Assignment 1

Wireshark Fundamentals

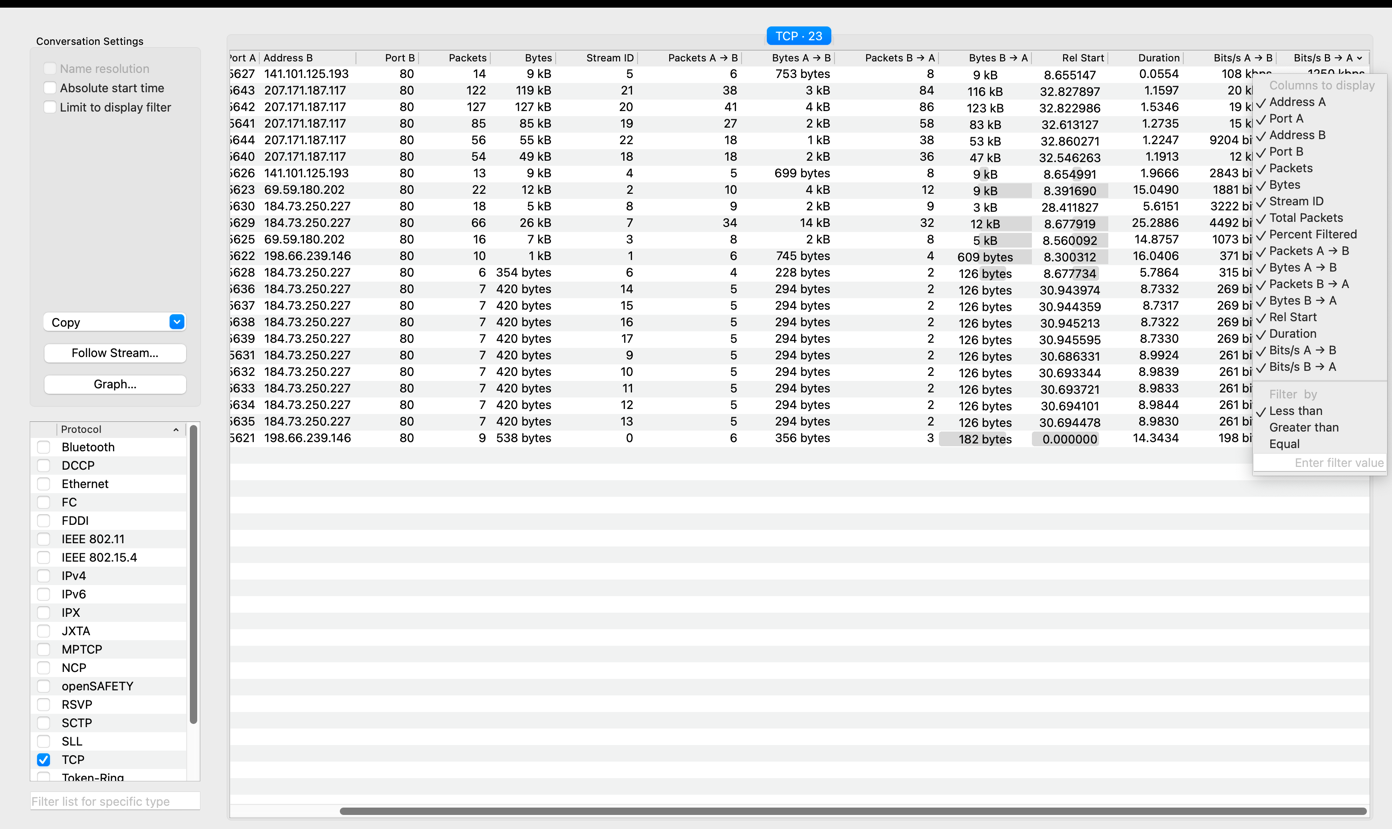
By Ziming Song

[zs2815@nyu.edu](mailto:zs2815@nyu.edu)

