

Student ID: z5195715

Name: Junyu Ren

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

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_PERM=1
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	1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 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=232129578 Ack=883061786 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=883061786 Ack=232129578 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 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=232132498 Ack=883061786 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=883061786 Ack=232131038 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 232129012, Len: 0
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 232129012
[Next sequence number: 232129012]
Acknowledgment number: 0
0111 = Header Length: 28 bytes (7)
> Flags: 0x002 (SYN)

IP address of gaia.cs.umass.edu is 128.119.245.12. Port number is 80.

IP address of client is 192.168.1.102. 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 Wireshark window, looking for a segment with a "POST" within its DATA field.

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_PERM=1
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	1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 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=232129578 Ack=883061786 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=883061786 Ack=232129578 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 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=232132498 Ack=883061786 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=883061786 Ack=232131038 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 232129013, Ack: 883061786, Len: 565
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 565]
Sequence number: 232129013
[Next sequence number: 232129578]
Acknowledgment number: 883061786
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P...A.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 50 2f -reply.htm HTTP/
0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 1.1.Hos t: gaia.
0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 55 73 cs.umass .edu..Us
0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0090 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 a/5.0 (w indows;
00a0 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e U; Windo ws NT 5.
00b0 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 30 1; en-US ; rv:1.0
00c0 2e 32 20 20 47 65 63 6b 6f 2f 32 30 33 30 32 .2) Gecko o/200302
00d0 30 3b 20 4e 65 74 73 63 61 70 65 2f 37 2e 30 32 00 Netsc ape/7.02
00e0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78 ..Accept : text/x

Sequence number of TCP segment containing HTTP POST command 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.

In this case, Estimated RTT = 0.875 * Estimated RTT + 0.125 * Sample RTT.

All results are listed in the table below.

Sequence Number	Time sent	Time ACK received	Sample RTT	Estimated RTT
232129013	0.026477	0.053937	0.027460	0.027460
232129578	0.041737	0.077294	0.035557	0.028472
232131038	0.054026	0.124085	0.070059	0.033670
232132498	0.054690	0.169118	0.114428	0.043765
232133958	0.077405	0.217299	0.139894	0.055781
232135418	0.078157	0.267802	0.189645	0.072514

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

Length of 1st segment:565 bytes, 2nd:1460 bytes, 3rd:1460 bytes,
4th:1460 bytes, 5th:1460 bytes, 6th:1460 bytes.

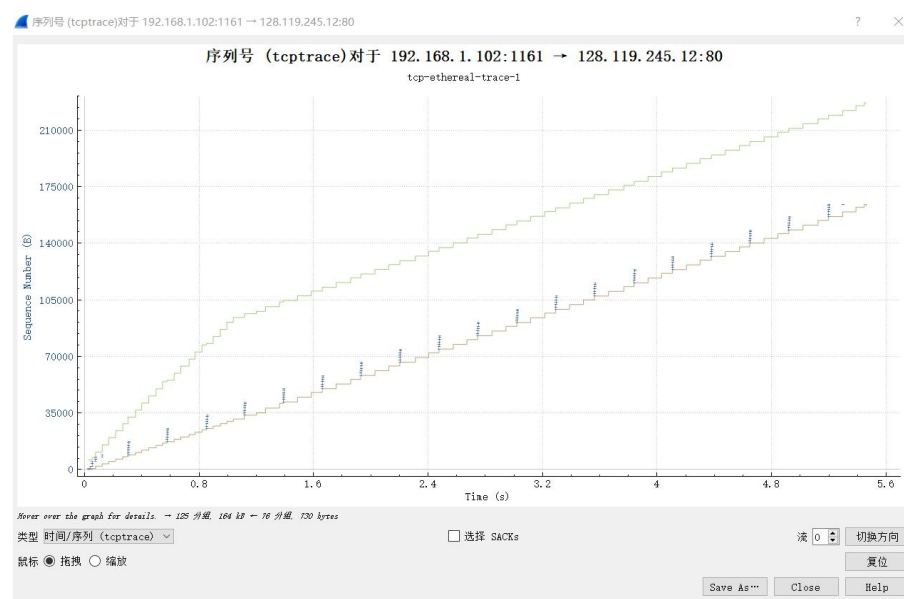
Question 5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

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_PERM=1
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80	[ACK]	Seq=232129013	Ack=883061786	Win=17520	Len=0		
50	0.994715	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK]	Seq=883061786	Ack=232158789	Win=61320	Len=0		
51	1.039820	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK]	Seq=883061786	Ack=232160249	Win=62780	Len=0		
52	1.117097	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK]	Seq=883061786	Ack=232162601	Win=62780	Len=0		

Minimum amount of available buffer space advertised at receiver for the entire trace is 5840 byte.

