

# Wireshark Lab : TCP

use tcp-ethereal-trace-1 as reference and set sequence number as absolute seq number

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.

**ANS: The IP address 192.168.1.102 TCP port is 1161**

The image shows a Wireshark packet capture of a TCP connection. The packet list pane displays a series of packets. Packet 199 is selected, showing an HTTP POST request. The packet details pane shows the TCP header with Source Port 1161 and Destination Port 80. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
182	09:44:25.492297	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232280209 Ack=883061786 Win=17520
183	09:44:25.493201	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232281669 Ack=883061786 Win=17520
184	09:44:25.494244	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232283129 Ack=883061786 Win=17520
185	09:44:25.495048	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=232284589 Ack=883061786 Win=17520
186	09:44:25.589570	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232280209 Win=62780
190	09:44:25.695400	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232283129 Win=62780
191	09:44:25.767667	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232285481 Win=62780
192	09:44:25.767889	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232285481 Ack=883061786 Win=17520
193	09:44:25.768769	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232286941 Ack=883061786 Win=17520
194	09:44:25.769656	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232288401 Ack=883061786 Win=17520
195	09:44:25.770633	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232289861 Ack=883061786 Win=17520
196	09:44:25.771531	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232291321 Ack=883061786 Win=17520
197	09:44:25.772405	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=232292781 Ack=883061786 Win=17520
198	09:44:25.867670	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232288401 Win=62780
199	09:44:25.867722	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/p...
200	09:44:25.959852	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232291321 Win=62780
201	09:44:26.019268	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232293053 Win=62780

Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 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: 232293053, Ack: 883061786, Len: 50

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 50]

Sequence number: 232293053

[Next sequence number: 232293103]

Acknowledgment number: 883061786

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 17520

[Calculated window size: 17520]

Window size scaling factor: -2 (no window scaling used)

0020 f5 0c 04 89 00 50 0d d8 82 bd 34 a2 74 1a 50 18 .....P...4.t.P.

0030 44 70 9f 0f 00 00 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d .....Dp.....

0040 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d .....

0050 2d 2d 2d 2d 2d 2d 32 36 35 30 30 31 39 31 36 39 31 .....265 00191691

0060 35 37 32 34 2d 2d 0d 0a 5724----

Frame (104 bytes) Reassembled TCP (164090 bytes)

Transmission Control Protocol (tcp), 20 bytes

Packets: 213 · Displayed: 202 (94.8%)

Profile: Default

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?

