

CS305B Lab Report 9

11812418 FanQingyuan

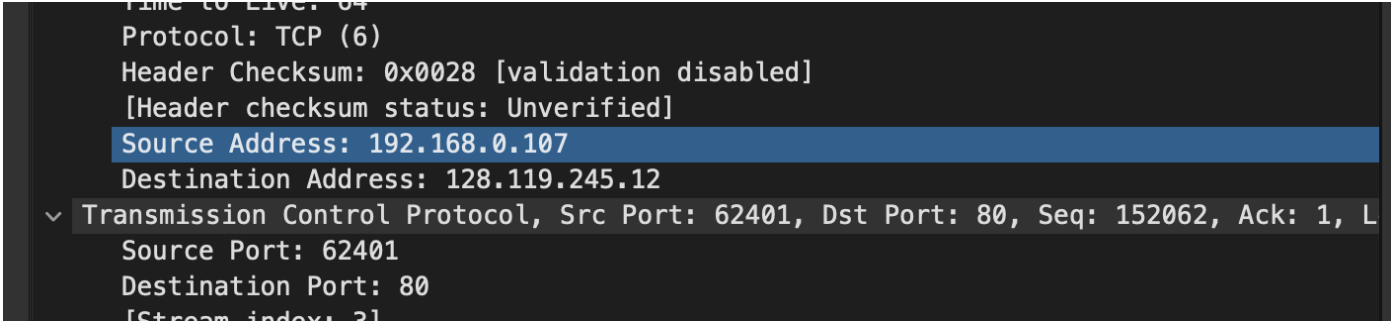
Questions 3-10 of Wireshark_TCP_v7.0.pdf

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?

IP address: 192.168.0.107

TCP port number: 62401



Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x0028 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.107
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 62401, Dst Port: 80, Seq: 152062, Ack: 1, L
Source Port: 62401
Destination Port: 80
[Stream index: 3]

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?

Sequence number: 0

The SYN flag is set to 1 and it indicates that this segment is a SYN segment

```
Destination Address: 128.119.245.12
v Transmission Control Protocol, Src Port: 62401, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 62401
  Destination Port: 80
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 4101011100
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1011 .... = Header Length: 44 bytes (11)
  v Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...0 = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....S.]
```

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?

SYNACK sequence number:

```

Transmission Control Protocol, Src Port: 80, Dst Port: 62401, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 62401
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2577391524
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 4101011101
  1010 .... = Header Length: 40 bytes (10)
  Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    0 .... = Congestion Window Reduced (CWR): Not set
0000 38 f9 d3 75 70 88 94 d9 b3 9b 2e 29 08 00 45 00 8 up... ..) ..E
0010 00 3c 00 00 40 00 1a 06 2a 25 80 77 f5 0c c0 a8 <...@...*%..w...
0020 00 6b 00 50 f3 c1 99 9f df a4 f4 70 76 9d a0 12 k.P... ..pv...
0030 71 20 69 77 00 00 02 04 05 78 04 02 08 0a b5 c2 q iw... ..x.....
0040 9b 0e f6 c0 17 06 01 03 03 07

```

Value of acknowledgement field in the SYNACK segment sequence number: 1

```

1010 .... = Header Length: 40 bytes (10)
  Flags: 0x012 (SYN, ACK)
    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
    .... .... ...0 = Fin: Not set
  [TCP Flags: .....A..S.]
Window: 28960

```

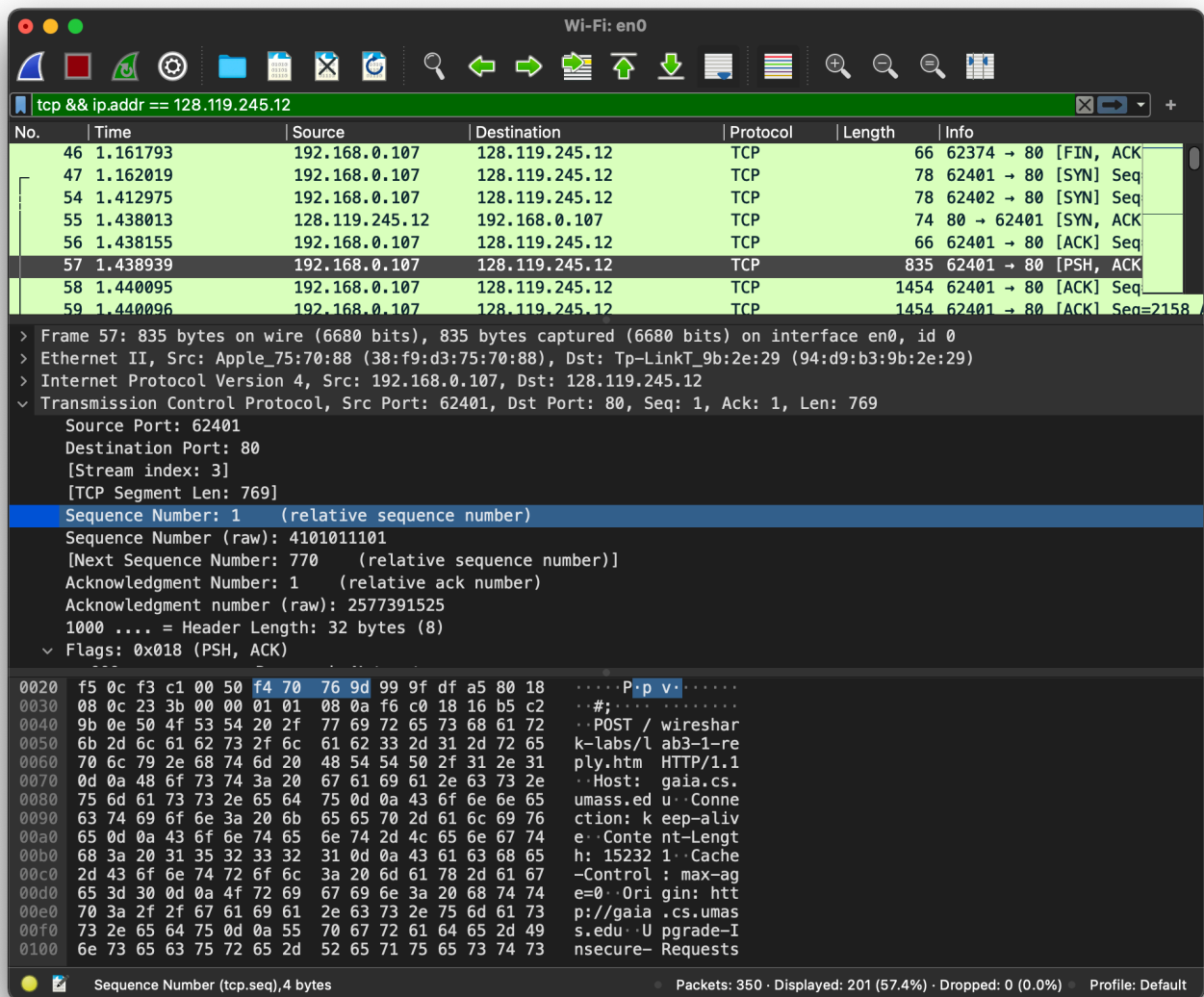
The value of the ACKnowledgement field in the SYNACK segment is determined by adding 1 to the initial sequence number of SYN segment from the client.

The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.

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.

Sequence number: 1



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

Segment NO	Capture NO	Capture NO (ACK)	Sequence number	Sent time (s)	ACK received time (s)	RTT (s)	Estimate RTT
1	57	72	1	1.438939	1.687464	0.248525	0.2485
2	58	75	770	1.440095	1.726096	0.286001	0.2813
3	59	77	2158	1.440096	1.729284	0.289188	0.2841
4	60	80	3546	1.440098	1.729821	0.289723	0.2846
5	61	Segment Lost	4934	1.440098	Lost	-	-
6	62	81	6322	1.440099	1.729826	0.289727	0.2846

$$EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT$$

8

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

Segment NO	Capture NO	Length
1	57	769
2	58	1388
3	59	1388
4	60	1388
5	61	1388
6	62	1388

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?

minimum amount of available buffer space: 28960

No.	Time	Source	Destination	Protocol	Length
46	1.161793	192.168.0.107	128.119.245.12	TCP	
47	1.162019	192.168.0.107	128.119.245.12	TCP	
54	1.412975	192.168.0.107	128.119.245.12	TCP	
55	1.438013	128.119.245.12	192.168.0.107	TCP	
56	1.438155	192.168.0.107	128.119.245.12	TCP	
57	1.438939	192.168.0.107	128.119.245.12	TCP	
58	1.440095	192.168.0.107	128.119.245.12	TCP	
59	1.440096	192.168.0.107	128.119.245.12	TCP	
60	1.440098	192.168.0.107	128.119.245.12	TCP	
61	1.440098	192.168.0.107	128.119.245.12	TCP	
62	1.440099	192.168.0.107	128.119.245.12	TCP	
63	1.440100	192.168.0.107	128.119.245.12	TCP	
64	1.440101	192.168.0.107	128.119.245.12	TCP	
65	1.440102	192.168.0.107	128.119.245.12	TCP	
66	1.440103	192.168.0.107	128.119.245.12	TCP	
Next Sequence Number: 1 (relative sequence number) Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 4101011101 1010 = Header Length: 40 bytes (10)					
> Flags: 0x012 (SYN, ACK)					
Window: 28960					
[Calculated window size: 28960]					
Checksum: 0x6977 [unverified]					
[Checksum Status: Unverified]					

The sender is never throttled due to lacking of receiver buffer space by inspecting this trace.

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

Yes, in the screenshot below, while the tcp stream encountered a retransmission, the windows size was reset to 2060.

The screenshot shows a Wireshark packet capture on the interface 'Wi-Fi: en0'. The filter is 'tcp && ip.addr == 128.119.245.12'. The packet list shows several TCP segments. Packet 19 (highlighted in blue) is a [TCP Retransmission] from 192.168.0.107 to 128.119.245.12, Seq=62374, Len=66. The packet details pane shows the Transmission Control Protocol section with the following information:

- Source Port: 62374
- Destination Port: 80
- [Stream index: 2]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1966591230
- [Next Sequence Number: 2 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 1900886569
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x011 (FIN, ACK)

The packet bytes pane shows the raw data of the packet, including the TCP header and payload. The window size value from the TCP header is 2 bytes.

At the bottom of the window, the status bar indicates: Packets: 350 · Displayed: 201 (57.4%) · Dropped: 0 (0.0%) · Profile: Default

