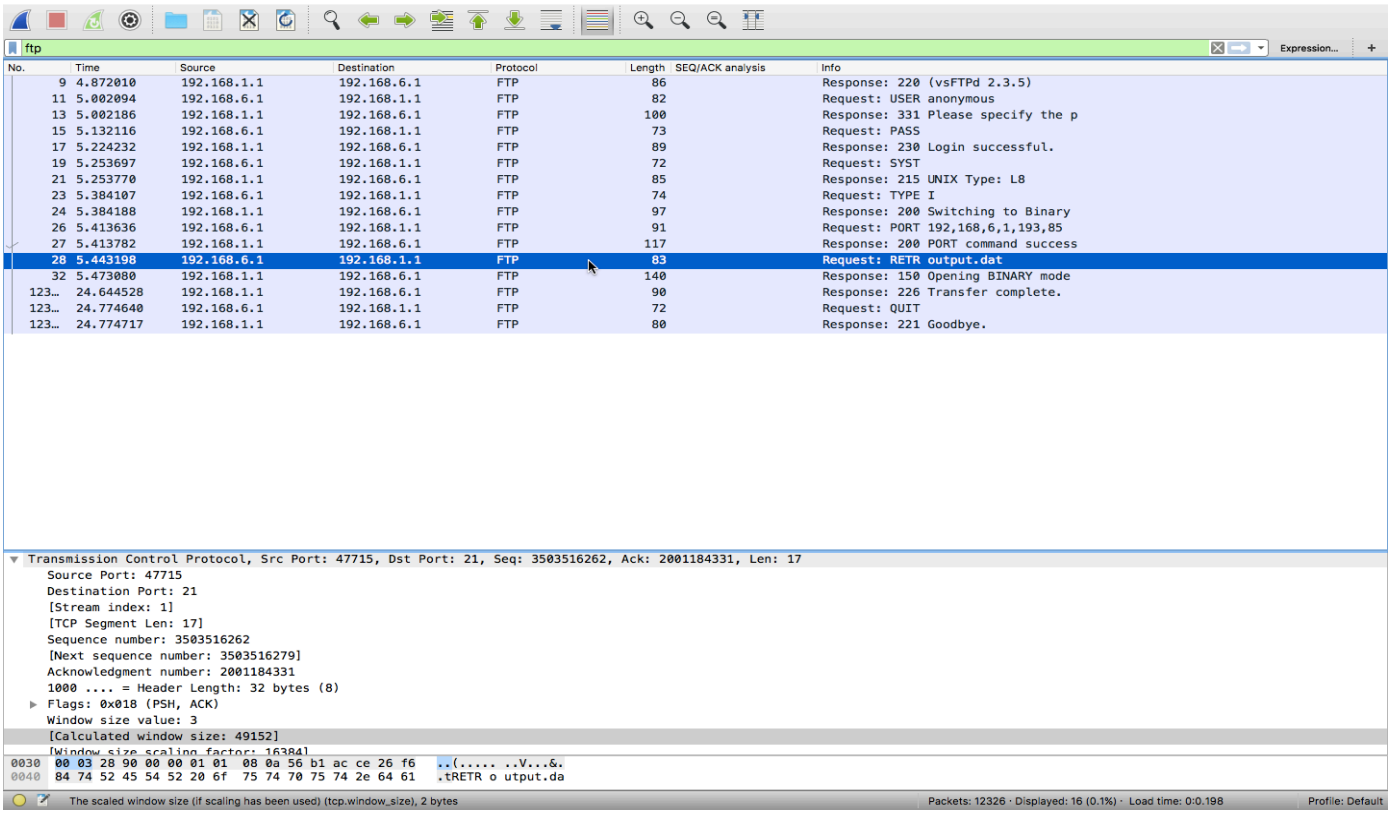
Compsci 314 assignment 2

A. The FTP Protocol

1. What well-known port number is used? 21

2. What usercode and password are used to log in to FTP?

   Usercode: anonymous, and there is no password