**ANS:**

**Sending IP address:192.168.1.102 TCP port: 1161**

**Receiving IP address: 128.119.245.12 TCP port: 80**

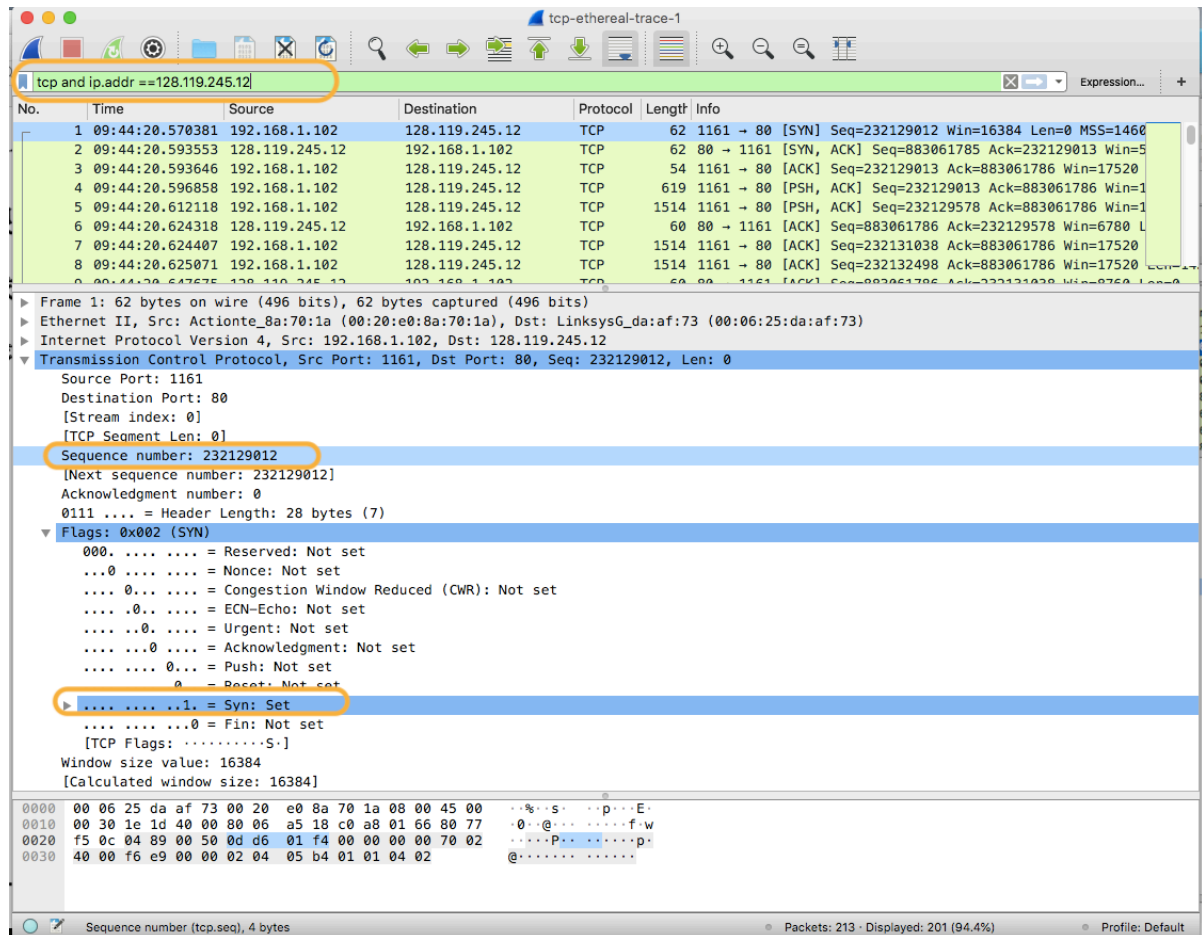
3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to [gaia.cs.umass.edu](http://gaia.cs.umass.edu)

**ANS:**

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?

