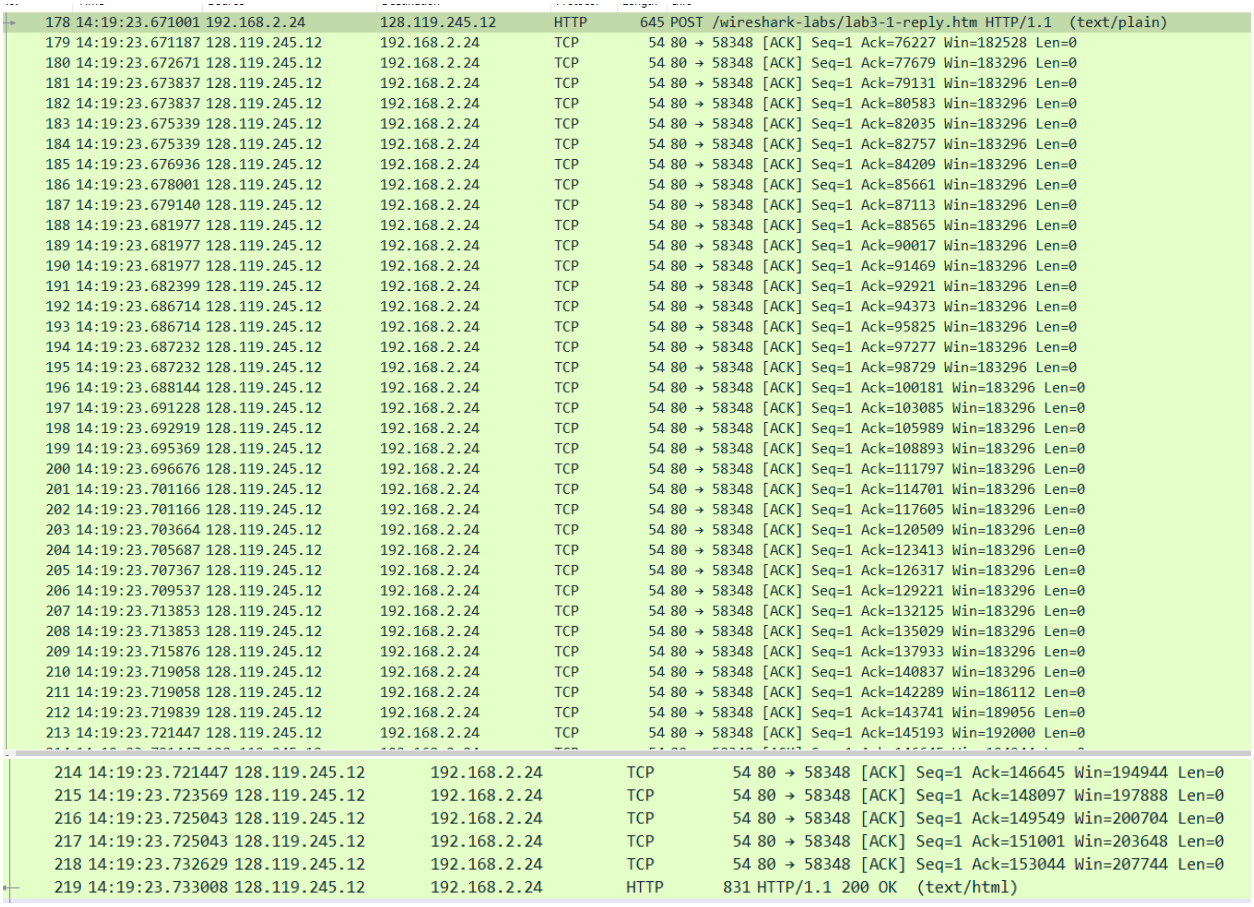
Wireshark lab 4

Name: Nirmith Victor D'Almeida
Student Number : 101160124

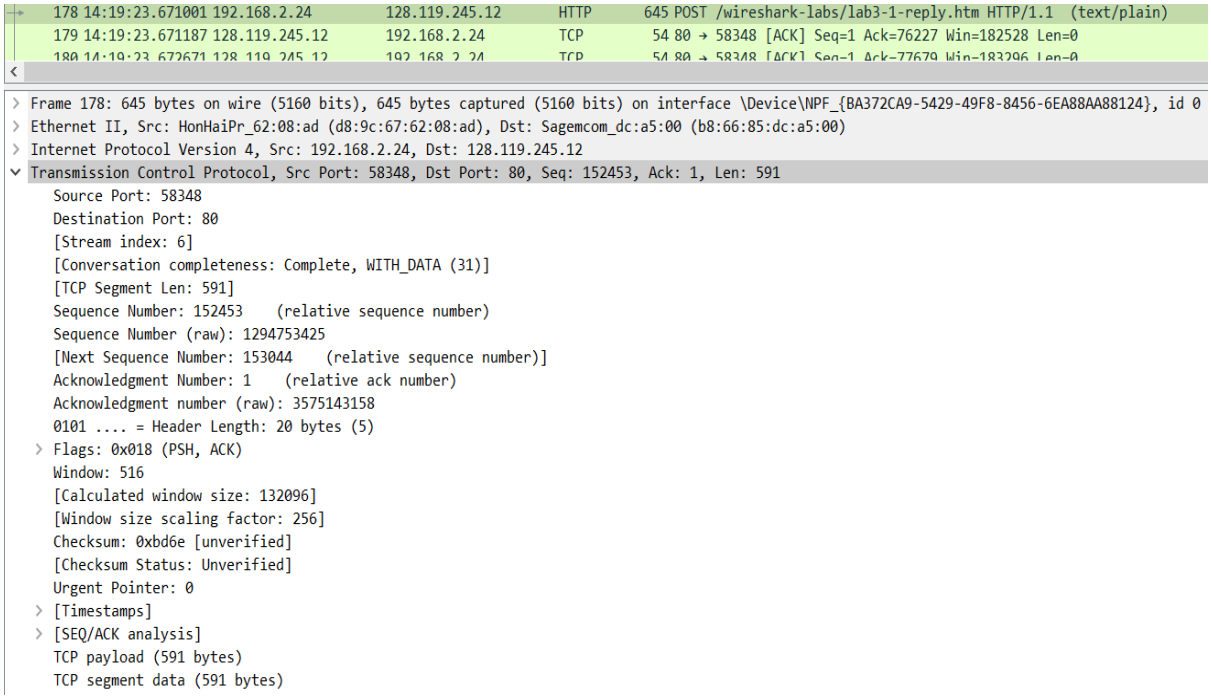
1. Capturing a bulk TCP transfer from your computer to a remote server



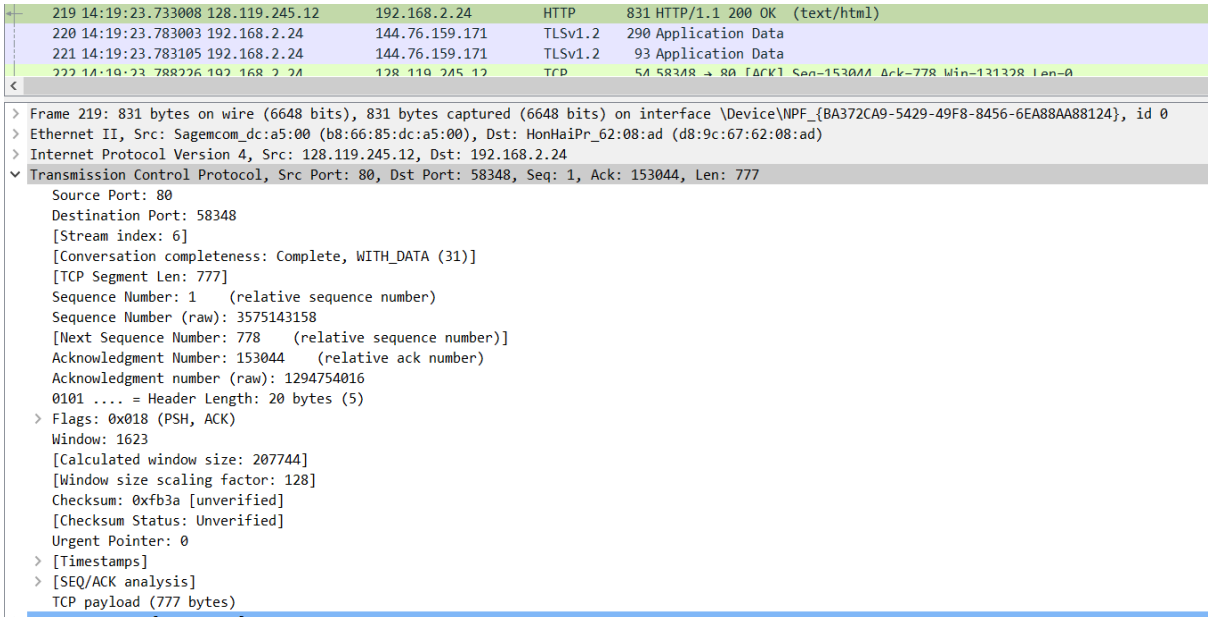
178	14:19:23.671001	192.168.2.24	128.119.245.12	HTTP	645	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
179	14:19:23.671187	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=76227 Win=182528 Len=0
180	14:19:23.672671	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=77679 Win=183296 Len=0
181	14:19:23.673837	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=79131 Win=183296 Len=0
182	14:19:23.673837	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=80583 Win=183296 Len=0
183	14:19:23.675339	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=82035 Win=183296 Len=0
184	14:19:23.675339	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=82757 Win=183296 Len=0
185	14:19:23.676936	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=84209 Win=183296 Len=0
186	14:19:23.678001	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=85661 Win=183296 Len=0
187	14:19:23.679140	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=87113 Win=183296 Len=0
188	14:19:23.681977	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=88565 Win=183296 Len=0
189	14:19:23.681977	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=90017 Win=183296 Len=0
190	14:19:23.681977	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=91469 Win=183296 Len=0
191	14:19:23.682399	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=92921 Win=183296 Len=0
192	14:19:23.686714	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=94373 Win=183296 Len=0
193	14:19:23.686714	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=95825 Win=183296 Len=0
194	14:19:23.687232	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=97277 Win=183296 Len=0
195	14:19:23.687232	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=98729 Win=183296 Len=0
196	14:19:23.688144	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=100181 Win=183296 Len=0
197	14:19:23.691228	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=103085 Win=183296 Len=0
