Project 3

Wireshark Lab: TCP

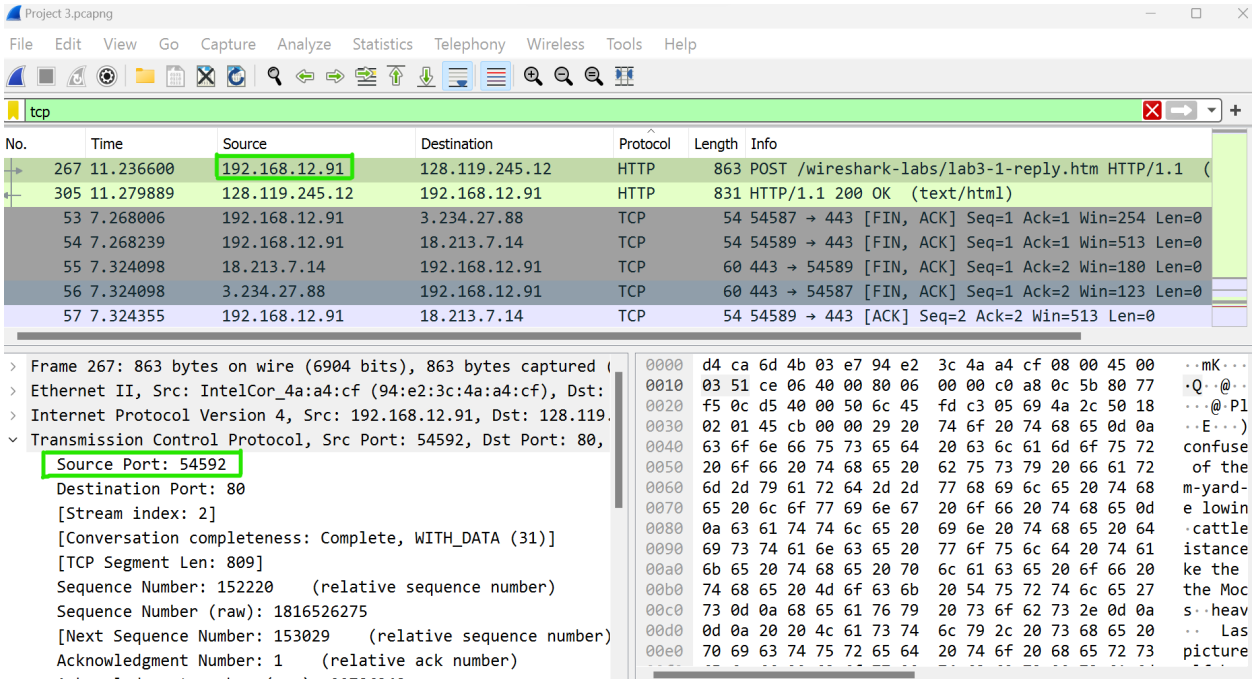
Puja Shah

CSIT-340-11 Computer Networks

Summer 2023

Dr. Murtadha Aldeer

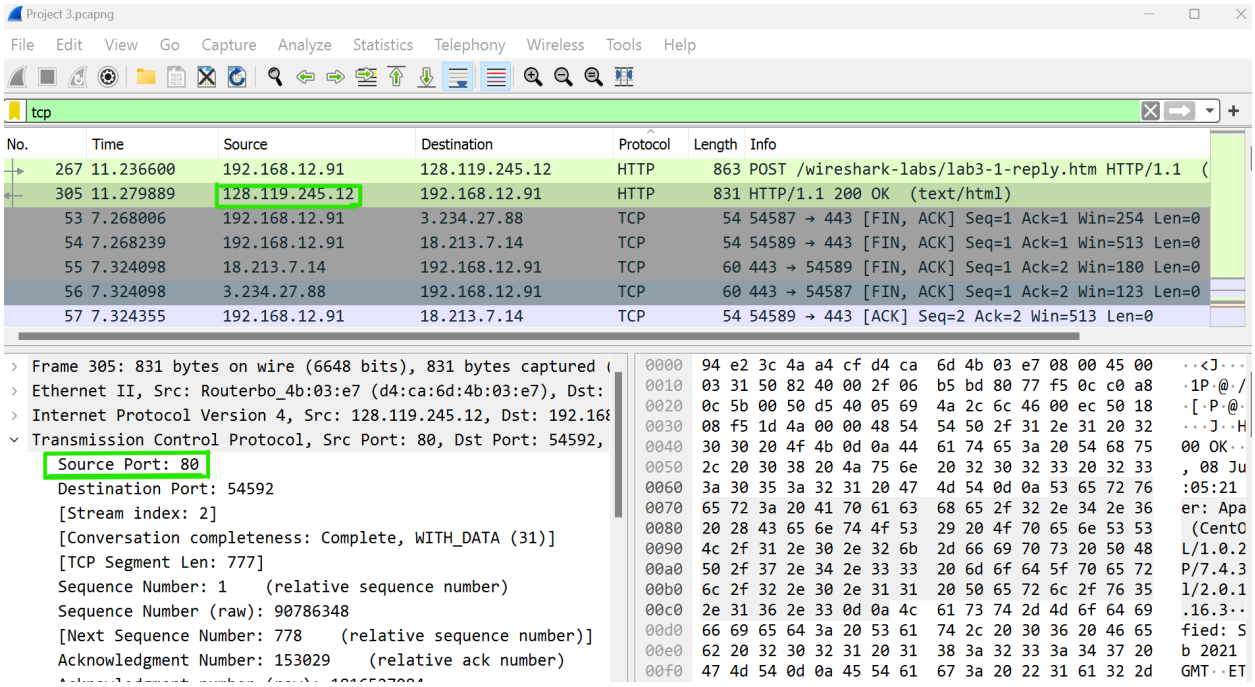
1. **What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details 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: 192.168.12.91

