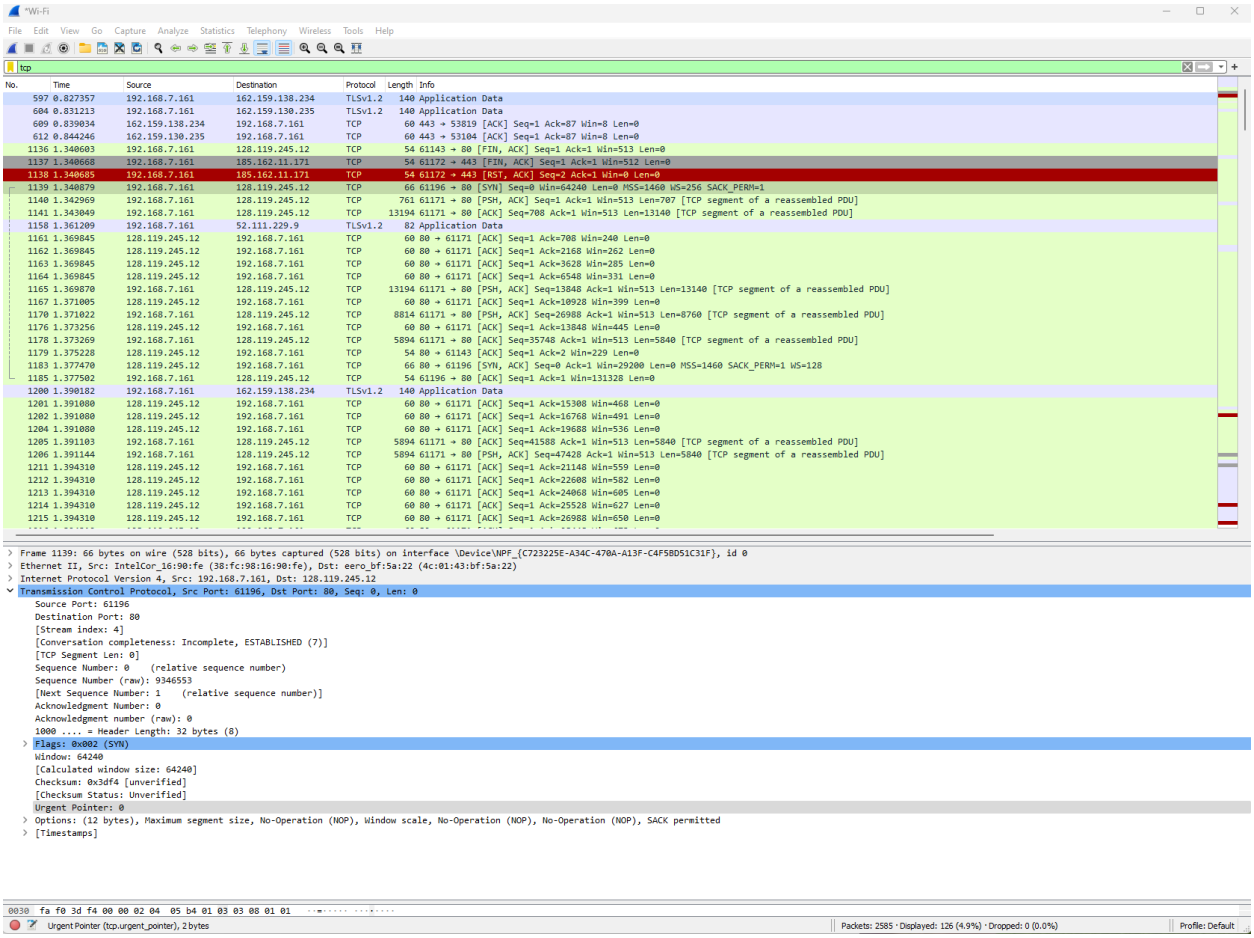
Betim Sejdiu

CS 446 UMB Fall 2022

Bo Sheng



1. The IP Address 192.168.7.161 and the port number is 61196

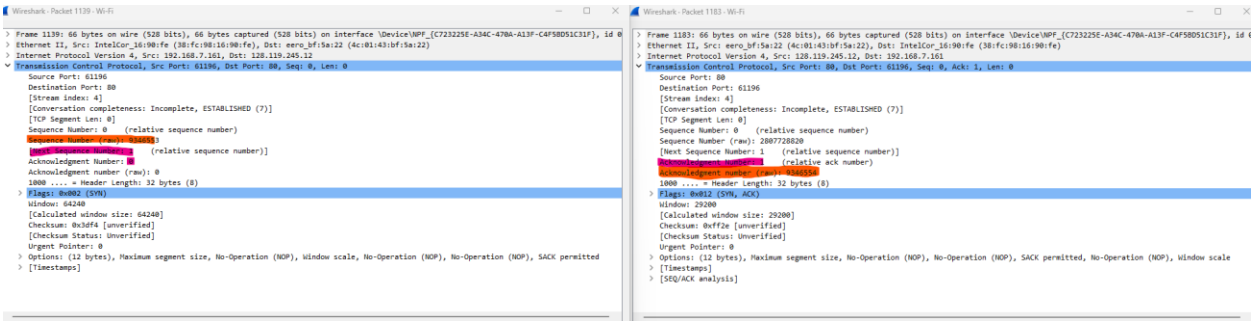
```
> Frame 1139: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{C723225E-A34C-470A-A13F-C4F5BD51C31F}, id 0
> Ethernet II, Src: IntelCor_16:90:fe (38:fc:98:16:90:fe), Dst: eero_bf:5a:22 (4c:01:43:bf:5a:22)
> Internet Protocol Version 4, Src: 192.168.7.161, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61196, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61196
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 9346553
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x3df4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

2. The Sequence number is 9346553

```
> Frame 1139: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{C723225E-A34C-470A-A13F-C4F5BD51C31F}, id 0
