

Wireshark TCP

TCP basics

10.000000	192.168.1.102	128.119.245.12	TCP	62.1161 → 80	[SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
20.023172	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
30.023265	192.168.1.102	128.119.245.12	TCP	54.1161 → 80	[ACK] Seq=1 Ack=1 Win=17520 Len=0
40.026477	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]
50.041737	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]
60.053937	128.119.245.12	192.168.1.102	TCP	60.80 → 1161	[ACK] Seq=1 Ack=566 Win=6780 Len=0
70.054026	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]
80.054690	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]
90.077294	128.119.245.12	192.168.1.102	TCP	60.80 → 1161	[ACK] Seq=1 Ack=2026 Win=8760 Len=0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

0111 = Header Length: 28 bytes (7)

Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

....0... = Congestion Window Reduced (CWR): Not set

....0... = ECN Echo: Not set

1.

Client computer (source)

IP address: 192.168.1.102

TCP port number: 1161

2.

Destination computer: gaia.cs.umass.edu

IP address: 128.119.245.12

TCP port number: 80

3.

Source computer/ Client

IP address: 10.136.77.101

TCP port number: 52696

Destination computer : gaia.cs.umass.edu

IP address: 128.119.245.12

TCP port number: 80

135.20.498945938	10.136.77.101	128.119.245.12	TCP	74.52696 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2034719104 TSecr=0 WS=128
136.20.532975208	8.6.245.30	10.136.77.101	DNS	104Standard query response 0x48e5 A gaia.cs.umass.edu A 128.119.245.12 OPT
137.20.535927572	10.136.77.101	8.6.245.30	TCP	132Destination unreachable (Port unreachable)
138.20.540499491	8.6.245.30	10.136.77.101	DNS	141Standard query response 0xb209 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu OPT
139.20.548538219	10.136.77.101	8.6.245.30	TCP	169Destination unreachable (Port unreachable)
140.20.544850291	128.119.245.12	10.136.77.101	TCP	74.80 → 52696 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3053014173 TSecr=2034719104 WS=128
141.20.544896241	10.136.77.101	128.119.245.12	TCP	66.52696 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2034719151 TSecr=3053014173
142.20.970622359	157.240.14.52	10.136.77.101	TLSV1.2	281Application Data
143.20.970657300	10.136.77.101	157.240.14.52	TCP	66.40502 → 443 [ACK] Seq=1 Ack=333 Win=2106 Len=0 TSval=2527051473 TSecr=2073920179
144.20.970691700	157.240.14.52	10.136.77.101	TLSV1.2	281Application Data
145.20.970703400	10.136.77.101	157.240.14.52	TCP	66.48582 → 443 [ACK] Seq=1 Ack=548 Win=2105 Len=0 TSval=2527051473 TSecr=2073920179
146.20.971220887	157.240.14.52	10.136.77.101	TLSV1.2	226Application Data
147.20.971252597	10.136.77.101	157.240.14.52	TCP	66.48582 → 443 [ACK] Seq=1 Ack=708 Win=2104 Len=0 TSval=2527051473 TSecr=2073920195
148.20.074646074	157.240.14.52	10.136.77.101	TLSV1.2	294Application Data
* Frame 135: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0				
* Ethernet II, Src: IntelCor_29:7a:7a (28:16:ad:29:7a:7a), Dst: All-HSRP-routers_01 (00:00:0c:07:ac:01)				
* Internet Protocol Version 4, Src: 10.136.77.101, Dst: 128.119.245.12				
* Transmission Control Protocol, Src Port: 52696, Dst Port: 80, Seq: 0, Len: 0				
Source Port: 52696				
Destination Port: 80				
[Stream index: 0]				
[TCP Segment Len: 0]				

4.

Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in this trace. The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

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
* Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)				
* Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)				
* Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12				
* Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0				
Source Port: 1161				
Destination Port: 80				
[Stream index: 0]				
[TCP Segment Len: 0]				
Sequence number: 0 (relative sequence number)				
[Next sequence number: 0 (relative sequence number)]				
Acknowledgment number: 0				
0111 = Header Length: 28 bytes (7)				
* Flags: 0x002 (SYN)				
000. = Reserved: Not set				
...0 = Nonce: Not set				
.... 0... = Congestion Window Reduced (CWR): 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 of the SYNACK segment from gaia.cs.umass.edu to the client computer in reply to the SYN has the value of 0 in this trace.

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 gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer (i.e. the sequence number of the SYN segment initiated by the client computer is 0). The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.

