Vlad Predovic

Due 5/24/2016

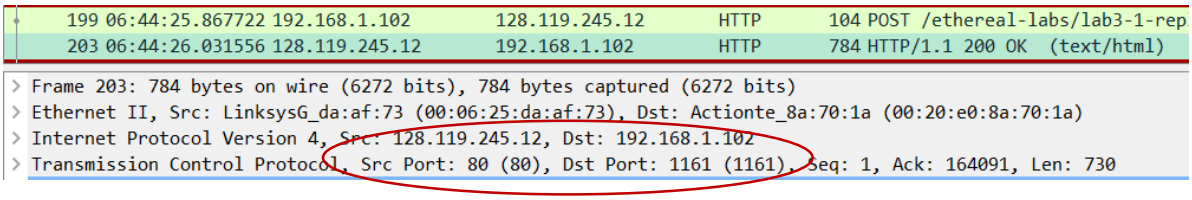
CS 372

Lab 2

1. Answer the following questions:

a) What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

IP Address: 192.168.1.102 Port Number: 1161

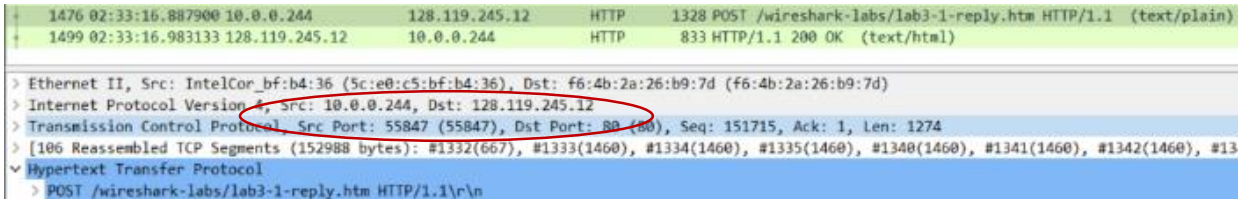


b) What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

IP Address: 128.119.245.12 Port Number: 80

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

c) What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?



IP Address: 10.0.0.244 Port Number: 55847

2. 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. In wireshark, the SYN flag is set raised (set to 1), identifying it as a SYN segment.

1	06:44:20.570381	192.168.1.102	128.119.245.12	TCP	62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	06:44:20.593553	128.119.245.12	192.168.1.102	TCP	62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1

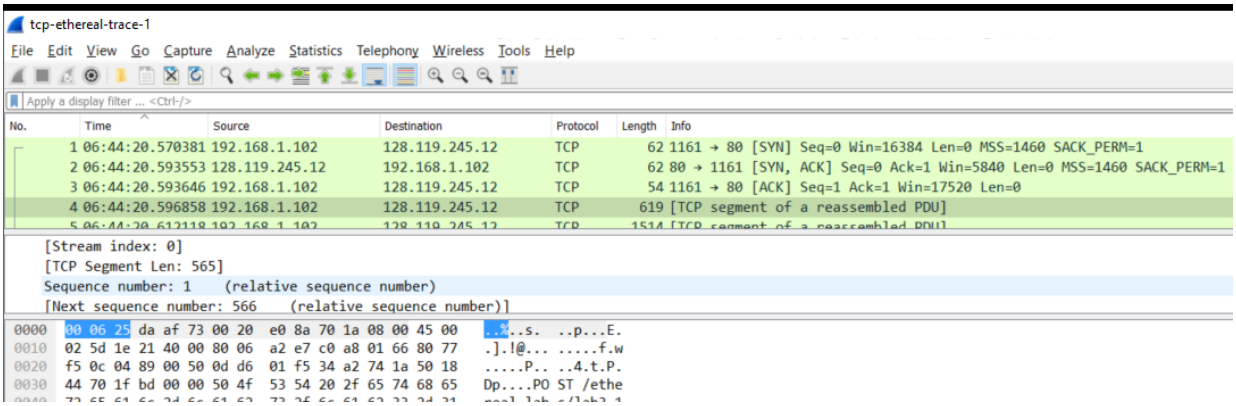
3. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

The sequence number is set to 0. The aacknowledgement field is set to 1. This is because the acknowledgement field is set to the client_isn + 1. In this case the client_isn(sequence number) was 0.

The SYN and ACK flags are both raised. This is why it constitutes as the SYNACK segment.

