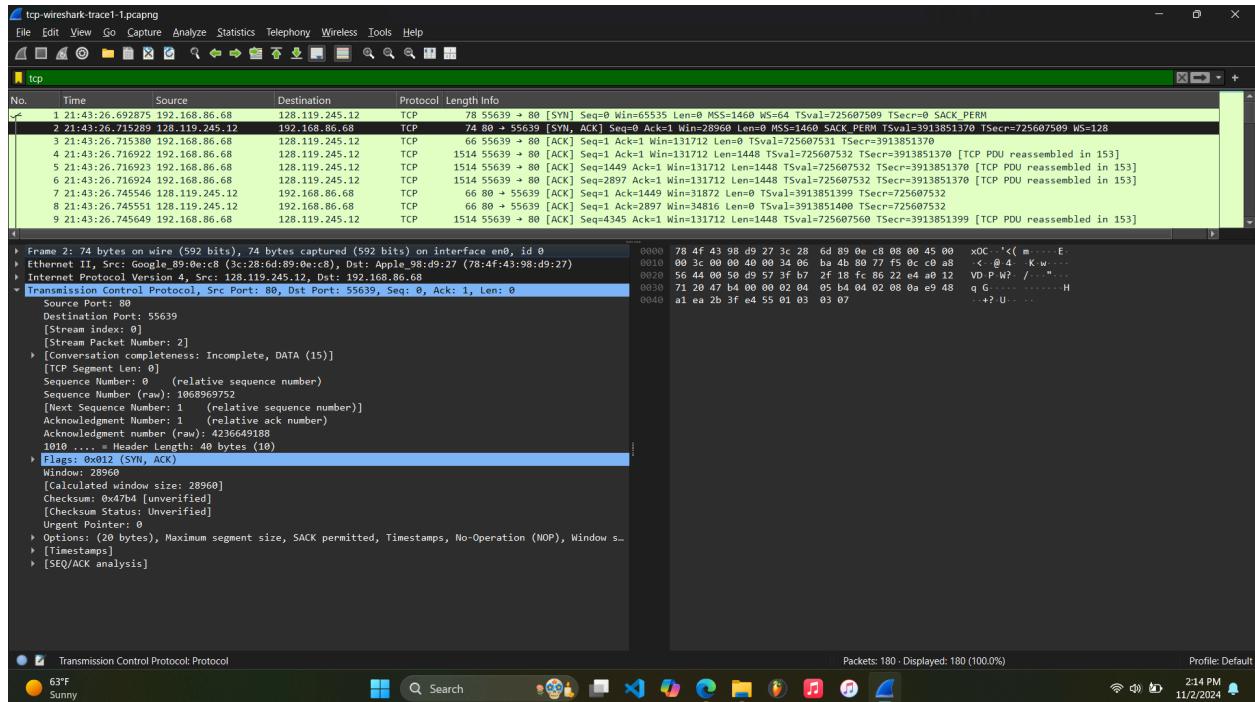
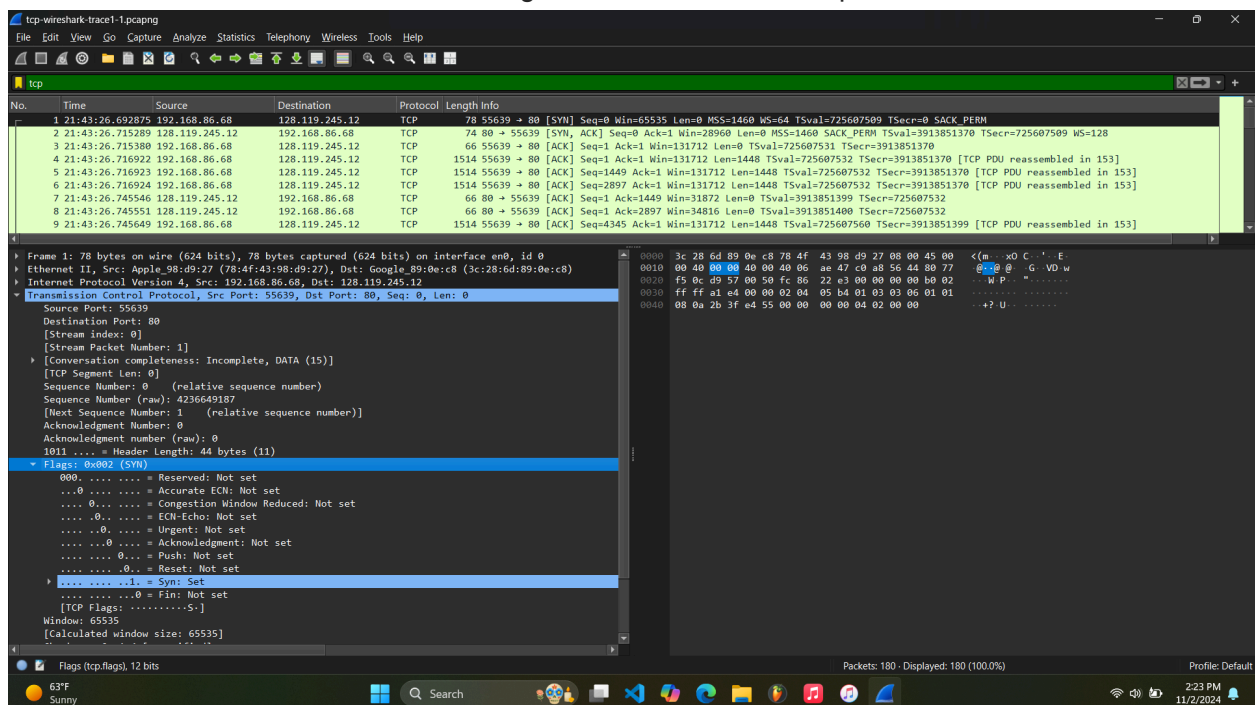


