Lab 7

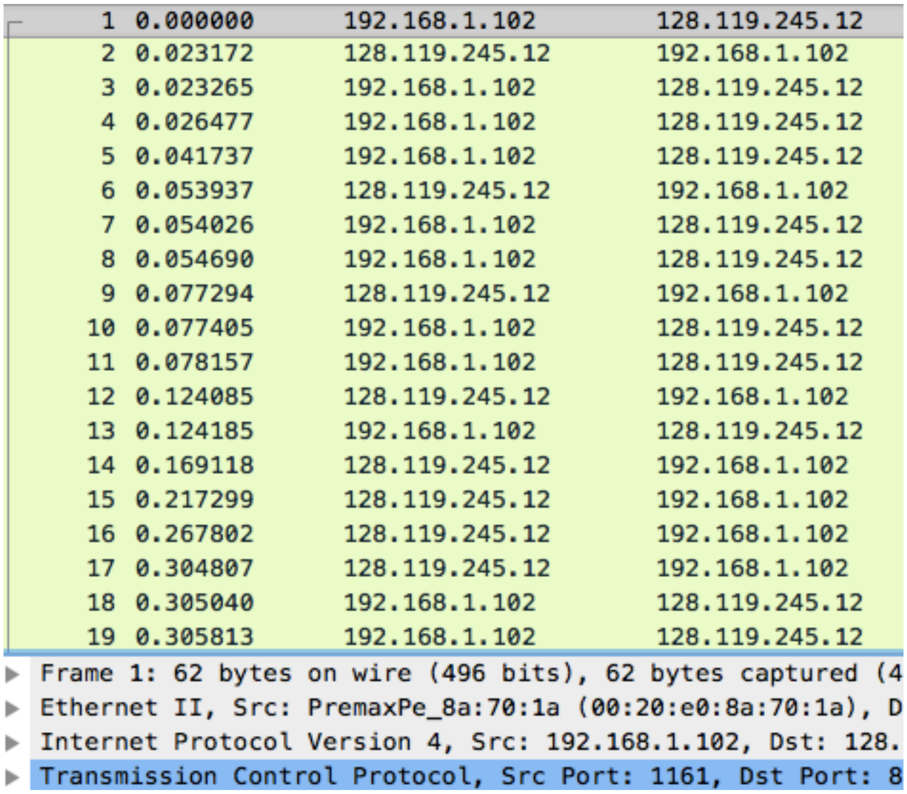
Wireshark TCP

Nicole Merritt

Questions

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.

