

# CS 655 Computer Network

## TCP Lab

Ziqi Tan  
U 88387934

A first look at the captured trace.

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/plain)
200	09:44:25.959852	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
201	09:44:26.018268	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
202	09:44:26.026211	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203	09:44:26.031556	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
206	09:44:26.221522	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0

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).

The client computer's IP address is 192.168.1.105 and the TCP port number is 1161.

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/plain)
<						
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: 164041, Ack: 1, Len: 50						
Source Port: 1161						
Destination Port: 80						
[Stream index: 0]						
[TCP Segment Len: 50]						
Sequence number: 164041 (relative sequence number)						
Sequence number (raw): 232293053						
[Next sequence number: 164091 (relative sequence number)]						
Acknowledgment number: 1 (relative ack number)						
Acknowledgment number (raw): 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: 0x9f0f [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
[SEQ/ACK analysis]						
[Timestamps]						
TCP payload (50 bytes)						
TCP segment data (50 bytes)						
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(1147), #18(1460), #1						

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 gaia.cs.umass.edu is 128.119.245.12 and the port number is 80.

If you have been able to create your own trace, answer the following question:

217	21:00:28.507007	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=55297 Win=133800 Len=0
218	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=54757 Win=138752 Len=0
219	21:00:28.587902	10.0.0.84	128.119.245.12	TCP	20494	58166 → 80 [PSH, ACK] Seq=102937 Ack=1 Win=131328 Len=20440 [TCP segment of a reassembled PDU]
220	21:00:28.589277	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=56217 Win=141696 Len=0
221	21:00:28.589289	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80 [ACK] Seq=123377 Ack=1 Win=131328 Len=2920 [TCP segment of a reassembled PDU]
222	21:00:28.589353	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=59137 Win=147584 Len=0
223	21:00:28.589366	10.0.0.84	128.119.245.12	TCP	5894	58166 → 80 [PSH, ACK] Seq=126297 Ack=1 Win=131328 Len=5840 [TCP segment of a reassembled PDU]
224	21:00:28.593808	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=63517 Win=156288 Len=0
225	21:00:28.593819	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80 [ACK] Seq=132137 Ack=1 Win=131328 Len=8760 [TCP segment of a reassembled PDU]
226	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=64977 Win=159232 Len=0
227	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=67897 Win=164992 Len=0
228	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=69357 Win=167936 Len=0
229	21:00:28.594529	10.0.0.84	128.119.245.12	HTTP	12215	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
230	21:00:28.594976	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=72277 Win=173824 Len=0
231	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=73737 Win=176768 Len=0

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 computer is 10.0.0.84 and the port number is 51456.

The IP address of gaia.cs.umass.edu is 128.119.245.12 and the port number is 80.

**I will use my own trace to answer the following questions.**

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 is 0.

No.	Time	Source	Destination	Protocol	Length	Info
56	21:00:19.520280	10.0.0.84	128.119.245.12	TCP	66	58166 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
57	21:00:19.520416	10.0.0.84	128.119.245.12	TCP	66	58167 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
59	21:00:19.540196	128.119.245.12	10.0.0.84	TCP	66	80 → 58166 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
60	21:00:19.540253	10.0.0.84	128.119.245.12	TCP	54	58166 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
61	21:00:19.548703	128.119.245.12	10.0.0.84	TCP	66	80 → 58167 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
62	21:00:19.548754	10.0.0.84	128.119.245.12	TCP	54	58167 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
169	21:00:28.493619	10.0.0.84	128.119.245.12	TCP	790	58166 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=736 [TCP segment of a reassembled PDU]
171	21:00:28.516011	128.119.245.12	10.0.0.84	TCP	56	80 → 58166 [ACK] Seq=1 Ack=737 Win=30720 Len=0
176	21:00:28.536373	10.0.0.84	128.119.245.12	TCP	14654	58166 → 80 [ACK] Seq=737 Ack=1 Win=131328 Len=14600 [TCP segment of a reassembled PDU]
180	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	56	80 → 58166 [ACK] Seq=1 Ack=3657 Win=36608 Len=0
181	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=5117 Win=39552 Len=0
182	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166 [ACK] Seq=1 Ack=6577 Win=42368 Len=0

The flag 0x002 (SYN) identifies the segment as a SYN segment.

```
Transmission Control Protocol, Src Port: 58166, Dst Port: 80, Seq: 0, Len: 0
Source Port: 58166
Destination Port: 80
[Stream index: 5]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 1608685471
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
```

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 sequence number is 0.

