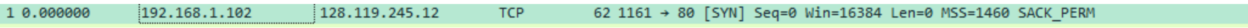
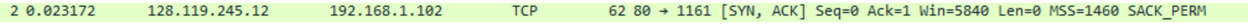
Astrid Delestine

Wireshark_TCP_v8 Lab 2

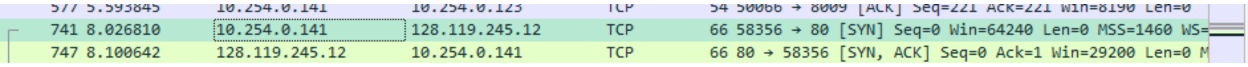
2/9/2023

1. 192.168.1.102, Port:1161
   a. 

```
1 0.000000    192.168.1.102    128.119.245.12    TCP    62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
```

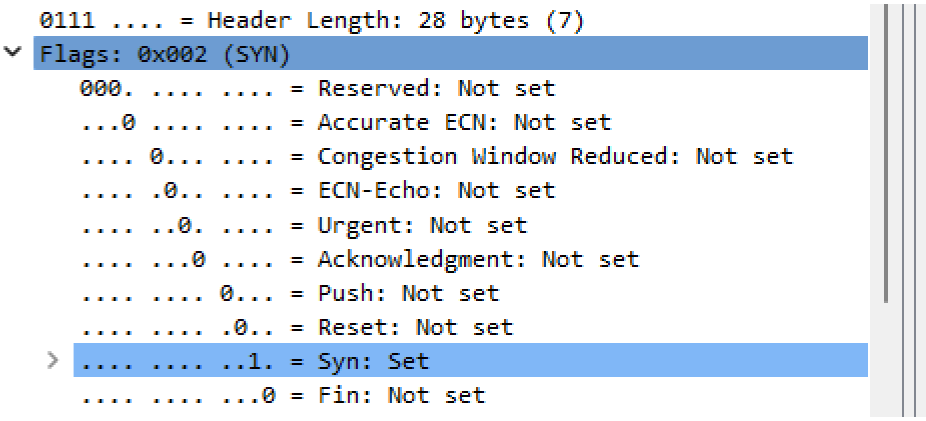
2. IP: 128.119.245.12, Port:80
   a. 

```
2 0.023172    128.119.245.12    192.168.1.102    TCP    62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
```

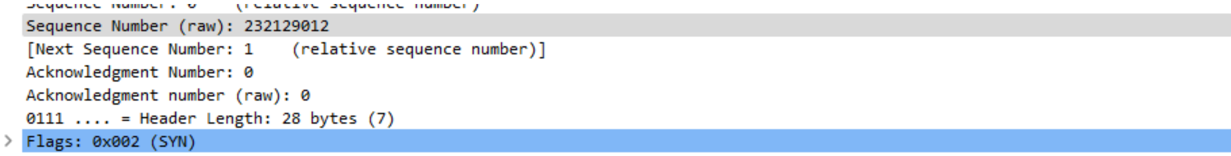
3. IP: 10.254.0.141 port:58356
   a. 

```
577 5.593845    10.254.0.141    10.254.0.123      TCP    54 50066 → 8009 [ACK] Seq=221 Ack=221 Win=8190 Len=0
741 8.026810    10.254.0.141    128.119.245.12    TCP    66 58356 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
747 8.100642    128.119.245.12  10.254.0.141      TCP    66 80 → 58356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
```

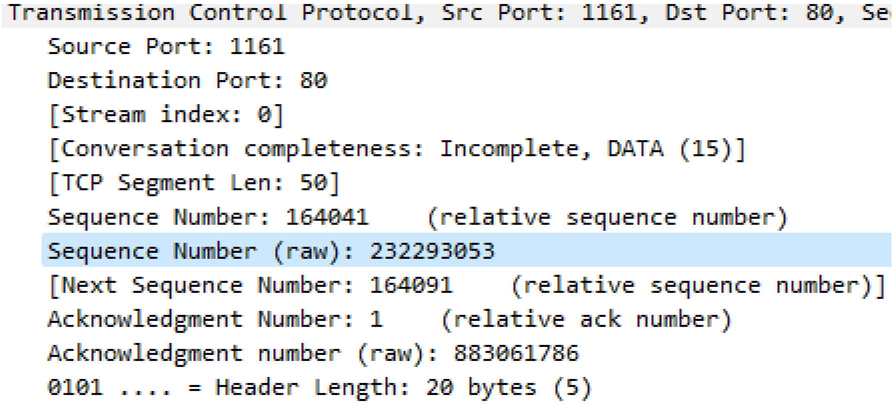
4. (using the given trace) sequence number = 0 (relative) 232129012 (raw). We know that it is the SYN segment because it has a SYN flag passed. 0x002 These bytes were 46 and 47