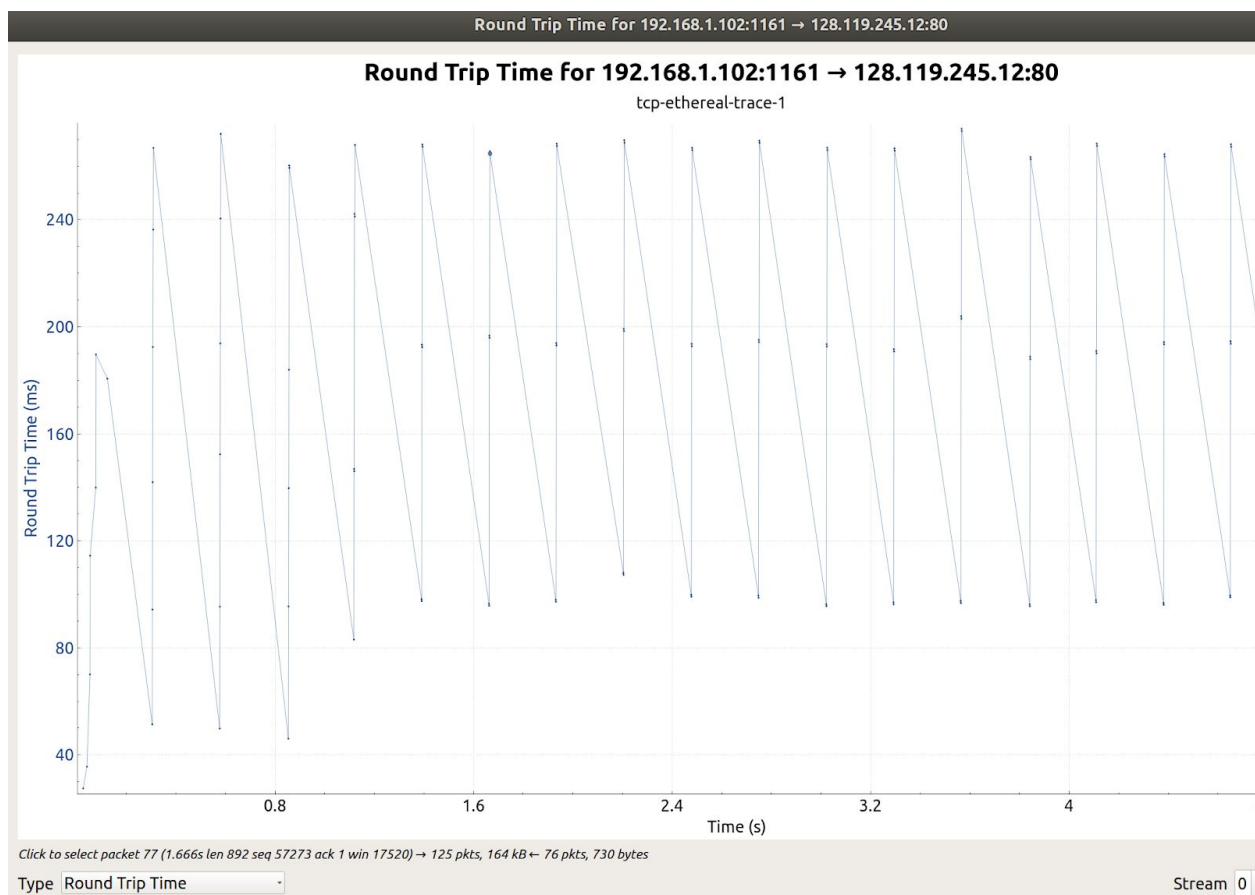
20.023172	128.119.245.12	192.168.1.102	TCP	62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
30.023265	192.168.1.102	128.119.245.12	TCP	54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
• Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)				
• Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)				
• Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102				
• Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0				
Source Port: 80				
Destination Port: 1161				
[Stream index: 0]				
[TCP Segment Len: 0]				
Sequence number: 0 (relative sequence number)				
[Next sequence number: 0 (relative sequence number)]				
Acknowledgment number: 1 (relative ack number)				
0111 = Header Length: 28 bytes (7)				
• Flags: 0x012 (SYN, 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				
....0... = Push: Not set				
....0.. = Reset: Not set				
•1. = Syn: Set				
....0 = Fin: Not set				
..... ..				

6.

No. 4 segment is the TCP segment containing the HTTP POST command. The sequence number of this segment has the value of 1.

