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?

Q1 :

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

Port Number: Destination Port: 80

Client computer (source): IP address (Source): 192.168.1.102;

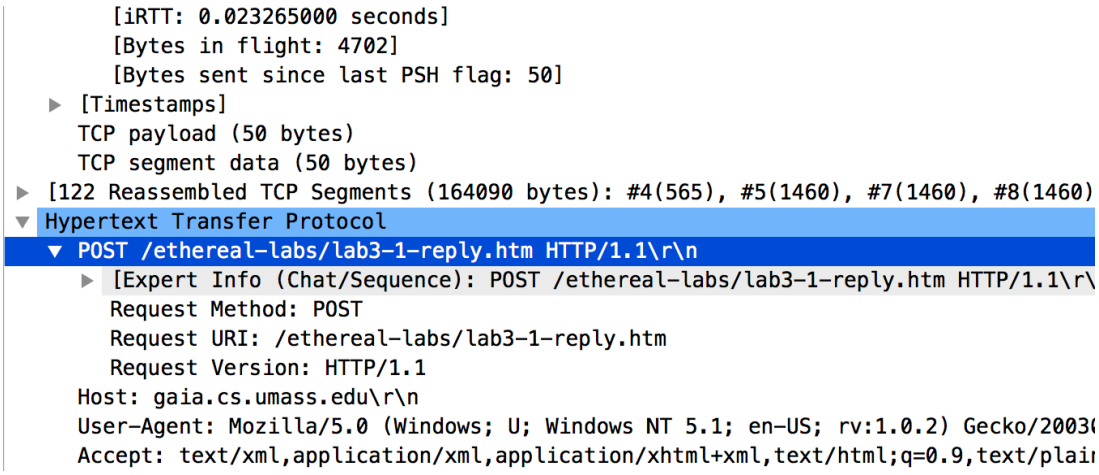
TCP port number: Source Port: 1161

Using port number 1161 and 80 sending and receiving TCP segments.

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.

Q2 :

The sequence number of the TCP segment containing the HTTP POST command: 232293053.



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.

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

Q3、Q4：

Segment number	Sequence number	Send Time(seconds)	ACK receive time	RTT (seconds)	EstimatedRTT (seconds)	Segment length
4	232129013	0.026477	0.053937	0.02764	0.02764	565
5	232129578	0.041737	0.077294	0.035557	0.0285	1460
7	232131038	0.054026	0.124085	0.070059	0.0337	1460
8	232132498	0.054690	0.169118	0.11443	0.0438	1460
10	232133958	0.077405	0.217299	0.13989	0.0558	1460
11	232135418	0.078157	0.267802	0.18964	0.0725	1460

EstimatedRTT = (1-a) * EstimatedRTT + a * SampleRTT

EstimatedRTT(1) = 0.02764

EstimatedRTT(2) =0.875 * 0.02764 + 0.125 * 0.035557 = 0.0285

EstimatedRTT(3) = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337

EstimatedRTT(4) = 0.875 * 0.0337 + 0.125 * 0.11443 = 0.0438

EstimatedRTT(5) = 0.875 * 0.0438 + 0.125 * 0.138989 = 0.0558

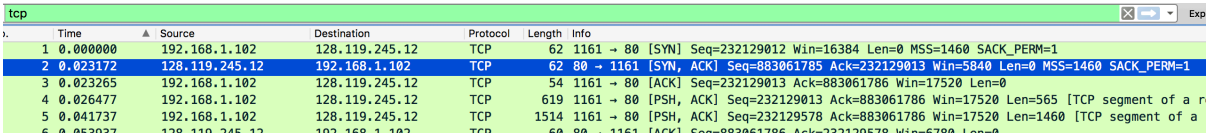
EstimatedRTT(6) = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725

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?

Q5:

The minimum amount of buffer space (receiver window) advertised at gaia.cs.umass.edu for the entire trace is 5840 bytes, which shows in the first acknowledgement from the server.