Acknowledgement number: 1.

The acknowledgment number that “gaia.cs.umass.edu” puts in its segment is the sequence number of the next byte “gaia.cs.umass.edu” is expecting from the client computer. Let’s see the next TCP segment sent from the client computer whose sequence number is exactly 1.

The Flags: 0x012 (SYN, ACK) identifies the segment as a SYNACK segment.

```

> Ethernet II, Src: ARRISGro_e0:16:8f (3c:04:61:e0:16:8f), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.84
* Transmission Control Protocol, Src Port: 80, Dst Port: 58166, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 58166
  [Stream index: 5]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 678543218
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 1608685472
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window size value: 29200
  [Calculated window size: 29200]
  Checksum: 0xba2b [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  > [SEQ/ACK analysis]
  > [Timestamps]

> Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: ARRISGro_e0:16:8f (3c:04:61:e0:16:8f)
> Internet Protocol Version 4, Src: 10.0.0.84, Dst: 128.119.245.12
* Transmission Control Protocol, Src Port: 58166, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 58166
  Destination Port: 80
  [Stream index: 5]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 1608685472
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 678543219
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window size value: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x7ff2 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]

```

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. The sequence number is 1.

From the HTTP POST request, find the first frame number 169 which is the first post request TCP segment. Then, turn to frame 169 and we find the sequence number is 1. In the raw data, we can see the "POST".

```

227 21:00:28.594512 128.119.245.12 10.0.0.84 TCP 60 80 → 58166 [ACK] Seq=1 Ack=67897 Win=164992 Len=0
228 21:00:28.594512 128.119.245.12 10.0.0.84 TCP 60 80 → 58166 [ACK] Seq=1 Ack=69357 Win=167936 Len=0
* 229 21:00:28.594529 10.0.0.84 128.119.245.12 HTTP 12215 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
  > Frame 229: 12215 bytes on wire (97720 bits), 12215 bytes captured (97720 bits) on interface \Device\NPF_{10558E5B-8099-4BA2-B549-CE934C3}
  > Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: ARRISGro_e0:16:8f (3c:04:61:e0:16:8f)
  > Internet Protocol Version 4, Src: 10.0.0.84, Dst: 128.119.245.12
  > Transmission Control Protocol, Src Port: 58166, Dst Port: 80, Seq: 140897, Ack: 1, Len: 12161
  > [15 Reassembled TCP Segments (153057 bytes): #169(736), #176(14600), #187(29200), #196(20440), #199(8760), #201(2920), #203(2920), #206(
    [Frame: 169, payload: 0-735 (736 bytes)]
    [Frame: 176, payload: 736-15335 (14600 bytes)]
    [Frame: 187, payload: 15336-44535 (29200 bytes)]
    [Frame: 196, payload: 44536-64975 (20440 bytes)]
    [Frame: 199, payload: 64976-73735 (8760 bytes)]
    [Frame: 201, payload: 73736-76655 (2920 bytes)]
    [Frame: 203, payload: 76656-79575 (2920 bytes)]
    [Frame: 206, payload: 79576-88335 (8760 bytes)]
    [Frame: 208, payload: 88336-91255 (2920 bytes)]
    [Frame: 212, payload: 91256-102935 (11680 bytes)]
    [Frame: 219, payload: 102936-123375 (20440 bytes)]
    [Frame: 221, payload: 123376-126295 (2920 bytes)]
    [Frame: 223, payload: 126296-132135 (5840 bytes)]
    [Frame: 225, payload: 132136-140895 (8760 bytes)]
    [Frame: 229, payload: 140896-153056 (12161 bytes)]
  [Segment count: 15]
  [Reassembled TCP length: 153057]
  [Reassembled TCP Data: 504f5354202f77697265736861726b2d6c61627272f6c6162...]
  > Hypertext Transfer Protocol
  > MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryEK71RhbkpeSplpvx"

