Assignment 1

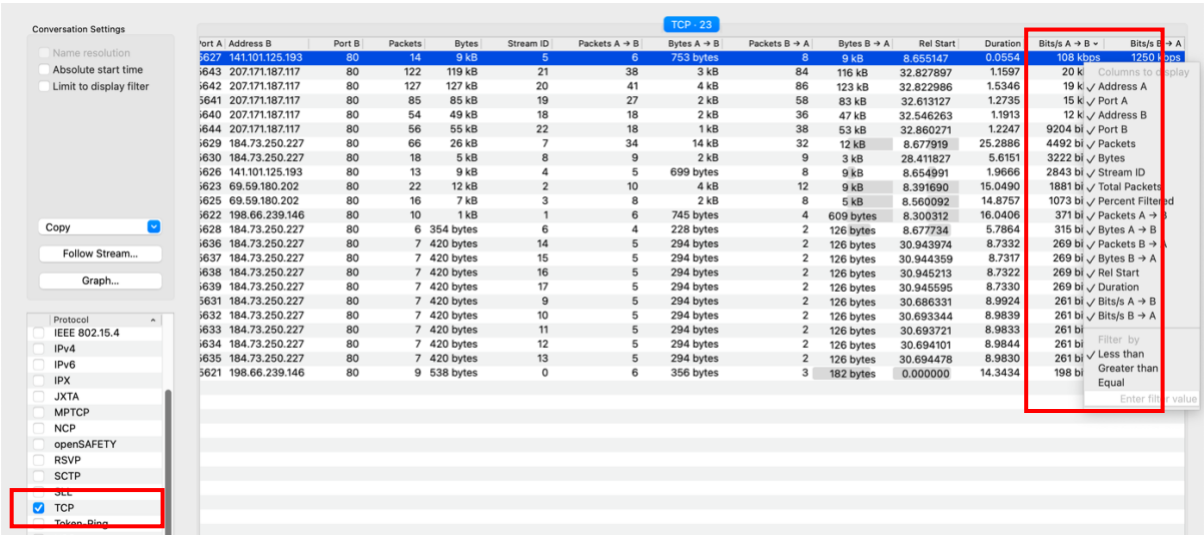
Wireshark Fundamentals

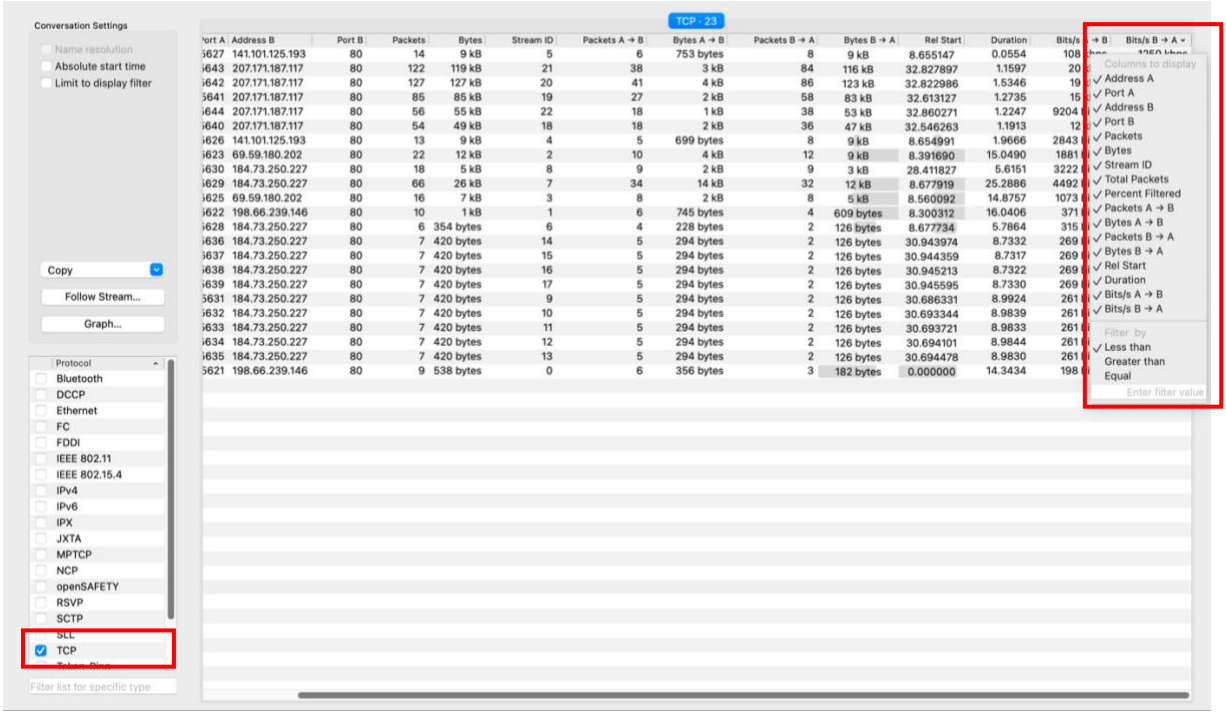
By Ziming Song
zs2815@nyu.edu

Part 1: tr-chappellu.pcapng

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

The most active TCP conversation is the first one marked as blue. The bits/s from A to B at 108kbps and the bits/s from B to A at 1250kbps.The filter method is marked with red boxes.

