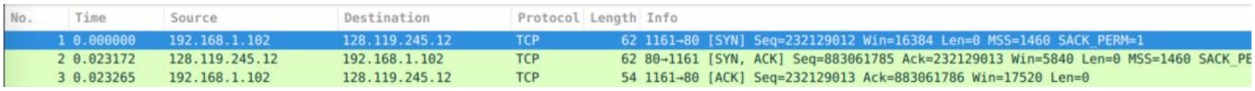
Z5187469
Yiyun Yang

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 is 128.119.245.12 and port number is 80.

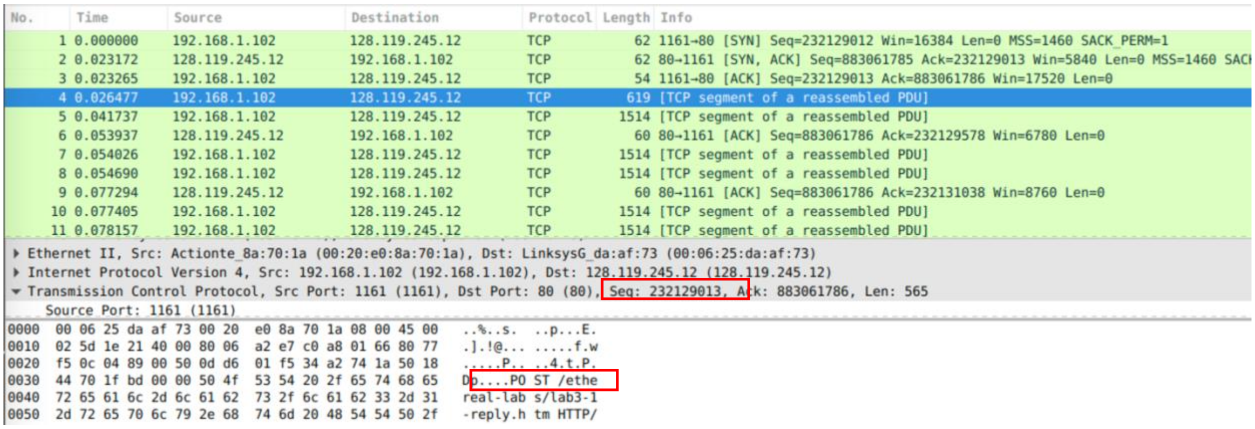
The IP address of the client is 192.168.1.102 and port number is 1161.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161→80 [SYN] Seq=232129012 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80→1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=5840 Len=0 MSS=1460 SACK_PE
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161→80 [ACK] Seq=232129013 Ack=883061786 Win=17520 Len=0

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 is 232129013.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161→80 [SYN] Seq=232129012 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80→1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=5840 Len=0 MSS=1460 SACK
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161→80 [ACK] Seq=232129013 Ack=883061786 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	[TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80→1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80→1161 [ACK] Seq=883061786 Ack=232131038 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]

```
▸ Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▸ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
▾ Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 232129013, Ack: 883061786, Len: 565
    Source Port: 1161 (1161)
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ..%..s.  ..p...E.
0010  02 5d 1e 21 40 00 80 06  a2 e7 c0 a8 01 66 80 77   .].!@... .....f.w
0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   .....P.. ..4.t.P.
0030  44 70 1f bd 00 00 50 4f  53 54 20 2f 65 74 68 65   Dp....PO ST /ethe
0040  72 65 61 6c 2d 6c 61 62  73 2f 6c 61 62 33 2d 31   real-lab s/lab3-1
0050  2d 72 65 70 6c 79 2e 68  74 6d 20 48 54 54 50 2f   -reply.h tm HTTP/
```

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 sequence number of first six segments are 232129013, 232129578, 232131038, 232132498, 232133958, 232135418. They are sent on 0.026477, 0.041737, 0.054026, 0.054690, 0.077405, 0.078157. To get the time when the ACK for each segment is received, we add the length of segment to the sequence number and find the one with that ACK number.

For segment 1, ACK = 232129013 + 565 = 232129578 → No.6, T = 0.053937

For segment 2, ACK = 232129578+ 1460 = 232131038 → No.9, T = 0.077294

For segment 3, ACK = 232131038+ 1460 = 232132498 → No.12, T = 0.124085

For segment 4, ACK = 232132498+ 1460 = 232133958→ No.14, T = 0.169118

For segment 5, ACK = 232133958+ 1460 = 232135418→ No.15, T = 0.217299

For segment 6, ACK = 232135418+ 1460 = 232136878 → No.16, T = 0.267802

To calculate the RTT, we find the difference of the time we got.