Client IP: 192.168.1.102 TCP Port: 1161

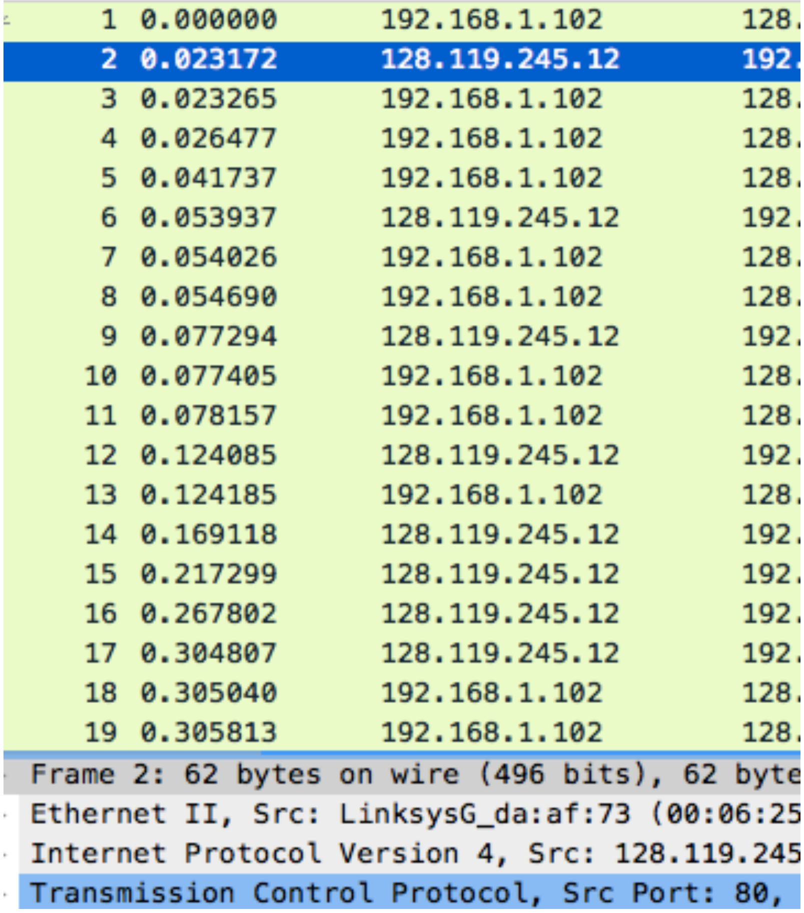


```
 1 0.000000     192.168.1.102      128.119.245.12
 2 0.023172     128.119.245.12     192.168.1.102
 3 0.023265     192.168.1.102      128.119.245.12
 4 0.026477     192.168.1.102      128.119.245.12
 5 0.041737     192.168.1.102      128.119.245.12
 6 0.053937     128.119.245.12     192.168.1.102
 7 0.054026     192.168.1.102      128.119.245.12
 8 0.054690     192.168.1.102      128.119.245.12
 9 0.077294     128.119.245.12     192.168.1.102
10 0.077405     192.168.1.102      128.119.245.12
11 0.078157     192.168.1.102      128.119.245.12
12 0.124085     128.119.245.12     192.168.1.102
13 0.124185     192.168.1.102      128.119.245.12
14 0.169118     128.119.245.12     192.168.1.102
15 0.217299     128.119.245.12     192.168.1.102
16 0.267802     128.119.245.12     192.168.1.102
17 0.304807     128.119.245.12     192.168.1.102
18 0.305040     192.168.1.102      128.119.245.12
19 0.305813     192.168.1.102      128.119.245.12
```

```
▶ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (4
▶ Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), D
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.
▶ Transmission Control Protocol, Src Port: 1161, Dst Port: 8
```

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?

Gaia.cs.umass.edu IP: 128.119.245.12 TCP Port: 80



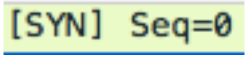
```
 1 0.000000   192.168.1.102      128.
 2 0.023172   128.119.245.12     192.
 3 0.023265   192.168.1.102      128.
 4 0.026477   192.168.1.102      128.
 5 0.041737   192.168.1.102      128.
 6 0.053937   128.119.245.12     192.
 7 0.054026   192.168.1.102      128.
 8 0.054690   192.168.1.102      128.
 9 0.077294   128.119.245.12     192.
10 0.077405   192.168.1.102      128.
11 0.078157   192.168.1.102      128.
12 0.124085   128.119.245.12     192.
13 0.124185   192.168.1.102      128.
14 0.169118   128.119.245.12     192.
15 0.217299   128.119.245.12     192.
16 0.267802   128.119.245.12     192.
17 0.304807   128.119.245.12     192.
18 0.305040   192.168.1.102      128.
19 0.305813   192.168.1.102      128.

Frame 2: 62 bytes on wire (496 bits), 62 byte
Ethernet II, Src: LinksysG_da:af:73 (00:06:25
Internet Protocol Version 4, Src: 128.119.245
Transmission Control Protocol, Src Port: 80,
```

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?

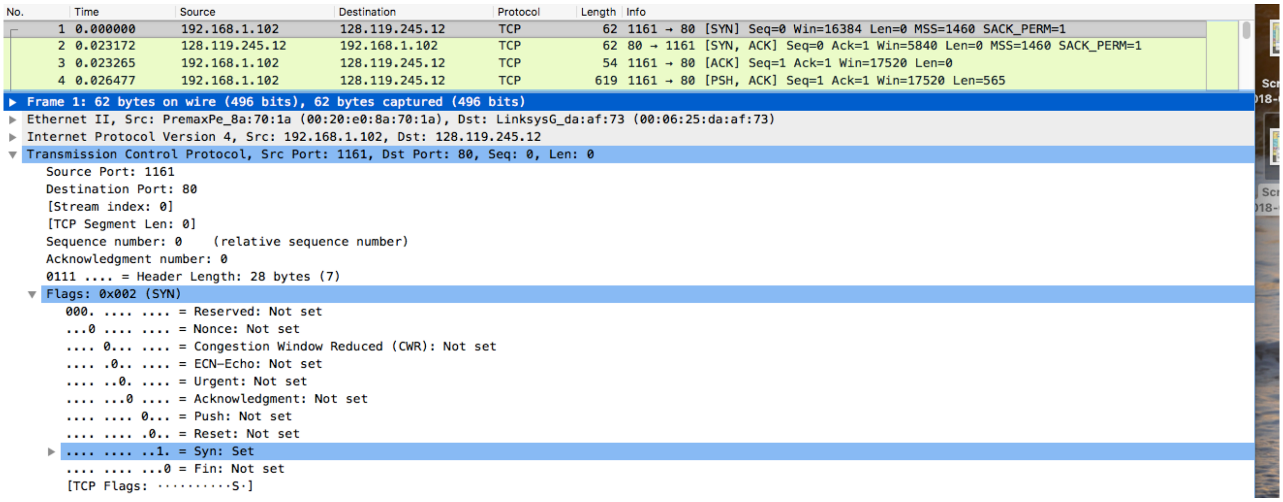
I did not create my own trace.