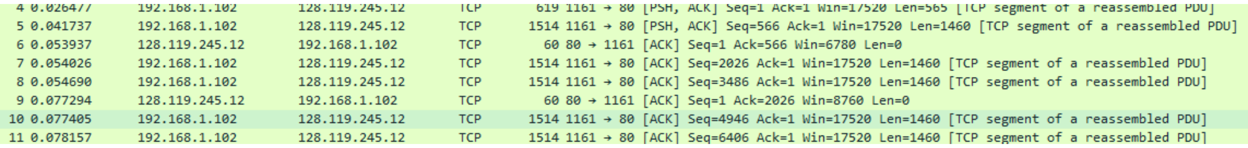
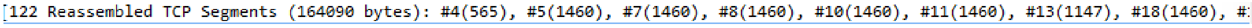
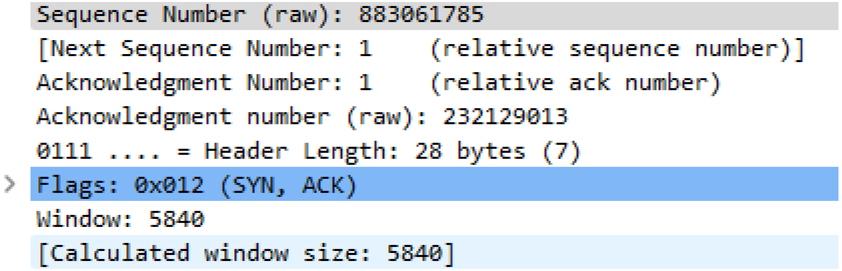
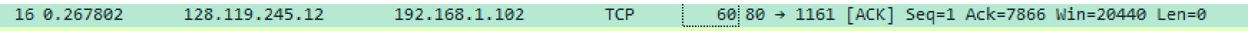
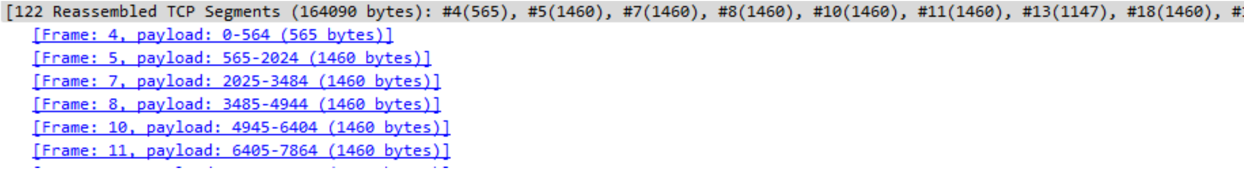
```
   0111 .... = Header Length: 28 bytes (7)
 v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
```

5. Sequence number = 0, The acknowledgement field was set to a relative 1, This number is the same as the raw sequence number sent in the SYN segment in question 4 plus 1. Bytes 46 and 47 identify the segment as a SYNACK segment.
   a. 