198	14:19:23.692919	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=105989 Win=183296 Len=0
199	14:19:23.695369	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=108893 Win=183296 Len=0
200	14:19:23.696676	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=111797 Win=183296 Len=0
201	14:19:23.701166	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=114701 Win=183296 Len=0
202	14:19:23.701166	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=117605 Win=183296 Len=0
203	14:19:23.703664	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=120509 Win=183296 Len=0
204	14:19:23.705687	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=123413 Win=183296 Len=0
205	14:19:23.707367	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=126317 Win=183296 Len=0
206	14:19:23.709537	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=129221 Win=183296 Len=0
207	14:19:23.713853	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=132125 Win=183296 Len=0
208	14:19:23.713853	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=135029 Win=183296 Len=0
209	14:19:23.715876	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=137933 Win=183296 Len=0
210	14:19:23.719058	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=140837 Win=183296 Len=0
211	14:19:23.719058	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=142289 Win=186112 Len=0
212	14:19:23.719839	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=143741 Win=189056 Len=0
213	14:19:23.721447	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=145193 Win=192000 Len=0
214	14:19:23.721447	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=146645 Win=194944 Len=0
215	14:19:23.723569	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=148097 Win=197888 Len=0
216	14:19:23.725043	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=149549 Win=200704 Len=0
217	14:19:23.725043	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=151001 Win=203648 Len=0
218	14:19:23.732629	128.119.245.12	192.168.2.24	TCP	54	80 → 58348 [ACK] Seq=1 Ack=153044 Win=207744 Len=0
219	14:19:23.733008	128.119.245.12	192.168.2.24	HTTP	831	HTTP/1.1 200 OK (text/html)