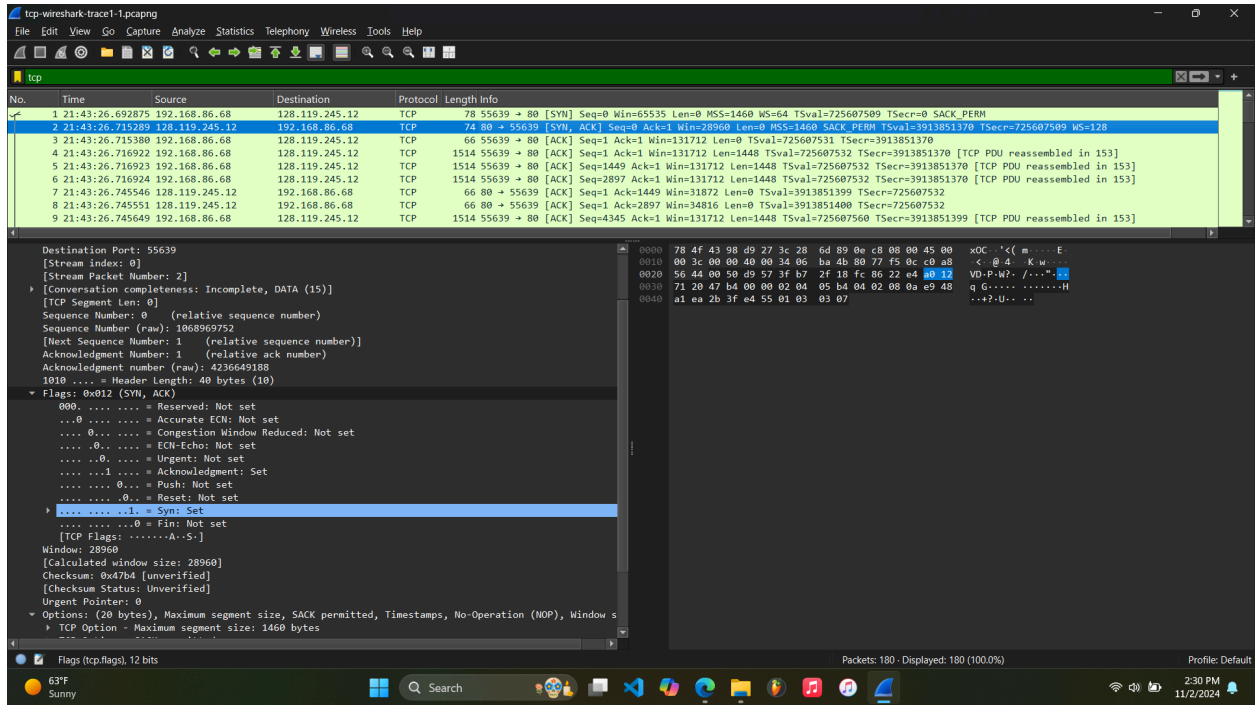
1. Source Address: 192.168.86.68 Source Port: 55639
2. IP address: 128.119.245.12 TCP port number: 80