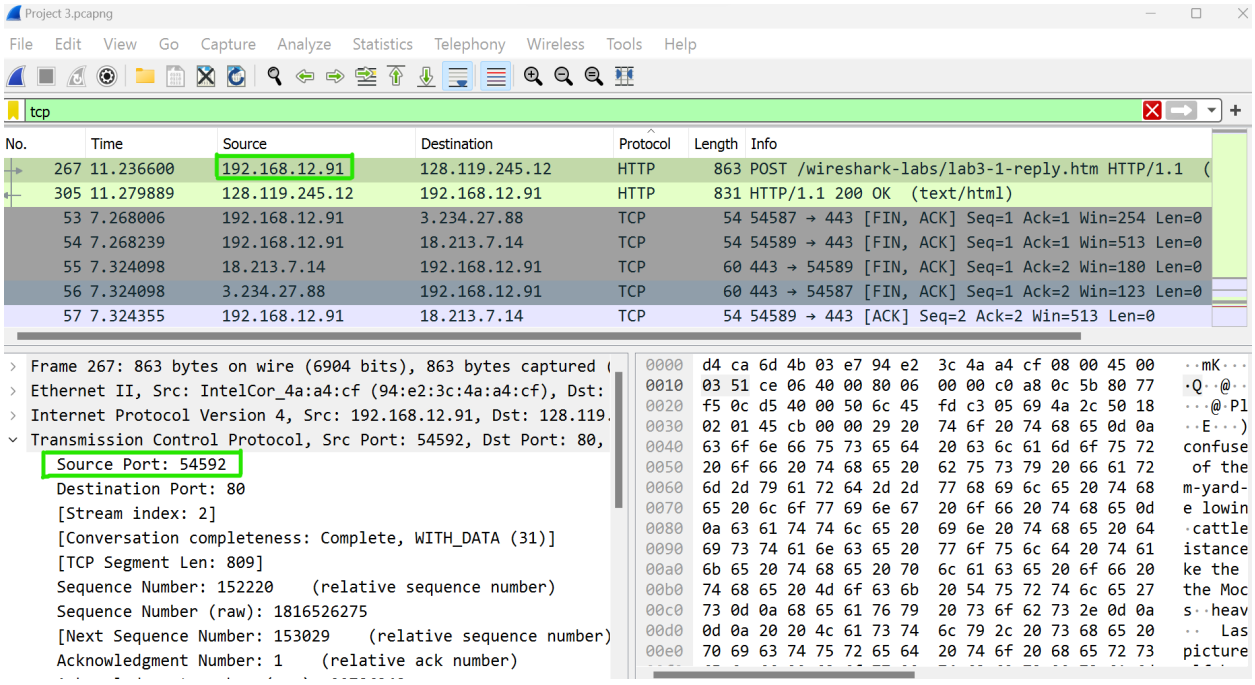
TCP Port number: 54592

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?**



The IP address of gaia.cs.umass.edu is 128.119.245.12 and the port number of sending and receiving TCP segments for this connection is 80.

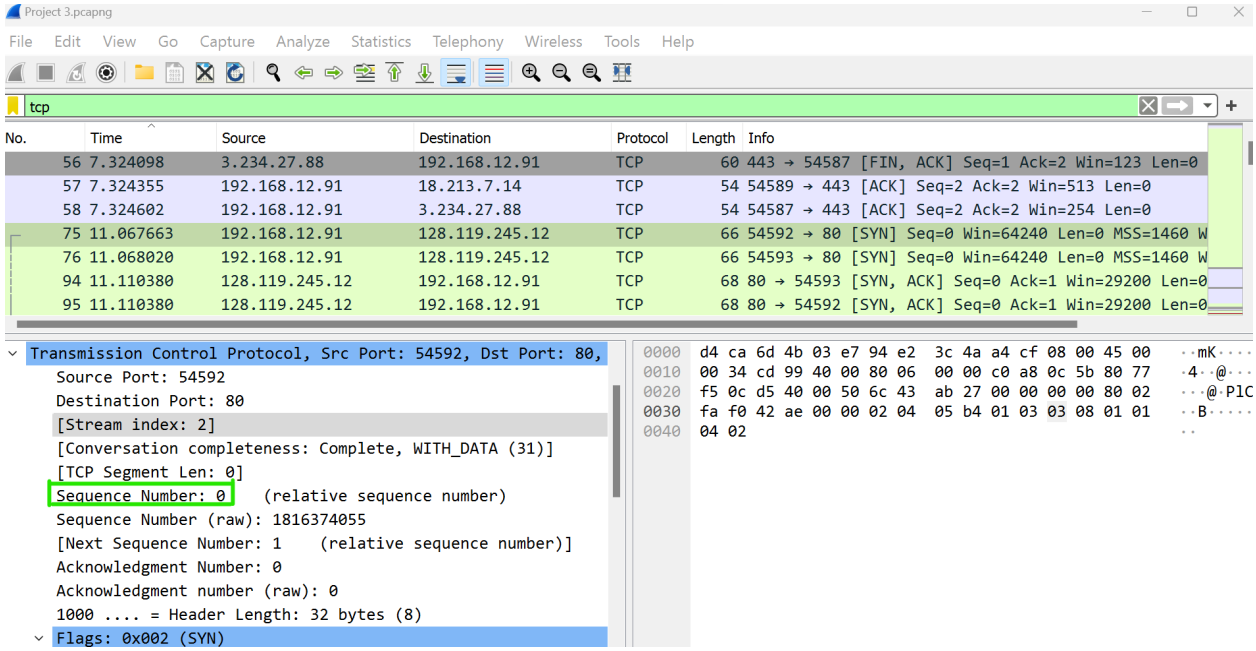
3. **What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?**



