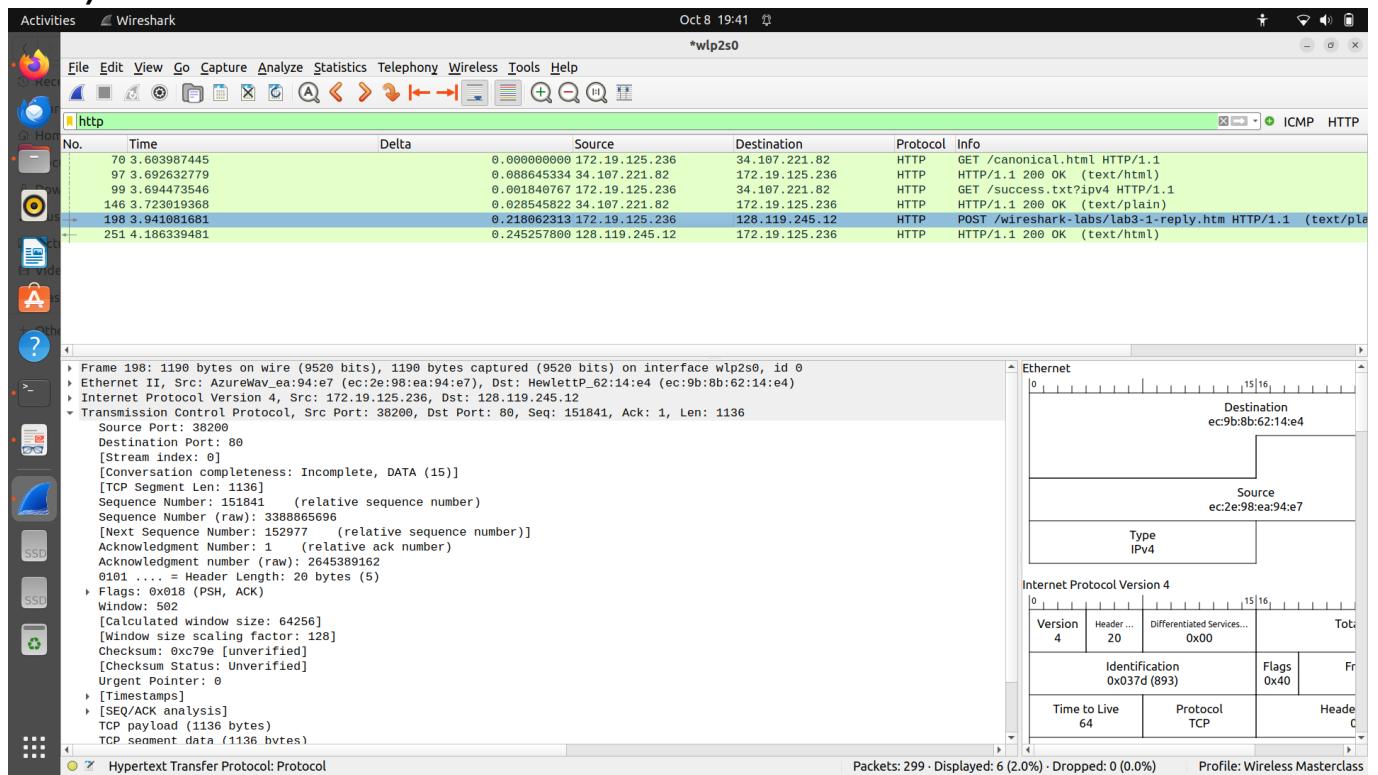


Wireshark assignment -2

Arjit Gupta
CS23mtech12001

1)



1)

IP address: 172.19.125.236

Source Port: 38200

2) IP address: 128.119.245.12

Source Port: 80

3)

Activities Wireshark Oct 8 19:49 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Delta	Source	Destination	Protocol	Info
28	2.846303700		0.000000000 172.19.125.236	128.119.245.12	TCP	38200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
29	3.096854403		0.250556703 172.19.125.236	128.119.245.12	TCP	38212 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
30	3.118760914		0.021906511 128.119.245.12	172.19.125.236	TCP	80 → 38200 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
31	3.118812085		0.000051171 172.19.125.236	128.119.245.12	TCP	38200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
32	3.119399074		0.000577989 172.19.125.236	128.119.245.12	TCP	38200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=1460 [TC]
33	3.119400524		0.000010450 172.19.125.236	128.119.245.12	TCP	38200 → 80 [PSH, ACK] Seq=1461 Ack=1 Win=64256 Len=0
34	3.120380415		0.000979891 172.19.125.236	128.119.245.12	TCP	38200 → 80 [ACK] Seq=2921 Ack=1 Win=64256 Len=1460
35	3.120383361		0.000002946 172.19.125.236	128.119.245.12	TCP	38200 → 80 [PSH, ACK] Seq=4381 Ack=1 Win=64256 Len=0

Transmission Control Protocol, Src Port: 38200, Dst Port: 80, Seq: 0, Len: 0

Source Port: 38200
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3388713855
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

000. = Reserved: Not set
...0. = Nonce: Not set
.... 0. = Congestion Window Reduced (CWR): Not set
.... .0. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... 0.... = Push: Not set
....0.... = Reset: Not set
....1.... = Syn: Set
....0.... = Fin: Not set
[TCP Flags:S.]
Window: 64240
[Calculated window size: 64240]
Checksum: 0xe372 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
[Timestamps]

