Exercise 1: Understanding TCP using Wireshark

Question 1 . What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

IP address of gaia.cs.umass.edu: 128.119.245.12

Port number: 80

IP address of client: 192.168.1.102

port number of client: 1161

Question 2. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Ethereal window, looking for a segment with a "POST" within its DATA field.

Sequence number: 23129013

Question 3. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST) sent from the client to the web server (Do not consider the ACKs received from the server as part of these six segments)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the *EstimatedRTT* value (see relevant parts of Section 3.5 or lecture slides) after the receipt of each ACK? Assume that the initial value of *EstimatedRTT* is equal to the measured RTT (*SampleRTT*) for the first segment, and then is computed using the *EstimatedRTT* equation for all subsequent segments. Set alpha to 0.125.

The first segment of HTTP POST are No.4 , 5, 7, 8, 10, 11.
The ACKS are No.6, 9, 12, 14, 15, 16.

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * sampleRTT

1.EstimatedRTT =0.02746 second
2.EstimatedRTT = 0.875 * 0.02746 + 0.125 *(0.077294-0.041737)= 0.0285 second
3.EstimatedRTT= ….= 0.0337
4.EstimatedRTT = 0.0438
5.EstimatedRTT = 0.0558
6.EstimatedRTT = 0.0725

Question 4. What is the length of each of the first six TCP segments?

Length of first TCP= 565

Lenth of other five = 1460

total = 565+1460 = 2025

Question 5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Minimum : 5840 bytes.

The lack of receiver buffer space will not throttle the sender.

Question 6. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

There is no retransmitted segments in the trace file.

I checked it by using the Time-sequence graph and the ACK numbers.

Question 7. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (recall the discussion about delayed acks from the lecture notes or Section 3.5 of the text).

The typical acknowledge data is 1460.

Question 8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

The total bytes transferred is 163516 bytes. The total time is 5.455 seconds. Hence the throughput is 163516 / 5.455 = 29,975 bytes/sec =29.9 kbytes/sec

Exercise2

Question 1 . What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server?

2818463618

Question 2. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value?

1247095790

The previous sequence +1

Question 3 . What is the sequence number of the ACK segment sent by the client computer in response to the SYNACK? What is the value of the Acknowledgment field in this ACK segment? Does this segment contain any data?

2818463619

1247095791

only 1 byte data

Question 4 . Who has done the active close? client or the server? how you have determined this? What type of closure has been performed? 3 Segment (FIN/FINACK/ACK), 4 Segment (FIN/ACK/FIN/ACK) or Simultaneous close?

The client has done the active close. It is simultaneous close(4 messages in total in abab form).

Question 5 . How many data bytes have been transferred from the client to the server and from the server to the client during the whole duration of the connection? What relationship does this have with the Initial Sequence Number and the final ACK received from the other side?

Client to server:

2818463653- 2818463618 = 35 bytes

Server to Client:

1247095832 -1247095790 =42 bytes