# **Part 1: tr-chappellu.pcapng**

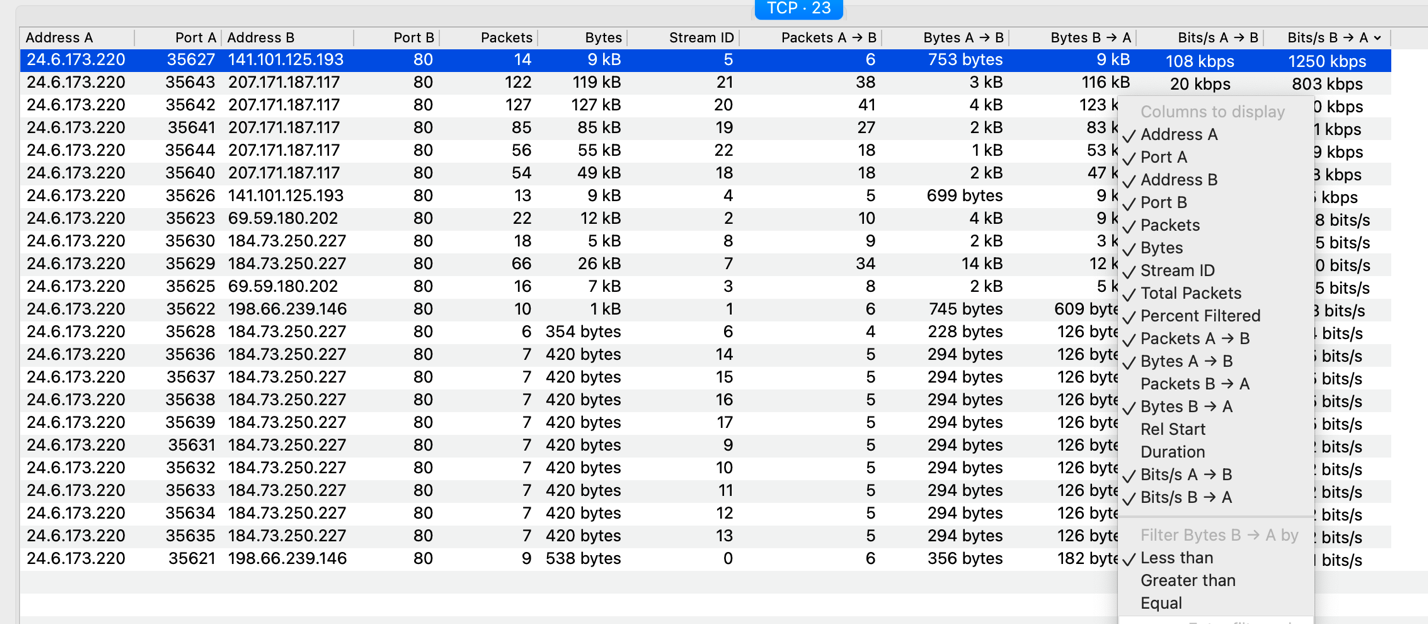
## **Find the most active TCP conversation in the file (by bits per second)**

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.

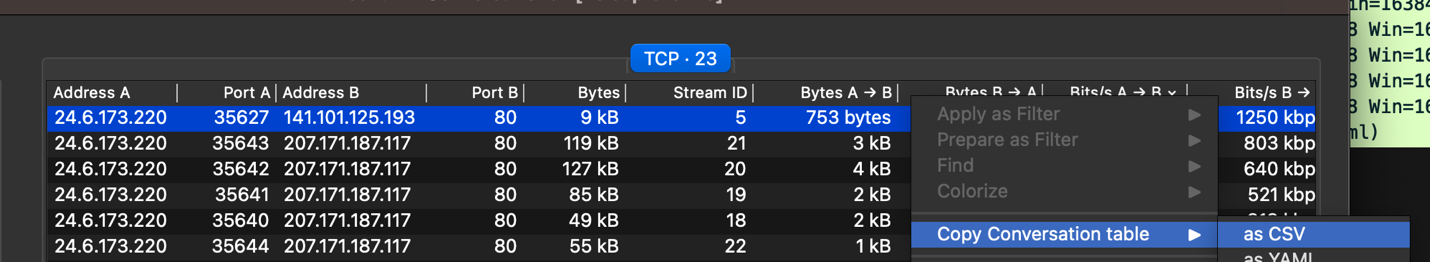


## **What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select Apply as Filter > Selected > A → B. Save the packets once the filter is applied)**

*753* bytes transferred from A to B. *8649* bytes[[1]](#footnote-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:

****

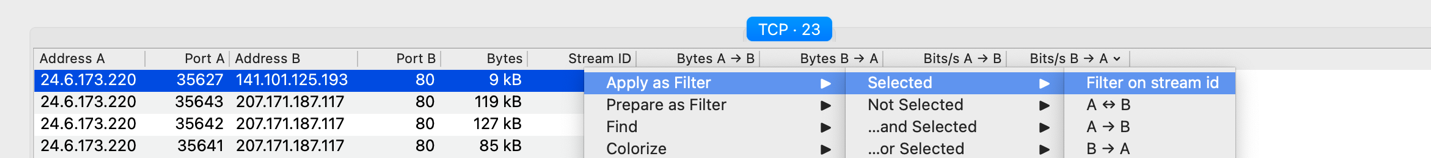
Related result on clipboard:

