Lab4

Exercise 1: Understanding TCP using Wireshark

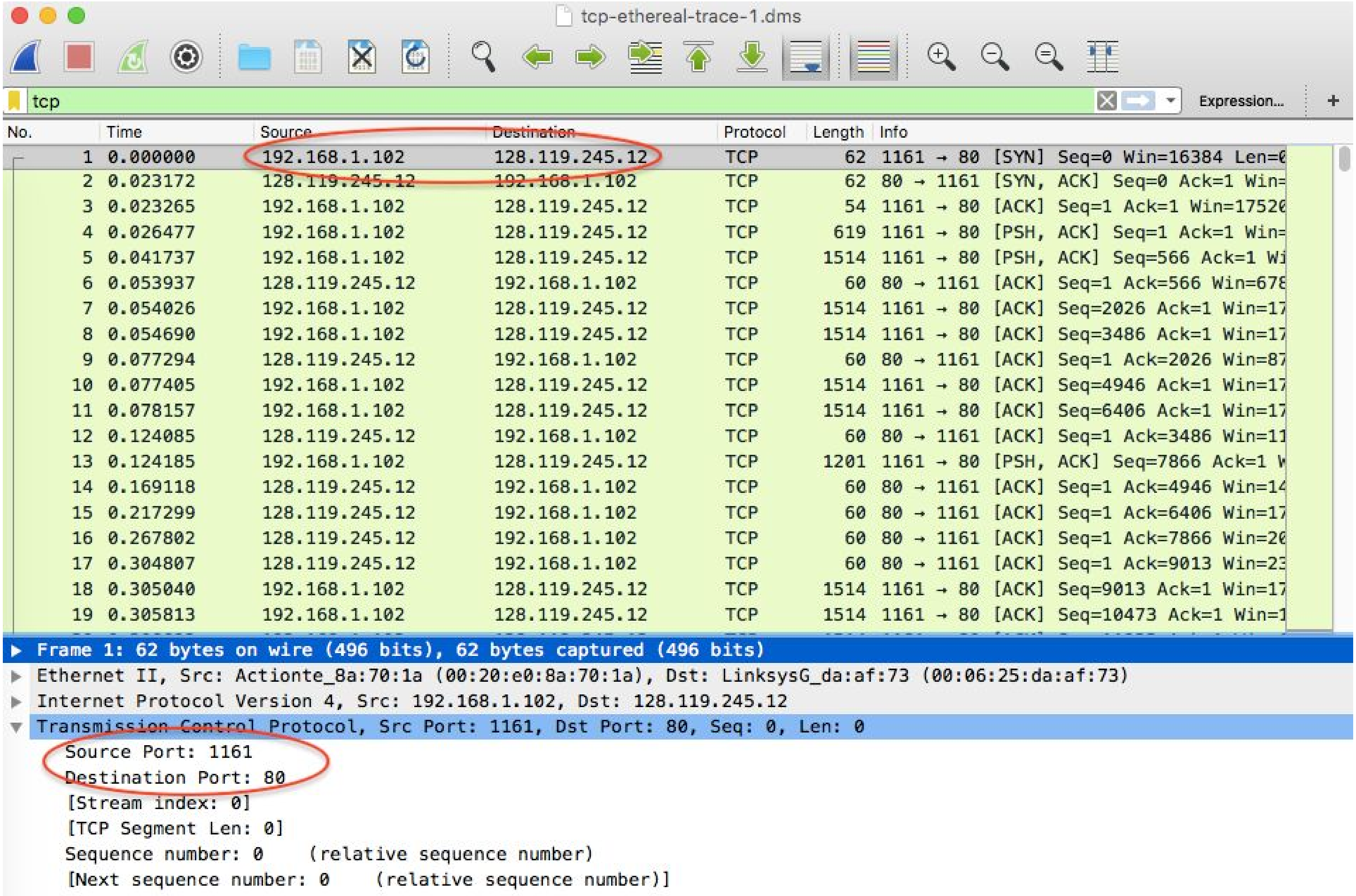
Question 1 . What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

