**Wireshark Lab 1: TCP**

**EEL 6935 (Spring 2019)**

**DATA NETWORKS, SYS & SECURITY**

 **PROJECT 1**

Department of Electrical Engineering

Under the Guidance of

**Prof Nasir Ghani**

**Submitted by**

**SAI KRISHNA KANDAGATLA**

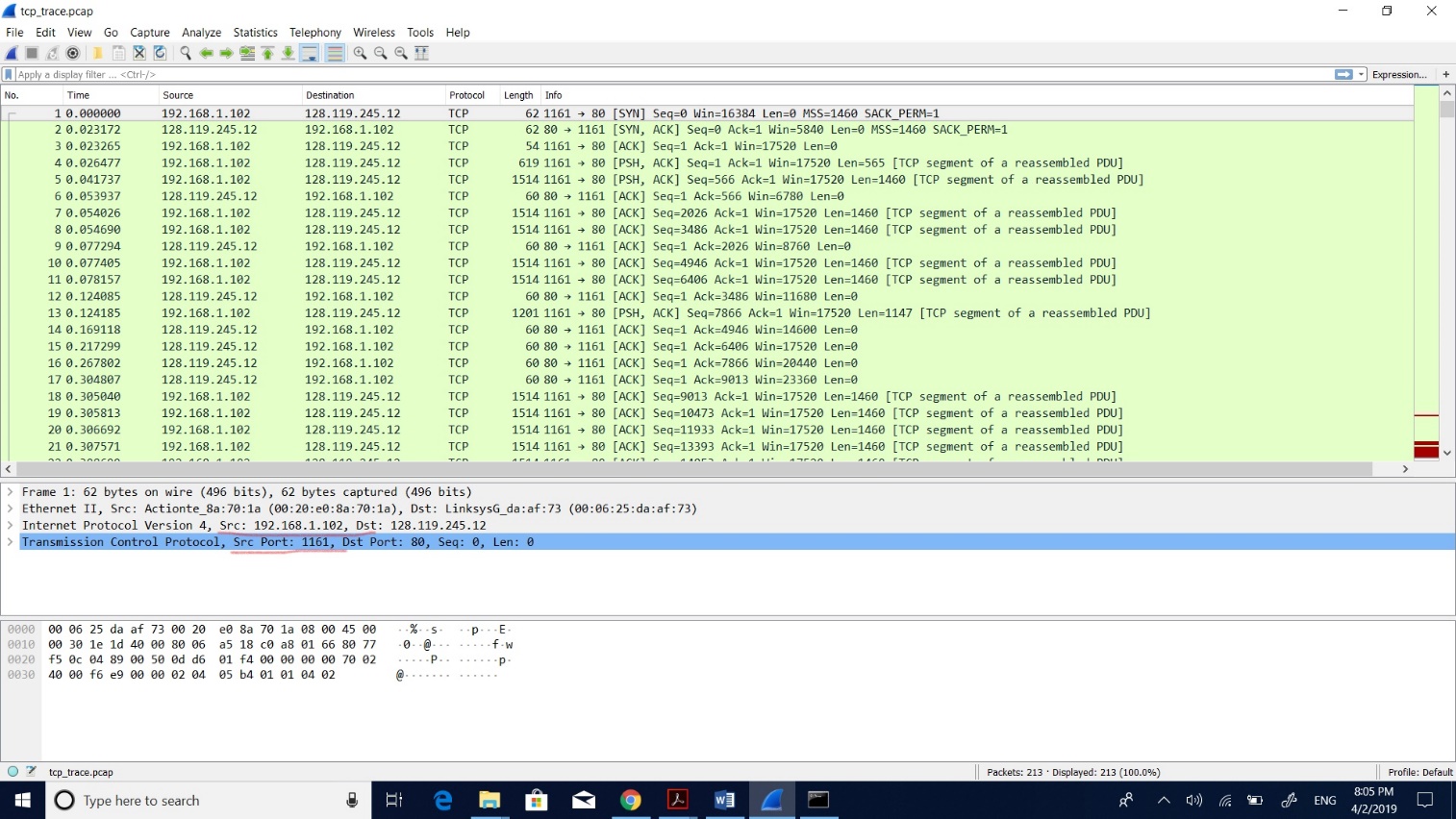
**U15974415**

**WIRESHARK LAB 1: TCP**

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, note that it is easier to select a 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”).

**Solution:**

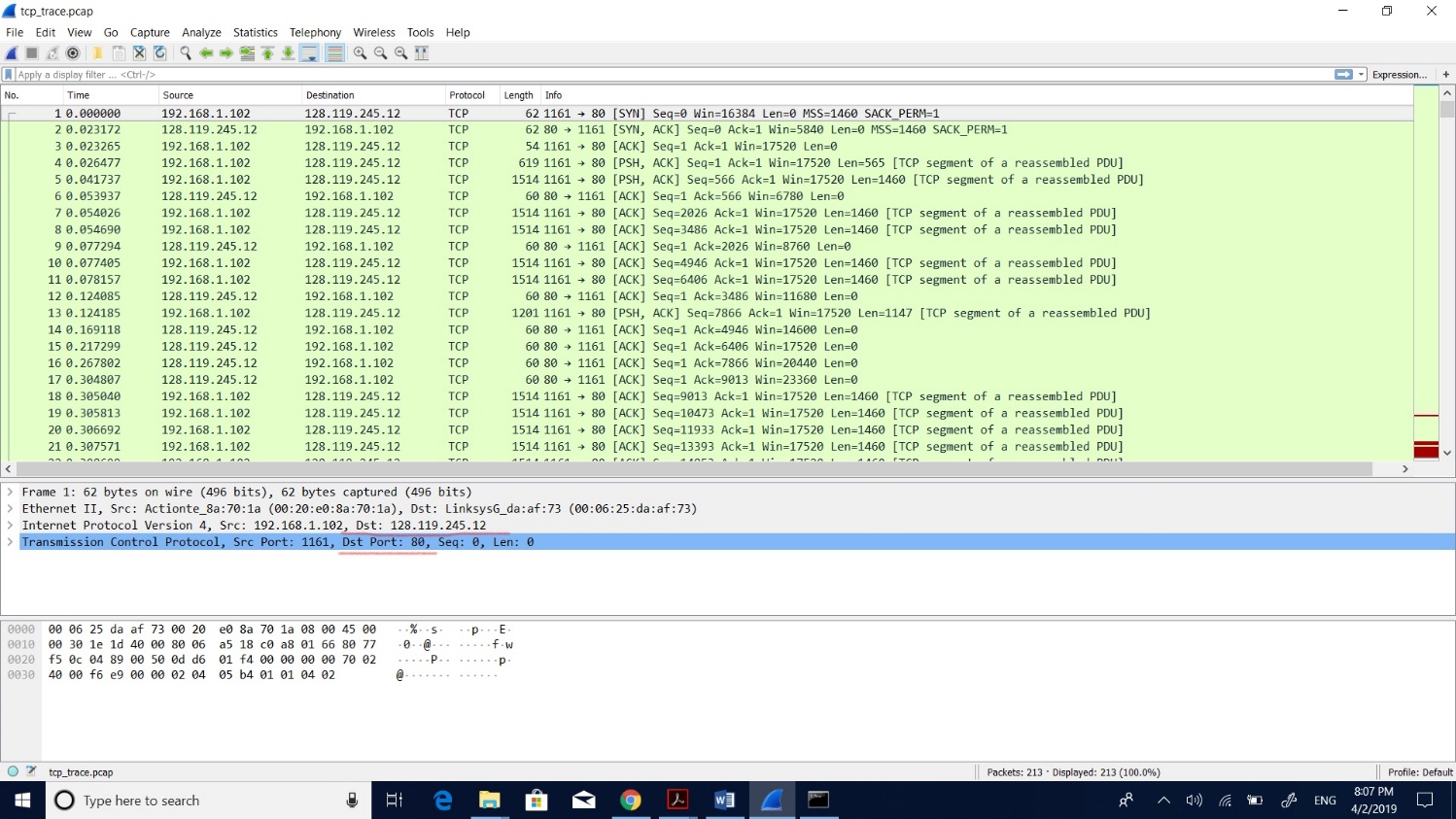
The source is client computer and the destination is gaia.cs.umass.edu for file transfer. The client computer (source)IP address is 192.168.1.102 and the client computer (source)TCP port number is 1161.