40.026477	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]
50.041737	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]
60.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
70.054026	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]
80.054690	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]
90.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
• Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)				
• Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)				
• Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12				
• Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565				
Source Port: 1161				
Destination Port: 80				
[Stream index: 0]				
[TCP Segment Len: 565]				
Sequence number: 1 (relative sequence number)				
[Next sequence number: 566 (relative sequence number)]				
Acknowledgment number: 1 (relative ack number)				
0101 = Header Length: 20 bytes (5)				
• Flags: 0x010 (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				
0020	f5 0c 04 89 90 50	0d d6 01 f5 34 a2 74 1a 50 18P...4.t.P.	
0030	44 70 1f bd 00 00 50 4f	53 54 20 2f 65 74 68 65	Dp...PO ST /ethe	
0040	72 65 61 6c 2d 6c 61 62	73 2f 6c 61 62 33 2d 31	real-lab s/lab3-1	
0050	2d 72 65 70 6c 79 2e 68	74 6d 20 48 54 54 50 2f	-reply.h tm HTTP/	
0060	31 2e 31 0d 0a 48 6f 73	74 3a 20 67 61 69 61 2e	1.1. Hos t: gaia.	
0070	63 73 2e 75 0d 61 73 73	2e 65 64 75 0d 0a 55 73	cs.umass .edu .Us	
0080	65 72 2d 41 67 65 6e 74	3a 20 4d 6f 7a 69 6c 6c	er-Agent : Mozill	
0090	61 2f 35 2e 30 28 57 69	6e 64 6f 77 73 3b 20	a/5.0 (W indows;	
00a0	55 3b 20 57 69 6e 64 6f	77 73 20 4e 54 20 35 2e	U; Windo ws NT 5.	

7.



segment	Relative Segment number	Segment number	Time sent	Acknowledgement Received	RTT	Estimated RTT
1	1	0dd601f	.026	.054	.028	.028
2	566	0dd6042	.042	.077	.035	.035
3	2026	0dd609d	.054	.124	.070	.70
4	3486	0dd60f9	.055	.169	.114	.114
5	4946	0dd60f9	.077	.217	.140	.140
6	6406	0dd61af	.078	.268	.190	.190

Estimated RTT packet 1 : $0.875 * .028 + 0.125 * .028 = .028$

Estimated RTT packet 2 : $0.875 * .042 + 0.125 * .035 = .035$

Estimated RTT packet 3 : $0.875 * .054 + 0.125 * .070 = .070$

Estimated RTT packet 4 : $0.875 * .055 + 0.125 * .114 = .114$

Estimated RTT packet 5 : $0.875 * .077 + 0.125 * .140 = .140$

Estimated RTT packet 6 : $0.875 * .078 + 0.125 * .190 = .190$

8.

Segment 1 = 565 bytes

Segment 2 = 1460 bytes

Segment 3 = 1460 bytes

Segment 4 = 1460 bytes

Segment 5 = 1460 bytes

Segment 6 = 1460 bytes

40.026477	192.168.1.102	128.119.245.12	TCP	6191161 → 80	[PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
50.041737	192.168.1.102	128.119.245.12	TCP	15141161 → 80	[PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
60.053937	128.119.245.12	192.168.1.102	TCP	6080 → 1161	[ACK] Seq=1 Ack=566 Win=6780 Len=0
70.054026	192.168.1.102	128.119.245.12	TCP	15141161 → 80	[ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
80.054690	192.168.1.102	128.119.245.12	TCP	15141161 → 80	[ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
90.077294	128.119.245.12	192.168.1.102	TCP	6080 → 1161	[ACK] Seq=1 Ack=2026 Win=8760 Len=0
100.077405	192.168.1.102	128.119.245.12	TCP	15141161 → 80	[ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
110.078157	192.168.1.102	128.119.245.12	TCP	15141161 → 80	[ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
120.124085	128.119.245.12	192.168.1.102	TCP	6080 → 1161	[ACK] Seq=1 Ack=3486 Win=11680 Len=0
130.124185	192.168.1.102	128.119.245.12	TCP	12011161 → 80	[PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a reassembled PDU]
140.169118	128.119.245.12	192.168.1.102	TCP	6080 → 1161	[ACK] Seq=1 Ack=4946 Win=14600 Len=0

9.