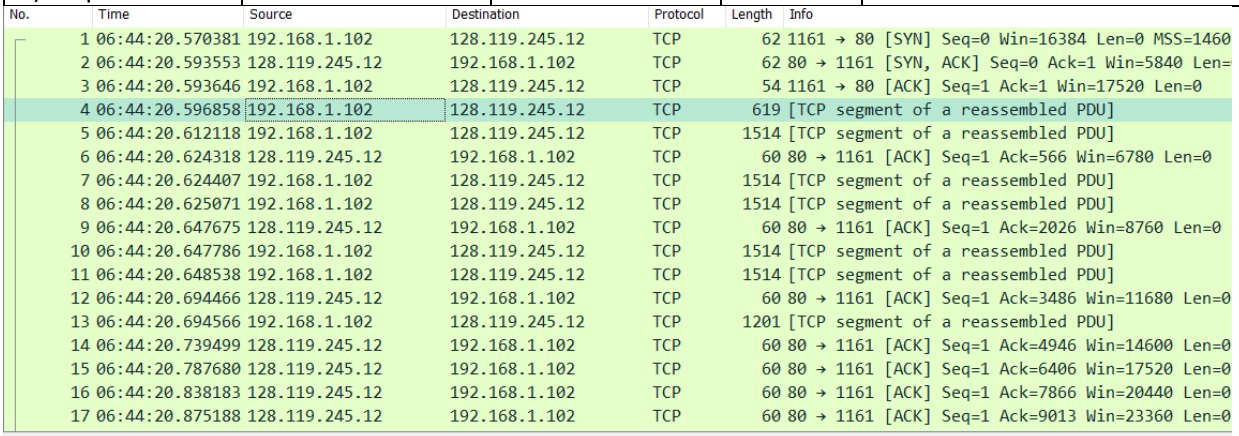
4. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Sequence Number: 1

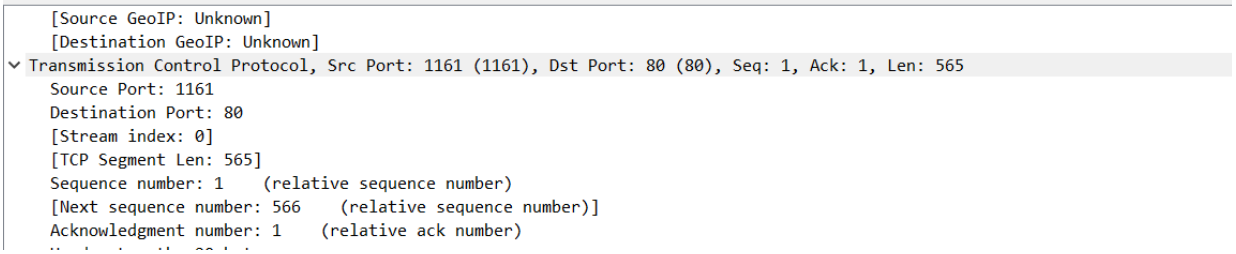


5.

	Sent Time	Time ACK received	RTT seconds	Est RTT (after ACK rcpt) In seconds
1) Seq #: 1	06:44:20.596858	06:44:20.624318	0.02746	0.02746
2) Seq #: 566	06:44:20.612118	06:44:20.647675	0.035557	0.0285
3) Seq #: 2026	06:44:20.624407	06:44:20.694466	0.070059	0.0337
4) Seq #: 3486	06:44:20.625071	06:44:20.739499	0.114428	0.0438
5) Seq #: 4946	06:44:20.647786	06:44:20.787680	0.139894	0.0558
6) Seq #: 6406	06:44:20.648538	06:44:20.838183	0.189645	0.0725



No.	Time	Source	Destination	Protocol	Length	Info
1	06:44:20.570381	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	06:44:20.593553	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
3	06:44:20.593646	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	06:44:20.596858	192.168.1.102	128.119.245.12	TCP	619	[TCP segment of a reassembled PDU]
5	06:44:20.612118	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
6	06:44:20.624318	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	06:44:20.624407	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
8	06:44:20.625071	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
9	06:44:20.647675	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	06:44:20.647786	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
11	06:44:20.648538	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
12	06:44:20.694466	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	06:44:20.694566	192.168.1.102	128.119.245.12	TCP	1201	[TCP segment of a reassembled PDU]
14	06:44:20.739499	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	06:44:20.787680	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	06:44:20.838183	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	06:44:20.875188	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0



```
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 565
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 565]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 566    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
```

$$EstimatedRTT_{New} = (1-\alpha)\,EstimatedRTT_{Prev} + \alpha \times SampleRTT_{Recent}$$

