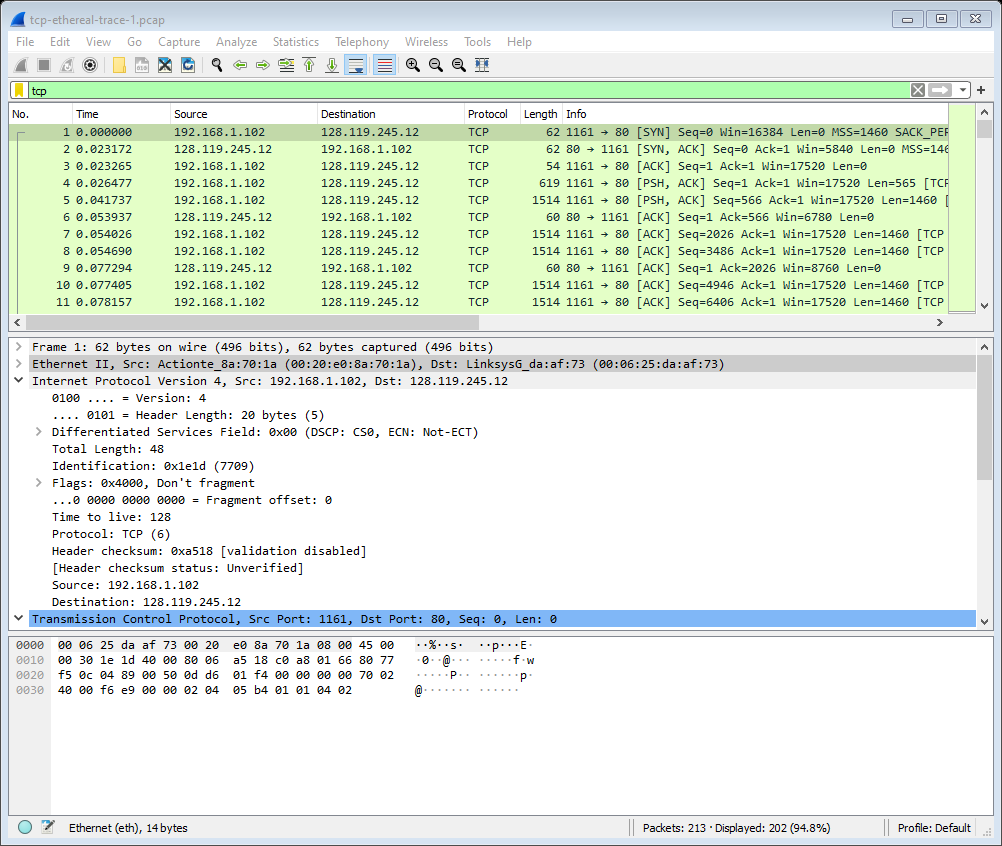
ECE 455 Wireshark Lab: TCP

By: Markail Bruner

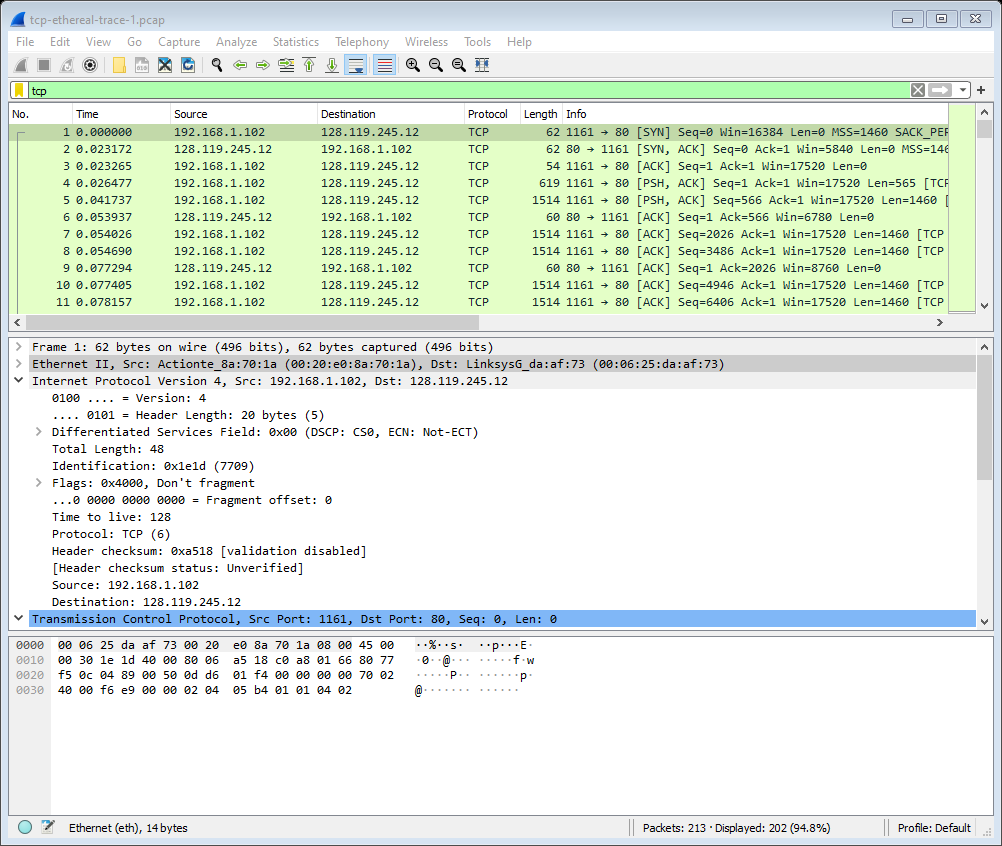
Due Date: 2/27/2020

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: 192.168.1.102, TCP port: 1161 

