Name	Rohit Ashiwal
Enr. No.	17114064
Dept	CSE
Batch	CS 2
Class	B. Tech. 3rd yr

Lab Assignment 4

This assignment aims to make us familiar with the hardware and software aspects of computer networking and extracting information related to computer networking using TCL programs.

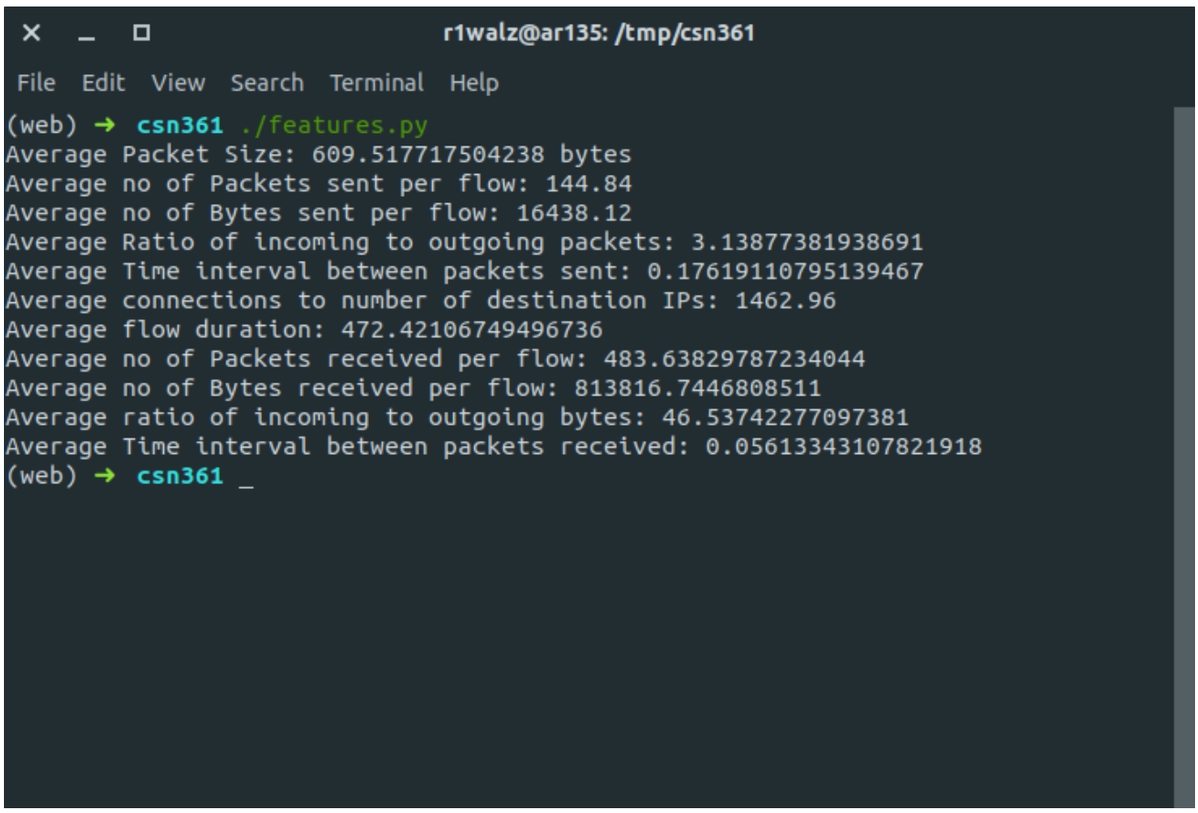
Problem Statement 1

Q: *Install Wireshark and explore its uses to capture network traffic. You have to capture normal internet traffic for 20-30 minutes from your system using Wireshark. You need to copy this data is CSV / TXT file.*

> **The CSV file is added in the folder.**

Problem Statement 2

Q: *Take the CSV / TXT, which is generated in Problem Statement 1 as an input. Write a code (in any programming language of your choice) to extract the following 11 features given below in the table:*

