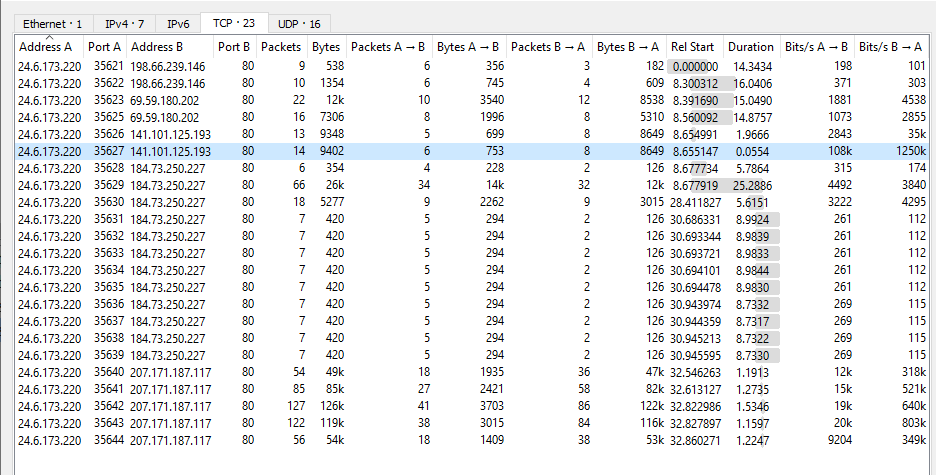
Homework 1

**Part 1: tr-chappelu.pcapng**

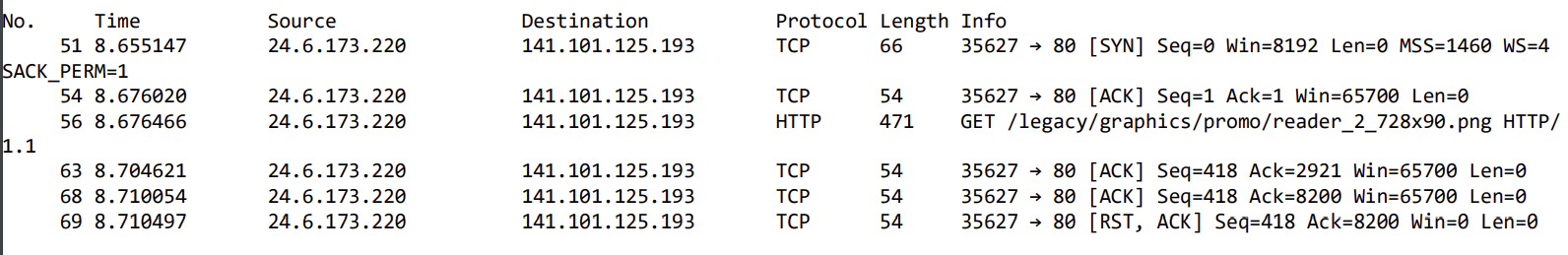
1. Find the most active TCP conversation in the file (by bits per second).

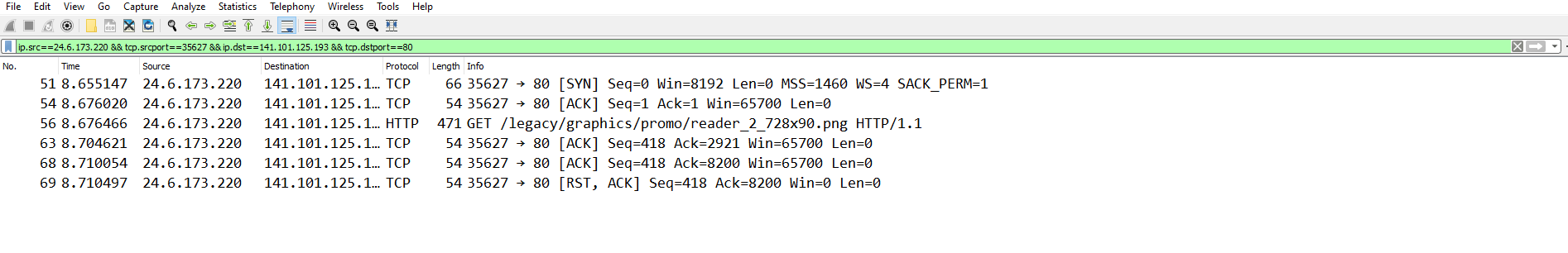
Under Wireshark TCP · 23: the TCP conversation of Address A (24.6.173.220), Port 35627 and Address B (141.101.125.193), Port 80 had the most active conversation.