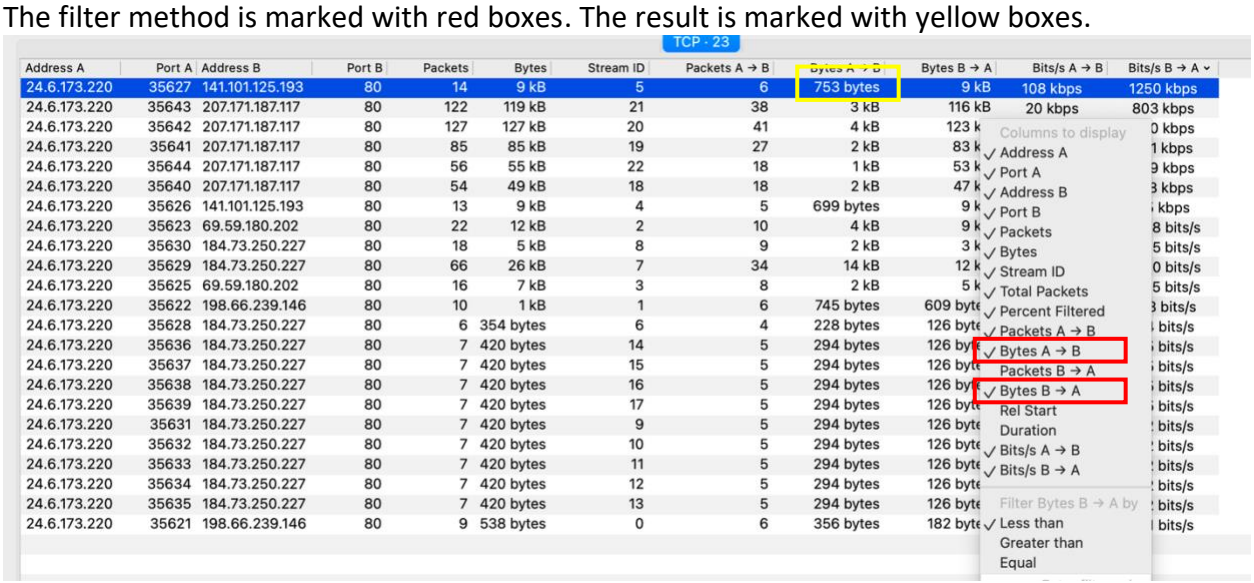




b. What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select Apply as Filter > Selected > A → B. Save the packets once the filter is applied)

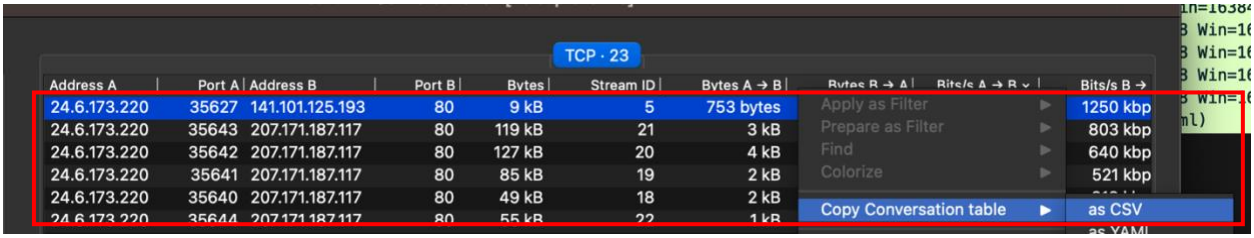
753 bytes transferred from A to B. *8649* bytes[1] transferred from B to A. For a total of 9402 bytes.[2]

The filter method is marked with red boxes. The result is marked with yellow boxes.