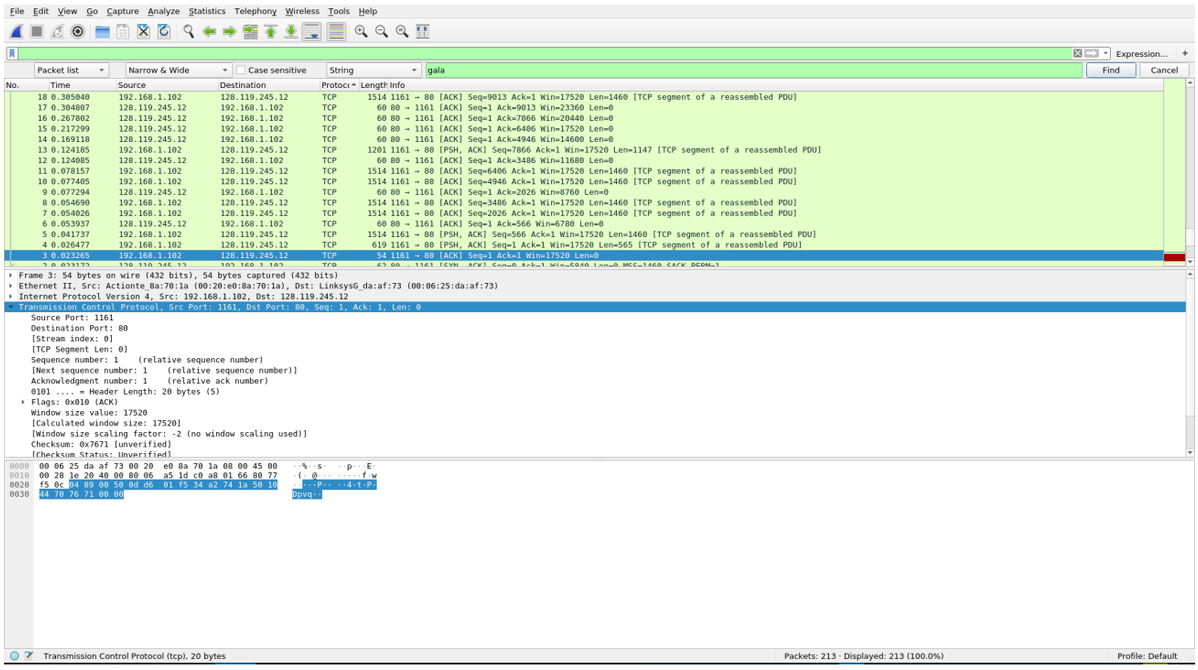


> **Python code is submitted in the folder.**

Problem Statement 3

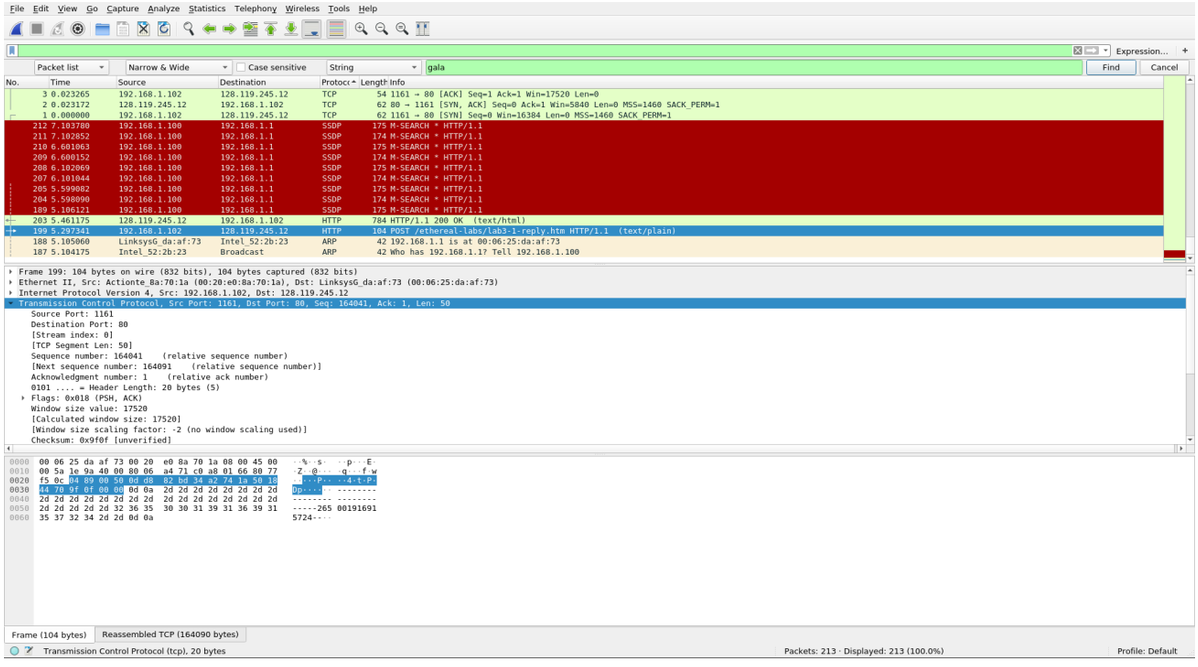
Q: *In this problem, the behavior of TCP protocol will be studied using Wireshark. For this assignment download the Wireshark captured trace file named as* ***tcpethe-trace*** *from Piazza, which is a packet trace of TCP tranfer of a file from a client machine. Open* ***tcpethe-trace*** *file in Wireshark and answer the following question:*

