

LAB 2 Assignment:

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

Answering the following questions, by opening the Wireshark captured packet file Tcp- Ethernet-trace-1 in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

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?

→ The IP address of the client computer is 192.168.1.102 and the TCP port used is 1161

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?

→ The IP address of the gaia.cs.umass.edu is 128.119.245.12 and the dest port used is 80.

Able to create my own trace:

Using my own Trace:

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?

The IP address of my client computer is 10.182.178.36 and the tcp port used is 53990.

The image shows a Wireshark packet capture window. The top pane displays a list of packets. Packet 607 is selected, showing an HTTP POST request from 10.182.178.36 to 128.119.245.12 on port 80. The middle pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
68	14:41:13.557210	10.182.178.36	128.119.245.12	HTTP	525	GET /wireshark-labs/TCP-wireshark-file1.html HTTP/1...
78	14:41:13.603524	128.119.245.12	10.182.178.36	HTTP	842	HTTP/1.1 200 OK (text/html)
89	14:41:13.730744	10.182.178.36	128.119.245.12	HTTP	471	GET /favicon.ico HTTP/1.1
91	14:41:13.774875	128.119.245.12	10.182.178.36	HTTP	538	HTTP/1.1 404 Not Found (text/html)
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (te...
618	14:42:11.334911	128.119.245.12	10.182.178.36	HTTP	831	HTTP/1.1 200 OK (text/html)

Frame 607: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA48}

Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

Internet Protocol Version 4, Src: 10.182.178.36, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 53990, Dst Port: 80, Seq: 152556, Ack: 1, Len: 473

Source Port: 53990

Destination Port: 80

[Stream index: 28]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 473]

0020 f5 0c d2 e6 00 50 9b b4 bf 42 30 64 57 3f 50 18P...B0dw?P.

0030 fa f0 34 52 00 00 20 73 69 6d 70 6c 65 20 61 6e ...4R...s imple an

0040 64 0d 0a 6c 6f 76 69 6e 67 20 68 65 61 72 74 20 d...lovin g heart

0050 6f 66 20 68 65 72 20 63 68 69 6c 64 68 6f 6f 64 of her c hildhood

0060 3a 20 20 61 6e 64 20 68 6f 77 20 73 68 65 20 77 : and h ow she w

0070 6f 75 6c 64 20 67 61 74 68 65 72 20 61 62 6f 75 ould gat her abou

Frame (527 bytes) Reassembled TCP (153028 bytes)

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 sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu to upload the file is 0.

→ In the flag section of the TCP segment, the SYN bit set to 1 identifies the segment as SYN segment.
(marked red in the screenshot)

No.	Time	Source	Destination	Protocol	Length	Info
423	14:42:10.945187	10.182.178.36	128.119.245.12	TCP	66	53990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14...
424	14:42:10.946137	10.182.178.36	128.119.245.12	TCP	66	53991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14...
437	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53984 [ACK] Seq=2680 Ack=890 Win=32120 L...
438	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53983 [ACK] Seq=2 Ack=2 Win=32120 Len=0
457	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53991 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
458	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
459	14:42:11.063920	10.182.178.36	128.119.245.12	TCP	54	53991 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

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

.... 0... = Urgent: Not set

.... 0... = Acknowledgment: Not set

.... 0... = Push: Not set

.... 0... = Reset: Not set

.... 1... = **Syn: Set**

> [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]

.... 0... = Fin: Not set

[TCP Flags:S.]

0000 00 00 5e 00 01 01 00 d4 9e 53 8f c2 08 00 45 00 ..^.....S....E.
0010 00 34 e2 3d 40 00 80 06 00 00 0a b6 b2 24 80 77 .4.=@...\$..w
0020 f5 0c d2 e6 00 50 9b b2 6b 56 00 00 00 80 02P...kV....
0030 fa f0 32 85 00 00 02 04 05 b4 01 03 03 08 01 01 ..2.....
0040 04 02 ..

Transmission Control Protocol: ProtocolPackets: 701 · Displayed: 510 (72.8%)Profile: Default

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?

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

No.	Time	Source	Destination	Protocol	Length	Info
457	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53991 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
458	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
459	14:42:11.063920	10.182.178.36	128.119.245.12	TCP	54	53991 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
460	14:42:11.064071	10.182.178.36	128.119.245.12	TCP	54	53990 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
461	14:42:11.065386	10.182.178.36	128.119.245.12	TCP	761	53990 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 L...
463	14:42:11.067262	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=708 Ack=1 Win=64240 Len=...
464	14:42:11.067262	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=2114 Ack=1 Win=64240 Len=...

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.182.178.36

Transmission Control Protocol, Src Port: 80, Dst Port: 53990, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 53990

[Stream index: 28]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 811882302

0000 00 d4 9e 53 8f c2 d4 04 ff 27 f3 f0 08 00 45 00 ...S....I...E.
0010 00 2c b1 24 00 2a 06 ad 49 80 77 f5 0c 0a b6 ..\$.*..I.w....
0020 b2 24 00 50 d2 e6 30 64 57 3e 9b b2 6b 57 60 12 ..\$.P...dW>..kW..
0030 7d 78 86 92 00 00 02 04 05 7ex.....~

What is the value of the Acknowledgement field in the SYNACK segment?

→ the value of the Acknowledgement field in the SYNACK segment id 1.

No.	Time	Source	Destination	Protocol	Length	Info
457	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53991 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
458	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=32120 L...
459	14:42:11.063920	10.182.178.36	128.119.245.12	TCP	54	53991 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
460	14:42:11.064071	10.182.178.36	128.119.245.12	TCP	54	53990 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
461	14:42:11.065386	10.182.178.36	128.119.245.12	TCP	761	53990 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 L...
463	14:42:11.067262	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=708 Ack=1 Win=64240 Len=...
464	14:42:11.067262	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=2114 Ack=1 Win=64240 Len=...