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



1. 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)





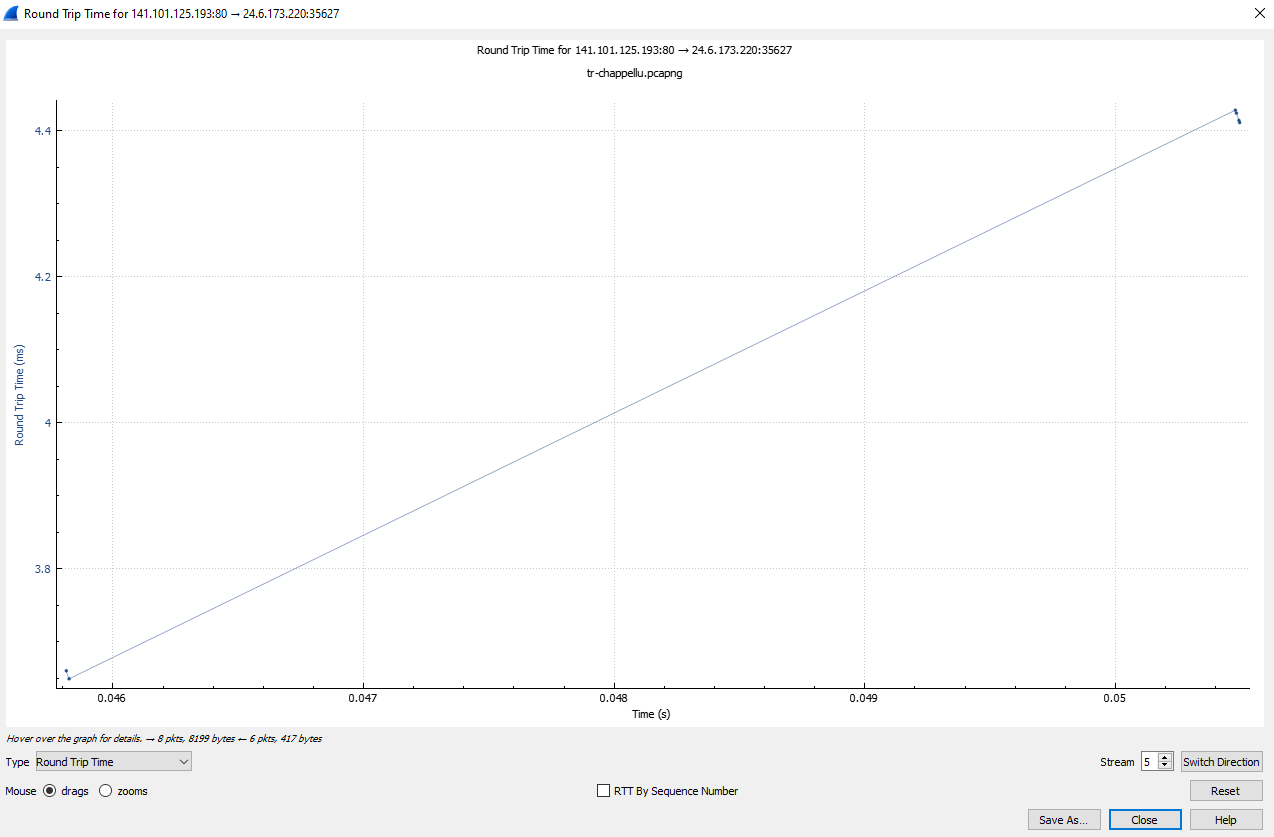


* Packets A → B: 753 bytes, 6 packets
* Packets B → A: 8649 bytes, 8 packets

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 |

1. 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 |

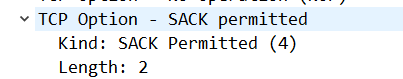
