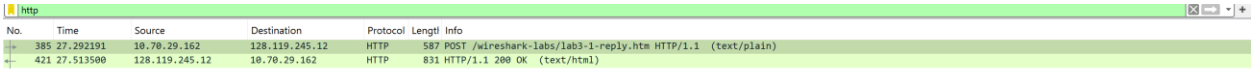
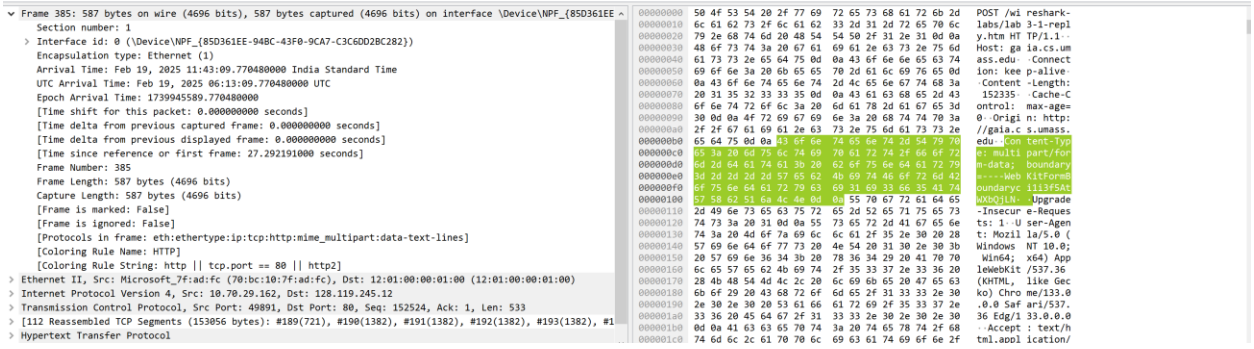
Wireshark CN: Lab 4

Submitted By: Stuti Garg (SE22UCSE263)

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".

- IP address is 10.70.29.162 and TCP port number is 49891 that is being used by the client computer that is transferring the file to gaia.cs.umass.edu.





2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? If you have been able to create your own trace, answer the following question:

- The IP address of gaia.cs.umass.edu is 10.70.29.162.
- It is sending on source port- 49891 and receiving TCP segments for this connection at destination port- 80.

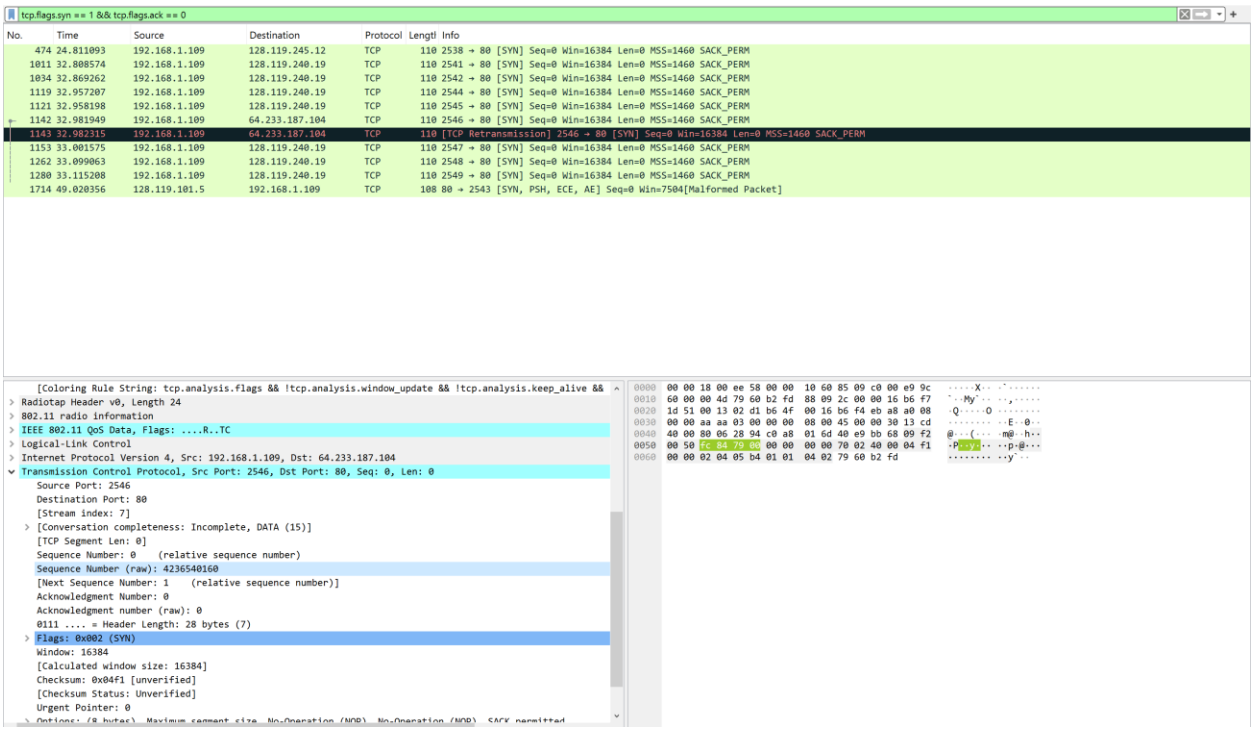
- ```
  Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
      Source Port: 49891
      Destination Port: 80
      [Stream index: 9]
    > [Conversation completeness: Incomplete (30)]
      [TCP Segment Len: 533]
      Sequence Number: 152524    (relative sequence number)
      Sequence Number (raw): 3887976164
      [Next Sequence Number: 153057    (relative sequence number)]
      Acknowledgment Number: 1    (relative ack number)
      Acknowledgment number (raw): 1459396136
      0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
      Window: 512
      [Calculated window size: 512]
      [Window size scaling factor: -1 (unknown)]
      Checksum: 0x78c9 [unverified]
  ```

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

- The IP address is 128.119.245.12.
- The TCP port number used by the client computer to transfer the file to gaia.cs.umass.edu is 49891.
  - ```
    Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