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

How did gaia.cs.umass.edu determine that value?

→ Since the sequence number from the client 10.182.178.36 had initial seq number as 0, hence the Acknowledgement from the gaia.cs.umass.edu server for the received segment from the client hence seq number is 0 and The server adds 1 to the sequence number of SYN tcp segments to give value 1 and SYN bit is 1.

What is it in the segment that identifies the segment as a SYNACK segment?

→ the Segment that identifies the segment as a SYNACK segment is the flag field in the TCP segment has Acknowledge and Syn bit set to 1 (shown in above screenshot)

6. What is the sequence number of the TCP segment containing the HTTP POST command?

→ the sequence number of TCP segment containing the HTTP POST command is 152556

No.	Time	Source	Destination	Protocol	Length	Info
68	14:41:13.557210	10.182.178.36	128.119.245.12	HTTP	525	GET /wireshark-labs/TCP-wireshark-file1.html HTTP/1...
78	14:41:13.603524	128.119.245.12	10.182.178.36	HTTP	842	HTTP/1.1 200 OK (text/html)
89	14:41:13.730744	10.182.178.36	128.119.245.12	HTTP	471	GET /favicon.ico HTTP/1.1
91	14:41:13.774875	128.119.245.12	10.182.178.36	HTTP	538	HTTP/1.1 404 Not Found (text/html)
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (te...
618	14:42:11.334911	128.119.245.12	10.182.178.36	HTTP	831	HTTP/1.1 200 OK (text/html)

> Internet Protocol Version 4, Src: 10.182.178.36, Dst: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 53990, Dst Port: 80, Seq: 152556, Ack: 1, Len: 473

Source Port: 53990
Destination Port: 80
[Stream index: 28]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 473]
Sequence Number: 152556 (relative sequence number)
Sequence Number (raw): 2612313922

0020	f5 0c d2 e6 00 50 9b b4	bf 42 30 64 57 3f 50 18P...B0dW?P-
0030	fa f0 34 52 00 00 20 73	69 6d 70 6c 65 20 61 6e	..4R... s imple an
0040	64 0d 0a 6c 6f 76 69 6e	67 20 68 65 61 72 74 20	d..lovin g heart
0050	6f 66 20 68 65 72 20 63	68 69 6c 64 68 6f 6f 64	of her c hildhood
0060	3a 20 20 61 6e 64 20 68	6f 77 20 73 68 65 20 77	: and h ow she w
0070	6f 75 6c 64 20 67 61 74	68 65 72 20 61 62 6f 75	ould gat her abou

Frame (527 bytes) Reassembled TCP (153028 bytes)

7. 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)?

→ The trace no of the first six segments are No: 602, 603, 604, 605, 606, 607

The sequence number for first six segments are 145526, 146932, 148338, 149744, 151150, 152556

The image shows a Wireshark packet capture window titled 'lab2.pcapng'. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
602	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=145526 Ack=1 Win=64240 Len=0
603	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [PSH, ACK] Seq=146932 Ack=1 Win=64240 Len=0
604	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=148338 Ack=1 Win=64240 Len=0
605	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=149744 Ack=1 Win=64240 Len=0
606	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=151150 Ack=1 Win=64240 Len=0
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
608	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=125842 Win=30714 Len=0

The packet details pane for packet 607 shows the following information:

- Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
- Source: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.182.178.36, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 53990, Dst Port: 80, Seq: 152556, Ack: 1, Len: 473
- Source Port: 53990
- Destination Port: 80
- [Stream index: 28]
- Conversation completeness: Complete. WITH DATA (31)

The packet bytes pane shows the raw data of the HTTP POST request, including the status bar: Frame (527 bytes) Reassembled TCP (153028 bytes).

At what time was each segment sent?

→ The segment with trace no 602, 603, 604, 605, 606, 607 was sent at 14:42:11.148790

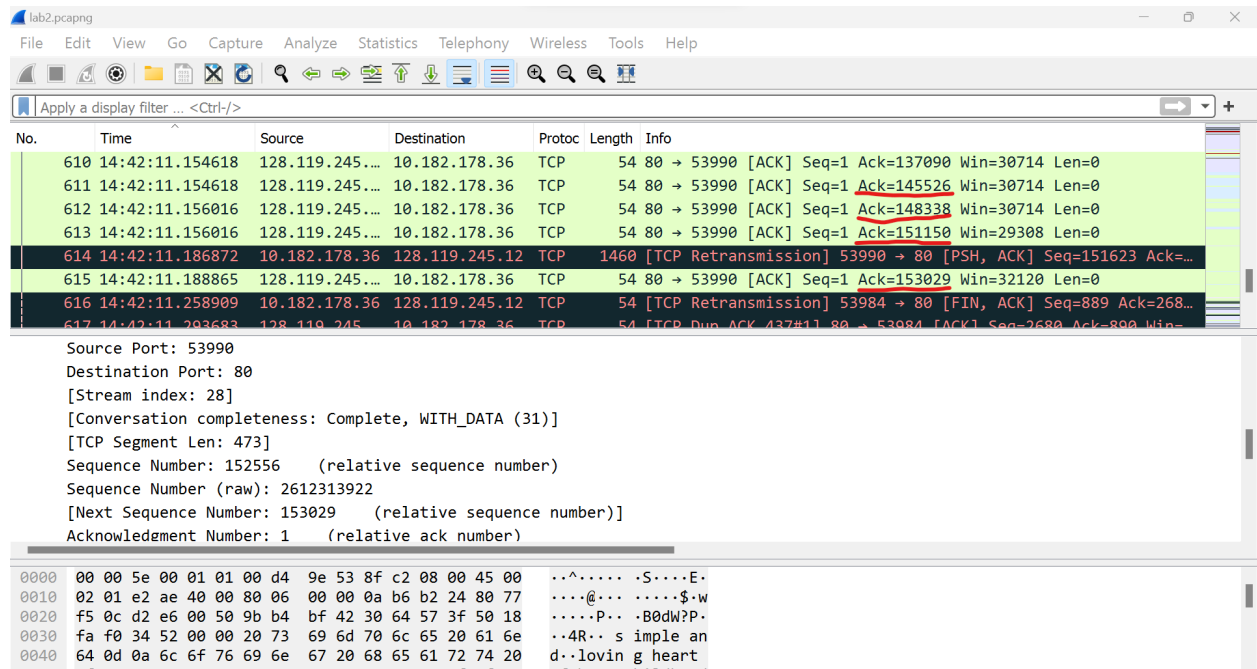
When was the ACK for each segment received?

