

Arthur Liou
CS372
Lab 3

Notes: I've attached my screenshots and boxed in red where I annotated my output.

1. 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? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows).

IP Address/TCP Port number:

192.168.1.102:1161

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

IP Address/TCP Port Number

128.119.245.12:80

For Q1-2

The screenshot shows a Wireshark packet capture titled "tcp-ethereal-trace-1". The packet list pane displays 20 packets. Packet 1 is a SYN packet from 192.168.1.102 to 128.119.245.12 on port 80. The packet details pane shows the following information:

- 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: LinksysG_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: 0, Len: 0
 - Source Port: 1161
 - Destination Port: 80
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - [Next sequence number: 0 (relative sequence number)]
 - Acknowledgment number: 0
 - 0111 = Header Length: 28 bytes (7)
 - Flags: 0x002 (SYN)
 - Window size value: 16384
 - [Calculated window size: 16384]
 - Checksum: 0xf6e9 [unverified]
 - [Checksum Status: Unverified]

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header.

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
172.20.4.134:57151

For Q3

No.	Time	Source	Destination	Protocol	Length	Info
23	1.481119	172.20.4.134	128.119.245.12	TCP	78	57151 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460
24	1.482055	172.20.4.134	128.119.245.12	TCP	78	57152 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460
33	1.477100	128.119.245.12	172.20.4.134	TCP	74	80 → 57151 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0
34	1.477156	172.20.4.134	128.119.245.12	TCP	66	57151 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=827
35	1.477366	128.119.245.12	172.20.4.134	TCP	74	80 → 57152 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0
36	1.477398	172.20.4.134	128.119.245.12	TCP	66	57152 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=827
37	1.477428	172.20.4.134	128.119.245.12	TCP	740	57151 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=674 TSval=827
38	1.477477	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=675 Ack=1 Win=131712 Len=1448 TSval=827
39	1.477478	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=2123 Ack=1 Win=131712 Len=1448 TSval=827
41	1.553054	128.119.245.12	172.20.4.134	TCP	66	80 → 57151 [ACK] Seq=1 Ack=675 Win=38336 Len=0 TSval=4
42	1.553057	128.119.245.12	172.20.4.134	TCP	66	80 → 57151 [ACK] Seq=1 Ack=2123 Win=33280 Len=0 TSval=4
43	1.553154	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=3571 Ack=1 Win=131712 Len=1448 TSval=827
44	1.553155	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=5919 Ack=1 Win=131712 Len=1448 TSval=827
45	1.553156	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=6467 Ack=1 Win=131712 Len=1448 TSval=827
46	1.553528	128.119.245.12	172.20.4.134	TCP	66	80 → 57151 [ACK] Seq=1 Ack=3571 Win=36224 Len=0 TSval=4
47	1.553566	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=7915 Ack=1 Win=131712 Len=1448 TSval=827
48	1.553567	172.20.4.134	128.119.245.12	TCP	1514	57151 → 80 [ACK] Seq=9363 Ack=1 Win=131712 Len=1448 TSval=827
49	1.598436	34.197.200.72	172.20.4.134	TCP	66	443 → 57128 [FIN, ACK] Seq=1 Ack=1 Win=114 Len=0 TSval=827
50	1.598442	34.197.200.72	172.20.4.134	TCP	66	443 → 57129 [FIN, ACK] Seq=1 Ack=1 Win=114 Len=0 TSval=827
51	1.598558	172.20.4.134	34.197.200.72	TCP	66	57128 → 443 [ACK] Seq=1 Ack=2 Win=2847 Len=0 TSval=827

Frame 23: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: Apple_C9:51:aa (8c:85:9b:c9:51:aa), Dst: CiscoMer_4e:d9:14 (00:18:0a:4e:d9:14)
Internet Protocol Version 4, Src: 172.20.4.134, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57151, Dst Port: 80, Seq: 0, Len: 0
Source Port: 57151
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1011 = Header Length: 44 bytes (11)
Flags: 0x02 (SYN, ECN, CWR)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x4d09 [unverified]
[Checksum Status: Unverified]
0000 00 18 0a 4e d9 14 8c 85 9b c9 51 aa 00 00 45 00 ... N ... Q ... E ...
0010 00 40 00 00 00 00 00 00 14 9a ac 14 04 05 00 77 ... @ ... @ ... W ...
0020 f5 0c df 3f 00 50 2e 4d b5 a9 00 00 00 00 b0 c2 ... ? P M ...
0030 ff ff 4d 09 00 00 02 04 05 b4 01 03 06 01 01 ... M ...
0040 08 0a 0a ee fa 9f 00 00 00 04 02 00 00 ...