Ans: The IP address: 128.119.245.12

Port number: 80

Client IP address: 192.168.1.102

Client port number: 1161

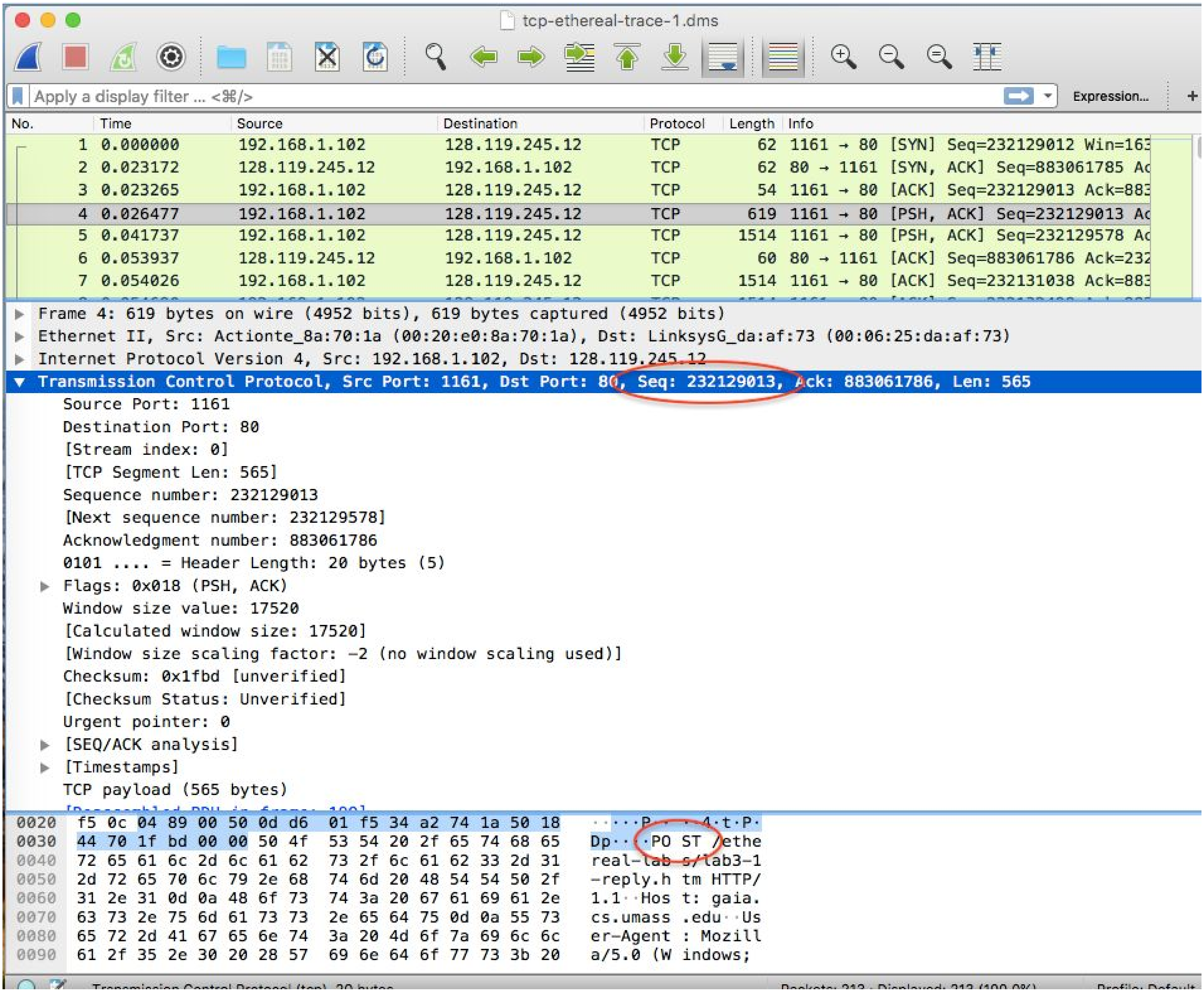


```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0
   2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=
   3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520
   4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=
   5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Wi
   6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=678
   7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17
   8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17
   9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=87
  10 0.077405  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17
  11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17
  12 0.124085  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11
  13 0.124185  192.168.1.102   128.119.245.12  TCP      1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 W
  14 0.169118  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14
  15 0.217299  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17
  16 0.267802  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20
  17 0.304807  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23
  18 0.305040  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17
  19 0.305813  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=1
```

```
▶ 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)]
```

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.