        Source Port: 49891
        Destination Port: 80
        [Stream index: 9]
      > [Conversation completeness: Incomplete (30)]
        [TCP Segment Len: 533]
        Sequence Number: 152524    (relative sequence number)
        Sequence Number (raw): 3887976164
        [Next Sequence Number: 153057    (relative sequence number)]
        Acknowledgment Number: 1    (relative ack number)
        Acknowledgment number (raw): 1459396136
        0101 .... = Header Length: 20 bytes (5)
      v Flags: 0x018 (PSH, ACK)
          000. .... .... = Reserved: Not set
          ...0 .... .... = Accurate ECN: Not set
          .... 0... .... = Congestion Window Reduced: Not set
          .... .0.. .... = ECN-Echo: Not set
    ```

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

- The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 4236540160.



- The segment identified as SYN is set to 1 under the flags section.

```
Sequence Number (raw): 4236540160
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Accurate ECN: Not set
   .... 0... .... = Congestion Window Reduced: 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: 16384
[Calculated window size: 16384]
Checksum: 0x04f1 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
```

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

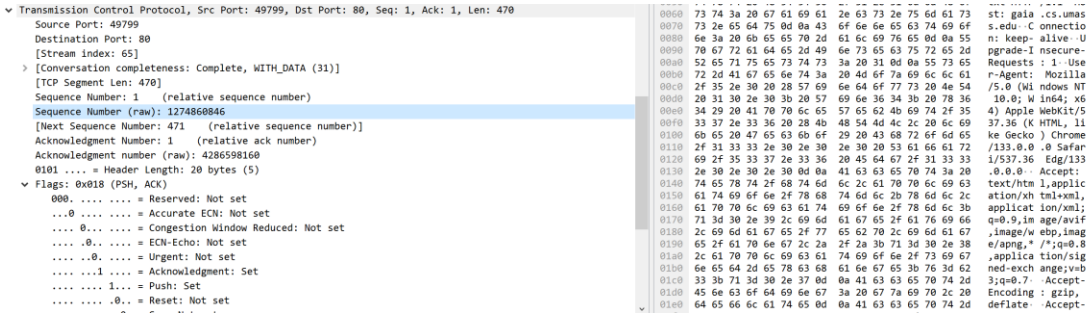
- The sequence number of the SYNACK segment sent by the gaia.cs.umass.edu to the client computer in reply to the SYN is 3887976164.
- The value of the Acknowledgement field in the SYNACK segment is (client's initial sequence number + 1) that is1459396136.