****

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?

**Solution:**

The destination computer (gaia.cs.umass.edu) IP address is 128.119.245.12 and the destination computer (gaia.cs.umass.edu) TCP port number is 80 for sending and receiving TCP segments.

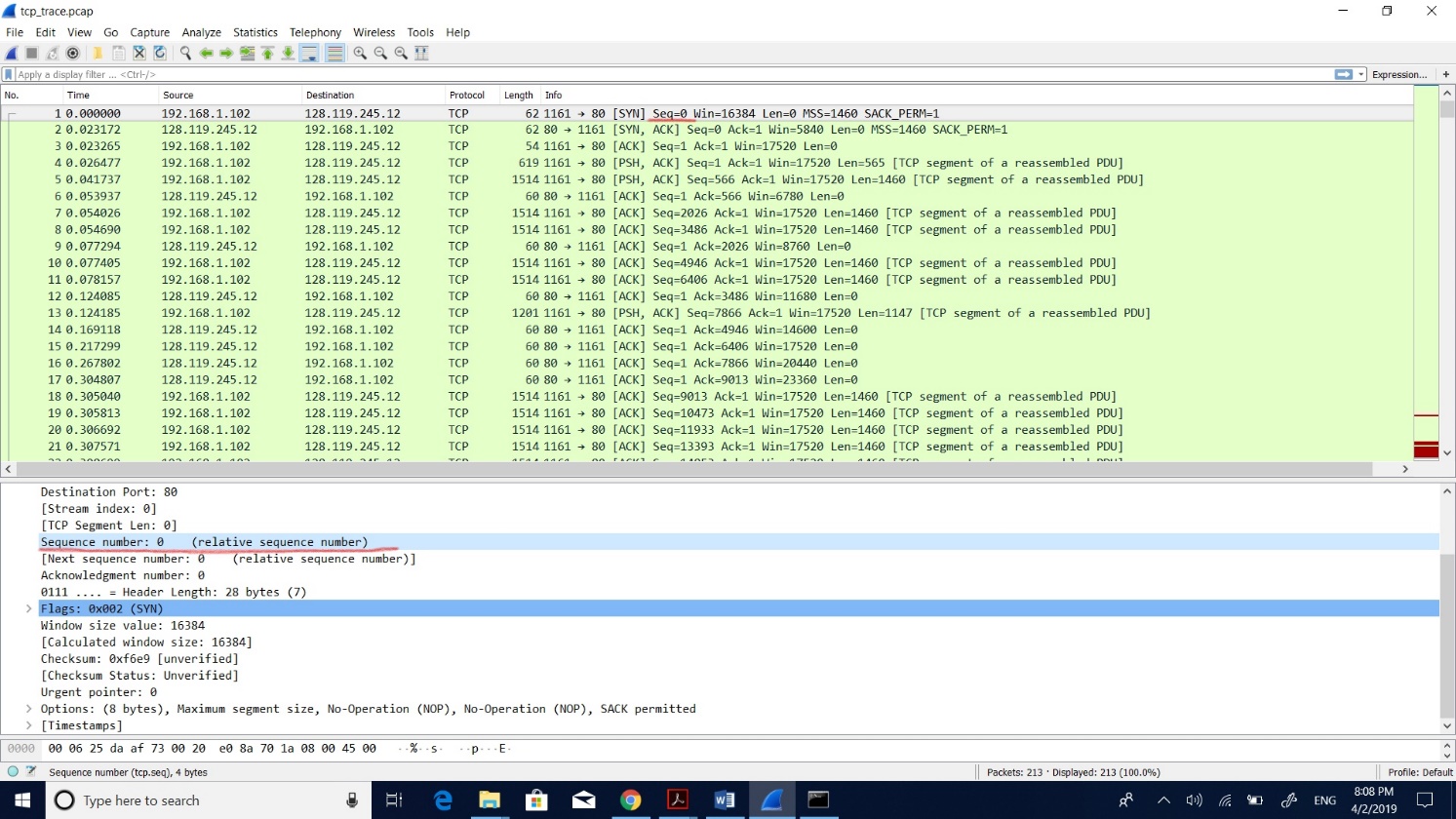
****

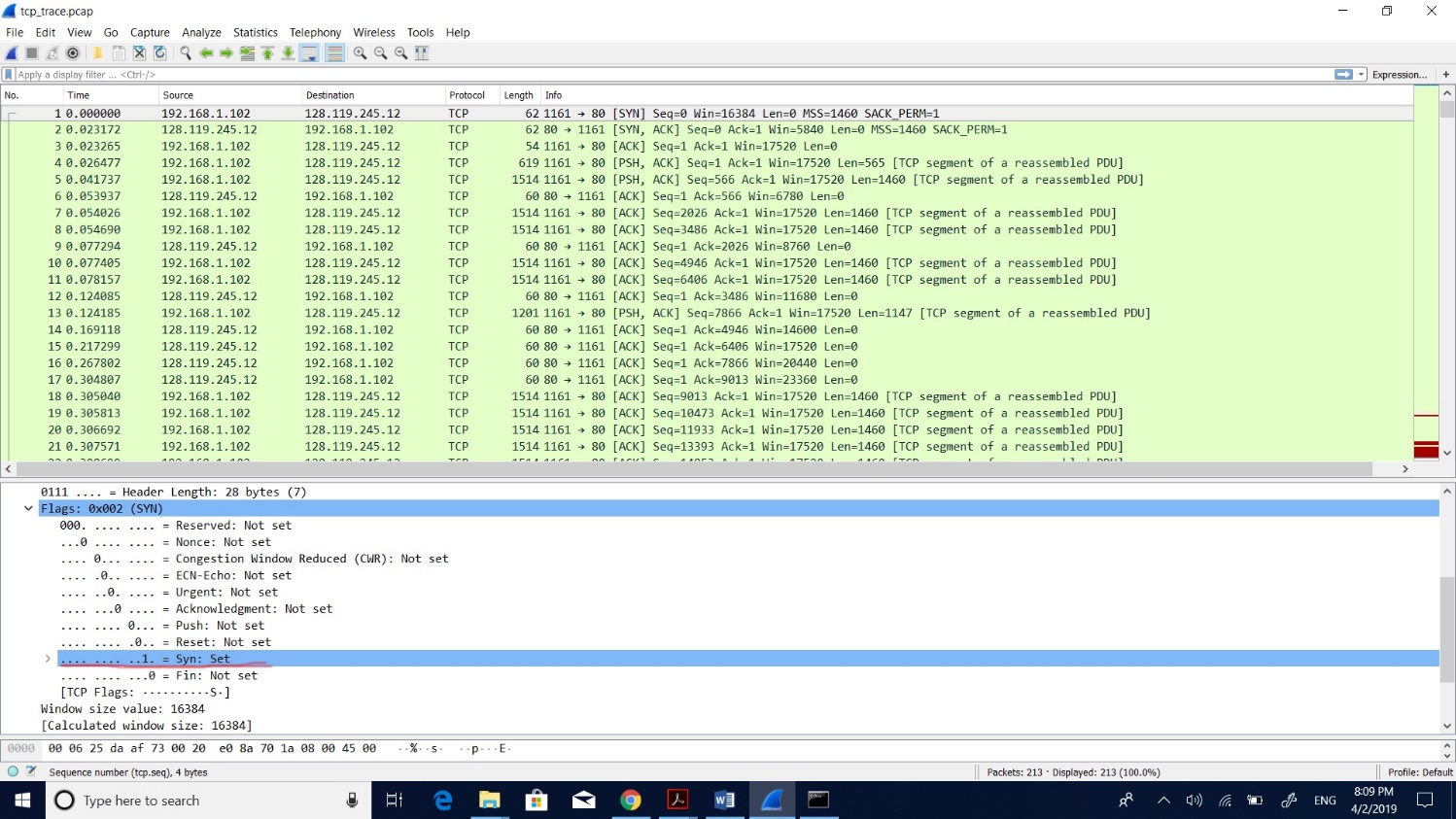
3)**TCP BASICS**

1) 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?

**Solution:**

The sequence number of the TCP SYN segment is usually used to establish the TCP connection. The segment identifies that SYN flag is 1 so we can see it as SYN segment. The value of sequence number of TCP SYN segment is 0.