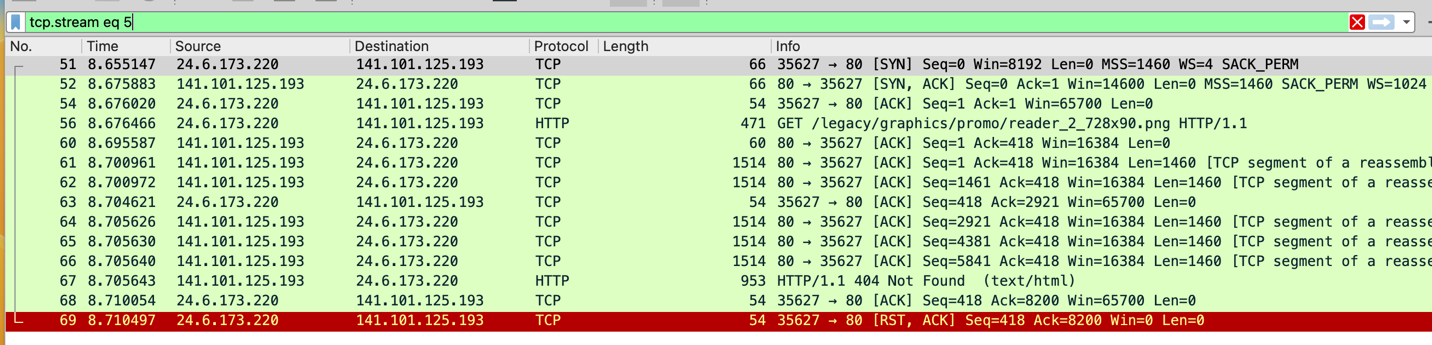
****

## **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]

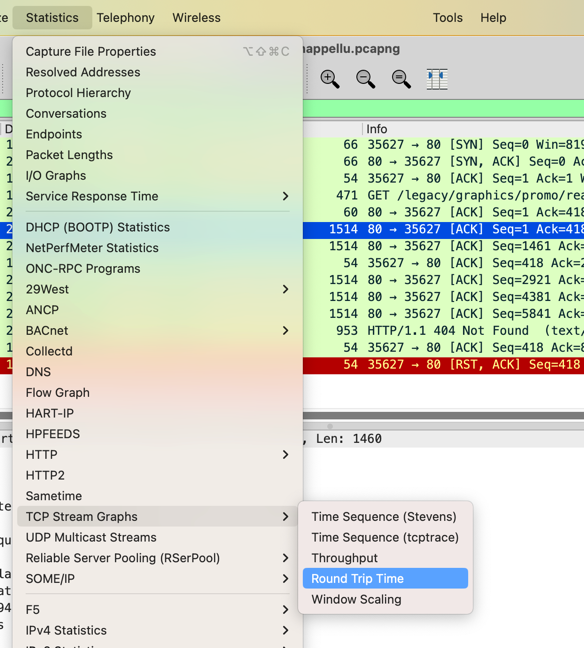
1. Set Filter and see the result. The filter method is marked with red boxes. The result is marked with yellow boxes. 

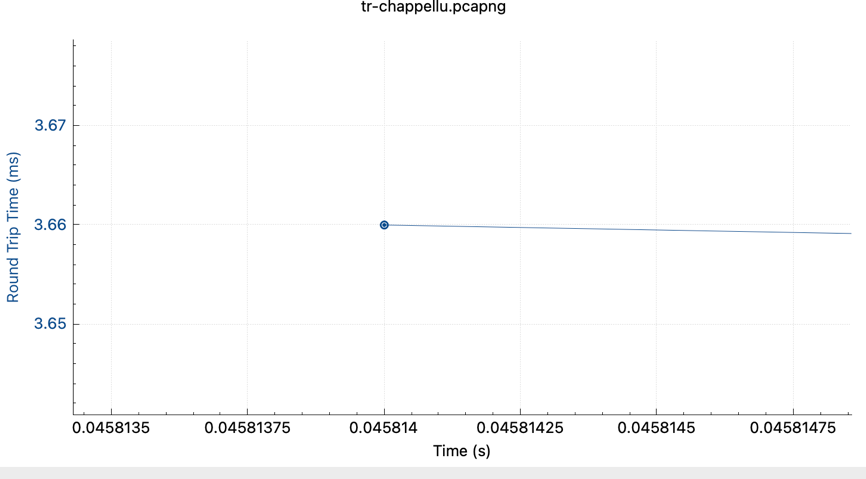


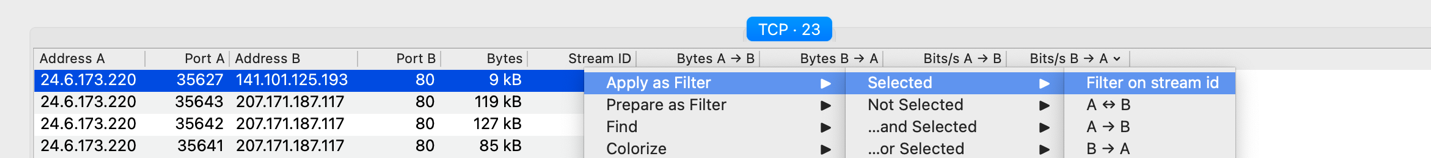
1. According to result in yellow boxes. Calculate time.