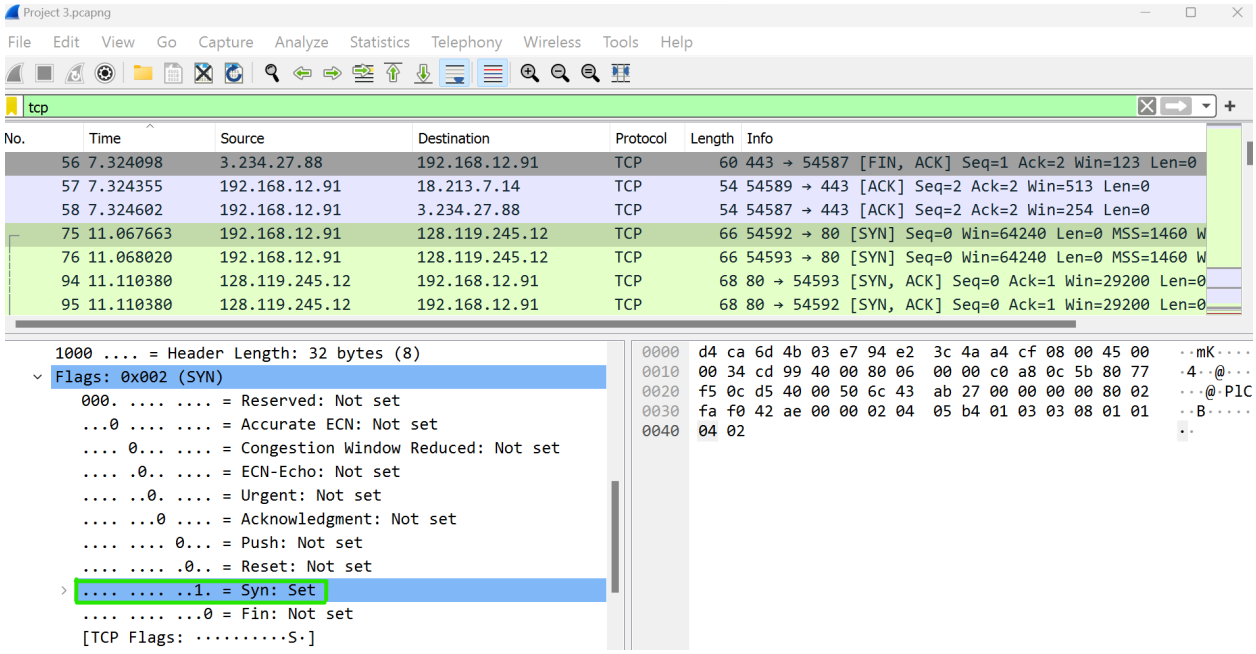
IP address: 192.168.12.91

TCP Port number: 54592

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?**

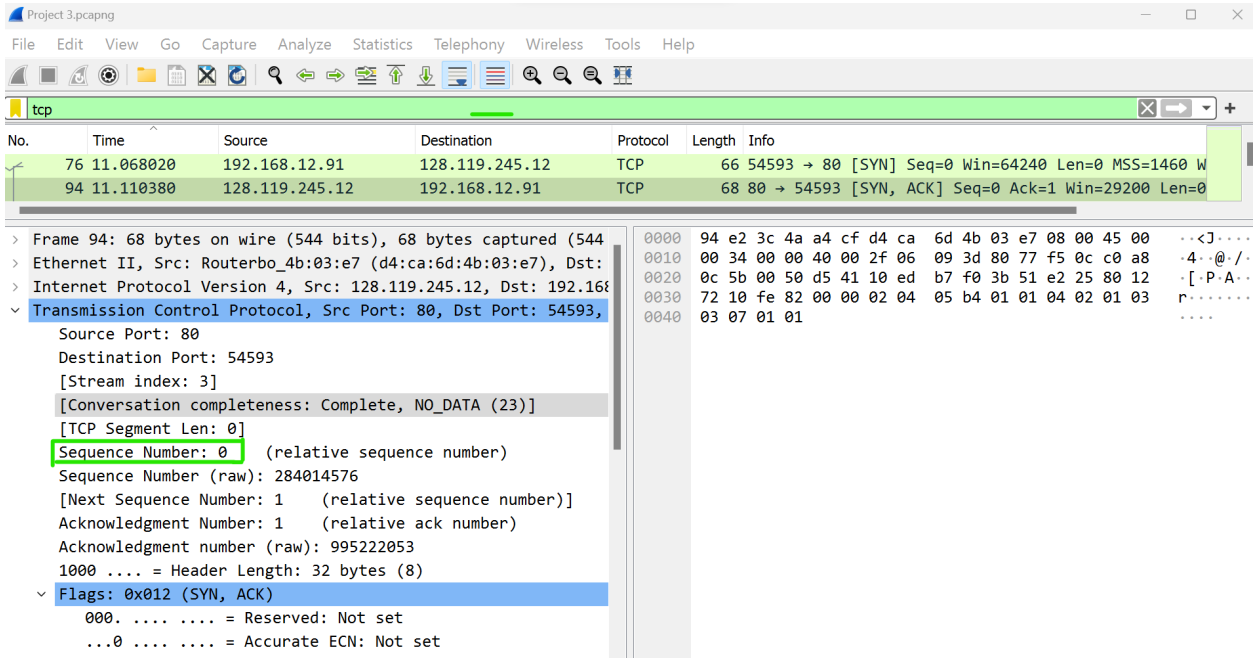


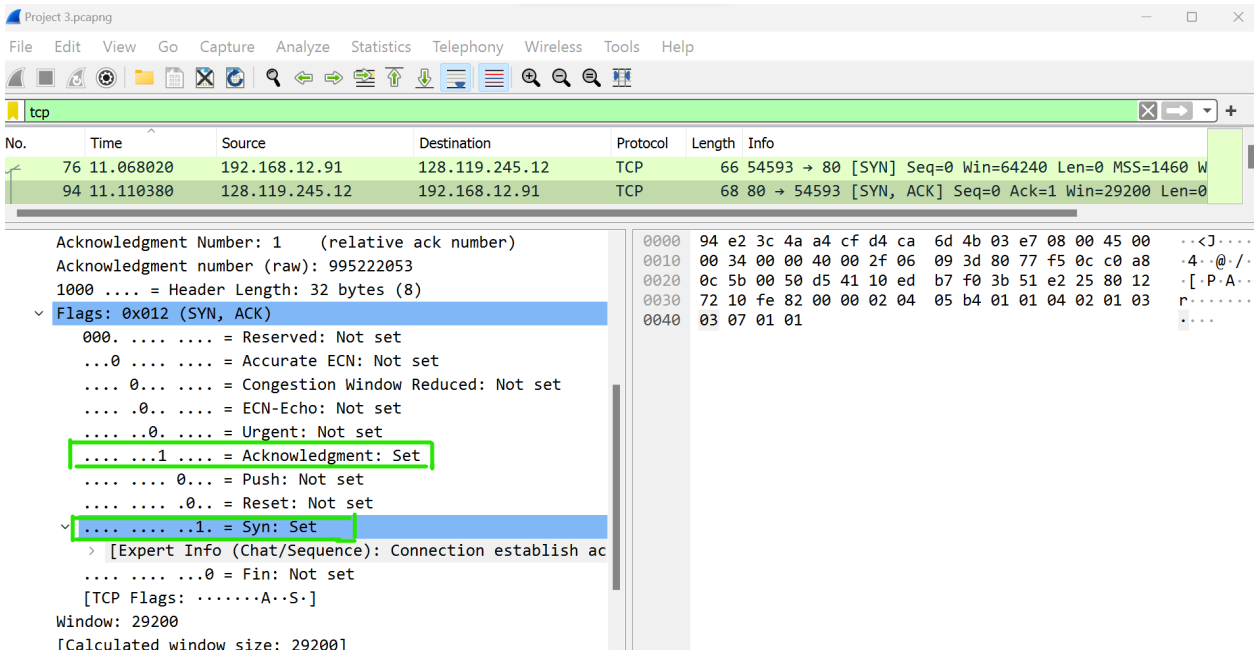
The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and gaia.cs.umass.edu.



The Syn flag is set to 1 which indicates that this segment is a SYN segment.

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?**



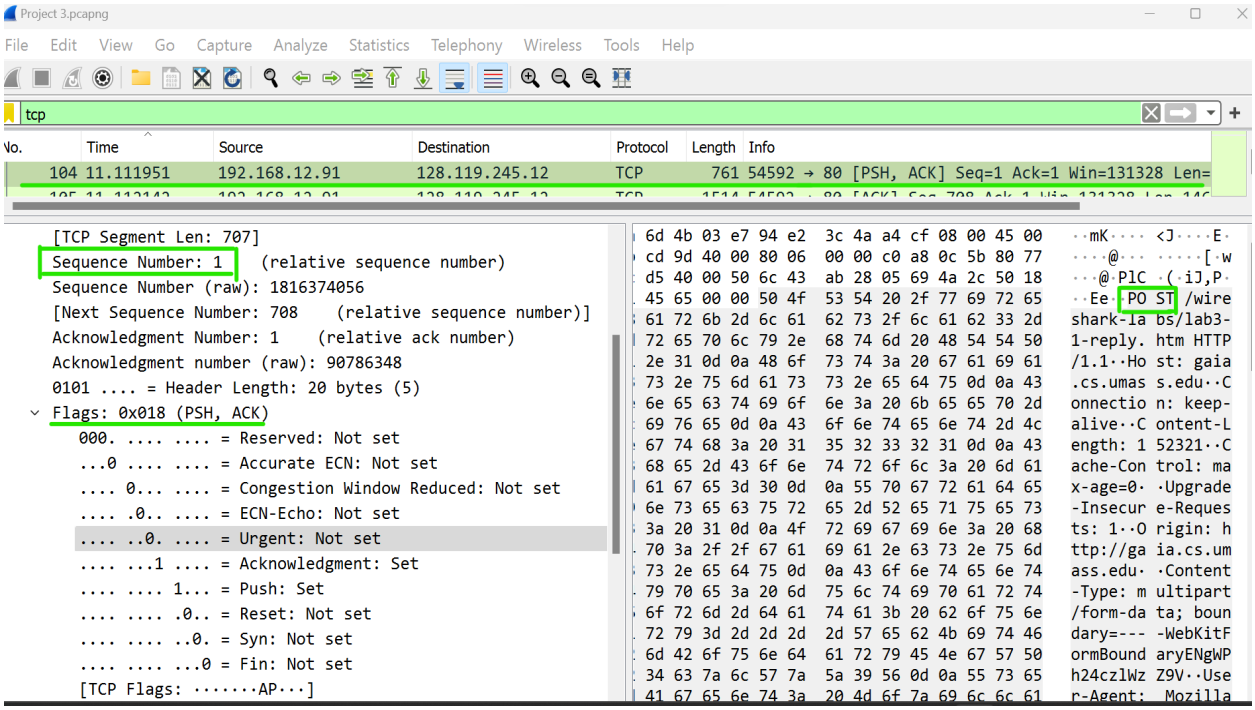


The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

The value of the acknowledgement field in the SYNACK segment is 1. The value of the Acknowledgement field in the SYNACK segment is determined by the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segments from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the Acknowledgement field in the SYNACK segment is 1.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