→ The Ack for segment with trace no 602 is trace no 611 with acknowledgement number as 145526.

The Ack for segment with trace no 603, 604 is trace no 612 with acknowledgement number as 148338.

The Ack for segment with trace no 605, 606 is trace no 613 with acknowledgement number as 151150.

The Ack for segment with trace no 607 is the trace no 615 with acknowledgement number as 153029.



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?

→

Segment Trace no	Sent time	Acknowledged time	RTT in sec
602	14:42:11.148790	14:42:11.154618	0.005828
603	14:42:11.148790	14:42:11.156016	0.007226
604	14:42:11.148790	14:42:11.156016	0.007226
605	14:42:11.148790	14:42:11.156016	0.007226
606	14:42:11.148790	14:42:11.156016	0.007226
607	14:42:11.148790	14:42:11.188865	0.040075

Sent time screenshot:

No.	Time	Source	Destination	Protoc	Length	Info
601	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=144120 Ack=1 Win=64240 Len=1406 [TCP ...
602	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=145526 Ack=1 Win=64240 Len=1406 [TCP ...
603	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [PSH, ACK] Seq=146932 Ack=1 Win=64240 Len=1406 ...
604	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=148338 Ack=1 Win=64240 Len=1406 [TCP ...
605	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=149744 Ack=1 Win=64240 Len=1406 [TCP ...
606	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=151150 Ack=1 Win=64240 Len=1406 [TCP ...
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plai...
608	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=125842 Win=30714 Len=0

Arrival Time: Oct 13, 2022 14:42:11.188865000 Central Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1665690131.188865000 seconds
 [Time delta from previous captured frame: 0.001993000 seconds]
 [Time delta from previous displayed frame: 0.001993000 seconds]
 [Time since reference or first frame: 65.189982000 seconds]
 Frame Number: 615
 Frame Length: 54 bytes (432 bits)
 Capture Length: 54 bytes (432 bits)

```

0000  00 d4 9e 53 8f c2 d4 04 ff 27 f3 f0 08 00 45 00  ...S....'....E.
0010  00 28 b6 eb 00 00 2a 06 a7 86 80 77 f5 0c 0a b6  .(....*. ...w...
0020  b2 24 00 50 d2 e6 30 64 57 3f 9b b4 c1 1b 50 10  .$.P..0d W?...P.
0030  7d 78 48 53 00 00                                }xHS..
  
```

Acknowledgement time screenshot:

No.	Time	Source	Destination	Protoc	Length	Info
609	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=128654 Win=30714 Len=0
610	14:42:11.154618	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=137090 Win=30714 Len=0
611	14:42:11.154618	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=145526 Win=30714 Len=0
612	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=148338 Win=30714 Len=0
613	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=151150 Win=29308 Len=0
614	14:42:11.186872	10.182.178.36	128.119.245.12	TCP	1460	[TCP Retransmission] 53990 → 80 [PSH, ACK] Seq=151623 Ack=...
615	14:42:11.188865	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=153029 Win=32120 Len=0
616	14:42:11.258000	10.182.178.36	128.119.245.12	TCP	54	[TCP Retransmission] 53990 → 80 [FIN, ACK] Seq=880 Ack=268

Arrival Time: Oct 13, 2022 14:42:11.188865000 Central Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1665690131.188865000 seconds
 [Time delta from previous captured frame: 0.001993000 seconds]
 [Time delta from previous displayed frame: 0.001993000 seconds]
 [Time since reference or first frame: 65.189982000 seconds]
 Frame Number: 615
 Frame Length: 54 bytes (432 bits)
 Capture Length: 54 bytes (432 bits)

```

0000  00 d4 9e 53 8f c2 d4 04 ff 27 f3 f0 08 00 45 00  ...S....'....E.
0010  00 28 b6 eb 00 00 2a 06 a7 86 80 77 f5 0c 0a b6  .(....*. ...w...
0020  b2 24 00 50 d2 e6 30 64 57 3f 9b b4 c1 1b 50 10  .$.P..0d W?...P.
0030  7d 78 48 53 00 00                                }xHS..
  
```

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,

→

The formula for the EstimatedRTT is $\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$

EstimatedRTT after the receipt of the ACK of segment 1:

$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.005828 + 0.125 * 0.005828 \\ &= 0.0050995 + 0.0007285 \\ &= 0.005828 \text{ sec}\end{aligned}$$

EstimatedRTT after the receipt of the ACK of segment 2:

$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.005828 + 0.125 * 0.007226 \\ &= 0.00600275 \text{ sec}\end{aligned}$$

EstimatedRTT after the receipt of the ACK of segment 3:

$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.00600275 + 0.125 * 0.007226 \\ &= 0.0061556563 \text{ sec}\end{aligned}$$

EstimatedRTT after the receipt of the ACK of segment 4:

$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.0061556563 + 0.125 * 0.007226 \\ &= 0.0062894493 \text{ sec}\end{aligned}$$

EstimatedRTT after the receipt of the ACK of segment 5:

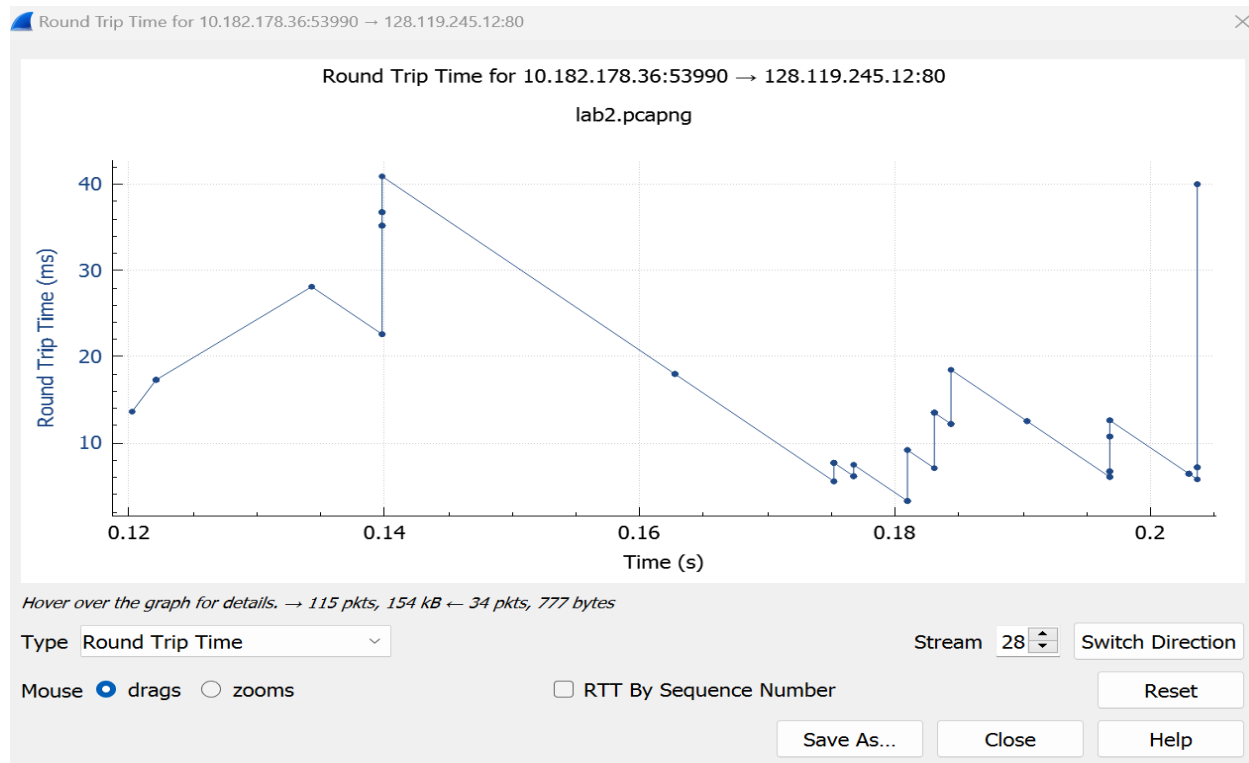
$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.0062894493 + 0.125 * 0.007226 \\ &= 0.0064065181 \text{ sec}\end{aligned}$$

EstimatedRTT after the receipt of the ACK of segment 6:

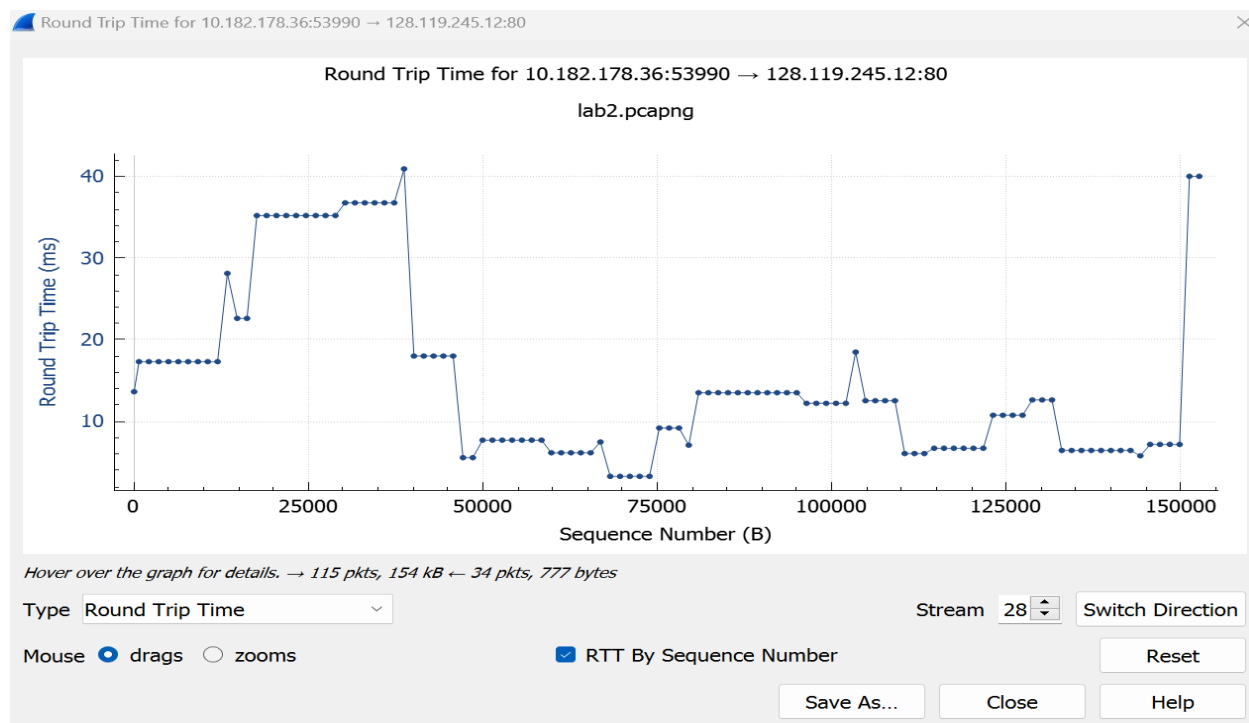
$$\begin{aligned}\text{EstimatedRTT} &= 0.875 * 0.0064065181 + 0.125 * 0.040075 \\ &= 0.0106150783 \text{ sec}\end{aligned}$$