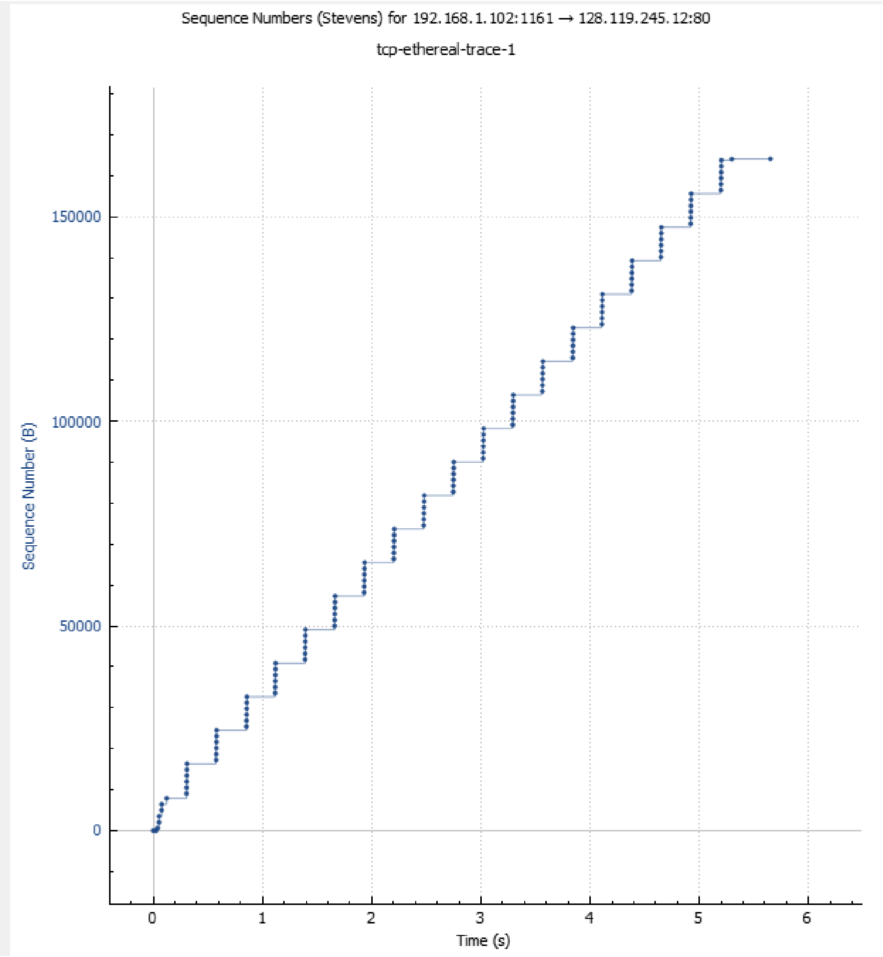
```
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 232129012
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  0111 .... = Header Length: 28 bytes (7)
> Flags: 0x002 (SYN)
```

6. The sequence number for the HTTP POST command was: 164041. The Sequence Number (raw) was: 232293053.
   a. 

```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Se
   Source Port: 1161
   Destination Port: 80
   [Stream index: 0]
   [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 50]
   Sequence Number: 164041    (relative sequence number)
   Sequence Number (raw): 232293053
   [Next Sequence Number: 164091    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 883061786
   0101 .... = Header Length: 20 bytes (5)
```

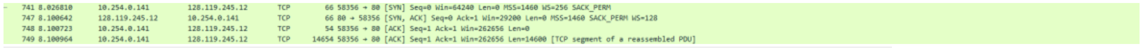
7. For this analysis the first six sequence numbers are [4,5,7,8,10,11], The time these packets were sent is [0.026477,0.041737,0.0540690,0.054690,0.077405,0.078157] in seconds sense initial capture. The time each ACK was received was [0.053937, 0.077294, 0.124085, 0.169118, 0.217299, 0.306692] in seconds sense initial capture, I was also unable to find the acknowledgement for the fourth segment. The RTT values are [0.02746, 0.035557, 0.070059, 0.114428, 0.139894, 0.189645] in seconds. The estimated RTT follows the equation,
   EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT
   [0.02746, 0.0285, 0.0337, 0.0438, 0.0558,0.0 725]
   a. 
```
 4 0.026477   192.168.1.102    128.119.245.12   TCP    619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
 5 0.041737   192.168.1.102    128.119.245.12   TCP   1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
 6 0.053937   128.119.245.12   192.168.1.102    TCP     60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
 7 0.054026   192.168.1.102    128.119.245.12   TCP   1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
 8 0.054690   192.168.1.102    128.119.245.12   TCP   1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
 9 0.077294   128.119.245.12   192.168.1.102    TCP     60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10 0.077405   192.168.1.102    128.119.245.12   TCP   1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11 0.078157   192.168.1.102    128.119.245.12   TCP   1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
```
8. The first segment size was 565 bytes, then the others were all 1460 bytes.
   a. 
```
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(1147), #18(1460), #
```
9. The minimum amount of data space, also known as the calculated window size, is 5840 bytes. For this reason, the sender is never throttled.
   a. 
```
Sequence Number (raw): 883061785
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 232129013
0111 .... = Header Length: 28 bytes (7)
> Flags: 0x012 (SYN, ACK)
Window: 5840
[Calculated window size: 5840]
```
10. There are no incomplete segments. To find an incomplete segment, you would need to check for each ACK. See the first graph on problem 13.
11. 60 bytes are used to acknowledge a typical amount of 1460 bytes in an ACK. We know that if the data is doubled then the sender is only acknowledging every other sequence.
    a. 
```
16 0.267802   128.119.245.12   192.168.1.102   TCP   60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
```
12. All data bytes 164090 bytes, I calculated 31.132Kbps from total time of the transmission, and the total amount of data.
    a. 
```
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(1147), #18(1460), #
   [Frame: 4, payload: 0-564 (565 bytes)]
   [Frame: 5, payload: 565-2024 (1460 bytes)]
   [Frame: 7, payload: 2025-3484 (1460 bytes)]
   [Frame: 8, payload: 3485-4944 (1460 bytes)]
   [Frame: 10, payload: 4945-6404 (1460 bytes)]
   [Frame: 11, payload: 6405-7864 (1460 bytes)]
```
13. Slow start begins at time 0 and switches at 0.1242 seconds to congestion avoidance. The measured data