* Packet No. 51 does not have any RTT info as it is not an ACK packet sent.

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



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 on[[1]](#footnote-1).

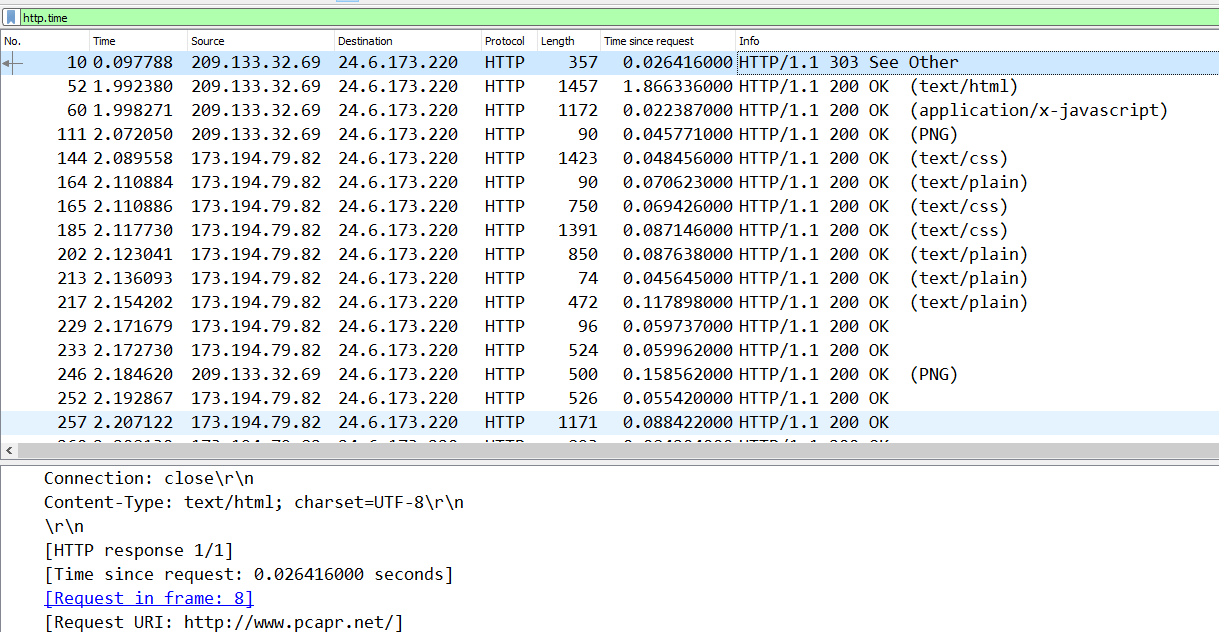
When inspecting other TCP conversations with SACK permitted, the client would send out retransmissions for packets of different frames, showing cases of Selective Acknowledgements.