a. *What is the IP address and TCP port number used by the client computer (source) that is transferring the file to server (ser1)?*



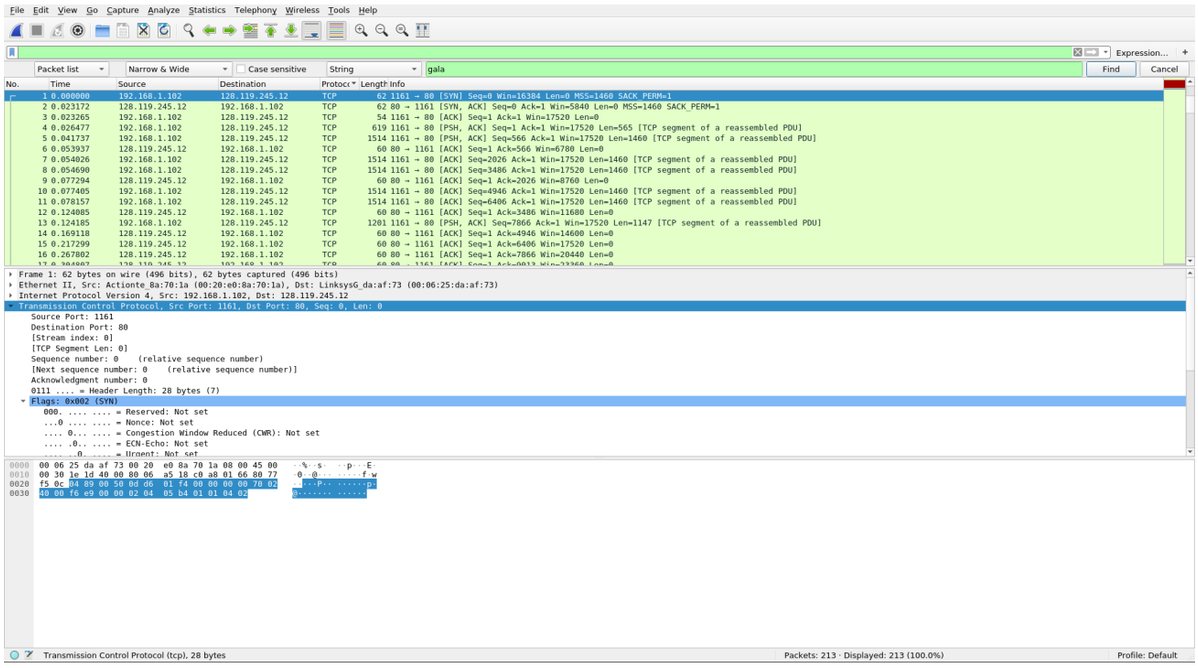
According to above figure, the client computer's (source) IP address is **192.168.1.102** and the TCP port number is **1161**.

b. *What is the IP address of server (ser1)? On what port number it is sending and receiving the TCP segments for this connection?*