Ans: # 4 segment is the TCP segment containing the HTTP POST command. The sequence #: 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=163
  2 0.023172   128.119.245.12   192.168.1.102    TCP           62  80 → 1161 [SYN, ACK] Seq=883061785 Ac
  3 0.023265   192.168.1.102    128.119.245.12   TCP           54  1161 → 80 [ACK] Seq=232129013 Ack=883
  4 0.026477   192.168.1.102    128.119.245.12   TCP          619  1161 → 80 [PSH, ACK] Seq=232129013 Ac
  5 0.041737   192.168.1.102    128.119.245.12   TCP         1514  1161 → 80 [PSH, ACK] Seq=232129578 Ac
  6 0.053937   128.119.245.12   192.168.1.102    TCP           60  80 → 1161 [ACK] Seq=883061786 Ack=232
  7 0.054026   192.168.1.102    128.119.245.12   TCP         1514  1161 → 80 [ACK] Seq=232131038 Ack=883
```

```
▶ 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: 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: 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)
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1fbd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
    TCP payload (565 bytes)
```

```
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/
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;
```

Transmission Control Protocol (tcp), 20 bytes
Packets: 213 · Displayed: 213 (100.0%)
Profile: Default

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.

	Sequence Num	Segment Sent (sec)	ACK Receive (sec)	RTT (sec)
Segment 1(No.4)	232129013	0.026477	0.053937	0.027460
Segment 2(No.5)	232129578	0.041737	0.077294	0.035557
Segment 3(No.7)	232131038	0.054026	0.124085	0.070059
Segment 4(No.8)	232132498	0.054690	0.169118	0.114428
Segment 5(No.10)	232133958	0.077405	0.217299	0.139894
Segment 6(No.11)	232135418	0.078157	0.267802	0.189645

EstimatedRTT = EstimatedRTT * (1-0.125) + 0.125 * SampleRTT

Segment 1: EstimatedRTT = 0.02746 second

Segment 2: EstimatedRTT = 0.02746 * 0.875 + 0.125 * 0.035557 = 0.02847 second

Segment 3: EstimatedRTT = 0.02847 * 0.875 + 0.125 * 0.070059 = 0.03367 second

Segment 4: EstimatedRTT = 0.03367 * 0.875 + 0.125 * 0.114428 = 0.04376 second

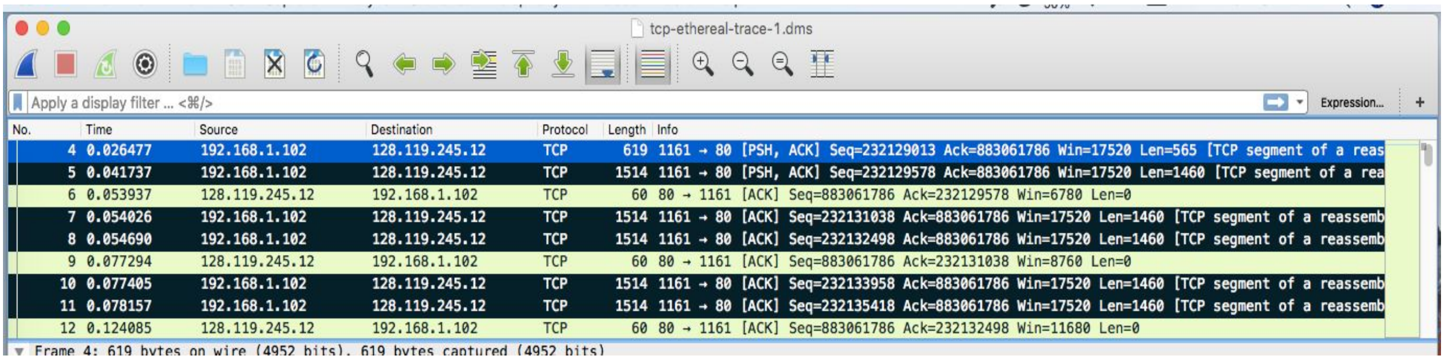
Segment 5: EstimatedRTT = 0.04376 * 0.875 + 0.125 * 0.139894 = 0.05578 second

Segment 6: EstimatedRTT = 0.05578 * 0.875 + 0.125 * 0.189645 = 0.07251 second

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

Ans: Segment 1: 565 bytes

Segment 2~6: 1460 bytes

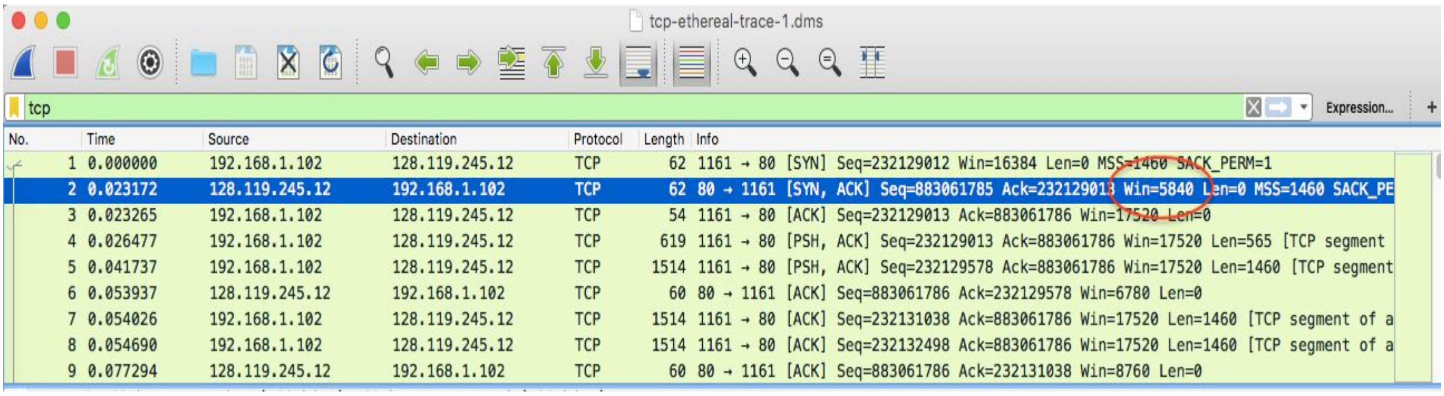


