

Project 3

Wireshark Lab: TCP

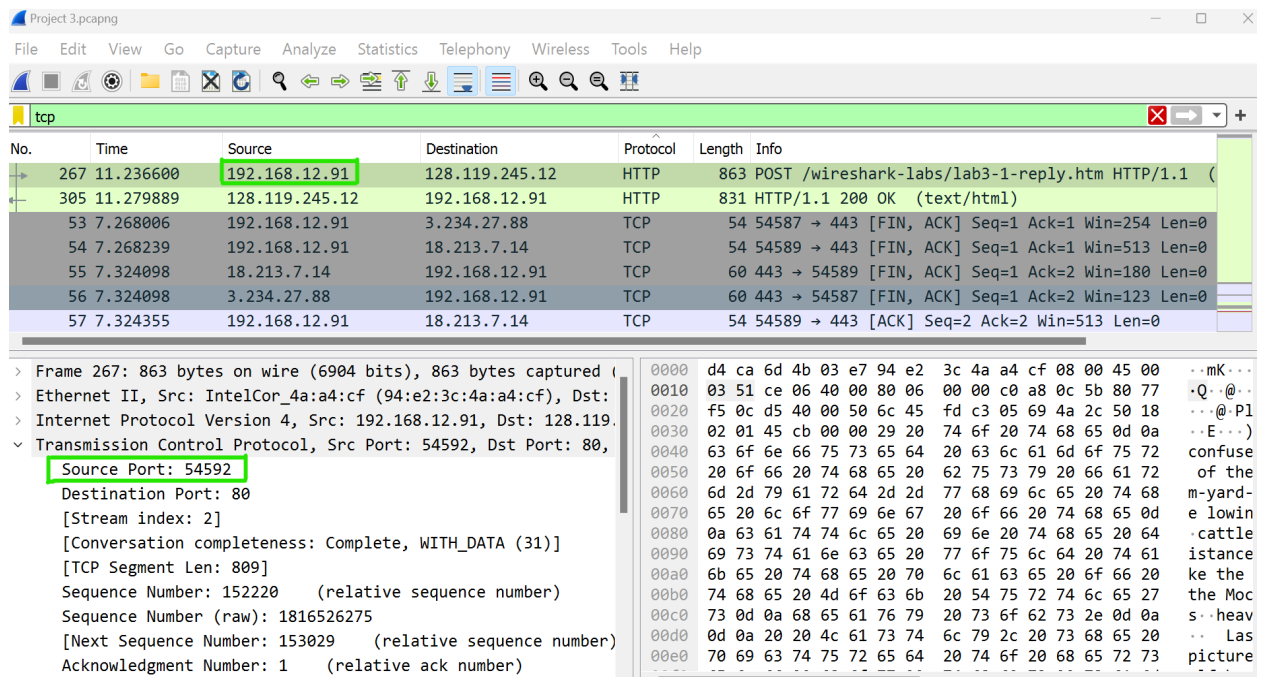
Puja Shah

CSIT-340-11 Computer Networks

Summer 2023

Dr. Murtadha Aldeer

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” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you're uncertain about the Wireshark windows.)



IP address: 192.168.12.91

TCP Port number: 54592

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?

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
267	11.236600	192.168.12.91	128.119.245.12	HTTP	863	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (
305	11.279889	128.119.245.12	192.168.12.91	HTTP	831	HTTP/1.1 200 OK (text/html)
53	7.268006	192.168.12.91	3.234.27.88	TCP	54	54587 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
54	7.268239	192.168.12.91	18.213.7.14	TCP	54	54589 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
55	7.324098	18.213.7.14	192.168.12.91	TCP	60	443 → 54589 [FIN, ACK] Seq=1 Ack=2 Win=180 Len=0
56	7.324098	3.234.27.88	192.168.12.91	TCP	60	443 → 54587 [FIN, ACK] Seq=1 Ack=2 Win=123 Len=0
57	7.324355	192.168.12.91	18.213.7.14	TCP	54	54589 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0

> Frame 305: 831 bytes on wire (6648 bits), 831 bytes captured (

> Ethernet II, Src: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7), Dst:

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.91

> Transmission Control Protocol, Src Port: 80, Dst Port: 54592,

Source Port: 80

Destination Port: 54592

[Stream index: 2]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 777]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 90786348

[Next Sequence Number: 778 (relative sequence number)]

Acknowledgment Number: 153029 (relative ack number)

Acknowledgment Number (raw): 4816526275

0000 94 e2 3c 4a a4 cf d4 ca 6d 4b 03 e7 08 00 45 00 ...<J...
 0010 03 51 ce 06 40 00 80 06 00 00 c0 a8 0c 5b 80 77 ...Q...@...
 0020 0c 5b 00 50 d5 40 05 69 fd c3 05 69 4a 2c 50 18 ...@...P...
 0030 08 f5 1d 4a 00 00 48 54 54 50 2f 31 2e 31 20 32 ...J...H...
 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 ...OK...
 0050 2c 20 30 38 20 4a 75 6e 20 32 30 32 33 20 32 33 ... , 08 Ju
 0060 3a 30 35 3a 32 31 20 47 4d 54 0d 0a 53 65 72 76 ...:05:21
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 ...er: Apa
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 ... (CentO
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 ...L/1.0.2
 00a0 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 ...P/7.4.3
 00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 ...l/2.0.1
 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 6916.3...
 00d0 66 69 65 64 3a 20 53 61 74 2c 20 30 36 20 46 65 ...fied: S
 00e0 62 20 32 30 32 31 20 31 38 3a 32 33 3a 34 37 20 ...b 2021
 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 61 32 2d ...GMT+ET

The IP address of gaia.cs.umass.edu is 128.119.245.12 and the port number of sending and receiving TCP segments for this connection is 80.

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?