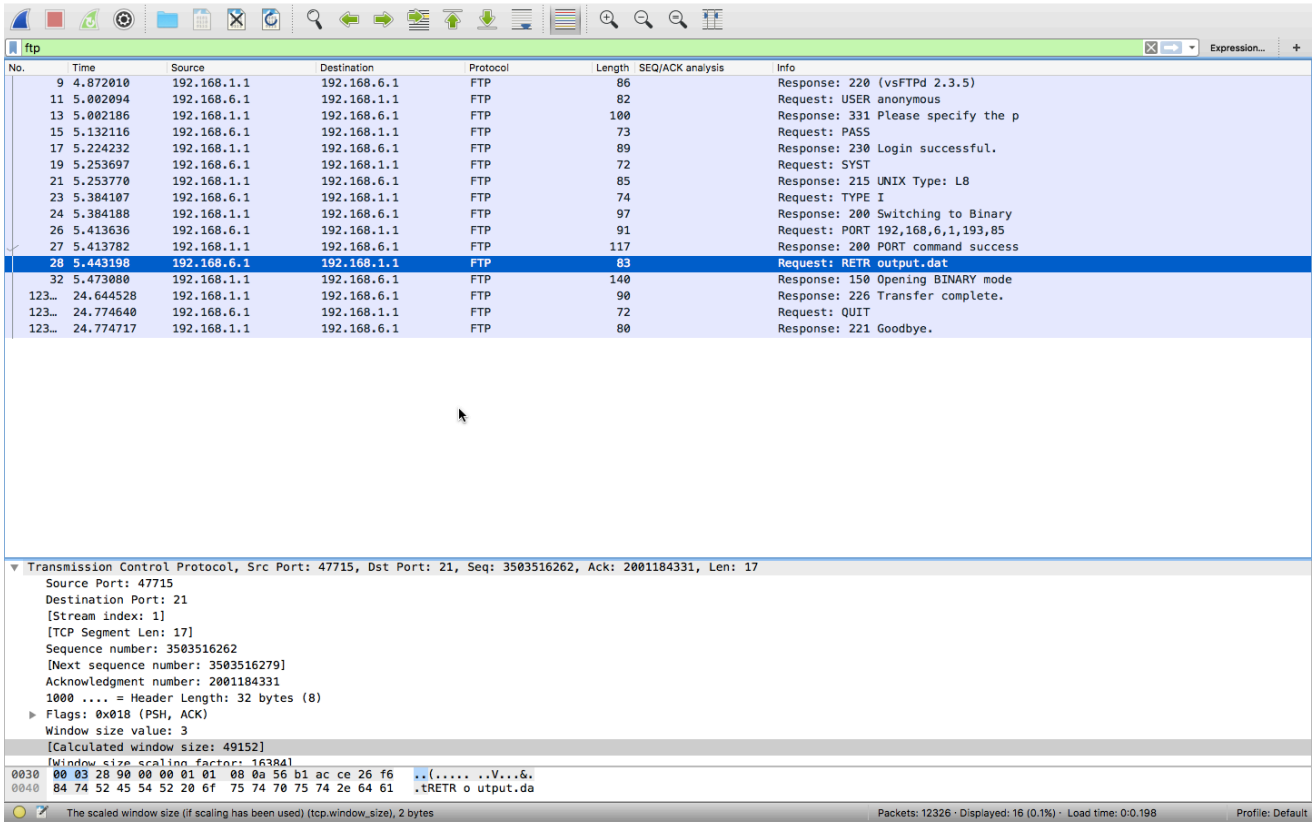


3. Why is FTP mode switched to binary?

   Binary transmits raw bytes of the file being transferred. Hence the file could be transferred in its exact original form

