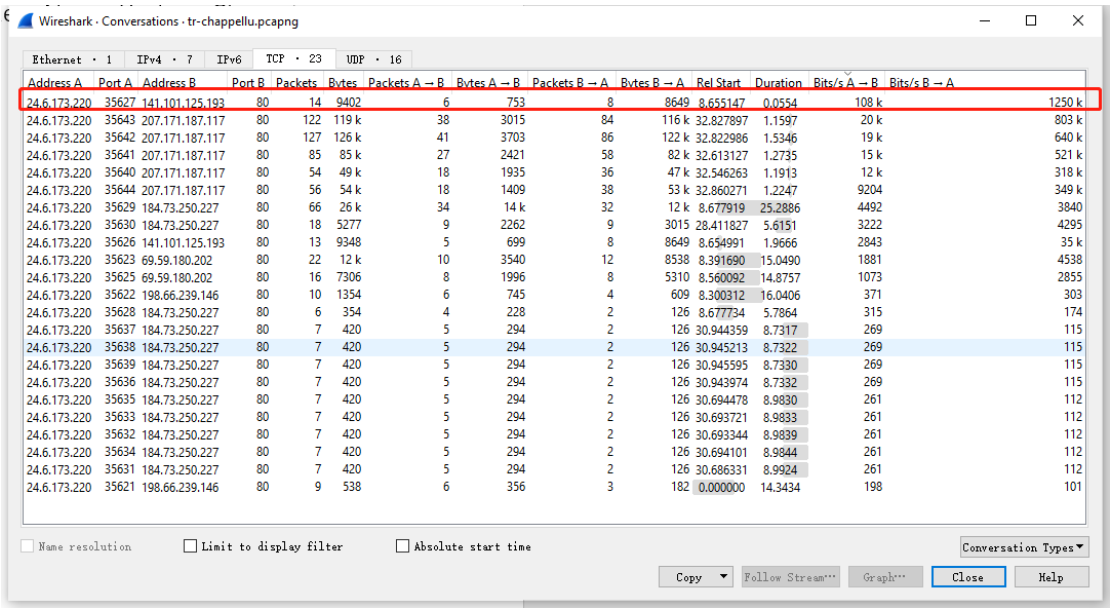
Assignment 1: Wireshark Fundamentals

Part 1

a.



Wireshark · Conversations · tr-chappellu.pcapng

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	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	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	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	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	35630	184.73.250.227	80	18	5277	9	2262	9	3015	28.411827	5.6151	3222	4295
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	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

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream... | Graph... | Close | Help

The red highlighted entry is the most active TCP conversation in the file by selecting filter descending from A to B

a-b with speed 108 k bit/s
b-a with speed 1250k bit/s
total/most active: 1358k Bits/s

b.

NetID: YC4909

Wireshark · Conversations · tr-chappellu.pcapng

Ethernet · 1 | IPv4 · 7 | IPv6 | TCP · 23 | UDP · 16

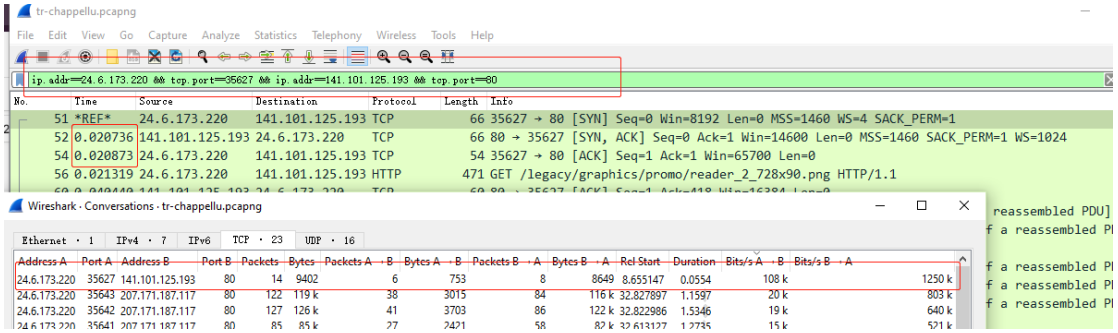
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B
24.6.173.220	35627	141.101.125.193	80	14	9402	6	753	8	8649	8.655147	0.0554	108 k	
24.6.173.220	35643	207.171.187.117	80	122	119 k	38	3015	84	116 k	32.827897	1.1597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

Name resolution | Limit to display filter | Absolute start time

After applying the filter, the most active conversation is the first entry in the table,.

Total byte is $753 + 8649 = 9402$ byte

c.