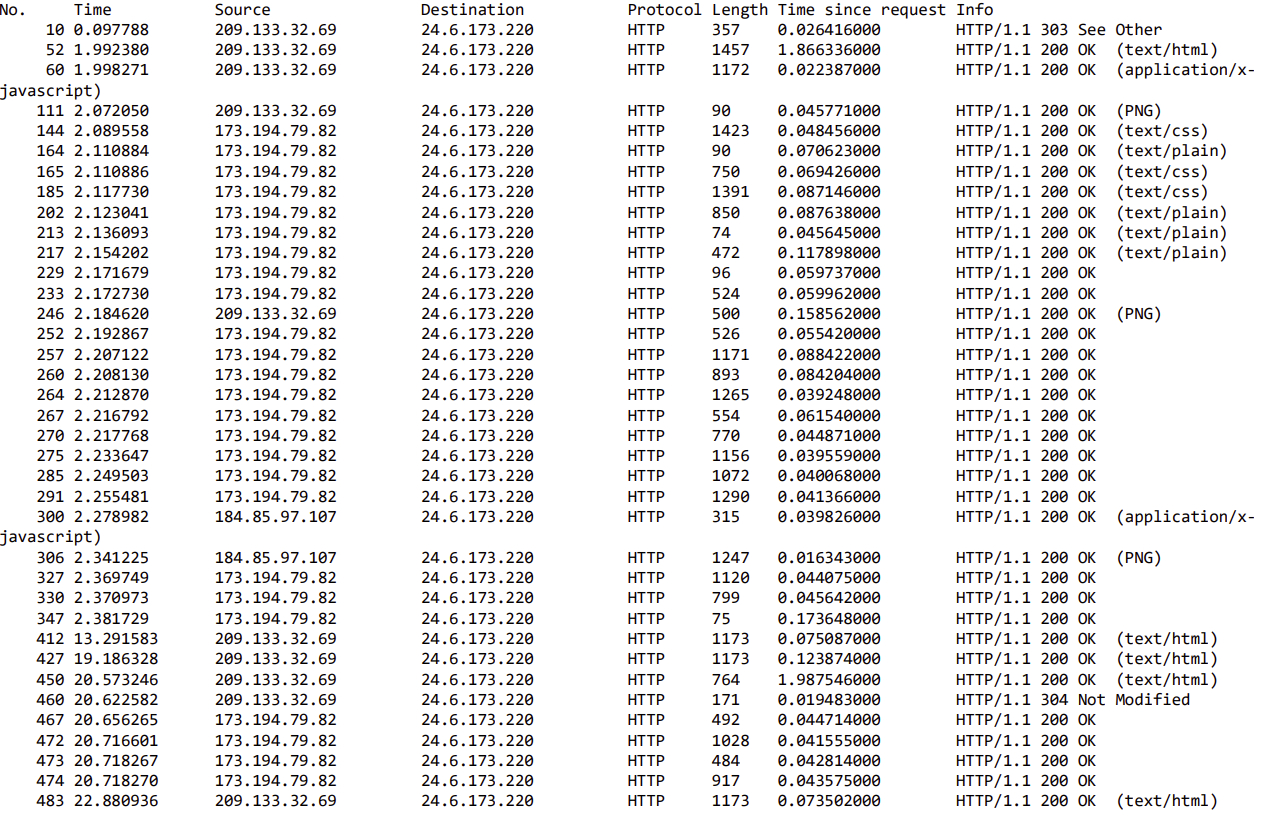


Selective Acknowledgements are a modification to the TCP protocol where the TCP receiver will selectively choose what packet segments to acknowledge in the event that packets sent are out of order or in the event of packet lost[[2]](#footnote-2). The TCP receiver will send duplicate acknowledgements 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 packet[[3]](#footnote-3). 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 received[[4]](#footnote-4).

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

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

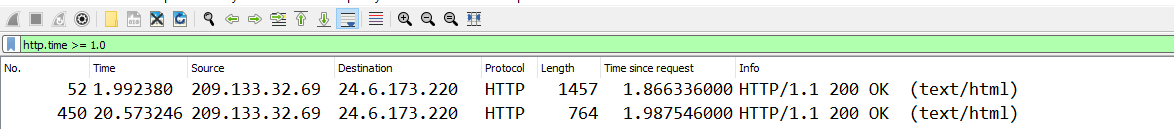




1. Define and explain the significance of each HTTP response status code.

* 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.