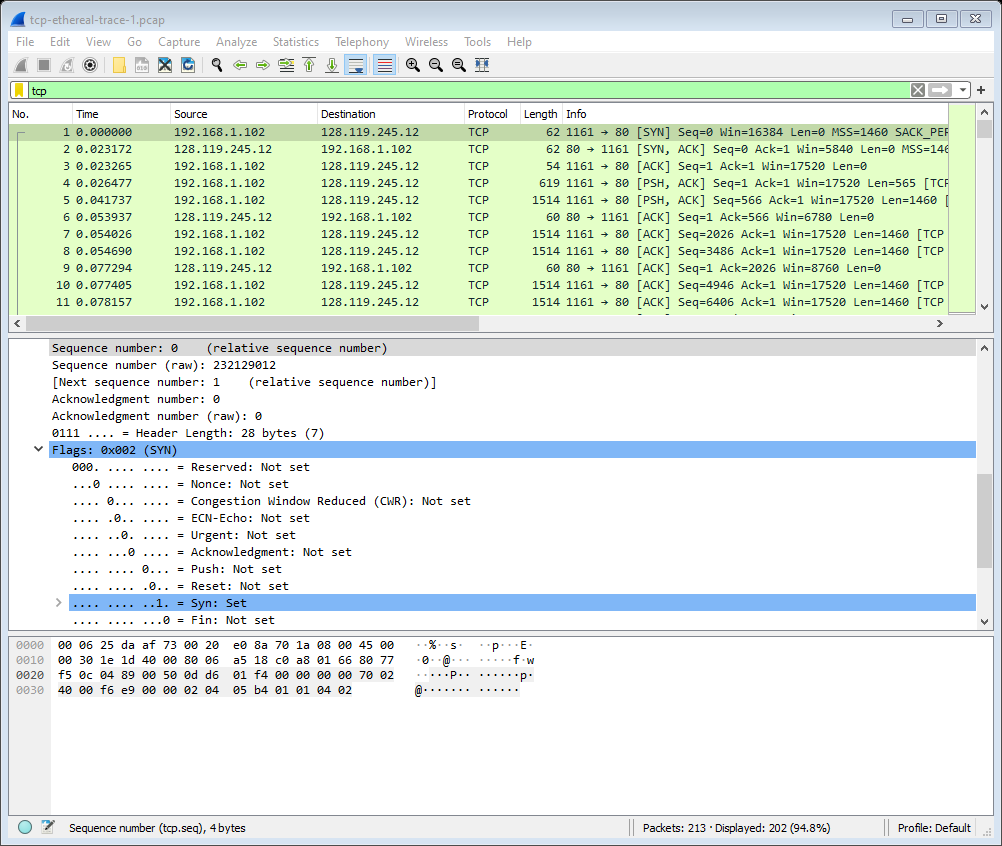
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

IP address: 128.119.245.12, Port: 80



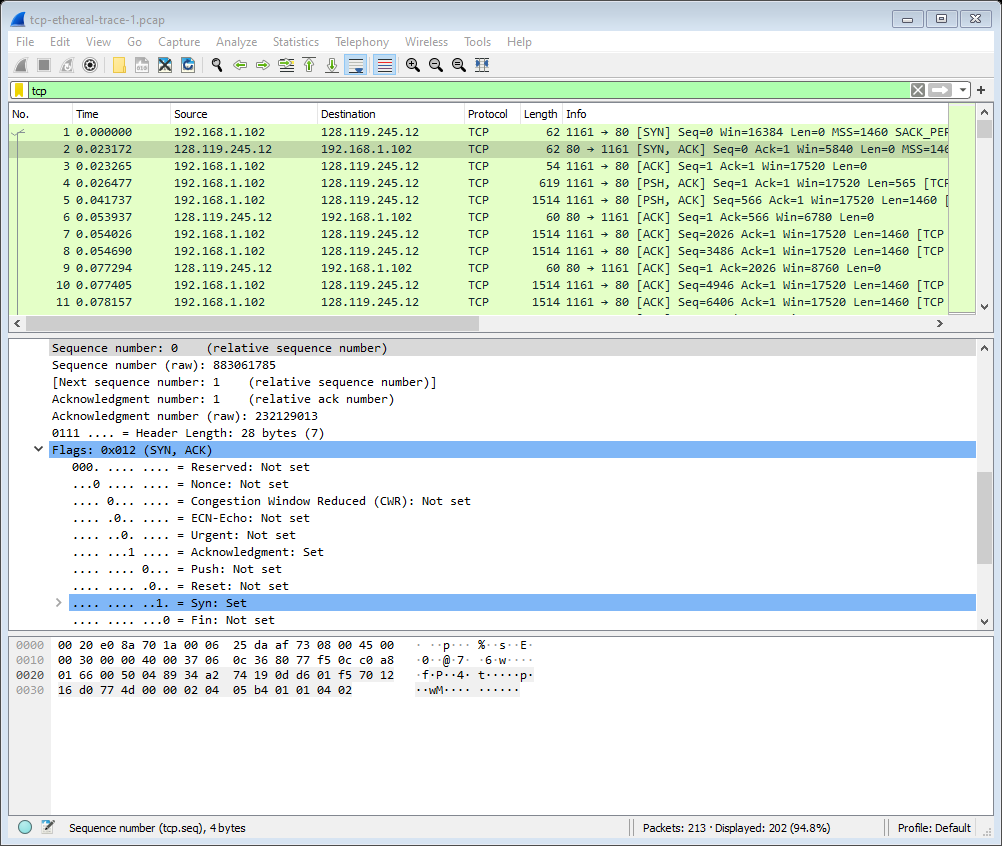
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Sequence number: 0, the syn is set to 1 and is set.