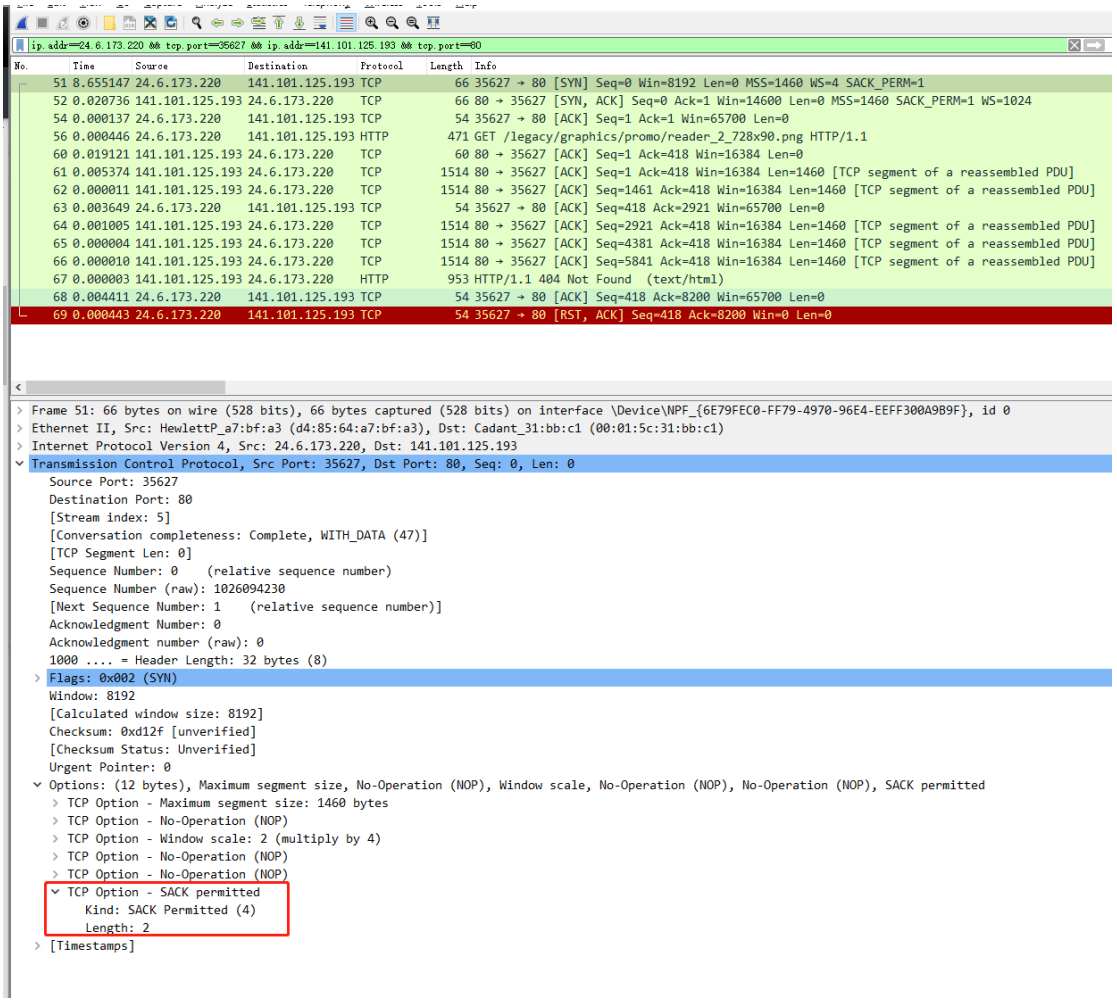


After find out the most active conversation, apply to filter
Set time reference
change time display format to “second since beginning capture.”
RTT is 0.020736s (Syn to Syn/Ack)
And 0.020873s (Syn to Syn/Ack to Ack)

d.