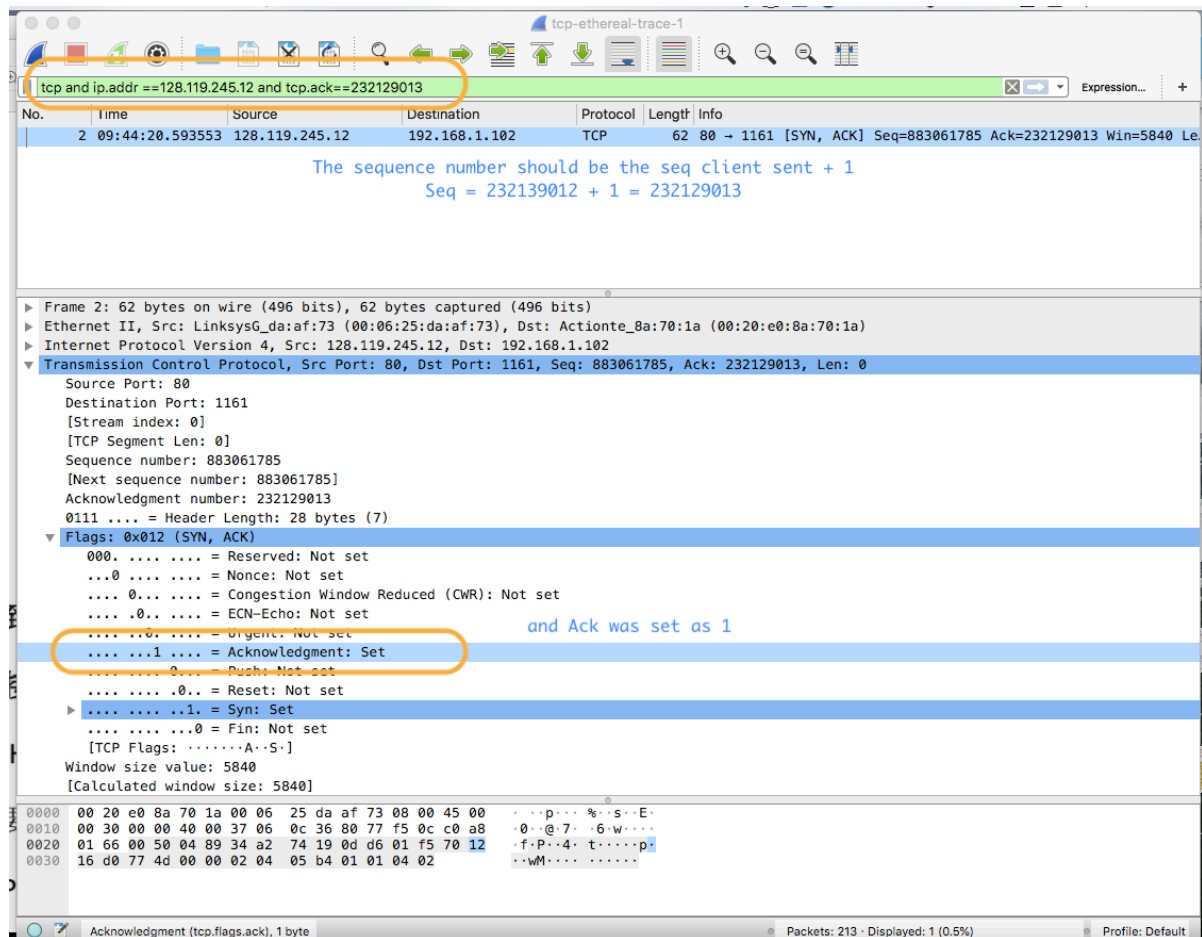
**ANS:** Client send SYN to start connection. I searched for the first sent request and find the client set SYN as 1 to establish the connection.

SEQ = 232129012, which is a random number. This is the first step of three-way handshake.



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?

ANS:



According to the sequence number SEQ = client SEQ + 1 of SYN-ACK response value, the SEQ (sequence number) = 232129013 can be used to search.

And Ack was set as 1, which means the sever has received the client's connection request and sent SYN-ACK to confirm.

This the second step of three-way handshake.

6. 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.

ANS: The sequence number is 232129013



tcp-ethereal-trace-1

Apply a display filter ... < %/ >

Time	Source	Destination	Protocol	Length	Info
2 09:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=584
3 09:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232129013 Ack=883061786 Win=17520 Le
4 09:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 Win=175
5 09:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=232129578 Ack=883061786 Win=175
6 09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len
7 09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=17520 Le
8 09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=17520 Le
9 09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 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: 232129013, Ack: 883061786, Len: 565

Source Port: 1161  
Destination Port: 80  
[Stream index: 0]  
[TCP Segment Len: 565]  
Sequence number: 232129013  
[Next sequence number: 232129578]  
Acknowledgment number: 883061786  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 17520  
[Calculated window size: 17520]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x1fbd [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[iRTT: 0.023265000 seconds]  
[Bytes in flight: 565]

0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18 ...P...x4.t.P.  
0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 Dp...Co ntent-Ty  
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 pe: mult ipart/fo  
0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f rm-data; boundar  
0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ys-----  
0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----265  
0080 2a 2a 21 2a 21 2a 2a 21 2a 21 2a 21 2a 21 2a 00101601 5774: 00

## segment2

tcp-ethereal-trace-1

Apply a display filter ... < %/ >

Time	Source	Destination	Protocol	Length	Info
2 09:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=584
3 09:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232129013 Ack=883061786 Win=17520 Le
4 09:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 Win=175
5 09:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=232129578 Ack=883061786 Win=175
6 09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len
7 09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=17520 Le
8 09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=17520 Le
9 09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=8760 Len=0

Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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: 232129578, Ack: 883061786, Len: 1460

Source Port: 1161  
Destination Port: 80  
[Stream index: 0]  
[TCP Segment Len: 1460]  
Sequence number: 232129578  
[Next sequence number: 232131038]  
Acknowledgment number: 883061786  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 17520  
[Calculated window size: 17520]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x3be5 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[iRTT: 0.023265000 seconds]  
[Bytes in flight: 2025]