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?



```
[SYN] Seq=0
```

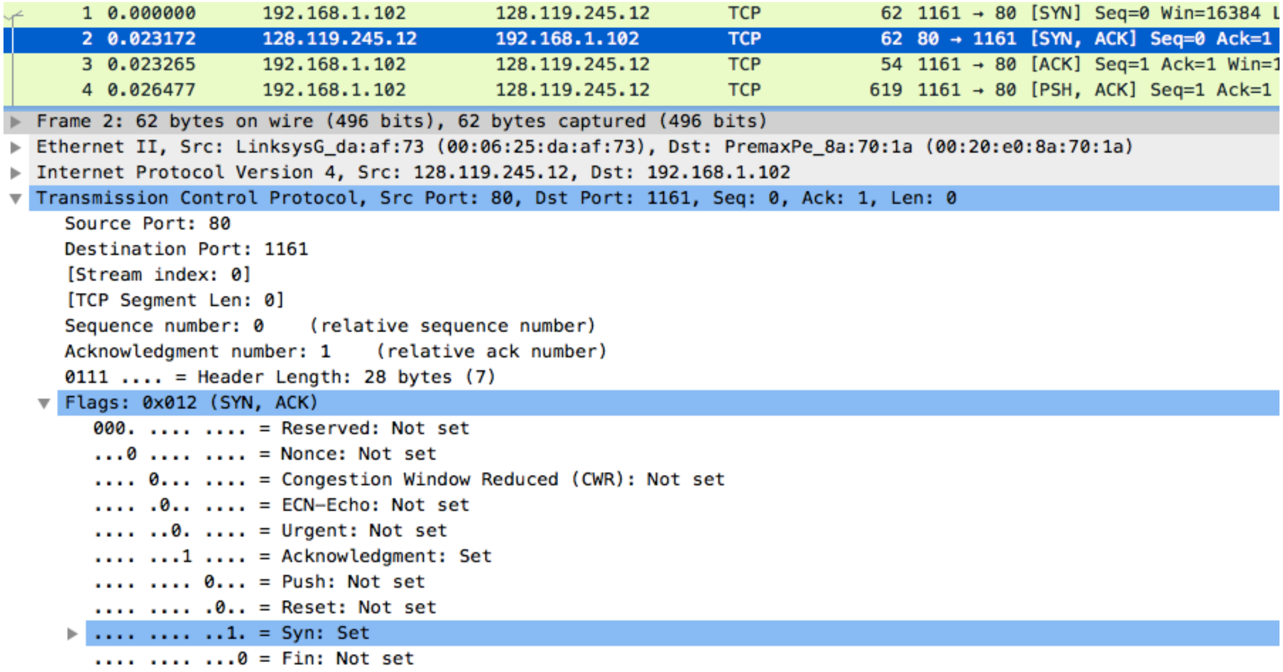
The flag that is 1 instead of 0



```
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 MSS=1460 SACK_PERM=1
    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=1
    3 0.023265   192.168.1.102    128.119.245.12   TCP           54  1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
    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
▶ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▶ Ethernet II, Src: PremaxPe_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)
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
  ▼ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▶ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
```

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?