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

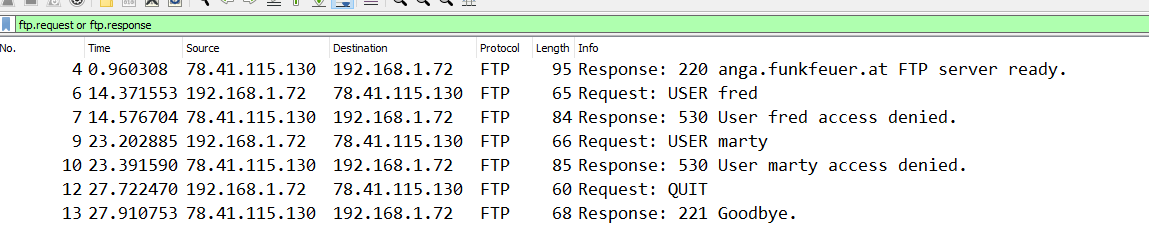


|  |  |
| --- | --- |
| No. | Time since request |
| 52 | 1.866336000 seconds |
| 450 | 1.987546 seconds |



**Part 3: tr-ftpfail.pcapng**

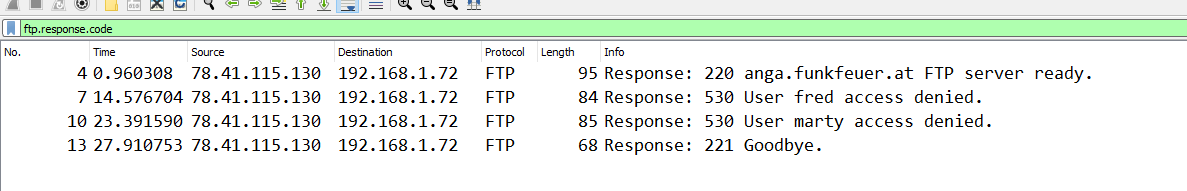
1. Use a filter to display the FTP request and response packets.

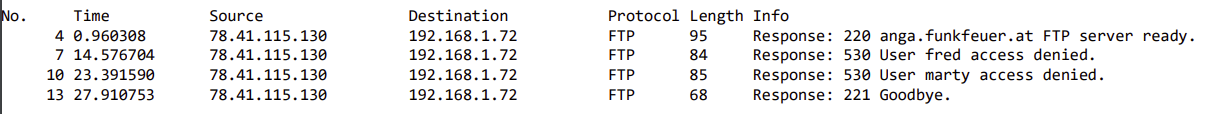


1. List the server and client IP addresses and port numbers.

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

1. Use another filter to display only the FTP response codes for the packets. Define and explain the significance of the response codes[[5]](#footnote-5).





* 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 out[[6]](#footnote-6).

1. 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 server[[7]](#footnote-7).

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.

1. How secure is FTP?

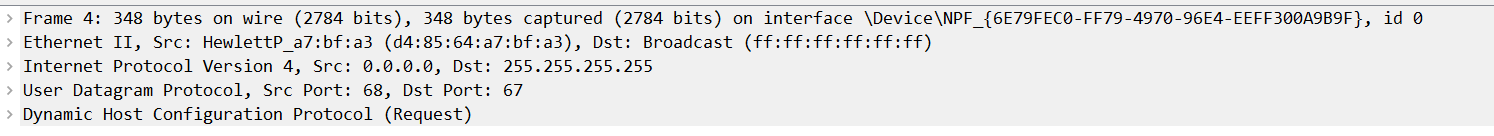
FTP is not very secure. Similarly, to a standard TCP connection, there is no encryption as passwords and usernames are sent as cleartext during authentication[[8]](#footnote-8). It requires additional protocols such as Secure File Transfer Protocol (SFTP) in order to add another layer of encryption and security for during authentication[[9]](#footnote-9).

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.