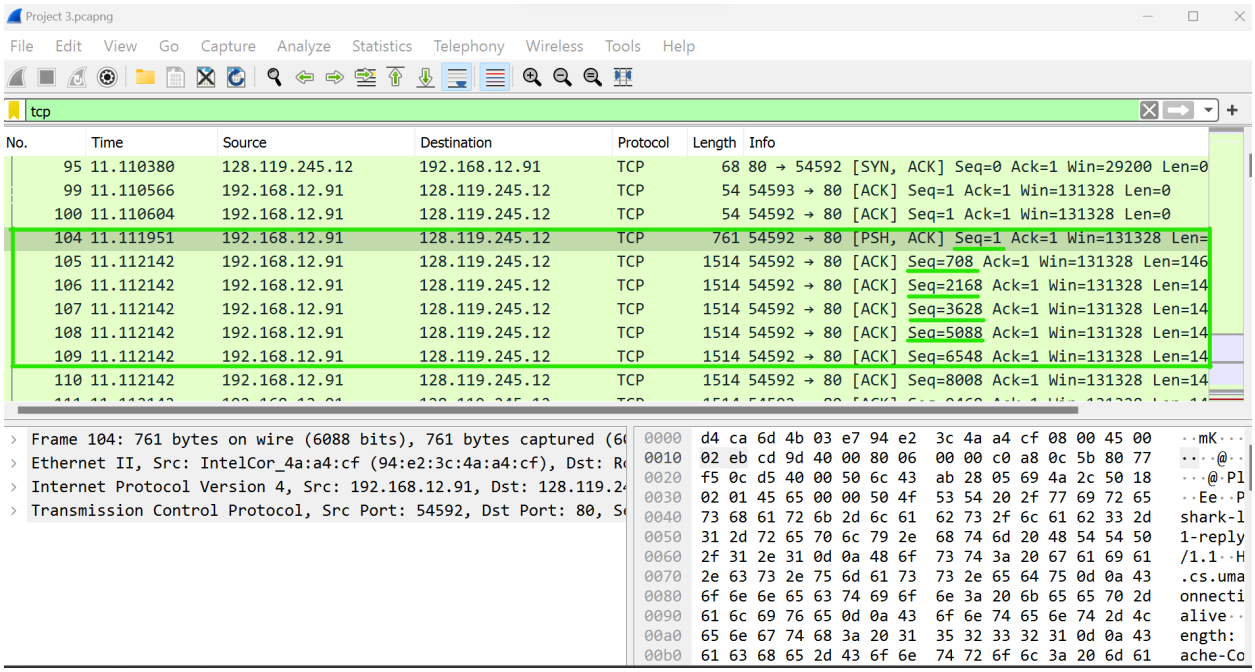
6. **What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.**



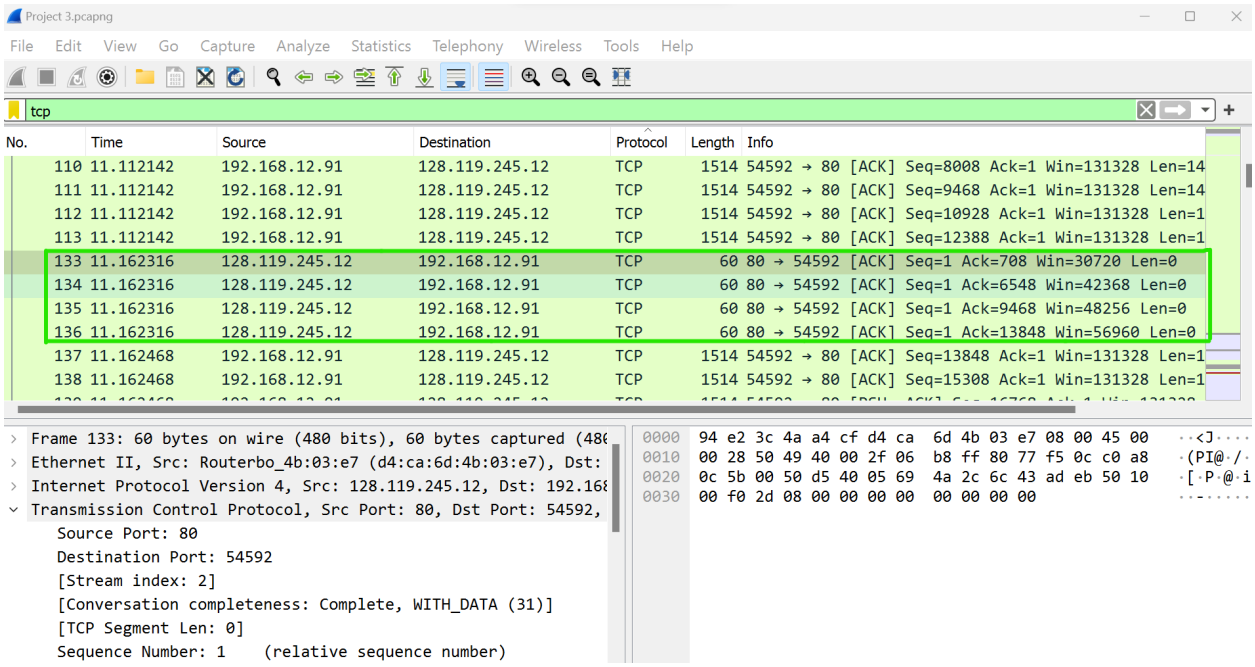
The segment No.104 contains the HTTP POST command, the sequence number of this segment is 1.

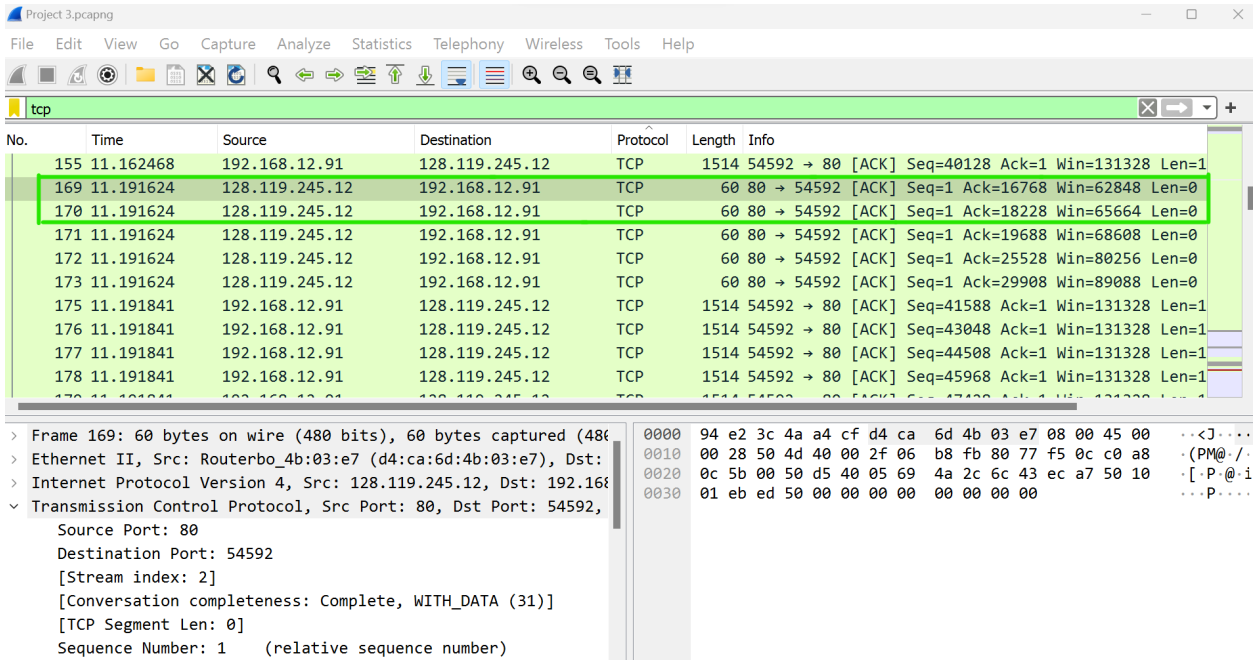
7. **Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?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

