktraining.com
1622	48.629476	192.168.1.254	192.168.1.72	DNS	84	Standard query 0x7f43 A ratings-wrs.symantec.com
1623	48.652928	192.168.1.72	192.168.1.254	DNS	97	Standard query response 0x6cf6 A wireesharktraining.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 143.127.102.125
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.gyl.b.yahoodns.net CNAME ds-fo-anyycs-l.gyl.b.yahoodns.net A 206.190.60.138
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 98.139.206.151

> Frame 1004: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{6E79FEC0-F779-4970-96E4-EFF300A9B9F}, id 0
 > Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9)
 > Internet Protocol Version 4, Src: 192.168.1.72, Dst: 192.168.1.254
 > User Datagram Protocol, Src Port: 57881, Dst Port: 53
 > Domain Name System (query)

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.afiliias-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 143.127.102.125
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.afiliias-nst.info						
1609	48.347989	192.168.1.72	192.168.1.254	DNS	81	Standard query 0xa002 A wireesharktraining.com
1611	48.455103	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0xa002 A wireesharktraining.com A 98.136.187.13
A wireesharktraining.com A 98.136.187.13						
1621	48.629120	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x6cf6 A wireesharktraining.com
1622	48.629476	192.168.1.254	192.168.1.72	DNS	84	Standard query 0x7f43 A ratings-wrs.symantec.com
1623	48.652928	192.168.1.72	192.168.1.254	DNS	97	Standard query response 0x6cf6 A wireesharktraining.com A 98.136.187.13
A wireesharktraining.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 143.127.102.125
wrs.symantec.com CNAME ratings-wrs.symantec.com.ntn.symantec.com A 143.127.102.125						
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.gyl.b.yahoodns.net CNAME ds-fo-anyycs-l.gyl.b.yahoodns.net A 206.190.60.138
geoycs-l.gyl.b.yahoodns.net CNAME ds-fo-anyycs-l.gyl.b.yahoodns.net A 206.190.60.138						
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 98.139.206.151
A visit.webhosting.yahoo.com CNAME pvisit1.geo.vip.bf1.yahoo.com A 98.139.206.151						
1852	49.445804	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x7d10 A www.wireesharkbook.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.wireesharkbook.com A 207.56.173.2
A www.wireesharkbook.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 wireesharkbook.orge
2165	55.872993	192.168.1.254	192.168.1.72	DNS	153	Standard query response 0xa830 No such name
A wireesharkbook.orge SOA a.root-servers.net						
2166	55.880214	192.168.1.72	192.168.1.254	DNS	82	Standard query 0xeb99 A www.wireesharkbook.orge
2168	55.931154	192.168.1.254	192.168.1.72	DNS	157	Standard query response 0xeb99 No such name
A www.wireesharkbook.orge SOA a.root-servers.net						
2302	58.315084	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x66e0 A www.wireesharkbook.org
2303	58.347961	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x66e0 A www.wireesharkbook.org A 207.56.173.2
A www.wireesharkbook.org A 207.56.173.2						
2322	58.567625	192.168.1.72	192.168.1.254	DNS	81	Standard query 0x4f89 A www.wireesharkbook.org
2324	58.591925	192.168.1.254	192.168.1.72	DNS	97	Standard query response 0x4f89 A www.wireesharkbook.org A 207.56.173.2
A www.wireesharkbook.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
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 symantec.georedirector.akadns.net CNAME a568.d.akamai.net CNAME user-att-107-219-144-0.a568.d.akamai.net A 23.72.181.96 A 23.72.181.129 A 23.72.181.90 A 23.72.181.51 A 23.72.181.114 A 23.72.181.56

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

DNS queries utilize UDP protocol encapsulated within an IP datagram¹⁴.

- c. What is the response for the DNS query for packet number 1004? What is the reason for this response?
- Standard query message for packet 1004: 0x4214
 - Query response: 0x4214 No such name

The response is given if the domain name wasn't found. In this scenario, this is because the domain was misspelt as www.wireeshark.org with 2 e's rather than www.wireshark.org.

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.afillias-nst.info

¹⁴ Kurose & Rose, page 131