Get data in bytes:

[1] I got this result using method mentioned in this question on my Windows 11 computer. It is weird that I can only get '9k bytes' on my macOS computer.



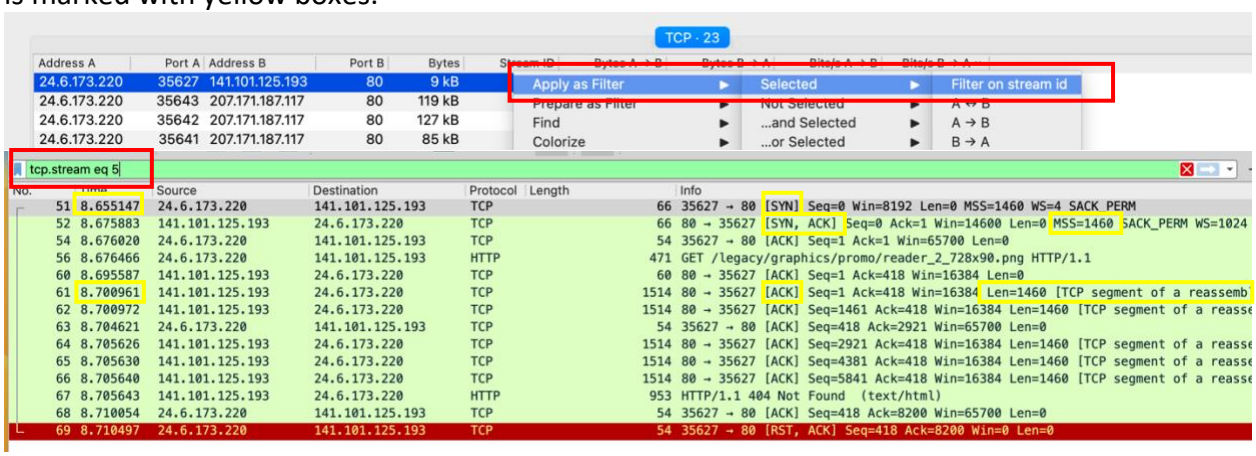
Related result on clipboard:

```
"24.6.173.220",35627,"141.101.125.193",80,14,9402,5,0,0,6,753,8,8649,8.655147,0.055350000000000676,108834,1250081
```

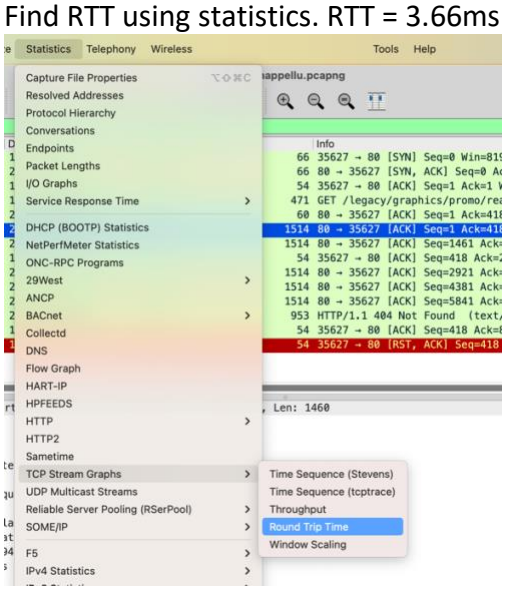
c. Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake.