First six segments:



ACK of first six segments:





The first six segments are no. 104, 105, 106, 107, 108 and 109. The ACK of the first six segments are no. 133, 134, 135, 136, 169 and 170.

Segment 1 sequence number is 1

Segment 2 sequence number is 708

Segment 3 sequence number is 2168

Segment 4 sequence number is 3628

Segment 5 sequence number is 5088

Segment 6 sequence number is 6548

	Sent Time	**ACK Received Time**	**RTT**
Segment 1	11.111951	11.162316	0.050365
Segment 2	11.112142	11.162316	0.050174
Segment 3	11.112142	11.162316	0.050174
Segment 4	11.112142	11.162316	0.050174

Segment 5	11.112142	11.191624	0.079482
Segment 6	11.112142	11.191624	0.079482

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:

EstimatedRTT = RTT for Segment 1 = 0.050365s

EstimatedRTT after the receipt of the ACK of segment 2:

EstimatedRTT = 0.875 * 0.050365 + 0.125 * 0.050174= 0.050341125s

EstimatedRTT after the receipt of the ACK of segment 3:

EstimatedRTT = 0.875 * 0.050341125 + 0.125 * 0.050174= 0.05032023437s

EstimatedRTT after the receipt of the ACK of segment 4:

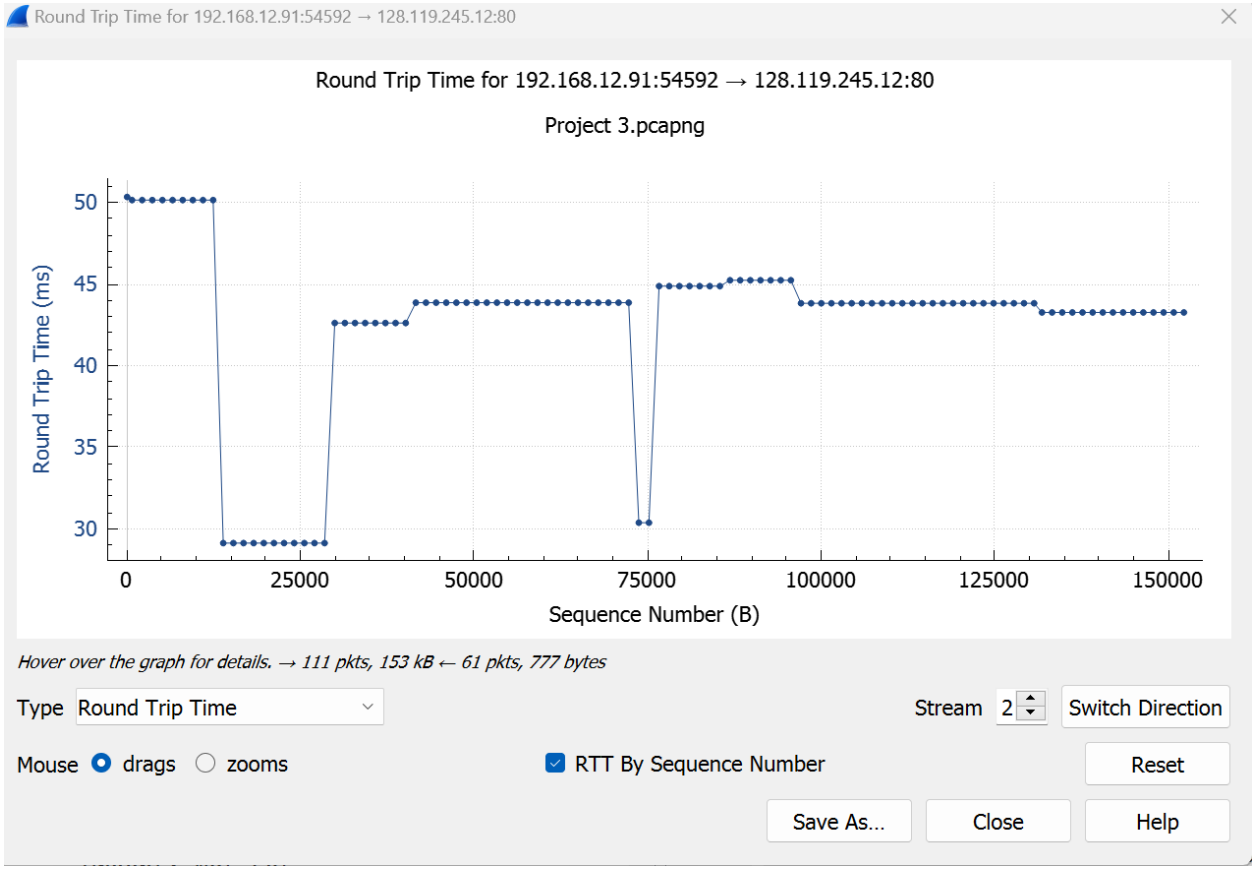
EstimatedRTT = 0.875 * 0.05032023437 + 0.125 * 0.050174= 0.05030195507s