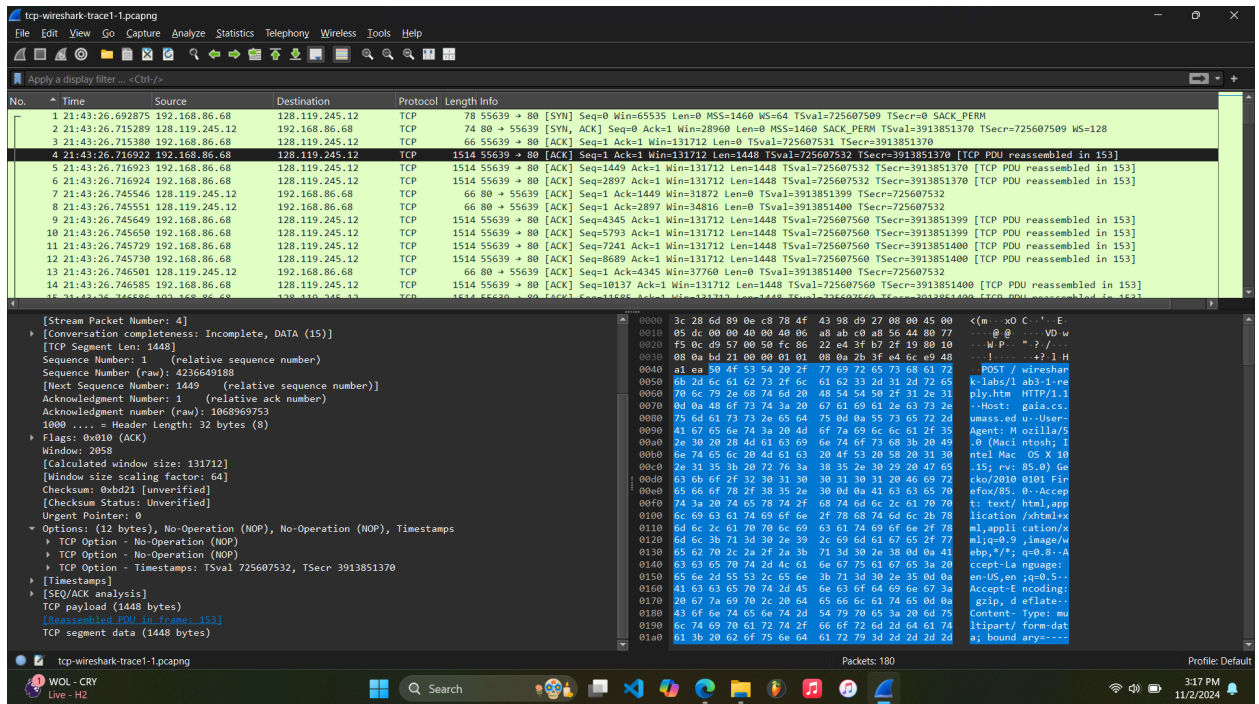
3. The sequence number is 0. This identifies it as a SYN segment because the SYN flag is set to 1. It can use selective acknowledgement because SACK is permitted.