For segment 1, RTT = 0. 053937 – 0.026477 = 0.027460

For segment 2, RTT = 0. 077294– 0. 041737= 0.035557

For segment 3, RTT = 0. 124085– 0. 054026= 0.070059

For segment 4, RTT = 0. 169118– 0. 054690= 0.114428

For segment 5, RTT = 0. 217299– 0. 077405= 0.139894

For segment 6, RTT = 0. 267802– 0. 078157= 0.189645

$$\text{EstimatedRTT}=(1-\alpha)\,\text{EstimatedRTT}+\alpha\ \text{SampleRTT}$$

For segment 1, EstimatedRTT = (1 – 0.125) * 0. 027460 + 0.125 * 0. 027460 = 0. 027460

For segment 2, EstimatedRTT = (1 – 0.125) * 0. 027460 + 0.125 * 0. 035557= 0. 028472

For segment 3, EstimatedRTT = (1 – 0.125) * 0. 028472+ 0.125 * 0. 070059= 0. 033670

For segment 4, EstimatedRTT = (1 – 0.125) * 0. 033670+ 0.125 * 0. 114428= 0. 043765

For segment 5, EstimatedRTT = (1 – 0.125) * 0. 043765 + 0.125 * 0. 139894= 0. 055781

For segment 6, EstimatedRTT = (1 – 0.125) * 0. 055781 + 0.125 * 0. 189645= 0. 072514

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

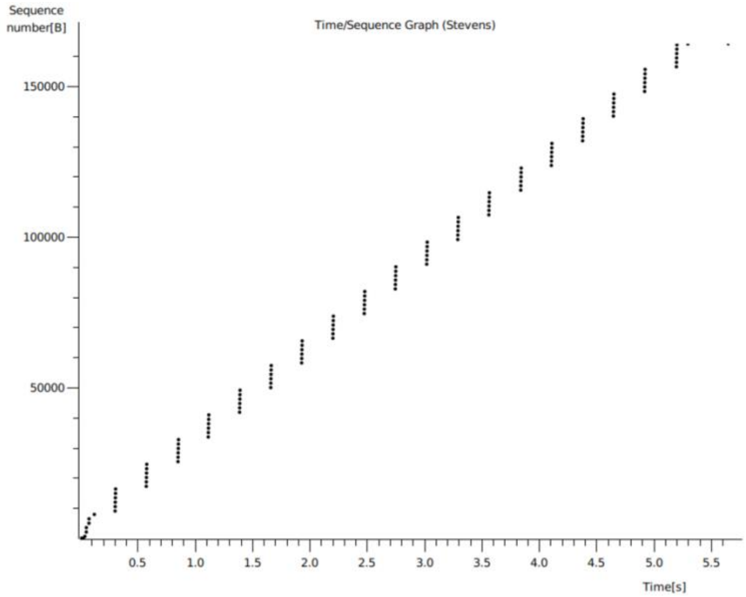
The length of the first segment is 565 and the rest are 1460.

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?**

As the window size keeps increasing during the whole connection, the minimum window size at receiver is 5840. The lack of receiver buffer space does not throttle the sender as the window size does not decrease significantly.

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?

From the time/sequence gragh, we can see that the sequence number increases during the connection and there is no duplicate of the sequence number, thus there is no retransmitted segments in the trace file.



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 data is 1460 bytes most of the time.

The receiver is ACKing every other received segment such as in segment No. 59 and No.60, we can see the ACK is 232164061 and 232166981, the difference of ACKs is double of 1460. This is because TCP uses delayed ACKs where the receiver waits for the arrival of another in-order segment and then sends a cumulative ACK for both of the received segments. Since this point, we can see several other cases where the receiver sends an ACK for every other received segment.

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

The throughput is equal to total number of bytes sent / total transmission time.

The total number of bytes sent is last ACK from server – the sequence number of the first segment from the client = 232293103 – 232129013 = 164090 bytes.

The total transmission time = 5.455830 – 0.026477 = 5.429353 sec

Thus the throughput = 164090/5.429353 = 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?
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 sequence number of the SYNACK segment is 1247095790. The value of acknowledgement field is 2818463619 which is adding 1 to the sequence number, as SYN is 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?
The sequence number is 2818463619, the value of acknowledgement field is 1247095791, which 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?
Both the client and server has done the active close, as they sent FINACK at almost the same time. Simultaneous close has been performed.

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?
From client to server, 2818463653 – 2818463618 – 2*(SYN + FIN) = 35 – 2 = 33 bytes.
From server to client, 1247095832 – 1247095790 – 2*(SYN + FIN) = 42 – 2 = 40 bytes.
The final ACK received is equal to the initial sequence number plus number of bytes of the data transferred plus 2 which is 1 byte of SYN and 1 byte of FIN sent(SYN and FIN message have no real data).