Assuming 1st estRTT = 1st sampleRTT α = .125

EstimatedRTT1: 0.875 * .02746 + 0.125 * .02746 = .02746

EstimatedRTT 2: 0.875 * .02746+ 0.125 * 0.035557 = 0.0285

EstimatedRTT 3: 0.875 * 0.035557+ 0.125 * 0.070059 = 0.0337

EstimatedRTT 4: 0.875 * 0.070059+ 0.125 * 0.114428 = 0.0438

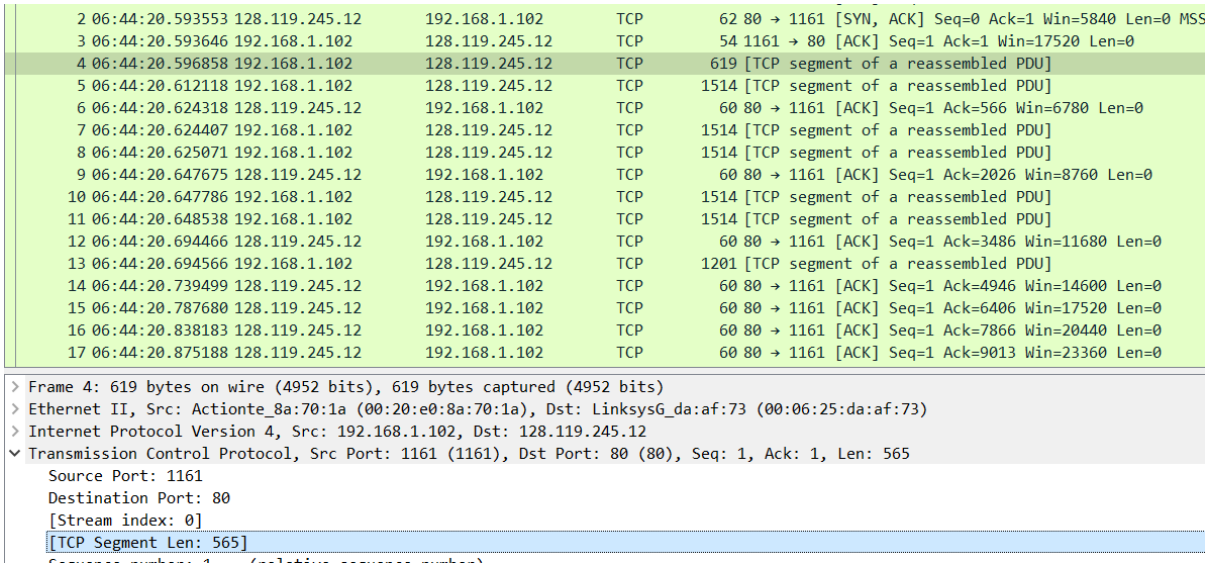
EstimatedRTT 5: 0.875 * 0.114428+ 0.125 * 0.139894 = 0.0558

