Lab 4: Exploring TCP/ z5146286

Exercise 1: Understanding TCP using Wireshark

Question 1. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? 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?

A:

1) IP Address: 128.119.245.12

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.102	128.119.245.12	TCP	62

2) Send port :80

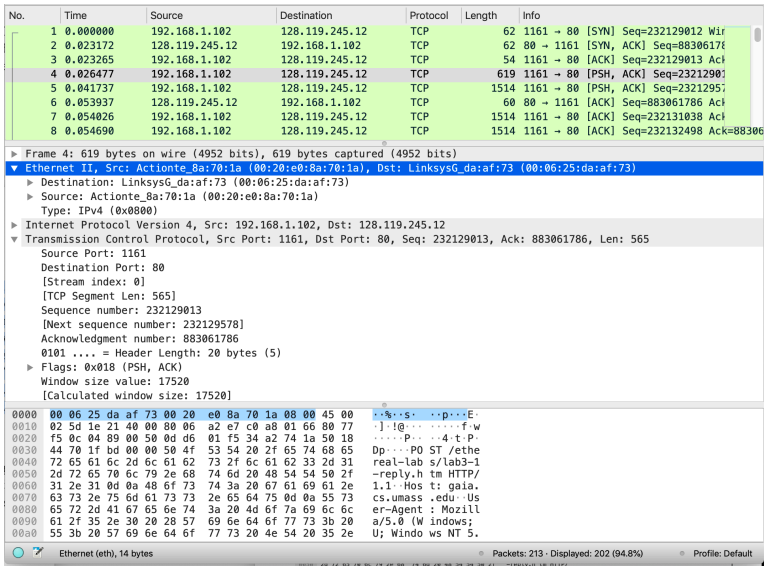
```
Source Port: 1161
Destination Port: 80
```

3) Source addresss:192.168.1.102
   Source port :1161

Question 2. 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 Ethereal window, looking for a segment with a "POST" within its DATA field.

A:

Sequence number: 232129013



Question 3. 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) sent from the client to the web server (Do not consider the ACKs received from the server as part of these six segments)? 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 relevant parts of Section 3.5 or lecture slides) after the receipt of each ACK? Assume that the initial value of EstimatedRTT is equal to the measured RTT (SampleRTT) for the first segment, and then is computed using the EstimatedRTT equation for all subsequent segments. Set alpha to 0.125.

A:

$$EstimatedRTT = 0.87*EstimatedRTT + 0.125*SampleRTT$$

Seq	Sent time	Receive ACK time	RTT	EstimatedRTT
232129013	0.026477	0.053937	0.027460	0.027460
232129578	0.041737	0.077294	0.035557	0.028472
232131038	0.054026	0.124085	0.124085	0.033670
232131498	0.054690	0.169118	0.114428	0.043765
232133958	0.077405	0.217299	0.139894	0.055781
232135418	0.078157	0.267802	0.189645	0.072514

Question 4. What is the length of each of the first six TCP segments?

Seq	TCP segment Len
232129013	565
232129578	1460
232131038	1460
232131498	1460
232133958	1460
232135418	1460

Question 5. 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?

A5:

the minimum amount of available buffer space at the receiver actually is window size, which is 5840 Bytes.

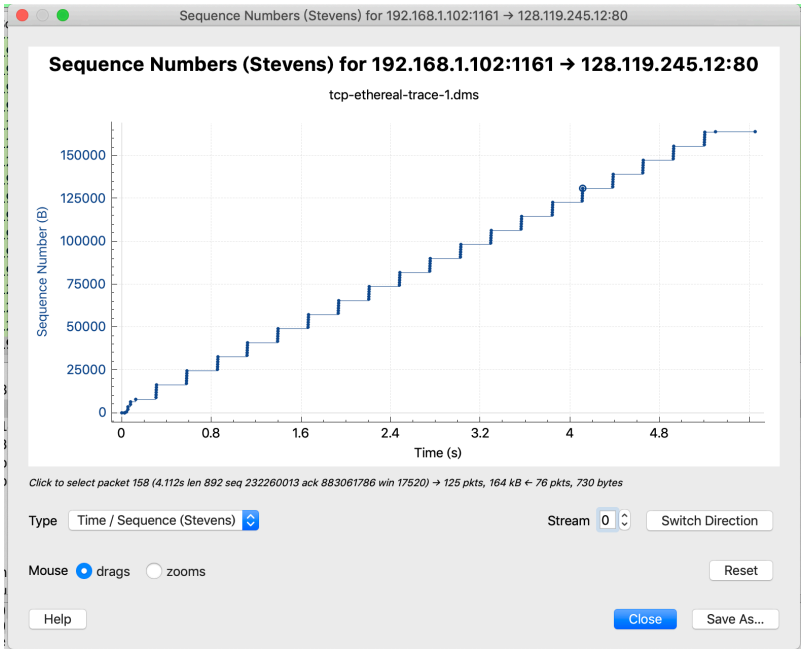
No, Since the sender' s buffer is always greater than segment size.

```
▶ Flags: 0x012 (SYN, ACK)
  Window size value: 5840
  [Calculated window size: 5840]
  Checksum: 0x774d [unverified]
  [Checksum Status: Unverified]
```