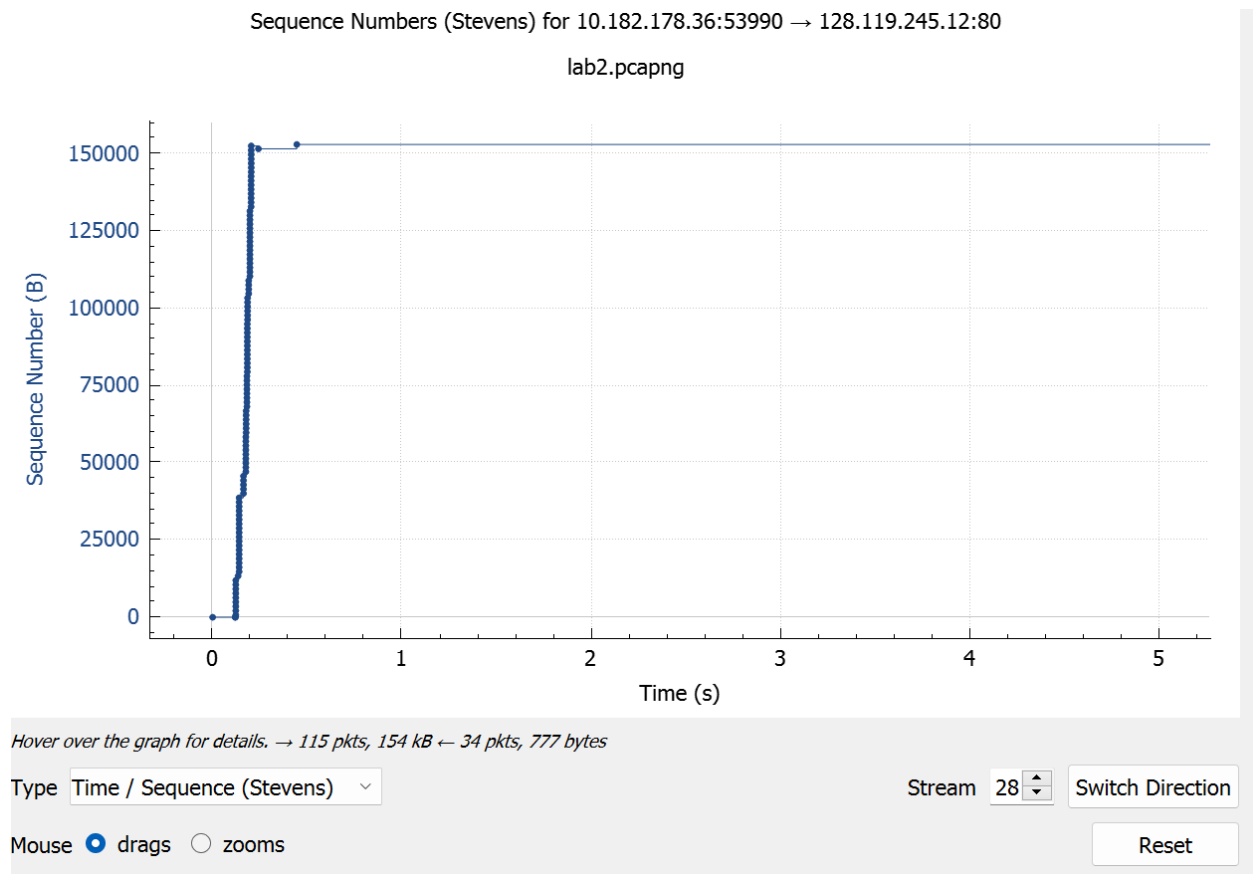
Graph:

The Round Trip time 10.182.178.36:53990 to 128.119.245.12:80 where X-axis is Time in s and Y axis is RTT in ms



The Round Trip time 10.182.178.36:53990 to 128.119.245.12:80 where X-axis is Sequence number in B and Y axis is RTT in ms





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

→

Segment Trace No	Length in bytes
602	1460
603	1460
604	1460
605	1460
606	1460
607	527 – HTTP Post

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protoc	Length	Info
602	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=145526 Ack=1 Win=64240 Len=1406 [TCP ...
603	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [PSH, ACK] Seq=146932 Ack=1 Win=64240 Len=1406 ...
604	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=148338 Ack=1 Win=64240 Len=1406 [TCP ...
605	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=149744 Ack=1 Win=64240 Len=1406 [TCP ...
606	14:42:11.148790	10.182.178.36	128.119.245.12	TCP	1460	53990 → 80 [ACK] Seq=151150 Ack=1 Win=64240 Len=1406 [TCP ...
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plai...
608	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=125842 Win=30714 Len=0
609	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=128654 Win=30714 Len=0

Frame 607: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}

Interface id: 0 (\Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 13, 2022 14:42:11.148790000 Central Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1665690131.148790000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 65.149907000 seconds]

```

0000  00 00 5e 00 01 01 00 d4 9e 53 8f c2 08 00 45 00  ..^.... .S....E.
0010  02 01 e2 ae 40 00 80 06 00 00 0a b6 b2 24 80 77  .@... ..$.w
0020  f5 0c d2 e6 00 50 9b b4 bf 42 30 64 57 3f 50 18  ....P...B0dW?P.
0030  fa f0 34 52 00 00 20 73 69 6d 70 6c 65 20 61 6e  ..4R.. s imple an
0040  64 0d 0a 6c 6f 76 69 6e 67 20 68 65 61 72 74 20  d..lovin g heart
0050  6f 66 20 68 65 72 20 63 68 69 6c 64 68 6f 6f 64  of her c hildhood

```

Frame (527 bytes) Reassembled TCP (153028 bytes)

9. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

→ The minimum amount of available buffer space advertised at the receiver for the entire trace is seen in the first ACK Received from the server, Its value is 32120

This receiver window grows until it reaches the maximum receiver buffer size.