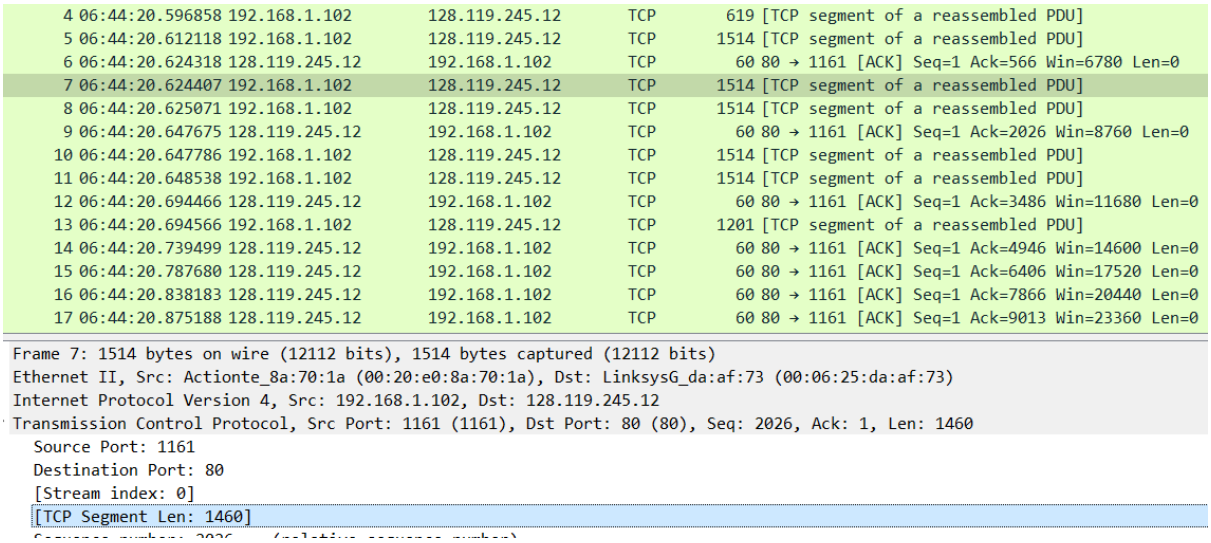
EstimatedRTT 6: 0.875 * 0.139894+ 0.125 * 0.189645 = 0.0725

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

1: 565 bytes

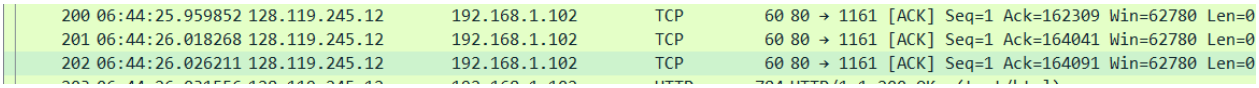
2 through 6: 1460 bytes





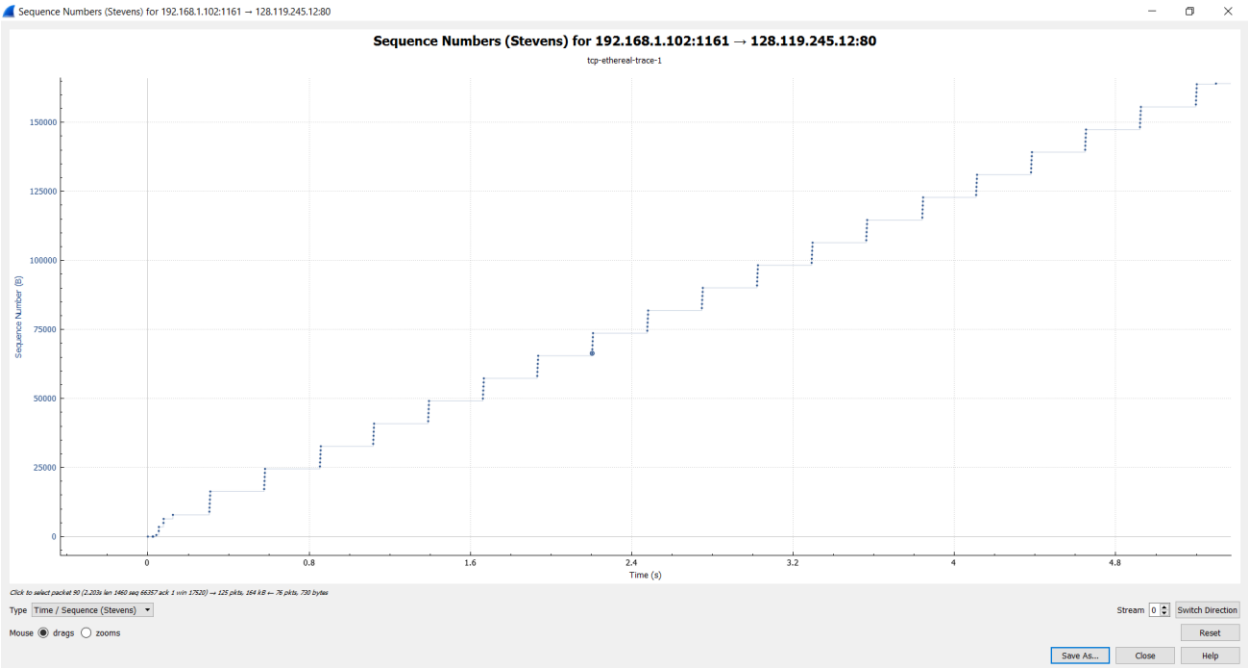
7. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Min amount of buffer space is 5840. Can be seen in the first picture at the top right of question 6. Increases to 62780 for the entinre trace. Sender is never throttled.