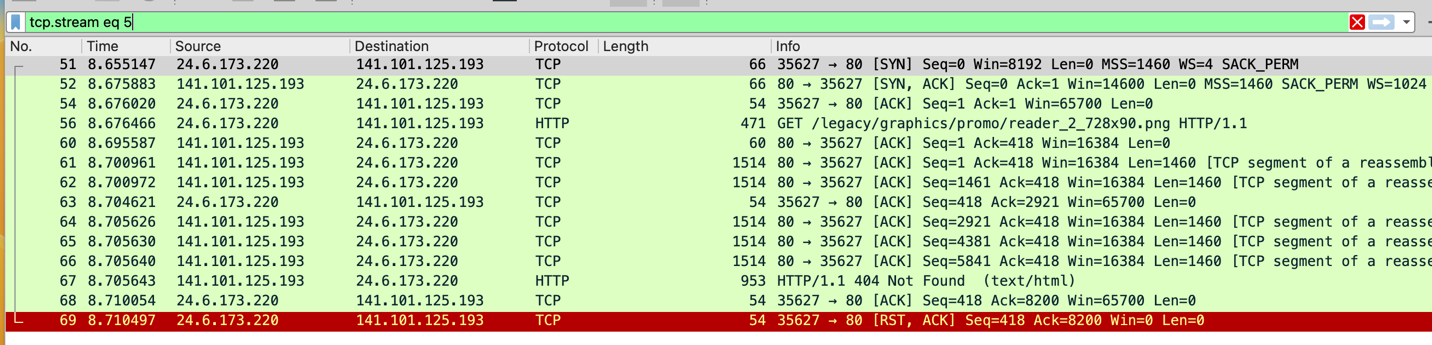
time = 8.700961 – 8.655147 = 0.045814

1. Find RTT using statistics. RTT = 3.66ms





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

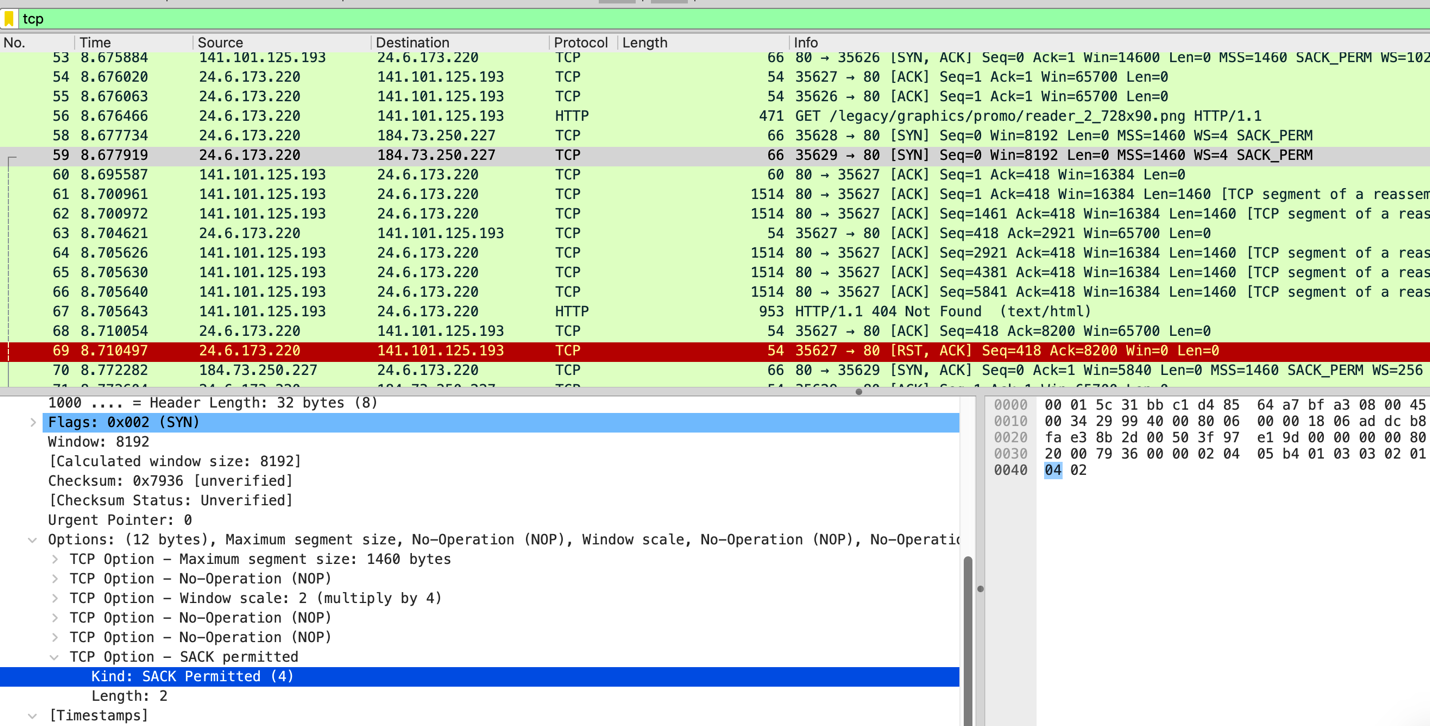


Initial Round Trip Time (iRTT) is 0.020873000 seconds. Round Trip Time for conversation between 24.6.173.220 on Port 35627 [A] and 141.101.125.193 on Port 80 [B] is 0.020736000 seconds (SYN to SYN, ACK) and 0.000137000 seconds (SYN, ACK to ACK).