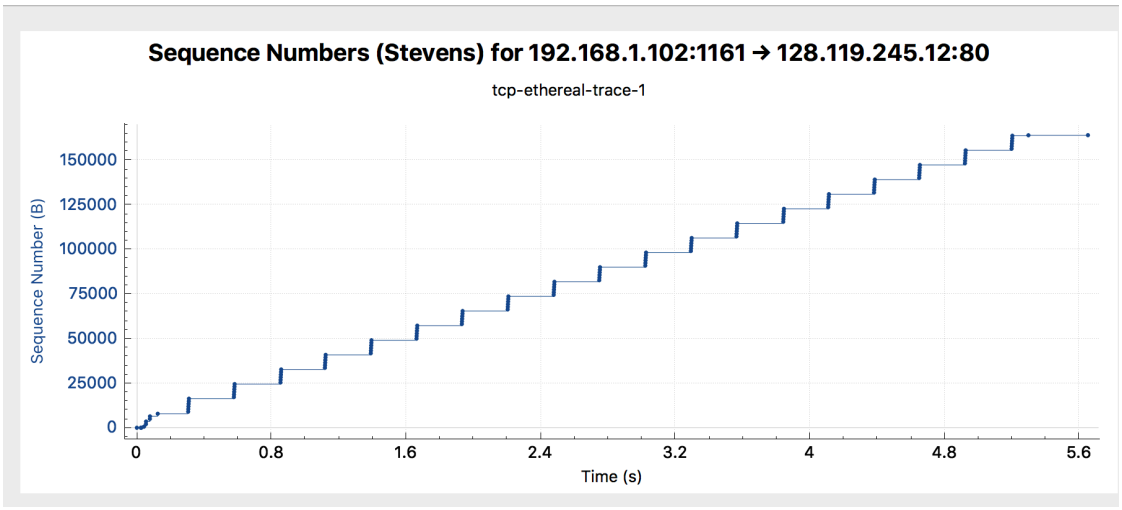
The sender never throttled because receiver buffer space in this case is always lager than segment size.



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?

Q6:

There are no retransmitted segments in the trace file. In the Time-Sequence-Graph, all sequence numbers from the source (192.168.1.102) to the destination (128.119.245.12) are increasing monotonically. If there is a retransmitted segment, the sequence number of this retransmitted segment should be smaller than those of its neighboring segments.



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).

Q7 :

Most of them acknowledged 1460 bytes. So the receiver typically acknowledge in an ACK is 1460 bytes.

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. The amount of acknowledged data by each ACK for example:

Ack no.6: 232129578

Ack no.9: 232131038

232131038 – 232129578 = 1460 it reflects the receiver is ACKing the segment no.5 length = 1460.

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

Q8：

TCP throughput can be calculated by the total data and the total transmission time, because R=total data/ total time. This result can be selected as bytes transferred per unit time for the TCP connection.

Total length : The last ACK number (no.202 segment) = 232293103 – the first TCP segment (no.4) = 232129013.

So the total content length = 164090 bytes

The total transmission time = The last ACK time (no.202 segment) = 5.455830 – the first TCP segment time (no.4) = 0.026477.

So the total time = 5.429353 s

Throughput R = 1654090/5.429353 = 30222.75 bytes/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?

Q1：

Sequence number of SYN segment: 2818463618 to initiate the TCP connection.

The SYN flag is set to 1.

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?

Q2：

Sequence number of SYNACK segment: 1247095790

the Acknowledgement field: 2818463619

The value of the Acknowledgement flag in the SYNACK segment: 1

It is determined by the server add 1 to the initial sequence number of SYN segment from client computer (2818463618 + 1 = 2818463619).

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?*

Q3：

The sequence number of the ACK segment: 2818463619

the Acknowledgement field: 1247095791

The value of the Acknowledgement flag in this ACK segment is:1.
(1247095790+1=1247095791)

It doesn't contain any payload/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?*

Q4 :

Both Client and Server active the close.

It can be determined by the segment 304 and 305. Both client and server send a segment with FIN flag and ACK.

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?*

Q5 :

Client to the Server:

The last ACK segment sequence number =2818463652

The first ACK segment sequence number =2818463619

So total data bytes = 2818463652 – 2818463619 = 33 bytes.

Server to the Client:

The last ACK segment ACK number = 1247095831

The first ACK segment ACK number = 1247095791

So total data bytes = 1247095832 – 1247095791 = 40 bytes.

Data transferred equal to the difference between the initial sequence number and the final ACK segment from the other side.