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

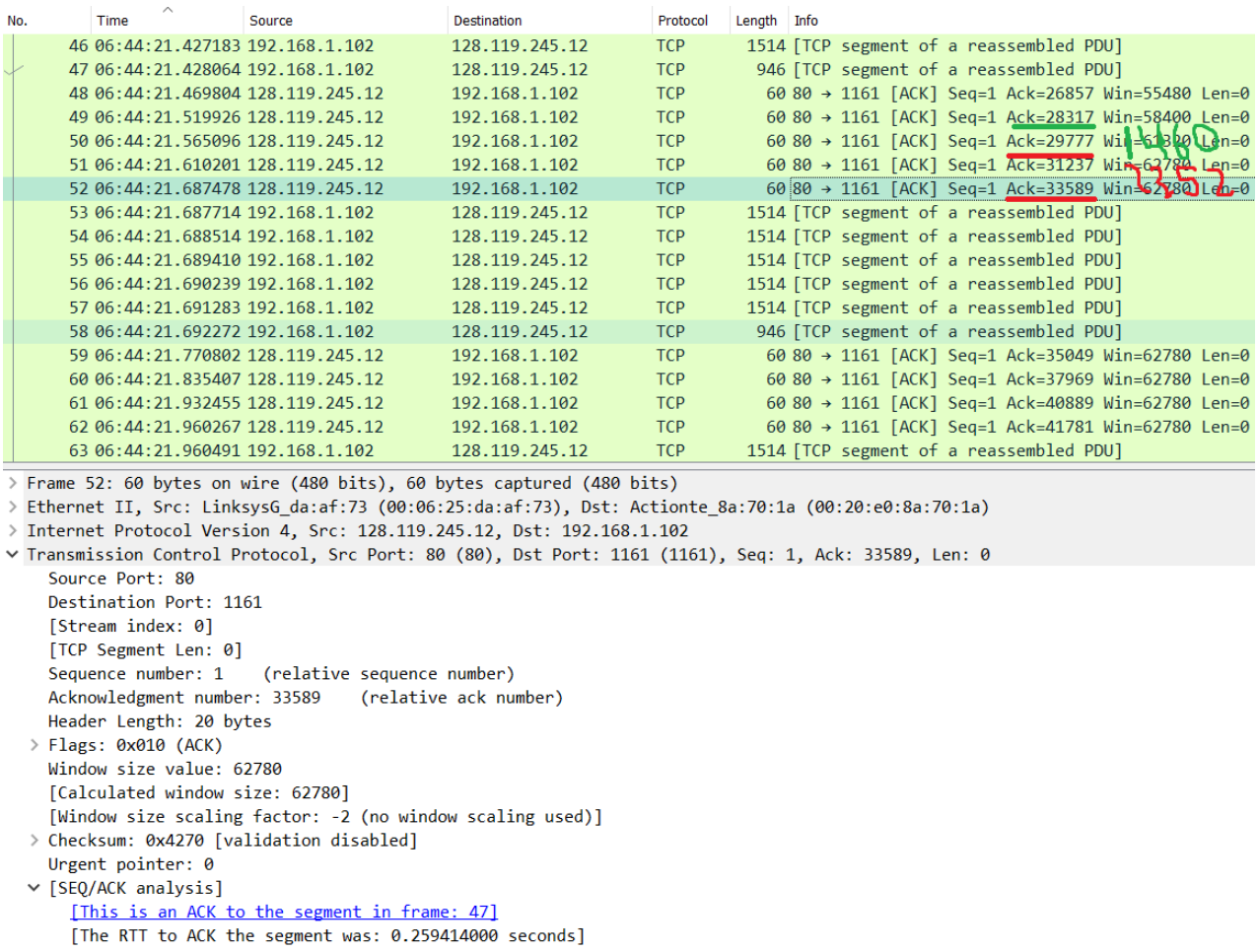
No, I checked the datils of the HTTP segment and also the sequence numbers. If a segment was retransmitted (due to getting lost for example), it's sequence number woud be lower than the ones before and after it (due to arriving out of order). In the following graph, you can clearly tell because all the sequence numbers increase with respect to time.