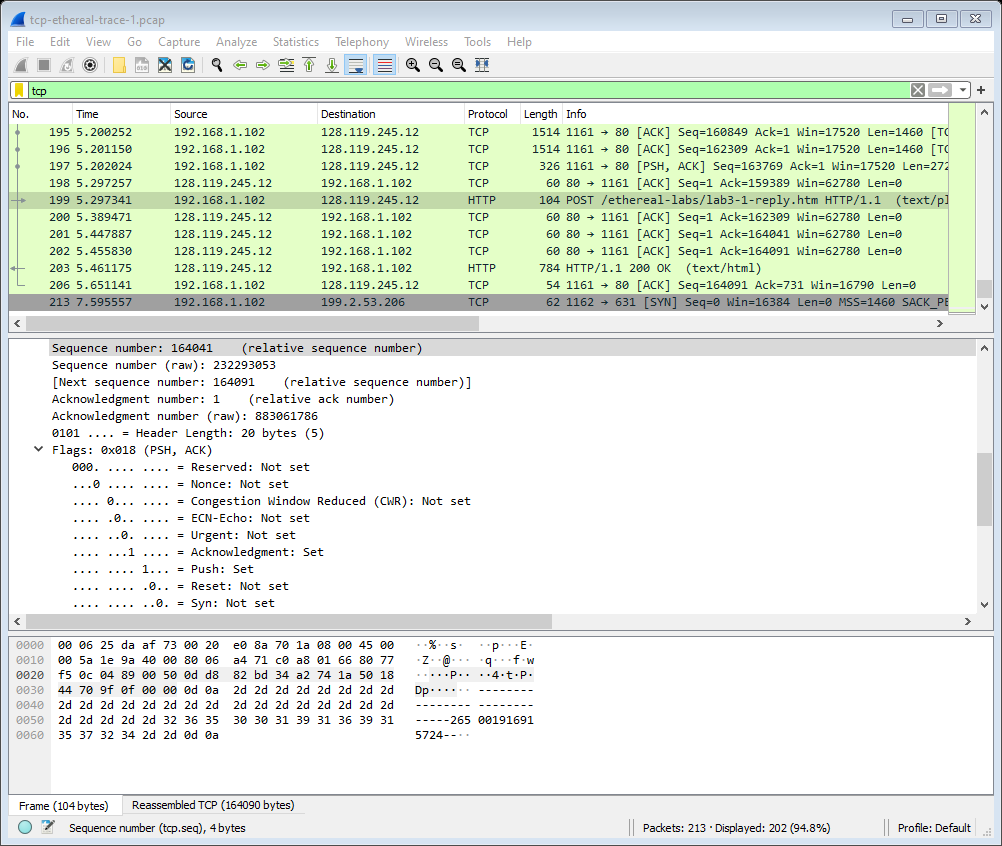
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Sequence number: 0, Acknowledgement value: 1 and is set, it added 1 to the sequence number of 0 on the client computer. Syn: 1. Shows that this is a SYNACK segment



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: 164041



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.