This shows the raw value of the sequence number (tcp.seq_raw), 4 bytes

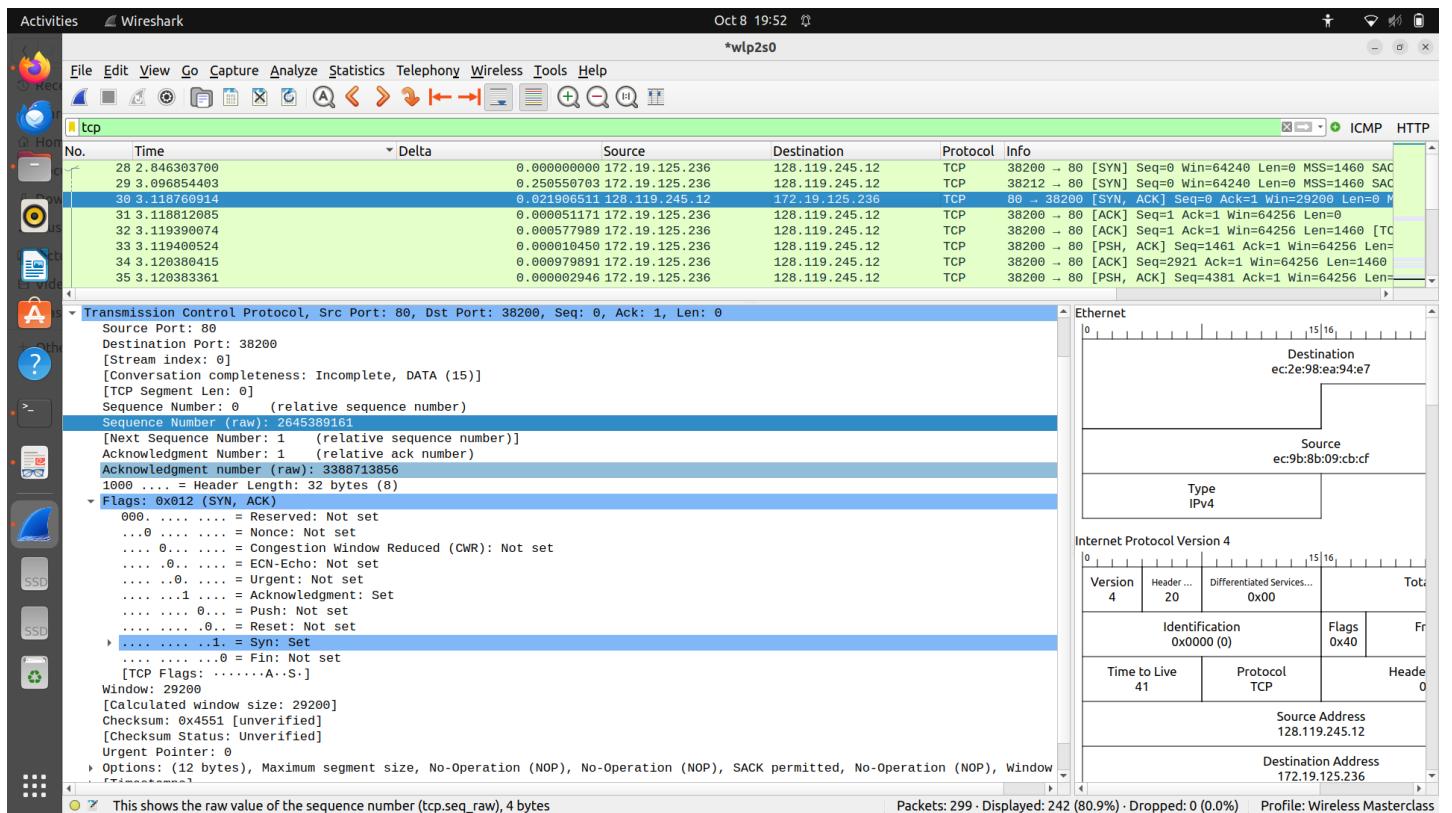
Ethernet

Internet Protocol Version 4

Packets: 299 · Displayed: 242 (80.9%) · Dropped: 0 (0.0%) · Profile: Wireless Masterclass

Seq no: 3388713855

4)

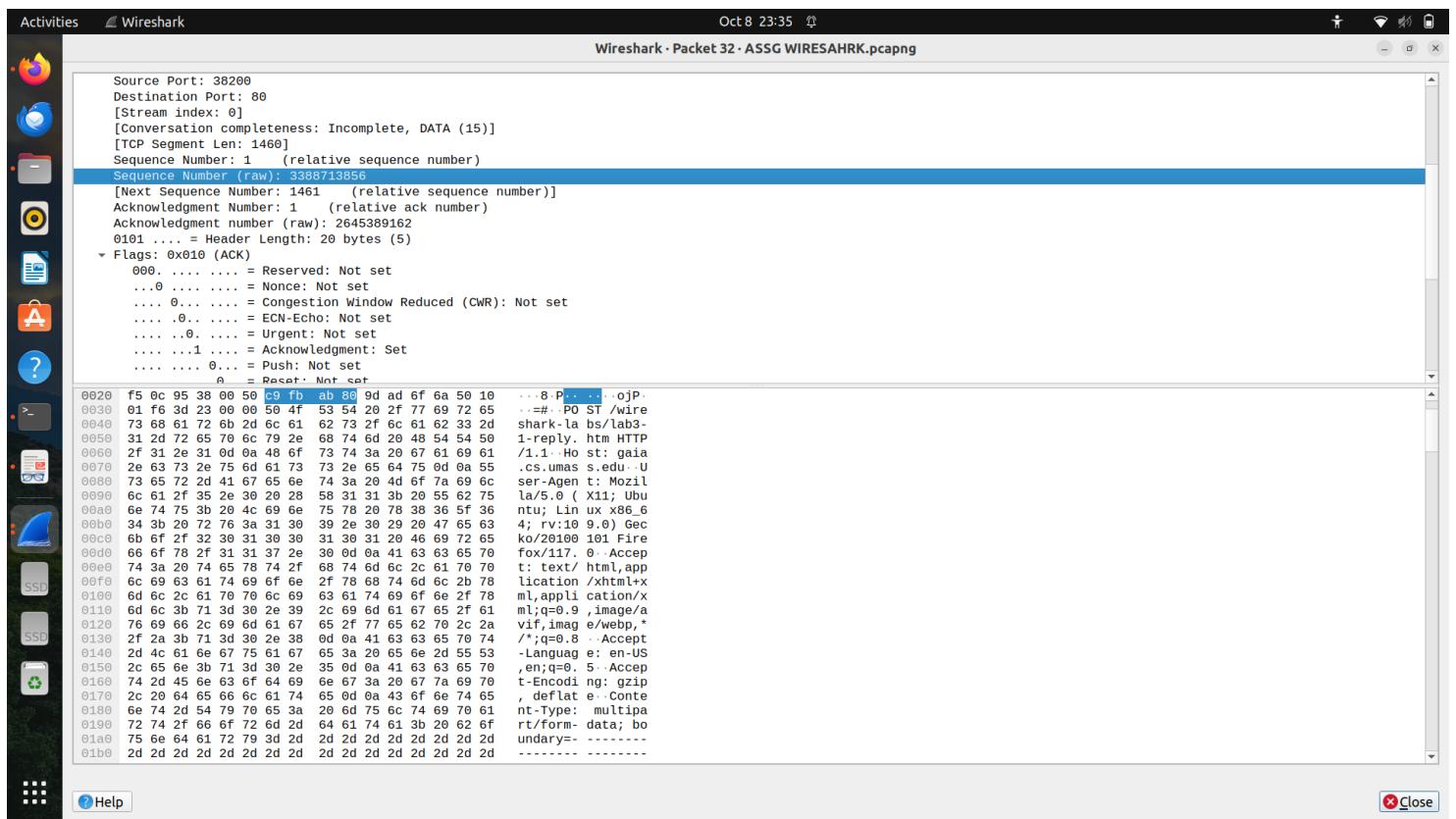


Sequence no(raw): 2645389161

Acknowledgement no. : 3388713856

See the flags, there Syn is “1” and Acknowledgement is “1”. This indicates that the packet is SYN ACK packet.

5)



Sequence number(raw): 3388713856

Payload: Tcp payload = 1460 bytes

No, data is divided into multiple segments

6)

```
▼ Frame 33: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp2s0, id 0
  ▶ Interface id: 0 (wlp2s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 8, 2023 19:34:01.245226965 IST
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1696773841.245226965 seconds
      [Time delta from previous captured frame: 0.000010450 seconds]
      [Time delta from previous displayed frame: 0.000010450 seconds]
      [Time since reference or first frame: 3.119400524 seconds]
    Frame Number: 33
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertvde:ip:tcp]
```



```
▼ Frame 32: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp2s0, id 0
  ▶ Interface id: 0 (wlp2s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 8, 2023 19:34:01.245216515 IST
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1696773841.245216515 seconds
      [Time delta from previous captured frame: 0.000577989 seconds]
      [Time delta from previous displayed frame: 0.000577989 seconds]
      [Time since reference or first frame: 3.119390074 seconds]
    Frame Number: 32
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
      [Frame is marked: True]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertvde:ip:tcp]
```

Arrival Time: Oct 8, 2023 19:34:01.245216515 IST

Ack receive time: Oct 8, 2023 19:34:01.245226965 IST

RTT for 1st packet : | 245226965 - 245216515 |

=.245210450 ms

RTT for second packet: 19:34:01.245228112 - 19:34:01.245226965

= .2452241147 ms

Estimated RTT:

$$\begin{aligned}
 \text{EstimatedRTT} &= (1 - \alpha) * \text{EstimatedRTT} + \alpha * \text{SampleRTT} \\
 &= (1 - 0.125) * .2452241147 + 0.125 * .245210450 \text{ ms} \\
 &= 0.21457110036 + 0.03065130625 \\
 &= 0.24522240661 \text{ seconds}
 \end{aligned}$$

7)

32 3.119390074	172.19.125.236	128.119.245.12	TCP	1514
33 3.119400524	172.19.125.236	128.119.245.12	TCP	1514
34 3.120380415	172.19.125.236	128.119.245.12	TCP	1514
35 3.120383361	172.19.125.236	128.119.245.12	TCP	1514
36 3.121302401	172.19.125.236	128.119.245.12	TCP	1514
37 3.121304305	172.19.125.236	128.119.245.12	TCP	1514
38 3.122232805	172.19.125.236	128.119.245.12	TCP	1514

Length of the first four TCP segments is 1460 +20 Bytes

1480 Bytes
(header + payload)

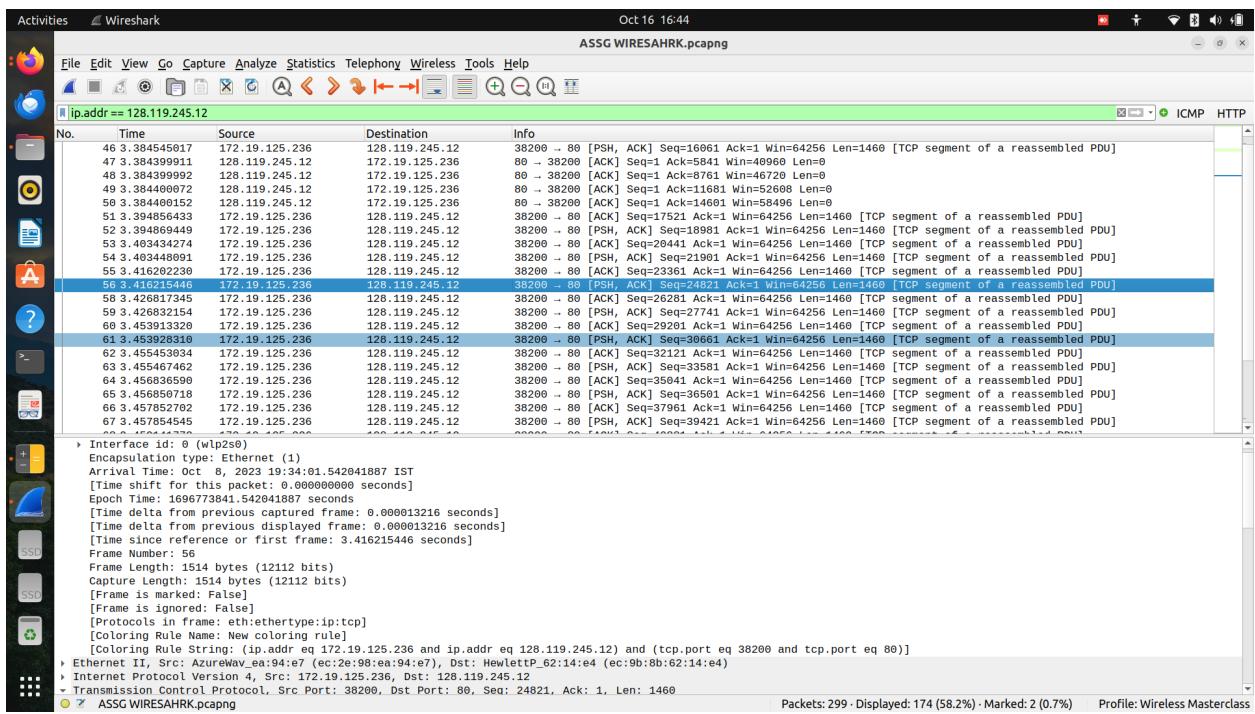
8)

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Info	
28 2.846303700	172.19.125.236	128.119.245.12		38200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3299605096 TSeср=0 WS=128	
29 3.096854493	172.19.125.236	128.119.245.12		38212 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3299605347 TSeср=0 WS=128	
30 3.118760914	128.119.245.12	172.19.125.236		80 → 38200 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128	
31 3.118812085	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0	
32 3.11940074	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
33 3.119400524	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=1461 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
34 3.120380415	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=2921 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
35 3.120383361	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=4381 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
36 3.121302401	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=5841 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
37 3.121304305	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=7301 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
38 3.122232805	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=8761 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
39 3.122235039	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=16221 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
40 3.123193888	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=11681 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
41 3.123196243	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=13141 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
42 3.384399280	128.119.245.12	172.19.125.236		80 → 38212 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128	
43 3.384561481	172.19.125.236	128.119.245.12		38212 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0	
44 3.384399831	128.119.245.12	172.19.125.236		80 → 38200 [ACK] Seq=1 Ack=2921 Win=35072 Len=0	
45 3.384541951	172.19.125.236	128.119.245.12		38200 → 80 [ACK] Seq=14601 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
46 3.384395017	172.19.125.236	128.119.245.12		38200 → 80 [PSH, ACK] Seq=16061 Ack=1 Win=64256 Len=1460 [TCP segment of a reassembled PDU]	
47 3.384399911	128.119.245.12	172.19.125.236		80 → 38200 [ACK] Seq=1 Ack=5841 Win=40960 Len=0	
48 3.384399992	128.119.245.12	172.19.125.236		80 → 38200 [ACK] Seq=1 Ack=8761 Win=46720 Len=0	
49 3.384400078	128.119.245.12	172.19.125.236		80 → 38200 [ACK] Seq=1 Ack=11681 Win=50000 Len=0	

Minimum window size advertised by receiver : 29200 B

No there is no throttle because we never sent more data than the available window size at the receiver side.