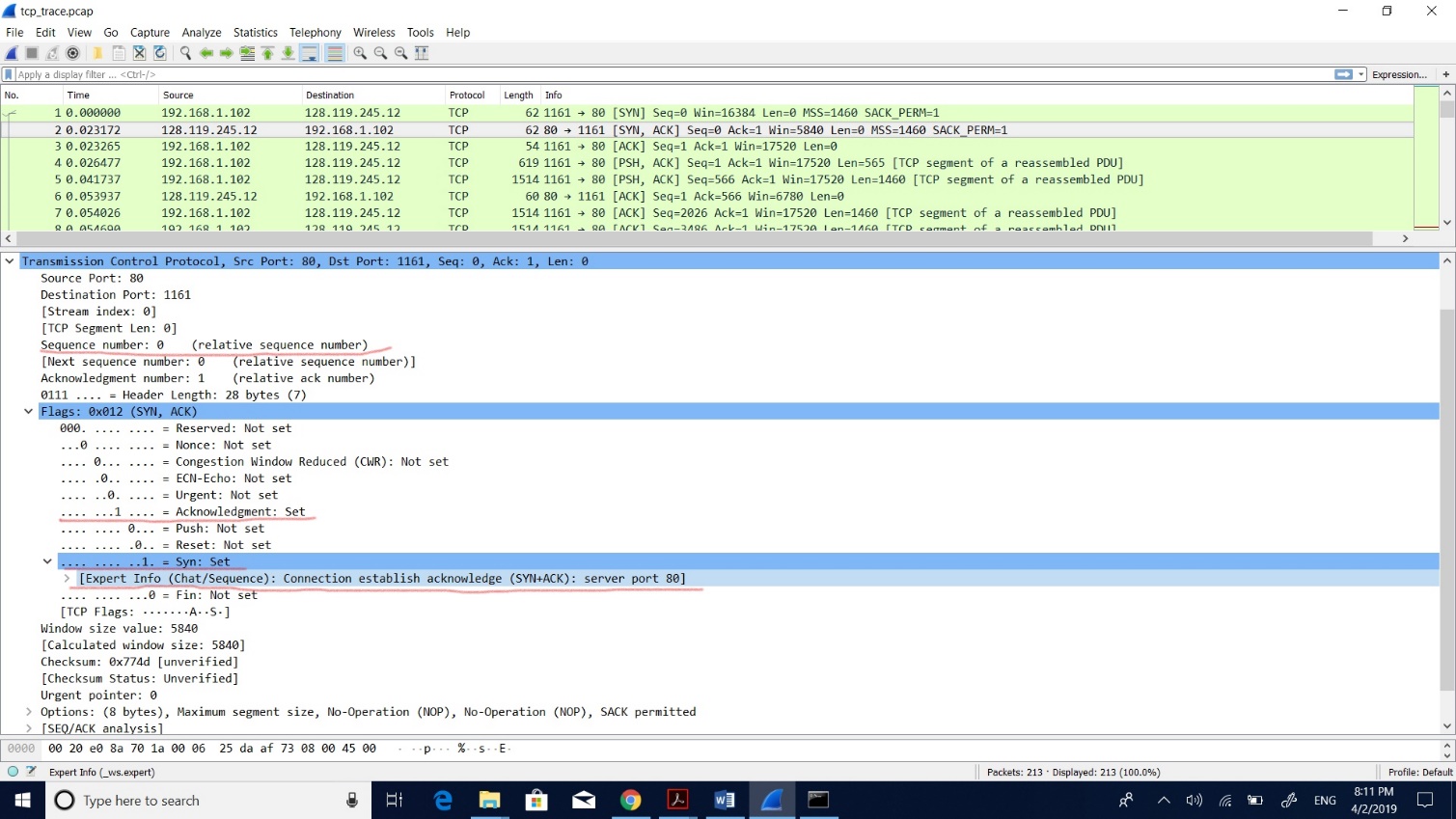




2) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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

**Solution:**

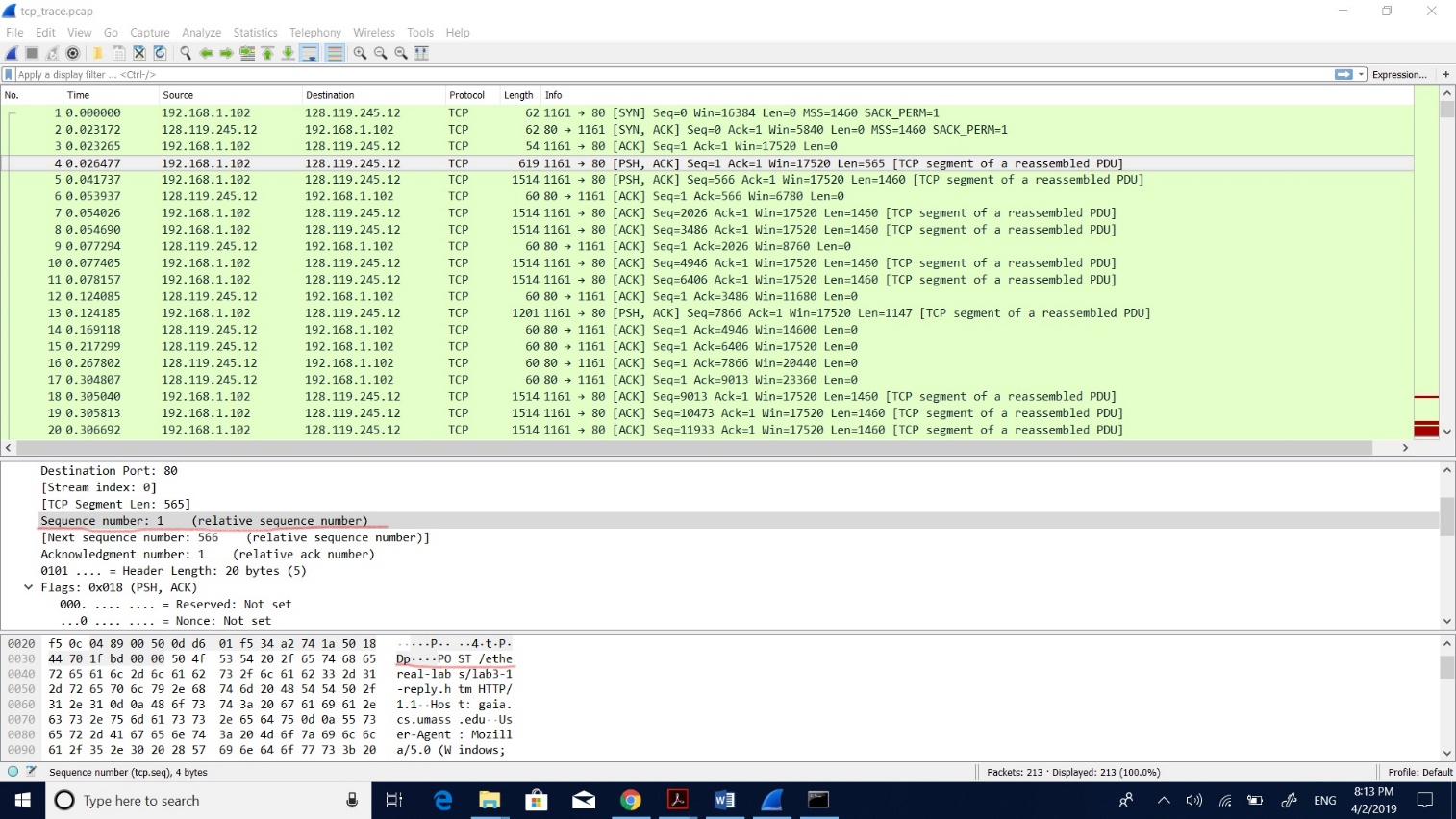
The sequence number of the SYNACK segment sent is 0. The value of acknowledgement field is 1. It is determined by the gaia.cs.umass.edu by increasing 1 to the initial sequence number of SYN segment from the client computer. The SYN and Acknowledgement flags are both set to 1, So we can see it as a SYNACK segment.



3) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you will need to check the packet content field at the bottom of the Wireshark window, i.e., for a segment with a “POST” within its DATA field.

**Solution:**

The sequence number of the TCP segment containing the HTTP POST command is 1.