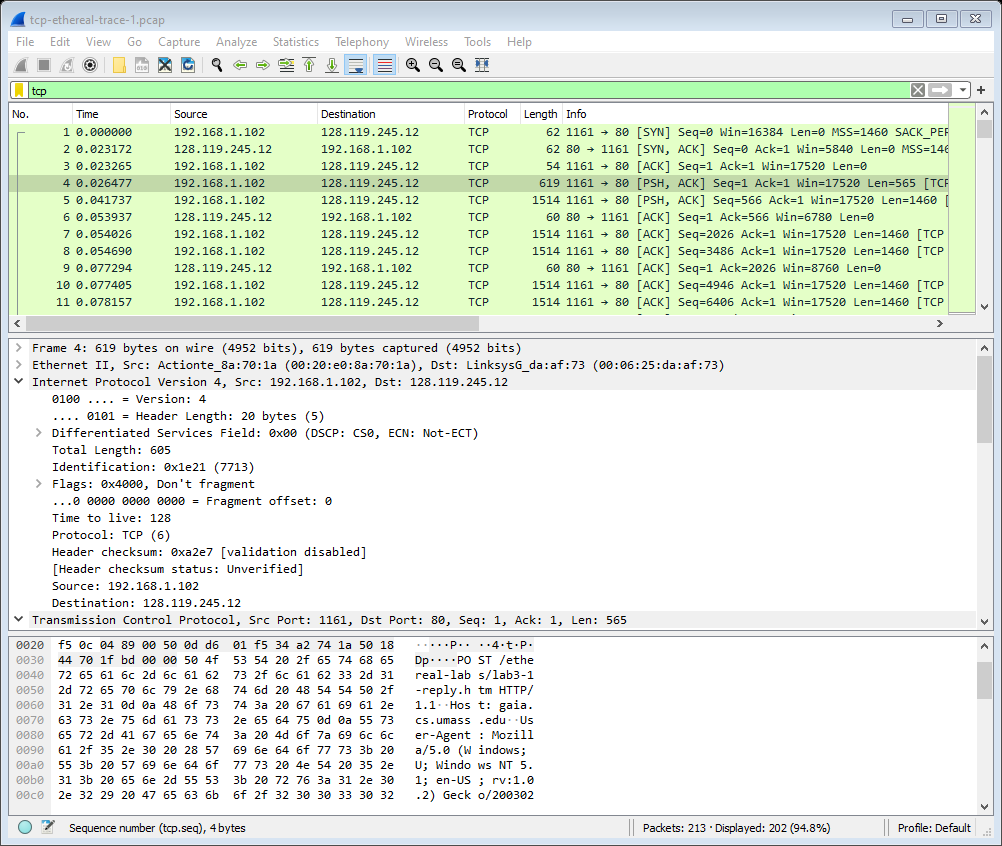
Sequence Numbers for Segments:

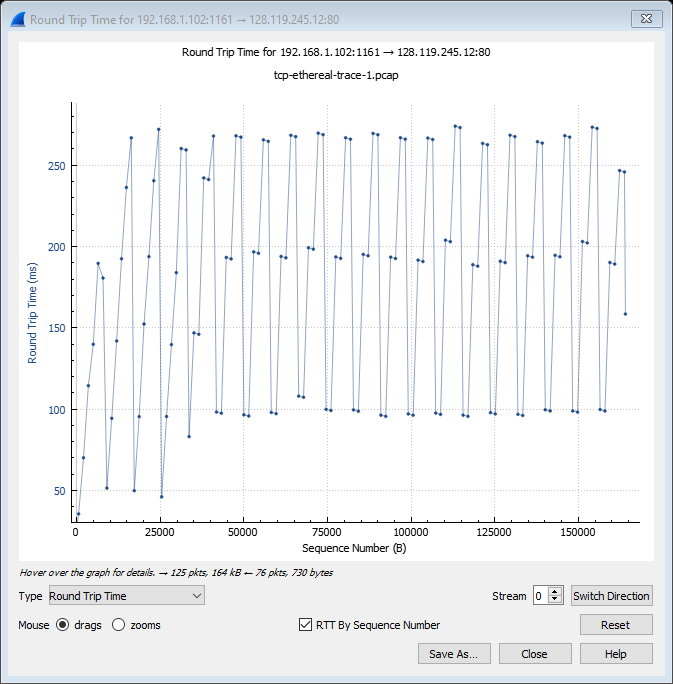
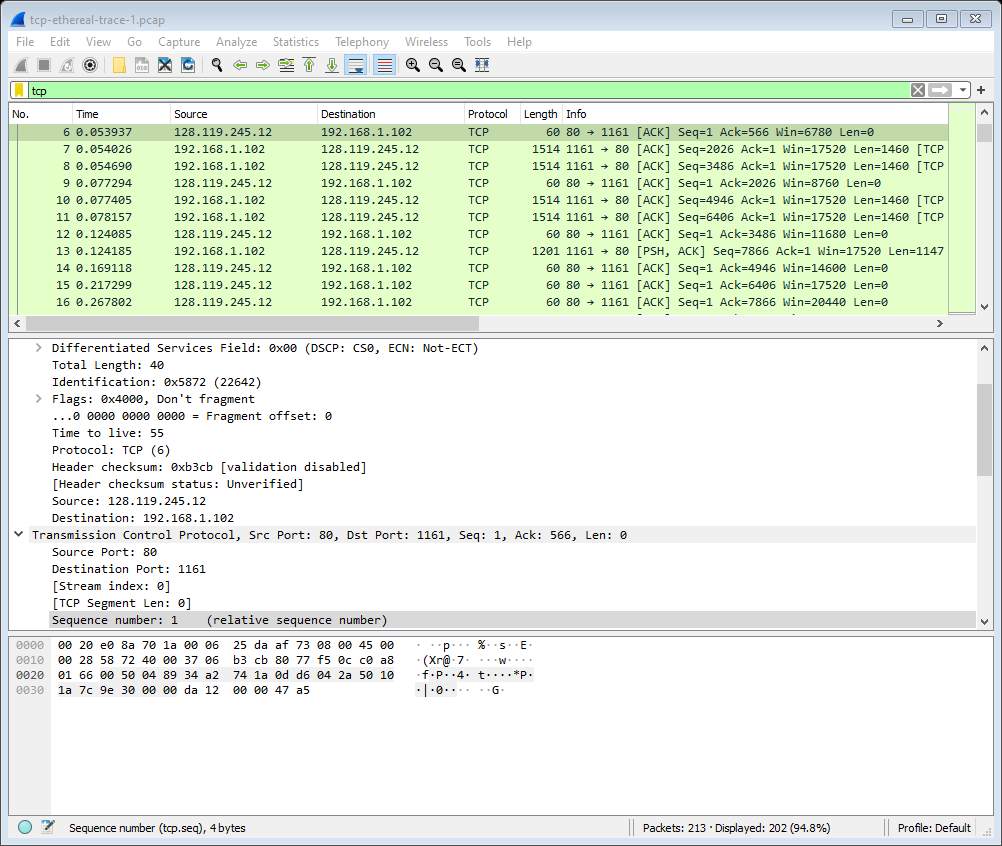
Seg 1- 1, Seg 2- 566, Seg 3- 2026, Seg 4- 3486, Seg 5- 4946, Seg6- 6406