**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

DHCP packets are located in the IP protocol where it operates using the link-layer addresses[[10]](#footnote-10). The IP protocol is located in the Network Layer (Layer 3)[[11]](#footnote-11). DHCP, itself, is an application layer (Layer 7) protocol. The DHCP Discover Packet is a UDP packet.



* Source:
  + IP address: 0.0.0.0
  + Port Number: 68
* Destination:
  + IP address: 255.255.255.255
  + Port Number: 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

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 notes un 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 specified[[12]](#footnote-12).
5. What is the significance of DHCP Release packet?

It lets the client release their IP address along with the allotted time given to the client[[13]](#footnote-13).

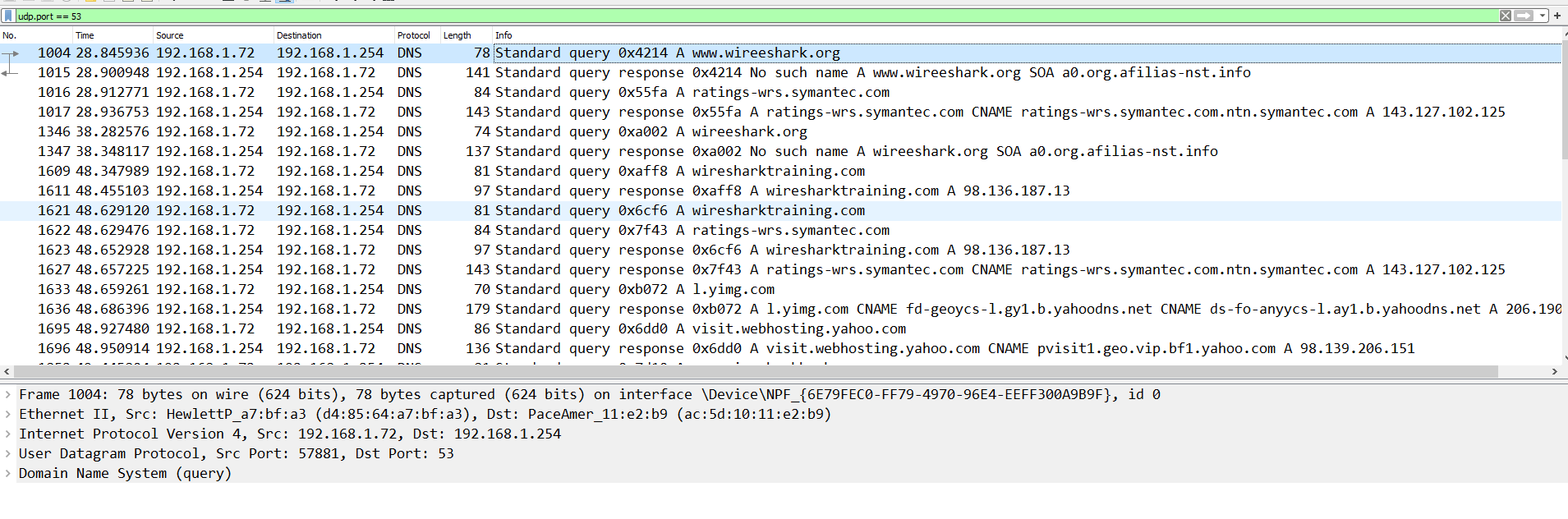
1. Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.