According to the trace, the sender is never throttled due to lacking of receiver buffer space.

tcp

No.	Time	Source	Destination	Protoc	Length	Info
421	14:42:10.943562	10.182.178.36	128.119.245.12	TCP	54	53983 → 80 [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
422	14:42:10.944003	10.182.178.36	128.119.245.12	TCP	54	53984 → 80 [FIN, ACK] Seq=889 Ack=2680 Win=64192 Len=0
423	14:42:10.945187	10.182.178.36	128.119.245.12	TCP	66	53990 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
424	14:42:10.946137	10.182.178.36	128.119.245.12	TCP	66	53991 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
437	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53984 [ACK] Seq=2680 Ack=890 Win=32120 Len=0
438	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53983 [ACK] Seq=2 Ack=2 Win=32120 Len=0
457	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53991 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1406
458	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1406

....1.... = Acknowledgment: Set

....0... = Push: Not set

....0... = Reset: Not set

>1... = Syn: Set

....0... = Fin: Not set

[TCP Flags:A..S.]

Window: 32120

[Calculated window size: 32120]

Checksum: 0x35f7 [unverified]

```

0000  00 d4 9e 53 8f c2 d4 04 ff 27 f3 f0 08 00 45 00  ...S.... ..'.E.
0010  00 2c b2 84 00 00 2a 06 ab e9 80 77 f5 0c 0a b6  .,....*. ..w....
0020  b2 24 00 50 d2 e7 c5 3a f5 6c 4e ad d5 f1 60 12  $.P.... .1N....
0030  7d 78 35 f7 00 00 02 04 05 7e                    }x5..... ~

```

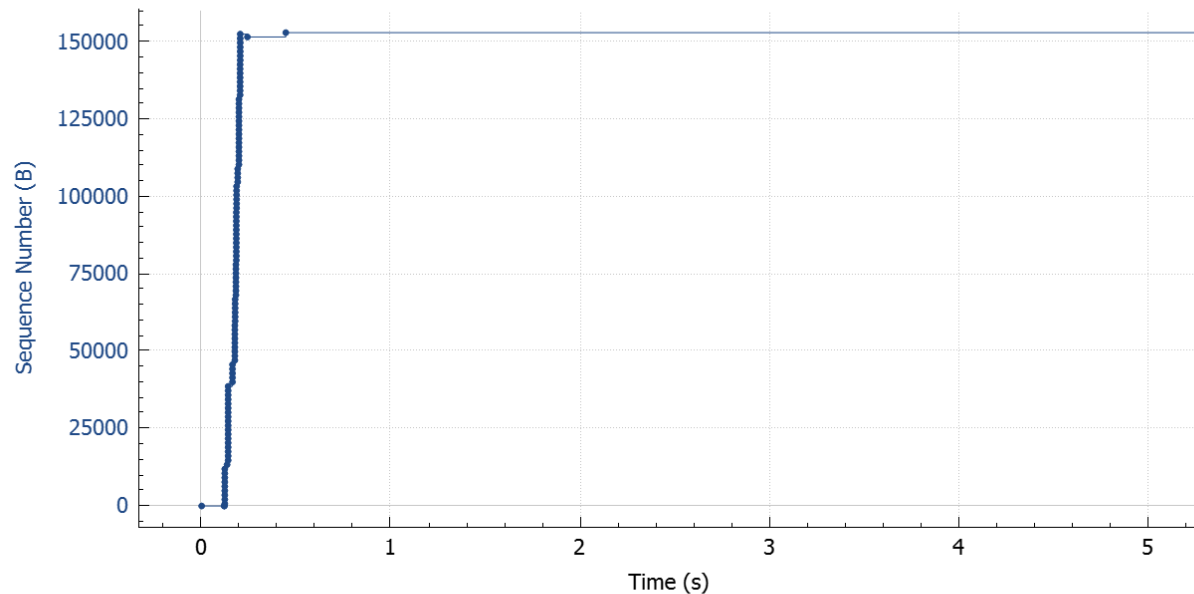
10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to

answer this question?

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

Sequence Numbers (Stevens) for 10.182.178.36:53990 → 128.119.245.12:80

lab2.pcapng



Hover over the graph for details. → 115 pkts, 154 kB ← 34 pkts, 777 bytes

Type Time / Sequence (Stevens) ▾

Stream 28 ▾

Switch Direction

Mouse ☒ drags ☐ zooms

Reset

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

Trace No	Ack Sequence number	Acknowledged data in bytes
477	708	708
479	4926	4218
480	9144	4218
481	13362	4218
504	17580	4218
510	21798	4218
511	26016	4218

512	30234	4218
522	38670	8436
530	47106	8436
531	49918	2812
540	61166	11248
541	66790	5624
554	72414	5624
555	75226	2812
562	78038	2812
563	80850	2812
569	89286	8436
570	97722	8436
571	103346	5624
589	106158	2812
590	114594	8436
599	120218	5624
600	123030	2812
608	125842	2812
609	128654	2812
610	137090	8436
611	145526	8436
612	148338	2812
613	151150	2812
615	153029	1879

→ One of the case where the receiver is ACKing every other received segment is
In the Ack sequence number 137090 acknowledges the 3 times the 2812.