0020 f5 0c 04 89 00 50 0d d6 04 2a 34 a2 74 1a 50 18 ...P...x4.t.P.  
0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74 2d 54 79 Dp...Co ntent-Ty  
0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f pe: mult ipart/fo  
0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 rm-data; boundar  
0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ys-----  
0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----265  
0080 2a 2a 21 2a 21 2a 2a 21 2a 21 2a 21 2a 21 2a 00101601 5774: 00

## segment3



tcp-ethereal-trace-1

Apply a display filter ... <=>

Time	Source	Destination	Protocol	Length	Info
2 09:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=584
3 09:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232129013 Ack=883061786 Win=17520 Le
4 09:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=232129013 Ack=883061786 Win=175
5 09:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=232129578 Ack=883061786 Win=175
6 09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len
7 09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=17520 Le
8 09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=17520 Le
9 09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=8760 Len=0

▶ Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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: 232131038, Ack: 883061786, Len: 1460  
     Source Port: 1161  
     Destination Port: 80  
     [Stream index: 0]  
     TCP Segment Len: 1460  
     Sequence number: 232131038  
     [Next sequence number: 232132498]  
     Acknowledgment number: 883061786  
     0101 .... = Header Length: 20 bytes (5)  
     ▶ Flags: 0x010 (ACK)  
     Window size value: 17520  
     [Calculated window size: 17520]  
     [Window size scaling factor: -2 (no window scaling used)]  
     Checksum: 0xb98e [unverified]  
     [Checksum Status: Unverified]  
     Urgent pointer: 0  
     ▼ [SEQ/ACK analysis]  
         [RTT: 0.023265000 seconds]  
         [Bytes in flight: 2920]

0020 f5 0c 04 89 00 50 0d d6 09 de 34 a2 74 1a 50 10 .....P...4.t.P.  
 0030 44 70 b9 8e 00 00 0d 0a 0d 0a 57 65 20 61 72 65 Dp.....We are  
 0040 20 6e 6f 77 20 74 72 79 69 6e 67 20 74 6f 20 72 now try ing to r  
 0050 65 6c 65 61 73 65 20 61 6c 6c 20 6f 75 72 20 62 elease a ll our b  
 0060 6f 6f 6b 73 20 6f 6e 65 20 6d 6f 6e 74 68 20 69 ooks one month i  
 0070 6e 20 61 64 76 61 6e 63 65 0d 0a 6f 66 20 74 68 n advanc e of th  
 0080 65 20 6f 66 66 69 63 69 61 6c 20 72 65 6c 65 61 e offici al relea  
 0090 73 65 20 64 61 74 65 73 7c 20 66 6f 72 20 74 69 se dates . for ti

## segment4

6 09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780
7 09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=17520
8 09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=17520
9 09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=8760
10 09:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=17520
11 09:44:20.648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232135418 Ack=883061786 Win=17520
12 09:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=1160
13 09:44:20.694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=232136878 Ack=883061786 Win=1160

▶ Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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: 232132498, Ack: 883061786, Len: 1460  
     Source Port: 1161  
     Destination Port: 80  
     [Stream index: 0]  
     [TCP Segment Len: 1460]  
     Sequence number: 232132498  
     [Next sequence number: 232133958]  
     Acknowledgment number: 883061786  
     0101 .... = Header Length: 20 bytes (5)  
     ▶ Flags: 0x010 (ACK)  
     Window size value: 17520  
     [Calculated window size: 17520]

## segment5

tcp-ethereal-trace-1

tcp

No.	Time	Source	Destination	Protocol	Length	Info
6	09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=678
7	09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=175
8	09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=175
9	09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=876
10	09:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=175
11	09:44:20.648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232135418 Ack=883061786 Win=175
12	09:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=116
13	09:44:20.694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=232136878 Ack=883061786 Win=17520

Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 883061786, Ack: 232131038, Len: 0

Source Port: 80

Destination Port: 1161

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 883061786

[Next sequence number: 883061786]