> Ethernet II, Src: IntelCor_16:90:fe (38:fc:98:16:90:fe), Dst: eero_bf:5a:22 (4c:01:43:bf:5a:22)
> Internet Protocol Version 4, Src: 192.168.7.161, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61196, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61196
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 9346553
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x3df4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

The flag of the packet signifies that it is SYN

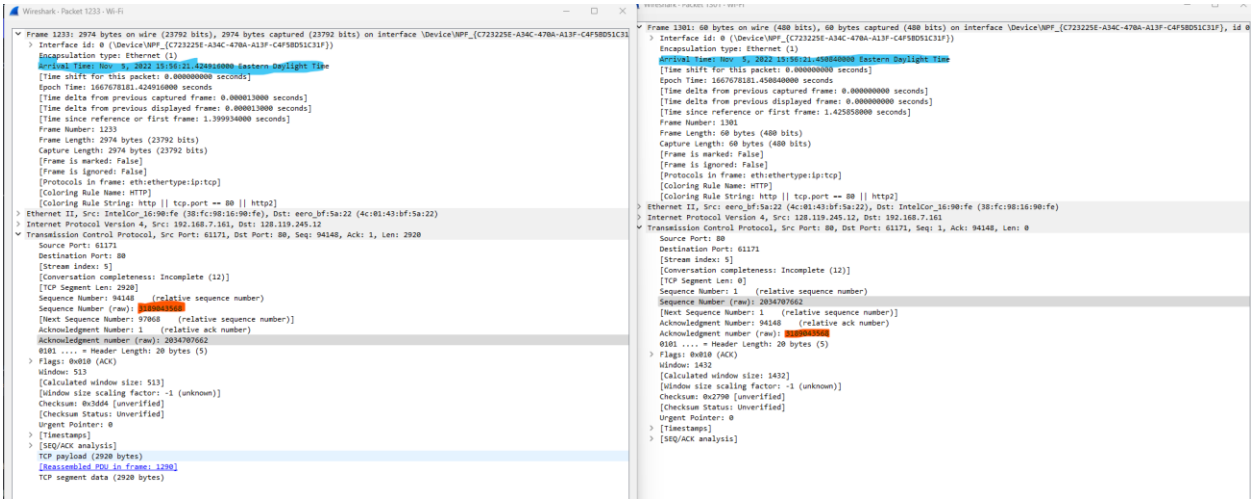
3. The Sequence number SYNACK is 2807728820. The value of the Acknowledgement field in SYNACK segment is 9346554. Gaia determined this value by incrementing the SYN Sequence number. We have an acknowledgement number of 1 in this SYNACK. This should mean that it successfully acknowledged the SYN argument.