2. A first Look at the Captured Trace

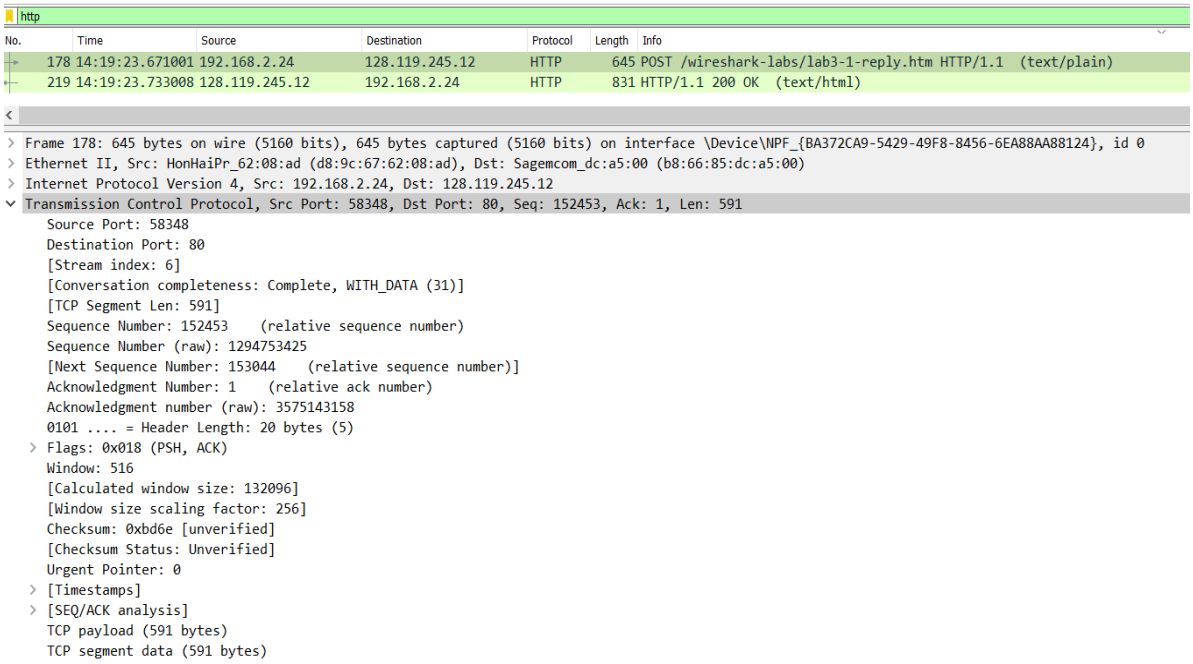
1. The Ip address is 192.168.2.24 and TCP port number is 58348