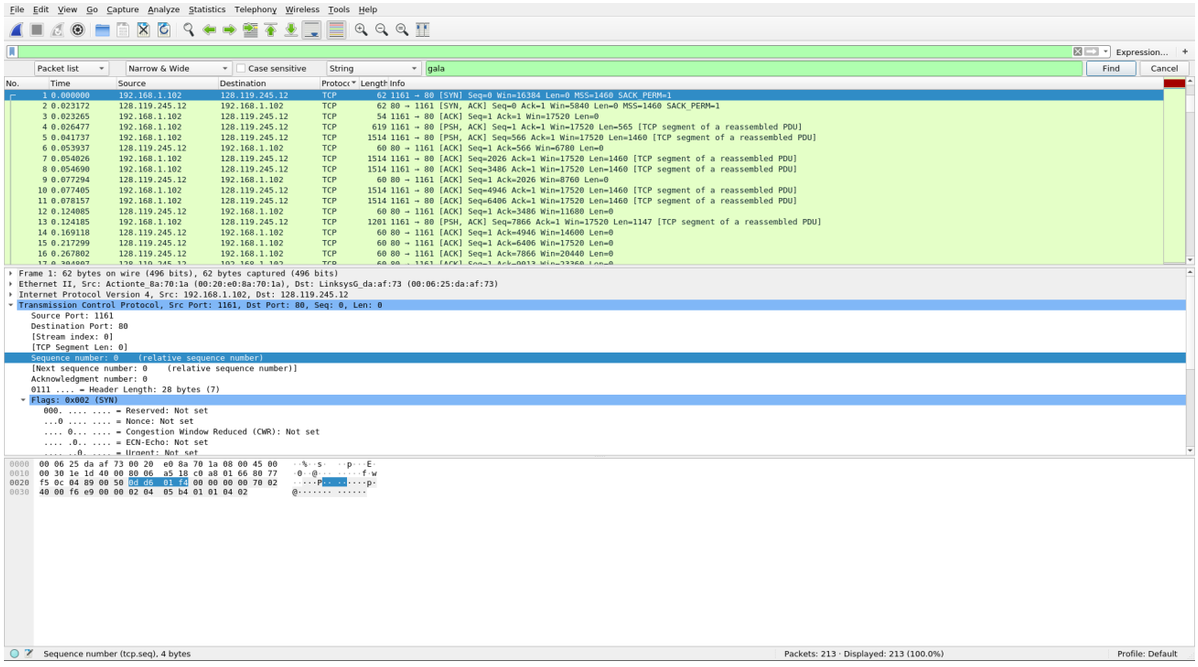
According to above figure, the IP address of ser1 is **128.119.245.12** and the TCP port number is *80*.

c. *What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ser1? What is it in the segment that identifies the segment as a SYN segment?*



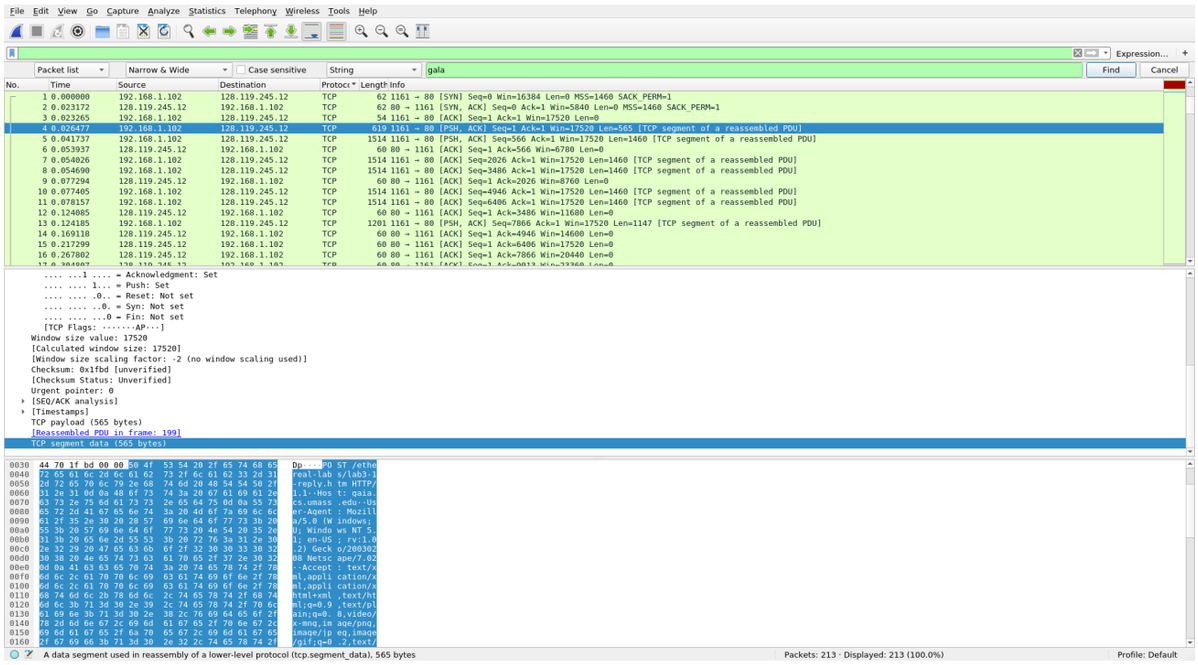
The sequence number of the SYN segment is **0** since it is used to imitate the TCP connection between the client computer and ser1. According to the above figure, in the Flags section, the SYN flag is set to **1** which indicates that this segment is a SYN segment.