```

No.	Time	Source	Destination	Protocol	Length	Info
56	21:00:19.520280	10.0.0.84	128.119.245.12	TCP	66	58166 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
57	21:00:19.520416	10.0.0.84	128.119.245.12	TCP	66	58167 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
59	21:00:19.540196	128.119.245.12	10.0.0.84	TCP	66	80 → 58166 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
60	21:00:19.540253	10.0.0.84	128.119.245.12	TCP	54	58166 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
61	21:00:19.548703	128.119.245.12	10.0.0.84	TCP	66	80 → 58167 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
62	21:00:19.548754	10.0.0.84	128.119.245.12	TCP	54	58167 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
169	21:00:28.493619	10.0.0.84	128.119.245.12	TCP	790	58166 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=736 [TCP segment of a reassembled PDU]
171	21:00:28.516011	128.119.245.12	10.0.0.84	TCP	56	80 → 58166 [ACK] Seq=1 Ack=737 Win=30720 Len=0
176	21:00:28.536373	10.0.0.84	128.119.245.12	TCP	14654	58166 → 80 [ACK] Seq=737 Ack=1 Win=131328 Len=14600 [TCP segment of a reassembled PDU]
180	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	56	80 → 58166 [ACK] Seq=1 Ack=3657 Win=36608 Len=0

  

> Internet Protocol Version 4, Src: 10.0.0.84, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58166, Dst Port: 80, Seq: 1, Ack: 1, Len: 736
Source Port: 58166
Destination Port: 80
[Stream index: 5]
[TCP Segment Len: 736]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 1608685472
Next sequence number: 737 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 678543219
0101 ... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)

  

0020	f5 0c e3 36 00 50 5f a2 97 a6 28 71 bf 73 50 18	...6 P...sq.sP
0030	02 01 82 d2 00 00 50 4f 53 54 20 2f 77 69 72 65	...POST wire
0040	73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d	shark-la bs/lab3-
0050	31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50	1-reply. htm HTTP
0060	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61	/1.1..Ho st: gaia
0070	2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43	.cs.umass.edu..C

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)? 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 Estimated RTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the Estimated RTT equation on page 242 for all subsequent segments.

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph- >Round Trip Time Graph.

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

The sequence numbers of the first six segments in the TCP connection are 1, 737, 15337, 45537, 64977, 73737. The sent time and the length are shown below.

169 21:00:28.493619 10.0.0.84 128.119.245.12 TCP 790 58166 → 80 [PSH, ACK]  
Seq=1 Ack=1 Win=131328 Len=736 [TCP segment of a reassembled PDU]  
176 21:00:28.536373 10.0.0.84 128.119.245.12 TCP 14654 58166 → 80 [ACK]  
Seq=737 Ack=1 Win=131328 Len=14600 [TCP segment of a reassembled PDU]  
187 21:00:28.555414 10.0.0.84 128.119.245.12 TCP 29254 58166 → 80 [PSH, ACK]  
Seq=15337 Ack=1 Win=131328 Len=29200 [TCP segment of a reassembled PDU]  
196 21:00:28.572104 10.0.0.84 128.119.245.12 TCP 20494 58166 → 80 [PSH, ACK]  
Seq=44537 Ack=1 Win=131328 Len=20440 [TCP segment of a reassembled PDU]  
199 21:00:28.574148 10.0.0.84 128.119.245.12 TCP 8814 58166 → 80 [PSH, ACK]  
Seq=64977 Ack=1 Win=131328 Len=8760 [TCP segment of a reassembled PDU]  
201 21:00:28.574593 10.0.0.84 128.119.245.12 TCP 2974 58166 → 80 [ACK]  
Seq=73737 Ack=1 Win=131328 Len=2920 [TCP segment of a reassembled PDU]

The ACK for sequence number 1:

171 21:00:28.516011 128.119.245.12 10.0.0.84 TCP 56 80 → 58166 [ACK]

Seq=1 **Ack=737** Win=30720 Len=0

The ACKs for sequence number 737:

176	21:00:28.536373	10.0.0.84	128.119.245.12	TCP	14654	58166 → 80	[ACK]	Seq=737	Ack=1	Win=131328	Len=14600	[TCP segment of a reassembled PDU]
180	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	56	80 → 58166	[ACK]	Seq=1	Ack=3657	Win=36608	Len=0	
181	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=5117	Win=39552	Len=0	
182	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=6577	Win=42368	Len=0	
183	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=9497	Win=48256	Len=0	
184	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=10957	Win=51200	Len=0	
185	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=12417	Win=54144	Len=0	
186	21:00:28.555378	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=15337	Win=59904	Len=0	

The ACKs for sequence number 15337 are circled in red rectangles:

187	21:00:28.555414	10.0.0.84	128.119.245.12	TCP	29254	58166 → 80	[PSH, ACK]	Seq=15337	Ack=1	Win=131328	Len=29200	[TCP segment of a reassembled PDU]
191	21:00:28.572068	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=18257	Win=65792	Len=0	
192	21:00:28.572068	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=19717	Win=68736	Len=0	
193	21:00:28.572068	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=22637	Win=74496	Len=0	
194	21:00:28.572068	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=24097	Win=77440	Len=0	
195	21:00:28.572068	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=25557	Win=80384	Len=0	
196	21:00:28.572104	10.0.0.84	128.119.245.12	TCP	20494	58166 → 80	[PSH, ACK]	Seq=44537	Ack=1	Win=131328	Len=20440	[TCP segment of a reassembled PDU]
197	21:00:28.574122	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=28477	Win=86272	Len=0	
198	21:00:28.574122	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=29937	Win=89088	Len=0	
199	21:00:28.574148	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[PSH, ACK]	Seq=64977	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
200	21:00:28.574580	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=31397	Win=92032	Len=0	
201	21:00:28.574593	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=73737	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
202	21:00:28.577868	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=32857	Win=94976	Len=0	
203	21:00:28.577893	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=76657	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
204	21:00:28.578324	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=34317	Win=97920	Len=0	
205	21:00:28.578324	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=37237	Win=103680	Len=0	
206	21:00:28.578340	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[PSH, ACK]	Seq=79577	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
207	21:00:28.578651	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=38697	Win=106624	Len=0	
208	21:00:28.578670	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=88337	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
209	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=40157	Win=109568	Len=0	
210	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=41617	Win=112512	Len=0	
211	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=44537	Win=118272	Len=0	
212	21:00:28.579251	10.0.0.84	128.119.245.12	TCP	11734	58166 → 80	[PSH, ACK]	Seq=91257	Ack=1	Win=131328	Len=11680	[TCP segment of a reassembled PDU]

The ACKs for sequence number 45537 are circled in red tangles:

196	21:00:28.572104	10.0.0.84	128.119.245.12	TCP	20494	58166 → 80	[PSH, ACK]	Seq=44537	Ack=1	Win=131328	Len=20440	[TCP segment of a reassembled PDU]
197	21:00:28.574122	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=28477	Win=86272	Len=0	
198	21:00:28.574122	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=29937	Win=89088	Len=0	
199	21:00:28.574148	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[PSH, ACK]	Seq=64977	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
200	21:00:28.574580	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=31397	Win=92032	Len=0	
201	21:00:28.574593	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=73737	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
202	21:00:28.577868	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=32857	Win=94976	Len=0	
203	21:00:28.577893	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=76657	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
204	21:00:28.578324	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=34317	Win=97920	Len=0	
205	21:00:28.578324	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=37237	Win=103680	Len=0	
206	21:00:28.578340	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[PSH, ACK]	Seq=79577	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
207	21:00:28.578651	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=38697	Win=106624	Len=0	
208	21:00:28.578670	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=88337	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
209	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=40157	Win=109568	Len=0	
210	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=41617	Win=112512	Len=0	
211	21:00:28.579230	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=44537	Win=118272	Len=0	
212	21:00:28.579251	10.0.0.84	128.119.245.12	TCP	11734	58166 → 80	[PSH, ACK]	Seq=91257	Ack=1	Win=131328	Len=11680	[TCP segment of a reassembled PDU]
213	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=47457	Win=124160	Len=0	
214	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=48917	Win=127104	Len=0	
215	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=50377	Win=130048	Len=0	
216	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=51837	Win=132992	Len=0	
217	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=53297	Win=135808	Len=0	
218	21:00:28.587867	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=54757	Win=138752	Len=0	
219	21:00:28.587902	10.0.0.84	128.119.245.12	TCP	20494	58166 → 80	[PSH, ACK]	Seq=102937	Ack=1	Win=131328	Len=20440	[TCP segment of a reassembled PDU]
220	21:00:28.589277	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=56217	Win=141696	Len=0	
221	21:00:28.589289	10.0.0.84	128.119.245.12	TCP	2974	58166 → 80	[ACK]	Seq=123377	Ack=1	Win=131328	Len=2920	[TCP segment of a reassembled PDU]
222	21:00:28.589353	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=59137	Win=147584	Len=0	
223	21:00:28.589366	10.0.0.84	128.119.245.12	TCP	5894	58166 → 80	[PSH, ACK]	Seq=126297	Ack=1	Win=131328	Len=5840	[TCP segment of a reassembled PDU]
224	21:00:28.593808	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=63517	Win=156288	Len=0	
225	21:00:28.593819	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[ACK]	Seq=132137	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
226	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=64977	Win=159232	Len=0	
227	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=67897	Win=164992	Len=0	
228	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=69357	Win=167936	Len=0	
229	21:00:28.594529	10.0.0.84	128.119.245.12	HTTP	12215	POST /wireshark-labs/lab3-1-reply.htm	HTTP/1.1 (text/plain)					
230	21:00:28.594976	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=72277	Win=173824	Len=0	
231	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=73737	Win=176768	Len=0	
232	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=75197	Win=179712	Len=0	
233	21:00:28.599843	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=76657	Win=182528	Len=0	
234	21:00:28.599942	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=78117	Win=183296	Len=0	