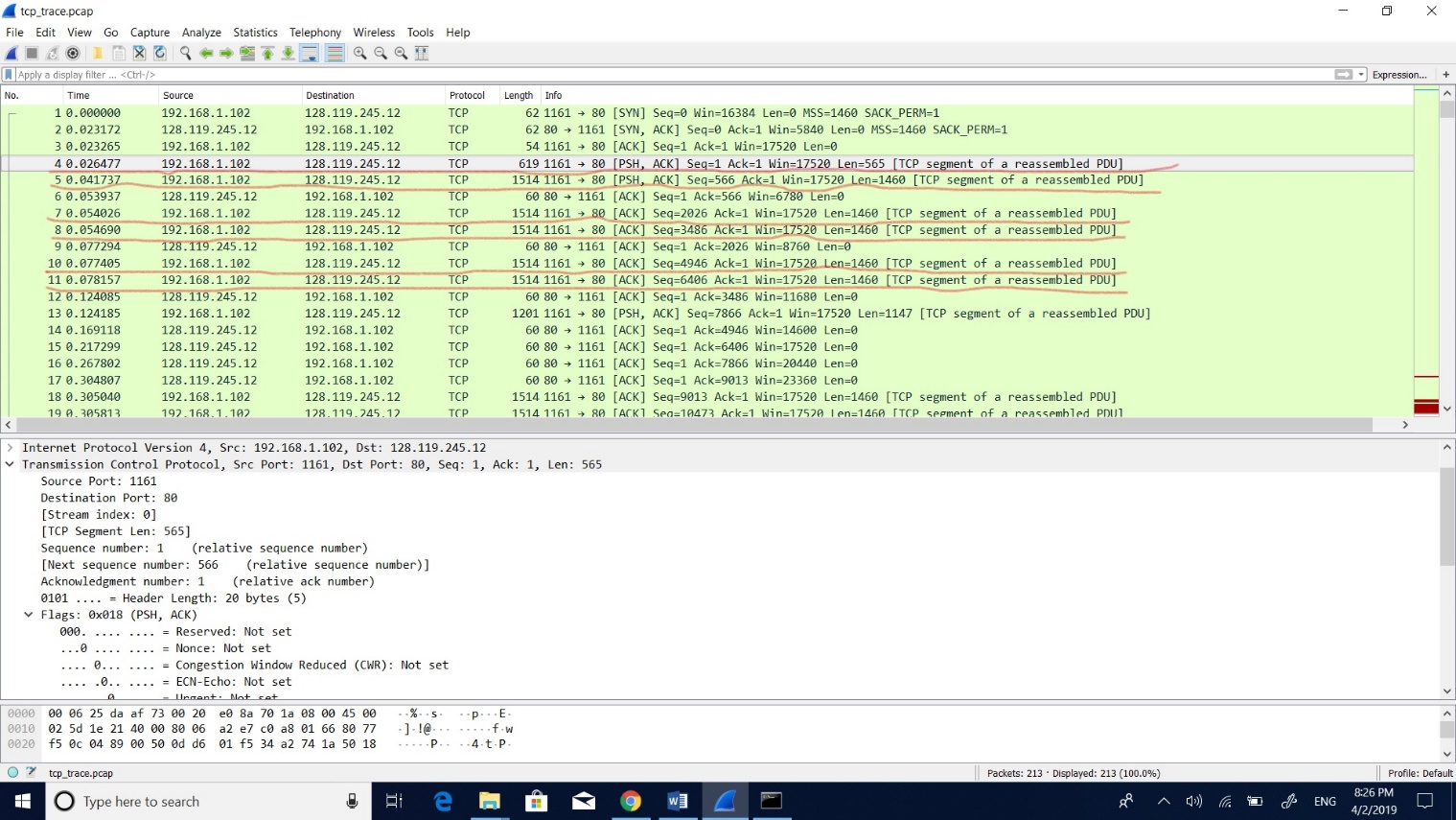


4) Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? When was each segment sent? When was the ACK for each segment received? Given 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? Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph>Round Trip Time Graph.

|  |  |
| --- | --- |
| Segment | Sequence number |
| 1 | 1 |
| 2 | 566 |
| 3 | 2026 |
| 4 | 3486 |
| 5 | 4946 |
| 6 | 6406 |

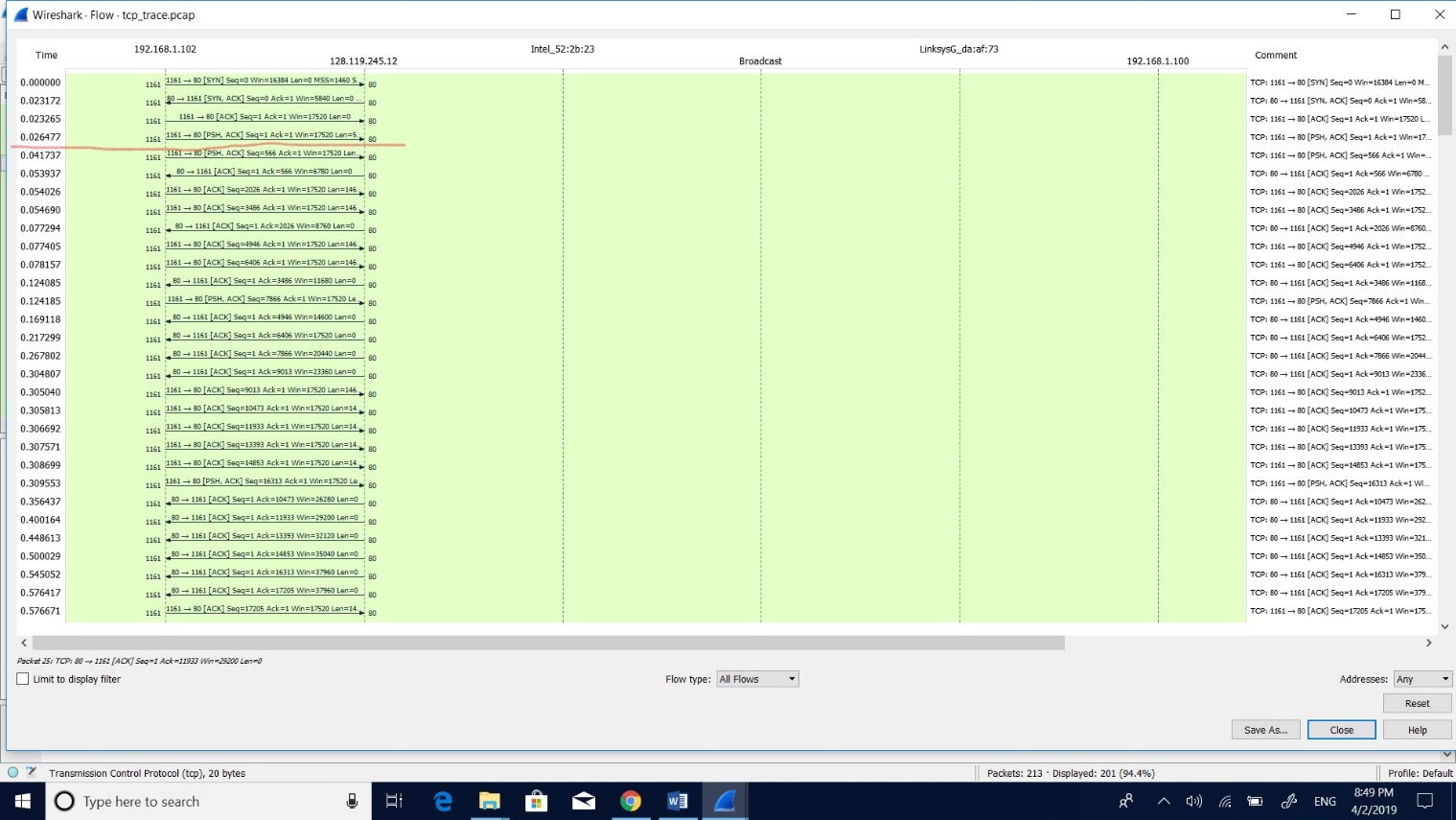
**Solution:**

The table above and screenshot below gives the sequence numbers of the first six segments considering the TCP segment containing the HTTP POST as the first segment.