Segments 1-6 are frames 4, 5,7,8,10, and 11. The ACK are 6,9,12,14,15

RTT ACK:

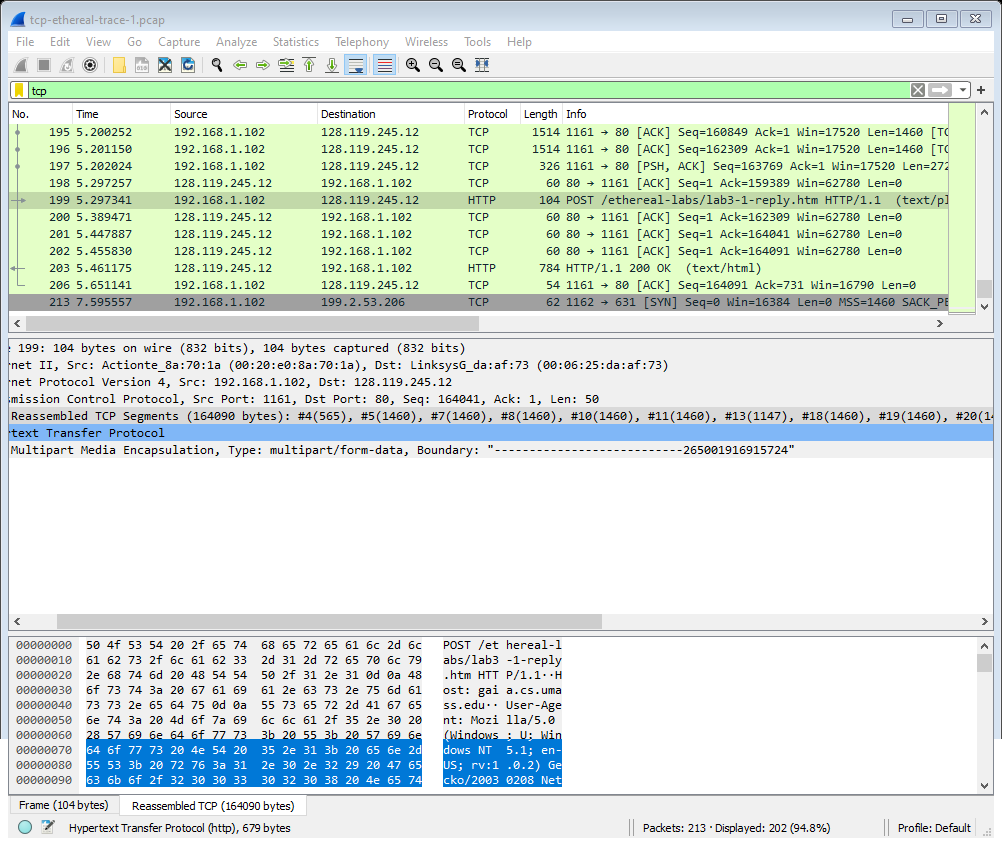
Seg 1- 0.02746, Seg2 – 0.0285, Seg3- 0.0337, Seg4- 0.0438, Seg5- 0.0558, Seg6- 0.0725