Acknowledgment number: 232131038

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window size value: 8760

[Calculated window size: 8760]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x90c0 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 5]

[The RTT to ACK the segment was: 0.035557000 seconds]

## segment6

tcp-ethereal-trace-1

tcp

No.	Time	Source	Destination	Protocol	Length	Info
6	09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=678
7	09:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=175
8	09:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=175
9	09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=876
10	09:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=175
11	09:44:20.648538	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=232135418 Ack=883061786 Win=175
12	09:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=116
13	09:44:20.694566	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=232136878 Ack=883061786 Win=17520

Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 883061786, Ack: 232132498, Len: 0

Source Port: 80

Destination Port: 1161

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 883061786

[Next sequence number: 883061786]

Acknowledgment number: 232132498

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window size value: 11680

[Calculated window size: 11680]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x7fa4 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 7]

[The RTT to ACK the segment was: 0.070059000 seconds]

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00 . . . p . . . % . s . . E .  
 0010 00 28 58 74 40 00 37 06 b3 c9 80 77 f5 0c c0 a8 . ( Xt @ . 7 . . . w . . . .  
 0020 01 66 00 50 04 89 34 a2 74 1a 0d d6 0f 92 50 10 . f . P . . 4 . t . . . . P .

Then use "tcp.analysis.ack\_rtt" to search rtt

tcp.analysis.ack\_rtt

No.	Time	Source	Destination	Protocol	Length	Info
2	09:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=175
3	09:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232129013 Ack=883061786 Win=175
6	09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=678
9	09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=876
12	09:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=1168

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 883061786, Ack: 232129578, Len: 0

Source Port: 80  
Destination Port: 1161  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence number: 883061786  
[Next sequence number: 883061786]  
Acknowledgment number: 232129578  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window size value: 6780  
[Calculated window size: 6780]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x9e30 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[This is an ACK to the segment in frame: 4]  
[The RTT to ACK the segment was: 0.027460000 seconds]  
[iRTT: 0.023265000 seconds]  
[Timestamps]

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00 ... p...%..s...E.  
0010 00 28 58 72 40 00 37 06 b3 cb 80 77 f5 0c c0 a8 ... (Xr@.7. ....w....  
0020 01 66 00 50 04 89 34 a2 74 1a 0d d6 04 2a 50 10 ... f.P...4. t....\*P.  
0030 1a 7c 9e 30 00 00 da 12 00 00 47 a5 ... .0.....\*G.

Then use "tcp.analysis.ack\_rtt" to search rtt

tcp.analysis.ack\_rtt

Setting filter

No.	Time	Source	Destination	Protocol	Length	Info
2	09:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=883061785 Ack=232129013 Win=175
3	09:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=232129013 Ack=883061786 Win=175
6	09:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=678
9	09:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=876
12	09:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=1168
14	09:44:20.739499	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232133958 Win=146
15	09:44:20.787680	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232135418 Win=175
16	09:44:20.838183	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232136878 Win=204
17	09:44:20.875188	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232138025 Win=233
24	09:44:20.926818	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232139485 Win=262
25	09:44:20.970545	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232140945 Win=292
26	09:44:21.018994	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232142405 Win=321
27	09:44:21.070410	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=883061786 Ack=232143865 Win=35040

From 4 below counting 6 segments

[TCP Segment Len: 0]  
Sequence number: 883061786  
[Next sequence number: 883061786]  
Acknowledgment number: 232129578  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window size value: 6780  
[Calculated window size: 6780]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x9e30 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[This is an ACK to the segment in frame: 4]  
[The RTT to ACK the segment was: 0.027460000 seconds]  
[iRTT: 0.023265000 seconds]  
[Timestamps]

RTT time

0000 00 20 e0 8a 70 1a 00 06 25 da af 73 08 00 45 00 ... p...%..s...E.  
0010 00 28 58 72 40 00 37 06 b3 cb 80 77 f5 0c c0 a8 ... (Xr@.7. ....w....  
0020 01 66 00 50 04 89 34 a2 74 1a 0d d6 04 2a 50 10 ... f.P...4. t....\*P.  
0030 1a 7c 9e 30 00 00 da 12 00 00 47 a5 ... .0.....\*G.