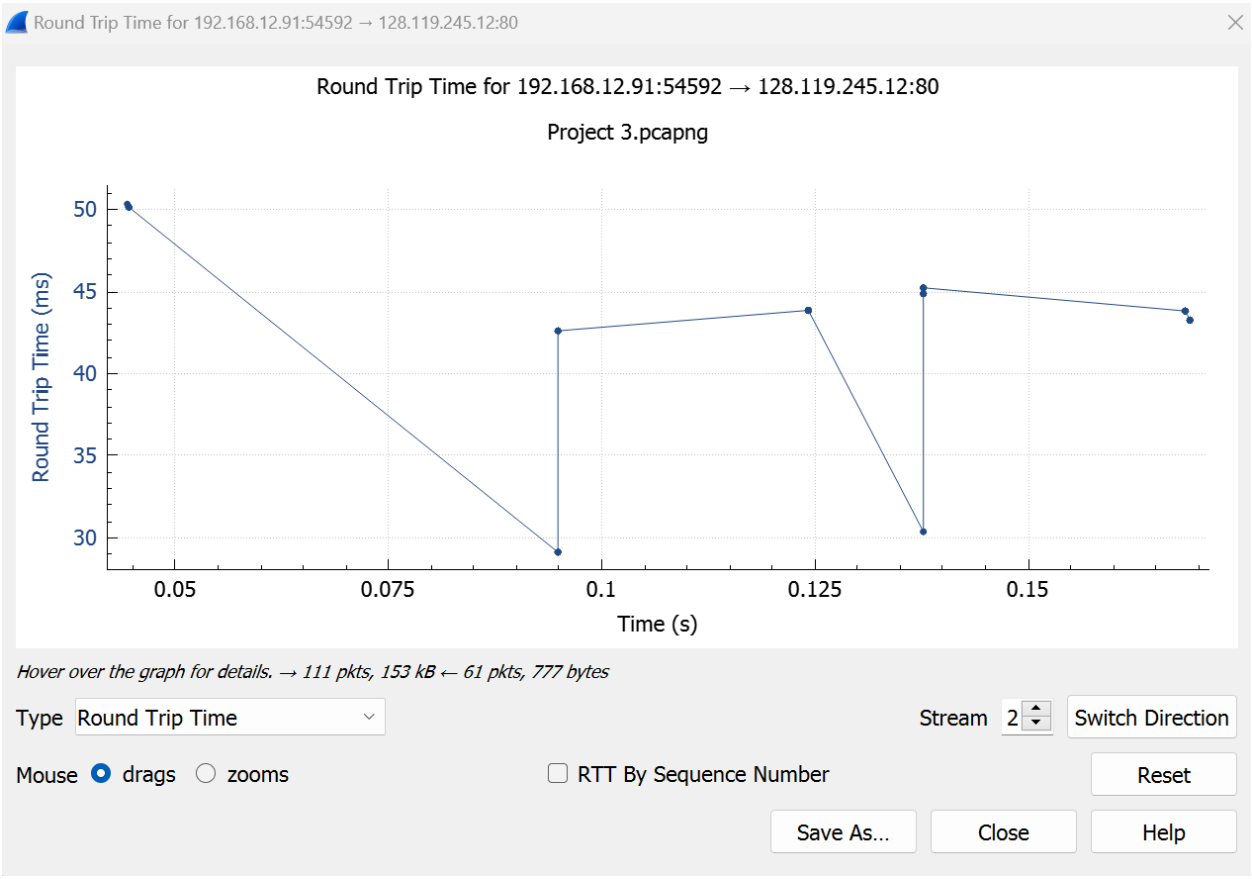
EstimatedRTT after the receipt of the ACK of segment 5:

EstimatedRTT = 0.875 * 0.05030195507 + 0.125 * 0.079482= 0.05394946068s

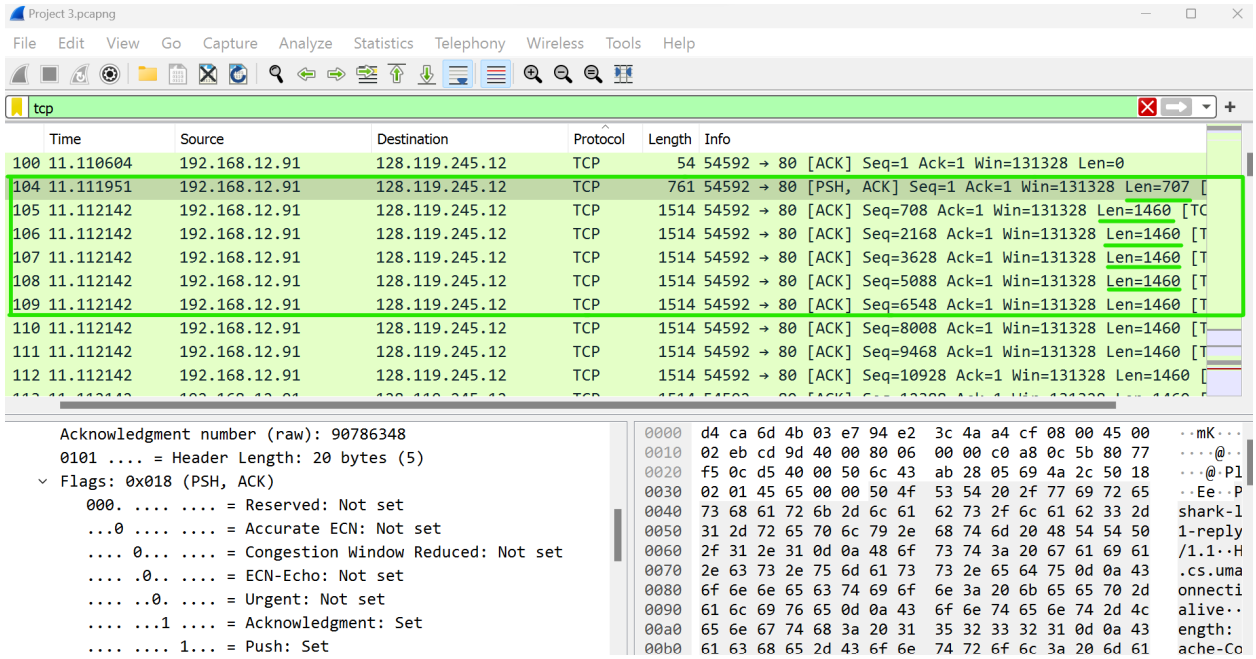
EstimatedRTT after the receipt of the ACK of segment 6:

EstimatedRTT = 0.875 *0.05394946068 + 0.125 * 0.079482= 0.05714102809s


Round Trip Time for 192.168.12.91:54592 → 128.119.245.12:80
Round Trip Time for 192.168.12.91:54592 → 128.119.245.12:80
Project 3.pcapng
Round Trip Time (ms)
50
45
40
35
30
0
25000
50000
75000
100000
125000
150000
Sequence Number (B)
Hover over the graph for details. → 111 pkts, 153 kB ← 61 pkts, 777 bytes
Type
Round Trip Time
Stream
2
Switch Direction
Mouse
drags
zooms
RTT By Sequence Number
Reset
Save As...
Close
Help