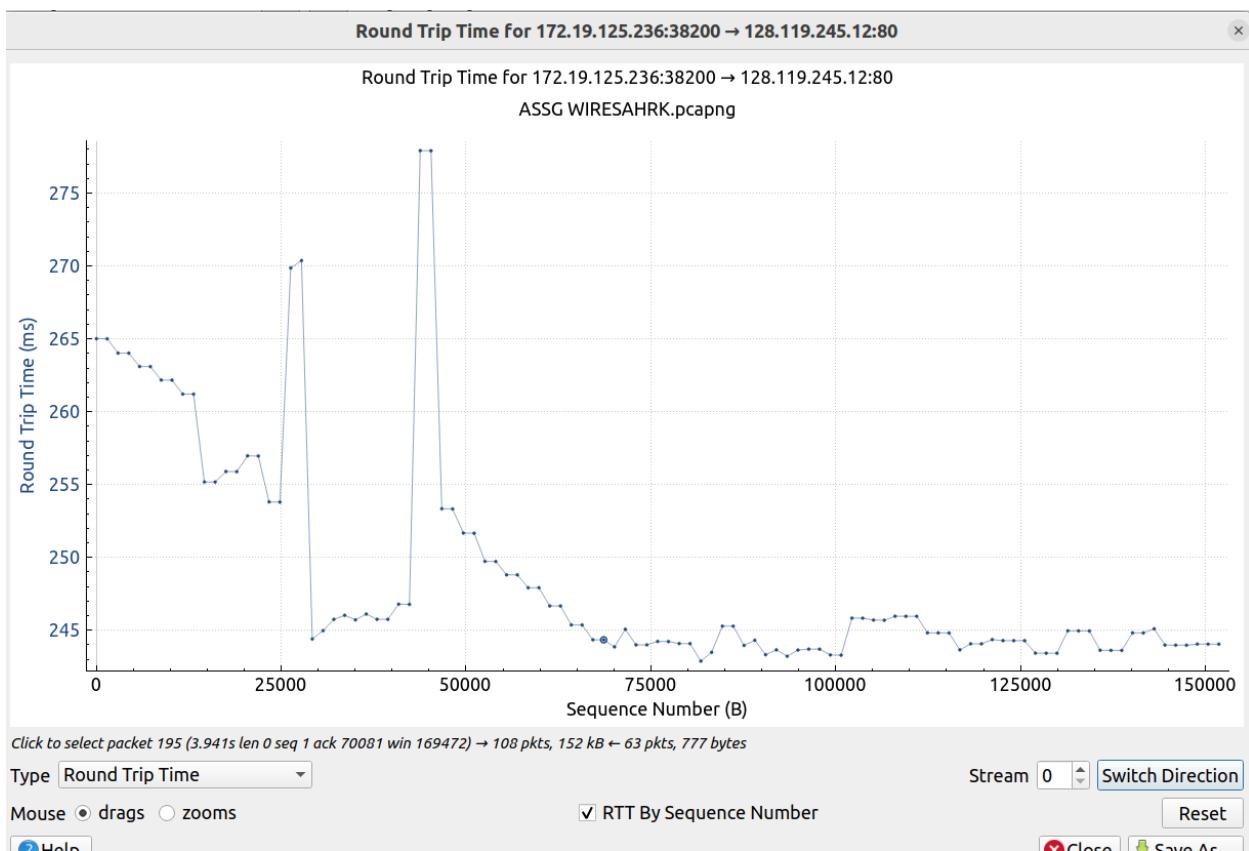
9)



It is 64256 B for data carrying segments. It is the same throughout the communication.

Q10) No there are no retransmissions as we can see using Round Trip Graph

If there were back lines as same sequence number would have been visited again then there are re-transmissions



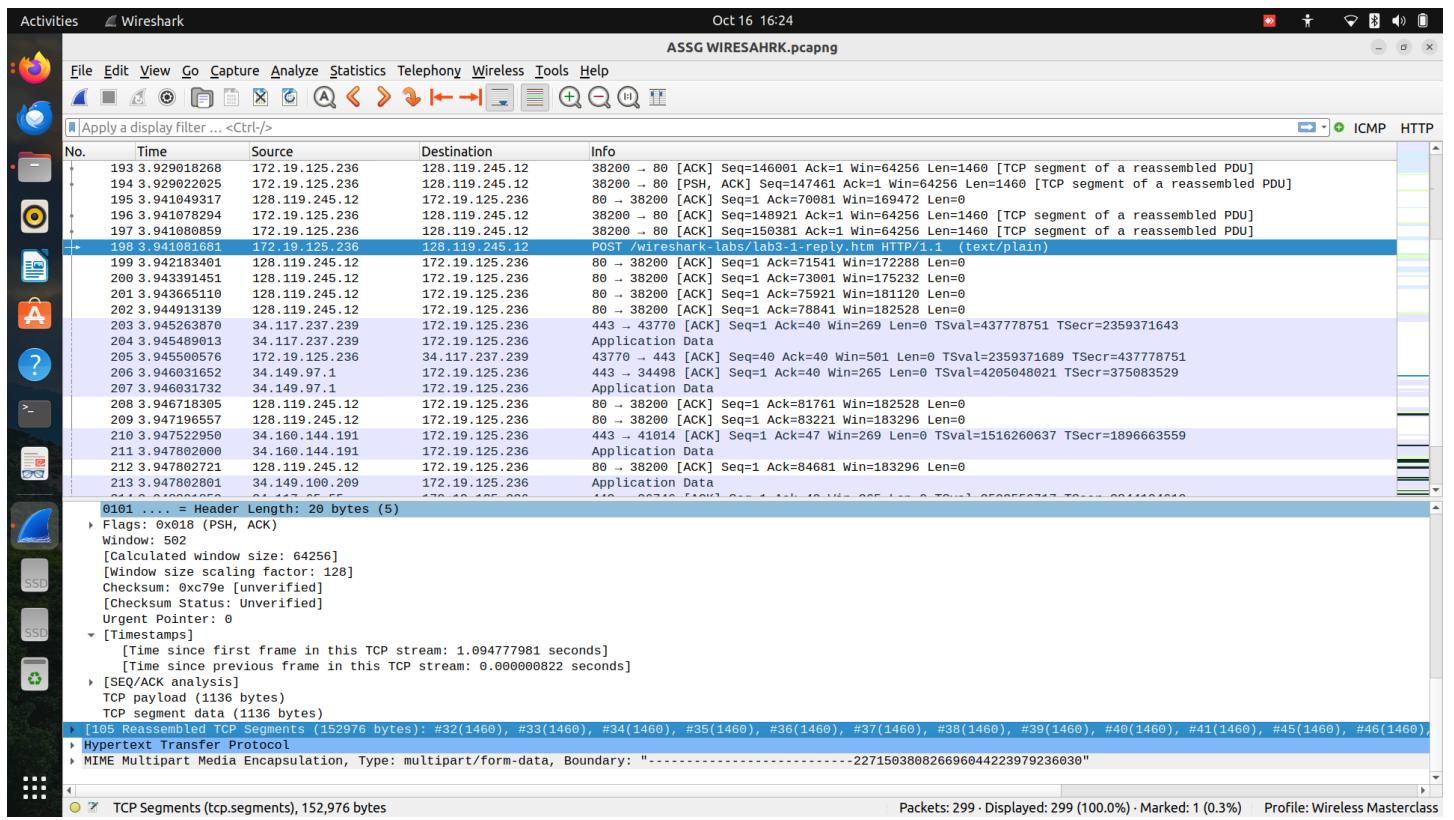
11)

	Ack Seq number	Acknowledged data
Ack 1	1	1460 Bytes
Ack 2	-	1460 Bytes
Ack 3	2921	1460 Bytes
Ack 4	-	1460 Bytes
Ack 5	5841	1460 Bytes
Ack 6	7301	1460 Bytes
Ack7	8761	1460 Bytes
Ack 8	-	1460 Bytes
Ack 9	11681	1460 Bytes
Ack 10		1460 Bytes

Yes there are cases when their is cumulative acknowledgement. For ack 2, there is cum ack, similarly for ack 4 and ack 8, there is cum acknowledgement.