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
267	11.236600	192.168.12.91	128.119.245.12	HTTP	863	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (
305	11.279889	128.119.245.12	192.168.12.91	HTTP	831	HTTP/1.1 200 OK (text/html)
53	7.268006	192.168.12.91	3.234.27.88	TCP	54	54587 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
54	7.268239	192.168.12.91	18.213.7.14	TCP	54	54589 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
55	7.324098	18.213.7.14	192.168.12.91	TCP	60	443 → 54589 [FIN, ACK] Seq=1 Ack=2 Win=180 Len=0
56	7.324098	3.234.27.88	192.168.12.91	TCP	60	443 → 54587 [FIN, ACK] Seq=1 Ack=2 Win=123 Len=0
57	7.324355	192.168.12.91	18.213.7.14	TCP	54	54589 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0

> Frame 267: 863 bytes on wire (6904 bits), 863 bytes captured (

> Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst:

> Internet Protocol Version 4, Src: 192.168.12.91, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 54592, Dst Port: 80,

Source Port: 54592

Destination Port: 80

[Stream index: 2]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 809]

Sequence Number: 152220 (relative sequence number)

Sequence Number (raw): 1816526275

[Next Sequence Number: 153029 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment Number (raw): 4816526275

0000 d4 ca 6d 4b 03 e7 94 e2 3c 4a a4 cf 08 00 45 00 ...mK...
 0010 03 51 ce 06 40 00 80 06 00 00 c0 a8 0c 5b 80 77 ...Q...@...
 0020 f5 0c d5 40 00 50 6c 45 fd c3 05 69 4a 2c 50 18 ...@...P...
 0030 02 01 45 cb 00 00 29 20 74 6f 20 74 68 65 0d 0a ...E...)
 0040 63 6f 6e 66 75 73 65 64 20 63 6c 61 6d 6f 75 72 ... confuse
 0050 20 6f 66 20 74 68 65 20 62 75 73 79 20 66 61 72 ... of the
 0060 6d 2d 79 61 72 64 2d 2d 77 68 69 6c 65 20 74 68 ...m-yard-
 0070 20 60 6c 6f 77 69 6e 67 20 6f 66 20 74 68 65 0d ...e lowin
 0080 0a 63 61 74 74 6c 65 20 69 6e 20 74 68 65 20 64 ... cattle
 0090 69 73 74 61 6e 63 65 20 77 6f 75 6c 64 20 74 61 ... instance
 00a0 6b 65 20 74 68 65 20 70 6c 61 63 65 20 6f 66 20 ... ke the
 00b0 74 68 65 20 4d 6f 63 6b 20 54 75 72 74 6c 65 27 ... the Moc
 00c0 73 0d 0a 68 65 61 76 79 20 73 6f 62 73 2e 0d 0a ... s heav
 00d0 0d 0a 20 20 4c 61 73 74 6c 79 2c 20 73 68 65 20 ... Las
 00e0 70 69 63 74 75 72 65 64 20 74 6f 20 68 65 72 73 ... picture

IP address: 192.168.12.91

TCP Port number: 54592

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 image shows a Wireshark packet capture of a TCP connection. The packet list shows a SYN segment from 192.168.12.91 to 128.119.245.12. The packet details pane shows the following information:

- Transmission Control Protocol, Src Port: 54592, Dst Port: 80
- Source Port: 54592
- Destination Port: 80
- [Stream index: 2]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 1816374055
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x002 (SYN)

The packet bytes pane shows the raw data of the segment, including the sequence number field (0000) and the flag field (0002).

The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and gaia.cs.umass.edu.

The screenshot shows a Wireshark capture of a TCP segment. The packet list shows a SYN segment from 192.168.12.91 to 128.119.245.12. The packet details pane shows the TCP header with the Syn flag set to 1.

No.	Time	Source	Destination	Protocol	Length	Info
56	7.324098	3.234.27.88	192.168.12.91	TCP	60	443 → 54587 [FIN, ACK] Seq=1 Ack=2 Win=123 Len=0
57	7.324355	192.168.12.91	18.213.7.14	TCP	54	54589 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0
58	7.324602	192.168.12.91	3.234.27.88	TCP	54	54587 → 443 [ACK] Seq=2 Ack=2 Win=254 Len=0
75	11.067663	192.168.12.91	128.119.245.12	TCP	66	54592 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
76	11.068020	192.168.12.91	128.119.245.12	TCP	66	54593 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
94	11.110380	128.119.245.12	192.168.12.91	TCP	68	80 → 54593 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
95	11.110380	128.119.245.12	192.168.12.91	TCP	68	80 → 54592 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

1000 = Header Length: 32 bytes (8)

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.]

The Syn flag is set to 1 which indicates that this segment is a SYN segment.

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 screenshot shows a Wireshark capture of a TCP SYNACK segment. The packet list shows a SYNACK segment from 128.119.245.12 to 192.168.12.91. The packet details pane shows the TCP header with the Syn and Ack flags set.

No.	Time	Source	Destination	Protocol	Length	Info
76	11.068020	192.168.12.91	128.119.245.12	TCP	66	54593 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
94	11.110380	128.119.245.12	192.168.12.91	TCP	68	80 → 54593 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

> Frame 94: 68 bytes on wire (544 bits), 68 bytes captured (544) on interface 0

> Ethernet II, Src: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7), Dst: 192.168.12.91

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.91

> Transmission Control Protocol, Src Port: 80, Dst Port: 54593, Seq: 0, Ack: 1, Win: 29200, Len: 0

Source Port: 80

Destination Port: 54593

[Stream index: 3]

[Conversation completeness: Complete, NO_DATA (23)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 284014576

[Next Sequence Number: 1 (relative sequence number)]