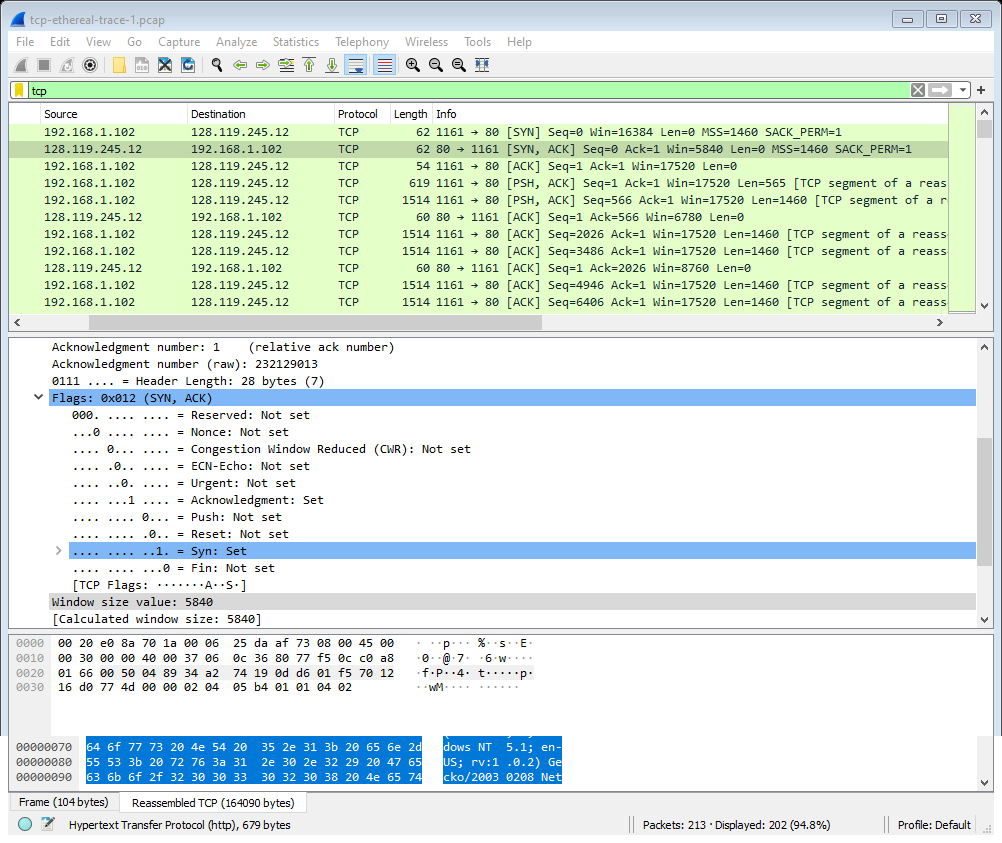
8. What is the length of each of the first six TCP segments?

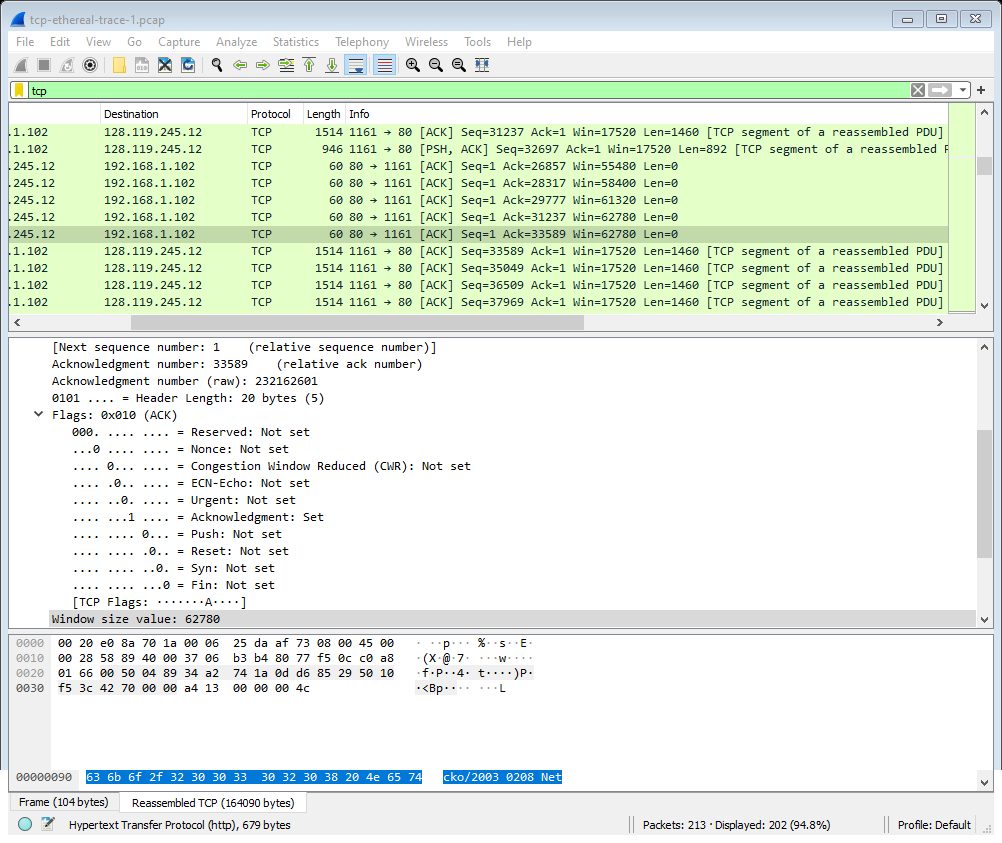
First segment is 565, and the rest are 1460 for following 5.