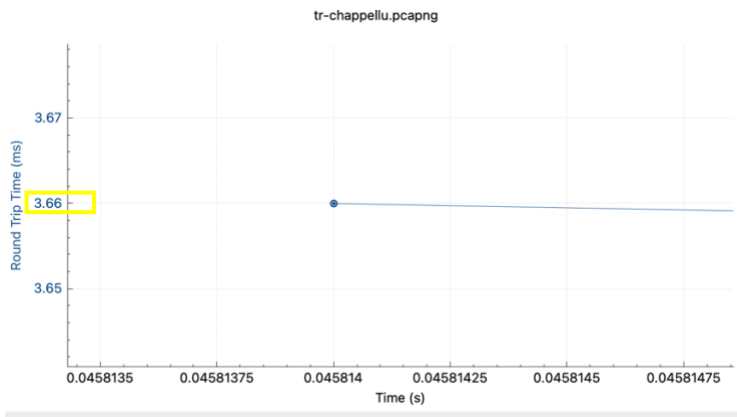
Take TCP conversation mentioned in Part1(a) as an example. [6]

1. Set Filter and see the result. The filter method is marked with red boxes. The result is marked with yellow boxes.



2. According to result in yellow boxes. Calculate time.
   time = 8.700961 – 8.655147 = 0.045814
3. Find RTT using statistics. RTT = 3.66ms

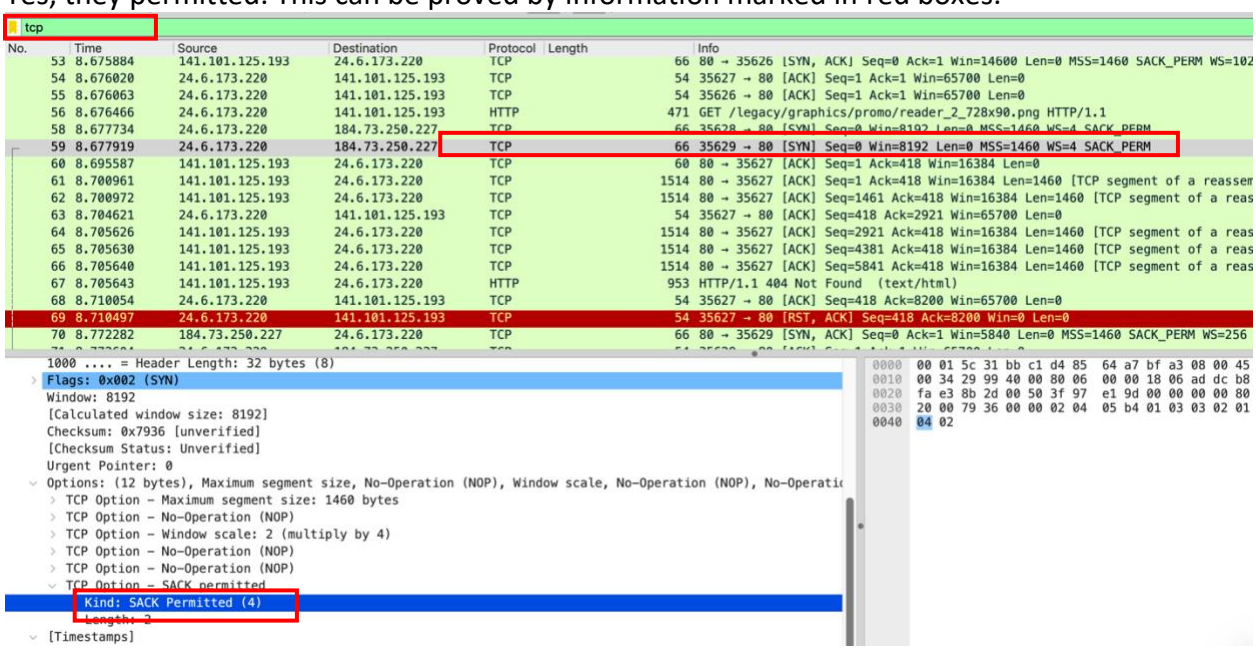




d. What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.