- gaia.cs.umass.edu determines the ACK number in the SYN-ACK by taking the client's Initial Sequence Number (ISN) + 1, acknowledging the next expected byte. This follows TCP's rule that a SYN flag consumes one sequence number.
- The segment that identifies it is under the Transmission Control Protocol section.

```
Transmission Control Protocol, Src Port: 49891, Dst Port: 80, Seq: 152524, Ack: 1, Len: 533
    Source Port: 49891
    Destination Port: 80
    [Stream index: 9]
  > [Conversation completeness: Incomplete (30)]
    [TCP Segment Len: 533]
    Sequence Number: 152524    (relative sequence number)
    Sequence Number (raw): 3887976164
    [Next Sequence Number: 153057    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1459396136
    0101 .... = Header Length: 20 bytes (5)
```

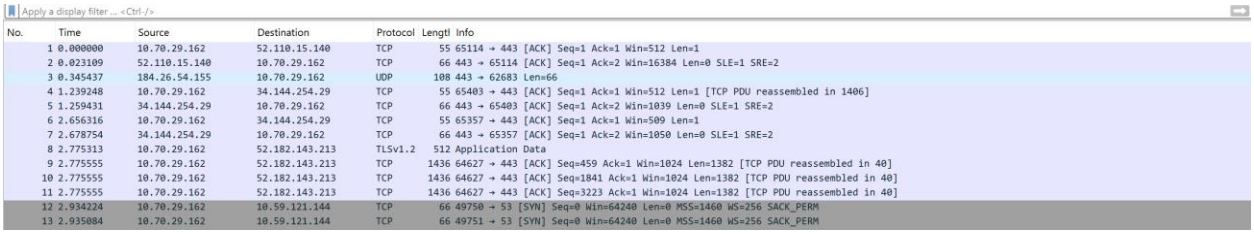
- The SYN and ACK flags must be set to 1.

```
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 691643676