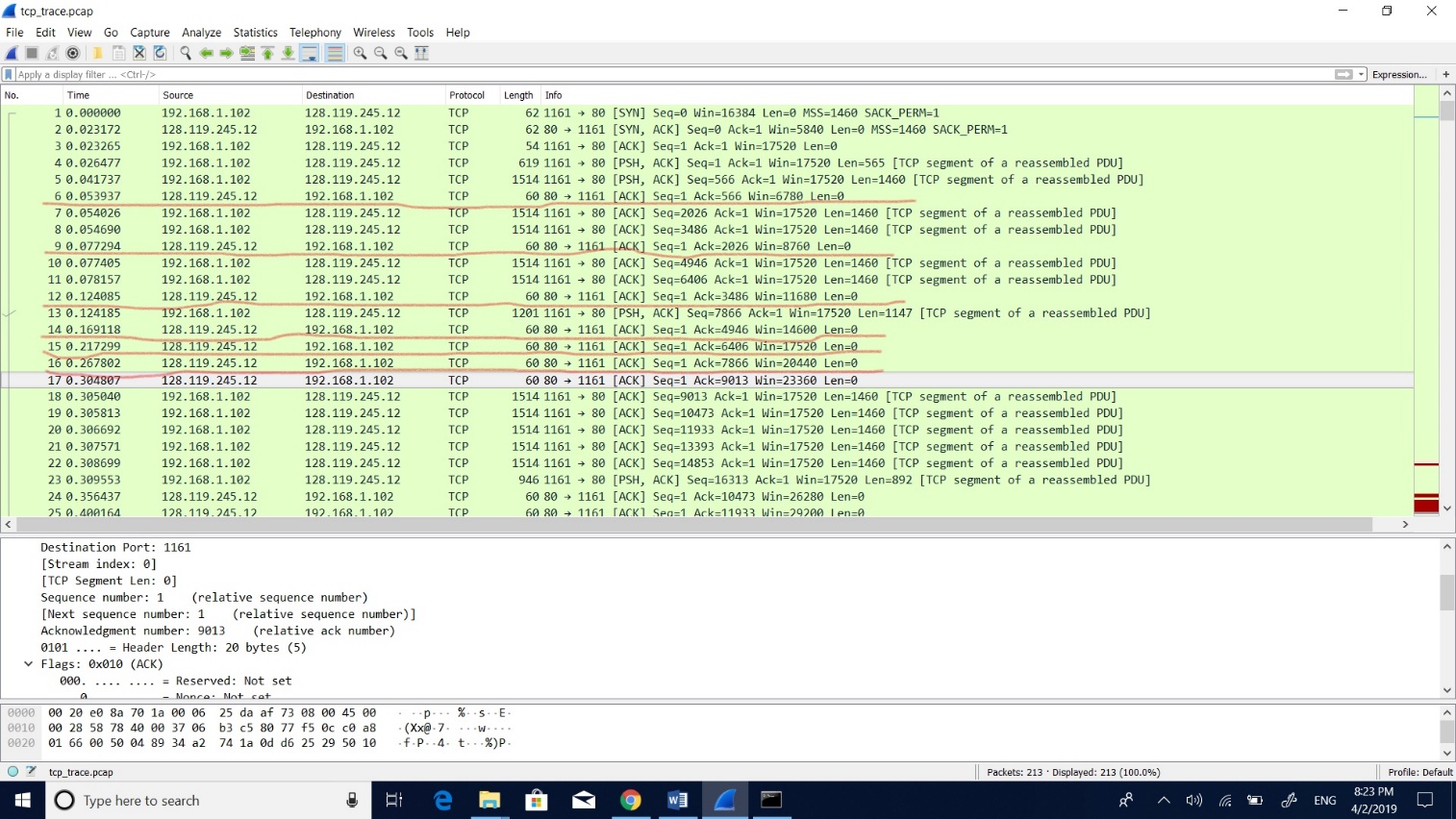


|  |  |  |  |
| --- | --- | --- | --- |
| Sequence number | Sent time | Received time | RTT= (received time-sent time) |
| 1 | 0.026477 | Acknowledgement not received | Hence, we can’t determine it |
| 566 | 0.041737 | 0.053937 | 0.0122 |
| 2026 | 0.054026 | 0.077294 | 0.023268 |
| 3486 | 0.05469 | 0.124085 | 0.069395 |
| 4946 | 0.077405 | 0.169118 | 0.091713 |
| 6406 | 0.078157 | 0.217299 | 0.139142 |

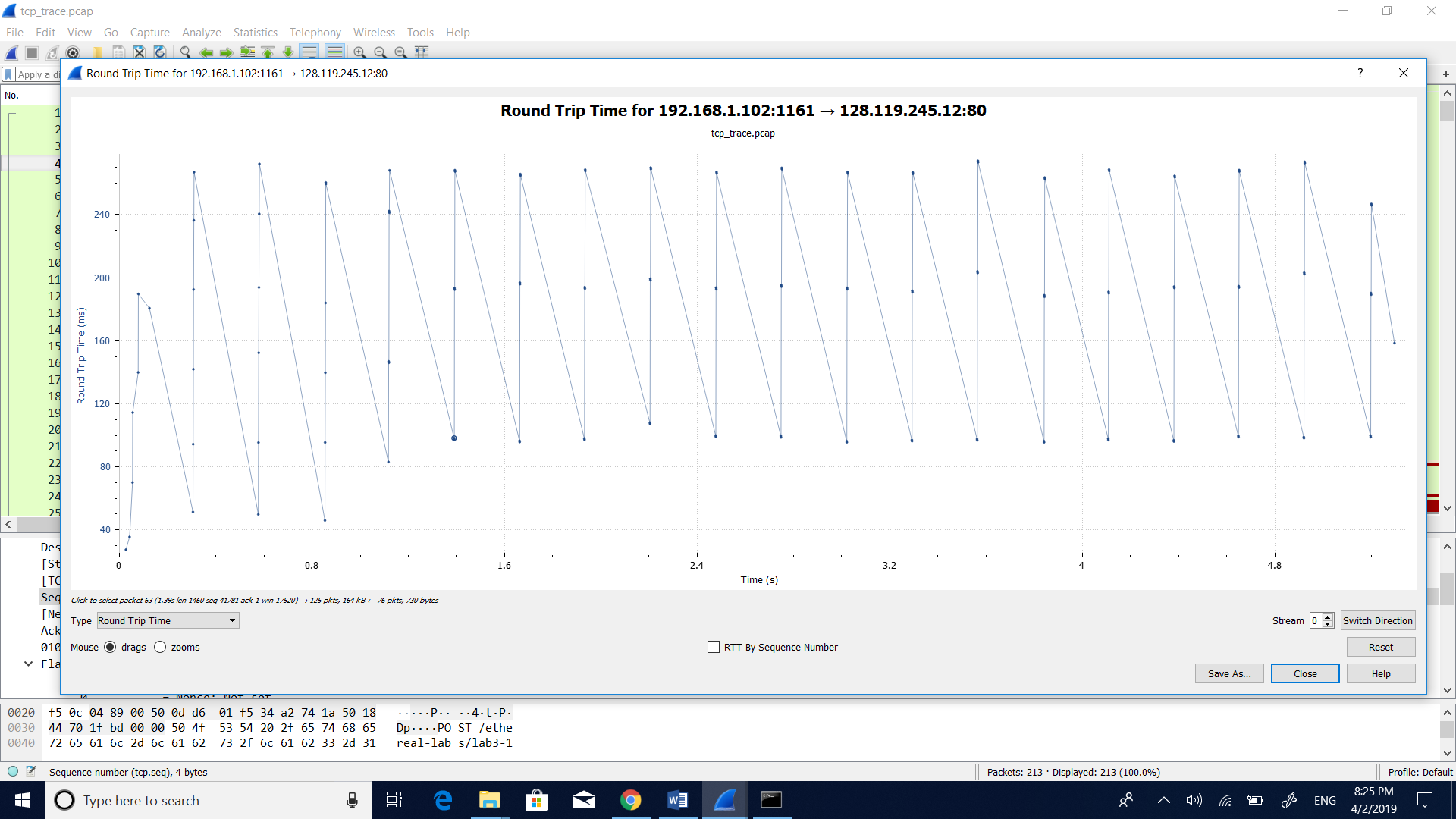
The table above and screenshot below shows sent time, received time and difference i.e., RTT for the first six segments considering the TCP segment with http post as the first segment.



The screenshot below shows the acknowledgment values of first six segments considering the TCP segment with http post as the first segment.



The screenshot below shows the Round-Trip Time graph in which time on the X-axis and the Round-trip time on Y-axis.



5) What is the length of each of the first six TCP segments?