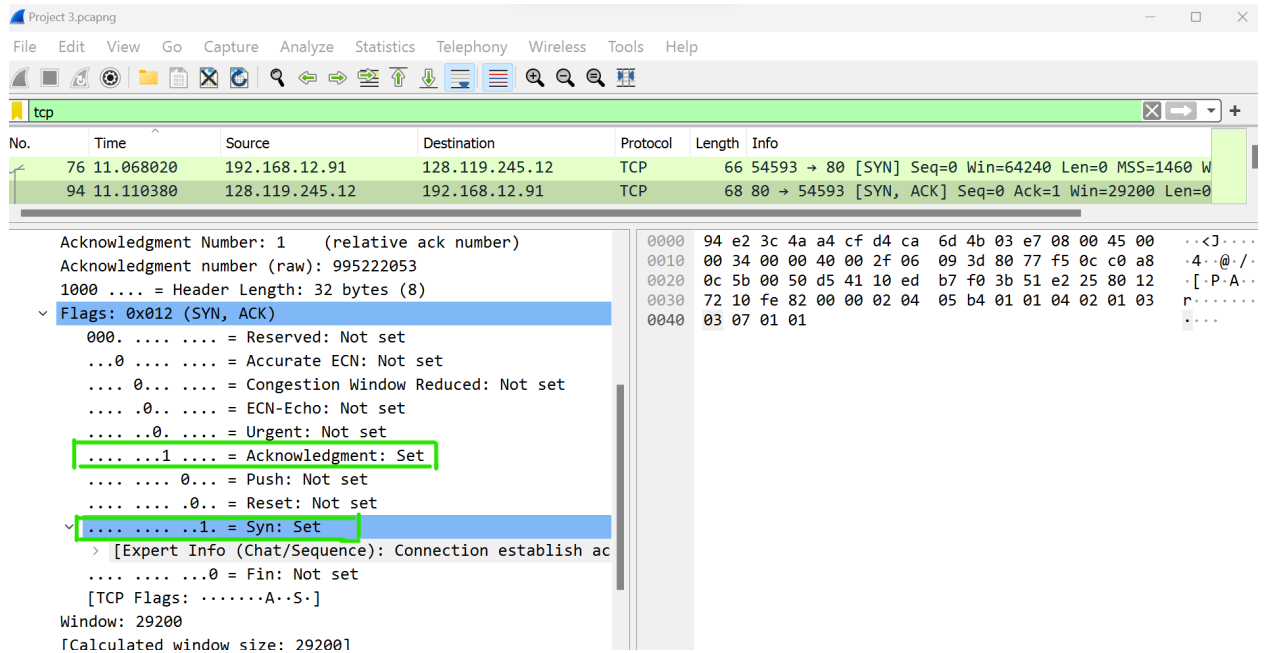
Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 995222053

1000 = Header Length: 32 bytes (8)

Flags: 0x012 (SYN, ACK)

- 000. = Reserved: Not set
- ...0 = Accurate ECN: Not set

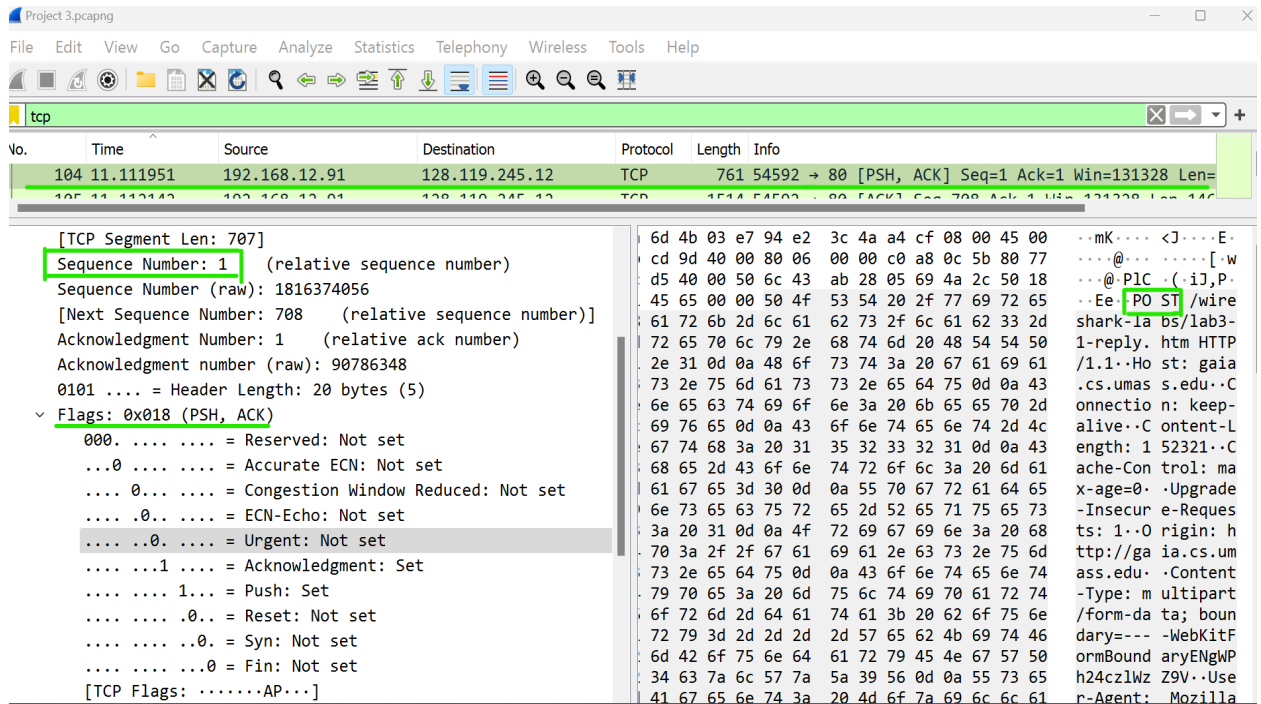


The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

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 the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segments from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the Acknowledgement field in the SYNACK segment is 1.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

- 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 segment No.104 contains the HTTP POST command, the sequence number of this segment is 1.

- 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? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation for all subsequent segments.

