COMP9331 – Lab4

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 are the IP address and TCP port numbers used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

1	0.000000	192.168.1.102	128.119.245.12	TCP	62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

Answer: The IP address of gaia.cs.umass.edu is *128.119.245.12* using port number *80*. The IP address used by the client computer is *192.168.1.102* using port number *1161*.

Question 2. What is the sequence number of the TCP segment containing the HTTP POST command? (Note that 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.)

4	0.026477	192.168.1.102	128.119.245.12	TCP	619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TC
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP

```
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 565]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 232129013
[Next Sequence Number: 566    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 883061786
```

Answer: The Sequence number is 1.

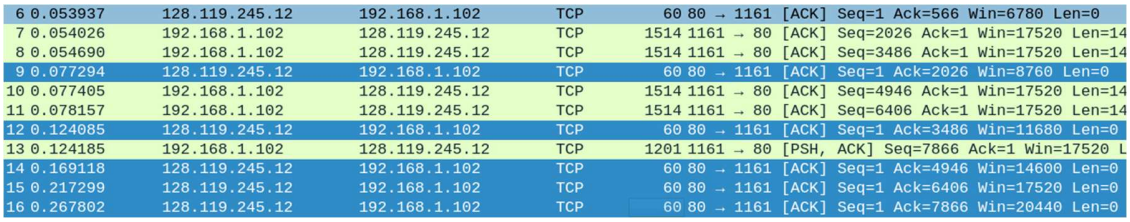
Question 3. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection.

(a) 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 webserver (Do not consider the ACKs received from the server as part of these six segments)?

4	0.026477	192.168.1.102	128.119.245.12	TCP	619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

Answer: The Sequence numbers are 1(4), 566(5), 2026(7), 3486(8), 4946(10), 6406(11).

(b) 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?



6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=14
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=14
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=14
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=14
12	0.124085	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 L
14	0.169118	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0

Answer: The time sent is 0.026477, 0.041737, 0.054026, 0.054690, 0.077405, and 0.078157 seconds. The ACKs were received at 0.053937(6), 0.077294(9), 0.124085(12), 0.169118(14), 0.217299(15), and 0.267802(16) seconds. Thus, the RTTs are 0.027460, 0.035557, 0.070059, 0.114428, 0.139894, and 0.189645 seconds.

Client -> Web Server				
Segment	Sequence	Time(sec)	ACKs	RTT(sec)
1	1	0.026477	1 + 565 = 566	0.053937 - Time[0] = 0.02746
2	566	0.041737	566 + 1460 = 2026	0.077294 - Time[1] =0.035557
3	2026	0.054026	2026 + 1460 = 3486	0.124085 - Time[2]= 0.070059
4	3486	0.054690	3486 + 1460 = 4946	0.169118 - Time[3]= 0.114428
5	4946	0.077405	4946 + 1460 = 6406	0.217299 - Time[4]= 0.139894
6	6406	0.078157	6406 + 1460 = 7866	0.267802 - Time[5]= 0.189645

(c) What is the EstimatedRTT value (see relevant parts of Section 3.5 or lecture slides) after receiving 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 TCP segment 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.)

Answer: Estimated RTT(sec) are:

Segment 1 -> (1-0.125) * 0.02746 + 0.125 * 0.02746 = 0.02746

Segment 2 -> (1-0.125) * 0.02746 + 0.125 * 0.035557 = 0.02847

Segment 3 -> (1-0.125) * 0.02847 + 0.125 * 0.070059 = 0.03367

Segment 4 -> (1-0.125) * 0.03367 + 0.125 * 0.114428 = 0.04376

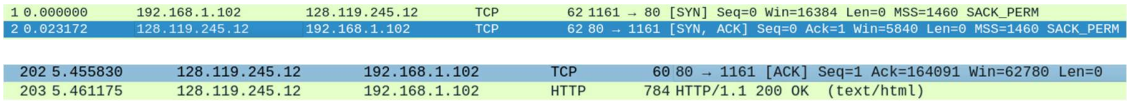
Segment 5 -> (1-0.125) * 0.04376 + 0.125 * 0.139894 = 0.05578

Segment 6 -> (1-0.125) * 0.05578 + 0.125 * 0.189645 = 0.07251

(d) What is the length of each of the first six TCP segments?