9. 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 247 in the text)?

In the first segment sent 566 bytes are acknowledged. For most of the others directly responded to 1460 bytes are acknowledged up until item 47.

However, at item number 47 the behaviour seems to change as the acknowledgements now come once every two packets and the ACK numbers increment by 2352 as opposed to 1460. This trend continues until the end of transmission.



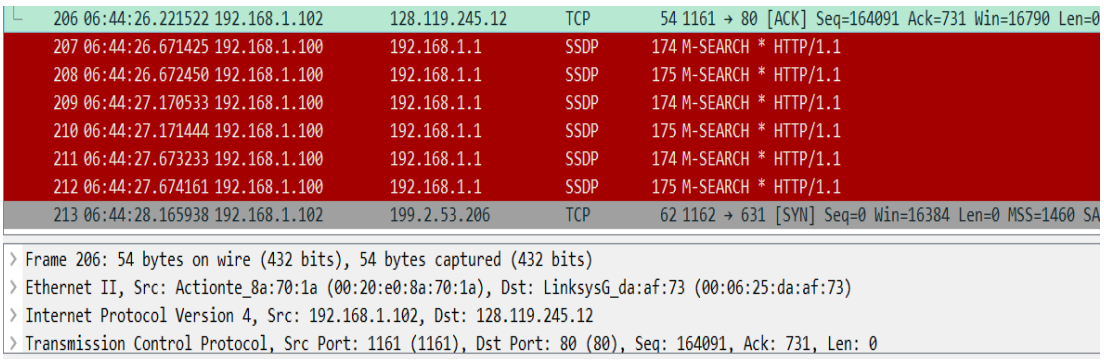
No.	Time	Source	Destination	Protocol	Length	Info
46	06:44:21.427183	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
47	06:44:21.428064	192.168.1.102	128.119.245.12	TCP	946	[TCP segment of a reassembled PDU]
48	06:44:21.469804	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=26857 Win=55480 Len=0
49	06:44:21.519926	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=28317 Win=58400 Len=0
50	06:44:21.565096	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=29777 Win=61320 Len=0
51	06:44:21.610201	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=31237 Win=62780 Len=0
52	06:44:21.687478	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=33589 Win=62780 Len=0
53	06:44:21.687714	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
54	06:44:21.688514	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
55	06:44:21.689410	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
56	06:44:21.690239	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
57	06:44:21.691283	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]
58	06:44:21.692272	192.168.1.102	128.119.245.12	TCP	946	[TCP segment of a reassembled PDU]
59	06:44:21.770802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=35049 Win=62780 Len=0
60	06:44:21.835407	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=37969 Win=62780 Len=0
61	06:44:21.932455	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=40889 Win=62780 Len=0
62	06:44:21.960267	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=41781 Win=62780 Len=0
63	06:44:21.960491	192.168.1.102	128.119.245.12	TCP	1514	[TCP segment of a reassembled PDU]

```
> Frame 52: 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
v Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1161 (1161), Seq: 1, Ack: 33589, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 33589    (relative ack number)
    Header Length: 20 bytes
  > Flags: 0x010 (ACK)
    Window size value: 62780
    [Calculated window size: 62780]
    [Window size scaling factor: -2 (no window scaling used)]
  > Checksum: 0x4270 [validation disabled]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 47]
      [The RTT to ACK the segment was: 0.259414000 seconds]
```

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

The last ACK represents the next byte number expected. The first byte had sequence number 1. Therefore 164090 bytes were sent during the time period the sniffer ran. Dividing this by the amount of time ran would give the result. The time ran is calculated by subtracting the time of this last packet from the first one (item 4 from item 206). 6:44:26.221522 – 6:44:20.596858 = 5.624664 seconds

As a result: 164090 bytes / 5.624664 sec = 29173.298 = 29.17 KB/sec



206	06:44:26.221522	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
207	06:44:26.671425	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
208	06:44:26.672450	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
209	06:44:27.170533	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
210	06:44:27.171444	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
211	06:44:27.673233	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
212	06:44:27.674161	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
213	06:44:28.165938	192.168.1.102	199.2.53.206	TCP	62	1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SA

```
> Frame 206: 54 bytes on wire (432 bits), 54 bytes captured (432 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 (1161), Dst Port: 80 (80), Seq: 164091, Ack: 731, Len: 0
```