No.	Time	Source	Destination	Protoc	Length	Info
607	14:42:11.148790	10.182.178.36	128.119.245.12	HTTP	527	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plai...
608	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=125842 Win=30714 Len=0
609	14:42:11.152741	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=128654 Win=30714 Len=0
610	14:42:11.154618	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=137090 Win=30714 Len=0
611	14:42:11.154618	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=145526 Win=30714 Len=0
612	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=148338 Win=30714 Len=0
613	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=151150 Win=29308 Len=0
614	14:42:11.186872	10.182.178.36	128.119.245.12	TCP	1460	[TCP Retransmission] 53990 → 80 [PSH, ACK] Seq=151623 Ack=...

Frame 612: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}

> Interface id: 0 (\Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 13, 2022 14:42:11.156016000 Central Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1665690131.156016000 seconds

[Time delta from previous captured frame: 0.001398000 seconds]

[Time delta from previous displayed frame: 0.001398000 seconds]

[Time since reference or first frame: 65.157133000 seconds]

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

→ The Tcp throughput for the tcp connection is calculated by considering the Total bytes transferred per unit time. So the total amount of data transmitted can be computed by the difference between the sequence number of first tcp Segment (ie value is 1) and the last ACK acknowledged sequence number (value is 153029). The value is shown in the screenshot below.

No.	Time	Source	Destination	Protocol	Length	Info
437	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53984 [ACK] Seq=2680 Ack=890 Win=32120 Len=0
438	14:42:11.017074	128.119.245.12	10.182.178.36	TCP	54	80 → 53983 [ACK] Seq=2 Ack=2 Win=32120 Len=0
457	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53991 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0
458	14:42:11.063440	128.119.245.12	10.182.178.36	TCP	58	80 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0
459	14:42:11.063920	10.182.178.36	128.119.245.12	TCP	54	53991 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
460	14:42:11.064071	10.182.178.36	128.119.245.12	TCP	54	53990 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

> Frame 459: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}

> Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

> Internet Protocol Version 4, Src: 10.182.178.36, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 53991, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
612	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=148338 Win=30714 Len=0
613	14:42:11.156016	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=151150 Win=29308 Len=0
614	14:42:11.186872	10.182.178.36	128.119.245.12	TCP	1460	[TCP Retransmission] 53990 → 80 [PSH, ACK] Seq=...
615	14:42:11.188865	128.119.245.12	10.182.178.36	TCP	54	80 → 53990 [ACK] Seq=1 Ack=153029 Win=32120 Len=0
616	14:42:11.258909	10.182.178.36	128.119.245.12	TCP	54	[TCP Retransmission] 53984 → 80 [FIN, ACK] Seq=...
617	14:42:11.293683	128.119.245.12	10.182.178.36	TCP	54	[TCP Dup ACK 437#1] 80 → 53984 [ACK] Seq=2680 A...

> Frame 615: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}

> Ethernet II, Src: JuniperN_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.182.178.36

> Transmission Control Protocol, Src Port: 80, Dst Port: 53990, Seq: 1, Ack: 153029, Len: 0

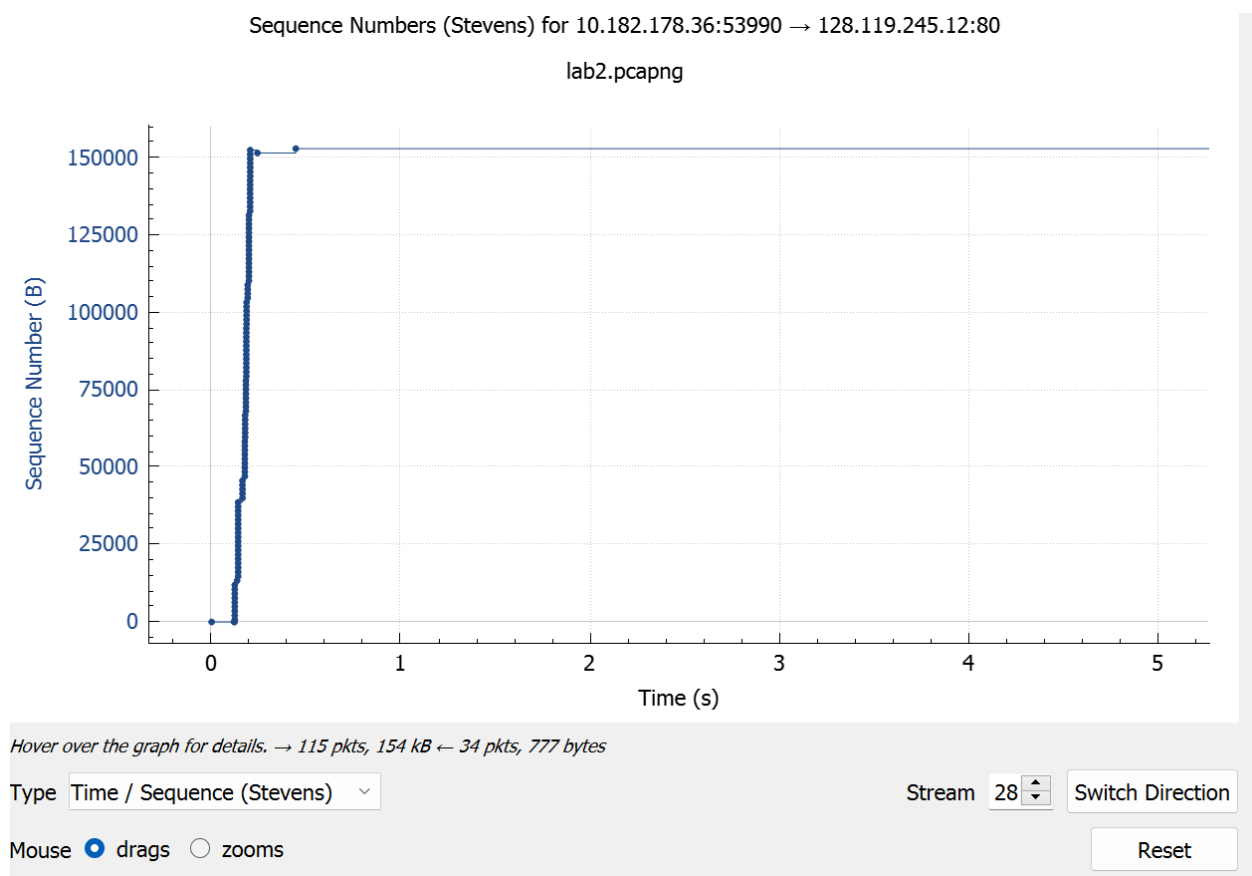
The time difference is calculated by the difference between the time of the first TCP segment (ie 14.42.11:063920 sec) And the last ACK segment(ie 14.42.11.188865 secs) as shown in the above screenshot.