2. The ip address is 128.119.245.12 and the TCP port is 80

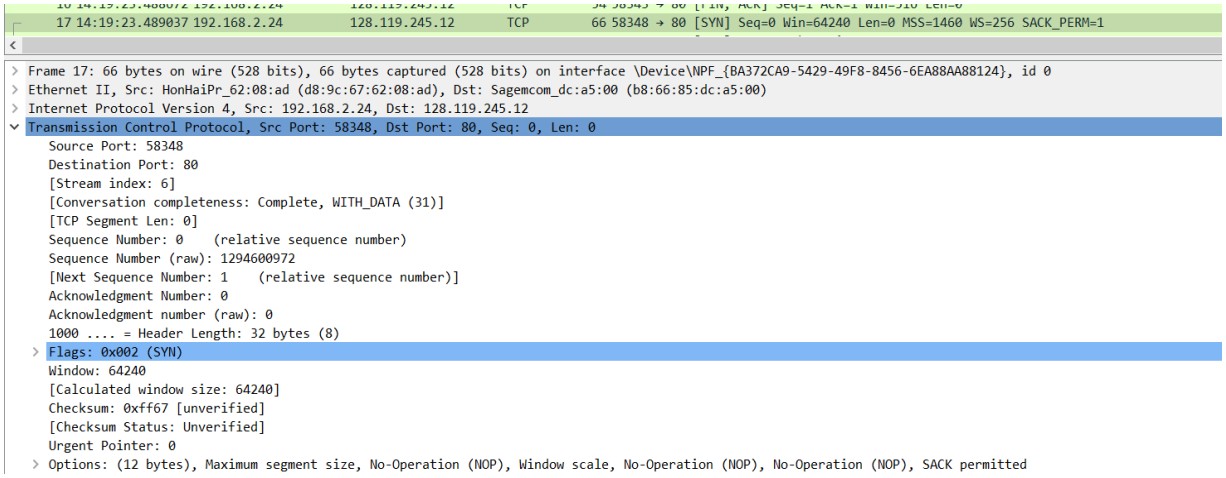


3. The IP address for my device is192.168.2.24 and port is 58348

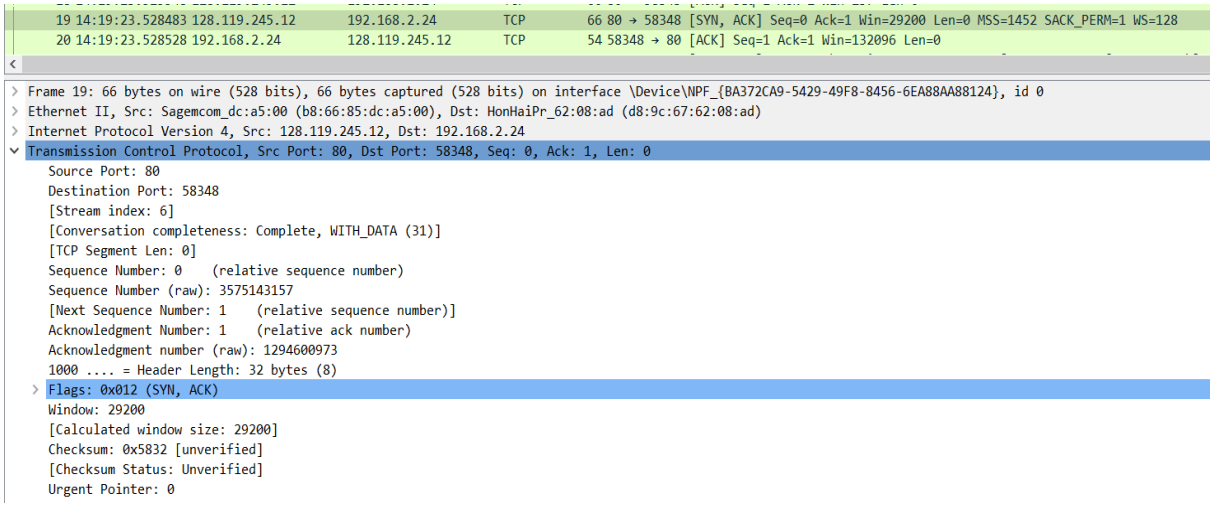


3. TCP basics

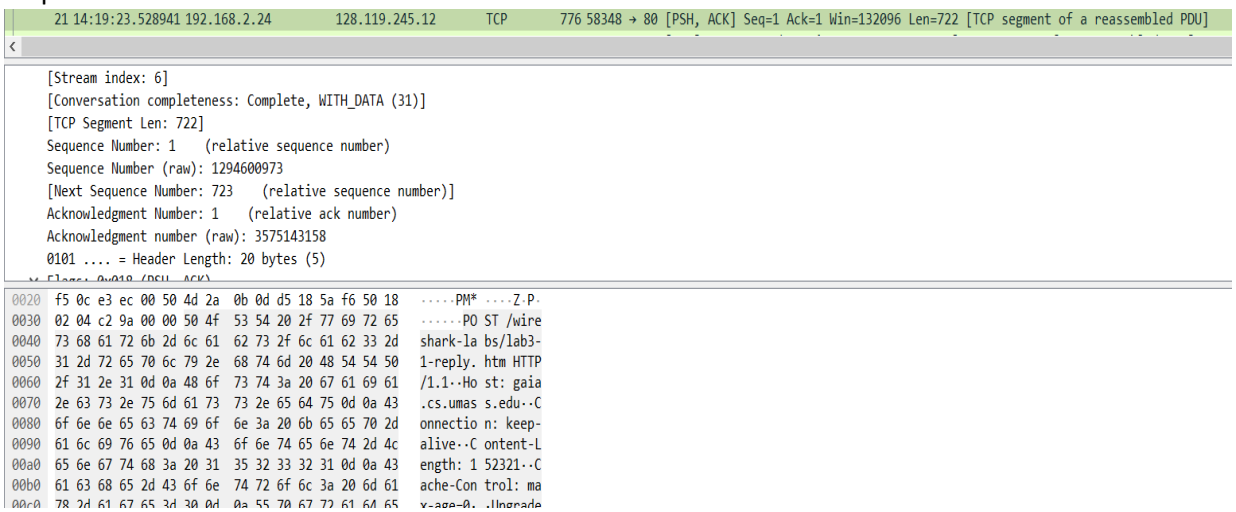
4. Sequence number is a 0 we can see the tag [SYN] which tells us that it is a SYN segment



5. Sequence number is 0, acknowledgement number is a 1, we can see the flag [syn,ack] which tells us that it is a synack segment



6. Sequence Number is 1



7. The 6 segments are no. 4, 5, 7, 8, 10, 11 and corresponding ack is 6, 9, 12, 14, 15, 16 (using tcp-ethereal-trace-1)

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=1
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=1
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
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]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0