Segment size is 1460 B in all the packets.

12)



First segment sent time:

Arrival Time: Oct 8, 2023 19:34:01.245216515 IST

Last segment ack time:

Arrival Time: Oct 8, 2023 19:34:02.066908124 IST

Total time taken = Last segment ack time - First segment sent time

$$02.066908124 - 01.245216515 = 0.821691609 \text{ seconds}$$

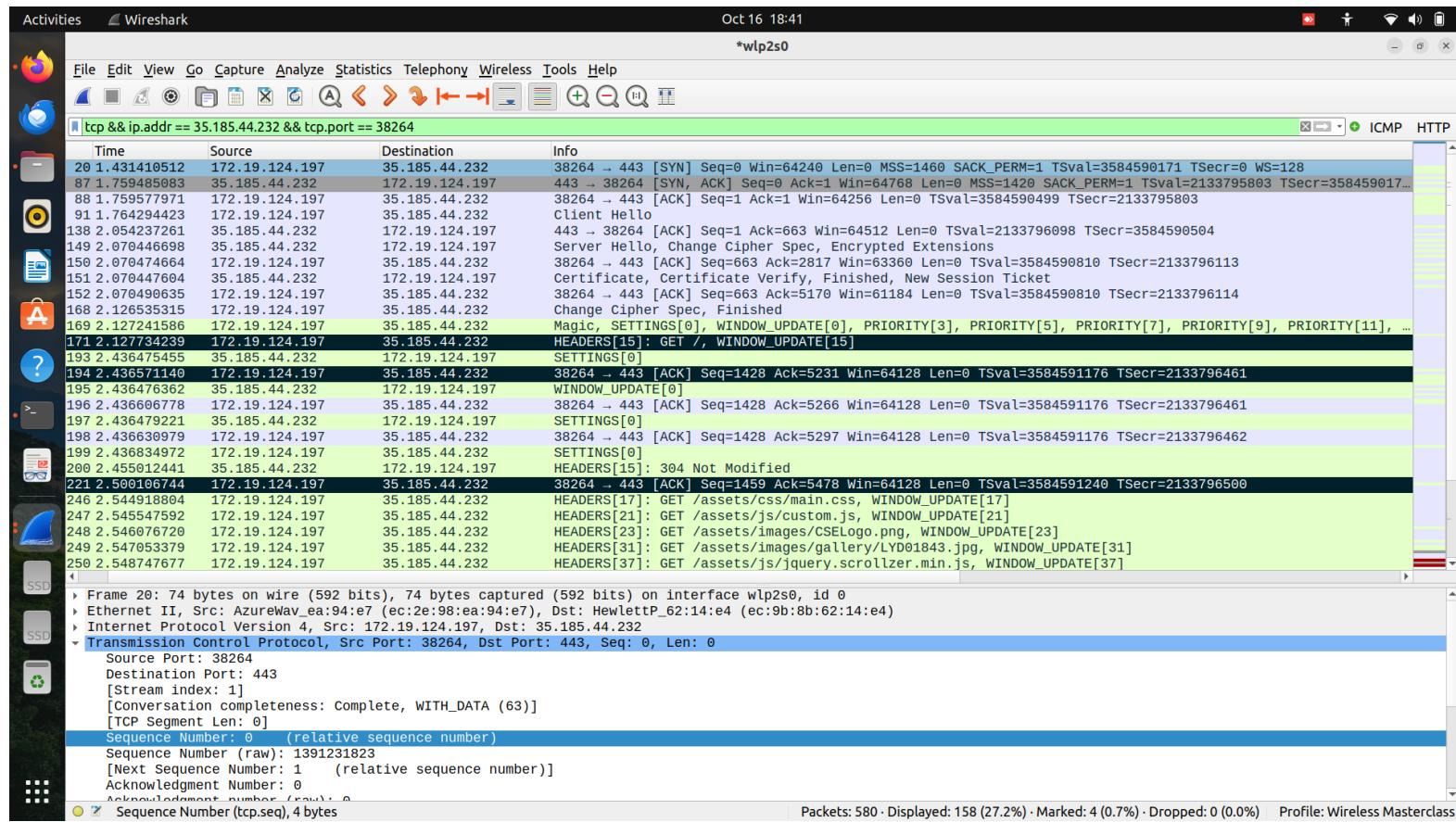
Throughput = total data sent / Total time taken

= 152976B / 0.821691609 seconds
=186172.036229227 B / sec

= 186 KB/sec

Part B -

1)



Q1 and Q2)