d. *What is the sequence number the SYNACK segment sent by ser1 to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?*



According to the above figure, the sequence number of the SYNACK segment sent by ser1 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 ser1. The server adds 1 to the initial sequence number of SYN segment from the computer. For this case, the initial computer sequence number of 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 ACK flag in the segment are set to **1**.

e. *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.*



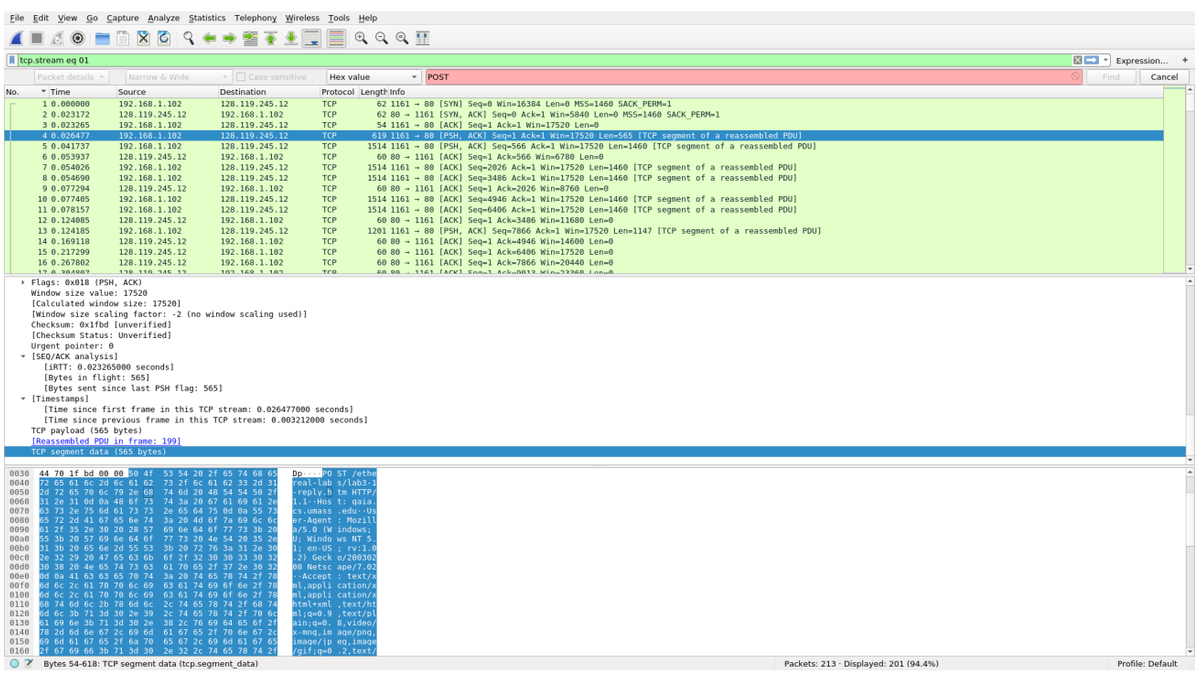
According to the above figure, the segment number **4** contains the HTTP POST command, the sequence number of this segment is **1**.

f. *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 Round Trip Time (RTT) value for each of the six segments? What is the Estimated RTT value after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the following Estimated RTT equation for all subsequent segments.*

> **Estimated RTT = (1 – α) * Estimated RTT + α * SampleRTT**

where, the new value of Estimated RTT is a weighted combination of the previous value of Estimated RTT and the new value for SampleRTT. The recommended value of α = 0.125.

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 ser1 server. Then select: Statistics→TCP Stream Graph→Round Trip Time Graph.*



The HTTP POST segment is considered as the first segment. Segments 1 – 6 are No. 4, 5, 7, 8, 10, and 11 in this trace respectively. The ACKs of segments 1 – 6 are No. 6, 9, 12, 14, 15, and 16 in this trace.