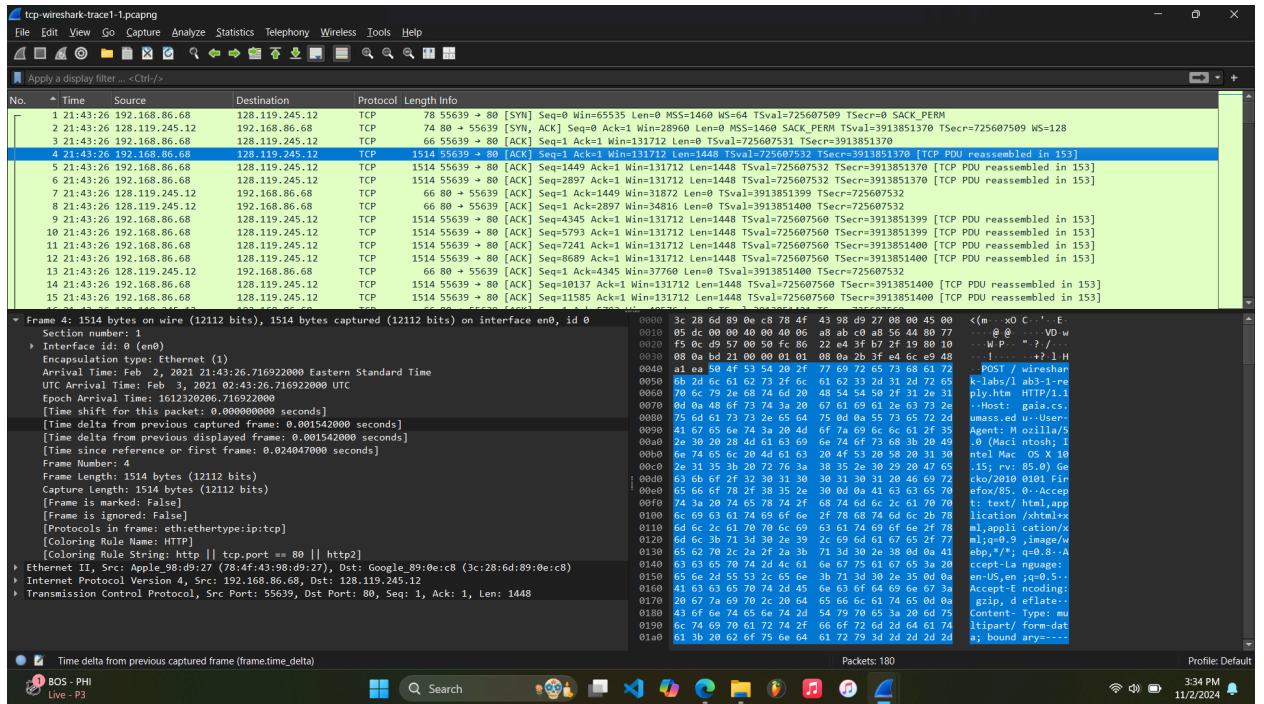
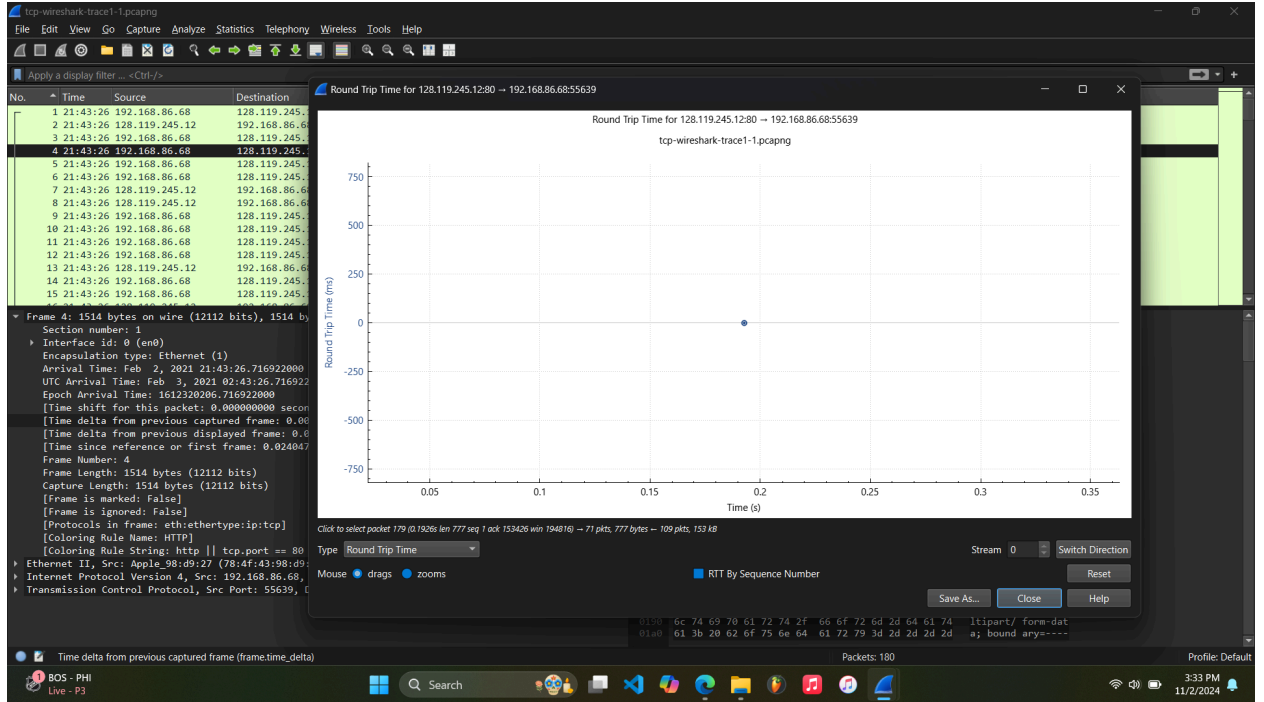
4. The SYNACK value has a value of 0. The value of the ACKnowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by adding 1 to the initial sequence number of the SYN segment from the client computer. The SYN flag and Acknowledgement flag in the segment are set to 1 which indicates that this is a SYNACK segment.