Selective acknowledgments is a sender and receiver side optimization to TCP. It is a mechanism that allows the sender to retransmit only what is missing at the receiver's end, so that the receiver can acknowledge non-consecutive data.[3]

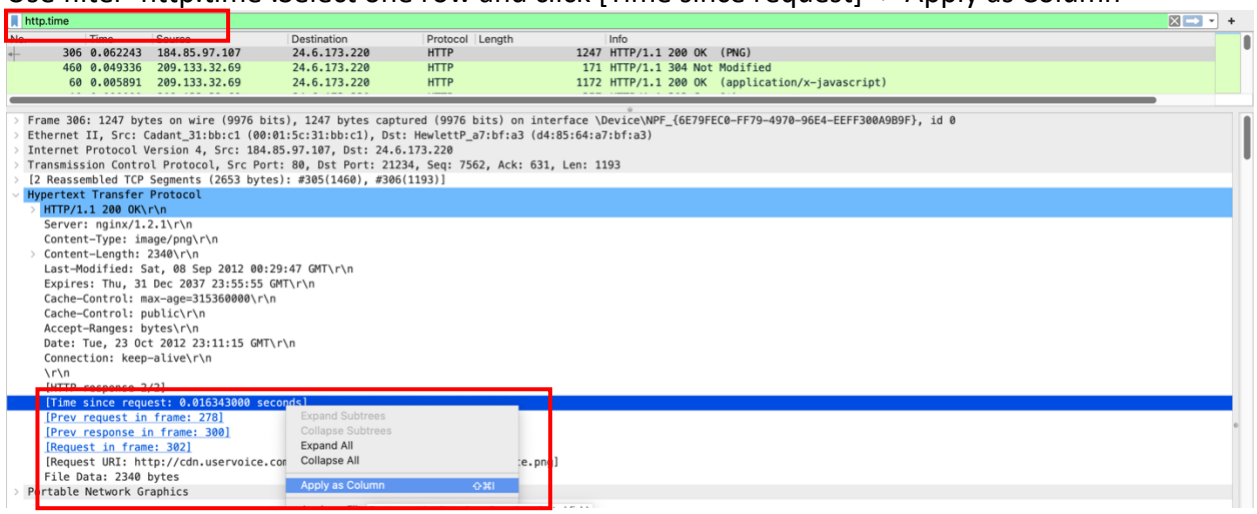
Yes, they permitted. This can be proved by information marked in red boxes.