```
No.     Time        Source            Destination       Protocol  Length  Info
     4 0.026477    192.168.1.102     128.119.245.12    TCP        619 1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 Win=17520 Len=565 [TCP segment of a reas
     5 0.041737    192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [PSH, ACK] Seq=232129578 Ack=883061786 Win=17520 Len=1460 [TCP segment of a rea
     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 reassemb
     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 reassemb
     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 reassemb
    11 0.078157    192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=232135418 Ack=883061786 Win=17520 Len=1460 [TCP segment of a reassemb
    12 0.124085    128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=11680 Len=0
▼ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
```

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?

Ans: The minimum amount of available buffer space at the receiver for the entire trace is 5840 bytes.

No, the buffer space grows steadily and the maximum receiver buffer size is 62780 bytes.

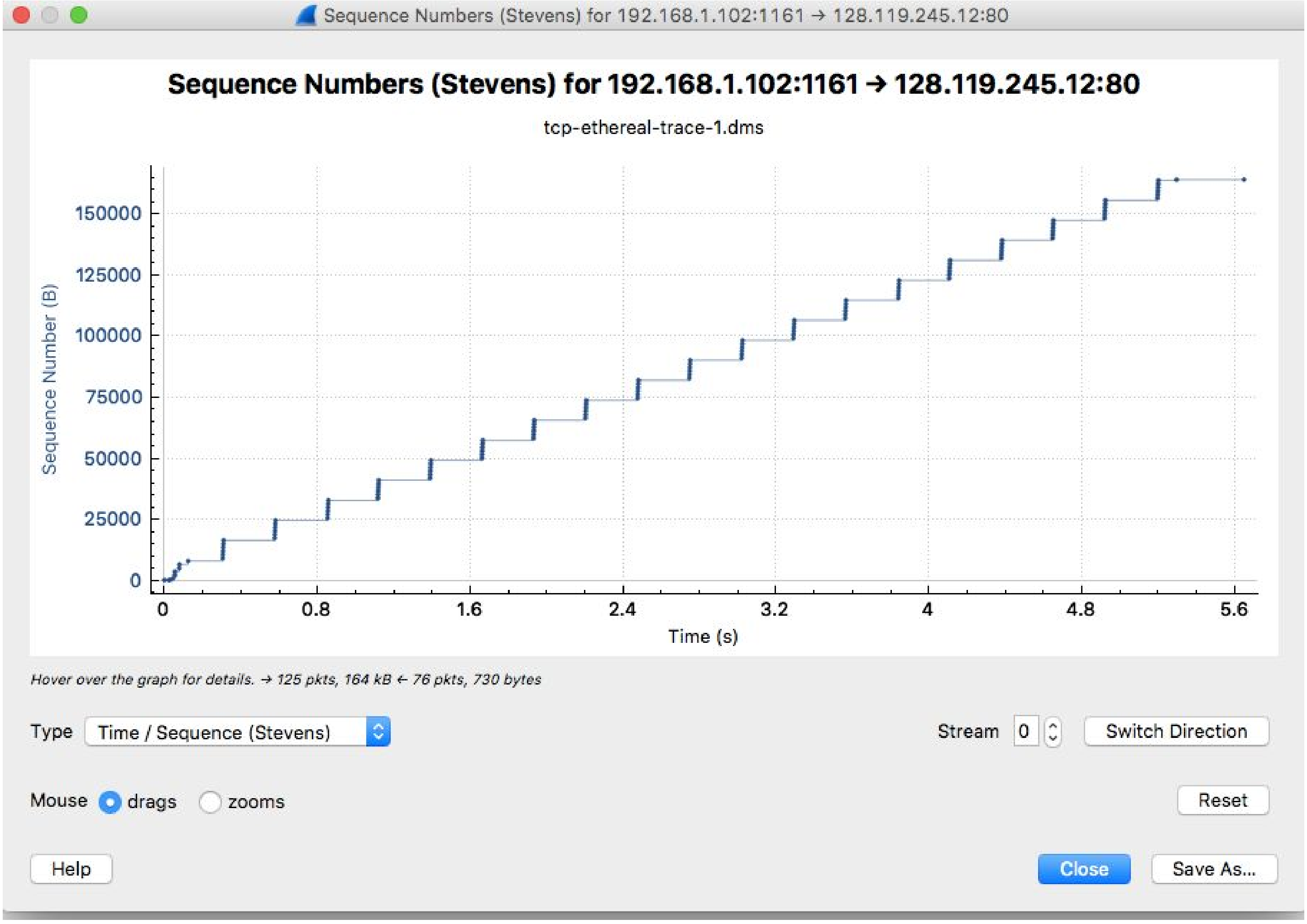


tcp

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
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
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
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
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
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=8760 Len=0

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?

Ans: No retransmitted segments in the trace file. Checking the segment sequence # by using Sequence Numbers (Stevens) graphics. The sequence # form the client to the server is increasing. If any segments retransmitted, the sequence # should be smaller than its neighboring segments.



Hover over the graph for details. → 125 pkts, 164 kB ← 76 pkts, 730 bytes

Type Time / Sequence (Stevens)

Stream 0

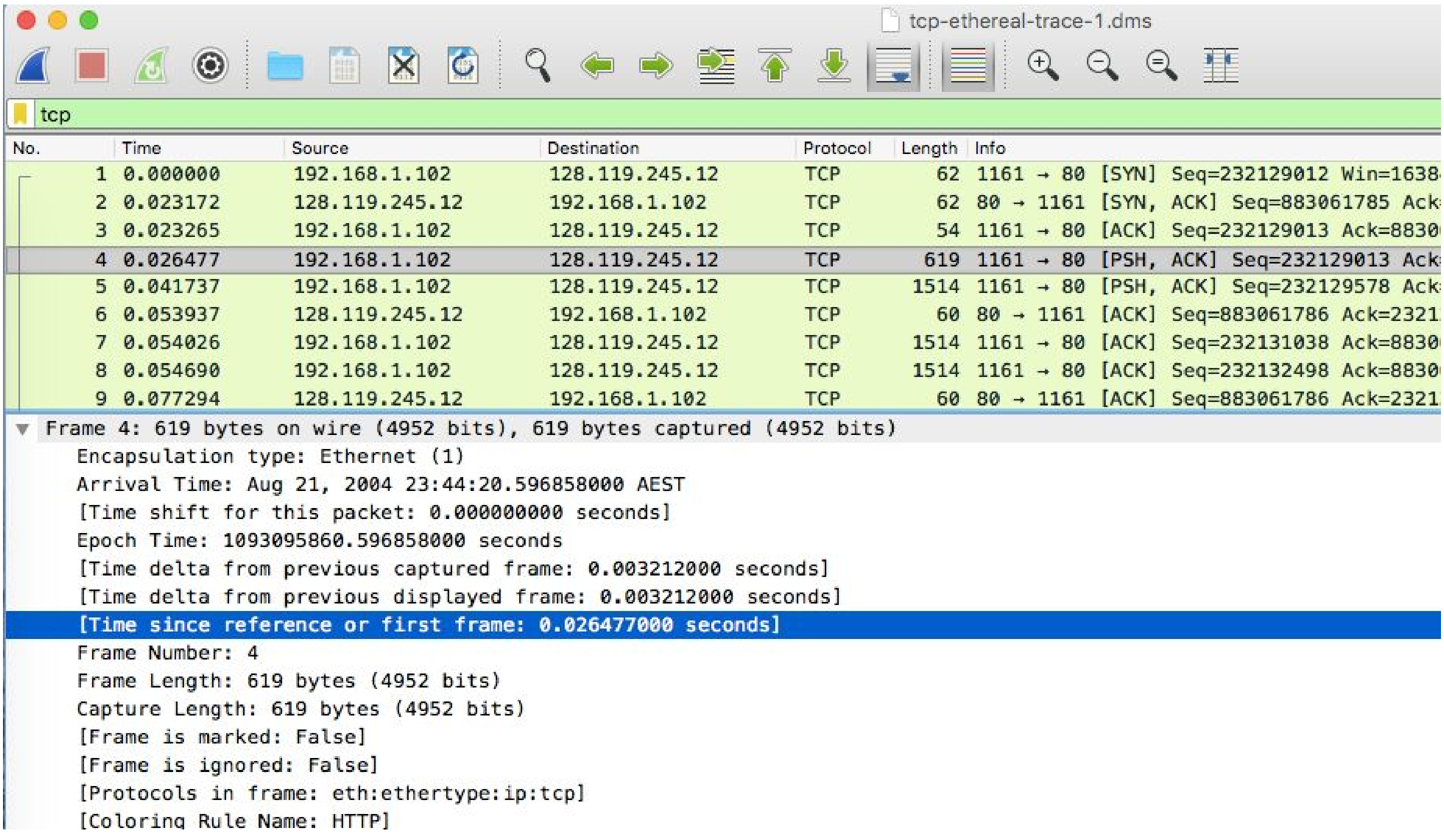
Mouse ● drags ○ zooms

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).