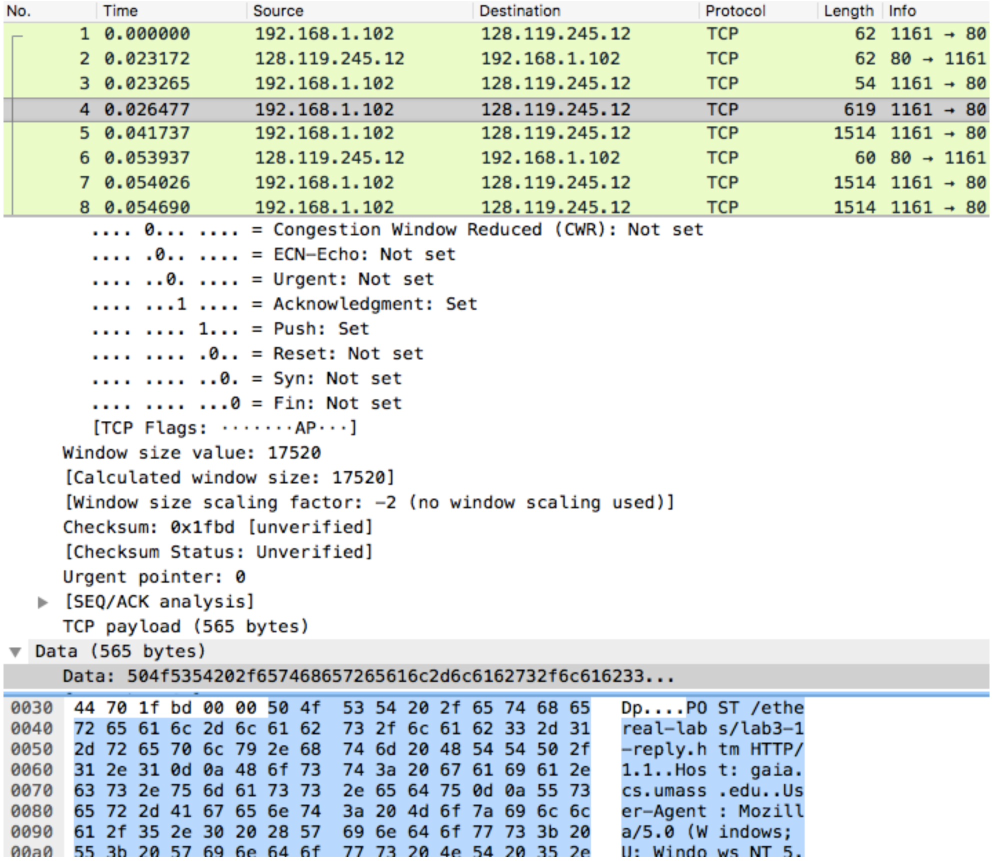
Seq = 0 again.
It is 1, because the initial segment is defaulted to 0, and then it continues in increments of 1until the connection is stopped.
In the flag section SYN is set to one and ACK is set to 1. That is why it is SYNACK



```
    1 0.000000   192.168.1.102    128.119.245.12   TCP           62  1161 → 80 [SYN] Seq=0 Win=16384 L
    2 0.023172   128.119.245.12   192.168.1.102    TCP           62  80 → 1161 [SYN, ACK] Seq=0 Ack=1
    3 0.023265   192.168.1.102    128.119.245.12   TCP           54  1161 → 80 [ACK] Seq=1 Ack=1 Win=1
    4 0.026477   192.168.1.102    128.119.245.12   TCP          619  1161 → 80 [PSH, ACK] Seq=1 Ack=1
▶ Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: PremaxPe_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: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
  ▼ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▶ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
```

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.

Seq=1



```
No.  Time       Source           Destination      Protocol  Length  Info
  1  0.000000   192.168.1.102    128.119.245.12   TCP           62  1161 → 80
  2  0.023172   128.119.245.12   192.168.1.102    TCP           62  80 → 1161
  3  0.023265   192.168.1.102    128.119.245.12   TCP           54  1161 → 80
  4  0.026477   192.168.1.102    128.119.245.12   TCP          619  1161 → 80
  5  0.041737   192.168.1.102    128.119.245.12   TCP         1514  1161 → 80
  6  0.053937   128.119.245.12   192.168.1.102    TCP           60  80 → 1161
  7  0.054026   192.168.1.102    128.119.245.12   TCP         1514  1161 → 80
  8  0.054690   192.168.1.102    128.119.245.12   TCP         1514  1161 → 80
```

```
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    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]
    TCP payload (565 bytes)
▼ Data (565 bytes)
    Data: 504f5354202f657468657265616c2d6c6162732f6c616233...
```

```
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; 
00a0  55 3b 20 57 69 6e 64 6f  77 73 20 4e 54 20 35 2e   U: Windo ws NT 5.
```

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 239 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 239 for all subsequent segments.