4. What FTP command is used to download the test file?

RETR output.dat

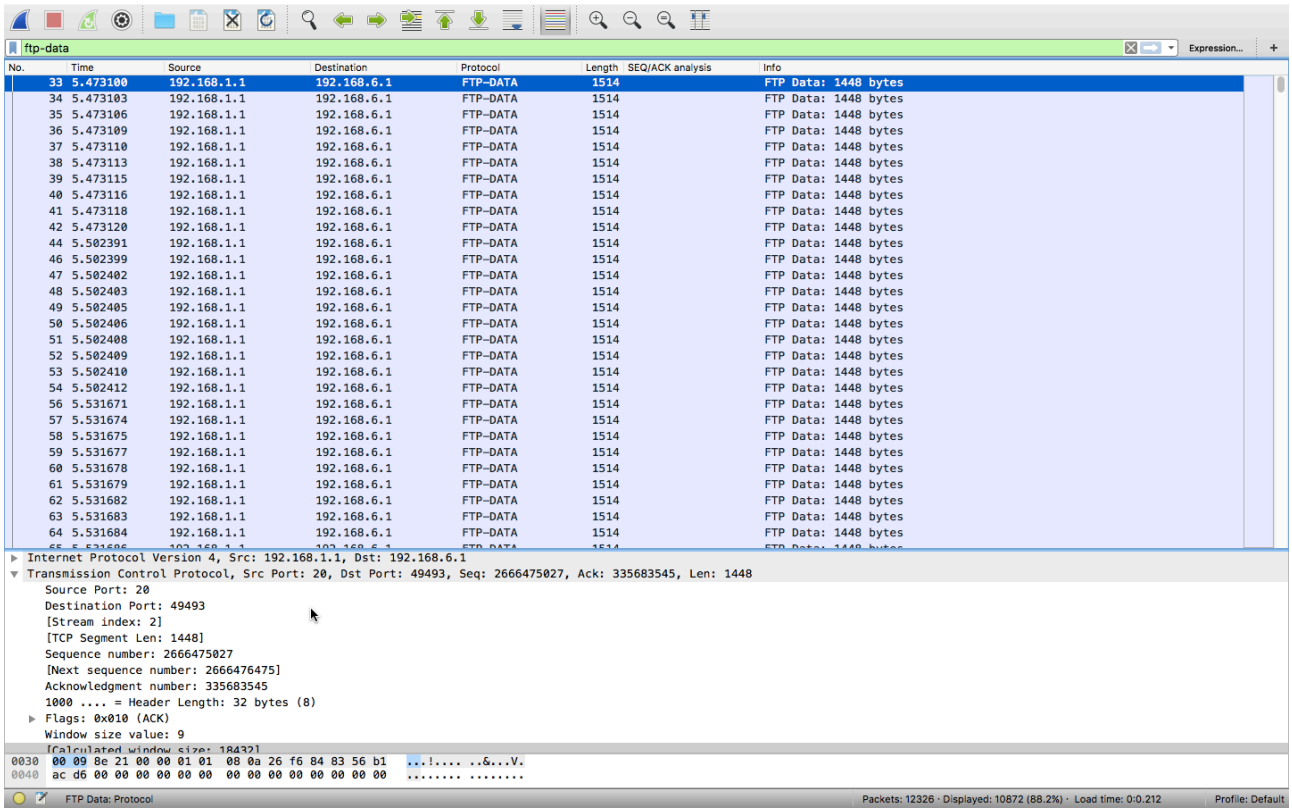


B: Data bytes transmitted by TCP [8 marks]

Set a Wireshark filter to look at all packets sent through the ftp-data flow:

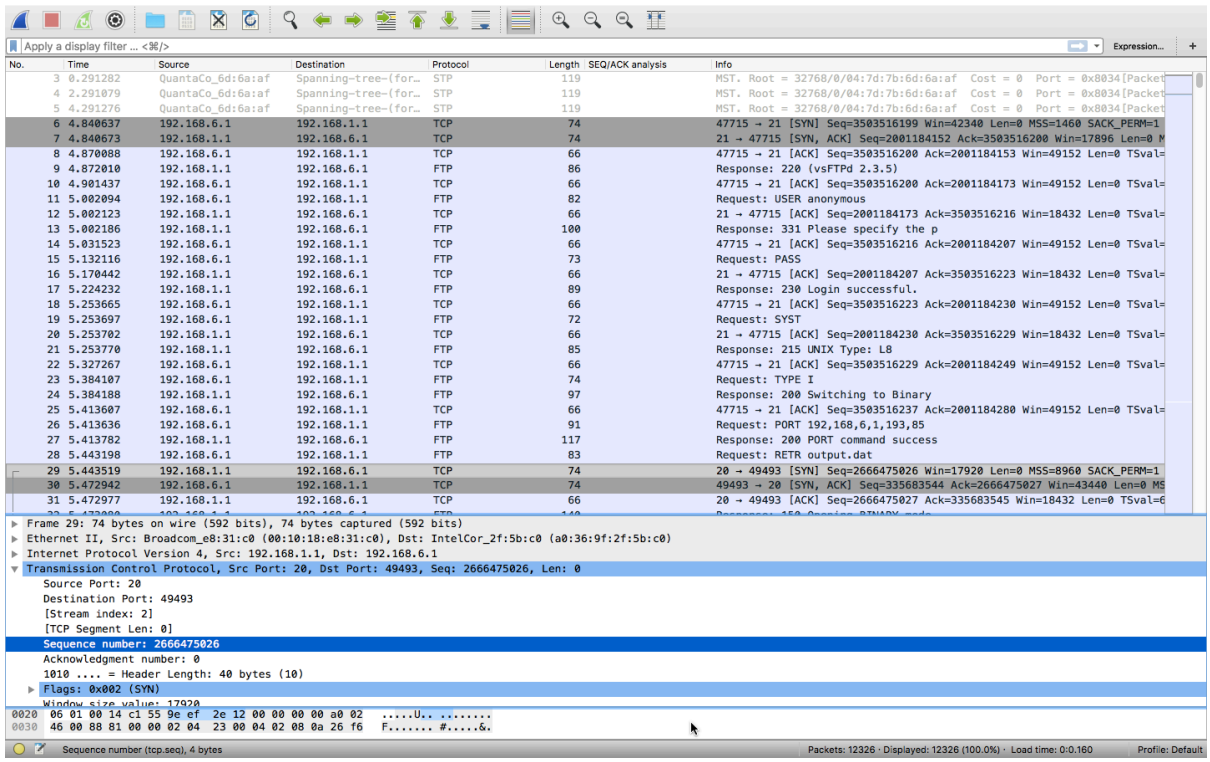
5a. What well-known port number is used for FTP data? [1 mark]