The window size value from the TCP header (tcp.window\_size\_value), 2 bytes

Packets: 213 · Displayed: 77 (36.2%)

Profile: Default

$$EstimatedRTT = \frac{1}{8}RTT + \frac{7}{8}LastEstimatedRTT$$

And you can get the following list



Table 1 Table 1-1

	segment No.	Seq	Len	RTT	EstimatedRTT
1	4	232129013	565	0.027460000	0.02746
2	5	232129578	1460	0.035557000	0.028472125
3	7	232131038	3486	0.070059000	0.033670484
4	8	232132498	1460	0.114428000	0.043765174
5	10	232133958	1460	0.139894000	0.055781277
6	11	232135418	1460	0.189645000	0.072514242

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

**ANS see above**

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?

**ANS :**

The screenshot shows a Wireshark packet capture of a TCP connection. The packet list at the top shows a SYN segment (Seq=883061785, Len=0) and subsequent ACK segments. The packet details for the first ACK segment (Seq=232129013, Len=0) show the window size value as 5840. The packet bytes at the bottom show the sequence number 16 d0 77 4d 00 02 04 05 b4 01 01 04 02.

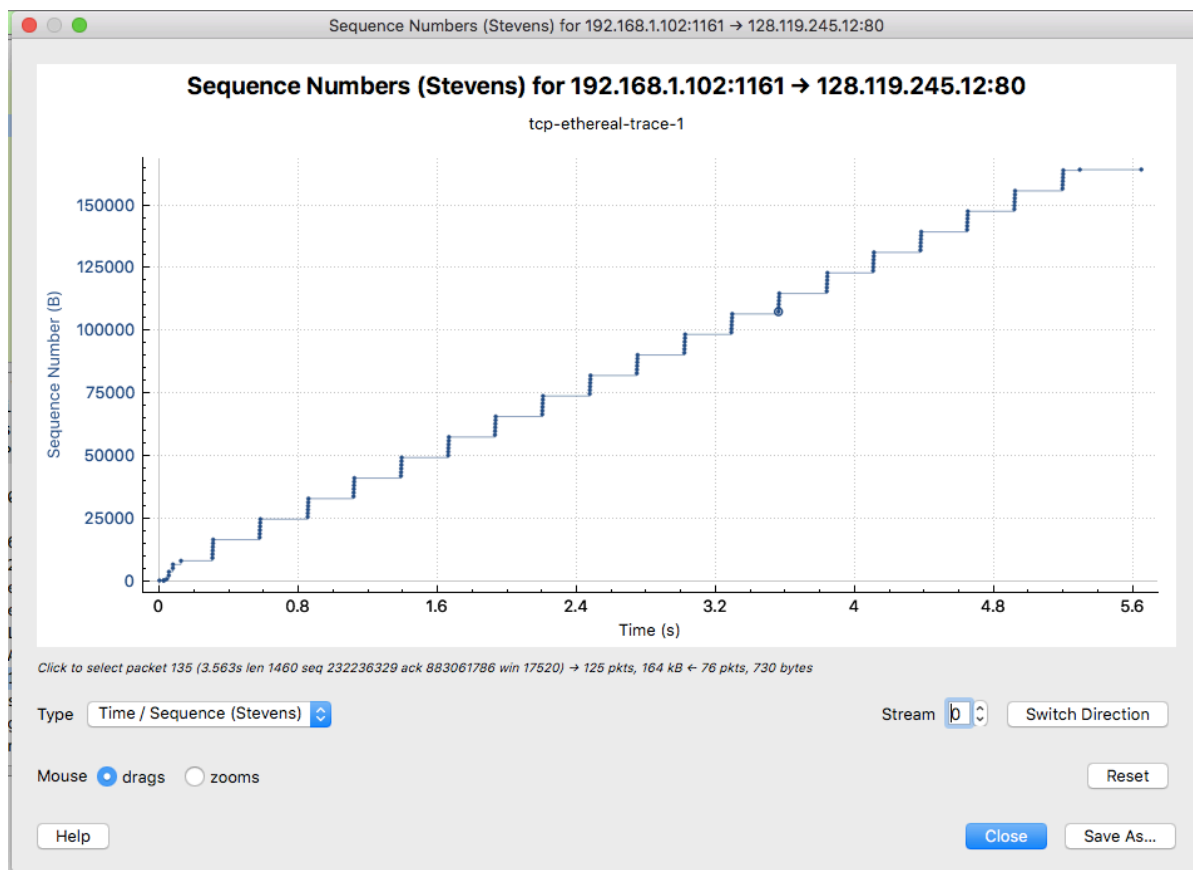
**The receiver window size grows steadily til a maximum window size comes. No throttle is made due to the lack of buffer space.**