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 2313716653
0111 .... = Header Length: 28 bytes (7)
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A··S·]
Window: 5840
[Calculated window size: 5840]
Checksum: 0x5372 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > TCP Option - Maximum segment size: 1460 bytes
```

6. 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.

- The sequence number of the TCP segment containing the HTTP POST command is 1274860846.
- 

7. 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 RTT value for each of the six segments? What is the EstimatedRTT value after the receipt of each ACK?

- The sequence numbers of the first six segments in the TCP connection are- 1, 459, 1841, 3223, 64240, 65535.
- The segment times for the first six sequence numbers- 1, 459, 1841, 3223, 64240, 65535 are 0.023109, 2.775555, 2.775555, 2.775555, 2.934224, 2.934428 respectively.
- 

- EstimatedRTT=(1−α)×EstimatedRTT+α×SampleRTT (alpha = 0.125)
- Calculations:

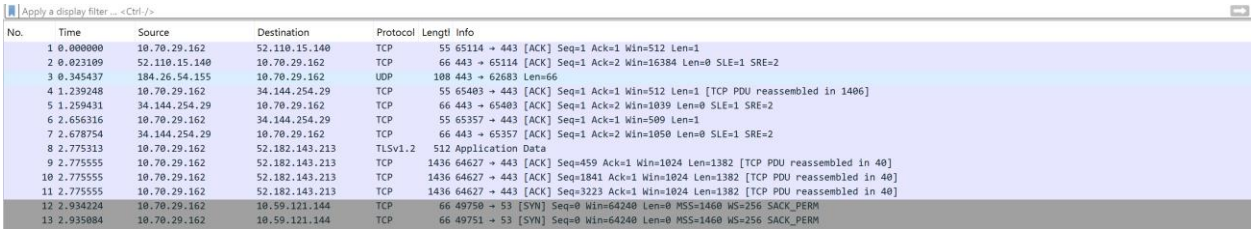
Segment	Sample RTT (ms)	Estimated RTT Calculations	Estimated RTT (ms)
1	2.752446	Initial RTT	2.752446
2	2.752446	No change	2.752446
3	2.752446	No change	2.752446
4	0.158669	(0.875 × 2.752446) + (0.125 × 0.158669)	2.4229

5	0.000204	(0.875 × 2.4229) + (0.125 × 0.000204)	2.1190

Estimated RTT after each segment:

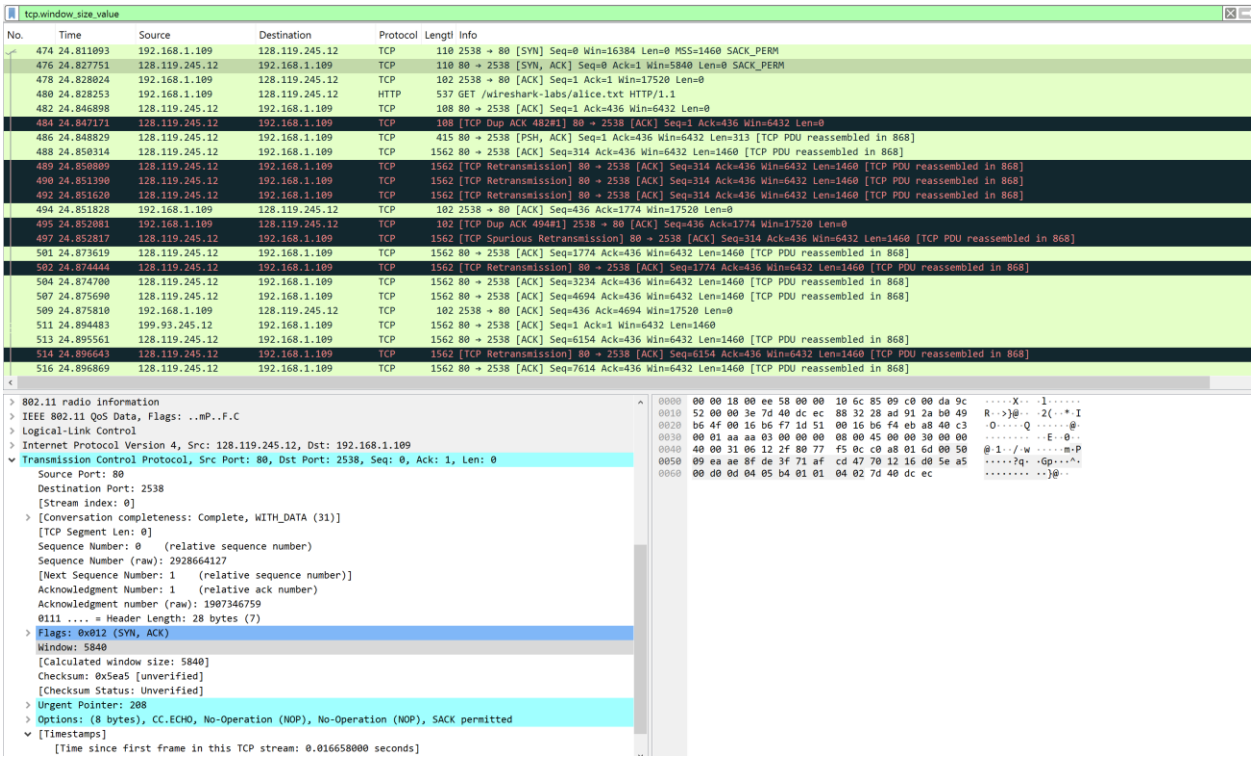
- After 1st segment: 2.752 ms
- After 4th segment: 2.422 ms
- After 5th segment: 2.119 ms

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

- Length of segment 1: 66
- Length of segment 2:1436
- Length of segment 3: 1436
- Length of segment 4: 1436
- Length of segment 5: 66
- Length of segment 6: 2186
- 

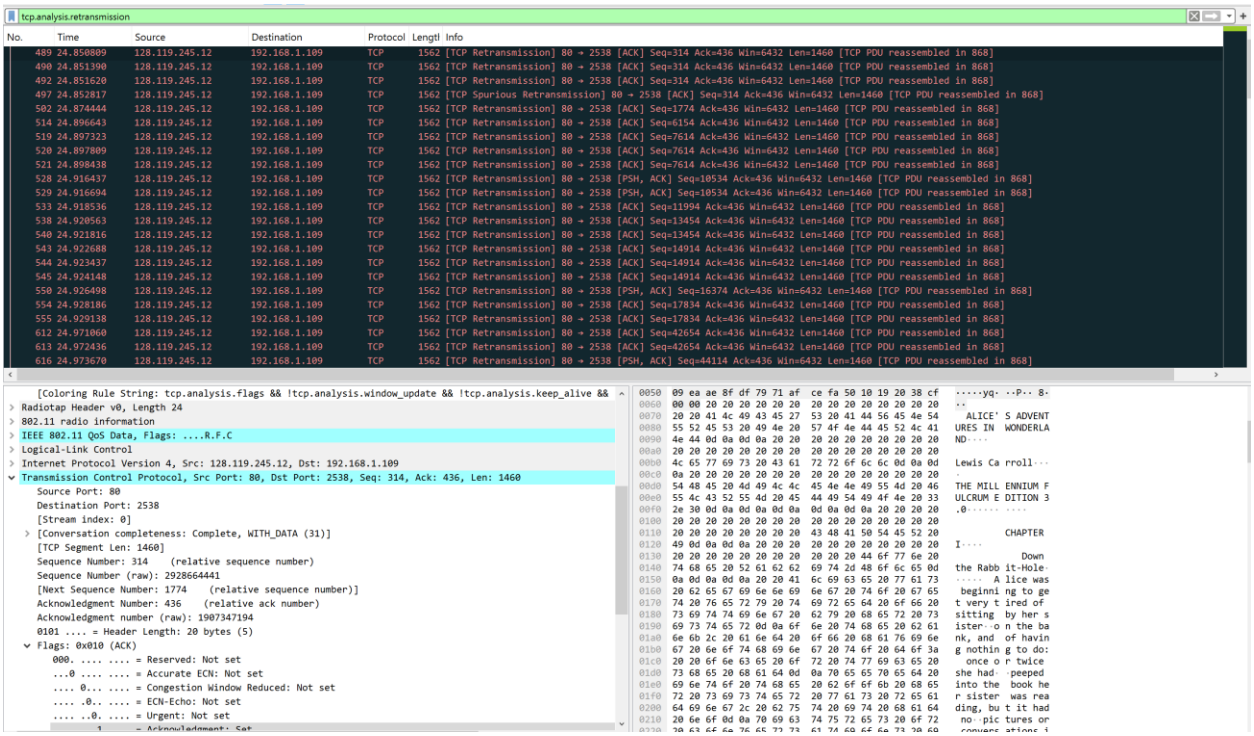
9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