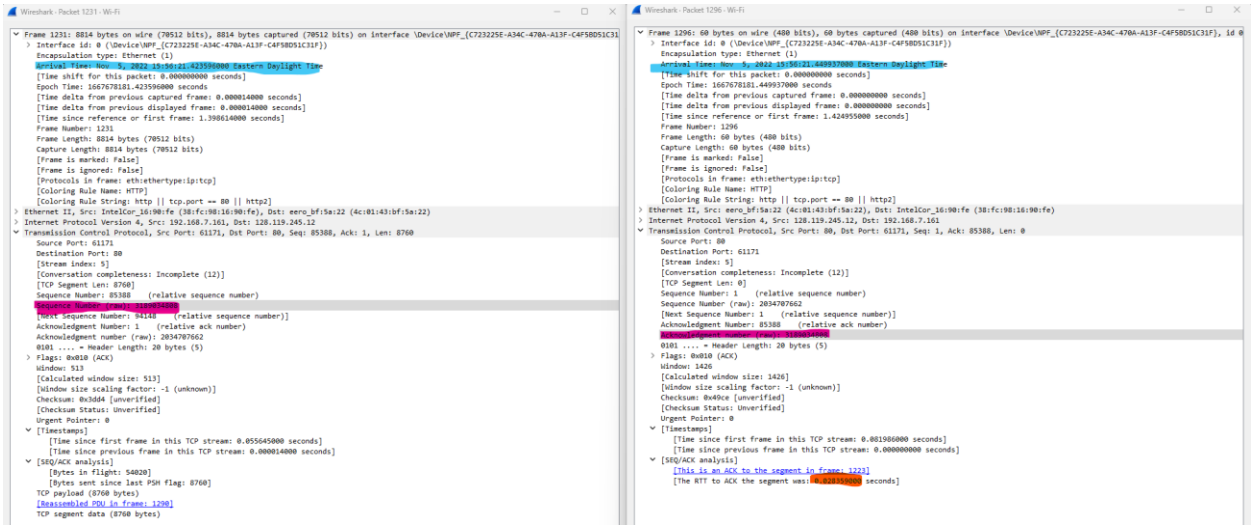
4. The Sequence number of the HTTP protocol is 2034707662

```
> Frame 1345: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{C723225E-A34C-470A-A13F-C4F5BD51C31F},
> Ethernet II, Src: eero_bf:5a:22 (4c:01:43:bf:5a:22), Dst: IntelCor_16:90:fe (38:fc:98:16:90:fe)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.7.161
v Transmission Control Protocol, Src Port: 80, Dst Port: 61171, Seq: 1, Ack: 153029, Len: 777
    Source Port: 80
    Destination Port: 61171
    [Stream index: 5]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 777]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2034707662
    [Next Sequence Number: 778    (relative sequence number)]
    Acknowledgment Number: 153029    (relative ack number)
    Acknowledgment number (raw): 3189102449
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1485
    [Calculated window size: 1485]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9a93 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (777 bytes)
> Hypertext Transfer Protocol
> Line-based text data: text/html (11 lines)
```