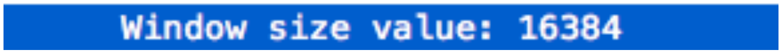
Segment	Packet number	Sequence number	Time sent	Time ACK received	Round Trip Time (RTT)	Estimated Round Trip Time
1	6	566	0.041737	0.053937	0.0122	0.0122
2	7	2026	0.054026	0.077294	0.023268	0.03976
3	8	3486	0.054690	0.0124085	0.069395	0.043464375
4	10	4946	0.077405	0.169118	0.091713	0.0494954531
5	11	6406	0.078157	0.217299	0.139142	0.0607102715
6	13	7866	0.124185	0.267802	0.143617	71.07 ms

Round Trip Time = Time Received – Time Sent
Estimated RTT = ((1-x)(EstimatedRTT(prev))) + (x * RTT)
Where 0 < x < 1 for this case x = .125

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

First segment was 565 bytes. The rest were 1460 bytes

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

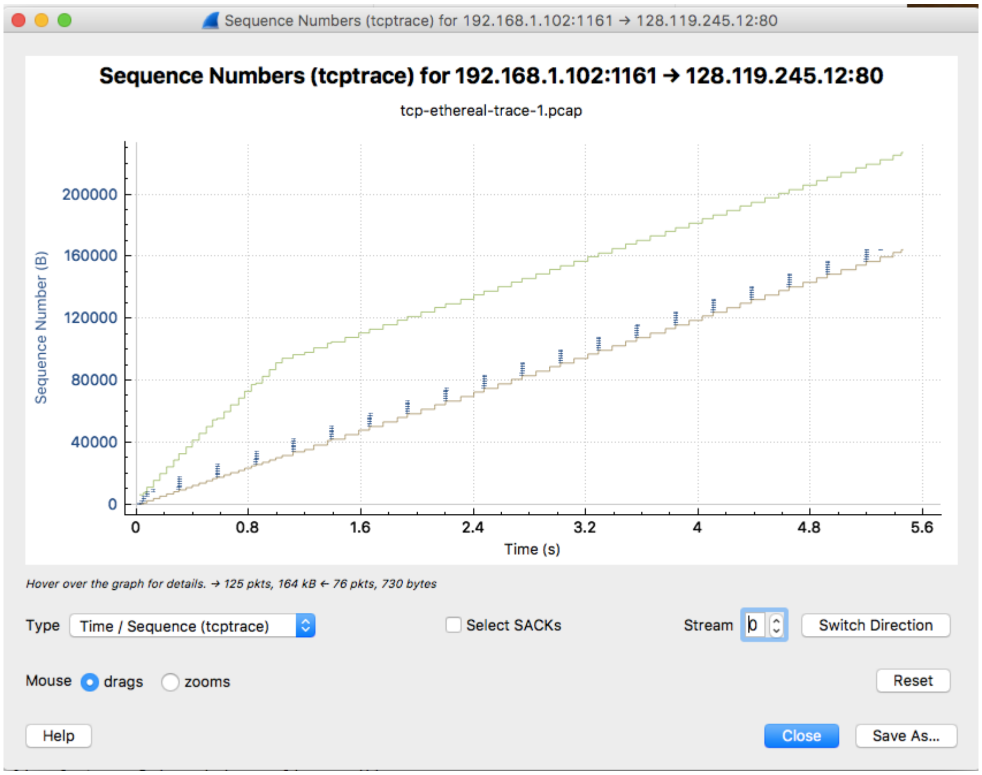


Window size value: 16384

It can throttle the sender if the window size is larger than the max TCP window size of 65535. Then, unless you use windows sliding then it can throttle the user.

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

There are no retransmitted segments in the trace file. We know this to be true because there no duplicate sequence numbers.