Ans: The typically acknowledge is 1460 bytes. In the early part of the trace file, we noticed that the receiver individually confirmed each packet. Observe the behavior of the sender sending a packet burst, and then the receiver sends back an ACK for each packet. However, later in the trace, especially at segment number 70, we will notice that the ACK with the acknowledgment field of 232176633 actually acknowledges the two segments with sequences 232173713 and 232175173. From this point on, the receiver sends an acknowledgment packet received by each. other. The receiver typically sends a cumulative ACK of the two TCP segments it receives. This is because TCP uses a delayed ACK where the receiver waits up to 500 milliseconds, the other arrives at the order segment, and then sends the accumulated ACK for the two segments received.

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

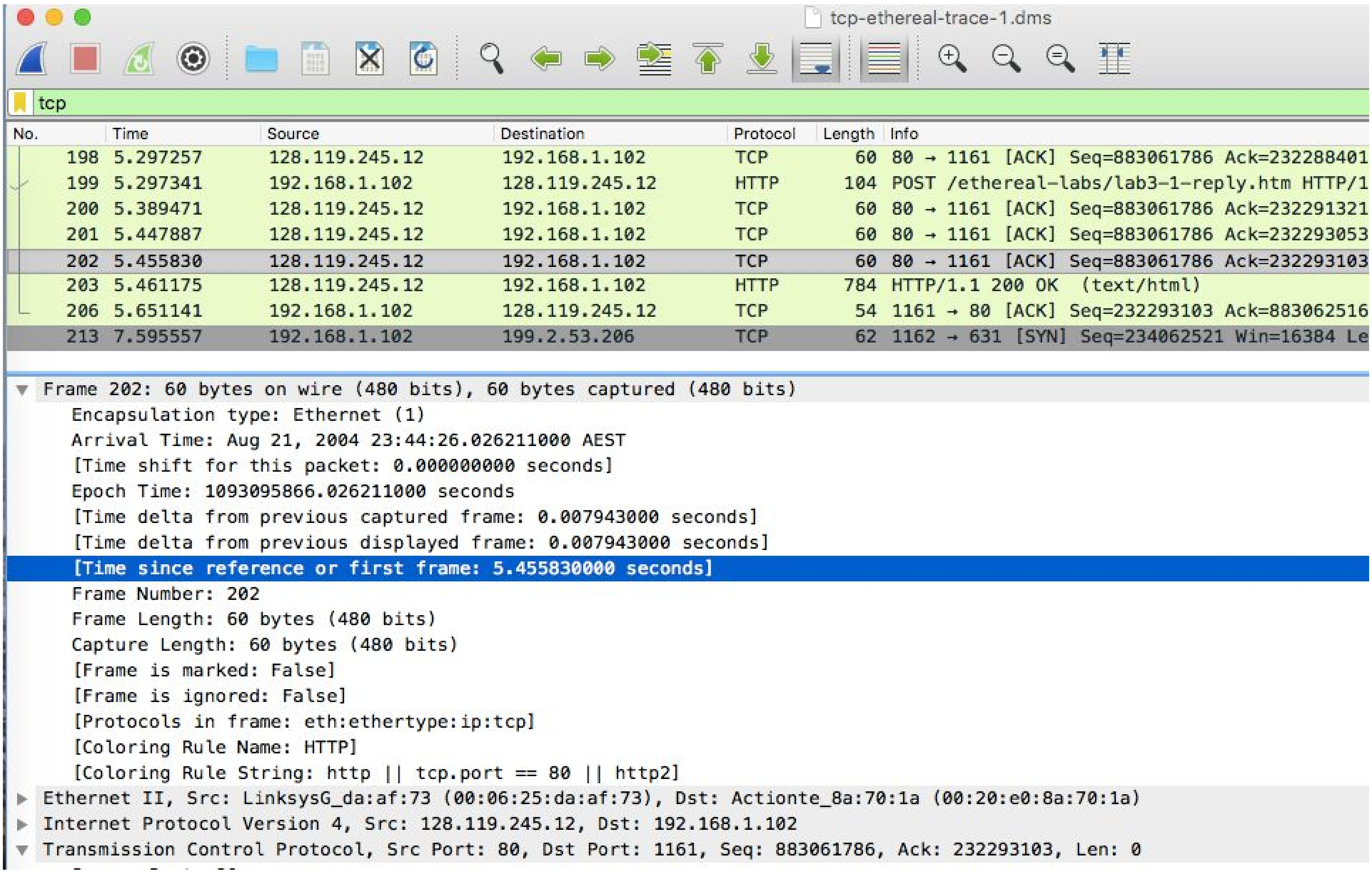
Ans: The total bytes transferred is the last ACK number – the first sequence number, which is 232293103 – 232129013 = 164090 bytes. Therefore, the throughput is total data/total time = 164090 / (5.455830-0.026477) = 30.222 Kbyte/sec.



tcp

```
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=1638
    2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=883061785 Ack
    3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=232129013 Ack=8830
    4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=232129013 Ack
    5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=232129578 Ack
    6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=883061786 Ack=2321
    7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=232131038 Ack=8830
    8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=232132498 Ack=8830
    9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=883061786 Ack=2321
```

```
▼ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 23:44:20.596858000 AEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093095860.596858000 seconds
    [Time delta from previous captured frame: 0.003212000 seconds]
    [Time delta from previous displayed frame: 0.003212000 seconds]
    [Time since reference or first frame: 0.026477000 seconds]
    Frame Number: 4
    Frame Length: 619 bytes (4952 bits)
    Capture Length: 619 bytes (4952 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
```



```
No.    Time      Source           Destination      Protocol  Length  Info
   198 5.297257  128.119.245.12   192.168.1.102    TCP        60  80 → 1161 [ACK] Seq=883061786 Ack=232288401
   199 5.297341  192.168.1.102    128.119.245.12   HTTP      104  POST /ethereal-labs/lab3-1-reply.htm HTTP/1
   200 5.389471  128.119.245.12   192.168.1.102    TCP        60  80 → 1161 [ACK] Seq=883061786 Ack=232291321
   201 5.447887  128.119.245.12   192.168.1.102    TCP        60  80 → 1161 [ACK] Seq=883061786 Ack=232293053
   202 5.455830  128.119.245.12   192.168.1.102    TCP        60  80 → 1161 [ACK] Seq=883061786 Ack=232293103
   203 5.461175  128.119.245.12   192.168.1.102    HTTP      784  HTTP/1.1 200 OK  (text/html)
   206 5.651141  192.168.1.102    128.119.245.12   TCP        54  1161 → 80 [ACK] Seq=232293103 Ack=883062516
   213 7.595557  192.168.1.102    199.2.53.206     TCP        62  1162 → 631 [SYN] Seq=234062521 Win=16384 Le
```

```
▼ Frame 202: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 23:44:26.026211000 AEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093095866.026211000 seconds
    [Time delta from previous captured frame: 0.007943000 seconds]
    [Time delta from previous displayed frame: 0.007943000 seconds]
    [Time since reference or first frame: 5.455830000 seconds]
    Frame Number: 202
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▶ 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
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 883061786, Ack: 232293103, Len: 0
```

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?

Ans: Sequence #: 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?

Ans: Sequence number: 1247095790

ACK: 2818463619

TCP is using 3-way handshake to set up a connection. SYNACK means initiating a connection. The client maintains a 32-bit sequence number to keep track of how much data it has sent. When a host initials a TCP session, its initial sequence number is effectively random. It may be any value between 0 and 4,294,967,295, inclusive. In the initial connection, the client would try to send one byte data to check the connection is done or not. Thus, the ACK is the current sequence number in client plus one.

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?

Ans: Sequence number: 2818463619

The ACK: 1247095791

The segment does not contain any data because the line 301, the sequence number is 1247095791.

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?

Ans: Client and server has done the active close. In line 304 and line 305, they both sent FIN ACK before they receive FIN from the other side. Thus, 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?

Ans: The data form the client to the server is 33 bytes and the data from server to client is 40 bytes. The different of Initial Sequence Number and the final ACK received form the other side is the same as the data transfer though the connection.