First six segments:

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
95	11.110380	128.119.245.12	192.168.12.91	TCP	68	80 → 54592 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
99	11.110566	192.168.12.91	128.119.245.12	TCP	54	54593 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
100	11.110604	192.168.12.91	128.119.245.12	TCP	54	54592 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
104	11.111951	192.168.12.91	128.119.245.12	TCP	761	54592 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=761
105	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=708 Ack=1 Win=131328 Len=146
106	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=2168 Ack=1 Win=131328 Len=14
107	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=3628 Ack=1 Win=131328 Len=14
108	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=5088 Ack=1 Win=131328 Len=14
109	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=6548 Ack=1 Win=131328 Len=14
110	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=8008 Ack=1 Win=131328 Len=14

> Frame 104: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits) on interface 0

> Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst: Routerbo_03:e7 (d4:ca:6d:4b:03:e7)

> Internet Protocol Version 4, Src: 192.168.12.91, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 54592, Dst Port: 80, Seq: 54592, Len: 761

0000 d4 ca 6d 4b 03 e7 94 e2 3c 4a a4 cf 08 00 45 00 ..mK...

0010 02 eb cd 9d 40 00 80 06 00 00 c0 a8 0c 5b 80 77 ...@...

0020 f5 0c d5 40 00 50 6c 43 ab 28 05 69 4a 2c 50 18 ...@P1

0030 02 01 45 65 00 00 50 4f 53 54 20 2f 77 69 72 65 ..Ee..P

0040 73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d shark-l

0050 31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 50 1-reply

0060 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 /1.1..H

0070 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43 .cs.uma

0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnecti

0090 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c alive..

00a0 65 6e 67 74 68 3a 20 31 35 32 33 32 31 0d 0a 43 length:

00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Co

ACK of first six segments:

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
110	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=8008 Ack=1 Win=131328 Len=14
111	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=9468 Ack=1 Win=131328 Len=14
112	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=10928 Ack=1 Win=131328 Len=1
113	11.112142	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=12388 Ack=1 Win=131328 Len=1
133	11.162316	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=708 Win=30720 Len=0
134	11.162316	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=6548 Win=42368 Len=0
135	11.162316	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=9468 Win=48256 Len=0
136	11.162316	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=13848 Win=56960 Len=0
137	11.162468	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=13848 Ack=1 Win=131328 Len=1
138	11.162468	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=15308 Ack=1 Win=131328 Len=1

> Frame 133: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> Ethernet II, Src: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7), Dst: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.91

> Transmission Control Protocol, Src Port: 80, Dst Port: 54592, Seq: 80, Len: 60

Source Port: 80

Destination Port: 54592

[Stream index: 2]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

0000 94 e2 3c 4a a4 cf d4 ca 6d 4b 03 e7 08 00 45 00 ..<J....

0010 00 28 50 49 40 00 2f 06 b8 ff 80 77 f5 0c c0 a8 ..(PI@./.

0020 0c 5b 00 50 d5 40 05 69 4a 2c 6c 43 ad eb 50 10 .[.P.@.i

0030 00 f0 2d 08 00 00 00 00 00 00 00 00

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
155	11.162468	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=40128 Ack=1 Win=131328 Len=1
169	11.191624	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=16768 Win=62848 Len=0
170	11.191624	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=18228 Win=65664 Len=0
171	11.191624	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=19688 Win=68608 Len=0
172	11.191624	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=25528 Win=80256 Len=0
173	11.191624	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [ACK] Seq=1 Ack=29908 Win=89088 Len=0
175	11.191841	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=41588 Ack=1 Win=131328 Len=1
176	11.191841	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=43048 Ack=1 Win=131328 Len=1
177	11.191841	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=44508 Ack=1 Win=131328 Len=1
178	11.191841	192.168.12.91	128.119.245.12	TCP	1514	54592 → 80 [ACK] Seq=45968 Ack=1 Win=131328 Len=1

> Frame 169: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> Ethernet II, Src: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7), Dst: 92:1b:1c:6a:70:12 (08:00:27:1b:1c:6a)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.91

> Transmission Control Protocol, Src Port: 80, Dst Port: 54592, Seq: 1, Len: 0

Source Port: 80

Destination Port: 54592

[Stream index: 2]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

0000 94 e2 3c 4a a4 cf d4 ca 6d 4b 03 e7 08 00 45 00 ...<J...

0010 00 28 50 4d 40 00 2f 06 b8 fb 80 77 f5 0c c0 a8 ... (PM@: /.

0020 0c 5b 00 50 d5 40 05 69 4a 2c 6c 43 ec a7 50 10 ...[.P:@:i

0030 01 eb ed 50 00 00 00 00 00 00 00 00 ...P....

The first six segments are no. 104, 105, 106, 107, 108 and 109. The ACK of the first six segments are no. 133, 134, 135, 136, 169 and 170.

Segment 1 sequence number is 1

Segment 2 sequence number is 708

Segment 3 sequence number is 2168

Segment 4 sequence number is 3628

Segment 5 sequence number is 5088

Segment 6 sequence number is 6548

	Sent Time	ACK Received Time	RTT
Segment 1	11.111951	11.162316	0.050365
Segment 2	11.112142	11.162316	0.050174
Segment 3	11.112142	11.162316	0.050174
Segment 4	11.112142	11.162316	0.050174

Segment 5	11.112142	11.191624	0.079482
Segment 6	11.112142	11.191624	0.079482

$$\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$$

EstimatedRTT after the receipt of the ACK of segment 1:

$$\text{EstimatedRTT} = \text{RTT for Segment 1} = 0.050365\text{s}$$

EstimatedRTT after the receipt of the ACK of segment 2:

$$\text{EstimatedRTT} = 0.875 * 0.050365 + 0.125 * 0.050174 = 0.050341125\text{s}$$

EstimatedRTT after the receipt of the ACK of segment 3:

$$\text{EstimatedRTT} = 0.875 * 0.050341125 + 0.125 * 0.050174 = 0.05032023437\text{s}$$

EstimatedRTT after the receipt of the ACK of segment 4:

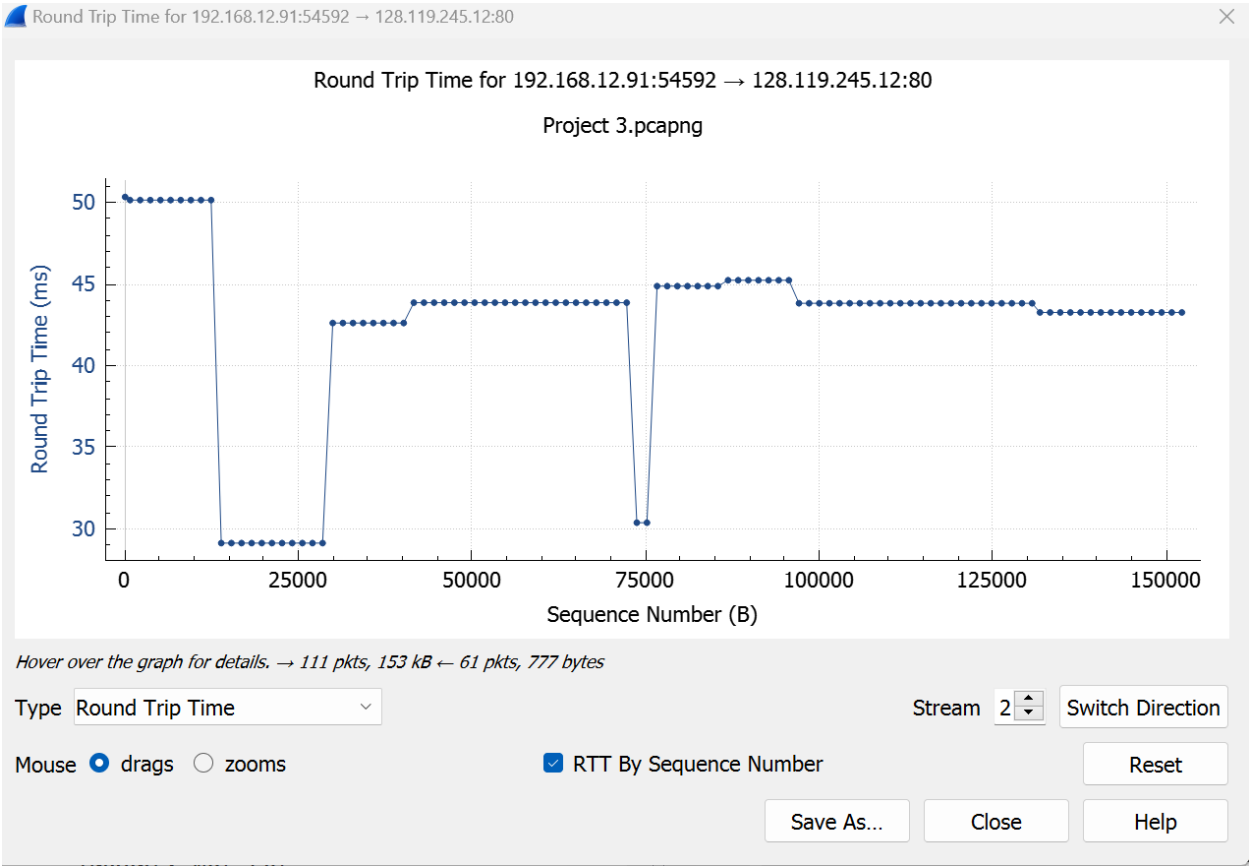
$$\text{EstimatedRTT} = 0.875 * 0.05032023437 + 0.125 * 0.050174 = 0.05030195507\text{s}$$

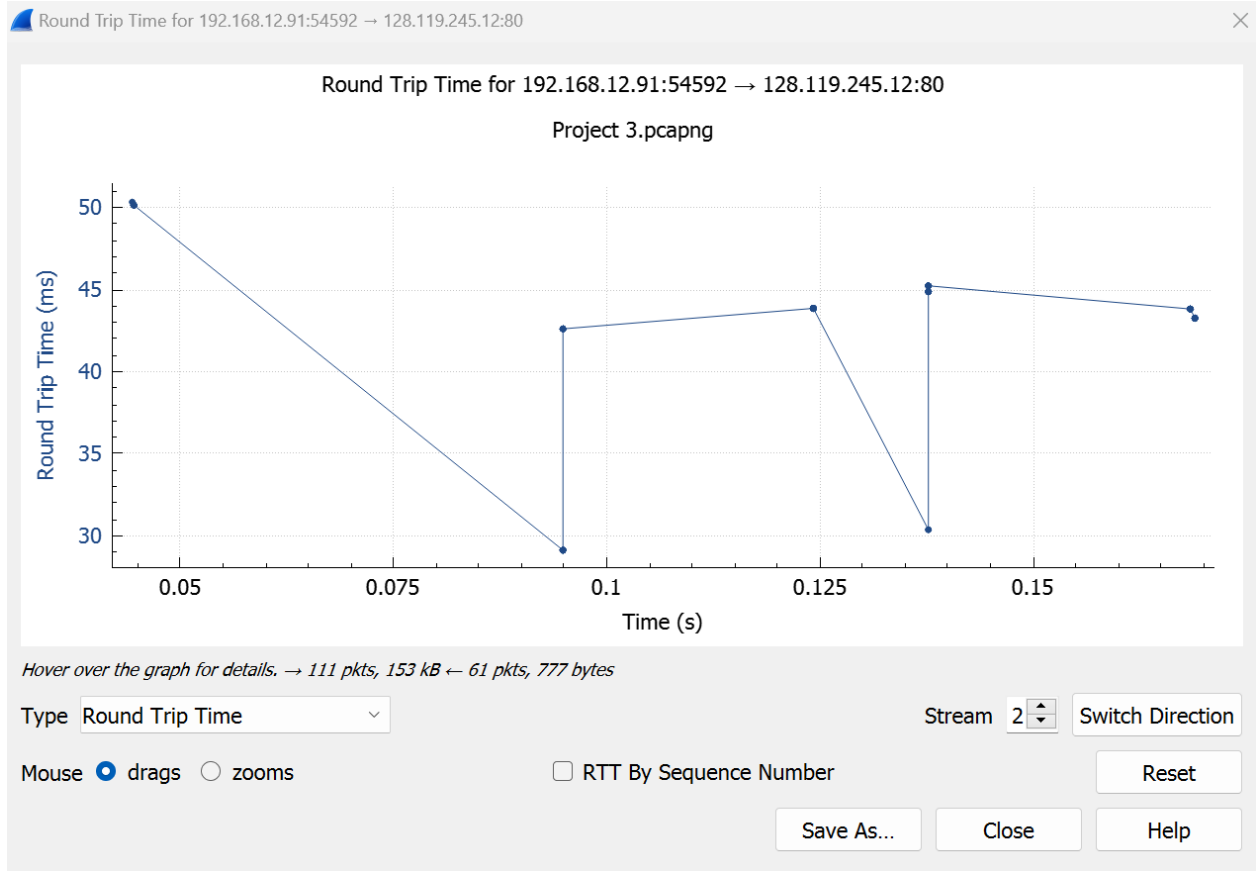
EstimatedRTT after the receipt of the ACK of segment 5:

$$\text{EstimatedRTT} = 0.875 * 0.05030195507 + 0.125 * 0.079482 = 0.05394946068\text{s}$$

EstimatedRTT after the receipt of the ACK of segment 6:

$$\text{EstimatedRTT} = 0.875 * 0.05394946068 + 0.125 * 0.079482 = 0.05714102809\text{s}$$





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

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

Time	Source	Destination	Protocol	Length	Info
100	11.110604	192.168.12.91	128.119.245.12	TCP	54 54592 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
104	11.111951	192.168.12.91	128.119.245.12	TCP	761 54592 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=707
105	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=708 Ack=1 Win=131328 Len=1460
106	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=2168 Ack=1 Win=131328 Len=1460
107	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=3628 Ack=1 Win=131328 Len=1460
108	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=5088 Ack=1 Win=131328 Len=1460
109	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=6548 Ack=1 Win=131328 Len=1460
110	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=8008 Ack=1 Win=131328 Len=1460
111	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=9468 Ack=1 Win=131328 Len=1460
112	11.112142	192.168.12.91	128.119.245.12	TCP	1514 54592 → 80 [ACK] Seq=10928 Ack=1 Win=131328 Len=1460

Acknowledgment number (raw): 90786348

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

- 0000 = Reserved: Not set
- 0000 = Accurate ECN: Not set
- 0000 = Congestion Window Reduced: Not set
- 0000 = ECN-Echo: Not set
- 0000 = Urgent: Not set
- 0001 = Acknowledgment: Set
- 0000 1... = Push: Set

0000 d4 ca 6d 4b 03 e7 94 e2 3c 4a a4 cf 08 00 45 00 ...mK...

0010 02 eb cd 9d 40 00 80 06 00 00 c0 a8 0c 5b 80 77 ...@...

0020 f5 0c d5 40 00 50 6c 43 ab 28 05 69 a4 2c 50 18 ...@P1

0030 02 01 45 65 00 00 50 4f 53 54 20 2f 77 69 72 65 ...Ee..P

0040 73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d shark-1

0050 31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 1-reply

0060 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 /1.1..H

0070 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43 .cs.uma

0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnecti

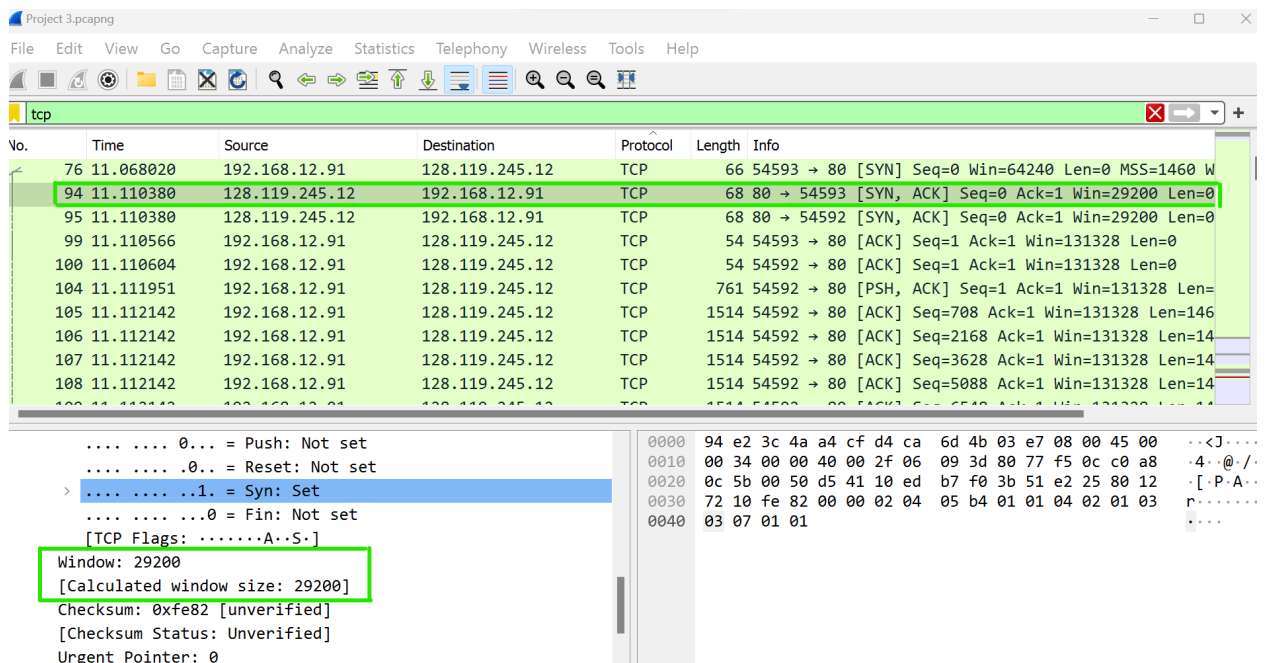
0090 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c alive..