Sequence Numbers (tcptrace) for 192.168.1.102:1161 → 128.119.245.12:80

Sequence Numbers (tcptrace) for 192.168.1.102:1161 → 128.119.245.12:80

tcp-ethereal-trace-1.pcap

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

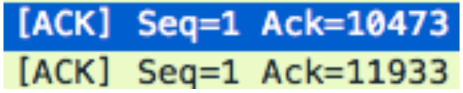
Type Time / Sequence (tcptrace)

□ Select SACKs

Stream 0

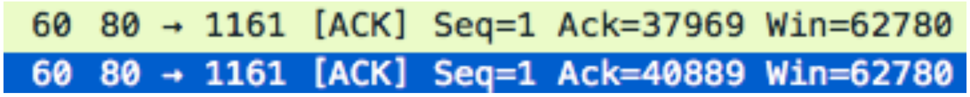
Mouse ● drags ○ zooms

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 247 in the text).



```
[ACK] Seq=1 Ack=10473
[ACK] Seq=1 Ack=11933
```

The difference between them is 1460. Others following this were found to be 1460 as well.



```
60  80 → 1161 [ACK] Seq=1 Ack=37969 Win=62780
60  80 → 1161 [ACK] Seq=1 Ack=40889 Win=62780
```

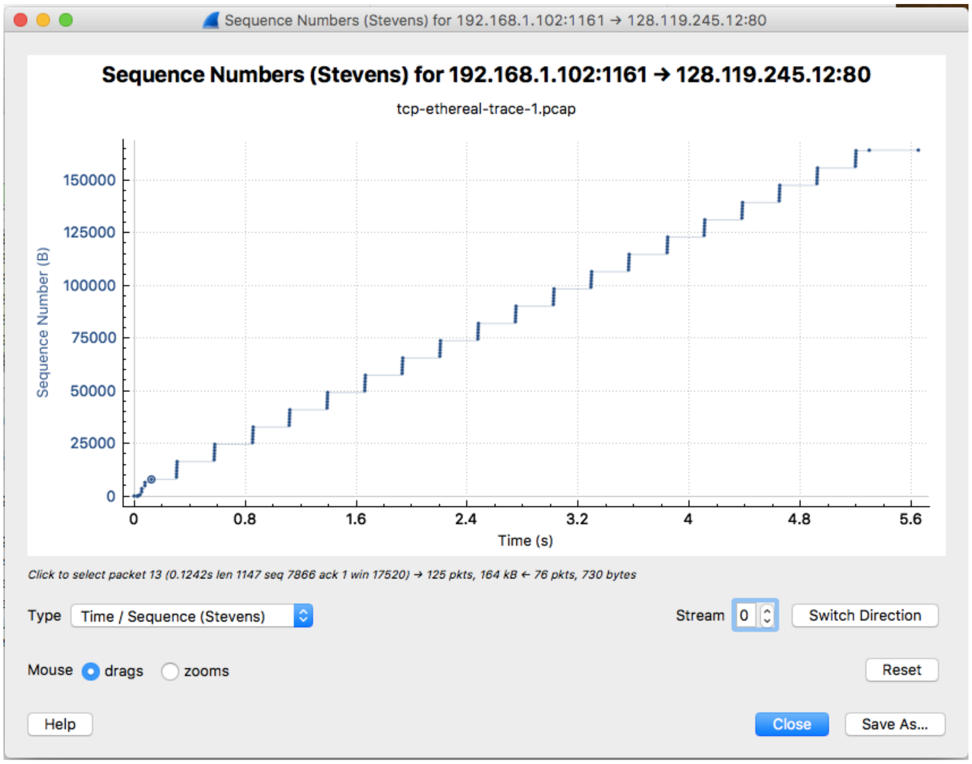
At this point it is ACKing every other received segment

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

Throughput = Amount of data/time occurred

Throughput =164041/5.270864
Throughput = 31.122 KB

13. Use the *Time-Sequence-Graph(Stevens*) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.


Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80
Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80
tcp-ethereal-trace-1.pcap
Sequence Number (B)
150000
125000
100000
75000
50000
25000
0
0
0.8
1.6
2.4
3.2
4
4.8
5.6
Time (s)
Switch Direction
Reset
Help
Close
Save As...

Click to select packet 13 (0.1242s len 1147 seq 7866 ack 1 win 17520) → 125 pkts, 164 kB ← 76 pkts, 730 bytes

Type Time / Sequence (Stevens)

Stream 0

Mouse ● drags ○ zooms

Slow start goes from packet 4-14
Congestion avoidance never happens.

The texts assume an aggressive constant stream of data. When in reality there is actually much more variation due to users and applications, we are not constantly doing data.

14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu