COMPUTER NETWORKS LABORATORY

ASSIGNMENT 9

NAME: Abhishek Rathod
ENR. NO. : 17114004
BATCH: CS1

Q1) 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.

Ans -> On running the Wireshark for around 22 minutes (1337 seconds), a total of 68360 packets were transferred.

Q2) 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: ...

Ans.->
Average Packet Size (in Bytes) : 1126.365433

For Ethernet :
Average Flow Duration (seconds) : 778.051995
Average no of packets sent per flow : 5432.800000
Average no of packets recieved per flow : 1403.200000
Average no of bytes sent per flow : 7450106.800000
Average no of bytes recieved per flow : 249727.300000
Average ratio of incoming to outgoing packets : 285.102041
Average ratio of incoming to outgoing bytes : 845.280127

For IPv4 Protocol :
Average Flow Duration (seconds) : 590.446382
Average no of packets sent per flow : 212.984848
Average no of packets recieved per flow : 822.424242
Average no of bytes sent per flow : 43976.818182
Average no of bytes recieved per flow : 1122646.196970
Average ratio of incoming to outgoing packets : 1.441374
Average ratio of incoming to outgoing bytes : 10.374664

For IPv6 Protocol :
Average Flow Duration (seconds) : 512.002181
Average no of packets sent per flow : 2.000000
Average no of packets recieved per flow : 0.000000

Average no of bytes sent per flow : 214.000000
Average no of bytes recieved per flow : 0.000000
Average ratio of incoming to outgoing packets : 0.000000
Average ratio of incoming to outgoing bytes : 0.000000

For TCP Protocol :
Average Flow Duration (seconds) : 75206.388889
Average no of packets sent per flow : 80.768519
Average no of packets recieved per flow : 35.555556
Average no of bytes sent per flow : 81999.268519
Average no of bytes recieved per flow : 6792.879630
Average ratio of incoming to outgoing packets : 0.521702
Average ratio of incoming to outgoing bytes : 0.316130

For UDP Protocol :
Average Flow Duration (seconds) : 197553.654762
Average no of packets sent per flow : 177.398810
Average no of packets recieved per flow : 30.276786
Average no of bytes sent per flow : 202794.833333
Average no of bytes recieved per flow : 5241.178571
Average ratio of incoming to outgoing packets : 0.512547
Average ratio of incoming to outgoing bytes : 0.439947

Average Time Interval b/w Packets Sent (in seconds): 0.095383
Average Time Interval b/w Packets Recieved (in seconds): 0.024620
Average ratio of connections to number of destination IP's : 0.985915

Screenshots :-

abhishek36@MrRathod: ~/Computer Networks/Assignment9_17114004

File Edit View Search Terminal Help

```
(base) abhishek36@MrRathod:~/Computer Networks/Assignment9_17114004$ python3 CodeQ2.py
Average Packet Size (in Bytes) : 1126.365433

For Ethernet :
Average Flow Duration (seconds) : 778.051995
Average no of packets sent per flow : 5432.800000
Average no of packets recieved per flow : 1403.200000
Average no of bytes sent per flow : 7450106.800000
Average no of bytes recieved per flow : 249727.300000
Average ratio of incoming to outgoing packets : 285.102041
Average ratio of incoming to outgoing bytes : 845.280127

For IPv4 Protocol :
Average Flow Duration (seconds) : 590.446382
Average no of packets sent per flow : 212.984848
Average no of packets recieved per flow : 822.424242
Average no of bytes sent per flow : 43976.818182
Average no of bytes recieved per flow : 1122646.196970
Average ratio of incoming to outgoing packets : 1.441374
Average ratio of incoming to outgoing bytes : 10.374664

For IPv6 Protocol :
Average Flow Duration (seconds) : 512.002181
Average no of packets sent per flow : 2.000000
Average no of packets recieved per flow : 0.000000
Average no of bytes sent per flow : 214.000000
Average no of bytes recieved per flow : 0.000000
Average ratio of incoming to outgoing packets : 0.000000
Average ratio of incoming to outgoing bytes : 0.000000

For TCP Protocol :
Average Flow Duration (seconds) : 75206.388889
Average no of packets sent per flow : 80.768519
Average no of packets recieved per flow : 35.555556
Average no of bytes sent per flow : 81999.268519
Average no of bytes recieved per flow : 6792.879630
Average ratio of incoming to outgoing packets : 0.521702
Average ratio of incoming to outgoing bytes : 0.316130
```

abhishek36@MrRathod: ~/Computer Networks/Assignment9_17114004

File Edit View Search Terminal Help

```
Average no of packets recieved per flow : 822.424242
Average no of bytes sent per flow : 43976.818182
Average no of bytes recieved per flow : 1122646.196970
Average ratio of incoming to outgoing packets : 1.441374
Average ratio of incoming to outgoing bytes : 10.374664

For IPv6 Protocol :
Average Flow Duration (seconds) : 512.002181
Average no of packets sent per flow : 2.000000
Average no of packets recieved per flow : 0.000000
Average no of bytes sent per flow : 214.000000
Average no of bytes recieved per flow : 0.000000
Average ratio of incoming to outgoing packets : 0.000000
Average ratio of incoming to outgoing bytes : 0.000000

For TCP Protocol :
Average Flow Duration (seconds) : 75206.388889
Average no of packets sent per flow : 80.768519
Average no of packets recieved per flow : 35.555556
Average no of bytes sent per flow : 81999.268519
Average no of bytes recieved per flow : 6792.879630
Average ratio of incoming to outgoing packets : 0.521702
Average ratio of incoming to outgoing bytes : 0.316130

For UDP Protocol :
Average Flow Duration (seconds) : 197553.654762
Average no of packets sent per flow : 177.398810
Average no of packets recieved per flow : 30.276786
Average no of bytes sent per flow : 202794.833333
Average no of bytes recieved per flow : 5241.178571
Average ratio of incoming to outgoing packets : 0.512547
Average ratio of incoming to outgoing bytes : 0.439947

Average Time Interval b/w Packets Sent (in seconds): 0.095383
Average Time Interval b/w Packets Recieved (in seconds): 0.024620
Average ratio of connections to number of destination IP's : 0.985915

(base) abhishek36@MrRathod:~/Computer Networks/Assignment9_17114004$
```

Q.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)?

Ans->
The client computer (source)'s IP address is 192.168.1.102 and the TCP port number is 1161.
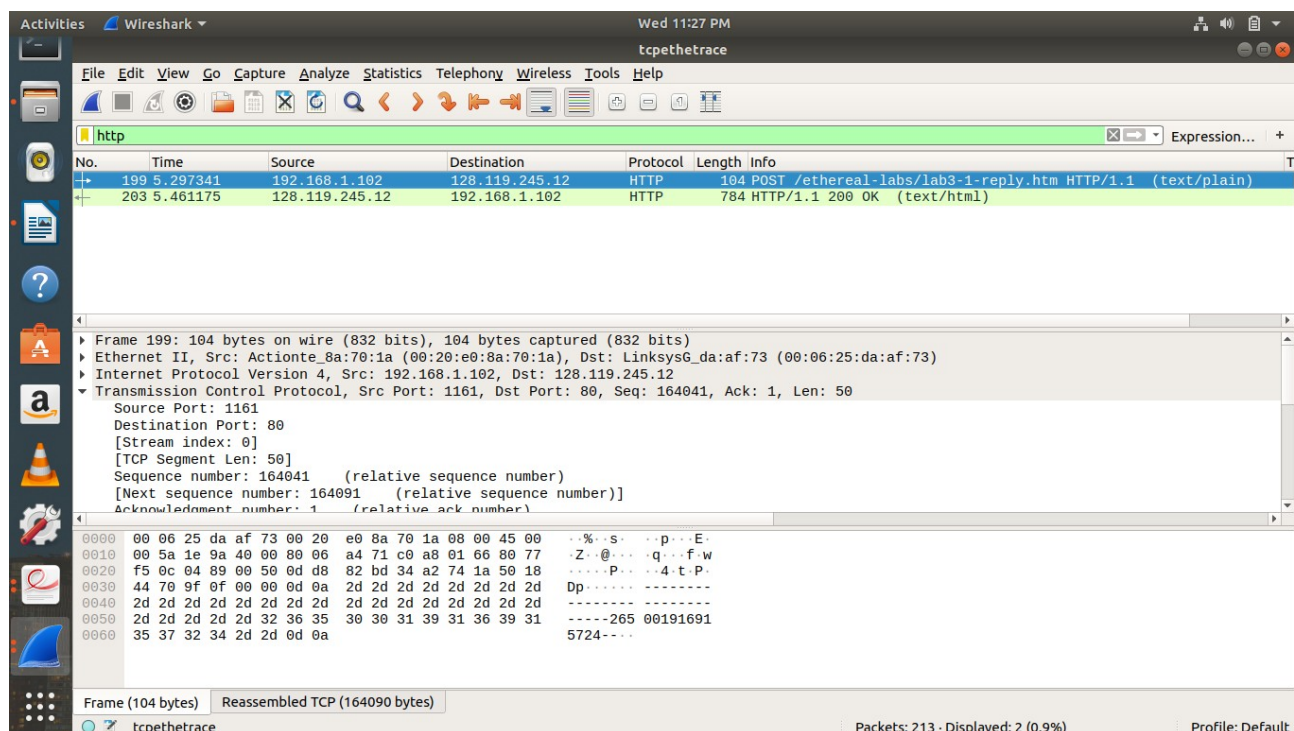
b. What is the IP address of server (ser1)? On what port number it is sending and receiving the TCP segments for this connection?

Ans-> The IP address of ser1 is 128.119.245.12 and the TCP port number is 80.
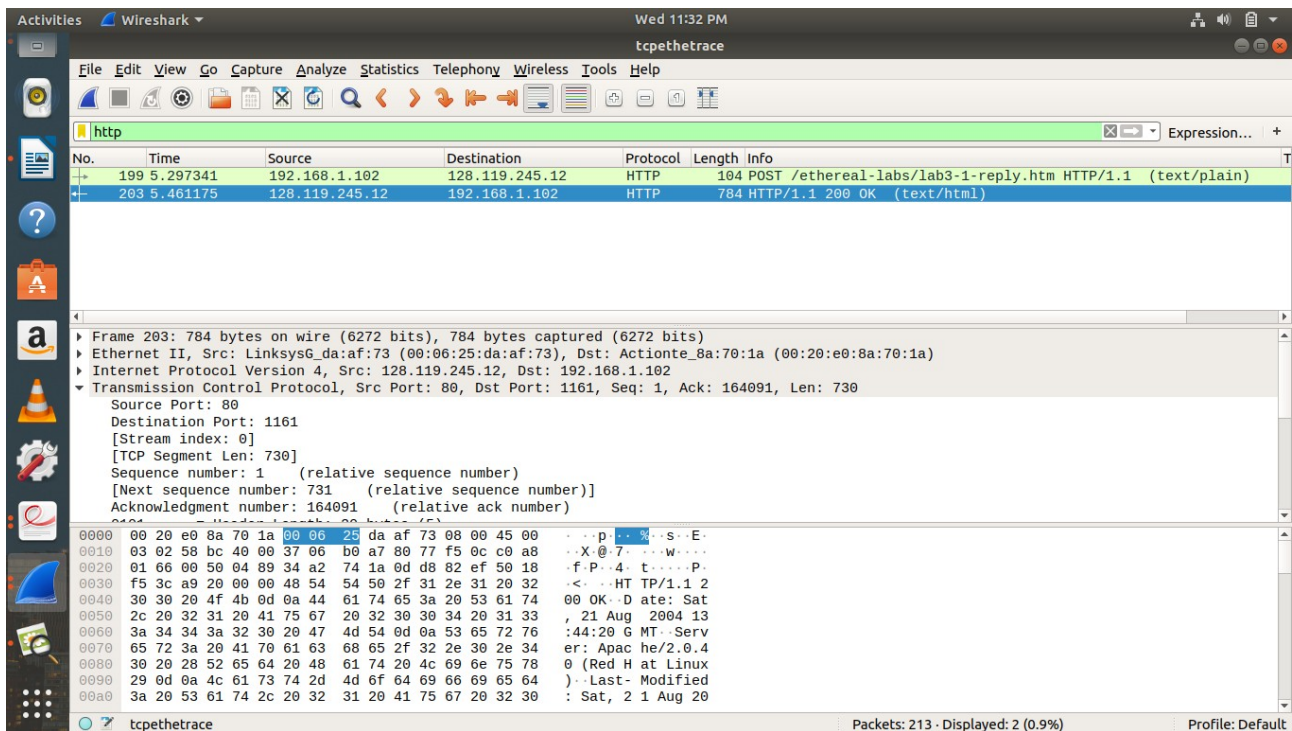
c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ser1? What is it in the segment that identifies the segment as a SYN segment?

Ans-> The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and ser1.
In the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.
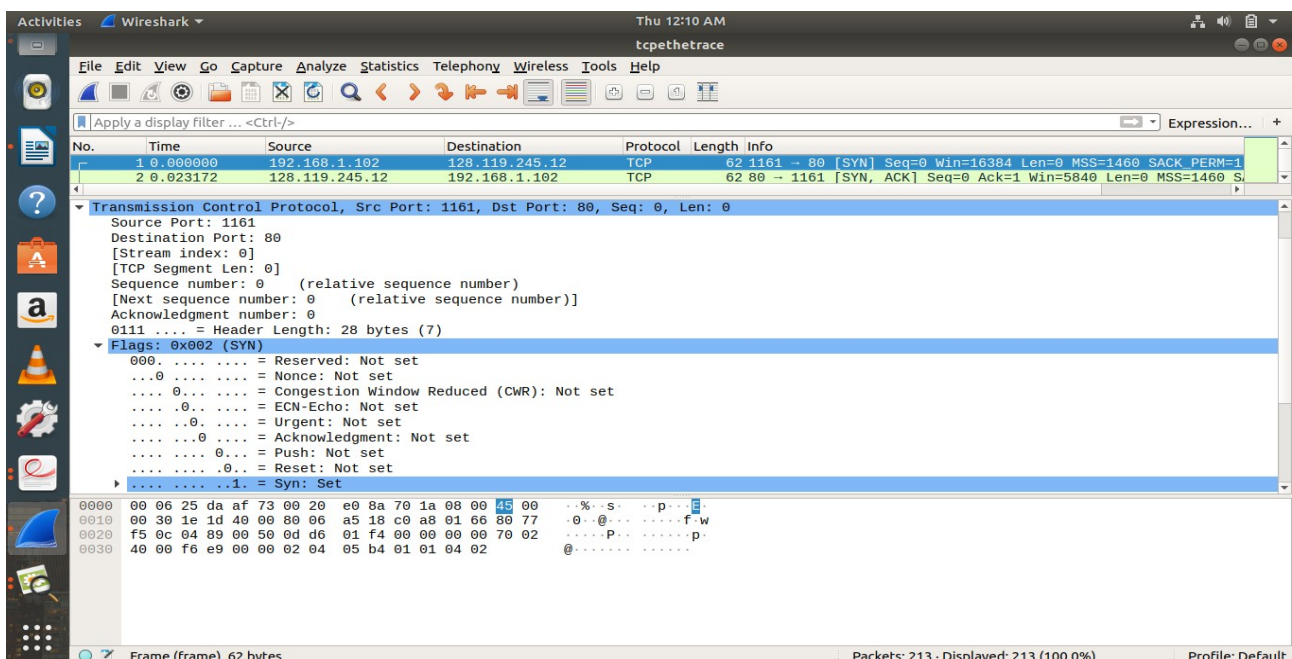
d. What is the sequence number of the SYNACK segment sent by ser1 to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Ans-> 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 form the client computer. For this case, the initial 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 Acknowledgement in the segment are set to 1.
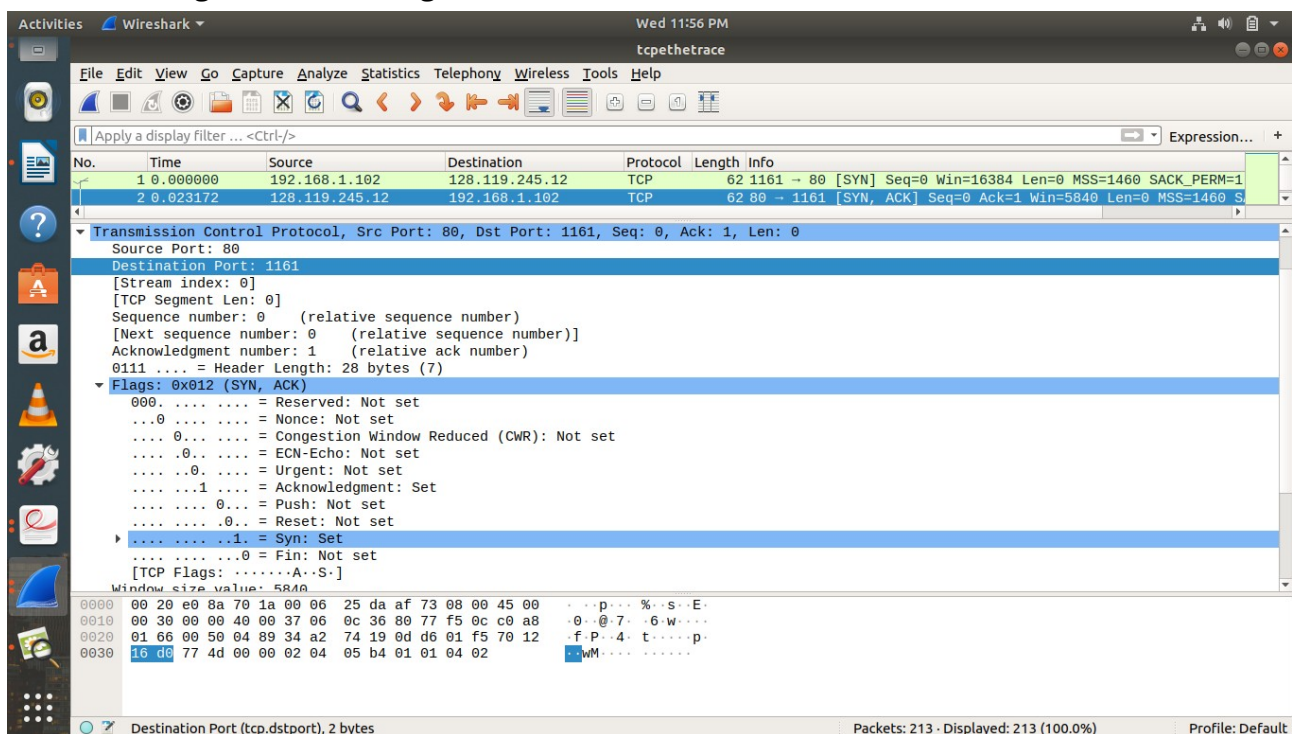
e. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Ans-> The segment No. 4 contains the HTTP POST command, the sequence number of this segment is 1.
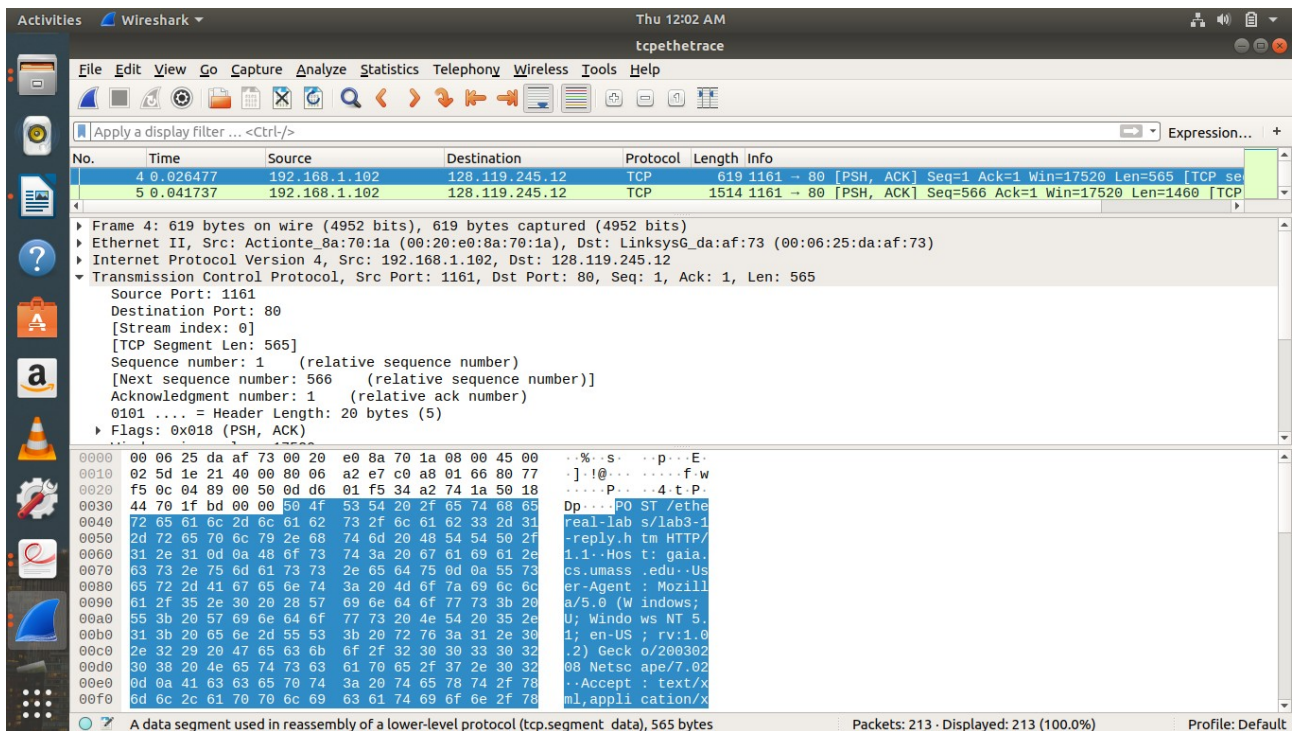
f. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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.

Ans->
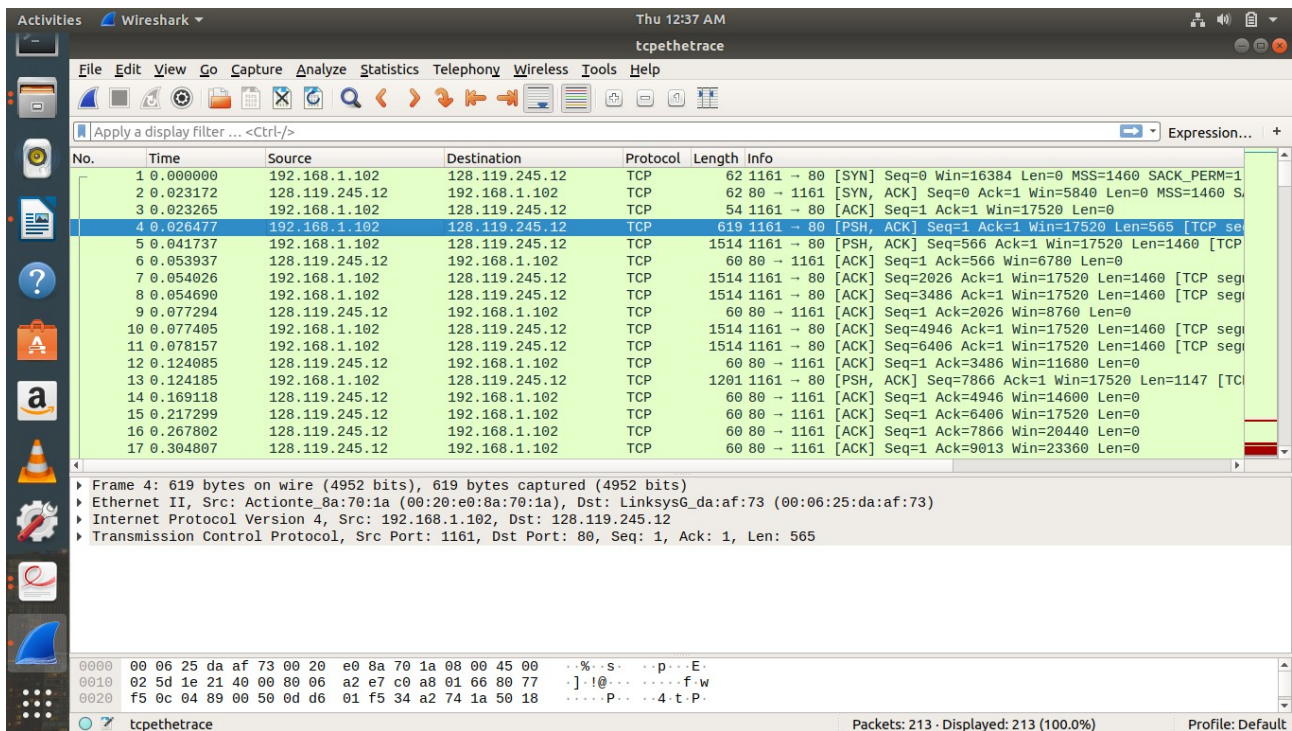
According to above figures, the segments 1-6 are No. 4, 5, 7, 8, 10 and 11. The ACK of segments 1-6 are No. 6, 9, 12, 14, 15 and 16.

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

	Sent time	ACK received time	RTT
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 s

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

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

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

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

EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 s
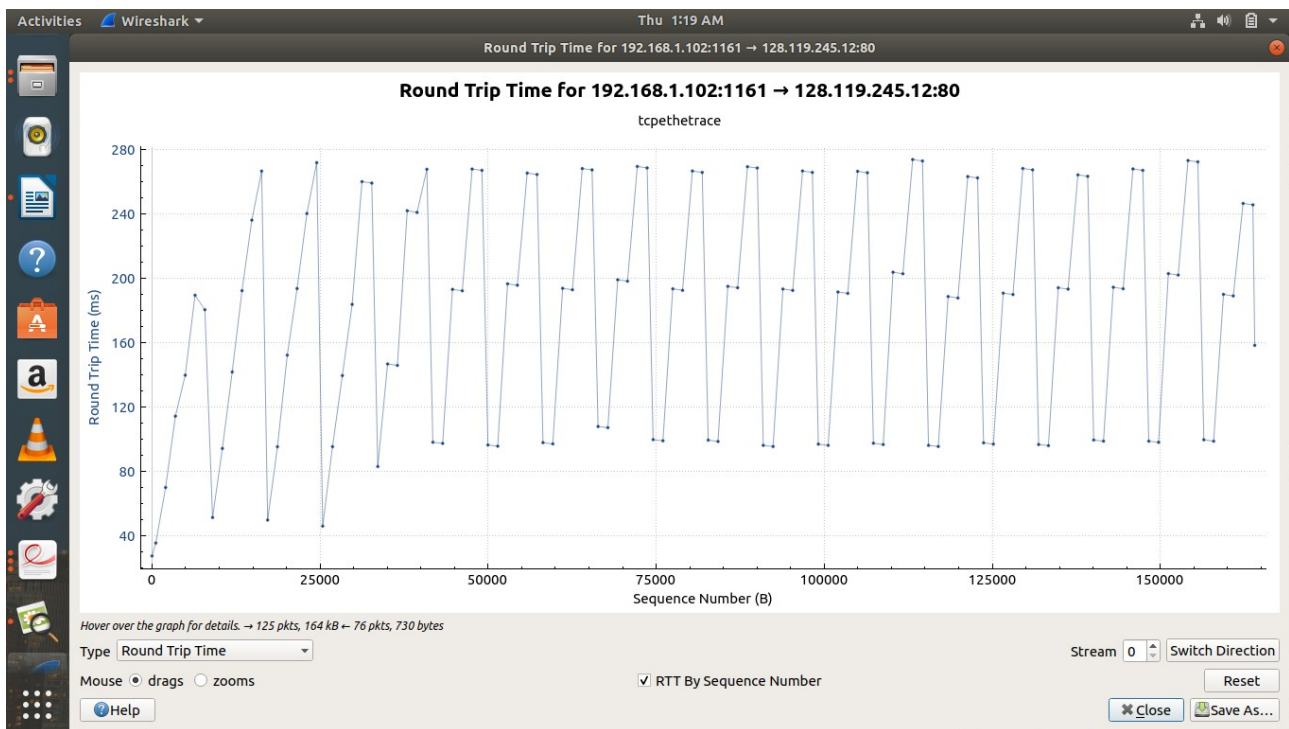
g. What is the length of each of the first six TCP segments?

Ans ->
Length of the first TCP segment (containing the HTTP POST): 565 bytes
Length of each of the other five TCP segments: 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?

Ans->
The minimum amount of buffer space (receiver window) advertised at
ser1 for the entire trace is 17520 bytes, which shows in 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.

The computation of TCP throughput largely depends on the selection of averaging time period. As a common throughput computation, in this question, we select the average time period as the whole connection time. Then, the average throughput for this TCP connection is computed as the 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). 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 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 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

tcpethetrace

File　Edit　View　Go　Capture　Analyze　Statistics　Telephony　Wireless　Tools　Help

Apply a display filter ... <Ctrl-/>　　　　　　　　　　　　　　　　　　　　　⇥ ▾　Expression...　+

No.	Time	Source	Destination	Protocol	Length	Info
194	5.199275	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=159389 Ack=1 Win=17520 Len=1460 [TCP s
195	5.200252	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520 Len=1460 [TCP s
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520 Len=1460 [TCP s
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520 Len=272 [T
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1　(text/plain
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK　(text/html)
204	5.598090	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
205	5.599082	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
207	6.101044	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
208	6.102069	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
209	6.600152	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
210	6.601063	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1

```
   [Next sequence number: 1    (relative sequence number)]
   Acknowledgment number: 164091    (relative ack number)
   0101 .... = Header Length: 20 bytes (5)
 ▸ Flags: 0x010 (ACK)
   Window size value: 62780
   [Calculated window size: 62780]
   [Window size scaling factor: -2 (no window scaling used)]
   Checksum: 0x44a8 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0
```

```
0010   00 28 58 bb 40 00 37 06  b3 82 80 77 f5 0c c0 a8   ·(X·@·7·  ···w····
0020   01 66 00 50 04 89 34 a2  74 1a 0d d8 82 ef 50 10   ·f·P··4·  t·····P·
0030   f5 3c 44 a8 00 00 e5 e7  00 00 07 fb               ·<D····· ····
```

Acknowledgment number (tcp.ack), 4 bytes　　　　　　　　Packets: 213 · Displayed: 213 (100.0%)　　　　Profile: Default