The ACKs for sequence number 64977 are circled in red tangles:

222	21:00:28.589353	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=59137	Win=147584	Len=0	
223	21:00:28.589366	10.0.0.84	128.119.245.12	TCP	5894	58166 → 80	[PSH, ACK]	Seq=126297	Ack=1	Win=131328	Len=5840	[TCP segment of a reassembled PDU]
224	21:00:28.593808	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=63517	Win=156288	Len=0	
225	21:00:28.593819	10.0.0.84	128.119.245.12	TCP	8814	58166 → 80	[ACK]	Seq=132137	Ack=1	Win=131328	Len=8760	[TCP segment of a reassembled PDU]
226	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=64977	Win=159232	Len=0	
227	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=67897	Win=164992	Len=0	
228	21:00:28.594512	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=69357	Win=167936	Len=0	
229	21:00:28.594529	10.0.0.84	128.119.245.12	HTTP	12215	POST /wireshark-labs/lab3-1-reply.htm	HTTP/1.1 (text/plain)					
230	21:00:28.594976	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=72277	Win=173824	Len=0	
231	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=73737	Win=176768	Len=0	
232	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=75197	Win=179712	Len=0	
233	21:00:28.599843	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=76657	Win=182528	Len=0	
234	21:00:28.599942	128.119.245.12	10.0.0.84	TCP	60	80 → 58166	[ACK]	Seq=1	Ack=78117	Win=183296	Len=0	



The ACKs for sequence number 73737 are circled in red tangles:

230	21:00:28.594976	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=72277 Win=173824 Len=0
231	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=73737 Win=176768 Len=0
232	21:00:28.595403	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=75197 Win=179712 Len=0
233	21:00:28.599843	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=76657 Win=182528 Len=0
234	21:00:28.599942	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=78117 Win=183296 Len=0
235	21:00:28.600951	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=79577 Win=183296 Len=0
236	21:00:28.601066	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=81037 Win=183296 Len=0
238	21:00:28.601066	128.119.245.12	10.0.0.84	TCP	60 80 → 58166 [ACK] Seq=1 Ack=82497 Win=183296 Len=0

In SEQ/ACK analysis of the wireshark, we have the measured RTT:

ACK to frame 169: 0.022392000 seconds

ACK to frame 176: 0.019005000 seconds

ACK to frame 187: 0.023816000 seconds

ACK to frame 196: 0.022408000 seconds

ACK to frame 199: 0.021255000 seconds

ACK to frame 201: 0.025250000 seconds

We use the equation in section 3.5.2:

$$EstimatedRTT = (1 - \alpha) * EstimatedRTT + \alpha * SampleRTT$$

Where  $\alpha$  is recommended as 0.125.

Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment.

Estimated RTT:

ACK to frame 176:  $(1-0.125) * 0.022392000 + 0.125 * 0.019005000 = 0.022$  seconds

ACK to frame 187:  $(1-0.125) * 0.022 + 0.125 * 0.023816000 = 0.0222$  seconds

ACK to frame 196:  $(1-0.125) * 0.0222 + 0.125 * 0.022408000 = 0.0222$  seconds

ACK to frame 199:  $(1-0.125) * 0.0222 + 0.125 * 0.021255000 = 0.0221$  seconds

ACK to frame 201:  $(1-0.125) * 0.0221 + 0.125 * 0.025250000 = 0.0226$  seconds

## 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 is 240.

169	21:00:28.493619	10.0.0.84	128.119.245.12	TCP	790 58166 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=736 [TCP segment of a reassembled PDU]
171	21:00:28.516011	128.119.245.12	10.0.0.84	TCP	56 80 → 58166 [ACK] Seq=1 Ack=737 Win=30720 Len=0