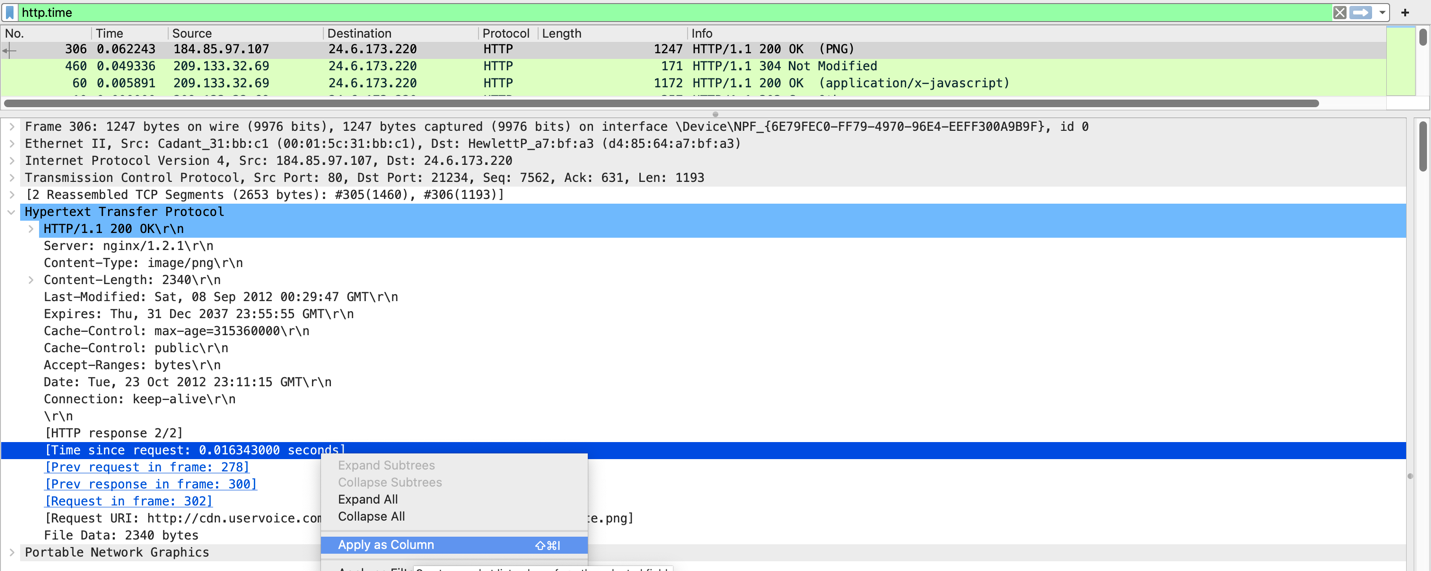
## **What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.**

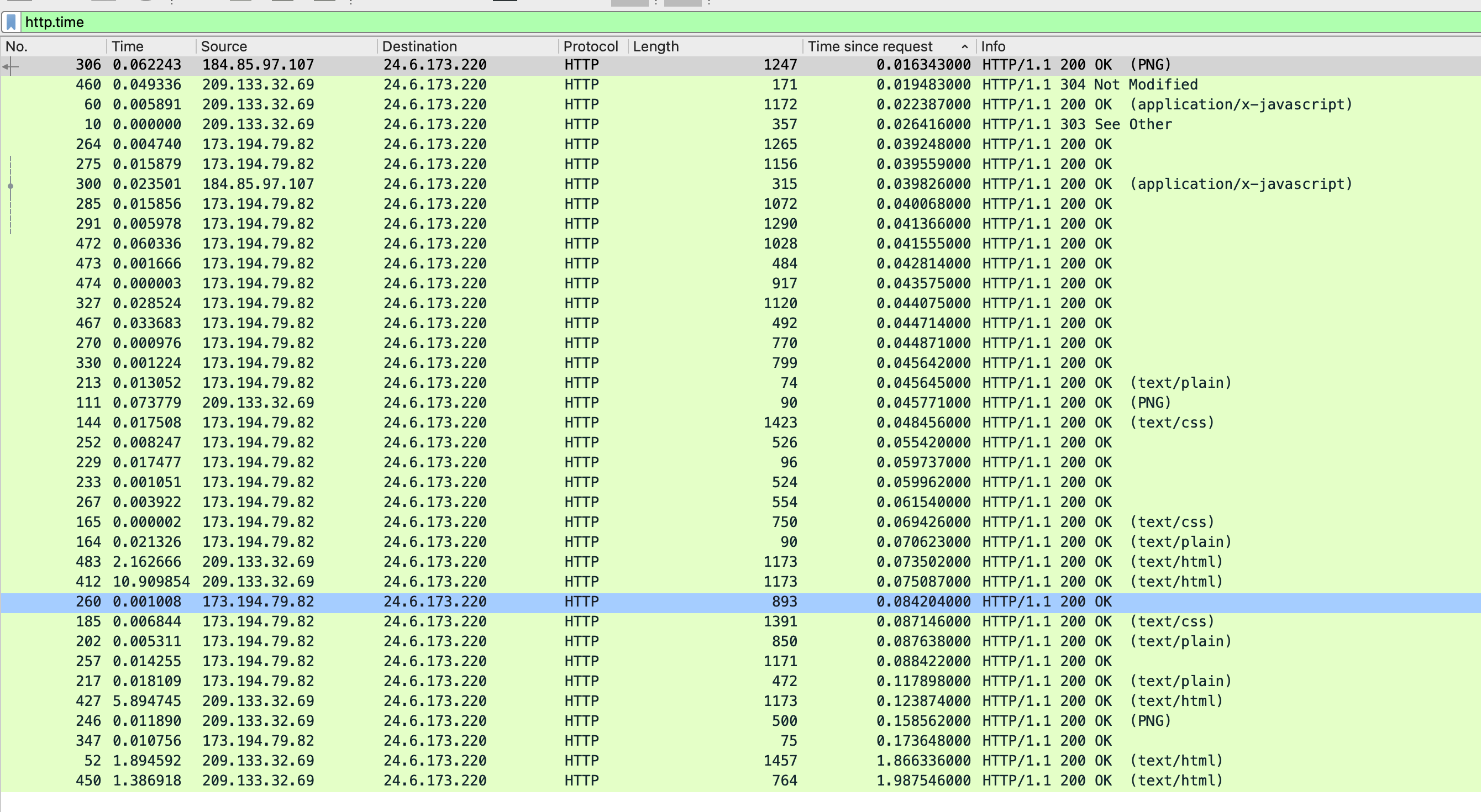
Selective acknowledgments is a sender and receiver side optimization to TCP. It is a mechanism that allows the sender to retransmit only what is missing at the receiver’s end, so that the receiver can acknowledge non-consecutive data.[3]

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



# **Part 2: tr-http-pcaprnet.pcapng**

1. **Use a filter to display the HTTP response time for each HTTP request.**
2. Use filter ‘http.time’.Select one row and click [Time since request] ->’Apply as Column’****
3. Then you can see results in ‘Times since request’ column.