Answer: The length is 565, 1460, 1460, 1460, 1460, and 1460 bytes from segment 1 to 6.

Question 4. 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?

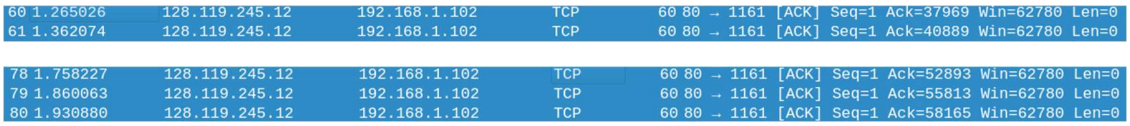


Answer: The minimum amount of available buffer space advertised to the receiver is 5840 bytes. The receive window grows steadily until it reaches the maximum receive buffer size of 62780 bytes. Examining this trace, you can see that the sender is never throttled by insufficient receive buffer space.

Question 5. Are there any retransmitted segments in the trace file? To answer this question, what did you check for (in the trace)?

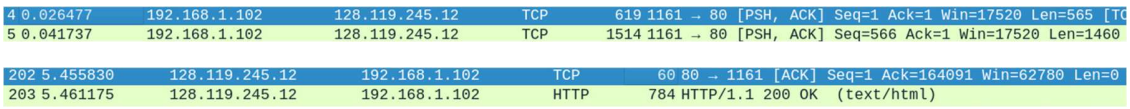
Answer: There are no retransmitted segments in the trace file. I sorted the sources into ascending orders and checked the sequence numbers, or prompt with *tcp.analysis.retransmission* in Wireshark, but it returned no results.

Question 6. 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)?



Answer: The receiver typically acknowledged data in an ACK is 1460 bytes. But there are other cases where the receiver is ACKing every other segment data with 2920 bytes = 1460*2 bytes.

Question 7. What is the TCP connection's throughput (bytes transferred per unit of time during the connection)?



Answer: 30222.7539819 bytes/second

Total amount of data = 164091 – 1 = 164090 bytes (D)

Total transmission time = 5.455830– 0.026477 = 5.429353 seconds. (T)

The throughput = D/T = 164090/5.429353 = 30222.75398 bytes/second.

Exercise 2: TCP Connection Management

Consider the following TCP transaction between a client (10.9.16.201) and a server (10.99.6.175).

No	Source IP	Destination IP	Protocol	Info
295	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [SYN] Seq=2818463618 win=8192 MSS=1460
296	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [SYN, ACK] Seq=1247095790 Ack=2818463619 win=262144 MSS=1460
297	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463619 Ack=1247095791 win=65535
298	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [PSH, ACK] Seq=2818463619 Ack=1247095791 win=65535
301	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [ACK] Seq=1247095791 Ack=2818463652 win=262096
302	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [PSH, ACK] Seq=1247095791 Ack=2818463652 win=262144
303	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463652 Ack=1247095831 win=65535
304	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [FIN, ACK] Seq=2818463652 Ack=1247095831 win=65535
305	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [FIN, ACK] Seq=1247095831 Ack=2818463652 win=262144
306	10.9.16.201	10.99.6.175	TCP	50045 > 5000 [ACK] Seq=2818463652 Ack=1247095832 win=65535
308	10.99.6.175	10.9.16.201	TCP	5000 > 50045 [ACK] Seq=1247095831 Ack=2818463653 win=262144

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?

Answer: The sequence number 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?

Answer: The sequence number is *1247095790* and the ACK is *2818463619*, determined by the sequence number from the client plus 1 byte.

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?

Answer: The sequence number is *2818463619*. The acknowledgment is *1247095791* and this segment doesn't contain any data.

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

Answer: Both sides have done the active close since the client and the server started sending the TCP segment with the FIN bit. Thus, it is a simultaneous Closure with ACK from both sides after the FIN bit segments.

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?

Answer: Data from client -> server = 2818463653 – 2818463618 – 2 = 33 bytes; Data from server -> client = 1247095832 – 1247095790 – 2 = 40 bytes; the relationship is that the difference between the initial sequence number and the final ACK received from the other side minus bits from SYN and FIN.