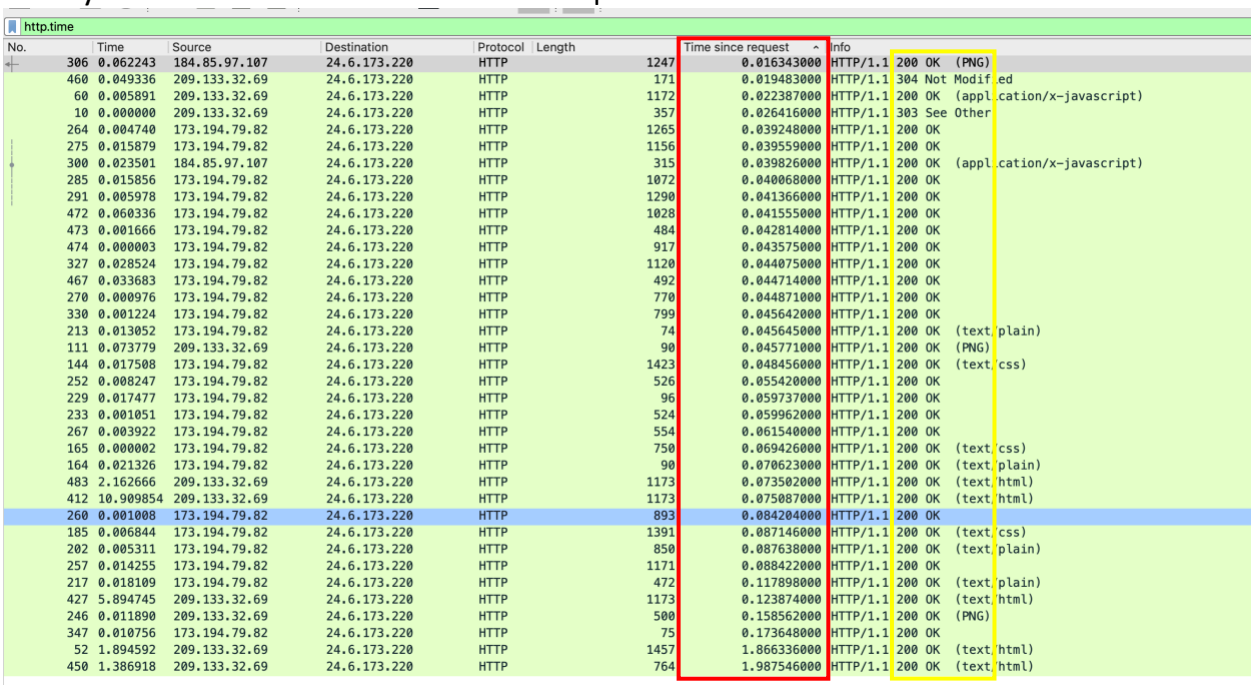
Part 2: tr-http-pcaprnet.pcapng

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

1. Use filter ‘http.time’.Select one row and click [Time since request] ->’Apply as Column’



2. Then you can see results in ‘Times since request’ column.



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

200 OK: The request succeeded.

303 See Other: The server sent this response to direct the client to get the requested resource at another URI with a GET request.

304 Not Modified: This is used for caching purposes. It tells the client that the response has not been modified, so the client can continue to use the same cached version of the response.[4]

Each HTTP response status code is marked in the picture in Part2(a) in yellow box.

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

Use filter ‘http.time>1’ based on Part2(a) [5]

http.time >1

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
52	0.000000	209.133.32.69	24.6.173.220	HTTP	1457	1.866336000	HTTP/1.1 200 OK (text/html)
450	18.580866	209.133.32.69	24.6.173.220	HTTP	764	1.987546000	HTTP/1.1 200 OK (text/html)

Part 3: tr-http-pcaprnet.pcapng

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

Use filter ‘ftp’

ftp

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.**

	IP address	Port number
server	78.41.115.130	21
client	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 codes.**

Use filter ‘ftp.response.code’

ftp.response.code

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.
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.

Select one row. Find Response Code, click ‘Apply as Column’

ftp.response.code

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.
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Response: 221 Goodbye.
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Response: 530 User marty access denied.
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.

```
> Frame 4: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0
> 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: 78.41.115.130, Dst: 192.168.1.72
> Transmission Control Protocol, Src Port: 21, Dst Port: 39322, Seq: 1, Ack: 1, Len: 41
v File Transfer Protocol (FTP)
  v 220 anga.funkfeuer.at FTP server ready.\r\n
      Response code: Service
      Response arg: anga.funk
  [Current working directory:
```

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column ⇧⌘I

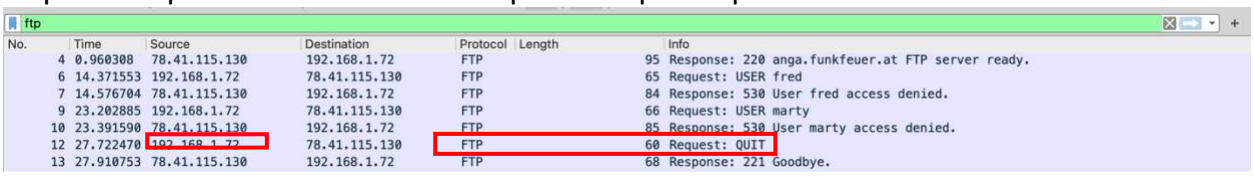
See the column ‘Response Code’ as a result.

ftp.response.code

No.	Time	Source	Destination	Protocol	Length	Response code	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP	95	Service ready for new user	Response: 220 anga.funkfeuer.at FTP server ready.
13	27.910753	78.41.115.130	192.168.1.72	FTP	68	Service closing control connection	Response: 221 Goodbye.
10	23.391590	78.41.115.130	192.168.1.72	FTP	85	Not logged in	Response: 530 User marty access denied.
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Not logged in	Response: 530 User fred access denied.

220 Service ready for new user: The server sent this code to a new user that the server is ready to connect new clients.
221 Goodbye: Service closing control connection
530 Not logged in: The code is sent to respond to requests/commands from user to log-in before commands is executed.

d. **Is the FTP termination initiated by server or client? Please justify your answer.**
FTP termination initiated by client according to the picture below. The client send request to quit first. Then server respond to quit request.