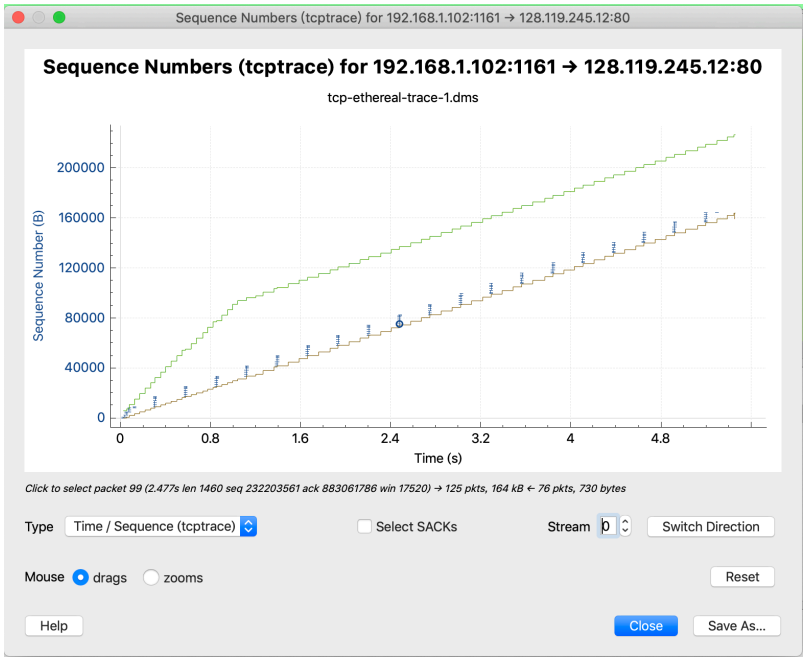
Question 6. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

A6:

I click Statistic->TCP stream graph ->Time Sequence(Stevens)/ Time Sequence(tcptrace)



-Time Sequence(Stevens)-



- Time Sequence(tcptrace)-

Both of graphs above show that none of segment with same sequence number is sent at different time. Thus, there are no retransmitted segments.

Question 7. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (recall the discussion about delayed acks from the lecture notes or Section 3.5 of the text).

A7: Most of receivers acknowledge 1460 bytes data in an ACK.

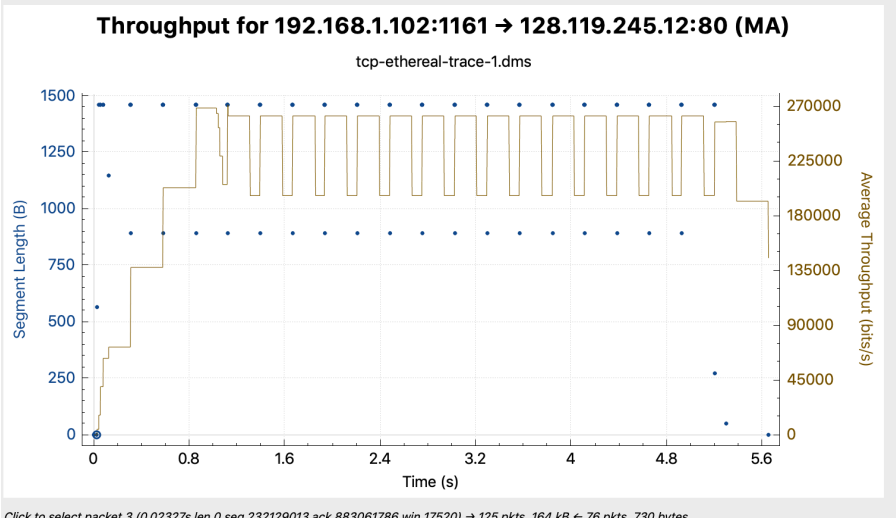
```
    [Time since previous frame in this
TCP payload (1460 bytes)
[Reassembled PDU in frame: 199]
TCP segment data (1460 bytes)
```

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between two ACKs. For example, the difference of the acknowledged sequence numbers of two consecutive ACKs No.79 and No.80 is 2352. Their acknowledged data No.75 and No.77 are 1460 bytes and 892 bytes.

1460 + 892 = 2352

Question 8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

A8:



$$\text{Throughput} = \frac{Total\ amount\ data}{Total\ time}$$

In this case, total time can be set as the whole connection time.

Total amount data = the last acknowledged sequence number of ACK – the first sequence number of segment + TCP segment header = 164090 bytes

Total time = the last ACK time – the first sending time after connection established = 5.455830-0.026477 = 5.429353 s

Throughput = 164090 bytes /5.429353 s = 30223 Byte/s

Exercise 2: TCP Connection Management

Question 1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server?

A1:

Seq number = 2818463618

Question 2. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value?

A2:

1) Sequence number = 1247095790
2) Value of the Acknowledgement = 2818463619
3) Server determine that by SYN sequence number +1 ,which sent by client.

Question 3. What is the sequence number of the ACK segment sent by the client computer in response to the SYNACK? What is the value of the Acknowledgment field in this ACK segment? Does this segment contain any data?

A3:

1) Sequence number = 28184636619
2) Value of the Acknowledgement = 1247095791
3) No, this segment does not contain any data

Question 4. Who has done the active close? client or the server? how you have determined this? What type of closure has been performed? 3 Segment (FIN/FINACK/ACK), 4 Segment (FIN/ACK/FIN/ACK) or Simultaneous close?

A4:

1) At No.304, client has done the active close, and at No.305, server has done it as well.
2) At No.304 and No.305, there is a flag – FIN, it shows client or server active close.
3) Simultaneous close

Question 5. How many data bytes have been transferred from the client to the server and from the server to the client during the whole duration of the connection? What relationship does this have with the Initial Sequence Number and the final ACK received from the other side?

A5:

From client to server:

ISN = 2818463618

2818463652 – 2818463619 = 33

SYN = 1

FIN = 1

Total = 2818463653

Total is equal the final ACK of server.

From client to server:

ISN = 1247095790

1247095831 – 1247095791 = 40

SYN =1

FIN = 1

Total = 1247095832

Total is equal the final ACK of client .