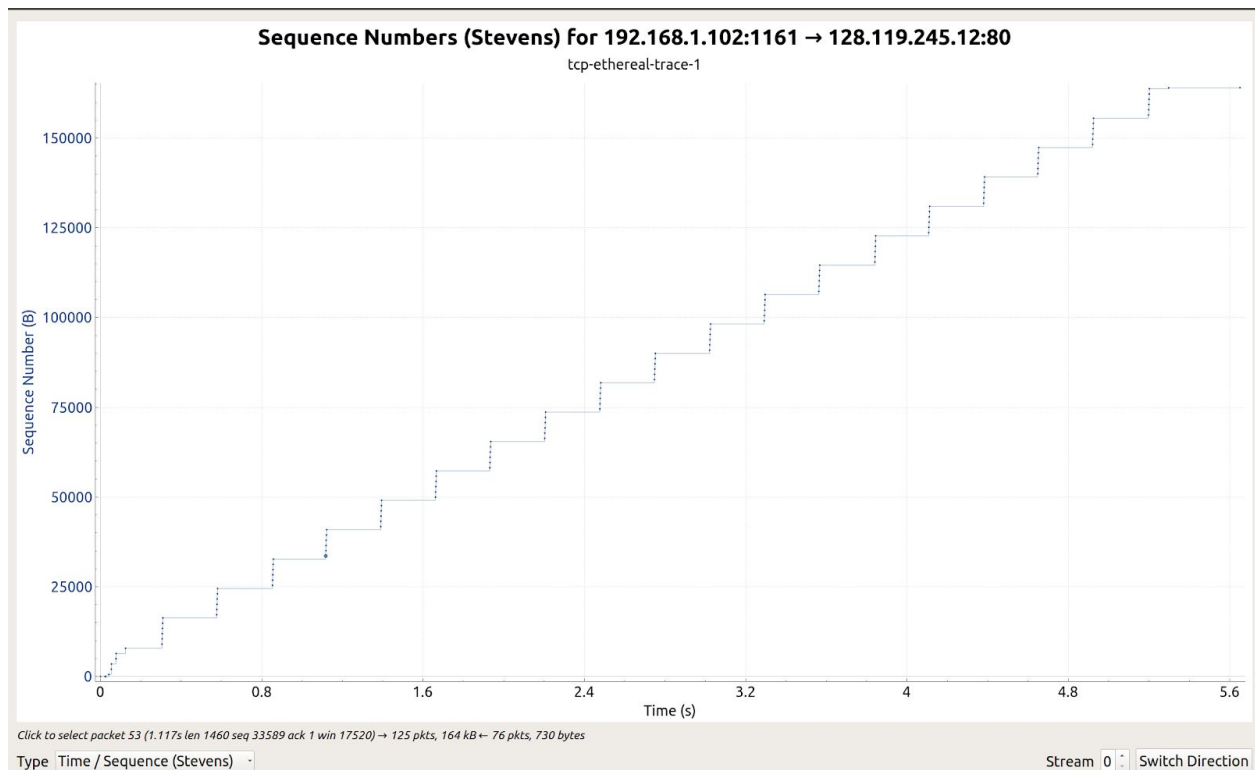
The minimum amount of available buffer space is advertised as 5840 bytes.

The lack of receiver buffer space does not ever throttle the sender.

10.000000	192.168.1.102	128.119.245.12	TCP	621161 → 80	[SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
20.023172	128.119.245.12	192.168.1.102	TCP	6280 → 1161	[SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
30.023265	192.168.1.102	128.119.245.12	TCP	541161 → 80	[ACK] Seq=1 Ack=1 Win=17520 Len=0

10.

There are no retransmitted segments in the trace file. This is verified by checking the sequence numbers of the TCP segments in the trace file.



If there is a retransmitted segment, the sequence number of this retransmitted segment should be smaller than those of its neighboring segments.

11.

The receiver typically acknowledges 1460 bytes in an ack. If the data is doubled then that segment is ACKing every other received segment.

Eg:

Segment 80,87,88...

80	1.930880	128.119.245.12	192.168.1.102	TCP	60 80 → 1161	[ACK]	Seq=1 Ack=58165 Win=62780 Len=0	
81	1.931099	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK]	Seq=58165 Ack=1 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
82	1.931879	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK]	Seq=59625 Ack=1 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
83	1.932757	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK]	Seq=61085 Ack=1 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
84	1.933636	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK]	Seq=62545 Ack=1 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
85	1.934770	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK]	Seq=64005 Ack=1 Win=17520 Len=1460	[TCP segment of a reassembled PDU]
86	1.935586	192.168.1.102	128.119.245.12	TCP	946 1161 → 80	[PSH, ACK]	Seq=65465 Ack=1 Win=17520 Len=892	[TCP segment of a reassembled PDU]
87	2.029069	128.119.245.12	192.168.1.102	TCP	60 80 → 1161	[ACK]	Seq=1 Ack=61085 Win=62780 Len=0	
88	2.126682	128.119.245.12	192.168.1.102	TCP	60 80 → 1161	[ACK]	Seq=1 Ack=64005 Win=62780 Len=0	

12.