****

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

200 OK: The request succeeded.

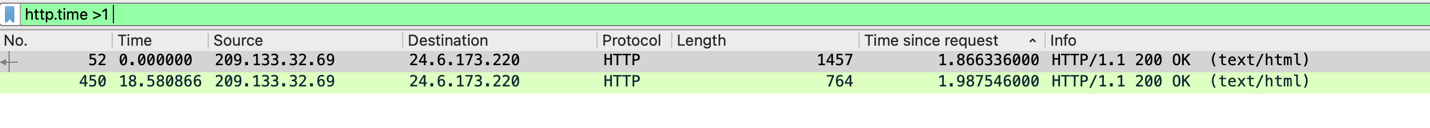
303 See Other: The server sent this response to direct the client to get the requested resource at another URI with a GET request.

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.

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

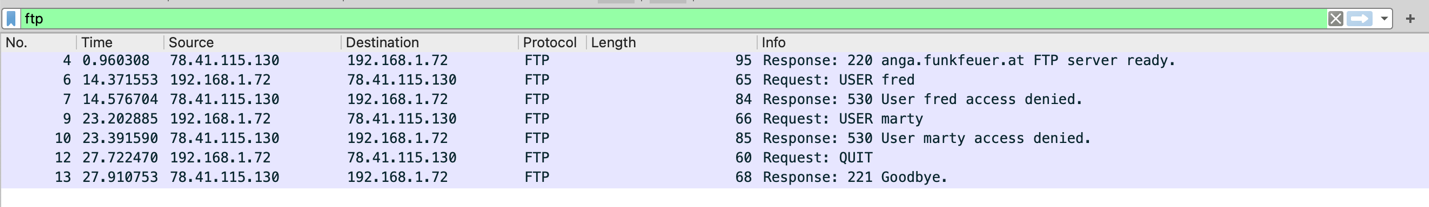
Use filter ‘http.time>1’ based on Part2(a) [5]

****

# **Part 3: tr-http-pcaprnet.pcapng**

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

Use filter ‘ftp’



1. **List the server and client IP addresses and port numbers.**

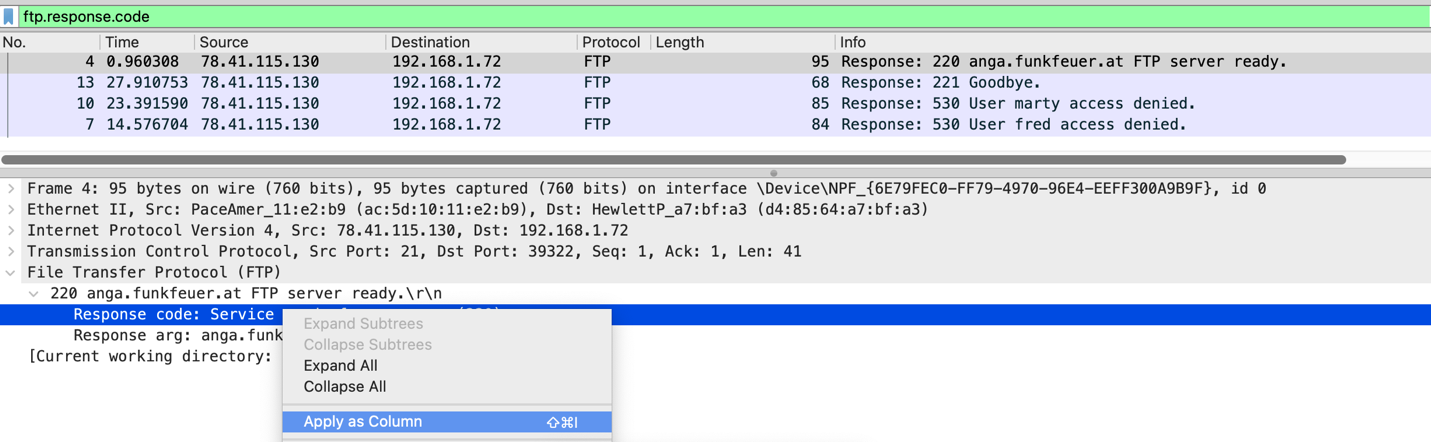
|  |  |  |
| --- | --- | --- |
|  | IP address | Port number |
| server | 78.41.115.130 | 21 |
| client | 192.168.1.72 | 39322 |

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

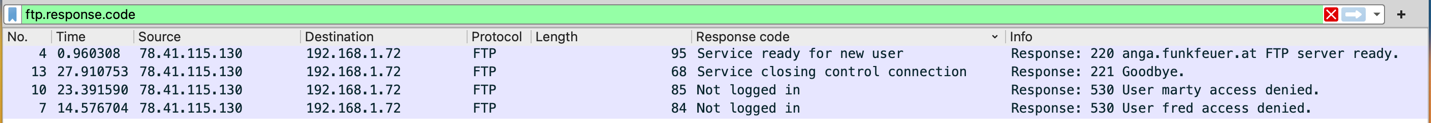
Use filter ‘ftp.response.code’



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



See the column ‘Response Code’ as a result.