Using tcp-ethereal-trace-1

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Sequence Number 1. Under Flags, the SYN flag is set to 1/True.

For Q4

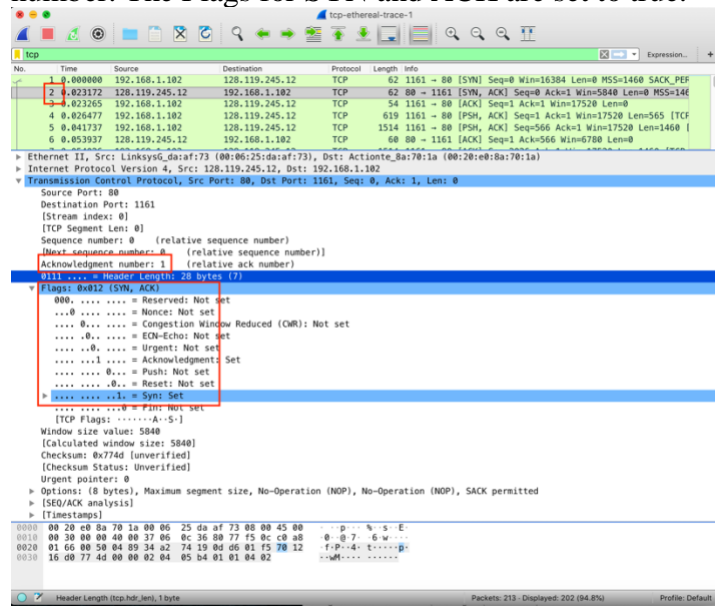
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.1.182	128.119.245.12	TCP	62	1351 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.013112	128.119.245.12	192.168.1.182	TCP	62	80 → 1351 [RST] Seq=0 Ack=1 Win=0 Len=0 RST=0
3	0.023055	192.168.1.182	128.119.245.12	TCP	54	1351 → 80 [ACK] Seq=1 Ack=1 Win=17528 Len=0
4	0.026477	192.168.1.182	128.119.245.12	TCP	610	1351 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17528 Len=565 [TS] TSval=1351
5	0.041757	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
6	0.053937	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=566 Ack=1 Win=17528 Len=0
7	0.054806	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=580 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
8	0.054808	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=586 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
9	0.072504	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=586 Ack=1 Win=17528 Len=0
10	0.077485	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=594 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
11	0.078157	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=6486 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
12	0.124805	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=6486 Ack=1 Win=1680 Len=0
13	0.124185	192.168.1.182	128.119.245.12	TCP	1281	1351 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17528 Len=1147 [TS] TSval=1351
14	0.169118	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=7866 Ack=1 Win=1680 Len=0
15	0.217299	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=7866 Ack=1 Win=17528 Len=0
16	0.267882	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=7866 Ack=1 Win=28480 Len=0
17	0.384887	128.119.245.12	192.168.1.182	TCP	68	80 → 1351 [ACK] Seq=9813 Ack=1 Win=2384 Len=0
18	0.385848	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=9813 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
19	0.385811	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=18473 Ack=1 Win=17528 Len=1460 [TS] TSval=1351
20	0.386692	192.168.1.182	128.119.245.12	TCP	1514	1351 → 80 [ACK] Seq=19353 Ack=1 Win=17528 Len=1460 [TS] TSval=1351

