Computer Network
Laboratory

Assignment 9

Name: Gagan Kumre
Enrollment Number: 17114028
Class: 3rd year, B.Tech CSE
Course: CSN-361

GitHub link - https://github.com/gagankumre/CSN361/tree/master/Assignment

Problems were given for this assignment. They are-

Problem Statement 1: 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 in CSV / TXT file.

Problem Statement 2: 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:

Problem Statement 3: 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 transfer of a file from a client system

to a remote server (named as ser1), obtained by running Wireshark on the 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)?

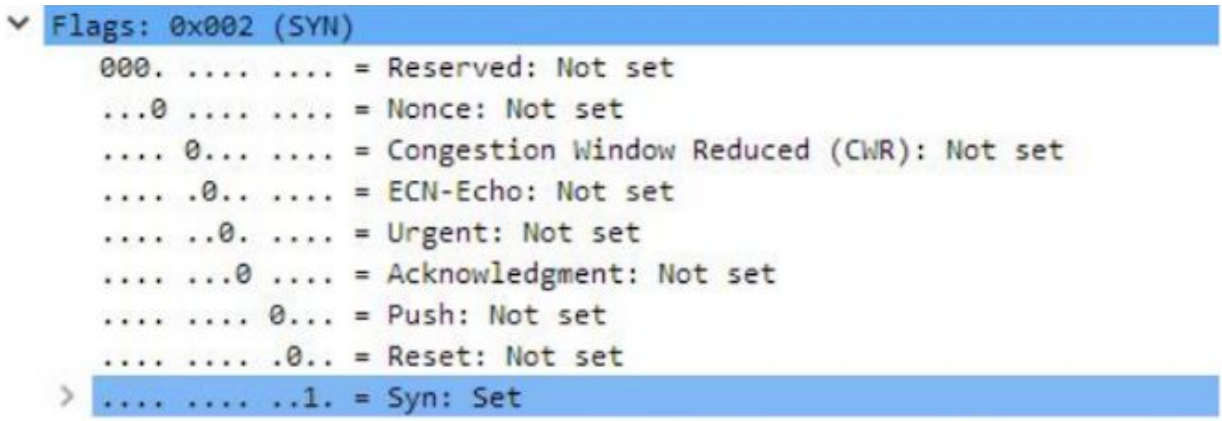
ANSWER = 192.168.1.102:1161

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

ANSWER = 128.119.245.12:80

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?

ANSWER = seq = 0, Flag being 0x002 signifies SYN segment bit is 1 and rest are 0. Refer below for screenshot.

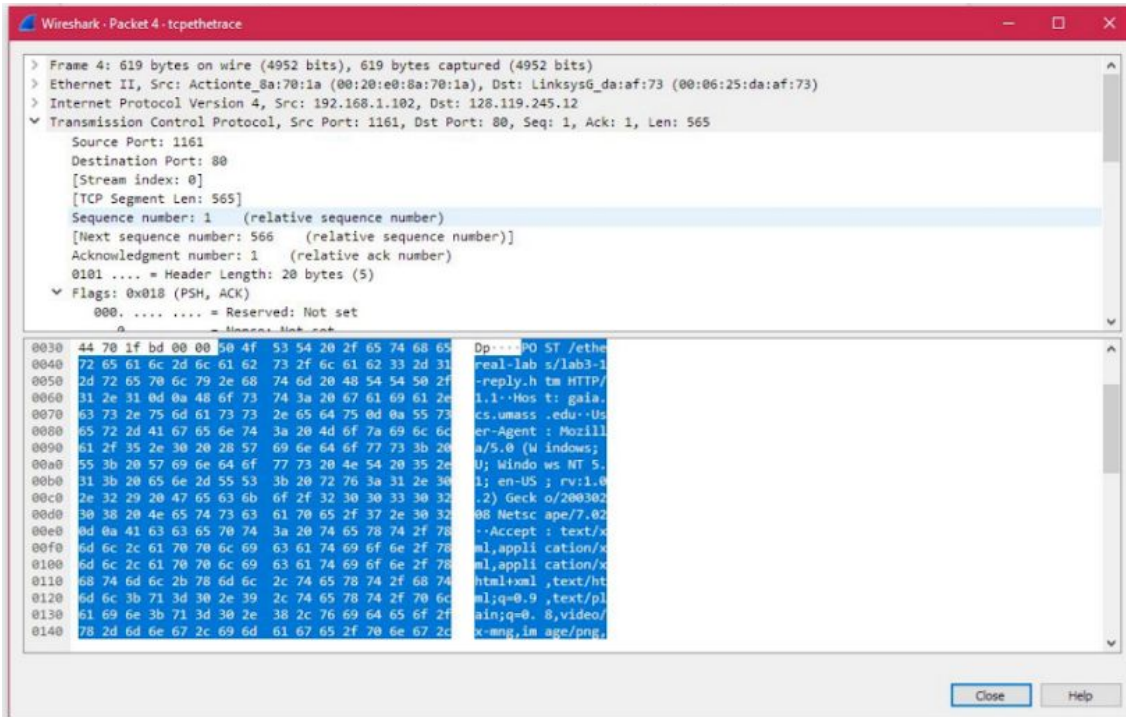


d. What is the sequence number of the SYNACK segment sent by ser1 to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

ANSWER: 0, Ack field is set to 1, ser1 determined that value by inverting the ack bit received in the SYN segment sent previously to initiate TCP communication, SYN and ACK segments are set to 1 and the rest are 0.

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.

ANSWER: seq = 164041



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.

ANSWER:

Seq numbers of first 6 segments in TCP connection = 1,566, 2026, 3486, 4946, 6406 Time of sending for each of the first 6 segments = 0.026477, 0.041737, 0.054026, 0.05469, 0.077405, 0.078157

Length of each segment is 1460 bytes

Times can be seen from the graph for sending and ACK received.

Est. RTT1 = 0.02746

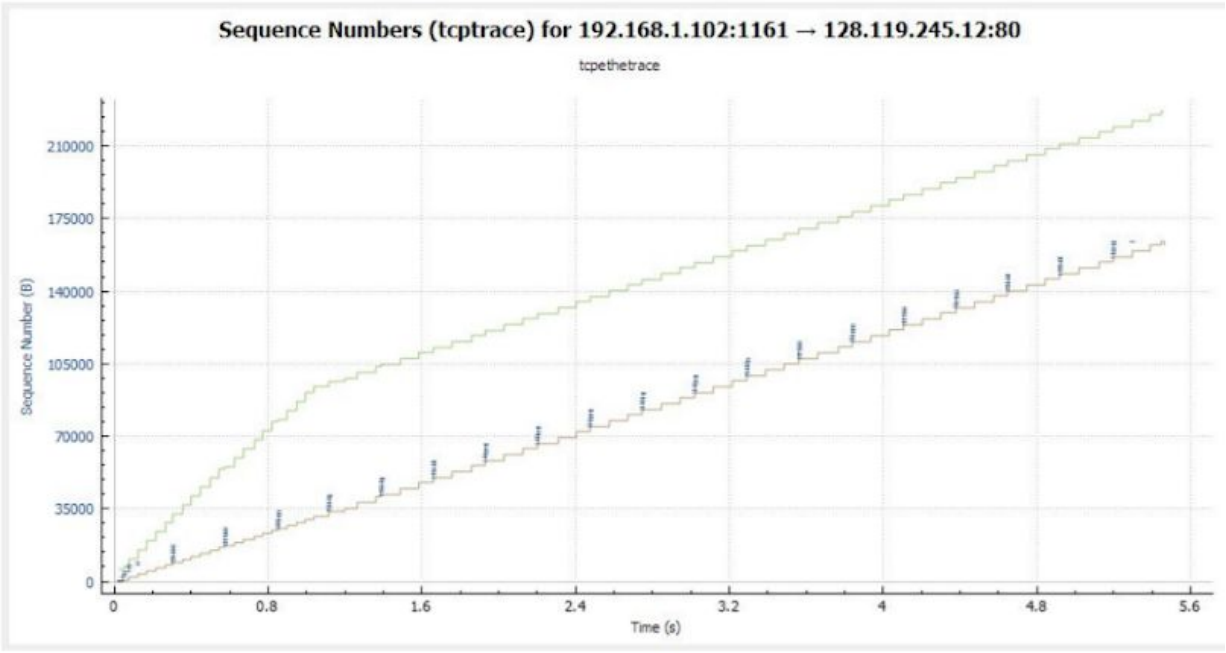
Est. RTT2 = 0.02746 * 0.75 + 0.25 * 0.035557 = 0.009621546415

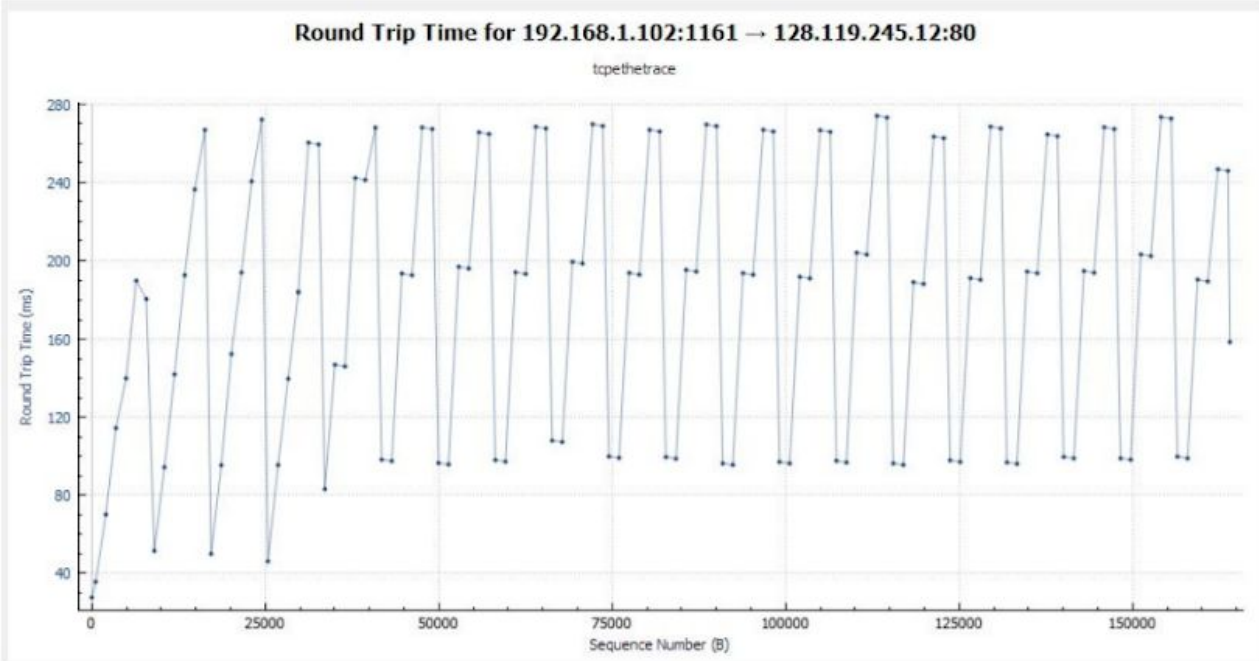
Est. RTT3 = 0.009621546415 * 0.75 + 0.25 * 0.070059 = 0.0180203069402164

Est. RTT4 = 0.0180203069402164 * 0.75 + 0.25 * 0.114428 = 0.0301535207619163

Est. RTT5 = 0.0301535207619163 * 0.75 + 0.25 * 0.139894 = 0.0381372224751006

Est. RTT6 = 0.0381372224751006 * 0.75 + 0.25 * 0.189645 = 0.0528356501672178





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

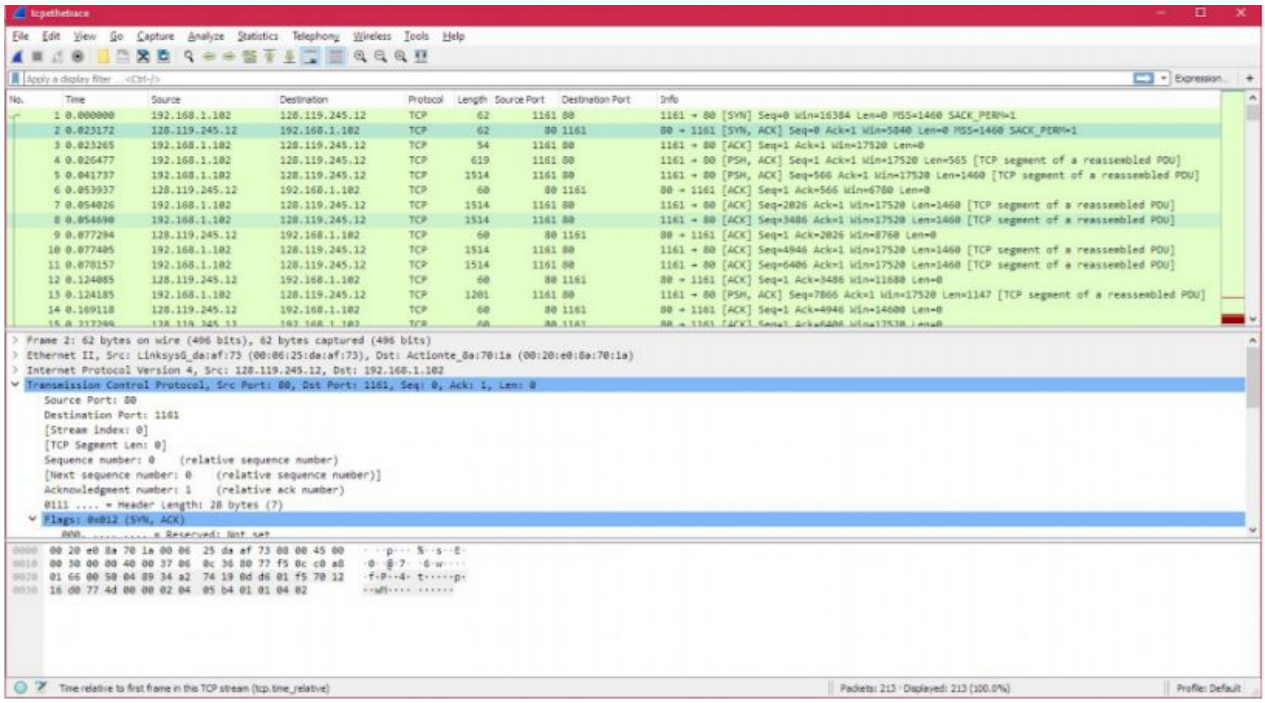
Answer: 1460 bytes

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?

Answer: The minimum amount of buffer space (receiver window) advertised at ser1 for the entire trace is 5840 bytes from the first acknowledgement from the server.

This receiver window grows steadily until a maximum receiver buffer size of 62780 bytes.

The sender is never throttled due to lacking of receiver buffer space by inspecting this trace.



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

Answer: The computation of TCP throughput largely depends on the selection of averaging time period.

We select the average time period as the whole connection time.

The average throughput for this TCP connection = ratio between the total amount data and the total transmission time.

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 No. 4 segment) and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment).

Total data = 164091 - 1 = 164090 bytes.

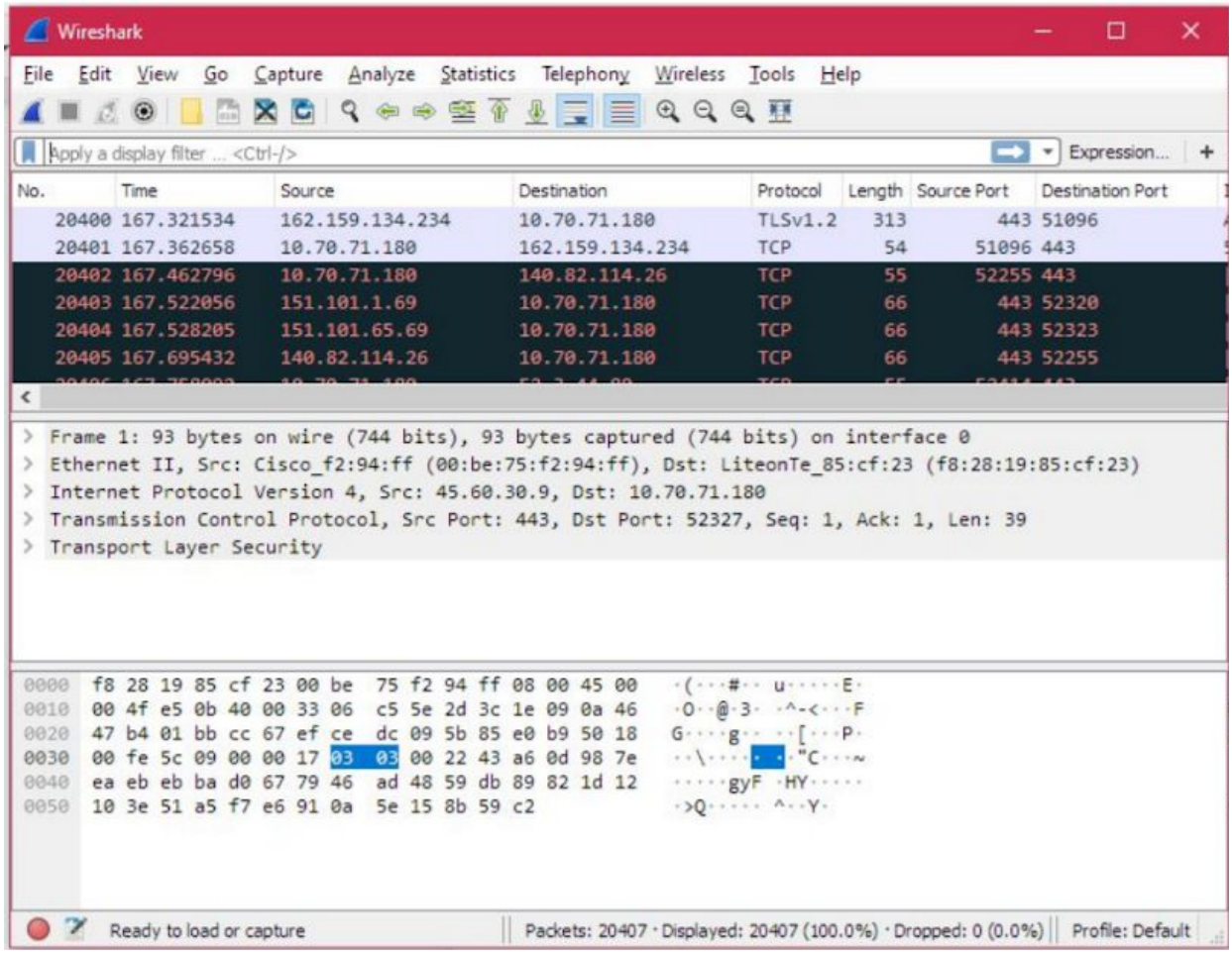
The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment).

Total transmission time = 5.455830 - 0.026477 = 5.4294 seconds.

Hence, the throughput for the TCP connection is computed as 164090/5.4294 = 30.222 KByte/sec.

Screenshots :

Q1.



Q2.

```
Average Packet Size : 720.5083549762336
Average Flow Duration : 21.480878862650638
Average Number of Packets Sent per Flow : 11.357831325301206
Average Number of Packets Received per Flow : 13.228915662650602
Average Number of Bytes Sent per Flow : 1236.4132530120482
Average Number of Bytes Received per Flow : 16478.543373493976
Average Ratio of Incoming Packets to Outgoing Packets : 0.8585610200364299
Average Ratio of Incoming Bytes to Outgoing Bytes : 0.07503170789967034
Average Time Interval b/w Packets Sent : 0.0008714212986660794
Average Ratio of Connections to Number of Destination IPs : 0.6666666666666666
PS C:\Users\Twarit\Desktop\netassign9>
```