Student Name: Luyang Ye
Student ID: z5280537

Lab 4

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?

The IP address of gaia.cs.umass.edu is 128.119.245.12

The port number is sending and receiving TCP segments for this connection is 80

The IP address and TCP port number used by the client computer that is transferring the file to gaia.cs.umass.edu is 192.168.1.102 and 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 Wireshark window, looking for a segment with a "POST" within its DATA field.

The sequence number of the TCP segment containing the HTTP POST command (which is the 4th TCP segment) is 232129013, and the next sequence number is 232129578.

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.

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph>Round Trip Time Graph . However, do not use this graph to answer the above question.

The sequence numbers for the first segments in the TCP connect sent from the client to the web server is 232129013.
The time it was sent is 0.026477
The ACK for this segment is received at 0.053937
The RTT value is 0.02746
The EstimatedRTT value after the receipt of this ACK is 0.02746

The sequence numbers for the second segments in the TCP connect sent from the client to the web server is 23219578
The time it was sent is 0.041737
The ACK for this segment is received at 0.077294
The RTT value is 0.035557
The EstimatedRTT value after the receipt of this ACK is 0.028472125

The sequence numbers for the third segments in the TCP connect sent from the client to the web server is 232131038
The time it was sent is 0.054026
The ACK for this segment is received at 0.124085
The RTT value is 0.070059
The EstimatedRTT value after the receipt of this ACK is 0.03367048

The sequence numbers for the fourth segments in the TCP connect sent from the client to the web server is 232132498
The time it was sent is 0.054690
The ACK for this segment is received at 0.169118
The RTT value is 0.114428
The EstimatedRTT value after the receipt of this ACK is 0.43765174

The sequence numbers for the fifth segments in the TCP connect sent from the client to the web server is 232133958
The time it was sent is 0.077405
The ACK for this segment is received at 0.217299
The RTT value is 0.139894
The EstimatedRTT value after the receipt of this ACK is 0.0557812771

The sequence numbers for the sixth segments in the TCP connect sent from the client to the web server is 232135418
The time it was sent is 0.078157
The ACK for this segment is received at 0.267802
The RTT value is 0.189645
The EstimatedRTT value after the receipt of this ACK is 0.07251424

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

Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection and not consider the ACKs received from the server as part of these six segments
Then length of the first TCP segment is 619

Then length of the second TCP segment is 1514

Then length of the third TCP segment is 1514

Then length of the fourth TCP segment is 1514

Then length of the fifth TCP segment is 1514

Then length of the sixth TCP segment is 1514

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?

The minimum amount of available buffer space advertised at the receiver for the entire trace is 5840, which is shown in the first ACK from receiver.

The lack of receiver buffer space never 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 segment in the trace file. I checked the sequence number to answer this question. Since the sequence numbers keep increasing without repeat, I think there is no retransmitted segment.

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 receiver typically acknowledge 1460 bytes since we can see that, normally, the ACK numbers increase 1460 each time.

The receiver is ACKing every other segment. Since the delayed ACK normally ACKs every other segment, we can identify these cases by compare the ACK numbers of 2 consecutive ACKs.

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

The throughput for the TCP connection is about 23173.30. I calculated this by first find the difference between the ACK number of the last ACK and the sequence number of the segment contain the HTTP POST, and then find the time used after the HTTP post to the last ACK, and finally divide these two value to calculate the throughput

Exercise 2: TCP Connection Management

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?

The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server is 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?

The SYNACK segment sent by the server to the client computer in reply to the SYN is 1247095790.

The value of the Acknowledgement field in the SYNACK segment is 2818463619.

The server determine that value by adding 1 to the initial sequence number of SYN segment from the client computer.

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?

The sequence number of the ACK segment sent by the client computer in response to the SYNACK is 2818463619.

The Acknowledgement field value in this ACK segment is 1247095791.

This segment does not contain any 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 active close is done by both client and server.

According to the segment 304 and 605, since the client send a FINACK segment with same sequence number as the ACK number of server's FINACK segment, and the ACK number of the client's FINACK segment is same as the sequence number of the server's FINACK segment.

The type of closure been performed is Simultaneous close.

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?

During the whole duration of the connection (including the close phrase), 35 bytes have been transferred from the client to the server and 42 bytes have been transferred from the server to the client.
These are calculated by find the difference between the Initial Sequence Number and the ACK number of the final ACK received from the other side.