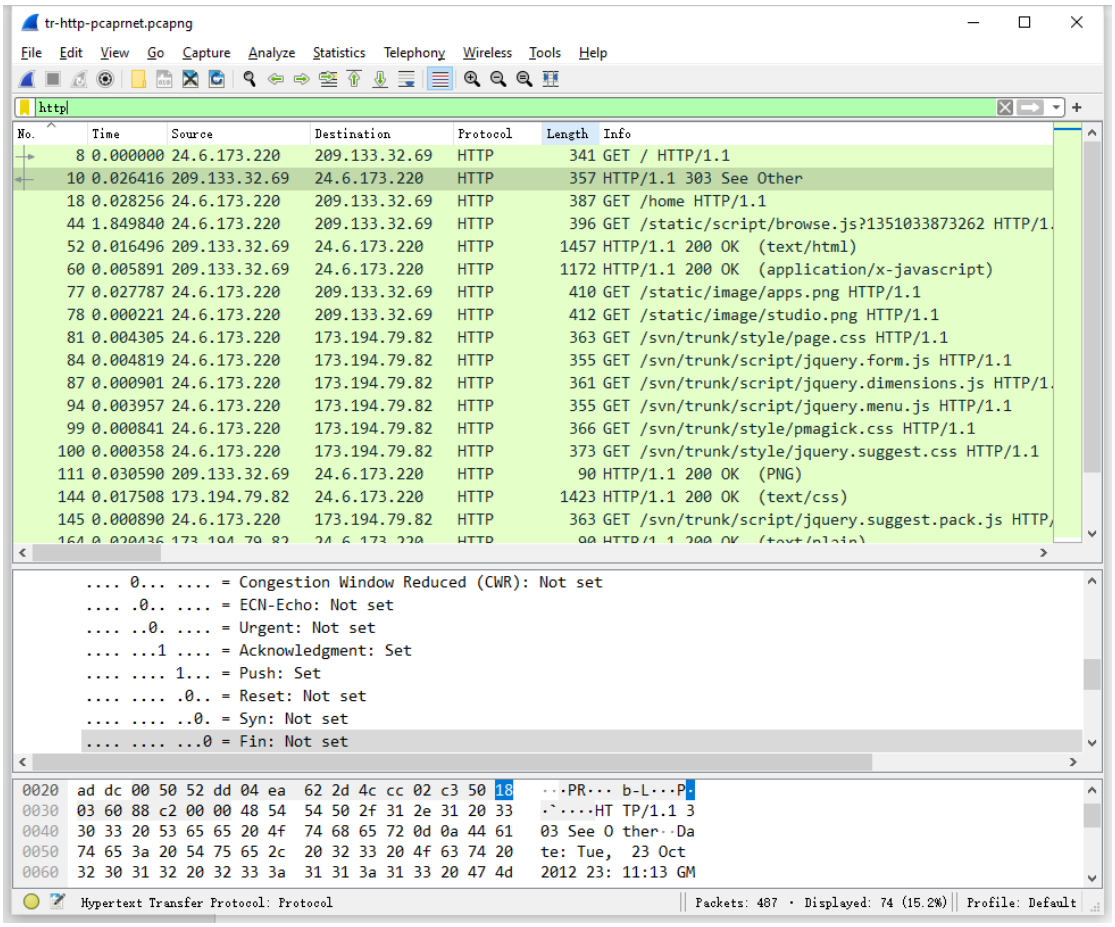
Selective Acknowledgment (SACK) is a strategy created to solve the problem for multiple dropped segments. With SACK, receiver can inform the sender what segments are received therefore the sender will be informed and start to resent the lost segments.

And Yes, it's permitted in the most active conversation.



Part 2

a.

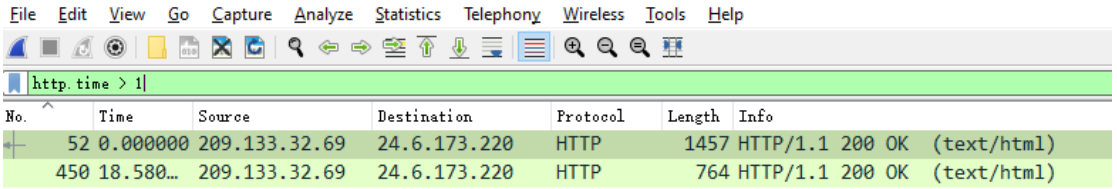

tr-http-pcaprnet.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
8 0.000000 24.6.173.220 209.133.32.69 HTTP 341 GET / HTTP/1.1
10 0.026416 209.133.32.69 24.6.173.220 HTTP 357 HTTP/1.1 303 See Other
18 0.028256 24.6.173.220 209.133.32.69 HTTP 387 GET /home HTTP/1.1
44 1.849840 24.6.173.220 209.133.32.69 HTTP 396 GET /static/script/browse.js?1351033873262 HTTP/1.
52 0.016496 209.133.32.69 24.6.173.220 HTTP 1457 HTTP/1.1 200 OK (text/html)
60 0.005891 209.133.32.69 24.6.173.220 HTTP 1172 HTTP/1.1 200 OK (application/x-javascript)
77 0.027787 24.6.173.220 209.133.32.69 HTTP 410 GET /static/image/apps.png HTTP/1.1
78 0.000221 24.6.173.220 209.133.32.69 HTTP 412 GET /static/image/studio.png HTTP/1.1
81 0.004305 24.6.173.220 173.194.79.82 HTTP 363 GET /svn/trunk/style/page.css HTTP/1.1
84 0.004819 24.6.173.220 173.194.79.82 HTTP 355 GET /svn/trunk/script/jquery.form.js HTTP/1.1
87 0.000901 24.6.173.220 173.194.79.82 HTTP 361 GET /svn/trunk/script/jquery.dimensions.js HTTP/1.
94 0.003957 24.6.173.220 173.194.79.82 HTTP 355 GET /svn/trunk/script/jquery.menu.js HTTP/1.1
99 0.000841 24.6.173.220 173.194.79.82 HTTP 366 GET /svn/trunk/style/pmagick.css HTTP/1.1
100 0.000358 24.6.173.220 173.194.79.82 HTTP 373 GET /svn/trunk/style/jquery.suggest.css HTTP/1.1
111 0.030590 209.133.32.69 24.6.173.220 HTTP 90 HTTP/1.1 200 OK (PNG)
144 0.017508 173.194.79.82 24.6.173.220 HTTP 1423 HTTP/1.1 200 OK (text/css)
145 0.000890 24.6.173.220 173.194.79.82 HTTP 363 GET /svn/trunk/script/jquery.suggest.pack.js HTTP/
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
0020 ad dc 00 50 52 dd 04 ea 62 2d 4c cc 02 c3 50 18 ···PR··· b-L···P·
0030 03 60 88 c2 00 00 48 54 54 50 2f 31 2e 31 20 33 ·`····HT TP/1.1 3
0040 30 33 20 53 65 65 20 4f 74 68 65 72 0d 0a 44 61 03 See O ther··Da
0050 74 65 3a 20 54 75 65 2c 20 32 33 20 4f 63 74 20 te: Tue, 23 Oct
0060 32 30 31 32 20 32 33 3a 31 31 3a 31 33 20 47 4d 2012 23: 11:13 GM
Hypertext Transfer Protocol: Protocol
Packets: 487 · Displayed: 74 (15.2%)
Profile: Default

