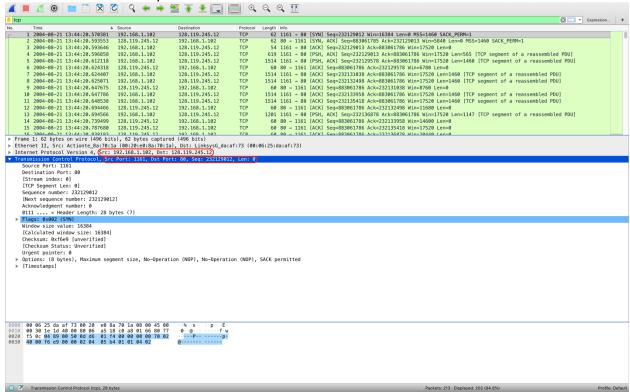
Comp9331 Lab4
StudentID: z5184142
StudentName: JiachenLi

## **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 <a href="mailto:gaia.cs.umass.edu">gaia.cs.umass.edu</a>? Answer:

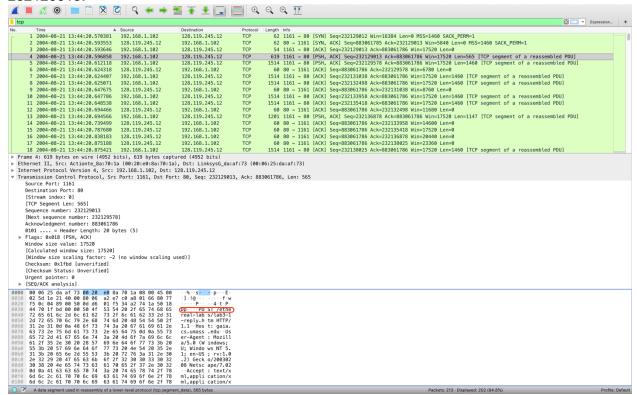
The IP address of <u>gaia.cs.umass.edu</u> is 128.119.245.12. The port number is 80 which is used to send and receive TCP segments for this connection. The IP address of the client is 192.168.1.102 and the port number is 1161.



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.

#### Answer:

The sequence number of the TCP segment containing the HTTP POST command is 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.

### Answer:

The sequence numbers of the first six segments in the TCP connection sent from the client to the webserver is

First:232129013. Second: 232129578. Third: 232131038. Fourth: 232132498. Fifth: 232133958. Sixth: 232135418.

### The time each segment sent is

First: 2004-08-21 13:44:20.596858. Second: 2004-08-21 13:44:20.612118. Third: 2004-08-21 13:44:20.624407. Fourth: 2014-08-21 13:44:20.625071. Fifth: 2004-08-21 13:44:20.647786. Sixth: 2004-08-21 13:44:20.648538.

The time of ACK for each segment received is

First: 2004-08-21 13:44:20.624318. Second: 2004-08-21 13:44:20.647675. Third: 2004-08-21 13:44:20.694466. Fourth: 2004-08-21 13:44:20.739499. Fifth: 2004-08-21 13:44:20.787680. Sixtrh: 2004-08-21 13:44:20.838183.

### The RTT of each segment is

First: 27.460ms. Second: 35.557ms. Third: 70.059ms. Fourth: 114.428ms. Fifth: 139.894ms. Sixth: 189.645ms.

The EstimatedRTT value is

First: 27.460ms. Second: 28.472ms. Third: 33.670ms. Fourth: 43.765ms. Fifth: 55.781ms. Sixth: 72.514ms.

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

### Answer:

The length of the first TCP segments is 565bytes.

The length of the second TCP segments is 1460bytes.

The length of the third TCP segments is 1460 bytes.

The length of the forth TCP segments is 1460bytes.

The length of the fifth TCP segments is 1460bytes.

The length of the sixth TCP segments is 1460bytes.

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? The minimum amount of the available buffer space advertised at the receiver for the entire trace is 5840bytes. Yes, the lack of receiver buffer space will throttle the sender.

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?

### Answer:

There are no retransmitted segments in the trace file. I have checked SEQ/ACK analysis in order to answer this question.

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).

# Answer:

The receiver typically acknowledge 1460 bytes of data in an ACK.

18 2004-08-21 13:44:20.875421	192.168.1.102	128.119.245.12 TCP	1514 1161 → 80 [ACK] S	Seq=232138025 Ack=883061786 Win=	=17520 Len=1460 [TCP segment of a reassemb
19 2004-08-21 13:44:20.876194	192.168.1.102	128.119.245.12 TCP	1514 1161 → 80 [ACK] S	Seq=232139485 Ack=883061786 Win=	=17520 Len=1460 [TCP segment of a reassemb
20 2004-08-21 13:44:20.877073	192.168.1.102	128.119.245.12 TCP	1514 1161 → 80 [ACK] S	Seq=232140945 Ack=883061786 Win=	=17520 Len=1460 [TCP segment of a reassemb
21 2004-08-21 13:44:20.877952	192.168.1.102	128.119.245.12 TCP	1514 1161 → 80 [ACK] S	Seq=232142405 Ack=883061786 Win=	=17520 Len=1460 [TCP segment of a reassemb
22 2004-08-21 13:44:20.879080	192.168.1.102	128,119,245,12 TCP	1514 1161 → 80 [ACK] S	Seg=232143865 Ack=883061786 Win=	=17520 Len=1460 [TCP segment of a reassemb

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

Answer:

The throughput for the TCP connection is 30222.75398 bytes per unit time.

The first transfer sequence number from the client to the server is 232129013, and the last acknowledge number from the server to the client is 232293103.

The time of sending the first packet is 13:44:20.596858, the time of receiving the last packet is 13:44:26.026211. So the throughput is (232293103-23219013)/(6.026211-0.596858) = 30222.75398.

First Sequence Number and sending time:

```
4 2004-08-21 13:44:20.596858 192.168.1.102 128.119.245.12 TCP 619 1161 - 80 [PSH, ACK] Seq=232129013 Ack=883061786 Win=17520 Len=565 [TCP segment of a re...

Last Acknowledge Number and receiving time:

202 2004-08-21 13:44:26.026211 128.119.245.12 192.168.1.102 TCP 60 80 - 1161 [ACK] Seq=883061786 Ack=232293103 Win=62780 Len=0 784 HTTP/1.1 200 0K (text/html)
```

## **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?

Answer:

The sequence number of the TCP SYN segment this is used to initiate the TCP connection between the client and server is 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?

Answer:

The sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN is 1247095790. The value of the Acknowledgement filed in the SYNACK segment is 2818463619. The server determined this value based on the sequence number that sent from the client and the data length of the packet.

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?

Answer:

The sequence number of the ACK segment sent by the client computer in response to the SYNACK is 2818463619. The value of the Acknowledgement field in this ACK segment is 1247095791. No data is contained in this segment.

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?

Answer:

Both have done the active close, because if the client or the server be the active close, then the sequence number of the packet would plus 1. However, the sequence number of the client and server has not been changed. So, it can be determined that both of them do the active close.

	304	10.9.16.201	10.99.6.175	ТСР	50045 > 5000 [FIN, ACK] Seq=2818463652 Ack=1247095831 win=65535
3	305	10.99.6.175	10.9.16.201	ТСР	5000 > 50045 [FIN, ACK] Seq=1247095831 Ack=2818463652 win=262144

Simultaneous closure has been performed.

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? Answer"

33 data bytes have been transferred from the client to the server and 40 data types from the server to the client during the whole duration of the connection. The final ACK received from the other side equals to the amount of data types plus the initial sequence number.