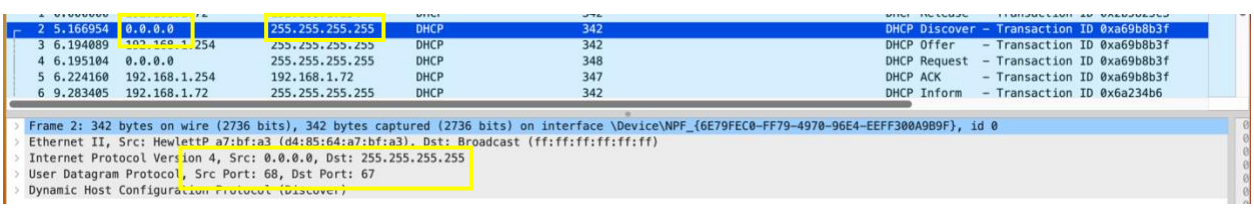
No.	Time	Source	Destination	Protocol	Length	Info
4	0.960308	78.41.115.130	192.168.1.72	FTP	95	Response: 220 anga.funkfeuer.at FTP server ready.
6	14.371553	192.168.1.72	78.41.115.130	FTP	65	Request: USER fred
7	14.576704	78.41.115.130	192.168.1.72	FTP	84	Response: 530 User fred access denied.
9	23.202885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

e. **How secure is FTP?**
FTP is not secure because it relies on plain text without encryption.

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.**
Application Layer.
DHCP Discover is UDP broadcast packet which source IP address is 0.0.0.0 and destination IP address is 255.255.255.255 or the specific subnet broadcast address.
For DHCP Discover:

	IP address	Port number
source	0.0.0.0	68
destination	255.255.255.255	67

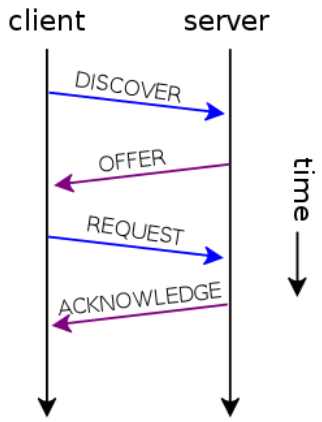


2	5.166954	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa69b8b3f
3	6.194089	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa69b8b3f
4	6.195104	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0xa69b8b3f
5	6.224160	192.168.1.254	192.168.1.72	DHCP	347	DHCP ACK - Transaction ID 0xa69b8b3f
6	9.283405	192.168.1.72	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6a234b6

```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 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 (Discover)
```

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.**

4 DHCP packets.
Discover: DHCP client broadcasts a DHCPDISCOVER message on the network subnet to discover DHCP available server.
Offer: DHCP server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client.
Request: DHCP client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address, in response to the DHCP offer.
ACK: DHCP server acknowledge the request, sending a DHCPACK packet with lease duration and other configuration information to the client.



c. **What is the significance of DHCP Release packet?**
DHCP Release packet is a message sent by a DHCP client to DHCP server to release IP address that was previously assigned to it. DHCP Release packet is significant because it allows the DHCP server to reclaim the IP address and make it available for other clients.

d. **Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.**
When a DHCP client sends a discover message requesting an IP address, both DHCP servers on the network receive the request. Client will use the first server to respond with an offer message. The client then sends a request message to the server which made the offer, indicating that it has accepted the offer. The server then sends an ACK message to the client, confirming that the IP address has been assigned.
Once the client has received ACK message with IP address, it will continue to use that address until its lease expires or it sends a release message.

Part 5: tr-bootp.pcapng

a. Use a filter to display DNS traffic only.

Use filter ‘dns’