Segment 1 sequence number: 1
Segment 2 sequence number: 566
Segment 3 sequence number: 2026
Segment 4 sequence number: 3486
Segment 5 sequence number: 4946
Segment 6 sequence number: 6406

	Sent time	ACK received time	RTT (seconds)
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.11443
Segment 5	0.077405	0.217299	0.13989
Segment 6	0.078157	0.267802	0.18964

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:
EstimatedRTT = RTT for Segment 1 = 0.02746 second

EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285

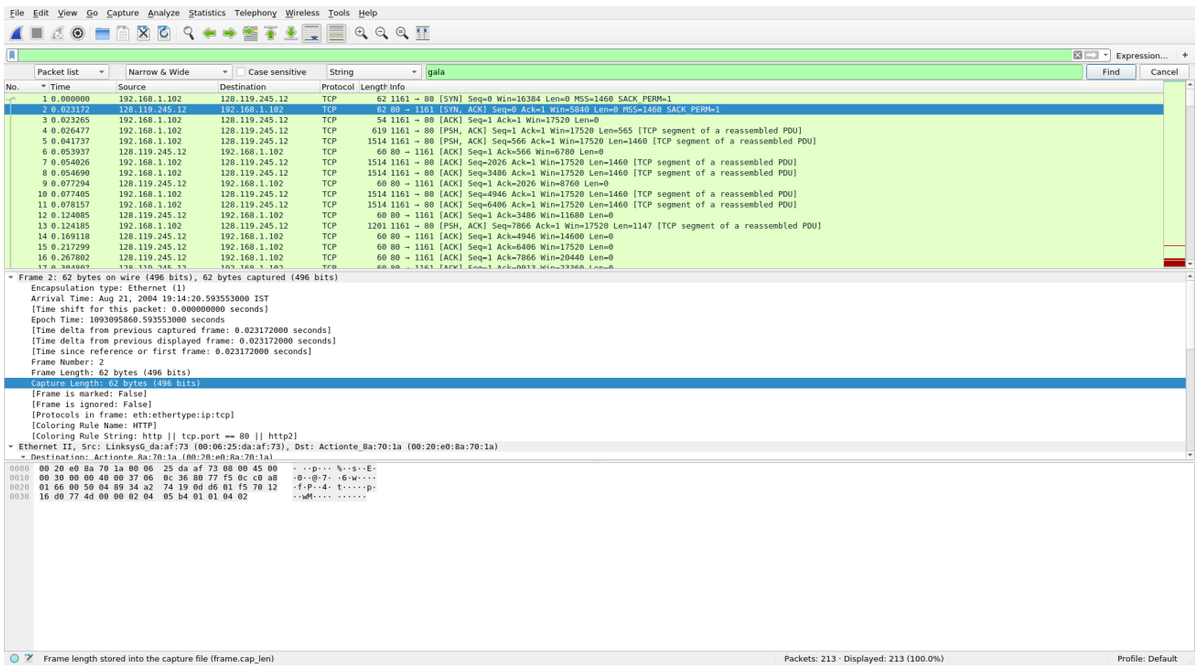
EstimatedRTT after the receipt of the ACK of segment 3:
EstimatedRTT = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337

EstimatedRTT after the receipt of the ACK of segment 4:
EstimatedRTT = 0.875 * 0.0337+ 0.125 * 0.11443 = 0.0438

EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT = 0.875 * 0.0438 + 0.125 * 0.13989 = 0.0558