20

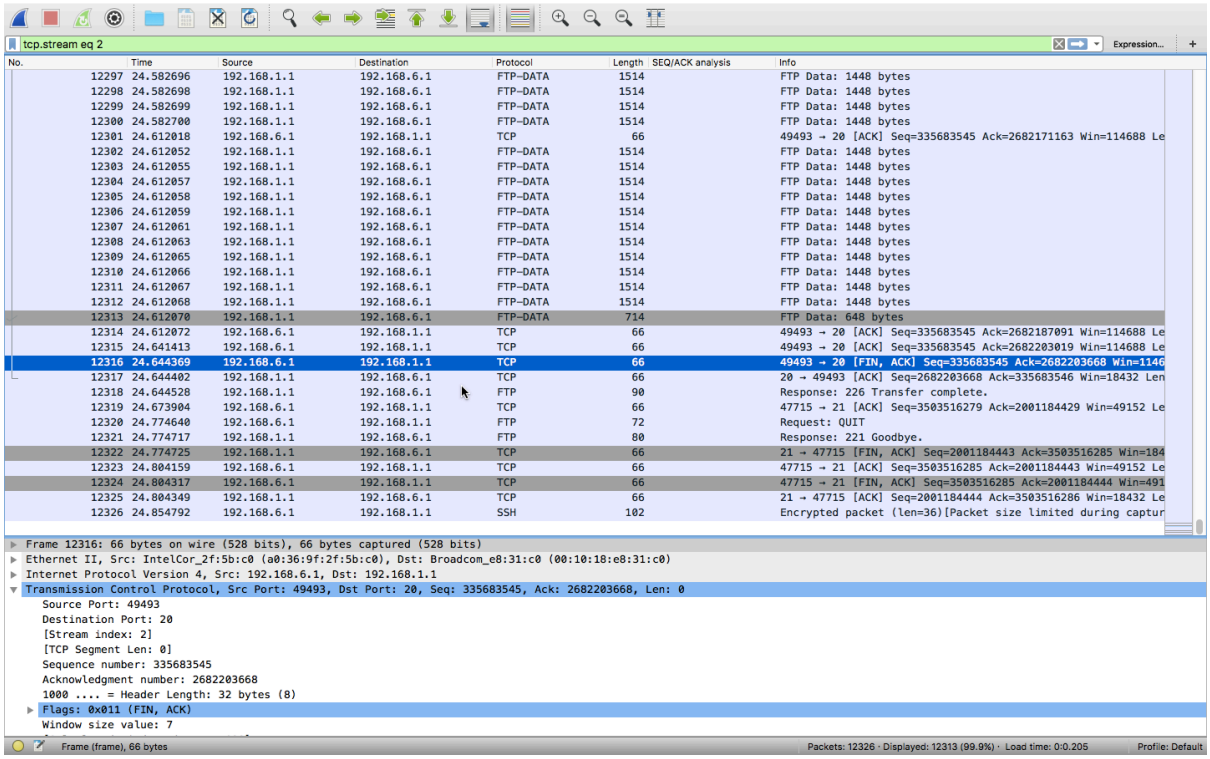


5b. What are the packet and sequence numbers for the file transfer's opening SYN? [2 marks]