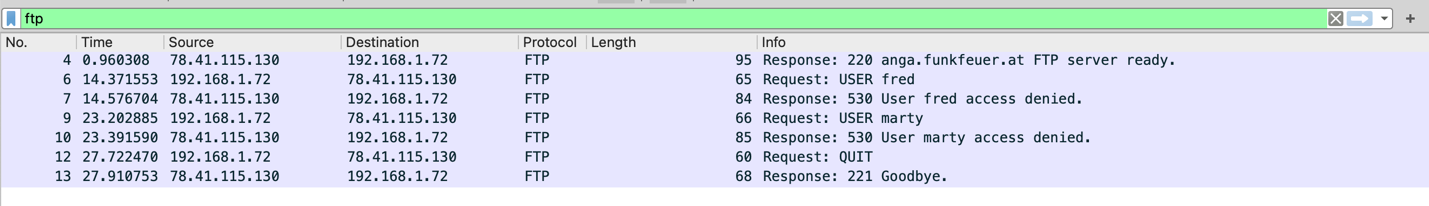
220 Service ready for new user: The server sent this code to a new user that the server is ready to connect new clients.

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.

1. **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.



1. **How secure is FTP?**

FTP is not secure because it relies on plain text without encryption.

# **Part 4: tr-bootp.pcapng**

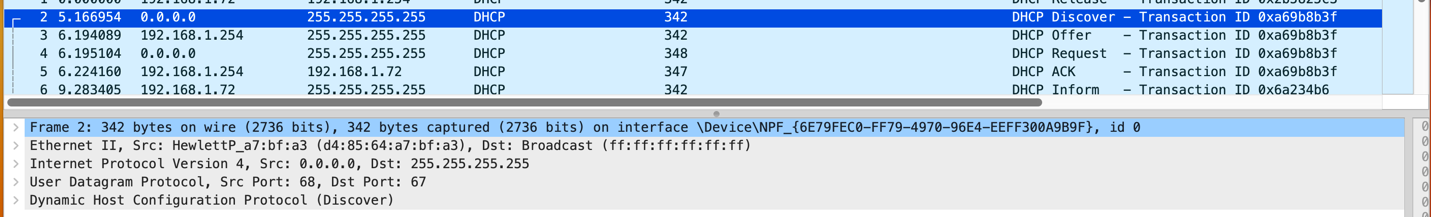
1. **What layer of the OSI model can DHCP Discover packets be found? What type of packet is DHCP Discover? List the source and destination IP addresses and port numbers.**

~~Application Layer.~~ Layer 2 Broadcast.

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 |



1. **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.**

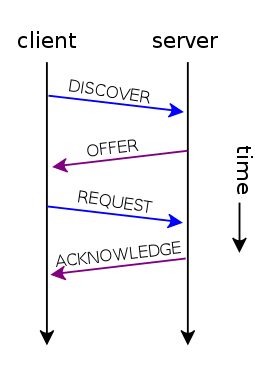
4 DHCP packets.

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.



1. **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.

1. **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.

DHCP Inform: The client (C) sends a DHCP Inform message to the server (S1), requesting parameters such as Subnet Mask, Domain name, DNS, etc.

Whole answer:

Following is the communication flow between Client (C) and Servers (S1 and S2):

1. DHCP Discover: The client (C) sends a broadcast message on its local physical subnet to find available servers.

2. DHCP Offer: Both servers (S1 and S2) respond to the discover message with an offer (broadcast) specifying available network addresses and configuration parameters.

3. DHCP Request: The client (C) sends a broadcast message with its Client ID. The server (S1) from which the client wants to accept the IP is informed that the offer is accepted and the other server (S2) is informed that the offer is declined. Also, the broadcast is meant to confirm that the IP address is valid and is not currently in use by others in the subnet.