a. Sequence number of first 6 segments are 1, 566, 2026, 3486, 4946, 6406

b.

Sequence Number	Sent Time
1	0.026477
566	0.041737
2026	0.054026
3486	0.054690
4946	0.077405
6406	0.078157

c.

Sequence Number	Received Time
1	0.053937
566	0.077294
2026	0.124085
3486	0.169118
4946	0.217299
6406	0.267802

d.

Sequence Number	Sent Time	Received Time	RTT
1	0.026477	0.053937	0.02746
566	0.041737	0.077294	0.035557
2026	0.054026	0.124085	0.070059
3486	0.054690	0.169118	0.114428
4946	0.077405	0.217299	0.139894
6406	0.078157	0.267802	0.189645

e.

Estimated RTT for first Segment after receipt of ACK (sequence 1) is equal to RTT for 1 (given) which is 0.02746

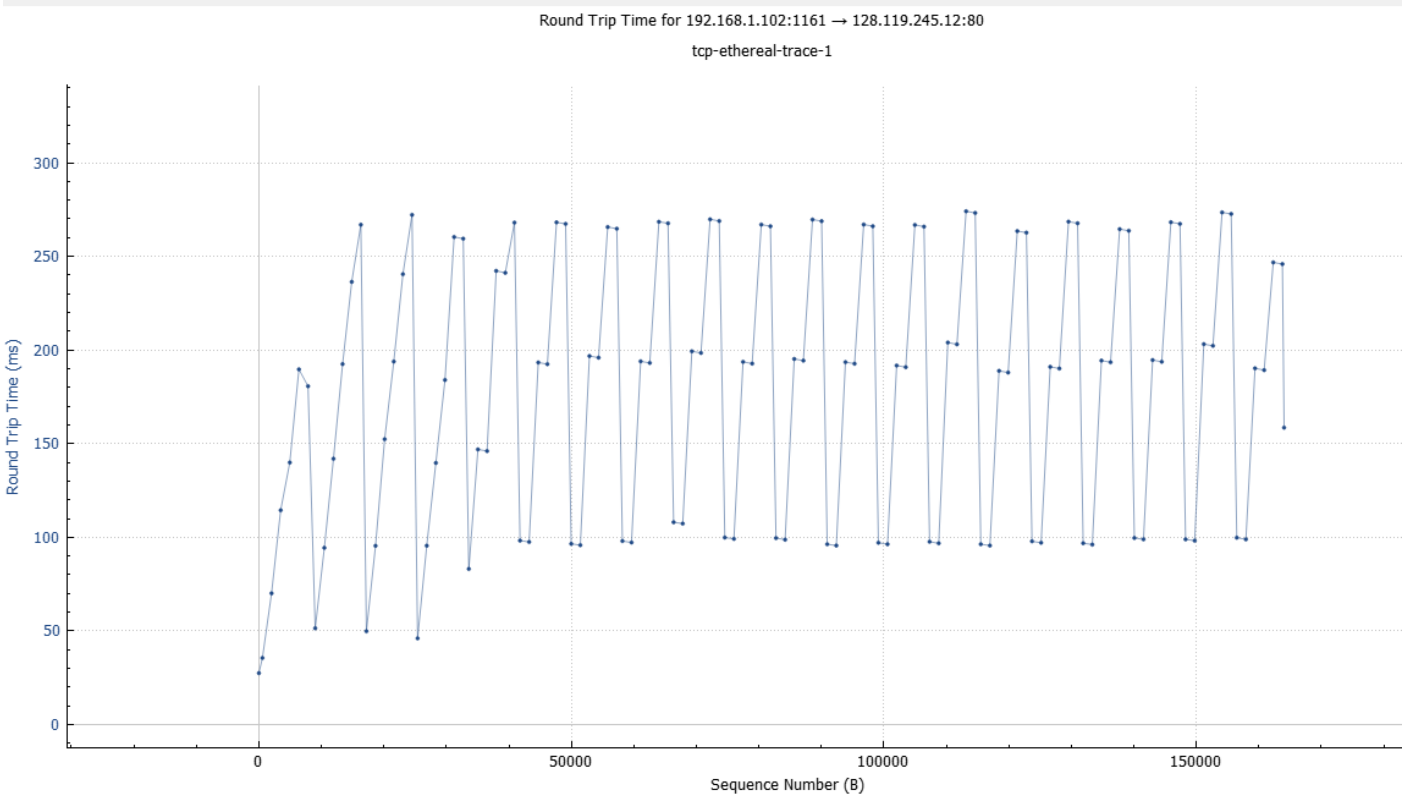
Estimated RTT for Second segment after receipt of ACK (sequence 566) is
= 0.875* 0.02746+0.125*0.035557 = 0.02842