Packet number 29, sequence number: 2666475026



5c. What are the packet and sequence numbers for the ACK to the file transfer's closing FIN (i.e. the FIN from the FTP data sender)? [2 marks]
Packet number: 12316, sequence number: 335683545

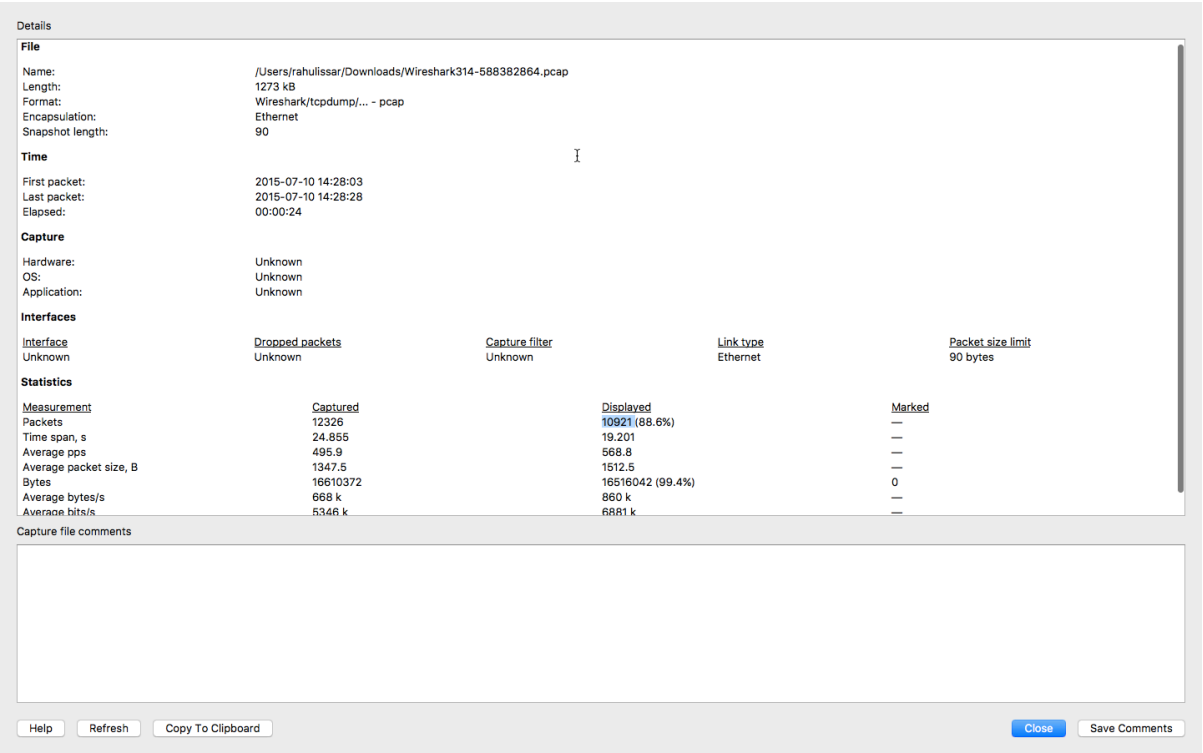


5d. How many actual data bytes were sent by the file transfer? [2 marks]
Ack – seq
= (2682203668 – 2666475026) -2 = 15728640 bytes

