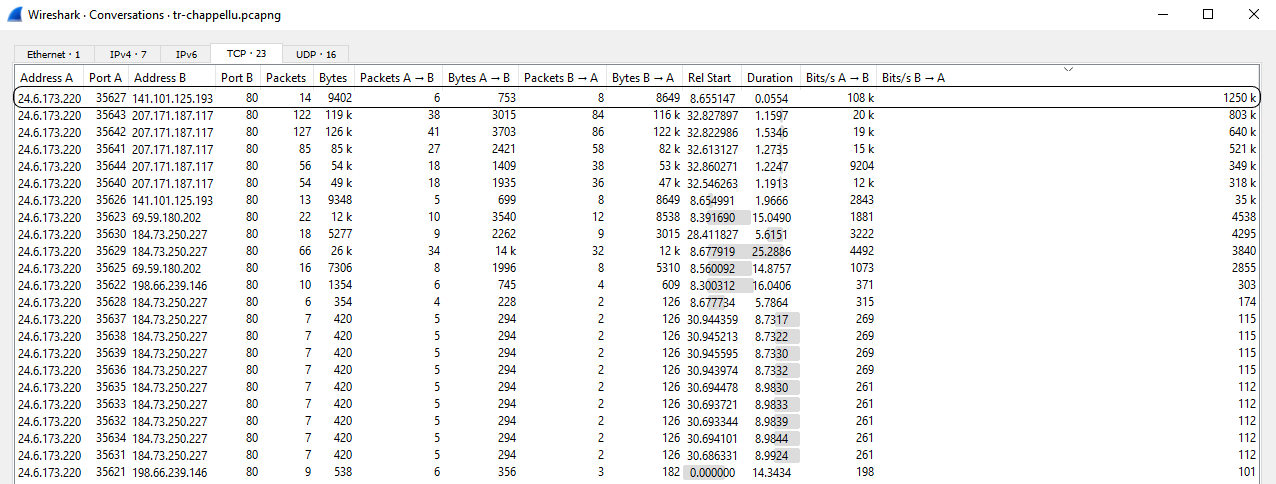
Part 1 Solutions

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

- The most active TCP conversation in this displayed as follows with 1250 bits/s



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)

-

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

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

Part 2 Solutions

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

Solution -

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

Solution –

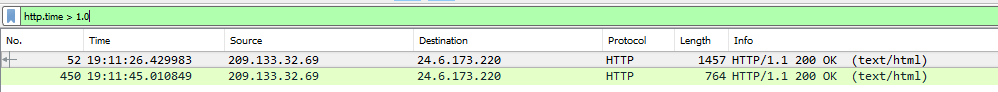
200 OK is the response for a successful HTTP request.

303 See Other

304 Not Modified

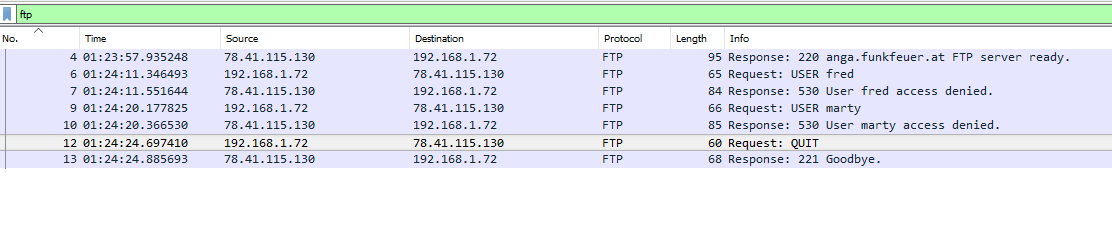
c. Apply a filter that lists packets wherein the HTTP response time is greater than one second.

Solution – The packets where HTTP response time is grater than one second are listed below :-



Part 3 Solutions

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



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

Client – 192.168.1.72 , 39322

Server – 78.41.115.130, 21

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

220

530

221

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

Client, Request quit

e. How secure is FTP?

Part 4 Solutions

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.

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.

c. What is the significance of DHCP Release packet?

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

Part 5 Solutions

a. Use a filter to display DNS traffic only.

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

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

No such name