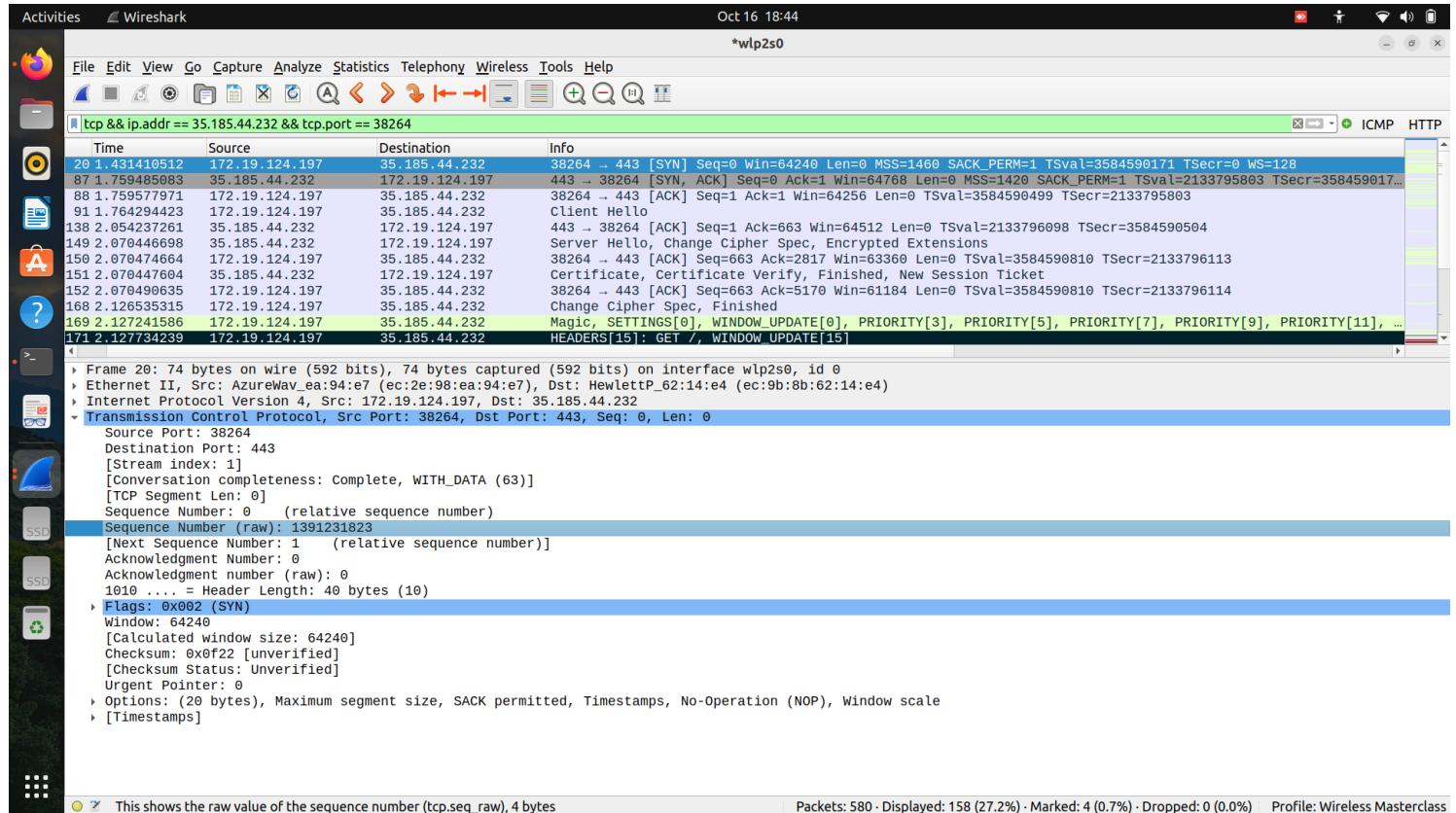
Source Port: 38264

Destination Port: 443

Source Address: 172.19.124.197

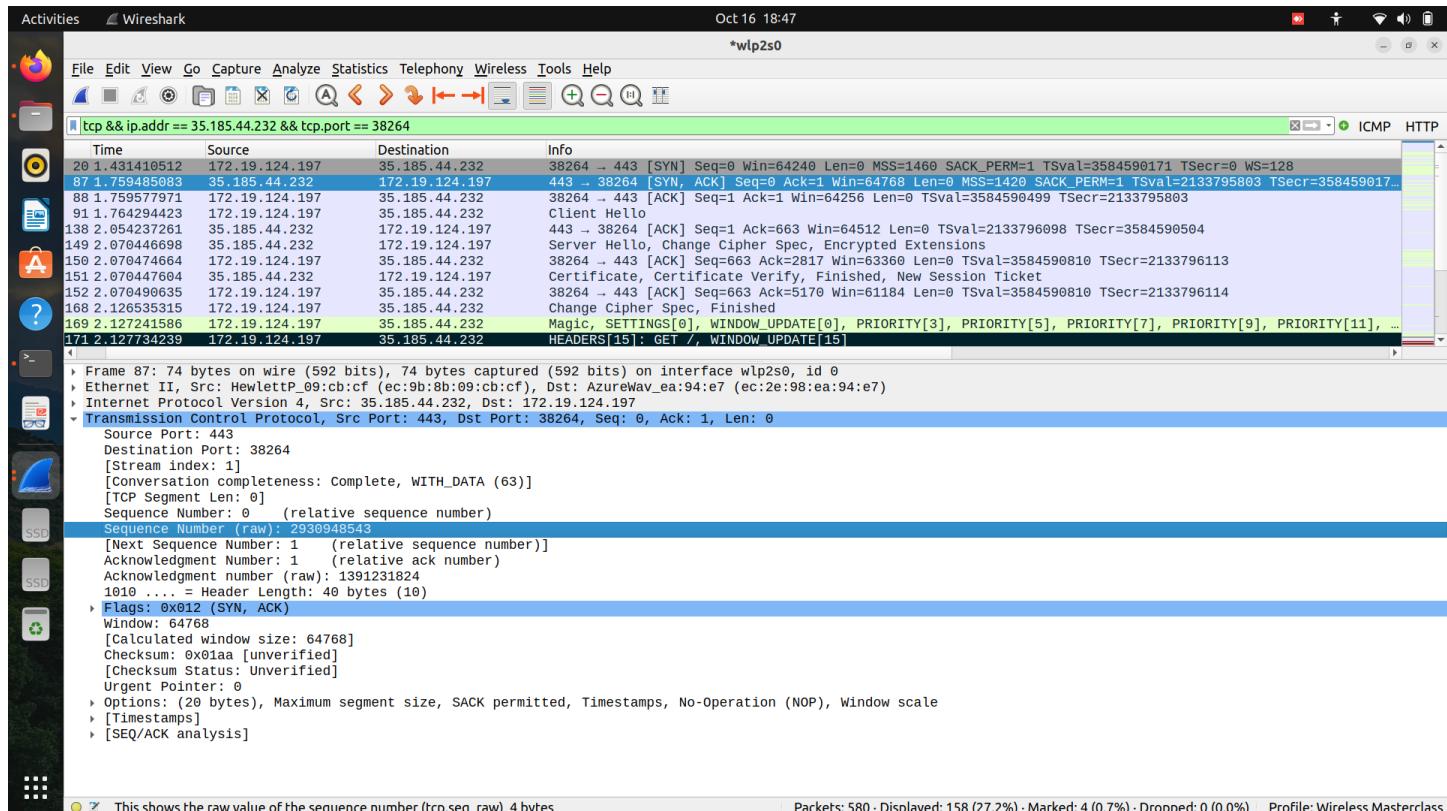
Destination Address: 35.185.44.232

Q3)



Sequence Number (raw): 1391231823

Q4)