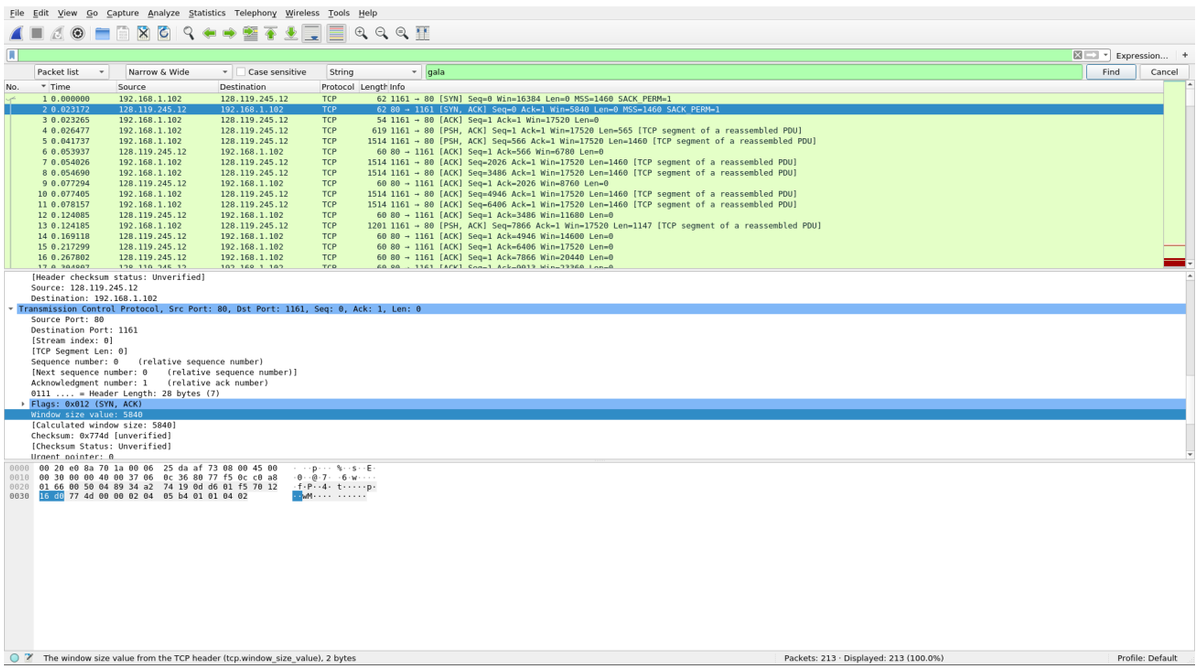
EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 second

g. *What is the length of each of the first six TCP segment?*



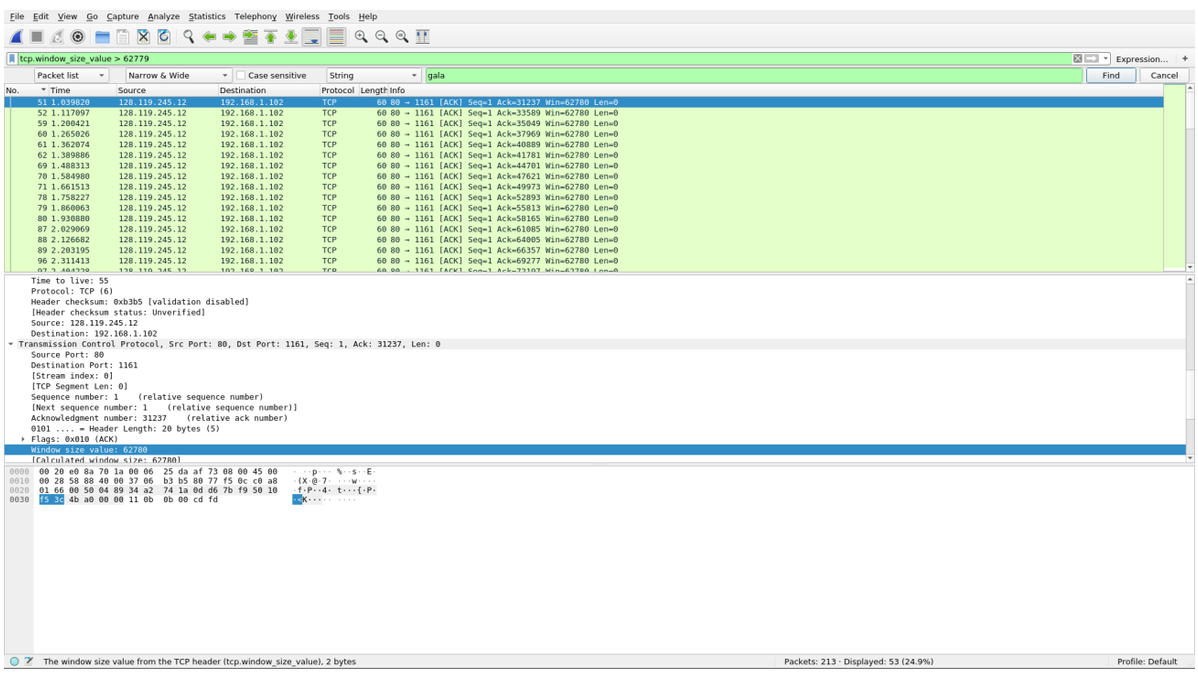
Packet Number	Length
1	62 bytes
2	62 bytes
3	54 bytes
4	619 bytes
5	1514 bytes
6	60 bytes