b.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	209.133.32.69	24.6.173.220	HTTP	357	HTTP/1.1 303 See Other
52	1.894592	209.133.32.69	24.6.173.220	HTTP	1457	HTTP/1.1 200 OK (text/html)
60	0.005891	209.133.32.69	24.6.173.220	HTTP	1172	HTTP/1.1 200 OK (application/x-javascript)
111	0.073779	209.133.32.69	24.6.173.220	HTTP	90	HTTP/1.1 200 OK (PNG)
144	0.017508	173.194.79.82	24.6.173.220	HTTP	1423	HTTP/1.1 200 OK (text/css)
164	0.021326	173.194.79.82	24.6.173.220	HTTP	90	HTTP/1.1 200 OK (text/plain)
165	0.000002	173.194.79.82	24.6.173.220	HTTP	750	HTTP/1.1 200 OK (text/css)
185	0.006844	173.194.79.82	24.6.173.220	HTTP	1391	HTTP/1.1 200 OK (text/css)
202	0.005311	173.194.79.82	24.6.173.220	HTTP	850	HTTP/1.1 200 OK (text/plain)
213	0.013052	173.194.79.82	24.6.173.220	HTTP	74	HTTP/1.1 200 OK (text/plain)
217	0.018109	173.194.79.82	24.6.173.220	HTTP	472	HTTP/1.1 200 OK (text/plain)
229	0.017477	173.194.79.82	24.6.173.220	HTTP	96	HTTP/1.1 200 OK
233	0.001051	173.194.79.82	24.6.173.220	HTTP	524	HTTP/1.1 200 OK
246	0.011890	209.133.32.69	24.6.173.220	HTTP	500	HTTP/1.1 200 OK (PNG)
252	0.008247	173.194.79.82	24.6.173.220	HTTP	526	HTTP/1.1 200 OK
257	0.014255	173.194.79.82	24.6.173.220	HTTP	1171	HTTP/1.1 200 OK
260	0.001008	173.194.79.82	24.6.173.220	HTTP	893	HTTP/1.1 200 OK
264	0.004740	173.194.79.82	24.6.173.220	HTTP	1265	HTTP/1.1 200 OK
267	0.003922	173.194.79.82	24.6.173.220	HTTP	554	HTTP/1.1 200 OK
270	0.000976	173.194.79.82	24.6.173.220	HTTP	770	HTTP/1.1 200 OK
275	0.015879	173.194.79.82	24.6.173.220	HTTP	1156	HTTP/1.1 200 OK
285	0.015856	173.194.79.82	24.6.173.220	HTTP	1072	HTTP/1.1 200 OK
291	0.005978	173.194.79.82	24.6.173.220	HTTP	1290	HTTP/1.1 200 OK
300	0.023501	184.85.97.107	24.6.173.220	HTTP	315	HTTP/1.1 200 OK (application/x-javascript)
306	0.062243	184.85.97.107	24.6.173.220	HTTP	1247	HTTP/1.1 200 OK (PNG)
327	0.028524	173.194.79.82	24.6.173.220	HTTP	1120	HTTP/1.1 200 OK
330	0.001224	173.194.79.82	24.6.173.220	HTTP	799	HTTP/1.1 200 OK
347	0.010756	173.194.79.82	24.6.173.220	HTTP	75	HTTP/1.1 200 OK
412	10.909…	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)
427	5.894745	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)
450	1.386918	209.133.32.69	24.6.173.220	HTTP	764	HTTP/1.1 200 OK (text/html)
460	0.049336	209.133.32.69	24.6.173.220	HTTP	171	HTTP/1.1 304 Not Modified
467	0.033683	173.194.79.82	24.6.173.220	HTTP	492	HTTP/1.1 200 OK
472	0.060336	173.194.79.82	24.6.173.220	HTTP	1028	HTTP/1.1 200 OK
473	0.001666	173.194.79.82	24.6.173.220	HTTP	484	HTTP/1.1 200 OK
474	0.000003	173.194.79.82	24.6.173.220	HTTP	917	HTTP/1.1 200 OK
483	2.162666	209.133.32.69	24.6.173.220	HTTP	1173	HTTP/1.1 200 OK (text/html)