No,it doesn't.Because in this example, buffer space is greater than size of sender segments.The receiver window size is very large (maximum 62780 bytes).

Question 6. Are there any re-transmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?



No re-transmission happened in this file.

If there are duplicate sequence numbers at different times means re-transmission. But i can't find any in the 'sequence number & time' graphs. The 2 graphs both show that the seq no. strictly increases as time increases.

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 of data.

72	1.661734	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK] Seq=232178985 Ack=883061786 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
73	1.662474	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK] Seq=232180445 Ack=883061786 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
74	1.663315	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK] Seq=232181905 Ack=883061786 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
75	1.664198	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK] Seq=232183365 Ack=883061786 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
76	1.665254	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK] Seq=232184825 Ack=883061786 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
77	1.666151	192.168.1.102	128.119.245.12	TCP	946	1161 → 80	[PSH, ACK] Seq=232186285 Ack=883061786 Win=17520 Len=892	[TCP segment of a reassembled PDU]
78	1.758227	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK] Seq=883061786 Ack=232181905 Win=62780 Len=0	

Above is one of this example. In line 72,73 and 78: Since $232181905 = 232178985 + 1460 + 1460$, the ACK for seq no.232178985 is delayed or lost and the receiver directly sends ACK 232181905 to tell the sender it successfully receive segments with seq no.232178985 and seq no.232180445.

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

Throughput = total amount of data / total transfer time.

No.	Time	Source	Destination	Protocol	Length	Info
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232293053 Win=62780 Len=0
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232293103 Win=62780 Len=0
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
204	5.598090	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
205	5.599082	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232293103 Ack=883062516 Win=16790 Len=0
207	6.101044	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
208	6.102069	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
209	6.600152	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
210	6.601063	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1

> Frame 202: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 > Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
 v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 883061786, Ack: 232293103, Len: 0
 Source Port: 80
 Destination Port: 1161
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 883061786
 [Next sequence number: 883061786]
 Acknowledgment number: 232293103
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)

From above,we know that $232293103 - 232129013 = 164090$ bytes of data is already transferred.

Total transfer time = end - start = 5.45583 - 0.026477 = 5.429353 s

So, Throughput = $164090 \text{ byte} / 5.429353 \text{ s} = 30222.75398 \text{ byte/s}$

Exercise 2: TCP Connection Management

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?

Seq no. of SYN 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?

Seq no. of SYNACK is 1247095790

Value of Ack field is 2818463619

This value is get from initial sequence number(ISN) + 1.

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?

Seq no in response to SYNACK is 2818463619

Value of Ack field is 1247095791

It doesn't contain any data.Because segment No.298 use the same sequence number as No.297.

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 have done active close.It is a Simultaneous close because No.304 and No.305 both send 'FIN ACK' flags.No.305 ack = No.304 seq no and No.304 ack = No.305 seq no,which means the ack is not added by 1 after a FIN received. So, the 2 'FIN ACK' send and close

both sides at the same time.

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?

Client ISN = 2818463618

Final ACK from server = 2818463653

$\text{Data_transfer_from_client_to_server} = \text{final ACK from server} - \text{client ISN} - 2(1 \text{ for SYN and } 1 \text{ for FIN}) = 33 \text{ bytes}$

Server ISN = 1247095790

Final ACK from client = 1247095832

$\text{Data_transfer_from_server_to_client} = \text{final ACK from client} - \text{server ISN} - 2(1 \text{ for SYN and } 1 \text{ for FIN}) = 40 \text{ bytes}$

General relationship:

$\text{Data_transfer_from_A_to_B} = \text{final ACK from B} - \text{ISN_A} - 2$

$\text{Data_transfer_from_B_to_A} = \text{final ACK from A} - \text{ISN_B} - 2$