a.

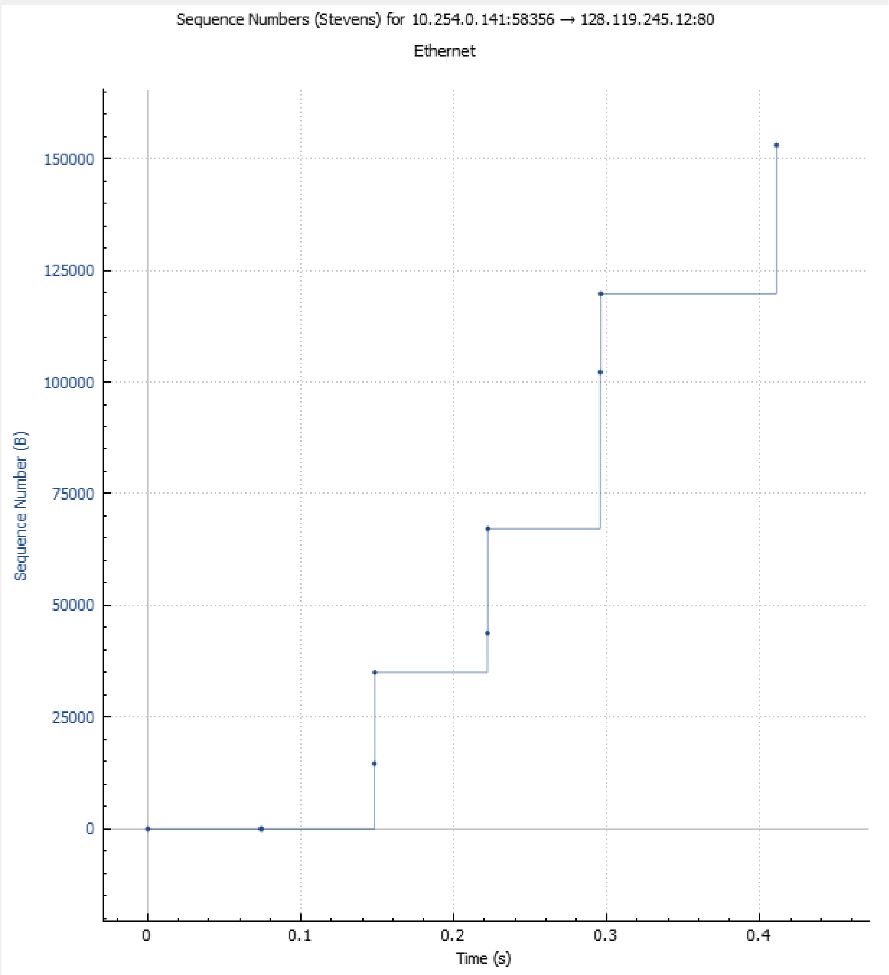


14. The throughput of the packets is 152975 bytes for all data and it was completed in 0.410917 seconds, thus I have 2.97821696mbps as the throughput. It is hard to tell when slow start begins as my packets are so large, thus I believe my system is in congestion avoidance for most of the TCP operation.

a.



```
741 8.026810   10.254.0.141     128.119.245.12   TCP      66 58356 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
747 8.100642   128.119.245.12   10.254.0.141     TCP      66 80 → 58356 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
748 8.100723   10.254.0.141     128.119.245.12   TCP      54 58356 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
749 8.100964   10.254.0.141     128.119.245.12   TCP   14654 58356 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
```


Sequence Numbers (Stevens) for 10.254.0.141:58356 → 128.119.245.12:80
Ethernet
Sequence Number (B)
Time (s)