**Solution:**

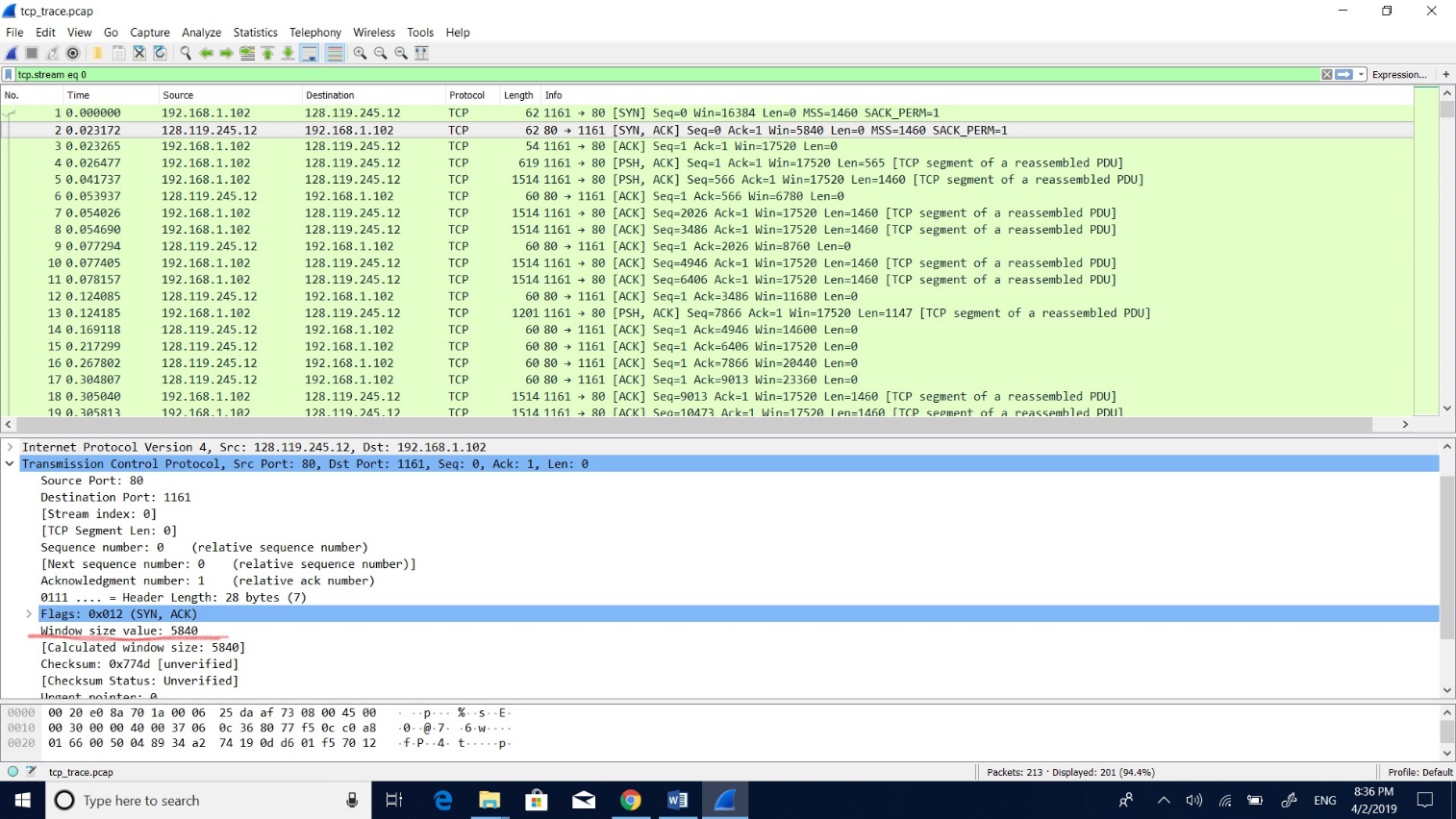
The length of each of the TCP segments are 565, 1460, 1460, 1460, 1460, 1460 respectively for the first six segments.



6) 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?

**Solution:**

The minimum amount of buffer space received for the entire trace is 5840 bytes. No, the sender is never throttled because of lack in buffer space.

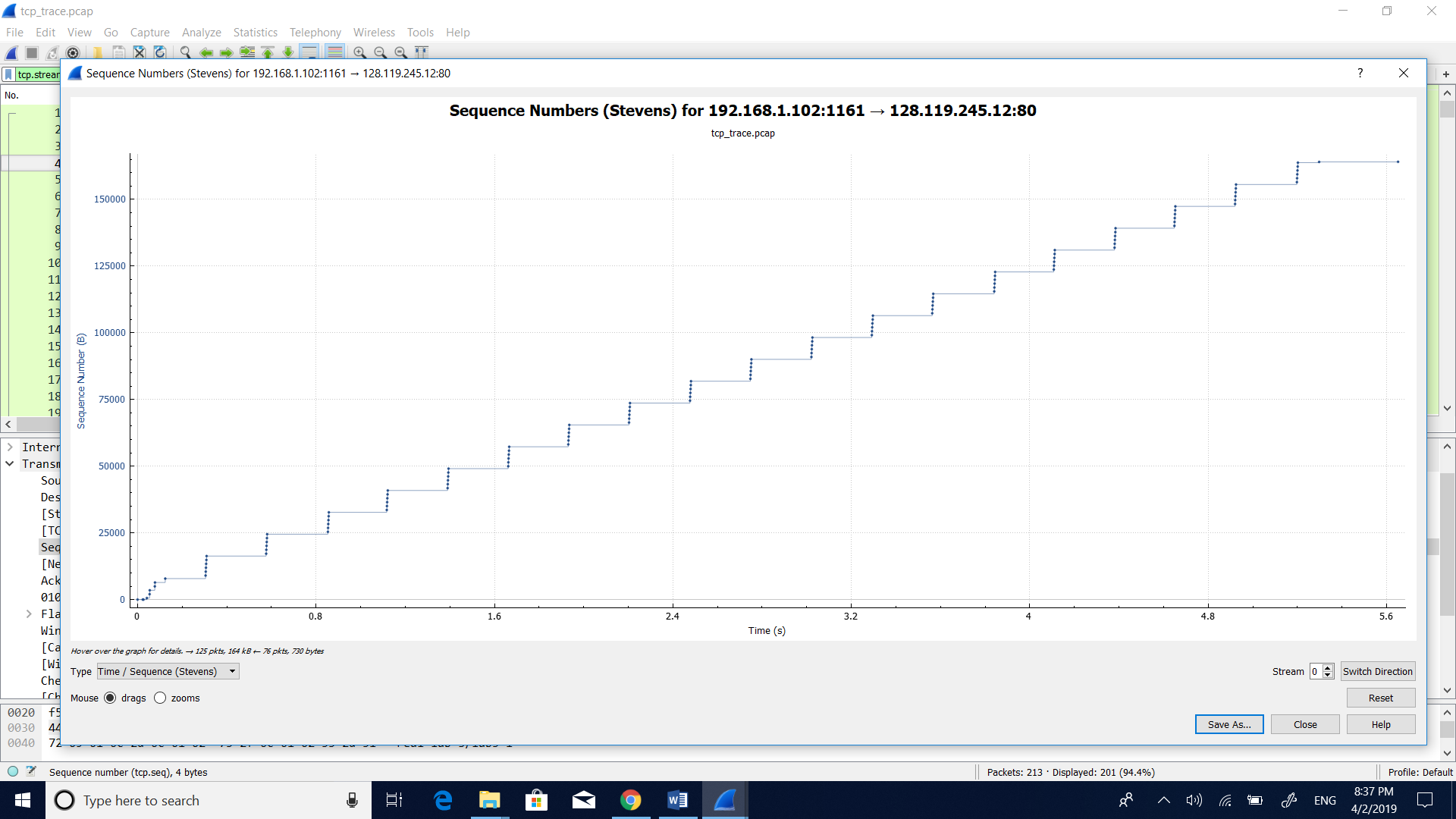


7) Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

**Solution:**

No, there are no retransmitted segments in the trace file. In the graph below the sequence numbers are increasing stepwise such that there will be no retransmitted segments.