Estimated RTT for Third Segment after receipt of ACK is
= 0.875*0.02842+0.125*0.070059 = 0.033624875

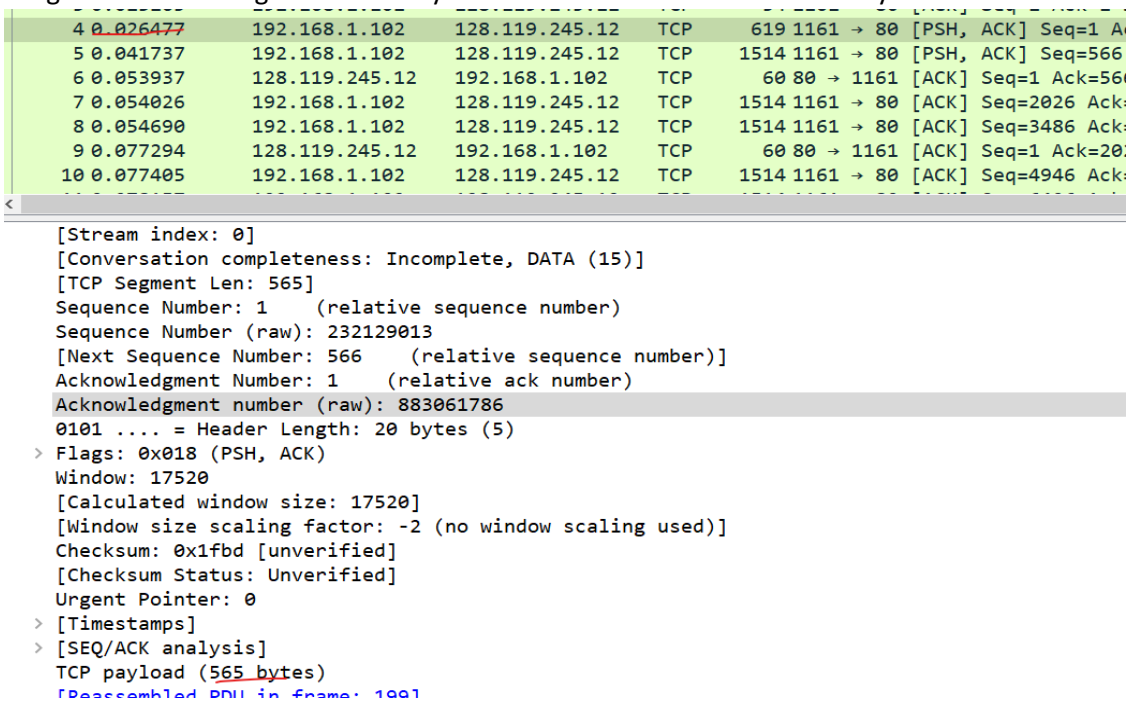
Estimated RTT for Fourth Segment after receipt of ACK is
= 0.875*0.033624875 + 0.125 * 0.114428 = 0.043725265625

Estimated RTT for Fifth Segment after receipt of ACK is
= 0.875* 0.043725265625+0.125*0.139894 = 0.055746357421875

Estimated RTT for Sixth Segment after receipt of ACK is
= 0.875*0.055746357421875+0.125*0.189645 = 0.072483687744140625



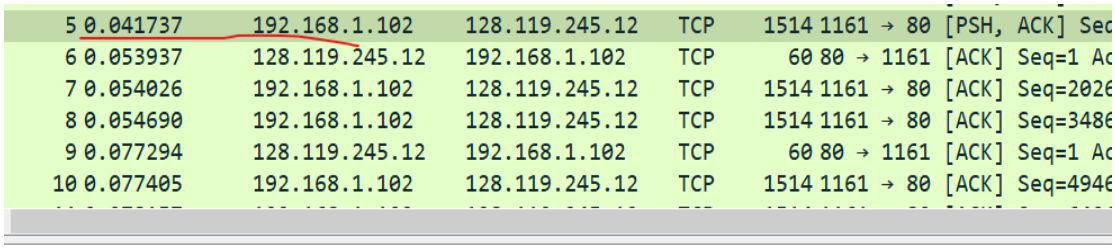
8. Length of first TCP segment is 565 bytes and rest 5 of them where 1460 bytes