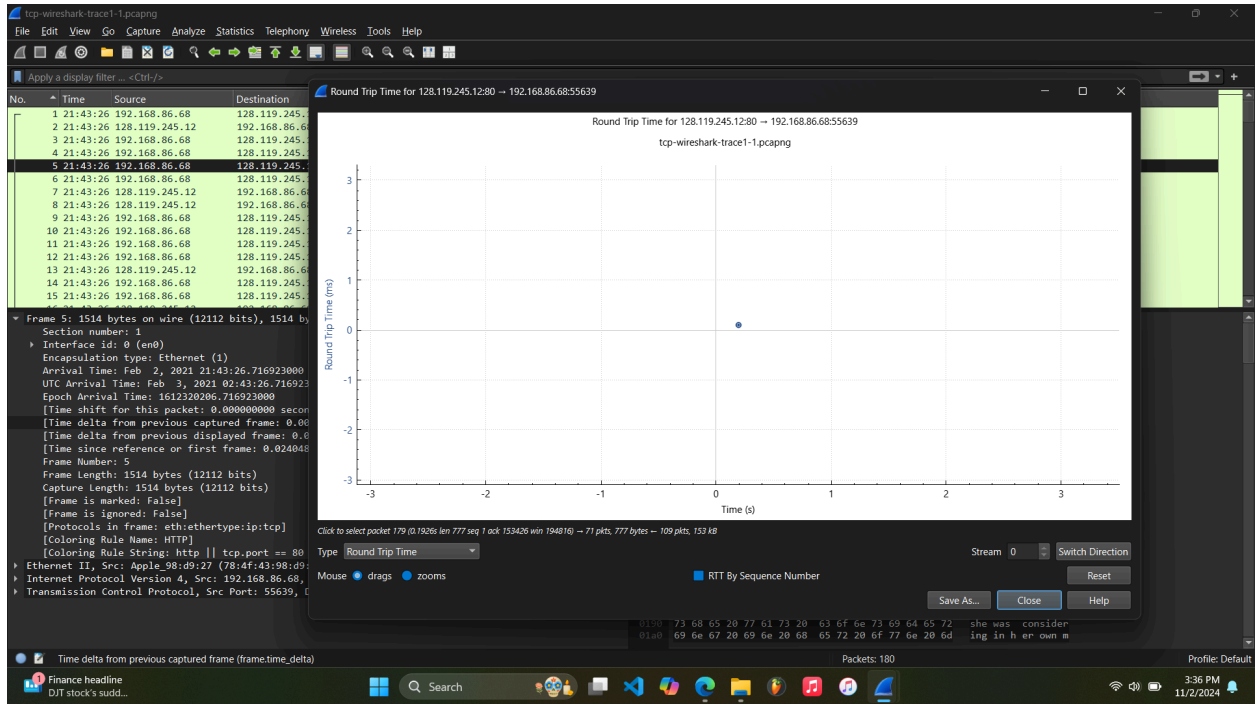


5. The sequence number is 1 (raw sequence number is 4236649188. TCP payload is 1448 bytes. It was done in multiple segments.

