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 is 129.119.245.12

Port number is 80

The IP address that using by Client computer is 192.168.1.102

And port number is 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.

The number is 232129013

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.

According to the question, the HTTP POST is considered as the first segment, so the first six segments is No. 4,5,7,8,10,11 in this trace,

Segment 1 seq-num:232129013

Segment 2 seq-num:232129578

Segment 3 seq-num:232131038

Segment 4 seq-num:232132498

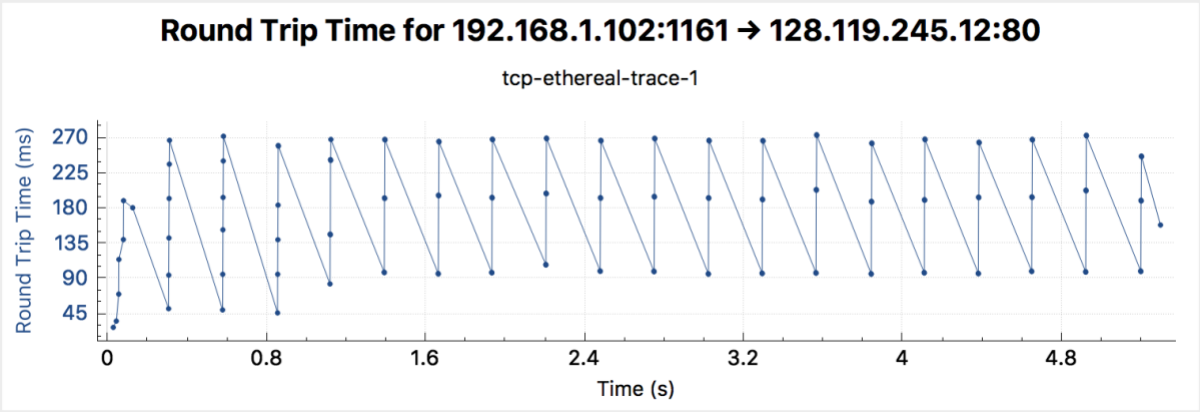
Segment 5 seq-num:232133958

Segment 6 seq-num:232135418

The sending time and received time of ACKs

	send time	ACK received	RTT
seg1	0.026477	0.053937	0.02746
seg2	0.041737	0.077294	0.035557
seg3	0.054026	0.124085	0.070059
seg4	0.05469	0.169118	0.114428
seg5	0.077405	0.217299	0.139894
seg6	0.078157	0.267802	0.189645

Formular:
EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT
No.1 EstimatedRTT = 0.02746
No.2 EstimatedRTT =0.875*0.02746 + 0.125*0.03557 = 0.0285
No.3 EstimatedRTT = 0.875*0.0285 + 0.125*0.070059 =0.0337
No.4 EstimatedRTT = 0.875 * 0.0337+ 0.125 * 0.114428 = 0.0438
No.5 EstimatedRTT = 0.875 * 0.0438 + 0.125 * 0.139894 = 0.0558
No.6 EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.189645 = 0.0725



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

The first segment length is 565bytes and the rest of segments length are all 1460bytes

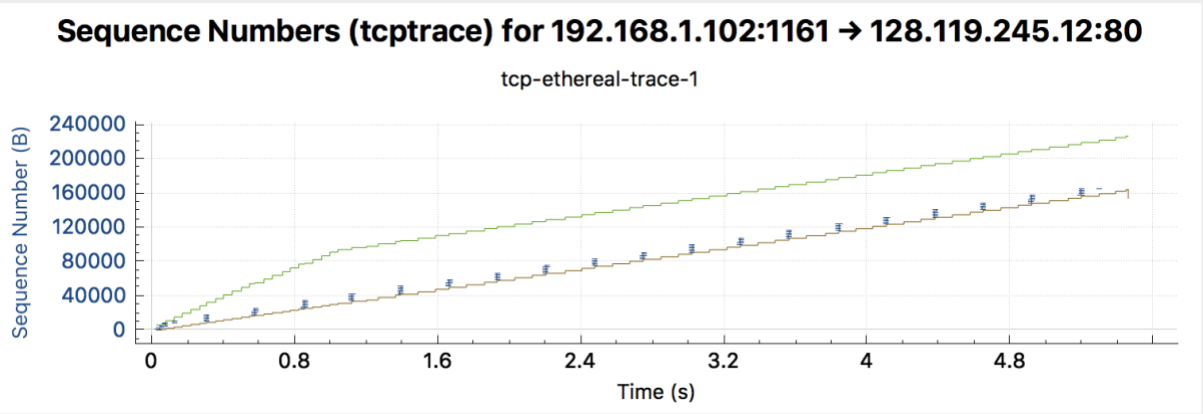
Question 5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

The minimum amount of available buffer space advertised at gaia.cs.umass.edu is 5840bytes

```
Window size value: 5840
[Calculated window size: 5840]
```

No the window size grows large enough early on to avoid any throttling.

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?



No, according to the sequence number show in the graph above, there are no duplicates in sequence numbers for any packets(straight line).

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).

From Payload of the TCP we can see that receiver typically ACKS 1460bytes of data

```
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)
```

#The receiver is ACKing every other segment for example for segment of No. 80 acknowledged data with 2920 bytes = 1460*2 bytes.

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

In this question, we need to know the average time period and total amount data that had been transmitted , I select the average time as whole connection time, therefore, the throughput is the ratio of the total amount of data / the time

The first segment seq number(4th) is 232129013

The last segment seq number(202th) is 232293103

The difference between the first and the last is 164090

0.026477 second for No.4 segment
5.455830 second for No. 202 segment
The difference between the first and the last time is 5.4294
Hence , 164090/5.4294 = 30.222Kbyte/sec

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 is 2818463618.

the SYN flag is set to 1 and it indicates that this segment is a SYN segment and indicated that the client wants to connect with server.

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 sequence number is 1247095790.

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

By adding 1 to the initial seq-number of SYN segment from the client.

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 is 2818463619

The value of the Acknowledgement field in the SYNACK segment is 1247095791.

No,it not contain any data(except data in header).

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?

Both(client and server) has done the active close.

This can be determined by the segment No.304.the server do not close when client send fin = 1 to the server, it just tell the server that client want to close, and server will wait until all the data been transmitted, then server will send Fin = 1 to the client, when server receive the reply of ACK, all the resource will be released and system will shuts down, hence, client initiated close procedure.

This 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?

No.298 segment 33bytes data transferred from client to server

No.302 segment 40bytes data transferred from client to server

Totally,73bytes data transferred from the client to server.

Date transferred equal to the difference of the initial sequence number and the final ACK received from the other side.