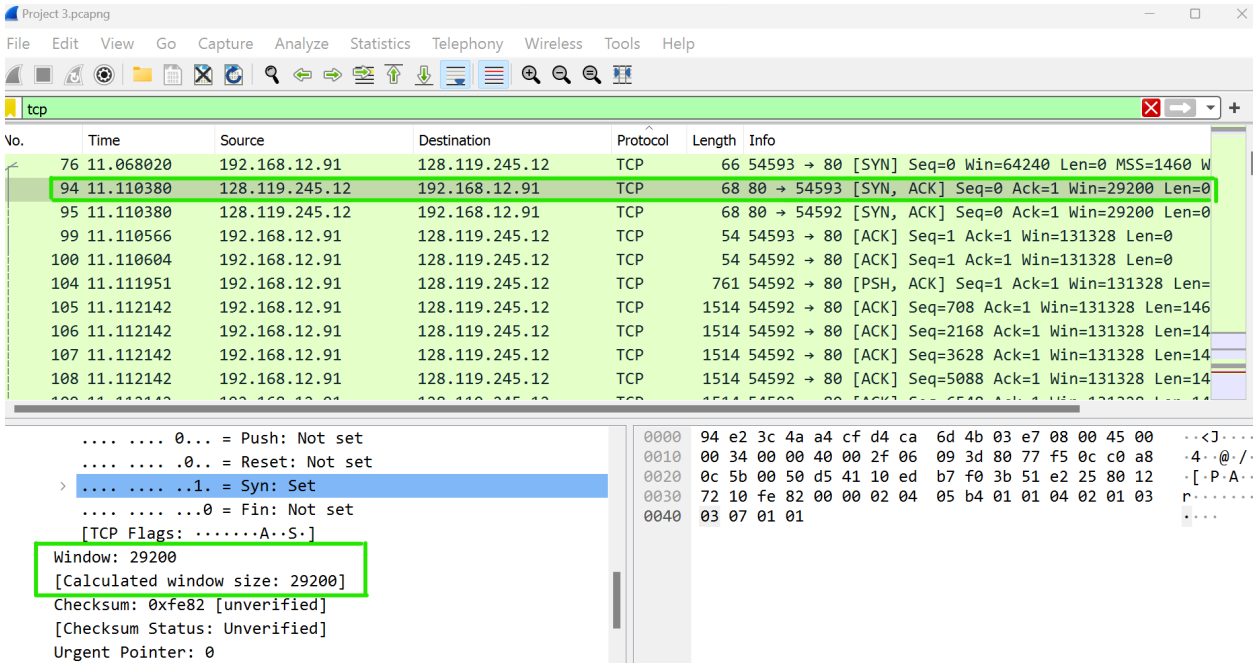


8. What is the length of each of the first six TCP segments?



The length of the first TCP segment is 707 bytes, the length of the second TCP segment is 1460 bytes, the length of the third TCP segment is 1460 bytes, the length of the fourth TCP segment is 1460 bytes, the length of the fifth TCP segment is 1460 bytes and the length of the sixth TCP segment is 1460 bytes.

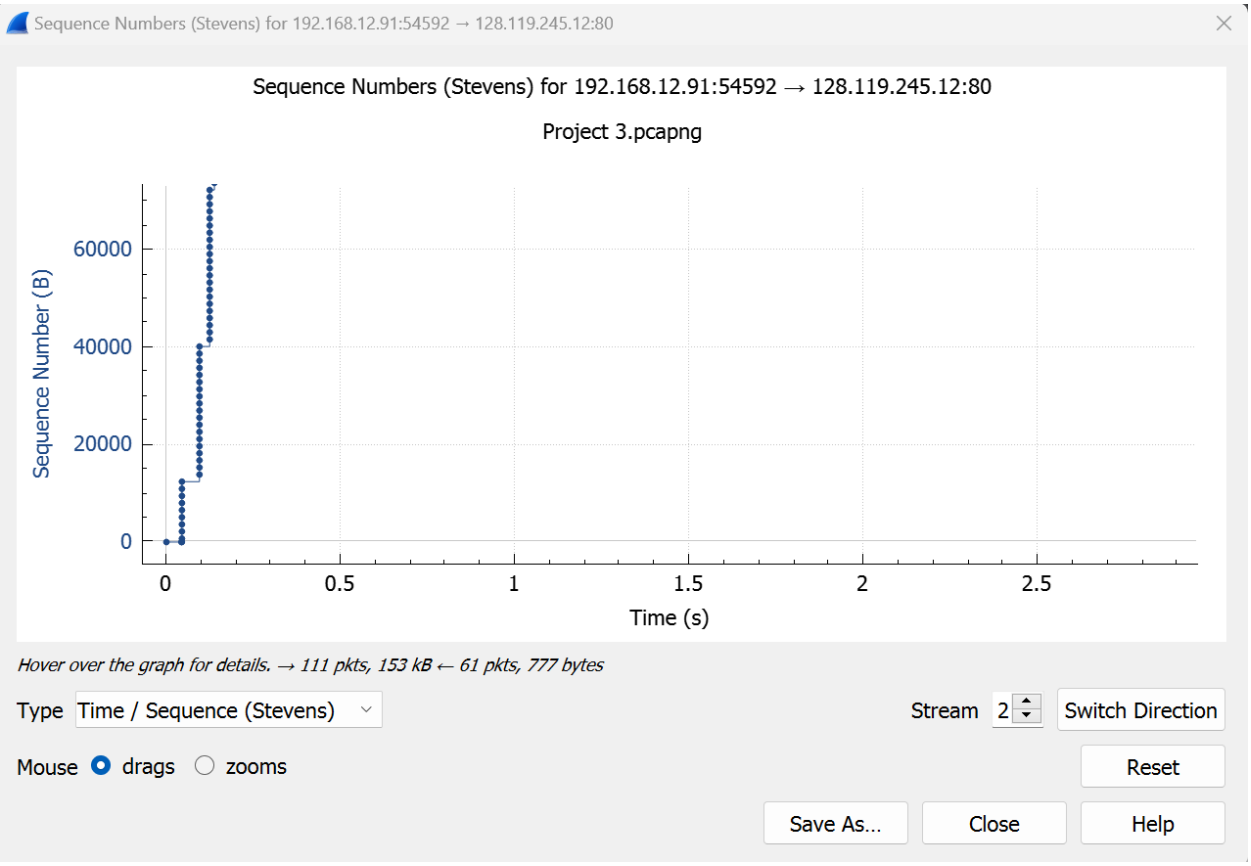
9. **What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?**



The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 29200 bytes. The sender is never throttled due to lacking of receiver buffer space.

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 since in the time sequence graph (stevens), all sequence numbers are monotonically increasing.



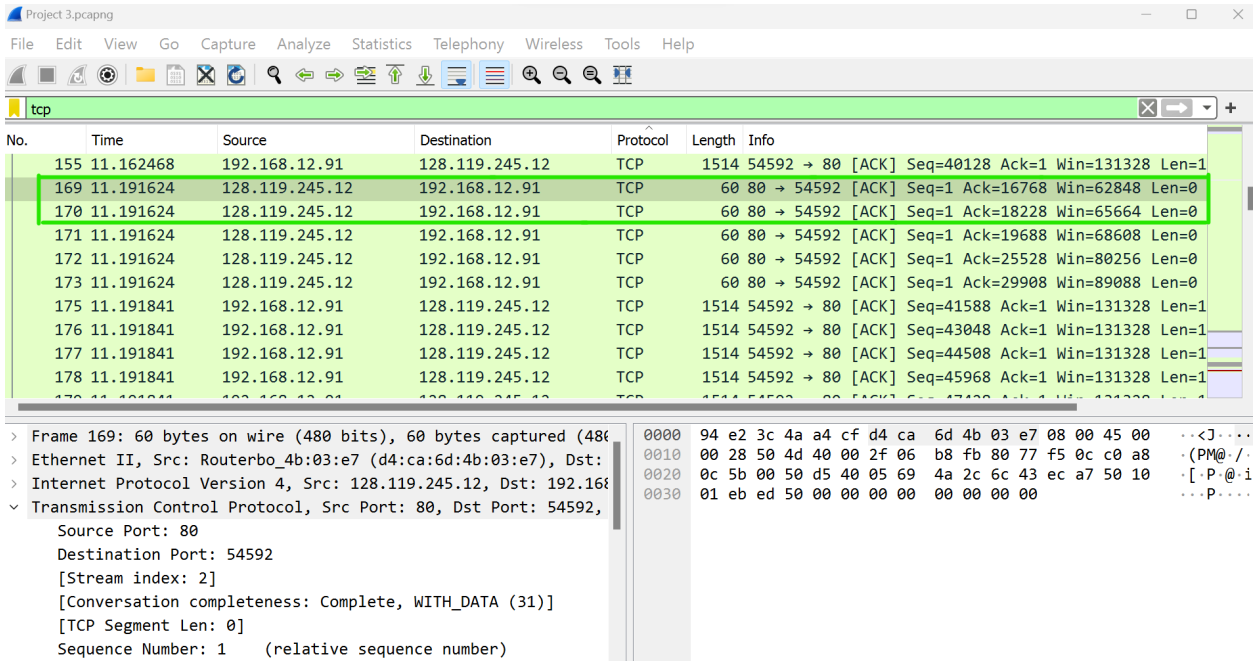
11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment?