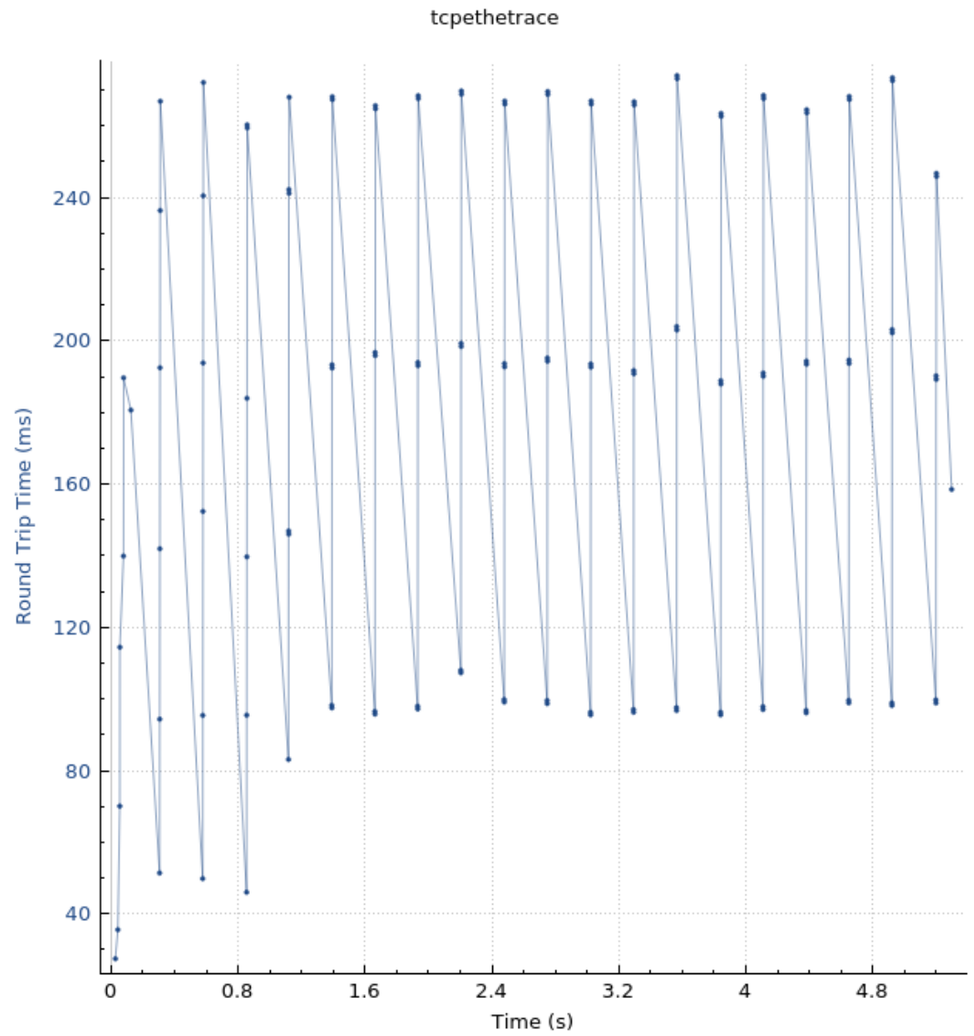
h. *What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?*



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 **5840** bytes (shown in above figure). This reviver window grows until it reaches the maximum receiver buffer size of **62780** bytes. According to the trace, the sender is never throttled due to lacking of receiver buffer space.

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





The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for number 4 segment) and the acknowledged sequence number of the last ACK (**164091** bytes for number **202** segment). Therefore, the total data are 164091 - 1 = **164090** bytes. The whole transmission time is the difference of the time instant of the first TCP segment (i.e., **0.026477** seconds for number 4 segment) and the time instant of the last ACK (i.e., **5.455830** seconds for number **202** segment). Therefore, the total transmission time is 5.455830 - 0.026477 = **5.4294** seconds. Hence, the throughput for the TCP connection is computed as 164090/5.4294 = **30.222 KByte/sec**.