4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 A
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=56
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=20
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack

```
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 565]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 232129013
[Next Sequence Number: 566    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1fbd [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (565 bytes)
```

TCP segment 1^



5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ac
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ac
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946

```
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 1460]
Sequence Number: 566    (relative sequence number)
Sequence Number (raw): 232129578
[Next Sequence Number: 2026    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x3be5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (1460 bytes)
```

TCP segment 2

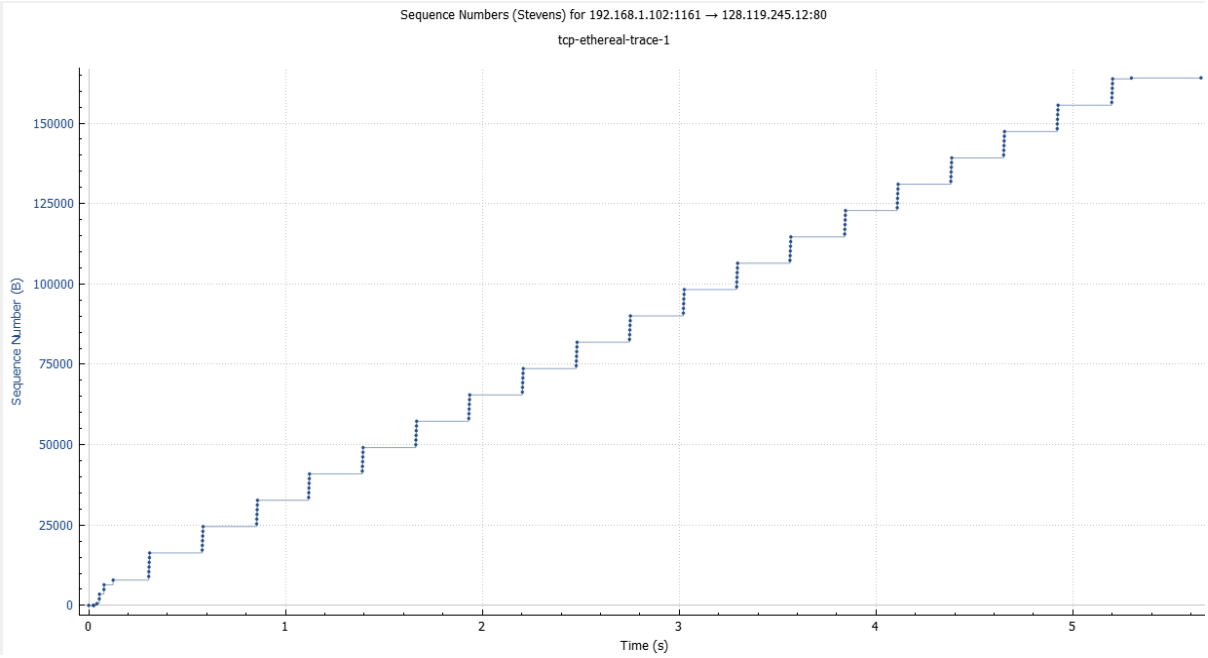
9.

4	0.026477	192.168.1.102	128.119.245.12	TCP	619 1161 → 80 [PSH, ACK] Seq=
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [PSH, ACK] Seq=
6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=2026
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=3486
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=4946

```
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 883061786
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: ·····AP···]
Window: 17520
```

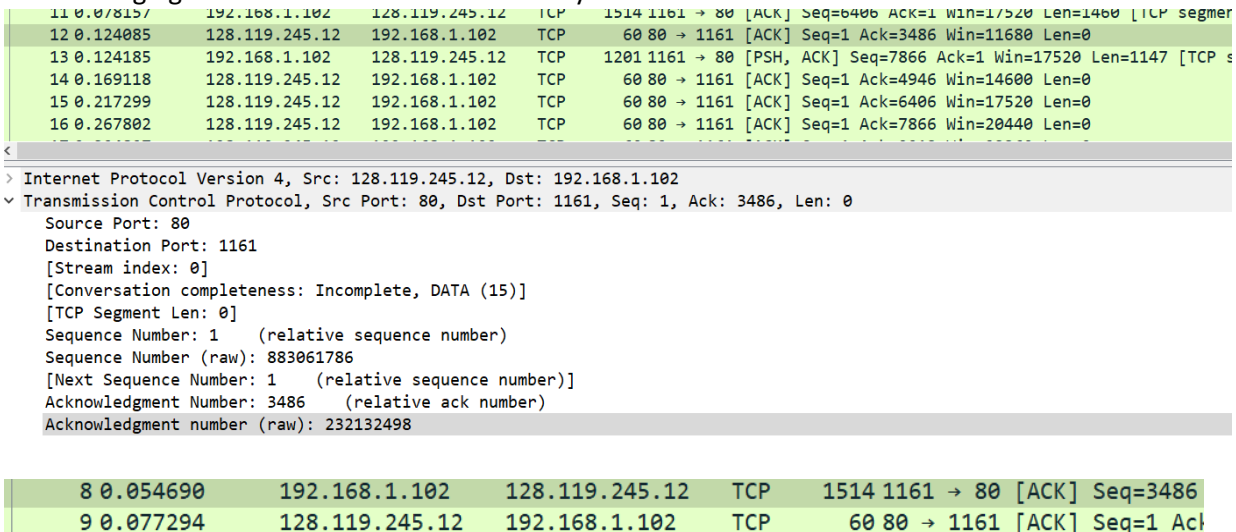
Minimum amount of buffer space advertised at the received for the entire trace is 17520. According to the trace the sender is never throttled.