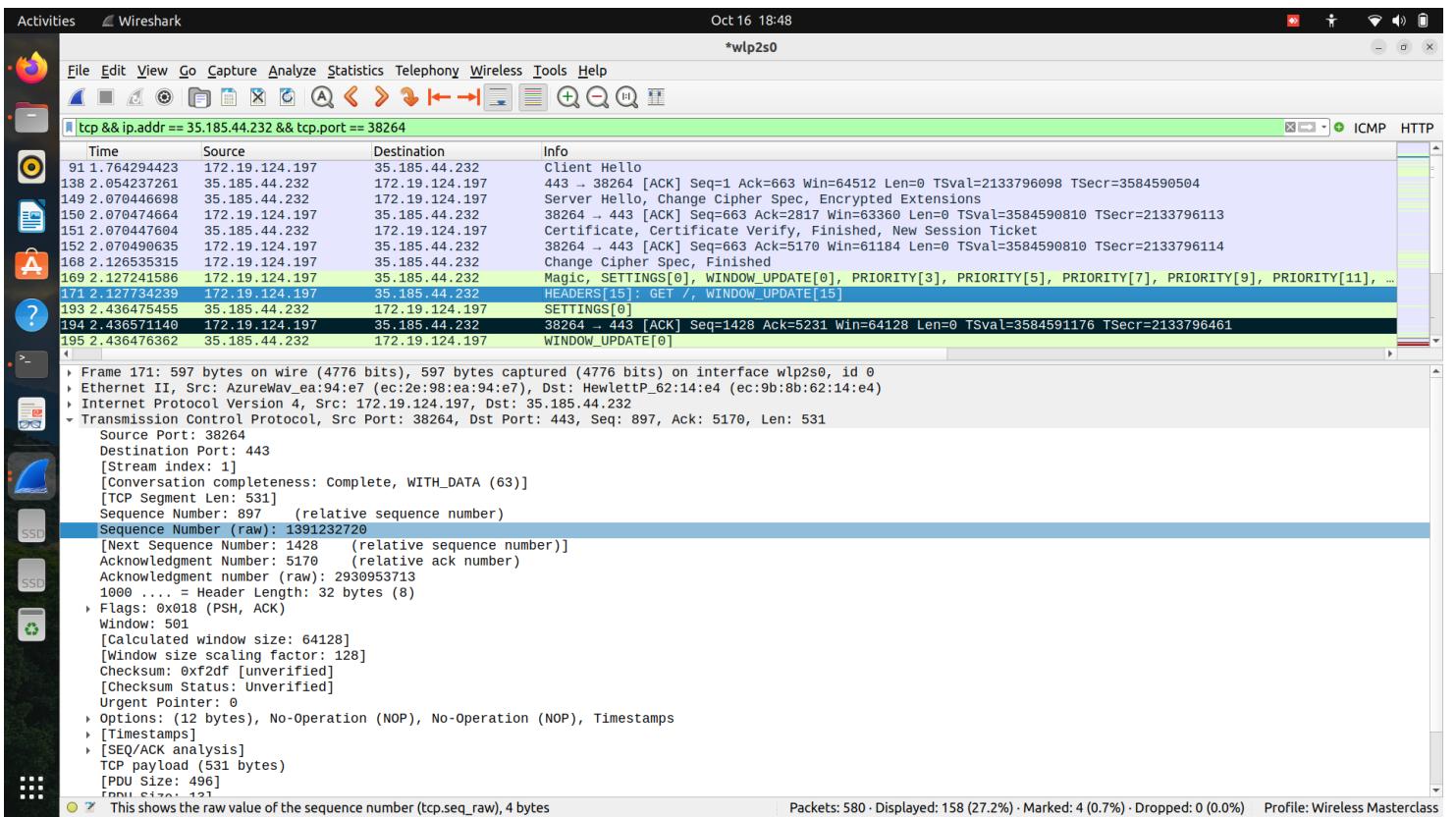


Sequence Number (raw): 2930948543

Acknowledgment number (raw): 1391231824

See the flags, there Syn is “1” and Acknowledgement is “1”. This indicates that the packet is SYN ACK packet.

Q5)

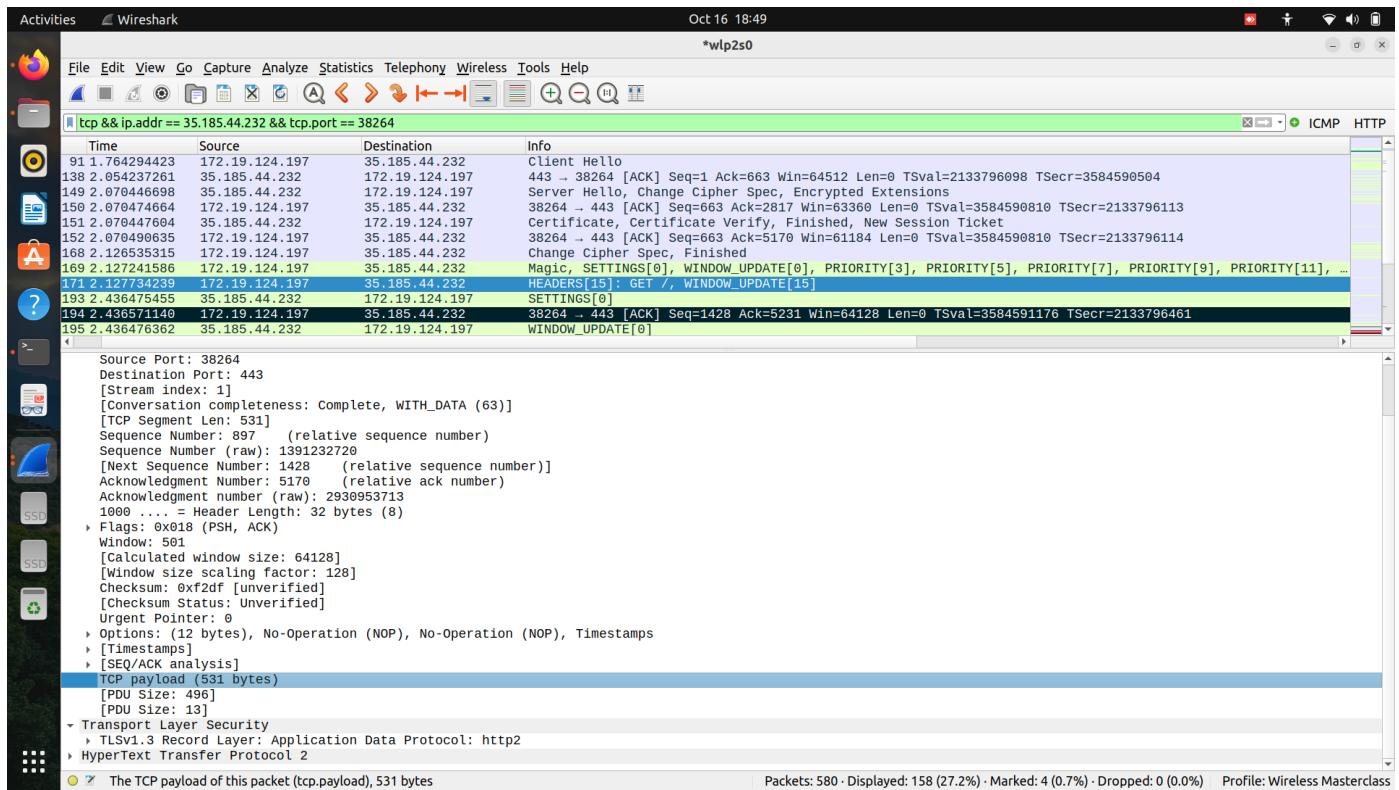


Sequence number of the packet containing GET request:

Sequence Number (raw): 1391232720

This was a get request so all the data was transferred in a single request

Q6)



TCP payload (531 bytes)

Time at which the GET was sent.