  

Frame 171: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{10558E58-8099-4BA2-8549-CE934C3E04AA}, id 0
Ethernet II, Src: ARISGno_e0:16:8f (3c:04:61:e0:16:8f), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.84
Transmission Control Protocol, Src Port: 80, Dst Port: 58166, Seq: 1, Ack: 737, Len: 0
Source Port: 80
Destination Port: 58166
[Stream index: 5]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 678543219
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 737 (relative ack number)
Acknowledgment number (raw): 1608686208
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 240
[Calculated window size: 30720]
[Window size scaling factor: 128]
Checksum: 0x693e [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
VSS Monitoring Ethernet trailer, Source Port: 0

The lack of receiver buffer space never throttled the sender.

240, 286, 309, 331, 377, 400, 423, 468, 514, 537, 582, 605, 628, 274, 696, 719, 742, 765, 810, 833,

856, 879, 924, ..., 1221, ..., 1500, ..., 2207.

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

Yes! Check the retransmission information.

275	21:00:28.670087	128.119.245.12	10.0.0.84	TCP	90	[TCP Window Update]	80 → 58166	[ACK]	Seq=1 Ack=108777 Win=224128 Len=0 SLE=143817 SRE=1511
276	21:00:28.671091	128.119.245.12	10.0.0.84	TCP	90	[TCP Window Update]	80 → 58166	[ACK]	Seq=1 Ack=108777 Win=227072 Len=0 SLE=143817 SRE=1521
277	21:00:28.671091	128.119.245.12	10.0.0.84	TCP	90	[TCP Window Update]	80 → 58166	[ACK]	Seq=1 Ack=108777 Win=230016 Len=0 SLE=143817 SRE=1534
287	21:00:28.732218	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[PSH, ACK]	Seq=151598 Ack=1 Win=131328 Len=1460
288	21:00:28.747322	128.119.245.12	10.0.0.84	TCP	90	[TCP Dup ACK 264#1]	80 → 58166	[ACK]	Seq=1 Ack=108777 Win=230016 Len=0 SLE=151598 SRE=1534
289	21:00:28.747359	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=108777 Ack=1 Win=131328 Len=1460
290	21:00:28.747391	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=110237 Ack=1 Win=131328 Len=1460
291	21:00:28.747403	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=113157 Ack=1 Win=131328 Len=1460
292	21:00:28.747403	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[PSH, ACK]	Seq=114617 Ack=1 Win=131328 Len=1460
293	21:00:28.747418	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=117537 Ack=1 Win=131328 Len=1460
294	21:00:28.747418	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=118997 Ack=1 Win=131328 Len=1460
295	21:00:28.747418	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=120457 Ack=1 Win=131328 Len=1460
296	21:00:28.747418	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=121917 Ack=1 Win=131328 Len=1460
297	21:00:28.747449	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=123377 Ack=1 Win=131328 Len=1460
298	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=126297 Ack=1 Win=131328 Len=1460
299	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=127757 Ack=1 Win=131328 Len=1460
300	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=129217 Ack=1 Win=131328 Len=1460
301	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[PSH, ACK]	Seq=130677 Ack=1 Win=131328 Len=1460
302	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=132137 Ack=1 Win=131328 Len=1460
303	21:00:28.747461	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=133597 Ack=1 Win=131328 Len=1460
304	21:00:28.747509	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=136517 Ack=1 Win=131328 Len=1460
305	21:00:28.747520	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=140897 Ack=1 Win=131328 Len=1460
306	21:00:28.747520	128.119.245.12	10.0.0.84	TCP	1514	[TCP Retransmission]	58166 → 80	[ACK]	Seq=142357 Ack=1 Win=131328 Len=1460
307	21:00:28.763905	128.119.245.12	10.0.0.84	TCP	90	80 → 58166	[ACK]	Seq=1 Ack=113157 Win=235776 Len=0 SLE=143817 SRE=153058 SLE=137977 SRE=12	

**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).**

The receiver typically acknowledges 1460 bytes data.

For the sequence number 1 from the client computer, the receiver sent an immediate cumulative ACK. For the other cases, the receiver always sent a partial ACK. Thus, the receiver sent multiple ACKs to acknowledge one TCP segment.

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

The throughput is almost 1.5 Mbps.

Wireshark -> Statistics -> TCP stream graph -> Throughput