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

**ANS: no**

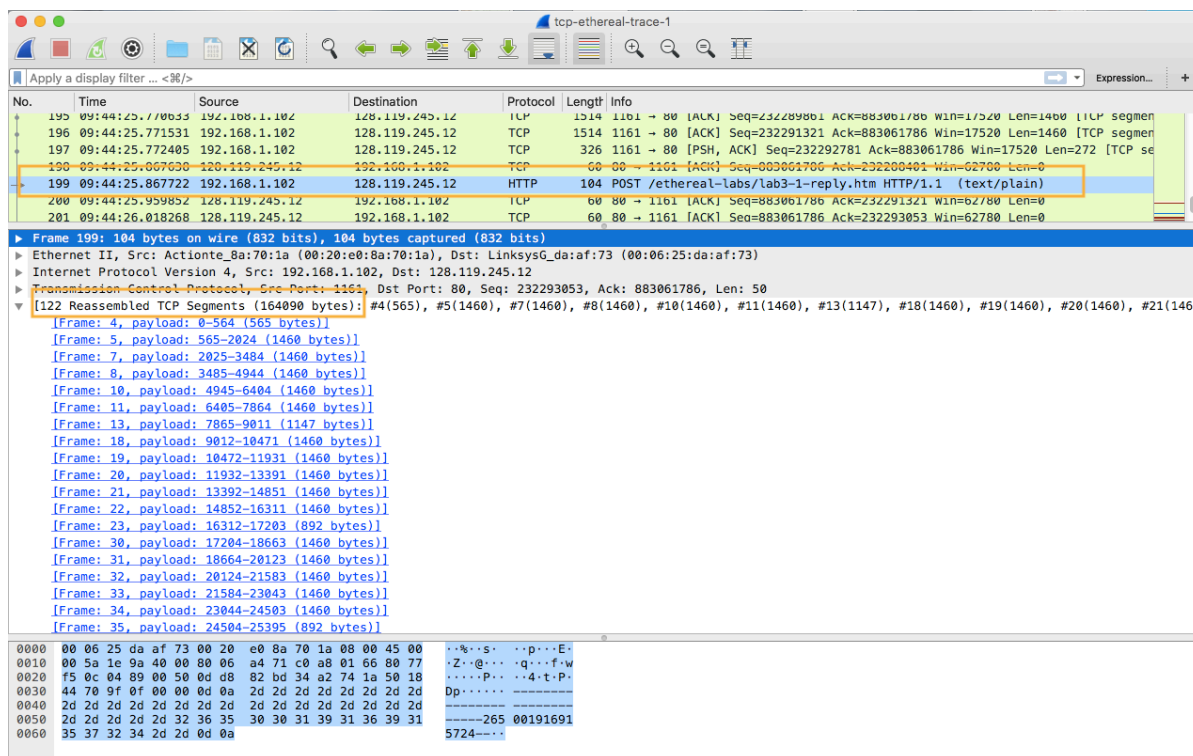
menu bar -> Statistic -> TCP -> Stevens

Because the sequence number is steadily 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 (see Table 3.2 on page 250 in the text).

**ANS: 122 reassembled TCP segment, totally 164090 bytes.**



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

**ANS:**  $Throughput = \frac{AmountOfDataTransmitted}{TimeIncurred}$

$Throughput = \frac{1640905.297341000}{52.75} = 30975.9179 \text{ bytes/s} = 30.976 \text{ kb/s}$

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 slowstart 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.

**ANS:**

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

**ANS:**