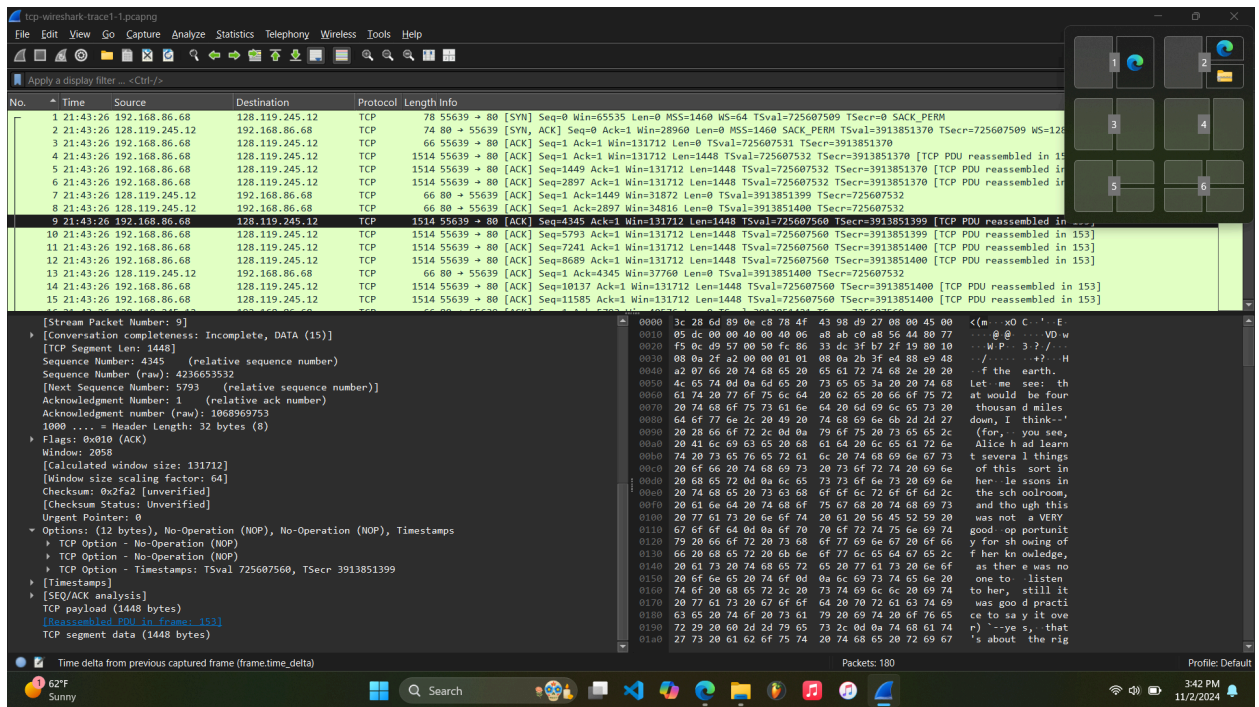


- The one that contained the post arrived at Feb 2, 2021 21:43:26.716922000 Eastern Standard Time and was sent at Arrival Time: Feb 2, 2021 21:43:26.715289000 Eastern Standard Time. The RTT for the first data-containing segment is .19 seconds. The time for the second is .2 seconds.