$$\text{Throughput} = \frac{\text{total amount of data in bytes}}{\text{Total amount taken in seconds}} = \frac{153029 - 1}{0.188865 - 0.063920} = \frac{153028 \text{ bytes}}{0.124945 \text{ secs}} = 1224762.8956 \text{ bytes/sec} = 1.224 \text{ Megabytes/secs}$$

TCP congestion control in action:

Time-Sequence-Graph(Stevens):

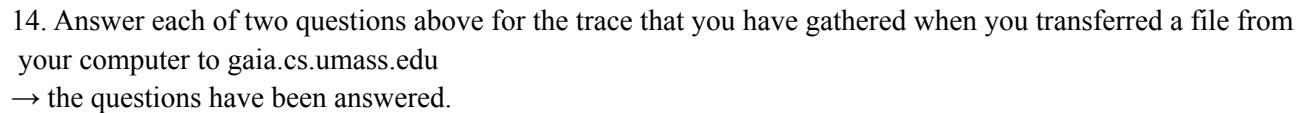
Using my own Trace:



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.

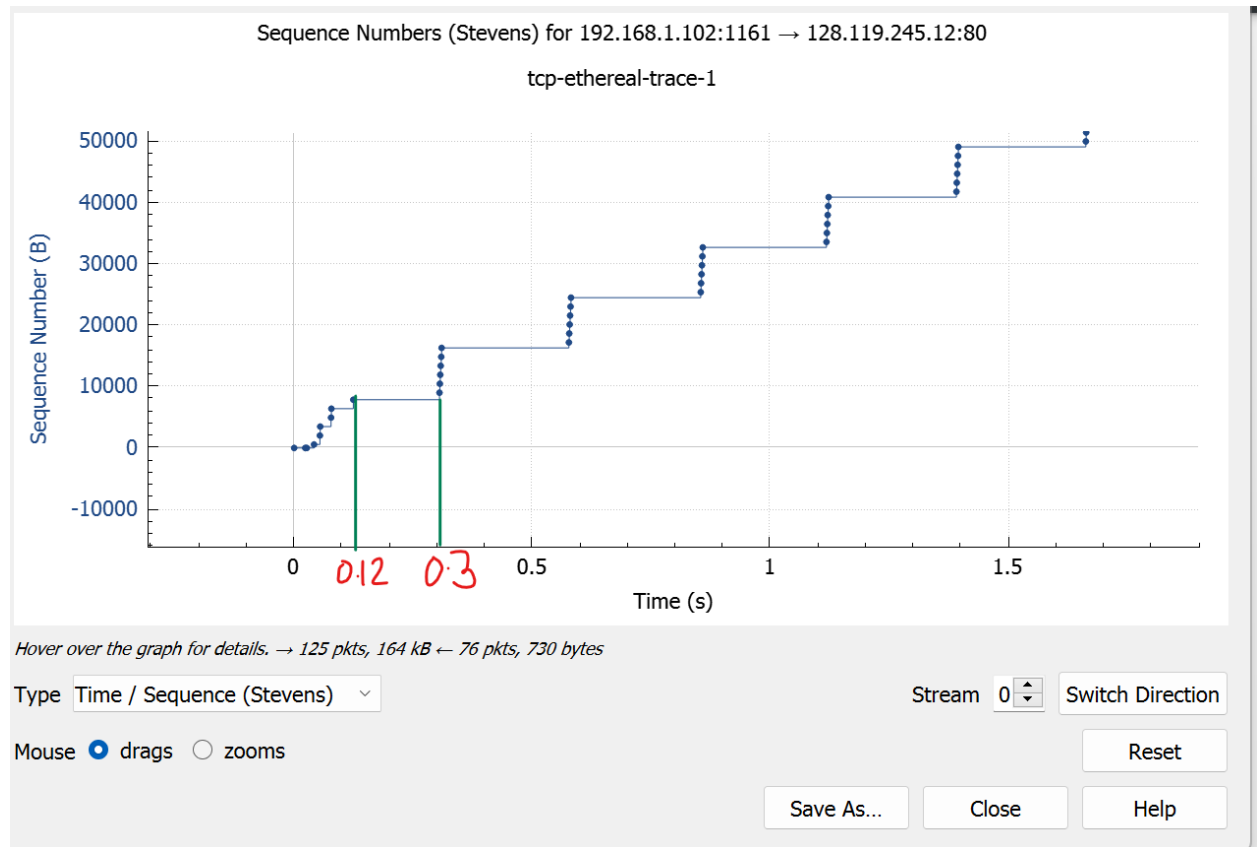
→ The slow start of the TCP seems to begin at about 0.125 seconds and then ends at about 0.15 seconds. The congestion avoidance takes place for 0.025 (0.15-0.125) secs because it cuts the amount of data to be sent.

The zoomed screenshot of the graph is attached below:



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 screenshot is attached below:



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
→ the questions have been answered.