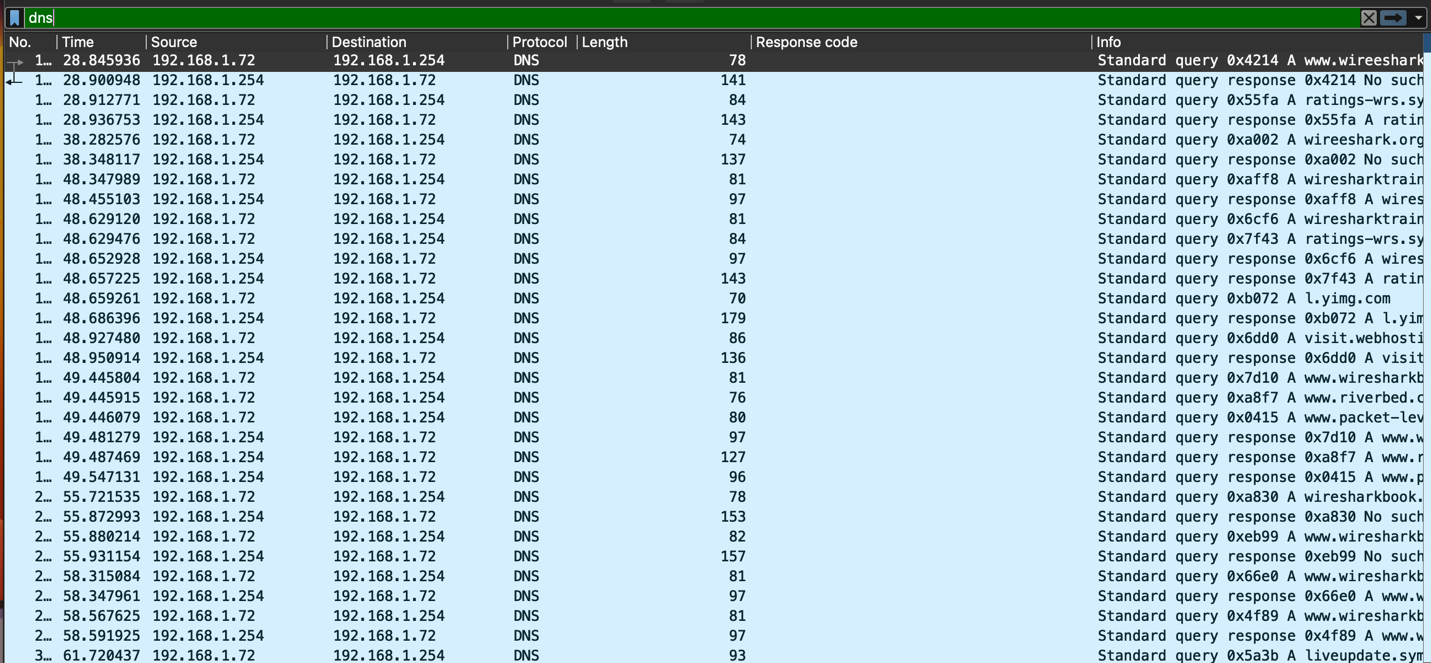
4. DHCP Acknowledgement: The server (S1) will make an entry with the specified client ID and bind the IP address offered with lease time. Now, the client (C) will have the IP address provided by the server (S1).

5. DHCP Inform: The client (C) sends a DHCP Inform message to the server (S1), requesting parameters such as Subnet Mask, Domain name, DNS, etc.

# **Part 5: tr-bootp.pcapng**

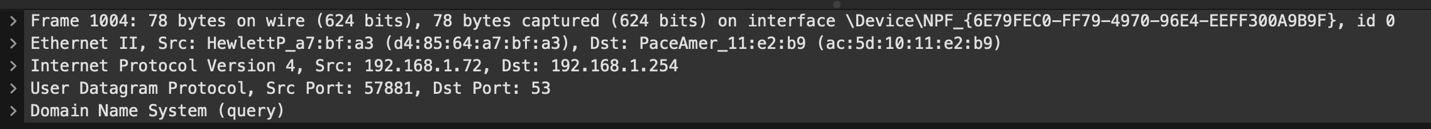
1. **Use a filter to display DNS traffic only.**

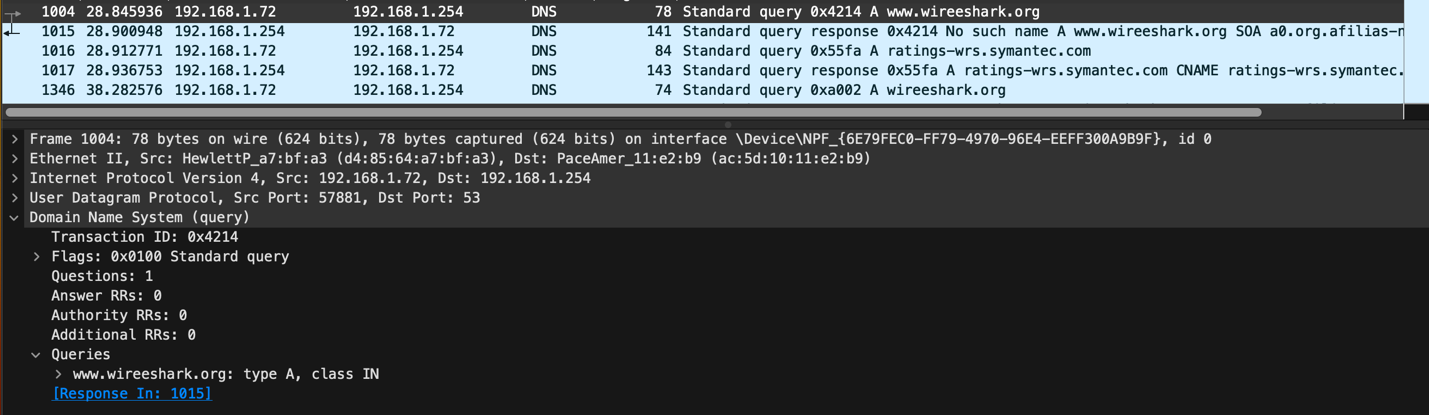
Use filter ‘dns’

****

1. **Which transport layer protocol is used for DNS queries?**

UDP



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

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

1. <https://ask.wireshark.org/question/14573/how-do-i-see-statisticsconversationsbytes-values-in-full-rather-than-abbreviated-as-n-k/>
2. <https://www.geeksforgeeks.org/selective-acknowledgments-sack-in-tcp/>
3. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status>
4. <https://www.youtube.com/watch?v=FMRI6ua2MjE>
5. Disscuss this Question with Jiaran Liu
6. <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>

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. [↑](#footnote-ref-1)