00a0 65 6e 67 74 68 3a 20 31 35 32 33 32 31 0d 0a 43 length:

00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Co

The length of the first TCP segment is 707 bytes, the length of the second TCP segment is 1460 bytes, the length of the third TCP segment is 1460 bytes, the length of the fourth TCP segment is 1460 bytes, the length of the fifth TCP segment is 1460 bytes and the length of the sixth TCP segment is 1460 bytes.

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 image shows a Wireshark packet capture analysis of a TCP connection. The packet list pane displays several TCP segments. The details pane for the selected packet (No. 94) shows the following information:

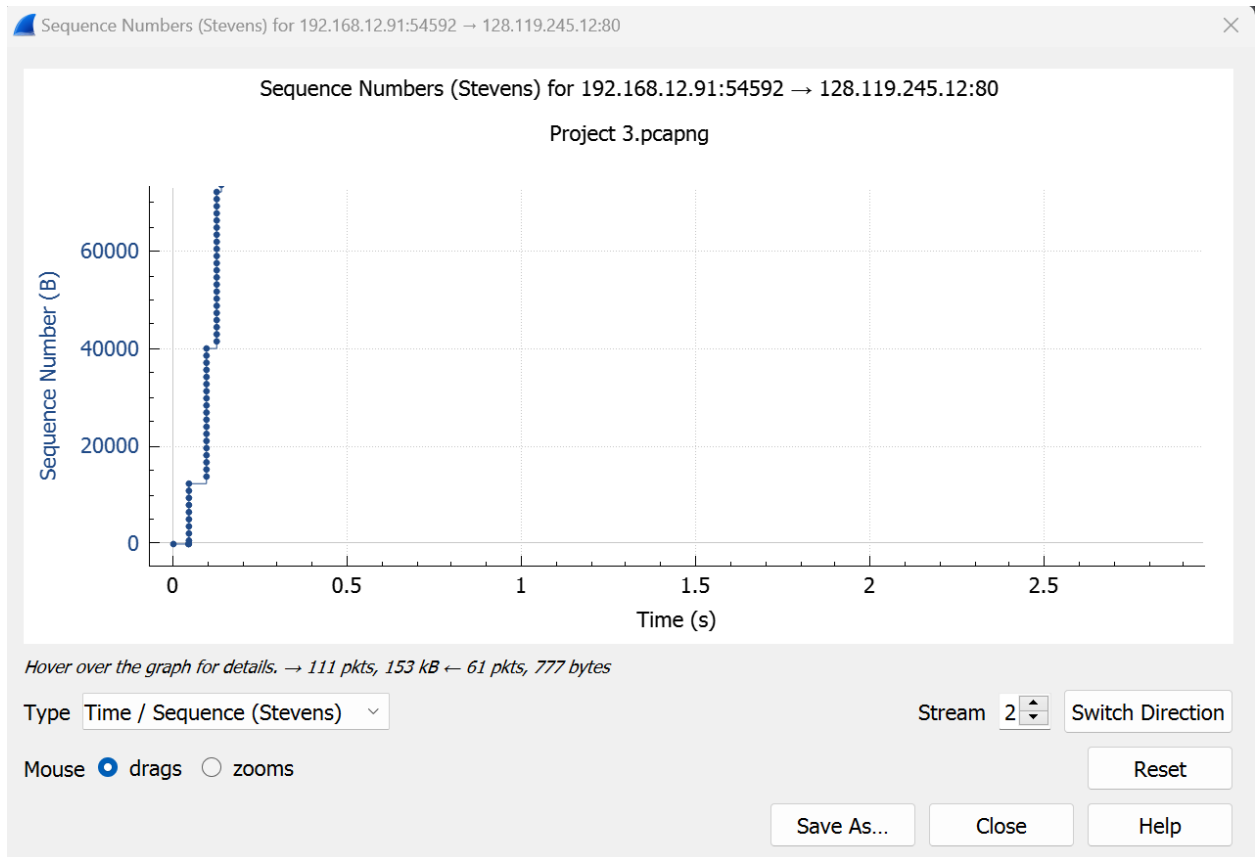
- Window: 29200
- [Calculated window size: 29200]
- Checksum: 0xfe82 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0

The packet details pane also shows the TCP flags: SYN, ACK, and the sequence number: 54593.

The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 29200 bytes. The sender is never throttled due to lacking of receiver buffer space.

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

There are no retransmitted segments in the trace file since in the time sequence graph (stevens), all sequence numbers are monotonically increasing.



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 difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs.

	Acknowledged sequence number	Acknowledged data
ACK 1	708	708
ACK 2	6548	5840
ACK 3	9468	2920
ACK 4	13848	4380
ACK 5	16768	2920
ACK 6	18228	1460

ACK 7	19688	1460
-------	-------	------

The receiver is ACKing every other segment. For example, segment No. 169 in the screenshot below.

The screenshot shows a Wireshark packet capture of a TCP connection. The packet list pane displays several segments, with segment 169 highlighted. The packet details pane for segment 169 shows the following information:

- Frame 169: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7), Dst: 192.168.12.91
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.91
- Transmission Control Protocol, Src Port: 80, Dst Port: 54592,
 - Source Port: 80
 - Destination Port: 54592
 - [Stream index: 2]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 0]
 - Sequence Number: 1 (relative sequence number)

12. What is the throughput (bytes transferred per unit time) for the TCP connection?

Explain how you calculated this value.

Project 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

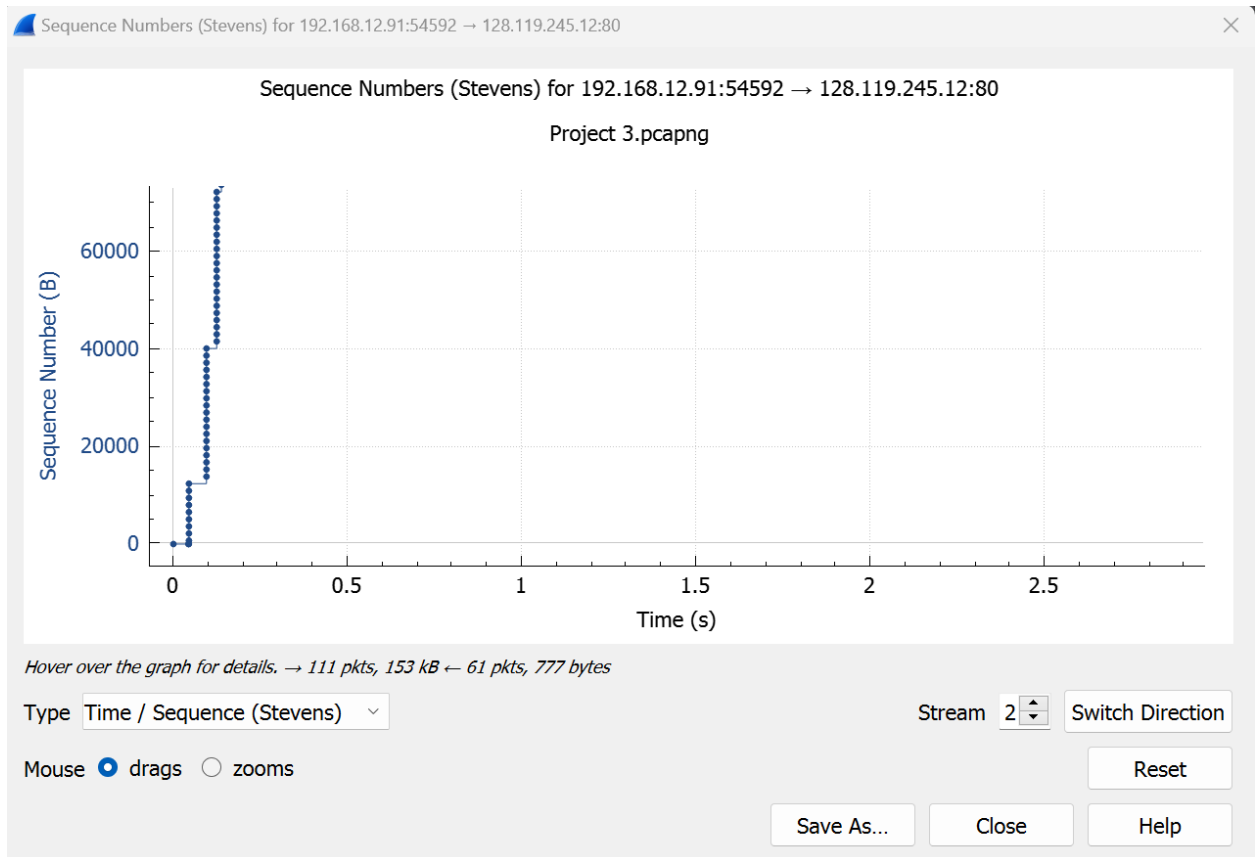
No.	Time	Source	Destination	Protocol	Length	Info
507	15.541899	192.168.12.91	18.213.7.14	TCP	54	54595 → 443 [ACK] Seq=518 Ack=112 Win=131072 Len=
510	15.542302	192.168.12.91	18.213.7.14	TCP	1514	54595 → 443 [ACK] Seq=674 Ack=157 Win=131072 Len=
514	15.565267	18.213.7.14	192.168.12.91	TCP	60	443 → 54595 [ACK] Seq=157 Ack=569 Win=28160 Len=0
518	15.583588	18.213.7.14	192.168.12.91	TCP	60	443 → 54595 [ACK] Seq=264 Ack=3381 Win=46080 Len=
520	15.599489	192.168.12.91	18.213.7.14	TCP	54	54595 → 443 [ACK] Seq=3419 Ack=601 Win=130560 Len=
572	16.291549	128.119.245.12	192.168.12.91	TCP	60	80 → 54592 [FIN, ACK] Seq=778 Ack=153029 Win=2935
573	16.291711	192.168.12.91	128.119.245.12	TCP	54	54592 → 80 [ACK] Seq=153029 Ack=779 Win=130560 Le
574	17.397275	192.168.12.91	128.119.245.12	TCP	54	54593 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=
575	17.397421	192.168.12.91	128.119.245.12	TCP	54	54592 → 80 [FIN, ACK] Seq=153029 Ack=779 Win=1305
576	17.397483	192.168.12.91	44.208.214.251	TCP	54	54594 → 443 [FIN, ACK] Seq=2020 Ack=6537 Win=1308

[Stream index: 2]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 778 (relative sequence number)
 Sequence Number (raw): 90787125
 [Next Sequence Number: 779 (relative sequence number)]
 Acknowledgment Number: 153029 (relative ack number)
 Acknowledgment number (raw): 1816527084
 0101 = Header Length: 20 bytes (5)
 Flags: 0x011 (FIN, ACK)

0000 94 e2 3c 4a a4 cf d4 ca 6d 4b 03 e7 08 00 45 00 ...<J....
 0010 00 28 50 83 40 00 2f 06 b8 c5 80 77 f5 0c c0 a8 ... (P@./..
 0020 0c 5b 00 50 d5 40 05 69 4d 35 6c 46 00 ec 50 11 ... [P@.i
 0030 08 f5 ce f5 00 00 00 00 00 00 00 00 00 00 00 00

The [FIN, ACK] packet no.572 shows an acknowledgement number of 153029, which means 153029 bytes were acknowledged. The time on this message is 16.291549. So an approximate average throughput can be calculated as $153029 \text{ bytes} / 16.291549 \text{ seconds} = 9393.15224108 \text{ bytes/seconds}$ for this connection.

- 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 slow start 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.**



The slow start of the TCP seems to begin at about 0.01 seconds and then ends at about 0.2 seconds. Congestion avoidance takes over at about 0.3 seconds because it cuts down the amount being sent.

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

When we have a lot of traffic on the network TCP sender uses AIMD algorithm for the reduction of window size.