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs.

	Acknowledged sequence number	**Acknowledged data**
ACK 1	708	708
ACK 2	6548	5840
ACK 3	9468	2920
ACK 4	13848	4380
ACK 5	16768	2920
ACK 6	18228	1460

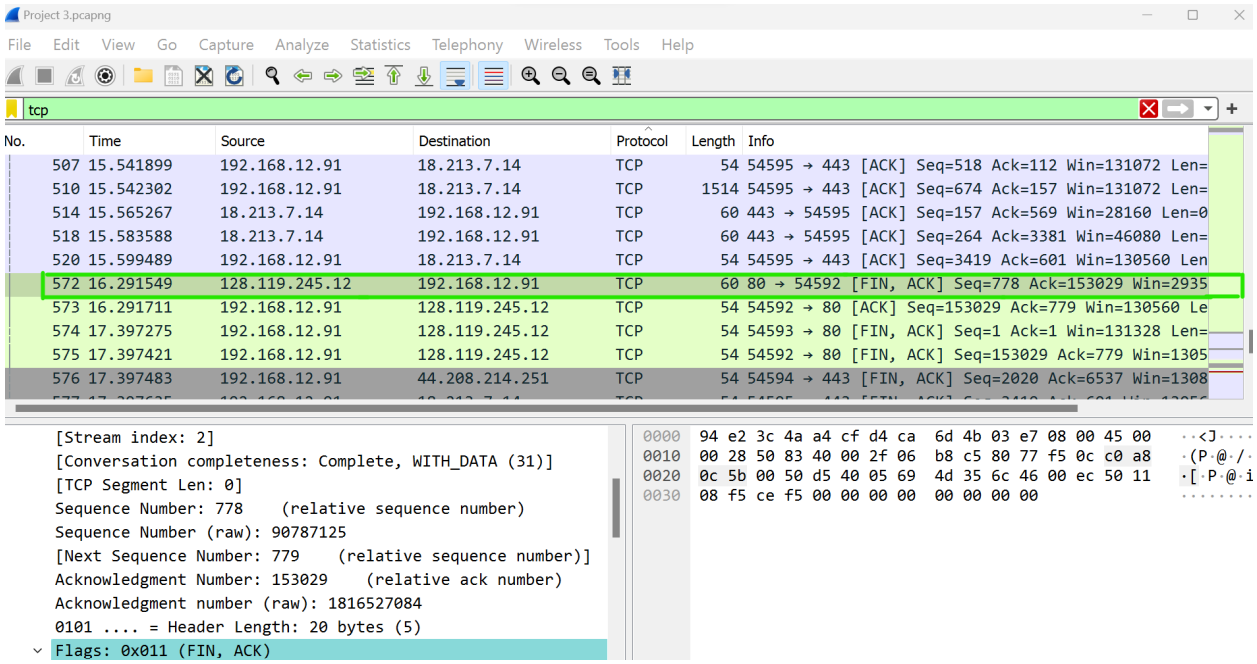
ACK 7	19688	1460

The receiver is ACKing every other segment. For example, segment No. 169 in the screenshot below.



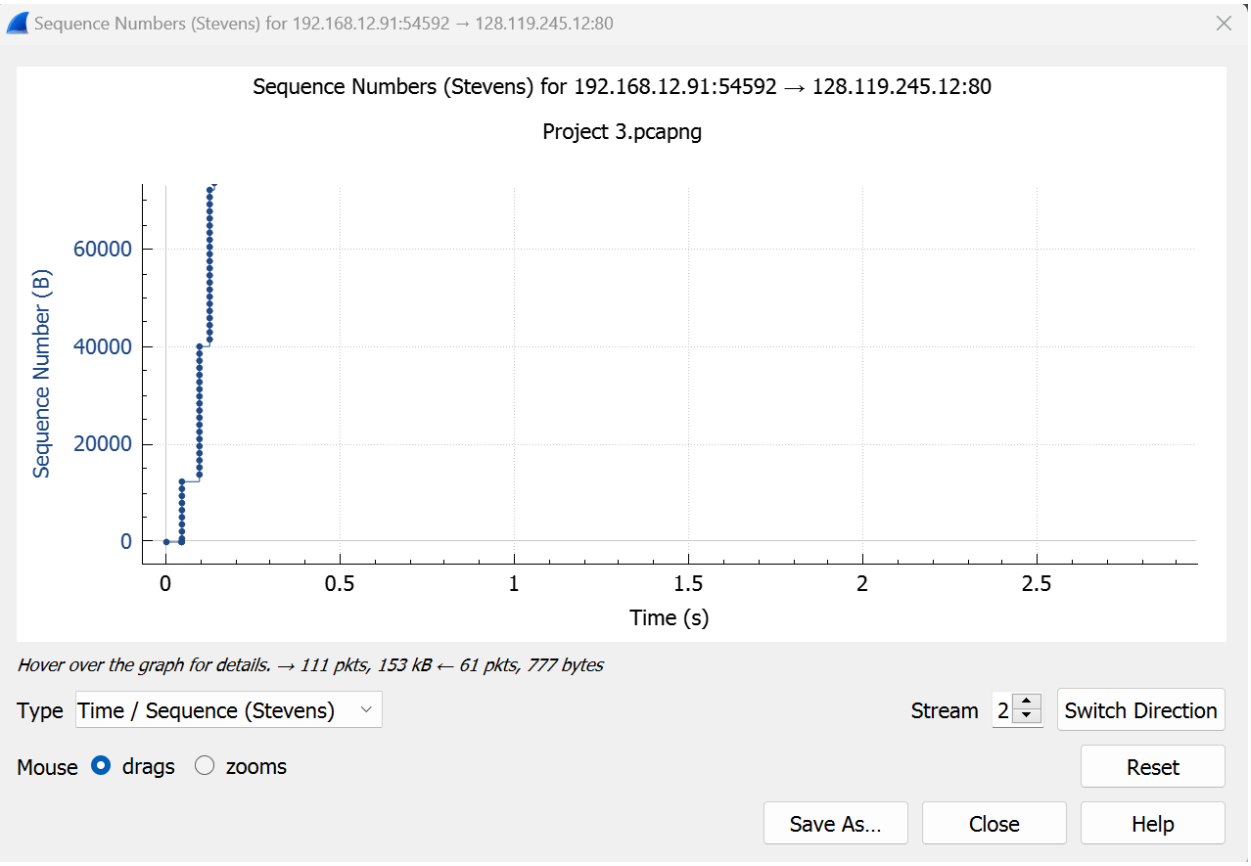
12. What is the throughput (bytes transferred per unit time) for the TCP connection?

Explain how you calculated this value.



The [FIN, ACK] packet no.572 shows an acknowledgement number of 153029, which means 153029 bytes were acknowledged. The time on this message is 16.291549. So an approximate average throughput can be calculated as 153029 bytes/16.291549 seconds = 9393.15224108 bytes/seconds for this connection.

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 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 that we've studied in the text.**



The slow start of the TCP seems to begin at about 0.01 seconds and then ends at about 0.2 seconds. Congestion avoidance takes over at about 0.3 seconds because it cuts down the amount being sent.

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

When we have a lot of traffic on the network TCP sender uses AIMD algorithm for the reduction of window size.