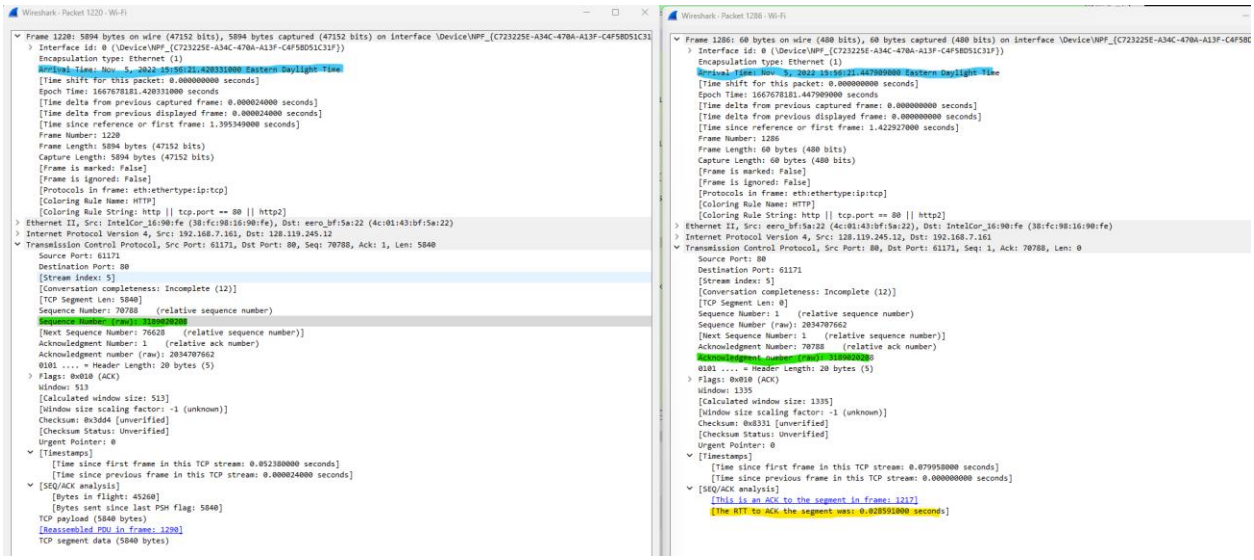
5.



This TCP data segment was received at 15:56:21.424916000. The TCP ACK was received at 15:56:21.450840000. The RTT value is then 0.027244000 seconds.