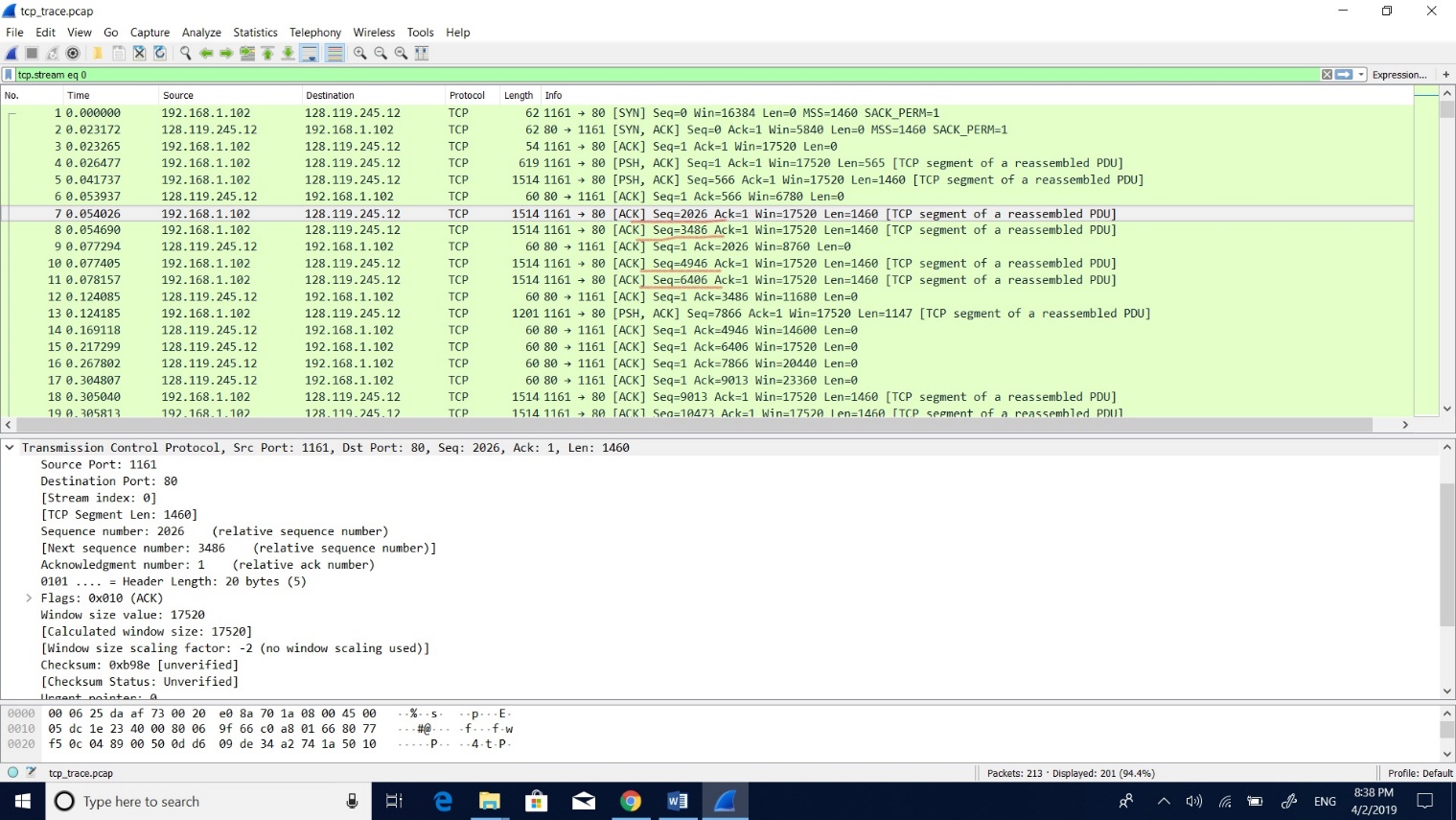
The screenshot below shows the Time Sequence graph (Stevens) in which time on the X-axis and the Sequence number on the Y-axis.



8) How much data does the receiver typically acknowledge in an ACK?

**Solution:**

The receiver typically acknowledges 1460 bytes of data in an ACK. The corresponding sequence numbers are 1,566,2026,3486,4946,6406,7866,9013 and more in this trace. The difference between the two ACK’s gives the ACK acknowledged at every 1460 bytes.



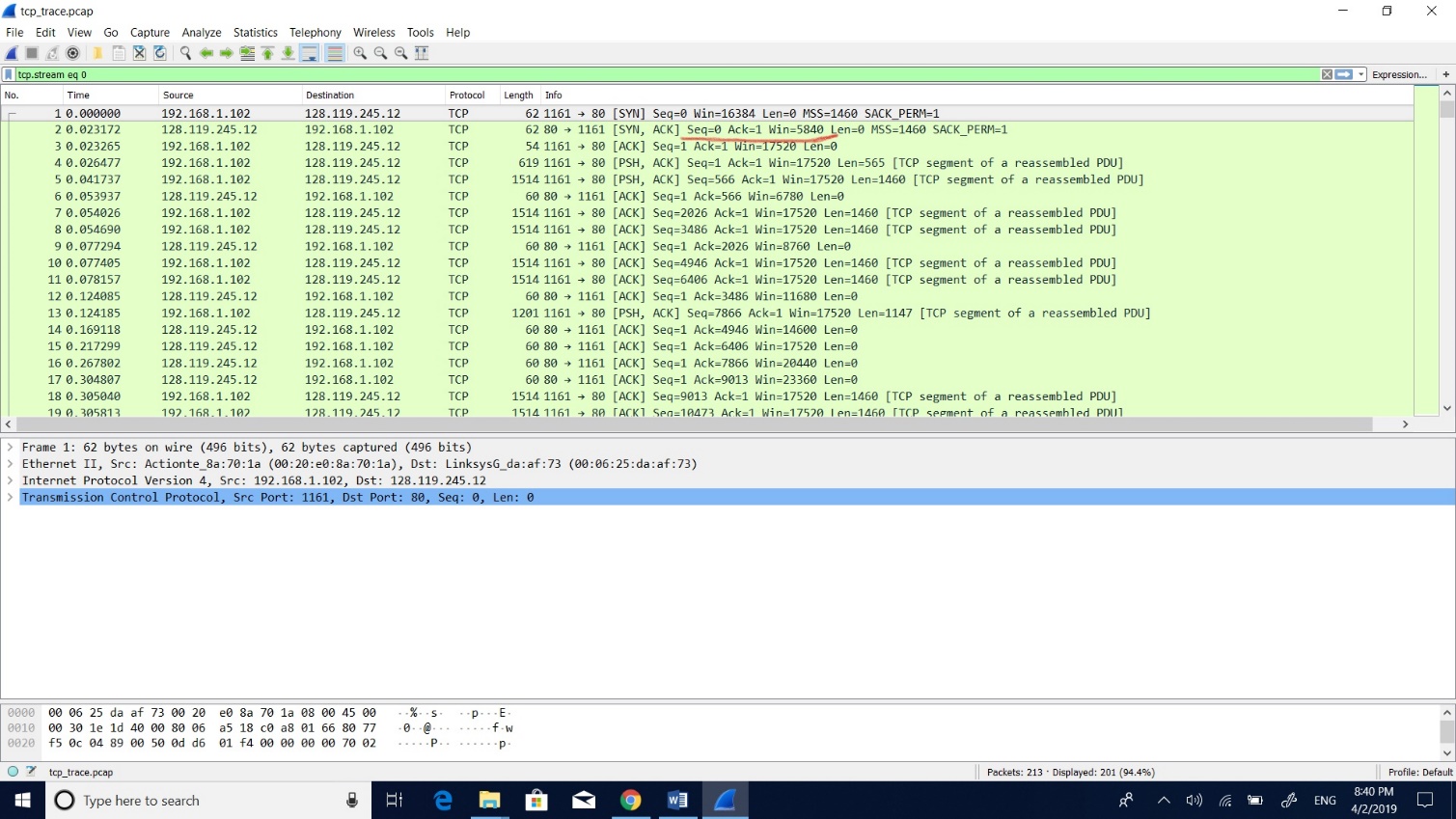
9) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