dns

No.	Time	Source	Destination	Protocol	Length	Response code	Info
1…	28.845936	192.168.1.72	192.168.1.254	DNS	78		Standard query 0x4214 A www.wireeshark
1…	28.900948	192.168.1.254	192.168.1.72	DNS	141		Standard query response 0x4214 No such
1…	28.912771	192.168.1.72	192.168.1.254	DNS	84		Standard query 0x55fa A ratings-wrs.sy
1…	28.936753	192.168.1.254	192.168.1.72	DNS	143		Standard query response 0x55fa A ratin
1…	38.282576	192.168.1.72	192.168.1.254	DNS	74		Standard query 0xa002 A wireeshark.org
1…	38.348117	192.168.1.254	192.168.1.72	DNS	137		Standard query response 0xa002 No such
1…	48.347989	192.168.1.72	192.168.1.254	DNS	81		Standard query 0xaff8 A wiresharktrain
1…	48.455103	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0xaff8 A wires
1…	48.629120	192.168.1.72	192.168.1.254	DNS	81		Standard query 0x6cf6 A wiresharktrain
1…	48.629476	192.168.1.72	192.168.1.254	DNS	84		Standard query 0x7f43 A ratings-wrs.sy
1…	48.652928	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0x6cf6 A wires
1…	48.657225	192.168.1.254	192.168.1.72	DNS	143		Standard query response 0x7f43 A ratin
1…	48.659261	192.168.1.72	192.168.1.254	DNS	70		Standard query 0xb072 A l.yimg.com
1…	48.686396	192.168.1.254	192.168.1.72	DNS	179		Standard query response 0xb072 A l.yim
1…	48.927480	192.168.1.72	192.168.1.254	DNS	86		Standard query 0x6dd0 A visit.webhosti
1…	48.950914	192.168.1.254	192.168.1.72	DNS	136		Standard query response 0x6dd0 A visit
1…	49.445804	192.168.1.72	192.168.1.254	DNS	81		Standard query 0x7d10 A www.wiresharkb
1…	49.445915	192.168.1.72	192.168.1.254	DNS	76		Standard query 0xa8f7 A www.riverbed.c
1…	49.446079	192.168.1.72	192.168.1.254	DNS	80		Standard query 0x0415 A www.packet-lev
1…	49.481279	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0x7d10 A www.w
1…	49.487469	192.168.1.254	192.168.1.72	DNS	127		Standard query response 0xa8f7 A www.r
1…	49.547131	192.168.1.254	192.168.1.72	DNS	96		Standard query response 0x0415 A www.p
2…	55.721535	192.168.1.72	192.168.1.254	DNS	78		Standard query 0xa830 A wiresharkbook.
2…	55.872993	192.168.1.254	192.168.1.72	DNS	153		Standard query response 0xa830 No such
2…	55.880214	192.168.1.72	192.168.1.254	DNS	82		Standard query 0xeb99 A www.wiresharkb
2…	55.931154	192.168.1.254	192.168.1.72	DNS	157		Standard query response 0xeb99 No such
2…	58.315084	192.168.1.72	192.168.1.254	DNS	81		Standard query 0x66e0 A www.wiresharkb
2…	58.347961	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0x66e0 A www.w
2…	58.567625	192.168.1.72	192.168.1.254	DNS	81		Standard query 0x4f89 A www.wiresharkb
2…	58.591925	192.168.1.254	192.168.1.72	DNS	97		Standard query response 0x4f89 A www.w
3…	61.720437	192.168.1.72	192.168.1.254	DNS	93		Standard query 0x5a3b A liveupdate.sym

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

UDP

```
> Frame 1004: 78 bytes on wire (624 bits), 78 bytes captured (624 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: 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)
```

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

1004	28.845936	192.168.1.72	192.168.1.254	DNS	78	Standard query 0x4214 A www.wireeshark.org
1015	28.900948	192.168.1.254	192.168.1.72	DNS	141	Standard query response 0x4214 No such name A www.wireeshark.org SOA a0.org.afilias-n
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.
1346	38.282576	192.168.1.72	192.168.1.254	DNS	74	Standard query 0xa002 A wireeshark.org

```
> Frame 1004: 78 bytes on wire (624 bits), 78 bytes captured (624 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: 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
v Domain Name System (query)
    Transaction ID: 0x4214
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.wireeshark.org: type A, class IN
    [Response In: 1015]
```

Find response in 1015. The response is ‘no such name’. The reason is marked in the picture above. ‘No such name A www.wireeshark.org SOA a0.org.afilias-nst.info’.

Reference

[1] Wireshark User's Guide: Version 3.5.1

[2] https://ask.wireshark.org/question/14573/how-do-i-see-statisticsconversationsbytes-values-in-full-rather-than-abbreviated-as-n-k/

[3] https://www.geeksforgeeks.org/selective-acknowledgments-sack-in-tcp/

[4] https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

[5] https://www.youtube.com/watch?v=FMRI6ua2MjE

[6] Disscuss this Question with Jiaran Liu

[7] https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol