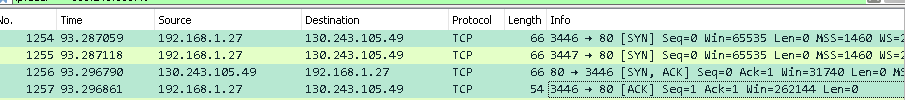
**4.- Monitoring TCP/UPD in Wireshark**

**Task 3.1.- The Transmission Control Protocol (TCP)**



Q1: When, in the datalog, does the “three-way handshake” process occur?

When a request is send by the client

Q2: How do you identify the segments that belong to the handshake process?

Above you can see the marked lines are when it occurs. Three steps:

Client🡪 server seq=y

Client 🡨 server seq=y ACK=x+1

Client🡪 server a seq=y+1 ACK

Q3: What happens during the “three-way handshake” process?

1. The connection between the client and the server is established --- - Seq=0

SYN packet is sent from the client

1. The SYN is received by the server, which the server then responds with SYN/ACK packet. ACK=1 if the server acknowledged correctly the packs of the client.
2. The client increases seq by one, and sends it back to the server along with an ACK

Q4: Who starts the “three-way handshake”?

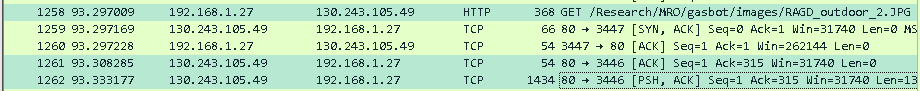
The client

Q5: Who sets the Maximum Segment Size (MSS)? The client or the server?

First the client send a suggestion and then both client and server agrees

Q6: In the datalog that you recorded, what is the MSS that client and server agreed on?

The clients suggestion was 1460 but the servers was 1380 and at the they agreed on 1380



Q7: What “sequence number” and “next sequence number” does the GET HTTP message have?

sequence number: 1

next sequence number:315

Q8: Find the ACK sent by the server when the GET is received. What is the ACK number that the server sends? Where does this number come from?

ACK: 315, it comes from next sequence number when the GET message was sent

Q9: Check the ACK numbers sent by the client (your browser). How does the client determine the ACK numbers?

It checks the next sequence number

Q10: Do all the data packets receive an ACK? If not, why not? (You will need to check the course material to answer this question)

TCP dose not ack packet but sequence numbers

Q11: Check the size of some of the received packets. Are all the packets of the same size? What is the maximum size of the packets? Which parameter determines the maximum size?

Packets size are different and the maximum is 1380

Q12: Using an α=0.15, compute the EstimatedRTT for the 20 segments you selected.

2.1837939852707912e-05

Q13: What happens if you set α=0.30, α=0.45, α=0.50 and α=0.70? Can you explain what does α do? Plot the Estimated RTT’s for the different α’s.

The alpha determines how much sampleRTT should be weighted. In the book the ideal ( recommended) alpha is 0.125.

Task 3.2.- The connectionless transport UDP

nslookup –nosearch www.nfl.com

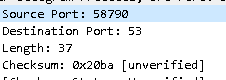
Q1: Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header?

Four fields

Q2: By consulting the displayed information in Wireshark’ s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

8 bytes

Q3: The value in the Length field is the length of what?. Verify this answer with your captured UDP packet.



Source Port, (2 bytes),

Destination Port (2 bytes),

Length (2 Bytes),

Checksum (2 Bytes)

=8 bytes

Q4: What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to Q2. above)

Largest UDP payload = largest possible source port number(65535)- header sizer(8)= 65527

Q5: What is the largest possible source port number? (Hint: see the hint in Q4.)

65535 is the largest possible port number . (2^16 -1) =65535