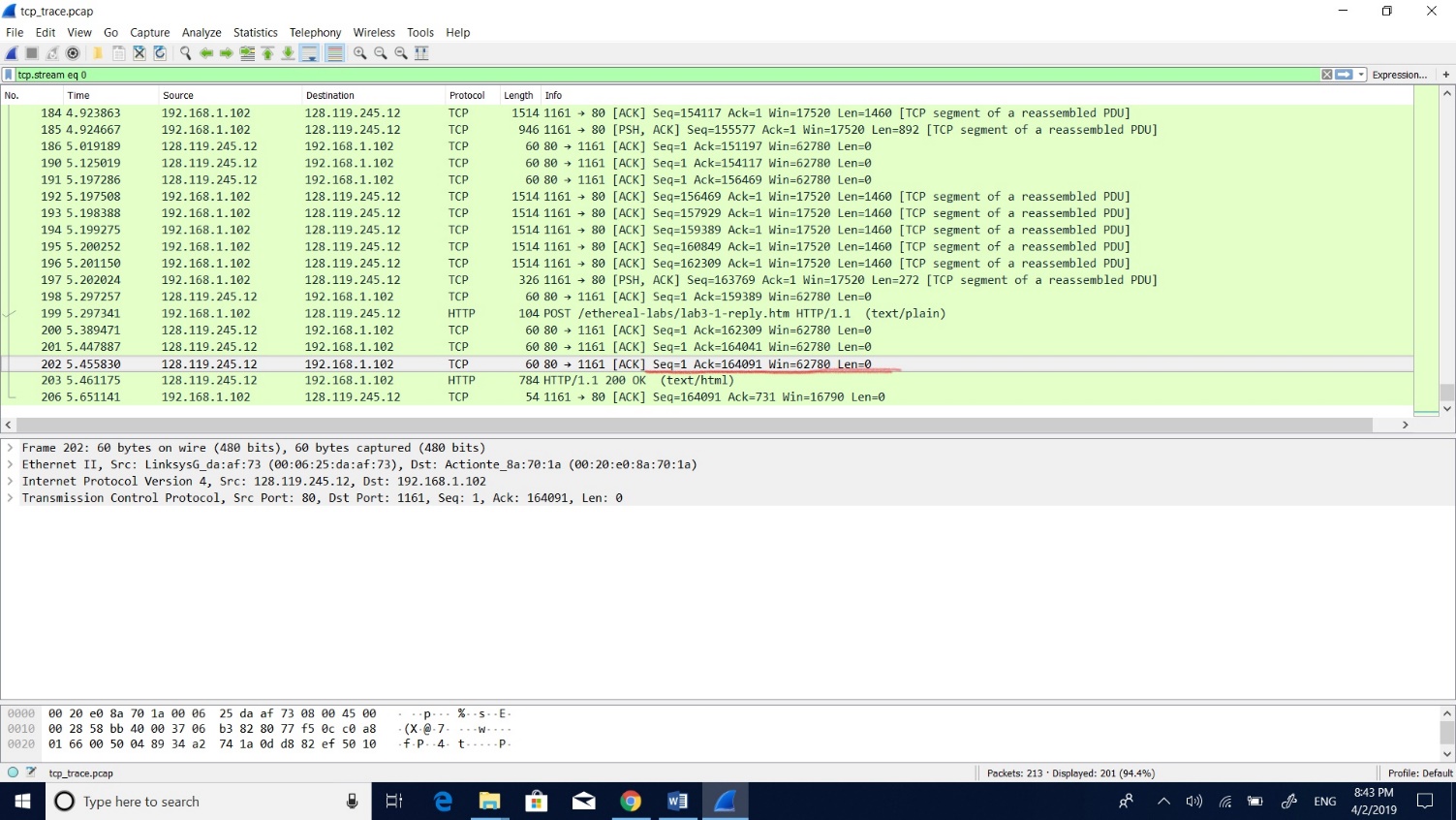
**Solution:**

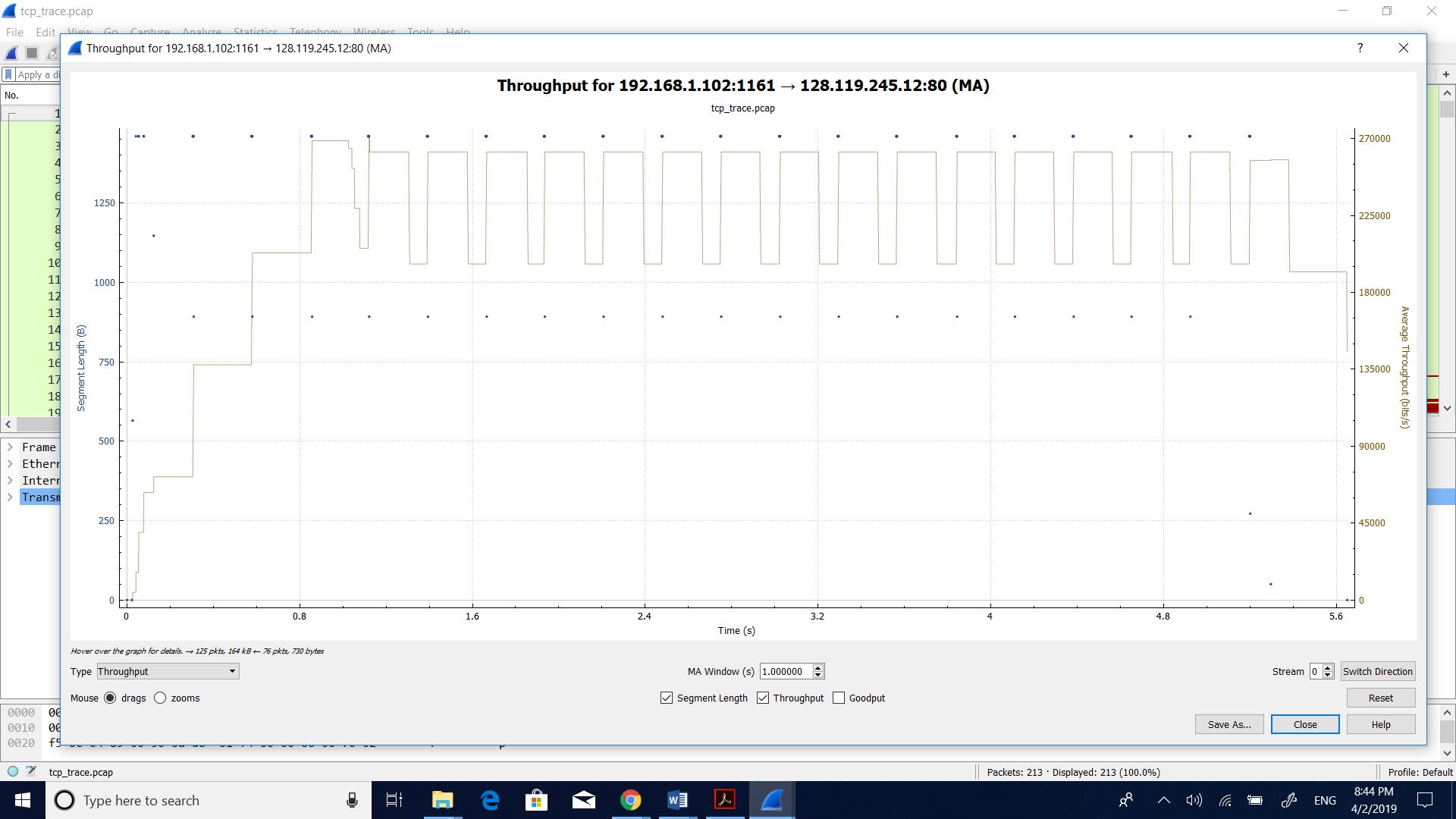
Formula for Throughput for the TCP connection is Throughput=Total transmitted data/Total transmission time.

It is shown that the total amount of data=First sequence – last ACK data. The total data is 164091 – 1 = 164090 bytes and the total transmission time = Time of first TCP segment – Time of the last ACK. The total transmission time is 5.455830 – 0.026477 = 5.4294 seconds.

Finally, Throughput =164090/5.4294=30.22 Kbytes/sec.







4)**TCP Congestion Control in action**

10) Use the Time-Sequence-Graph 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 slow start 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?

**Solution:**

The TCP's slow begins at 0sec to 0.13sec and the avoidance begins there. From the congestion avoidance we get the value of the congestion window size value and with the win=17520 of the TCP sender. Then the congestion avoidance takes place at the sequence number 7866 and at the time 0.1242 sec where the slow start ends. The measured data sent is 8192 bytes which cannot increase more than the half window size due to the congestion avoidance.