- The minimum amount of available buffer space advertised at the received for the entire trace is 5840 bytes
- Yes, due to the lack of receiver buffer space, sender was throttled.
- The presence of Zero Window packets indicates that the receiver's buffer space was exhausted, forcing the sender to pause data transmission.
- This behavior helps prevent packet loss and congestion but can also lead to temporary delays in data transfer.
- .

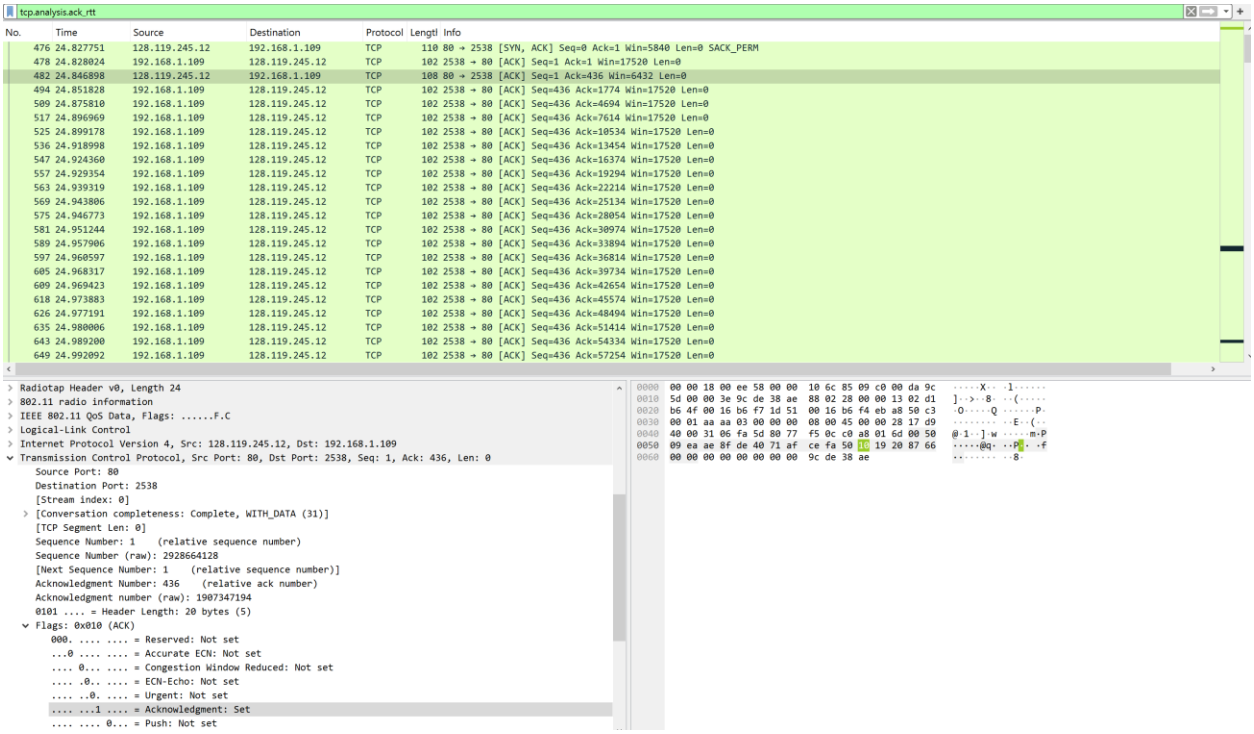


10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

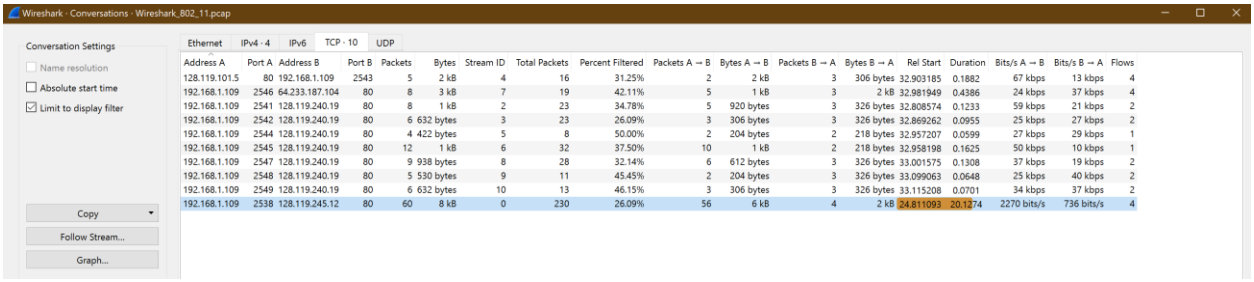
- Yes, there are retransmitted segments in the trace file as given in the screenshot below.
- Used filter tcp.analysis.retransmission to find re-transmitted packets.
- I also checked for duplicate sequence numbers, Higher-than-normal RTT values and TCP Fast Retransmission events.

- 

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