1. **303 see other**: The response to the request can be found under another URI using the GET method. When received in response to a POST (or PUT/DELETE), the client should presume that the server has received the data and should issue a new GET request to the given URI.
2. **200 ok** : Standard response for successful HTTP requests. The actual response will depend on the request method used. In a GET request, the response will contain an entity corresponding to the requested resource. In a POST request, the response will contain an entity describing or containing the result of the action
3. **304 not modify**: indicates that the resource has not been modified since the version specified by the request headers If-Modified-Since or If-None-Match. In such case, there is no need to retransmit the resource since the client still has a previously downloaded copy

c.



No.	Time	Source	Destination	Protocol	Length	Info
52	0.000000	209.133.32.69	24.6.173.220	HTTP	1457	HTTP/1.1 200 OK (text/html)
450	18.580…	209.133.32.69	24.6.173.220	HTTP	764	HTTP/1.1 200 OK (text/html)

Part 3

a.

ftp.request || ftp.response

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	14.371…	192.168.1.72	78.41.115.130	FTP	65	Request: USER fred
7	14.576…	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
9	23.202…	192.168.1.72	78.41.115.130	FTP	66	Request: USER marty
10	23.391…	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
12	27.722…	192.168.1.72	78.41.115.130	FTP	60	Request: QUIT
13	27.910…	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.

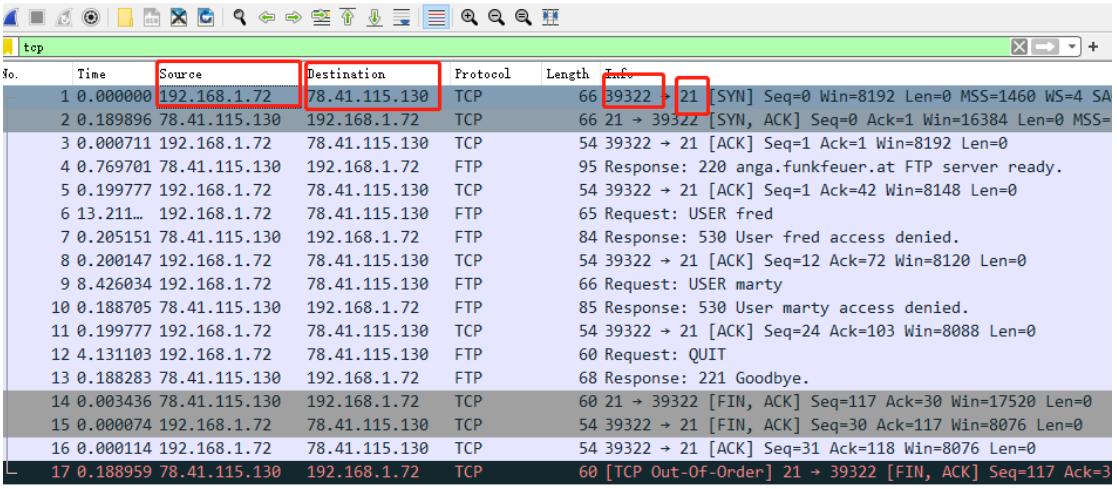
b.

client ip: 192.168.1.72

server ip: 78.41.115.130

client port: 39322

server port: 21



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.72	78.41.115.130	TCP	66	39322 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA
2	0.189896	78.41.115.130	192.168.1.72	TCP	66	21 → 39322 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=
3	0.000711	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.769701	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
5	0.199777	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [ACK] Seq=1 Ack=42 Win=8148 Len=0
6	13.211…	192.168.1.72	78.41.115.130	FTP	65	Request: USER fred
7	0.205151	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
8	0.200147	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [ACK] Seq=12 Ack=72 Win=8120 Len=0
9	8.426034	192.168.1.72	78.41.115.130	FTP	66	Request: USER marty
10	0.188705	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
11	0.199777	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [ACK] Seq=24 Ack=103 Win=8088 Len=0
12	4.131103	192.168.1.72	78.41.115.130	FTP	60	Request: QUIT
13	0.188283	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.
14	0.003436	78.41.115.130	192.168.1.72	TCP	60	21 → 39322 [FIN, ACK] Seq=117 Ack=30 Win=17520 Len=0
15	0.000074	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [FIN, ACK] Seq=30 Ack=117 Win=8076 Len=0
16	0.000114	192.168.1.72	78.41.115.130	TCP	54	39322 → 21 [ACK] Seq=31 Ack=118 Win=8076 Len=0
17	0.188959	78.41.115.130	192.168.1.72	TCP	60	[TCP Out-Of-Order] 21 → 39322 [FIN, ACK] Seq=117 Ack=3

c.

ftp.response.code

	Time	Source	Destination	Protocol	Length	Info
4	0.000000	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
7	13.616…	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
10	8.814886	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
13	4.519163	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.