1011 = Header Length: 28 bytes (7)
Flags: 0x02 (SYN)
0000 = Reserved: Not set
...R... = RST: Not set
...R... = Retransmission: Not set
...R... = Congestion Window reduced (CWR): Not set
...R... = ECN-Echo: Not set
...R... = Urgent: Not set
...R... = Acknowledgment: Not set
...R... = Push: Not set
...R... = Reset: Not set
...R... = Synchronize: Not set
...R... = FIN: Not set
[TCP Flags: 0x02]
Window size value: 16384
[Calculated window size: 16384]
Checksum: 0x1f0f [unverified]
[Checksum Status: Unverified]
0000 00 00 25 5a 77 08 28 08 0a 7a 1a 08 00 45 00 P E ...
0010 00 30 1a 1a 00 00 00 05 15 12 00 01 00 00 7f ... @ F ...
0020 f5 0c df 3f 00 50 2e 4d b5 a9 00 00 00 00 b0 c2 ... ? P M ...
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK

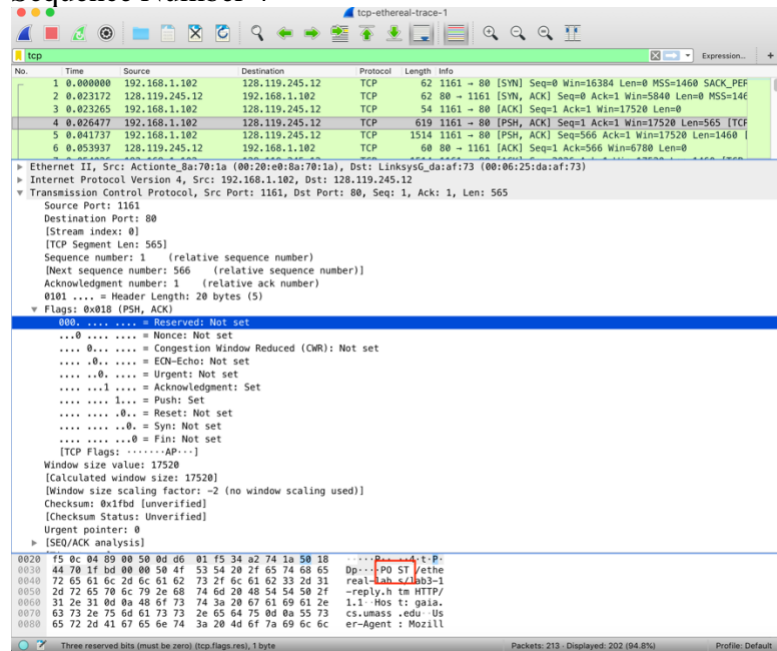
segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Sequence Number 2. Value of the Acknowledgement field = 1. Determined by the relative ack number. The Flags for SYN and ACK are set to true.



6. 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.

Sequence Number 4



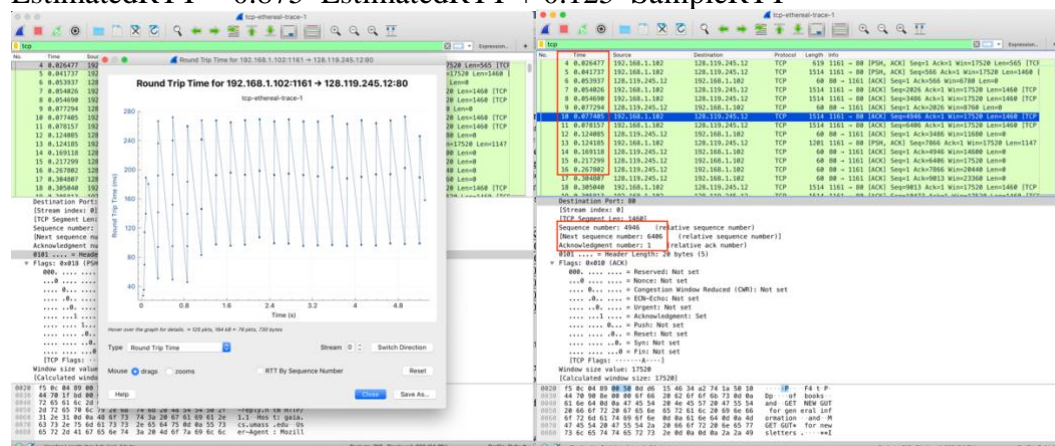
7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent?