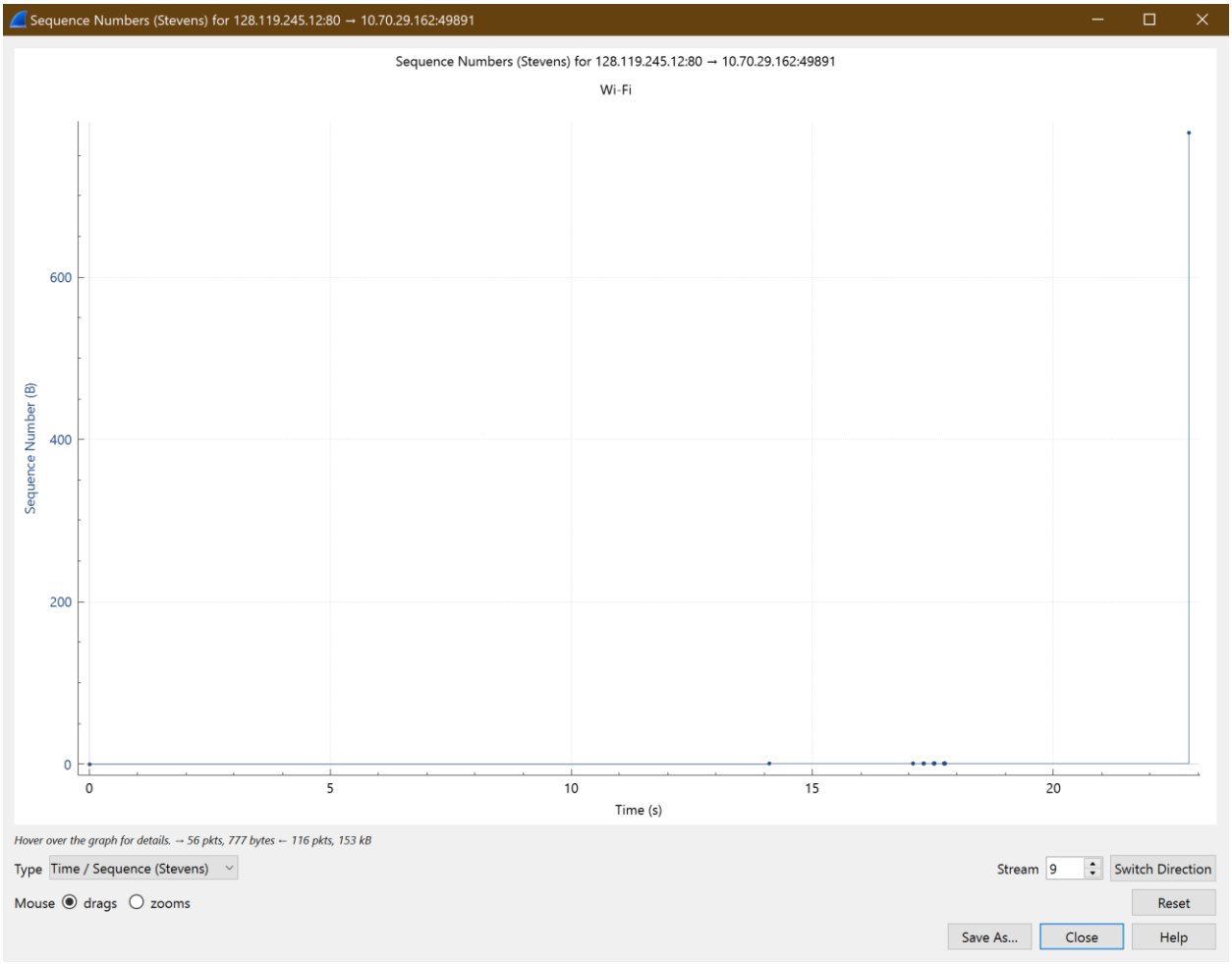
- The receiver acknowledges 1460 bytes of data.
- Yes, but some cases existed where the receiver ACKs every two segments (2920 bytes).
- Also, the raw acknowledgement number received is 1907347194.
- 

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

- Throughput measures how much data is transferred per unit time in a TCP connection. It is calculated using the total bytes sent and the duration of the transfer.
- I opened Wireshark and went to Statistics -Conversations - TCP Tab to find the Total Bytes Transferred. I noted the timestamp of the first and last packet to calculate the Total Time Taken by subtracting the first timestamp from the last.
- I used the formula Throughput = Total Bytes Transferred / Total Time Taken to determine the throughput in bytes per second (Bps).
- When it was needed, I converted Bps to bps by multiplying by 8.
- Total Bytes Transferred: 180154.