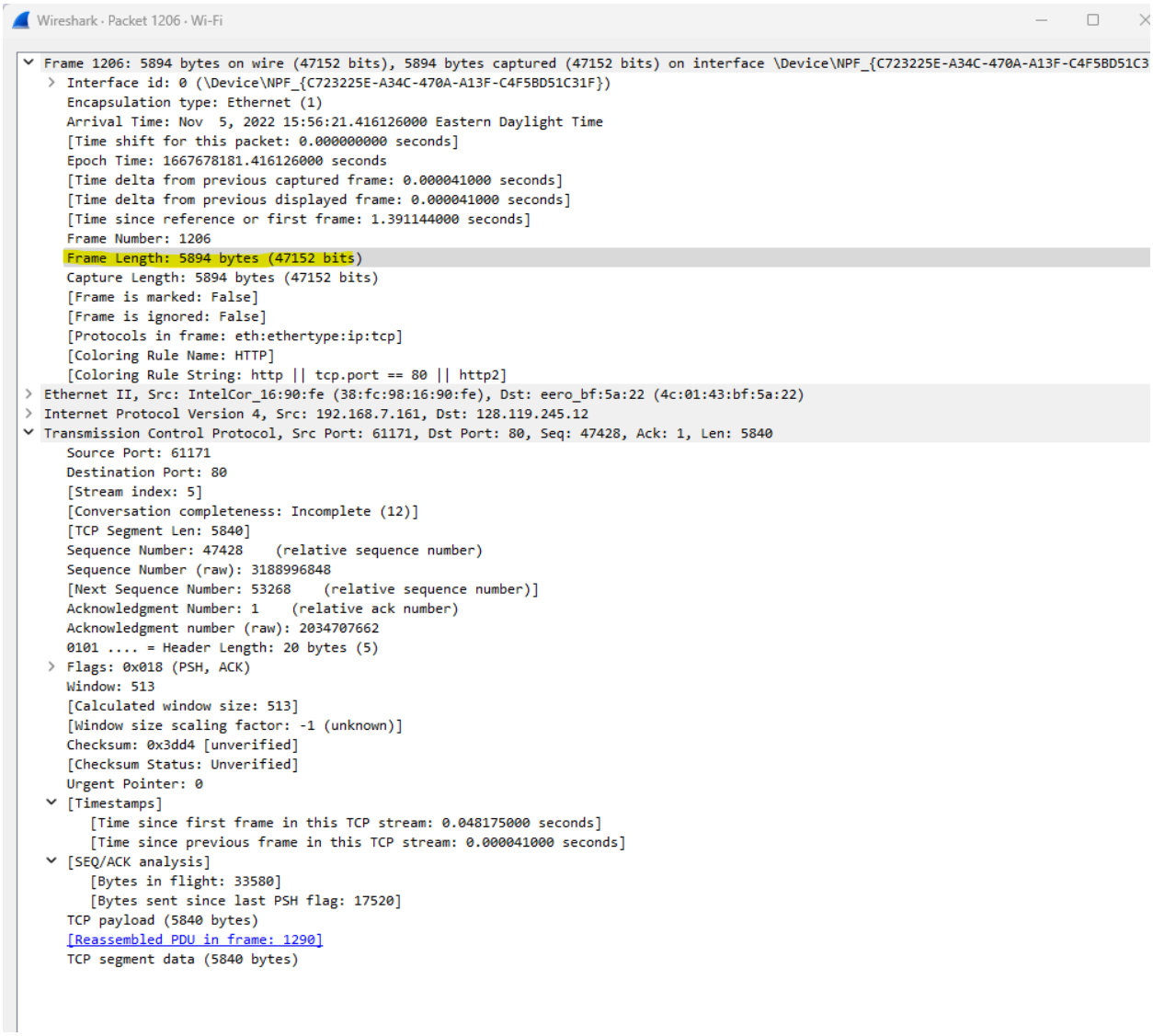
This TCP data segment was received at 15:56:21.43596000. The TCP ACK was received at 15:56:21.449937000. The RTT value is then 0.028359000 seconds.