The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for No. 4 segment) and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment). Therefore, Total data = $164091 - 1 = 164090$ bytes.

The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment).

Therefore, Total transmission time is $5.455830 - 0.026477 = 5.4294$ seconds

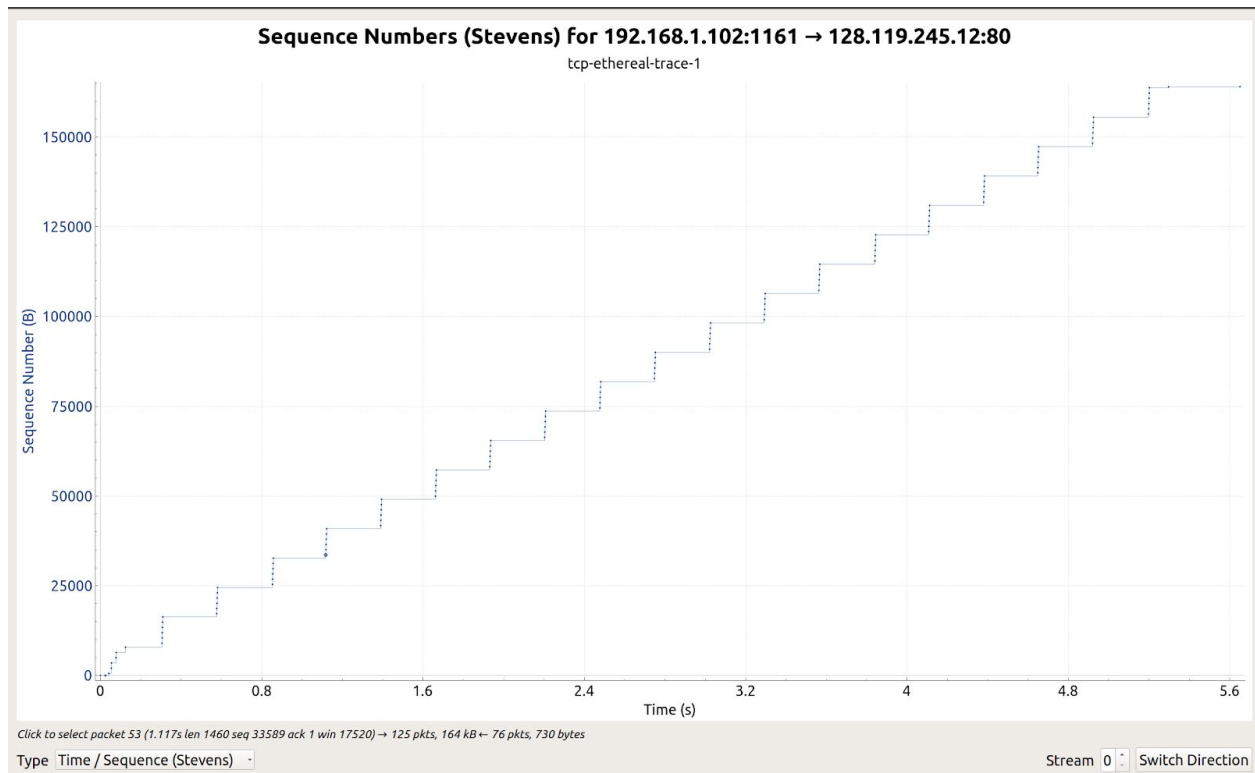
The average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time.

Throughput for the TCP connection = $164090/5.4294 = 30.222$ KByte/sec.

TCP congestion control in action

13.

The slowstart phase begins at about zero and ends at about .15 seconds according to the graph then congestion avoidance takes over. The measured data is only using a fraction of the window size instead of the idealized 1/3 to a half.



14.

The slowstart phase begins at about zero and ends at about 2.8 seconds according to the graph then congestion avoidance takes over.

In this case, we observe the expected linear increase behavior, i.e. the TCP transmit window does grows linearly during this phase.