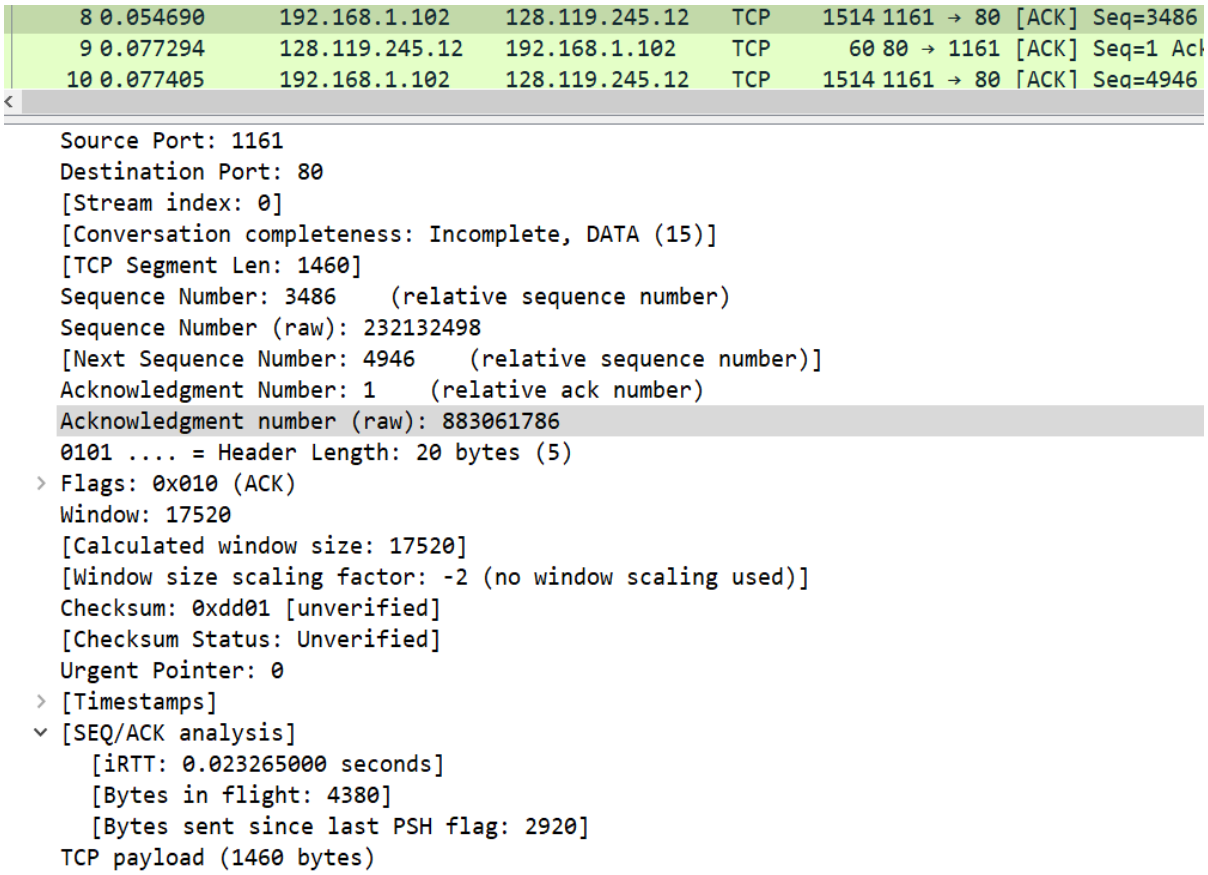
10. As we can see in the graph below we can see that there are no retransmitted segments since they are increasing



11.

The receiver is acknowledging ever other received segment for instance packet 12 is acknowledging 3486 which has a data of 1460 bytes.





12. We can calculate throughput by getting the file size on disk which is 152,138 bytes and divide by the total time taken to get it (ethereal-trace-1 file) which is 5.651141 s

therefore we get $\frac{152{,}138}{5.651141} = 26921.6429036189\ bytes\ per\ second\ (bps)$

4. TCP congestion control in action

13.