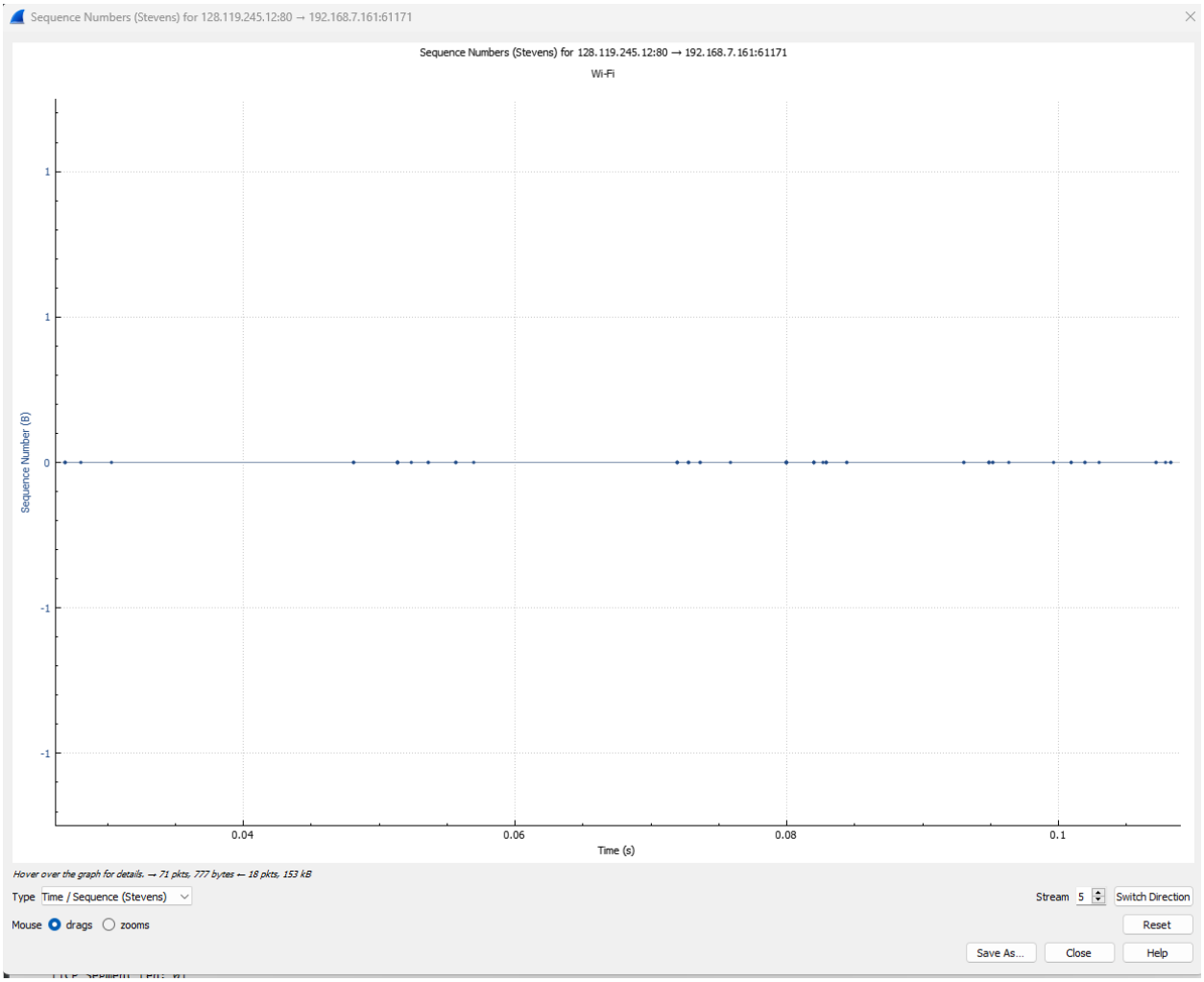
This TCP data segment was received at 15:56:21.420331000. The TCP ACK was received at 15:56:21.447909000. The RTT value is then 0.028591000seconds.

The way I determined the 3 TCP segments is that I looked for packets in which my IP was uploading data, this means it would be the source. Then I would look at the Seq number of that ACK and find where the server IP has an Ack value of the Seq number from my IP address packet.

6. The size of the available buffer space advertised at the received for the entire trace is 5894. It does not seem to throttle the sender.



7. By getting the size of the file and dividing by the time of the entire TCP connection. I obtained this from the 200OK HTTP Protocol and checked the time since first frame. That value was 0.108253000 sec. I got the size of the file through windows file explorer and that was 149,000 bytes. Doing 149,000/ 0.108253000 we get 1,376,405.272833085 bytes per second.
8. For some reason the graph that I obtained is nowhere near the one that was given as an example. I think the reason might be because of the speed of my internet and computer. For this reason, I don't see a congestion or slow phase.


Sequence Numbers (Stevens) for 128.119.245.12:80 → 192.168.7.161:61171
Sequence Numbers (Stevens) for 128.119.245.12:80 → 192.168.7.161:61171
Wi-Fi
Sequence Number (B)
1
1
0
-1
-1
0.04
0.06
0.08
0.1
Time (s)
Hover over the graph for details. → 71 pkts, 777 bytes ← 18 pkts, 153 kB
Type
Time / Sequence (Stevens)
Stream
5
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help