1. **220 server ready** : A 220 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. It can also be sent in response to a REIN command, which is meant to reset the connection to the moment the client first connected to the server.
2. **530 access denied** : A 530 response code can be sent in response to any command that requires a user to log in before the command is processed. It is a permanent negative response, which means the client is discouraged from sending the command again before logging in since the server will respond with the same response code.
3. **221 goodbye** : A 221 code is sent over the control connection in response to the client's QUIT command. It is sent immediately before the control connection is closed by the server.

d.
the FTP termination is initiated by client.

e.

FTP was a protocol that was not built to be secure. As it relies on clear-text usernames and passwords for authentication and does not use encryption. Therefore, data sent via FTP is vulnerable to sniffing.

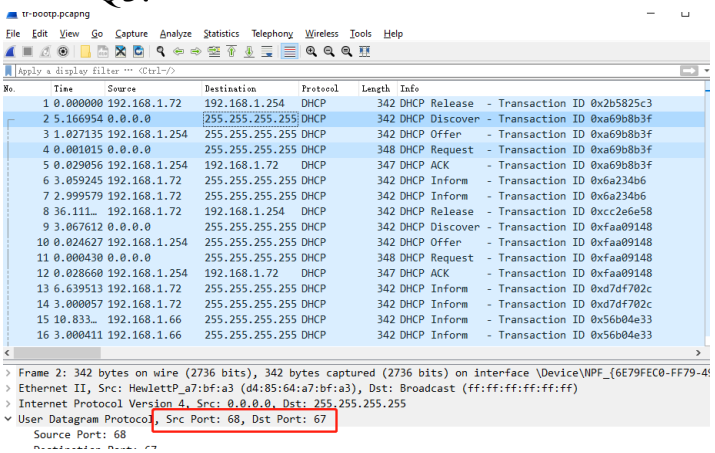
Part 4

a.

Q1: In Layer 2

Q2: broadcast packet

Q3:



before assigning the ip address

Source ip: 0.0.0.0

Destination ip: 255.255.255.255

Src port: 68

Dst port: 67

After assigning the ip address

Destination/Client ip: 192.168.1.72

Source/Server ip: 192.168.1.254

Destination/Client port: 68

Source/Server port: 67

b.
Q1: 3 packets
there are 4 packets are exchanged between the client and server in a DHCP handshake. They are discover, offer, request, and acknowledgment (Ack). Ack packet contain the IP address for clients so there are 3 packets before
the client receives an IP address.

Q2:
DHCPDISCOVER:
This message is generated by Client host to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server.
DHCPOFFER:
The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.
DHCPREQUEST:
When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address. A Client ID is also added in this message.
DHCPACK: DHCP Acknowledgement
In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

c.

when client doesn’t need the IP address, it will automatically send DHCP release packet to server to release IP address and cancel any remaining lease time.

d.

the process is quiet similar to normal 1 client 1 DHCP handshake.