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 Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

First 6 Segments of the TCP Connection

Segment Number	Sequences	Time	ACK w/ Time	RTT	Estimated RTT
4	1	0.026477	6, 0.053937	0.02746	0.02746
5	566	0.041737	9, 0.077294	0.035557	0.028595
7	2026	0.054026	12, 0.124085	0.070059	0.033777
8	3486	0.054690	14, 0.169118	0.114428	0.043859
10	4946	0.077405	15, 0.217299	0.139894	0.055863
11	6406	0.078157	16, 0.267802	0.189645	0.072586

EstimatedRTT = 0.875*EstimatedRTT + 0.125*SampleRTT

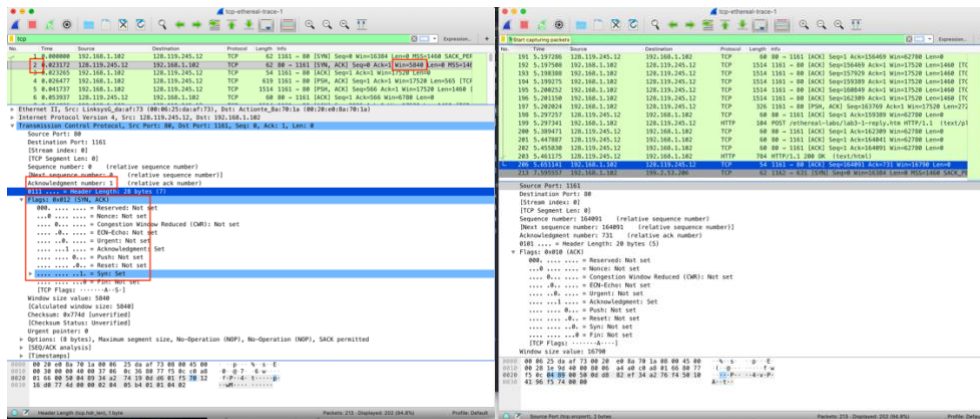


8. What is the length of each of the first six TCP segments?

Number	Length
4	565
5	1460
7	1460
8	1460
10	1460
11	1460

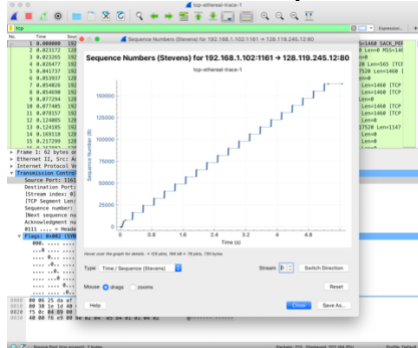
9. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Buffer space is 5840 (from first ACK / Segment 2). It will go up to 164091, and no it does not get throttled.



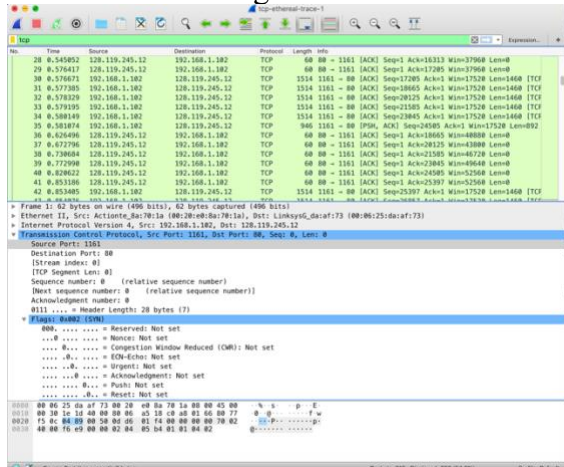
10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

No, I looked at the Sequence Numbers Graph / Time Sequence (Stevens) within Wireshark.



11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).

The receiver acknowledges each segment near the beginning. Then (like in the case below), it starts to acknowledge them in “chunks” and is such in every other received segment



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

Throughput = total data / transmission rate.

Total Data = first post to lack ACK sequences. 164091 bytes

Send Time = 5.6511

My Trace

We can see where TCP's slowstart phase begins and ends; it quickly sends each part until there is a good congestion window, at which it then starts to send it in a predetermined sequence as ACKs are received. There's a better view of the congestion window here. But comparing to the last question, windows are a lot bigger, and the "steps" of the sequences are bigger.