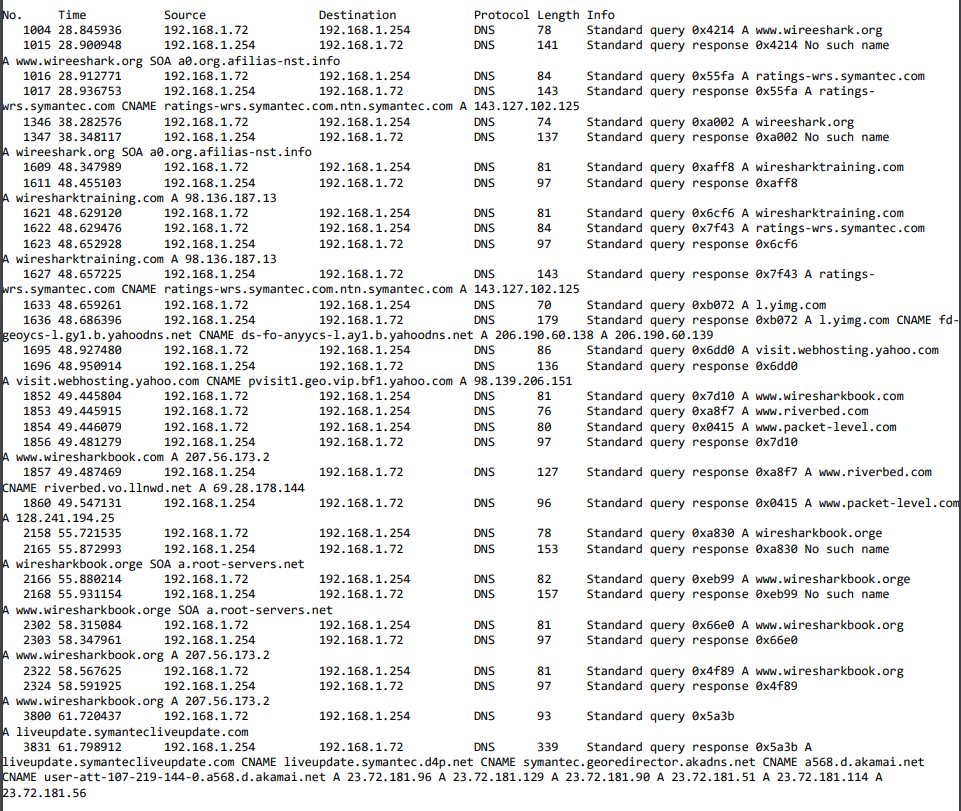
Because the client and server have to broadcast the DHCP Discover and DHCP Offer messages to all nodes within a network, this can inform multiple servers about the DHCP client’s request. Every DHCP server that receives the request will transmit their own DHCP offer messages via broadcast, allowing the 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**

1. 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.





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

DNS queries utilize UDP protocol encapsulated within an IP datagram[[14]](#footnote-14).

1. 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](http://www.wireeshark.org) with 2 e’s rather than [www.wireshark.org](http://www.wireshark.org).



1. https://blog.catchpoint.com/2014/06/17/sack-transmissions-improve-web-performance/ [↑](#footnote-ref-1)
2. Kurose & Ross, chapter 3, page 250 [↑](#footnote-ref-2)
3. https://packetlife.net/blog/2010/jun/17/tcp-selective-acknowledgments-sack/ [↑](#footnote-ref-3)
4. https://blog.catchpoint.com/2014/06/17/sack-transmissions-improve-web-performance/ [↑](#footnote-ref-4)
5. https://www.wireshark.org/docs/dfref/f/ftp.html [↑](#footnote-ref-5)
6. https://help.globalscape.com/help/cuteftpmacpro3/Numbered\_FTP\_status\_and\_error\_codes.htm [↑](#footnote-ref-6)
7. Kurose and Ross, page 117 [↑](#footnote-ref-7)
8. https://digitalguardian.com/blog/what-ftp-security-securing-ftp-usage [↑](#footnote-ref-8)
9. https://www.ssh.com/ssh/ftp/server [↑](#footnote-ref-9)
10. https://tools.ietf.org/html/rfc2131 [↑](#footnote-ref-10)
11. Kurose & Ross, page 344 [↑](#footnote-ref-11)
12. Kurose & Ross, page 346 [↑](#footnote-ref-12)
13. https://tools.ietf.org/html/rfc2131 [↑](#footnote-ref-13)
14. Kurose & Rose, page 131 [↑](#footnote-ref-14)