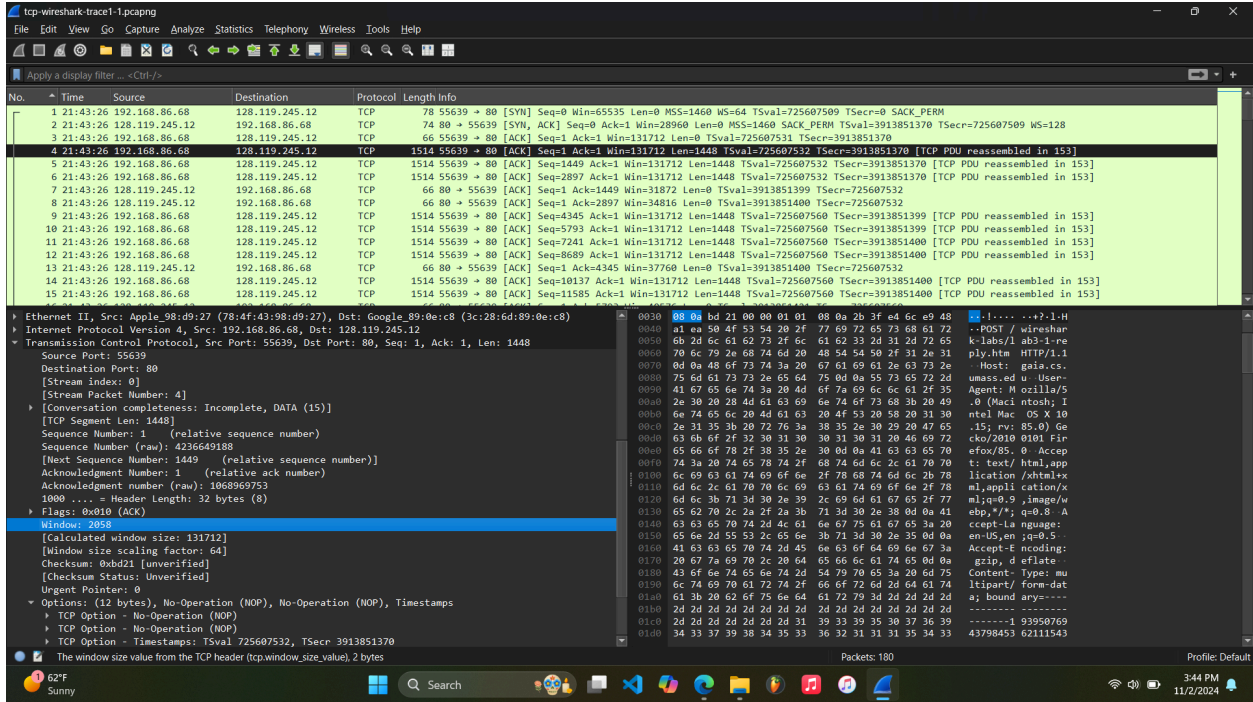


7. The length of each of the first four data carrying packets are  $1448 + 1448 = 2896$

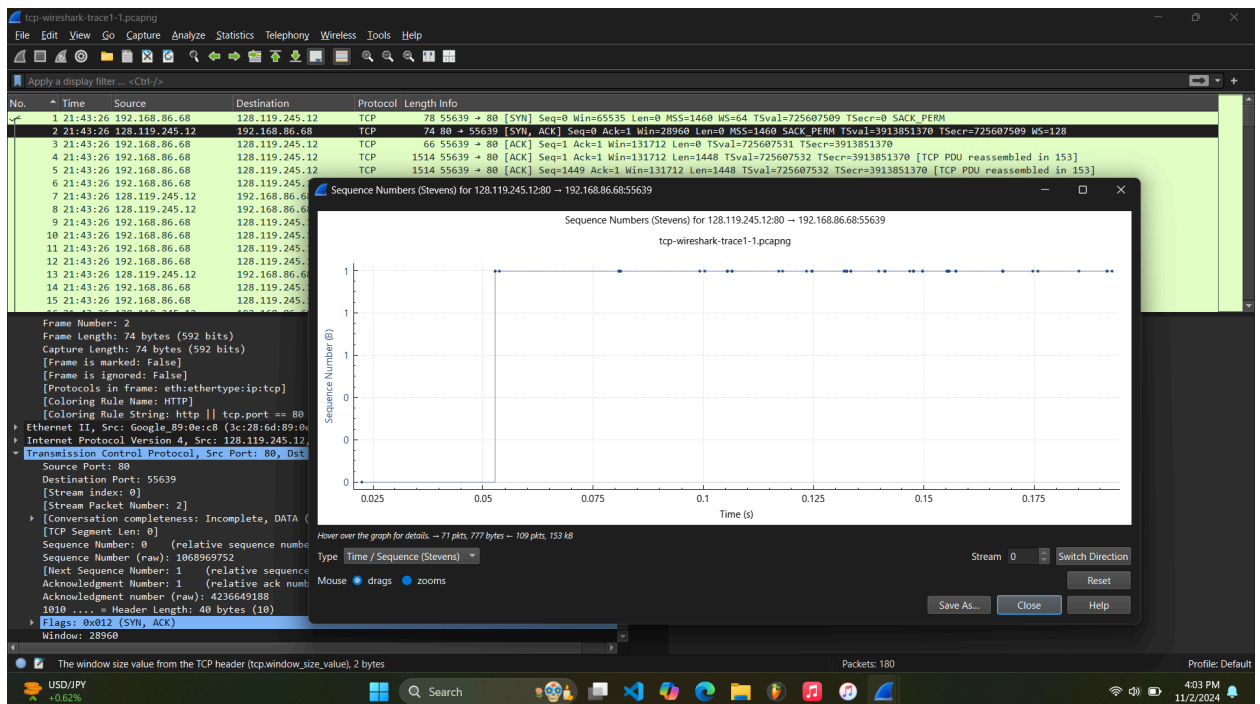


8. The minimum buffer space is showed in the tcp window 2048 and no it doesn't throttle





9. There are no retransmitted files because the sequence number graph didnt have any downward trends.



From 10 and down I use a different packet capture file

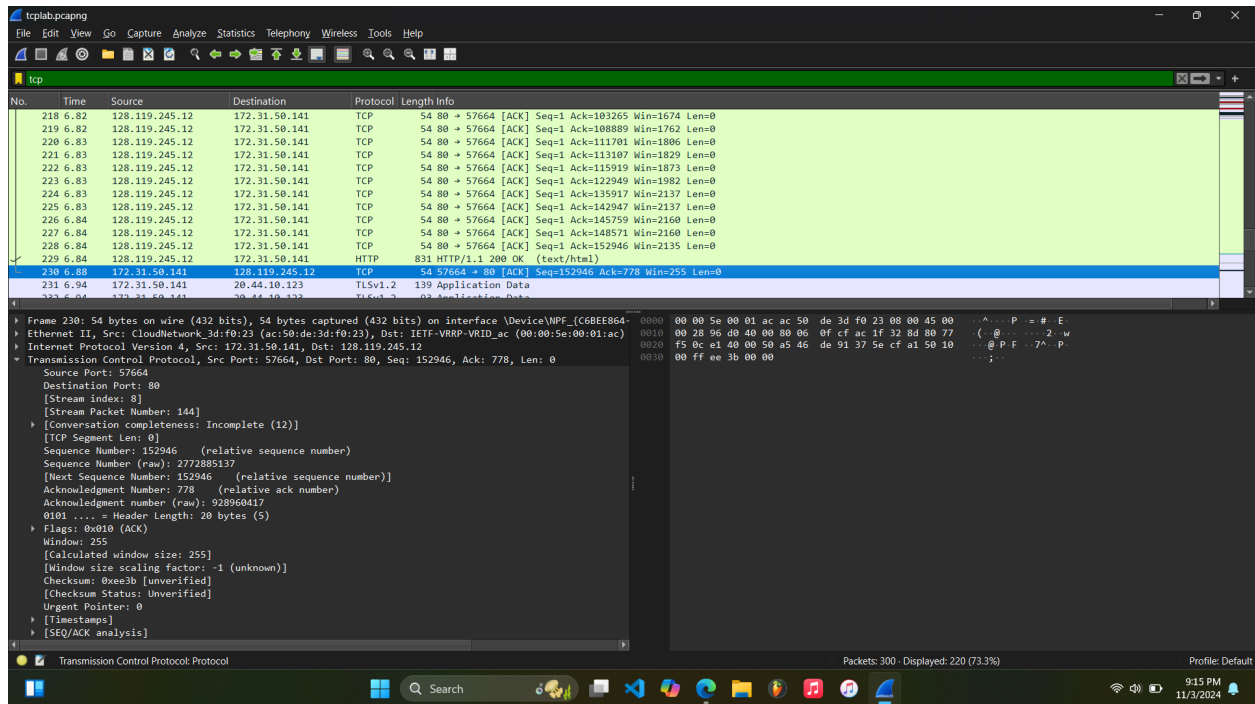
10. The receiver is typically ACKing 432 bits of data. There are cases where a receiver ACKs every other received segment. This can be seen when this is two ACKs in a row

The image shows a Wireshark packet capture of a TCP connection. The packet list pane displays several packets, with packet 98 highlighted. The packet details pane shows the structure of frame 98, which is a TCP segment with a length of 54 bytes (432 bits). The segment is an ACK with sequence number 1 and acknowledgment number 7657. The packet bytes pane shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
93	6.70	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=7657 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
94	6.70	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=9063 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
95	6.70	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=10469 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
96	6.70	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=11875 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
97	6.73	128.119.245.12	172.31.50.141	TCP	54	80 → 57664 [ACK] Seq=1 Ack=527 Win=238 Len=0
98	6.73	128.119.245.12	172.31.50.141	TCP	54	80 → 57664 [ACK] Seq=1 Ack=7657 Win=348 Len=0
99	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=13281 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
100	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=14687 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
101	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [PSH, ACK] Seq=16093 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
102	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=17499 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