Arrival Time: Oct 16, 2023 18:06:36.276286698 IST

Ack is received at

Arrival Time: Oct 16, 2023 18:06:36.585028821 IST

$$\begin{aligned} \text{RTT} &= 18:06:36.585028821 - 18:06:36.276286698 \\ &= 18:06:36.308742123 \end{aligned}$$

Estimated RTT:

$$\begin{aligned}\text{EstimatedRTT} &= (1 - \alpha) * \text{EstimatedRTT} + \alpha * \text{SampleRTT} \\ &= (1 - 0.125) * .585028821 + 0.125 * .276286698 \text{ ms} \\ &= .0.51190021837 + 0.03453583725 \\ &= 0.54643605562 \text{ seconds}\end{aligned}$$

Q7)

segment 1: 531 bytes

Segment 2: 142 bytes

Segment 3: 52 bytes

Segment 4: 104 bytes

Q8)

Oct 16 19:10 *wlp2s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp & ip.addr == 35.185.44.232 & tcp.port == 38264

No. Time Source Destination Info

No.	Time	Source	Destination	Info
150	2.070474664	172.19.124.197	35.185.44.232	38264 → 443 [ACK] Seq=663 Ack=2817 Win=63360 Len=0 TSval=3584590810 TSecr=2133796113
151	2.070447604	35.185.44.232	172.19.124.197	35.185.44.232 → 172.19.124.197 Certificate, Certificate Verify, Finished, New Session Ticket
152	2.070490635	172.19.124.197	35.185.44.232	38264 → 443 [ACK] Seq=663 Ack=5170 Win=61184 Len=0 TSval=3584590810 TSecr=2133796114
168	2.126535315	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 Change Cipher Spec, Finished
169	2.127241586	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 Magic, SETTINGS[0], WINDOW_UPDATE[0], PRIORITY[3], PRIORITY[5], PRIORITY[7], PRIORITY[9], PRIORITY[11]
171	2.127734239	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 HEADERS[15]: GET /, WINDOW_UPDATE[15]
193	2.436475455	35.185.44.232	172.19.124.197	35.185.44.232 → 172.19.124.197 SETTINGS[0]
194	2.436571140	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 38264 → 443 [ACK] Seq=1428 Ack=5231 Win=64128 Len=0 TSval=3584591176 TSecr=2133796461
195	2.436476362	35.185.44.232	172.19.124.197	35.185.44.232 → 172.19.124.197 WINDOW_UPDATE[0]
196	2.436606778	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 38264 → 443 [ACK] Seq=1428 Ack=5266 Win=64128 Len=0 TSval=3584591176 TSecr=2133796461
197	2.436479221	35.185.44.232	172.19.124.197	35.185.44.232 → 172.19.124.197 SETTINGS[0]
198	2.436630979	172.19.124.197	35.185.44.232	35.185.44.232 → 172.19.124.197 38264 → 443 [ACK] Seq=1428 Ack=5297 Win=64128 Len=0 TSval=3584591176 TSecr=2133796462

Source Port: 38264
Destination Port: 443
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (63)]
[TCP Segment Len: 531]
Sequence Number: 897 (relative sequence number)
Sequence Number (raw): 1391232720
[Next Sequence Number: 1428 (relative sequence number)]
Acknowledgment Number: 5170 (relative ack number)
Acknowledgment number (raw): 2930953713
1000 = Header Length: 32 bytes (8)
Flags: PSH, ACK
Window: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0xf2df [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (531 bytes)
[PDU Size: 496]
[PDU Size: 13]
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: http2
HyperText Transfer Protocol 2

The scaled window size (if scaling has been used) (tcp.window_size), 2 bytes

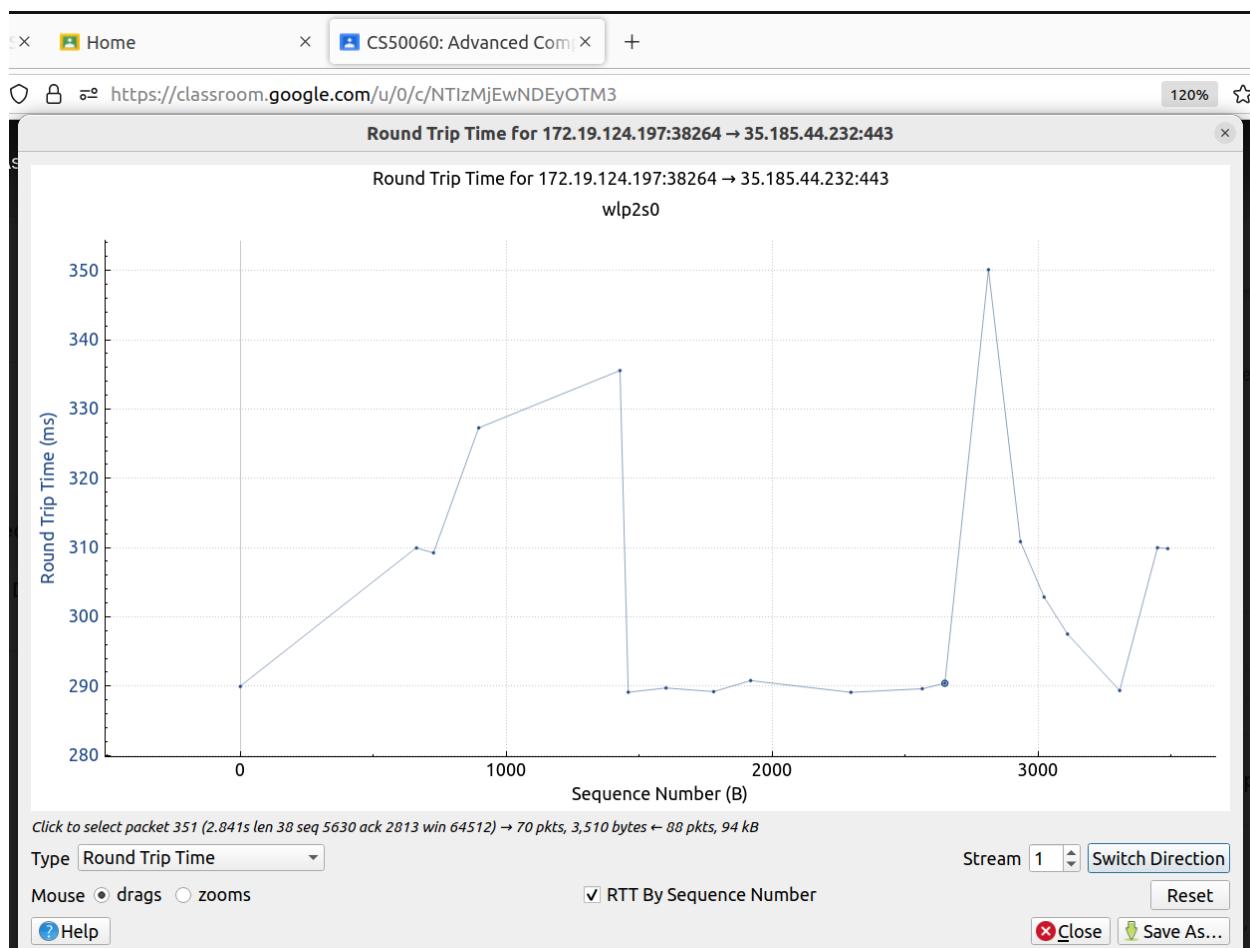
Packets: 580 · Displayed: 158 (27.2%) · Marked: 4 (0.7%) · Dropped: 0 (0.0%) · Profile: Wireless Masterclass

**Minimum window size advertised in the 5 segments is
Window size : 64128 Bytes**

**Q9)Minimum window size advertised by the client
Window size : 64369 Bytes**

Q10)No, there is no retransmission of the packets

We can verify them via the graph



Q11)

- Receiver has acknowledged all the data in the first 10 segments since here we are sending GET requests.

Q 12)

[Reassembled PDU length: 16393]

Arrival Time: Oct 16, 2023 18:06:38.223798592 IST

- Arrival Time: Oct 16, 2023 18:06:38.223781433 IST

0.223798592 - 0.223781433

0.000017159 ms

Throughput = data sent/ time taken

16393 B/ 0.000017159 ms