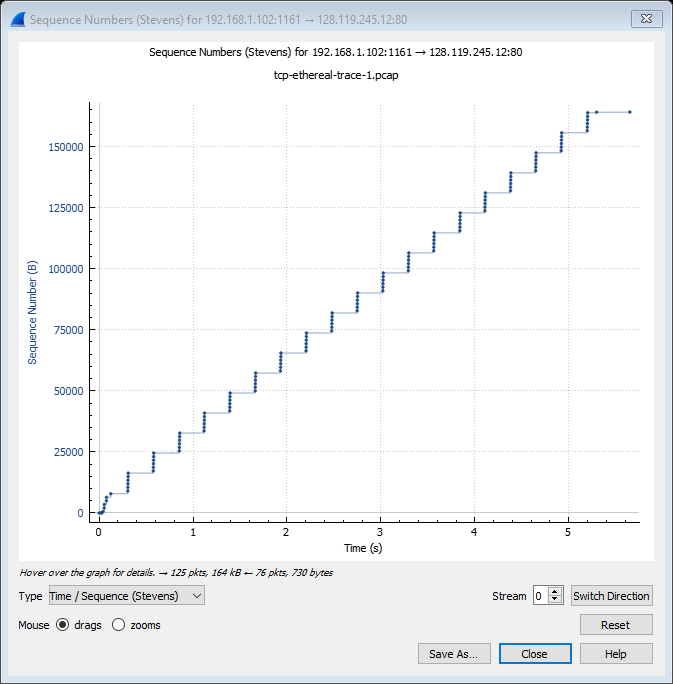
9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Minimum amount: 5840

No, it does not throttle the sender. There is a max buffer space of 62780. 



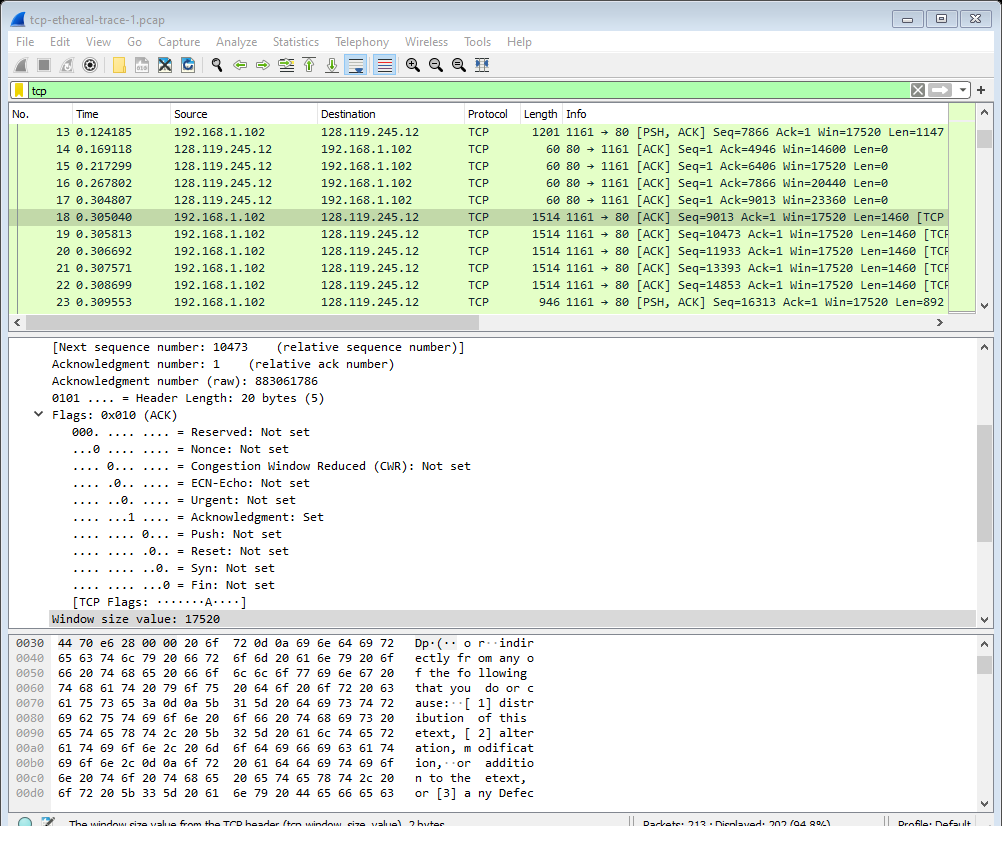
10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Does not seem to have any retransmitted segments because it continues to increase instead of going down. 

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).

1460 is acknowledge each time, I pulled a frame below.