- Total Time Taken: 21.4611
- Therefore: Throughput is 8394.4439 bytes/sec
- 

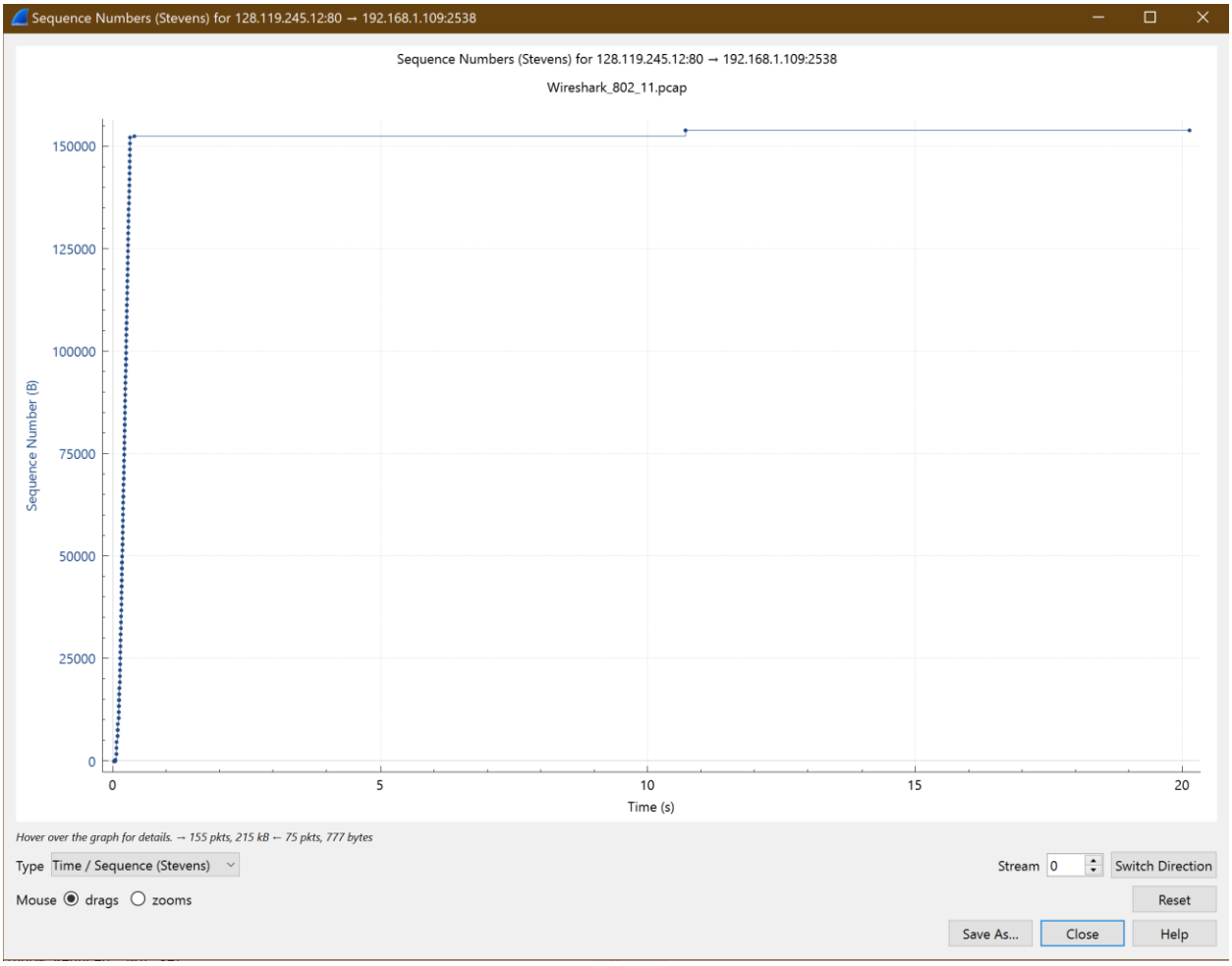
13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

- In the Time-Sequence Graph (Stevens), I observed a slow increase in the sequence number initially, indicating the congestion avoidance phase, where TCP increases the congestion window linearly. TCP's slow start begins at time t = 14 seconds and ends at t = 25 seconds.
- At time = 25s, there was a sudden rise, suggesting a possible transition to fast recovery or a retransmission event, where TCP injected more data into the network after detecting lost or delayed packets.
- This behavior differs from the ideal TCP model, where slow start should show exponential growth until reaching a threshold. In my trace, the linear growth before the sudden rise suggests that external factors like network conditions, RTT variations, or delayed ACKs influenced TCP's behavior.
-

- 

14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

- In my trace, I observed a sudden exponential growth in the sequence number vs. time plot, which indicates the TCP slow start phase.
- Compared to the ideal TCP model, my measured data showed some variations in growth due to network delay, packet loss, or varying RTTs, which are not always accounted for in theoretical models.


Sequence Numbers (Stevens) for 128.119.245.12:80 → 192.168.1.109:2538
Sequence Numbers (Stevens) for 128.119.245.12:80 → 192.168.1.109:2538
Wireshark_802_11.pcap
Sequence Number (B)
150000
125000
100000
75000
50000
25000
0
0
5
10
15
20
Time (s)
Hover over the graph for details. → 155 pkts, 215 kB ← 75 pkts, 777 bytes
Type
Time / Sequence (Stevens)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help