5e. What was the size of the transferred file? [1 marks]
15728640 bytes

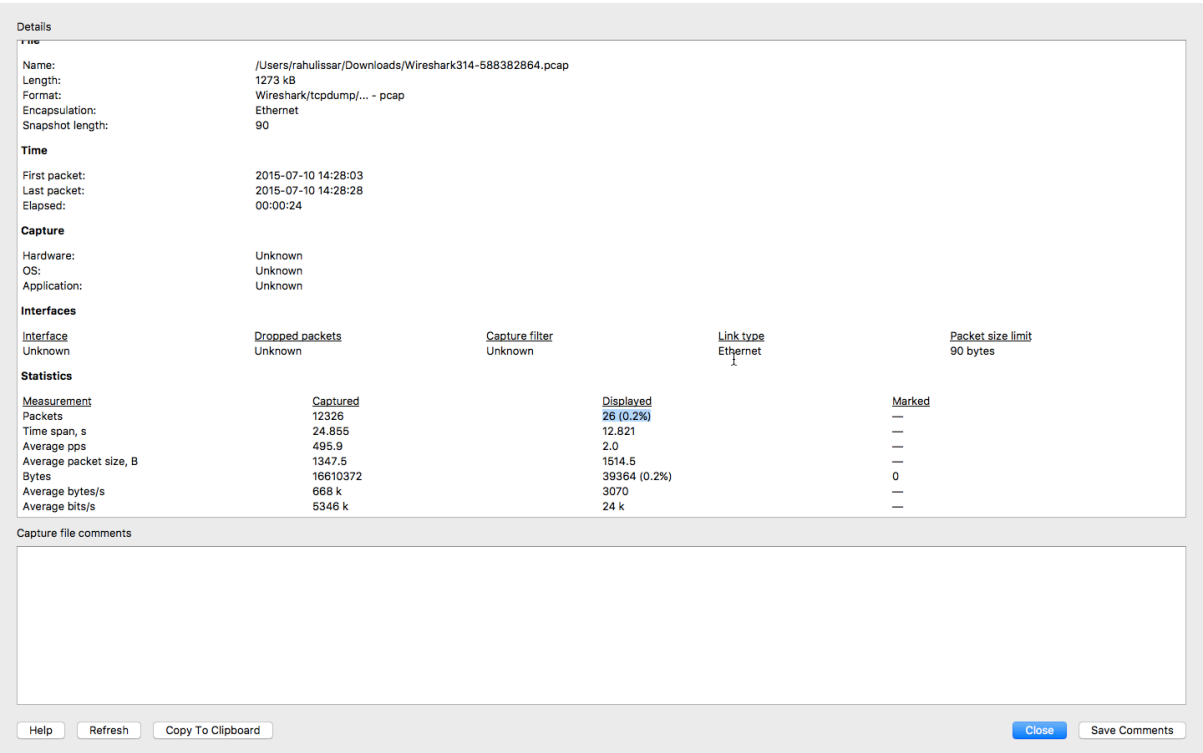
C: Packets retransmitted by TCP [7 marks]
Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

6a. How many packets are displayed using this filter? [1 mark] Hint: Try Wireshark's Statistics | Summary Set a Wireshark filter to look at packets with TCP source port FTP-DATA that were retransmitted.
10921



6b. How many retransmitted packets does Wireshark display? [1 mark]

26.



6c. How does Wireshark recognise a packet retransmission? Hint: Use a search engine to find out about this. [3 marks]

Regardless of the sequence and acknowledge numbers, dropping packets are not possible in Wireshark. Wireshark shows any packet which is captured. It does not consider using checksum or IP id in recognising a packet transmission. It recognises a packet retransmission with a comparison that shows the difference between the sequence numbers and the expected sequence number from the last packet of the conversation into the same direction. The packets are placed in order.

6d. What is the observed packet loss percentage for this trace file? [2 marks]

(10921 – 26) / 10921 * 100 = 99.76% . This is the successfully transmitted packets. Therefore, the packet loss is 100 – 99.76 = 0.24%

D: Protocol overhead [8 marks]

Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

7a. In question 5e you determined the number of data bytes transferred. How many bytes were actually sent during that transfer? [2 marks]

16516042 bytes

7b. What was the percentage of “protocol overhead” for that file transfer? [2 marks]

16516042 – 15728640 = 787402, this equals the total overhead. Therefore, (787402/ 16516042) * 100 = 4.77% (2dp) this gives the percentage protocol overhead for the file transfer.

7c. What parts of the packets contributed to that overhead? Note: your answer to this question must be a proper English sentence. An answer that is not a sentence will score zero marks. Hint: “overhead” means everything except the actual data. [4 marks]

Overhead is everything except the actual data. Frame length is 1514 bytes whereas actual data is 1448 bytes (1514 – 1448 = 66). The 66 bytes is therefore the overhead. 32 bytes from these 66 bytes is from the TCP header length, 20 bytes from the IP header length and the rest of It is from the Ethernet layer (resent packets).

E: Round-trip time [4 marks]

8. What is the most common Round-Trip Time (RTT) for packets from sender and receiver and back? [4 marks] Hint: Try Wireshark's Statistics | TCPStreamGraph | Round Trip Time Graph You can drag the mouse to form a rectangle over any section of interest on that graph.

According to the Round-Trip time graphs shown below, the most common RTT for packets is 29.50 ms.