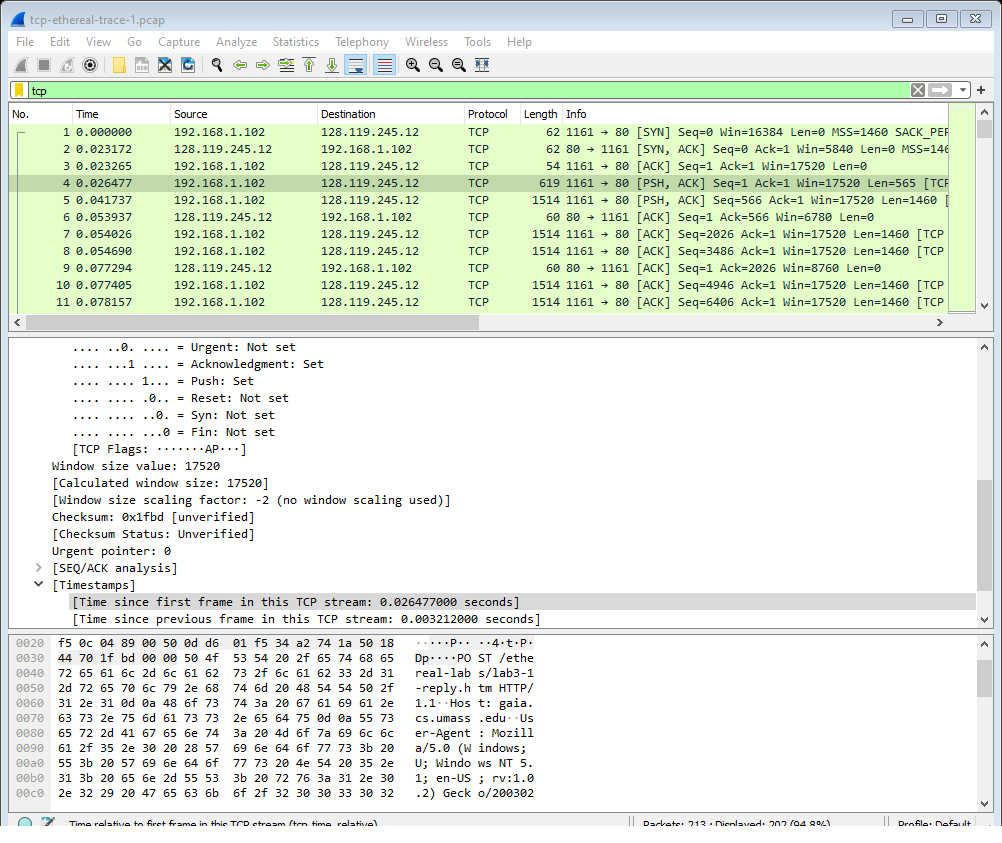
From No 18 to No 19 and increase from, 9013 to 10473

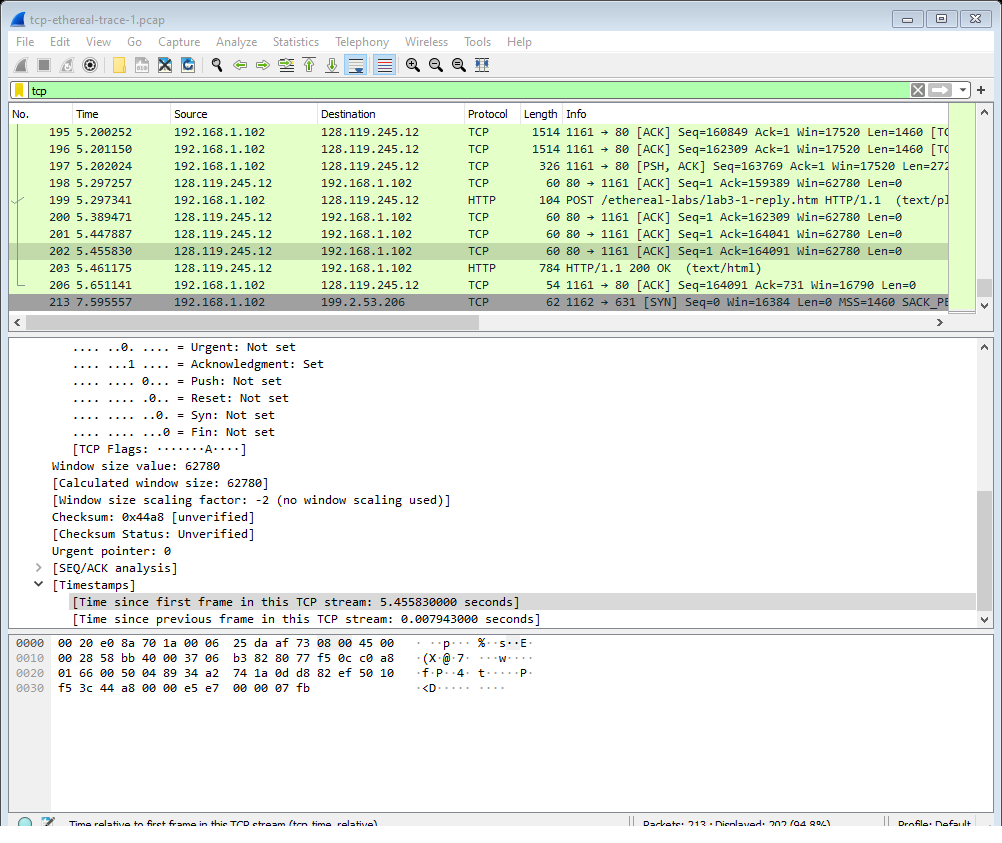


12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Sequence number starts at 1 on frame 4 and ends at 202, with ACK being 164091. So, 164091 – 1 = 164090 bytes. I am trying to find the time so I use transmission time, therefore I do the same with transmission time. Frame 4 – 0.26477, Frame 202 – 5.45583. 5.45583 – 0.026477 is 5.429353

Now I take , 164090 / 5.429353 = 30.222 Kbs for the throughput.





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.

Slow start from 0-13 , and avoidance congestion 199-206.