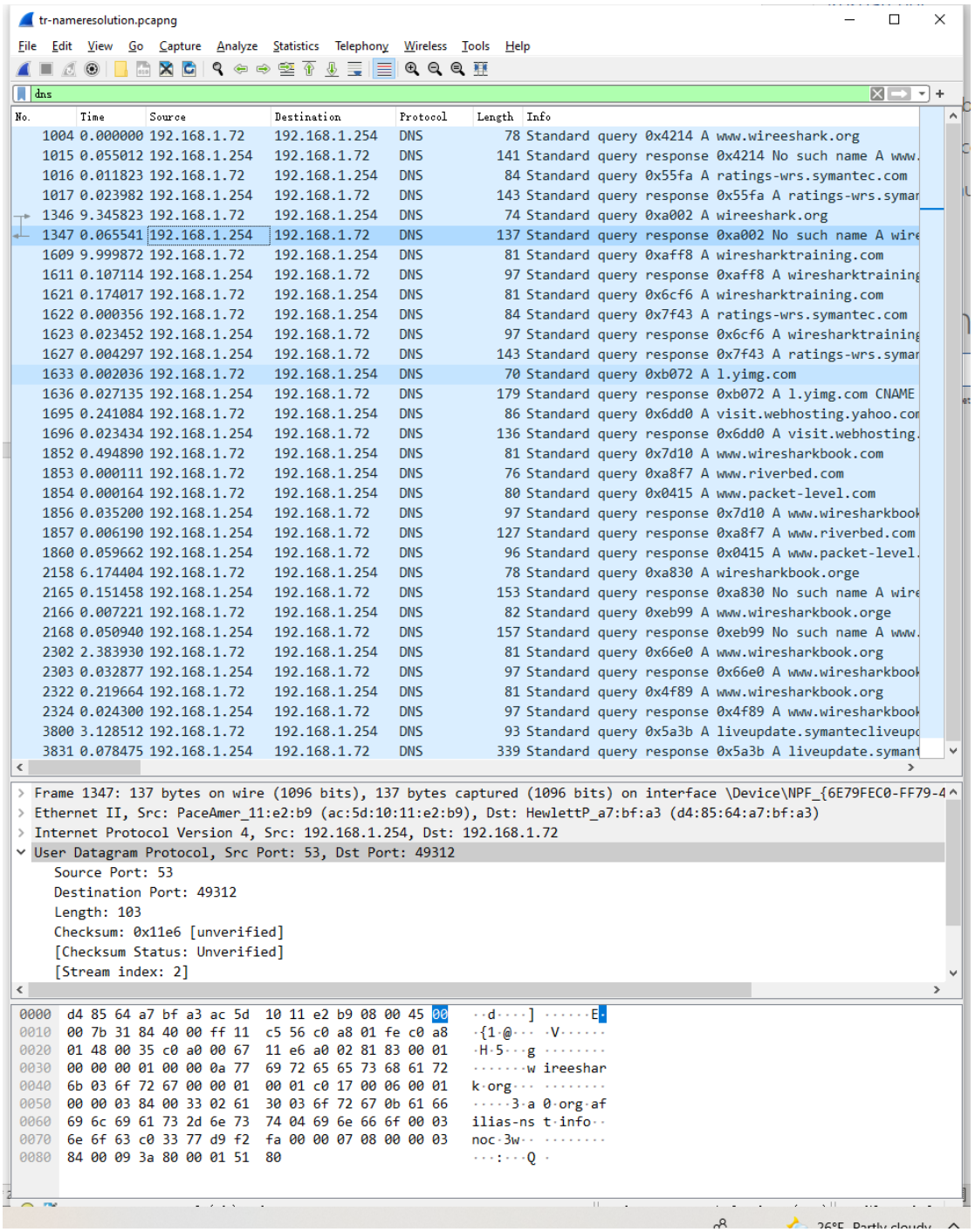
First, the client will broadcast DHCPDISCOVER, both DHCP server(1 and 2) received will send back DHCPOFFER packets (2 packets here)

Then, the client received the DHCPOFFER and reply to the DHCP server(assume server 1 first here) with DHCPREQUEST. DHCP server received DHCPREQUEST will broadcast DHCPACK so the client will know it's own ip addr assigned by the DHCP server, and the other DHCP server(server 2) will know that the client's ip addr and the client doesn't take DHCPOFFER from server 2.

Finally, DHCP server 2 will take back the ip address it gives to the client in DHCPOFFER

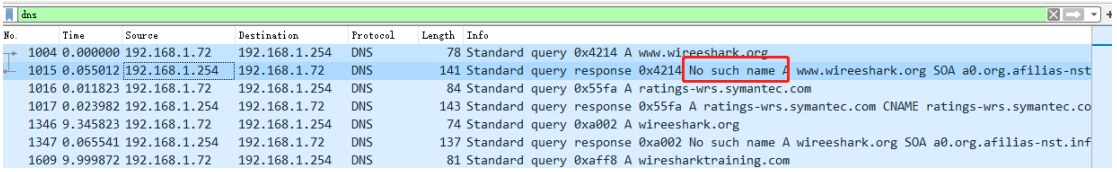
Part 5

a.