103	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=18905 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
104	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=20311 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
105	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=21717 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]
106	6.73	172.31.50.141	128.119.245.12	TCP	1460	57664 → 80 [ACK] Seq=23123 Ack=1 Win=258 Len=1406 [TCP PDU reassembled in 213]

Frame 98: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{C6BEE864-465C-473B-B1D7-32B3AB273C5D} [eth 0]  
 Section number: 1  
 Encapsulation type: Ethernet (1)  
 Interface id: 0 (\Device\NPF\_{C6BEE864-465C-473B-B1D7-32B3AB273C5D})  
 Arrival Time: Nov 2, 2024 19:16:09.726282000 Eastern Daylight Time  
 UTC Arrival Time: Nov 2, 2024 23:16:09.726282000 UTC  
 Epoch Arrival Time: 1739589369.726282000  
 [Time shift for this packet: 0.000000000 seconds]  
 [Time delta from previous captured frame: 0.000000000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 6.735624000 seconds]  
 Frame Number: 98  
 Frame Length: 54 bytes (432 bits)  
 Capture Length: 54 bytes (432 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:tcp]  
 [Coloring Rule Name: HTTP]  
 [Coloring Rule String: http || tcp.port == 80 || http2]  
 Ethernet II, Src: Cisco-Cat6e7 (38:00:56:c0:ac:e7), Dst: CloudNetwork\_3d:f0:23 (ac:50:de:3d:f0:23)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.31.50.141  
 Transmission Control Protocol, Src Port: 80, Dst Port: 57664, Seq: 1, Ack: 7657, Len: 0

11. To calculate the throughput I calculated the total amount of data sent over the period of the connection. First the difference between the first sequence number and the last ACK number.  $152946 - 1 = 152945$ . Then the total time transfer between the first message and the last ack.  $6.88 \text{ s} - 6.69$ . So  $152946 \text{ bytes} / 6.88 \text{ seconds} = 22231 \text{ bytes per second}$



12. I would say it's to avoid congestion avoidance.

13. I can say that the period is showing a consistent pattern so it suggests a periodic sending behavior from the client.