tr-nameresolution.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1004 0.000000 192.168.1.72 192.168.1.254 DNS 78 Standard query 0x4214 A www.wireeshark.org
1015 0.055012 192.168.1.254 192.168.1.72 DNS 141 Standard query response 0x4214 No such name A www.
1016 0.011823 192.168.1.72 192.168.1.254 DNS 84 Standard query 0x55fa A ratings-wrs.symantec.com
1017 0.023982 192.168.1.254 192.168.1.72 DNS 143 Standard query response 0x55fa A ratings-wrs.symar
1346 9.345823 192.168.1.72 192.168.1.254 DNS 74 Standard query 0xa002 A wireeshark.org
1347 0.065541 192.168.1.254 192.168.1.72 DNS 137 Standard query response 0xa002 No such name A wire
1609 9.999872 192.168.1.72 192.168.1.254 DNS 81 Standard query 0xaff8 A wiresharktraining.com
1611 0.107114 192.168.1.254 192.168.1.72 DNS 97 Standard query response 0xaff8 A wiresharktraining
1621 0.174017 192.168.1.72 192.168.1.254 DNS 81 Standard query 0x6cf6 A wiresharktraining.com
1622 0.000356 192.168.1.72 192.168.1.254 DNS 84 Standard query 0x7f43 A ratings-wrs.symantec.com
1623 0.023452 192.168.1.254 192.168.1.72 DNS 97 Standard query response 0x6cf6 A wiresharktraining
1627 0.004297 192.168.1.254 192.168.1.72 DNS 143 Standard query response 0x7f43 A ratings-wrs.symar
1633 0.002036 192.168.1.72 192.168.1.254 DNS 70 Standard query 0xb072 A l.yimg.com
1636 0.027135 192.168.1.254 192.168.1.72 DNS 179 Standard query response 0xb072 A l.yimg.com CNAME
1695 0.241084 192.168.1.72 192.168.1.254 DNS 86 Standard query 0x6dd0 A visit.webhosting.yahoo.com
1696 0.023434 192.168.1.254 192.168.1.72 DNS 136 Standard query response 0x6dd0 A visit.webhosting.
1852 0.494890 192.168.1.72 192.168.1.254 DNS 81 Standard query 0x7d10 A www.wiresharkbook.com
1853 0.000111 192.168.1.72 192.168.1.254 DNS 76 Standard query 0xa8f7 A www.riverbed.com
1854 0.000164 192.168.1.72 192.168.1.254 DNS 80 Standard query 0x0415 A www.packet-level.com
1856 0.035200 192.168.1.254 192.168.1.72 DNS 97 Standard query response 0x7d10 A www.wiresharkbook
1857 0.006190 192.168.1.254 192.168.1.72 DNS 127 Standard query response 0xa8f7 A www.riverbed.com
1860 0.059662 192.168.1.254 192.168.1.72 DNS 96 Standard query response 0x0415 A www.packet-level.
2158 6.174404 192.168.1.72 192.168.1.254 DNS 78 Standard query 0xa830 A wiresharkbook.orge
2165 0.151458 192.168.1.254 192.168.1.72 DNS 153 Standard query response 0xa830 No such name A wire
2166 0.007221 192.168.1.72 192.168.1.254 DNS 82 Standard query 0xeb99 A www.wiresharkbook.orge
2168 0.050940 192.168.1.254 192.168.1.72 DNS 157 Standard query response 0xeb99 No such name A www.
2302 2.383930 192.168.1.72 192.168.1.254 DNS 81 Standard query 0x66e0 A www.wiresharkbook.org
2303 0.032877 192.168.1.254 192.168.1.72 DNS 97 Standard query response 0x66e0 A www.wiresharkbook
2322 0.219664 192.168.1.72 192.168.1.254 DNS 81 Standard query 0x4f89 A www.wiresharkbook.org
2324 0.024300 192.168.1.254 192.168.1.72 DNS 97 Standard query response 0x4f89 A www.wiresharkbook
3800 3.128512 192.168.1.72 192.168.1.254 DNS 93 Standard query 0x5a3b A liveupdate.symantecliveupd
3831 0.078475 192.168.1.254 192.168.1.72 DNS 339 Standard query response 0x5a3b A liveupdate.symant
Frame 1347: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \Device\NPF_{6E79FEC0-FF79-4
Ethernet II, Src: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.72
User Datagram Protocol, Src Port: 53, Dst Port: 49312
Source Port: 53
Destination Port: 49312
Length: 103
Checksum: 0x11e6 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
0000 d4 85 64 a7 bf a3 ac 5d 10 11 e2 b9 08 00 45 00
0010 00 7b 31 84 40 00 ff 11 c5 56 c0 a8 01 fe c0 a8
0020 01 48 00 35 c0 a0 00 67 11 e6 a0 02 81 83 00 01
0030 00 00 00 01 00 00 0a 77 69 72 65 65 73 68 61 72
0040 6b 03 6f 72 67 00 00 01 00 01 c0 17 00 06 00 01
0050 00 00 03 84 00 33 02 61 30 03 6f 72 67 0b 61 66
0060 69 6c 69 61 73 2d 6e 73 74 04 69 6e 66 6f 00 03
0070 6e 6f 63 c0 33 77 d9 f2 fa 00 00 07 08 00 00 03
0080 84 00 09 3a 80 00 01 51 80

b.
User Datagram Protocol (UDP)

c.



dns

No.	Time	Source	Destination	Protocol	Length	Info
1004	0.000000	192.168.1.72	192.168.1.254	DNS	78	Standard query 0x4214 A www.wireeshark.org
1015	0.055012	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
1016	0.011823	192.168.1.72	192.168.1.254	DNS	84	Standard query 0x55fa A ratings-wrs.symantec.com
1017	0.023982	192.168.1.254	192.168.1.72	DNS	143	Standard query response 0x55fa A ratings-wrs.symantec.com CNAME ratings-wrs.symantec.co
1346	9.345823	192.168.1.72	192.168.1.254	DNS	74	Standard query 0xa002 A wireeshark.org
1347	0.065541	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.inf
1609	9.999872	192.168.1.72	192.168.1.254	DNS	81	Standard query 0xaff8 A wiresharktraining.com

The response is “no such name”
this code signifies that the domain name referenced in the query does not exist (www.wireesharks.org is not exist)