Vigomar Kim Algador

CPE 138 – 03

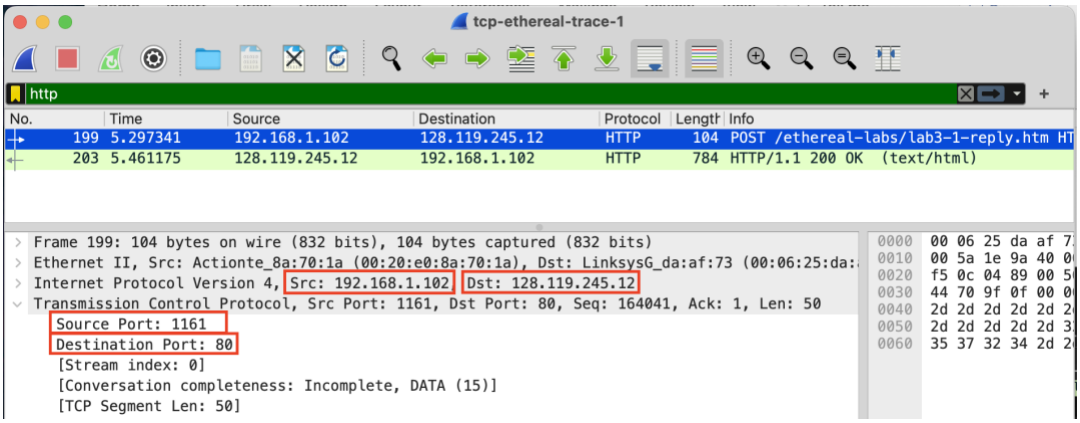
Professor Jun Dai

16 April 2023

Lab 3 – Wireshark – TCP

PART 1: Capturing a bulk TCP transfer from your computer to a remote server

PART 2: A first look at the captured trace

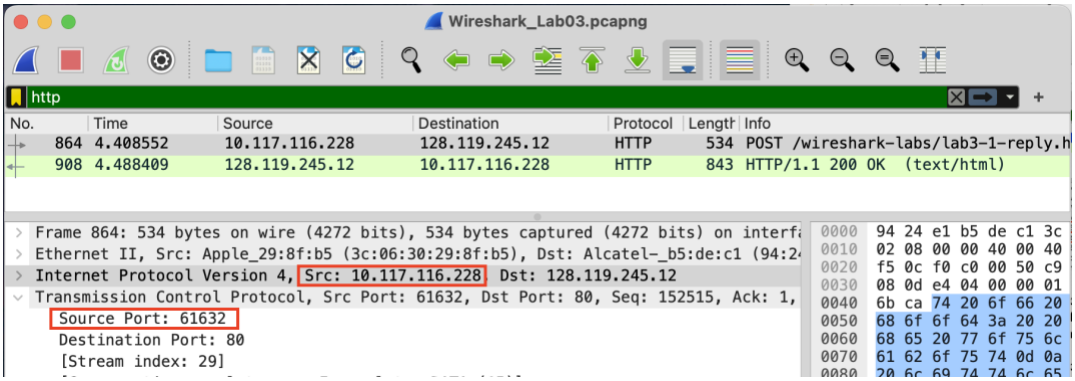


1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
    - The IP address is 192.168.1.102 and TCP port number is 1161.

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 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:

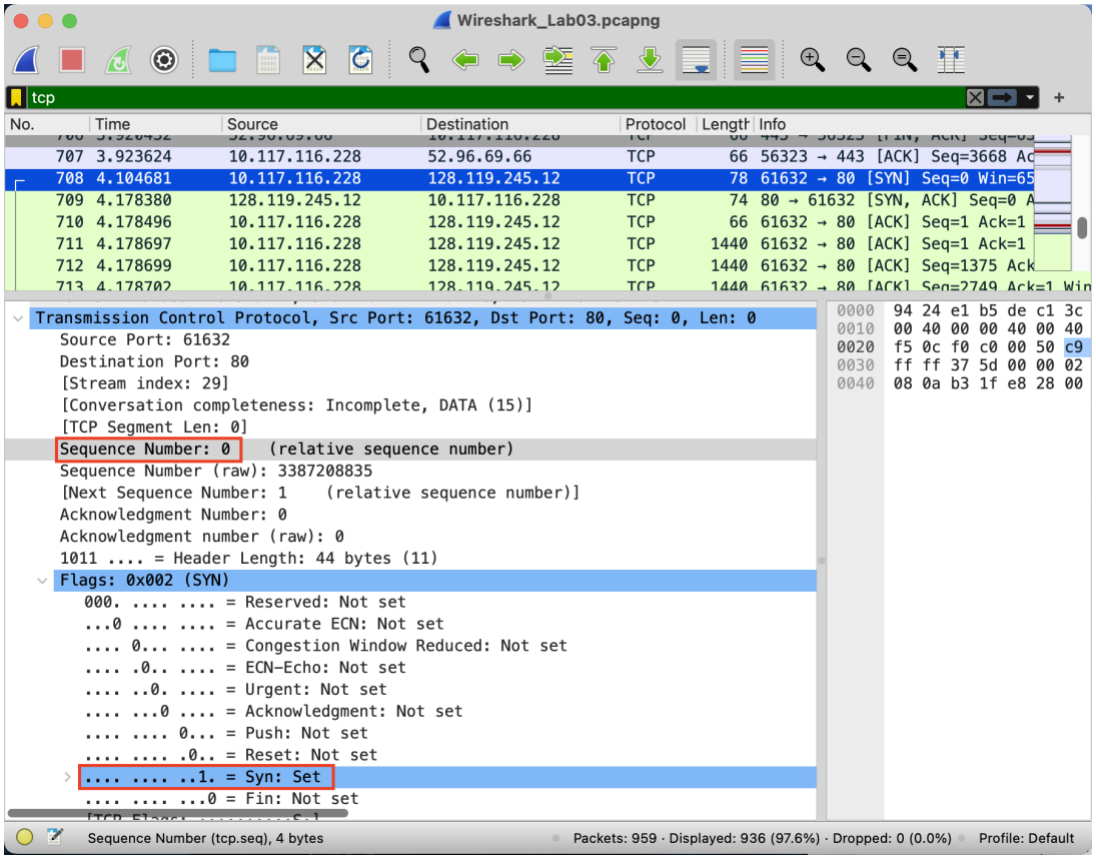
3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?
    - The IP address is 10.117.116.228 and TCP port number is 61632 used to transfer the file.



PART 3: TCP Basics

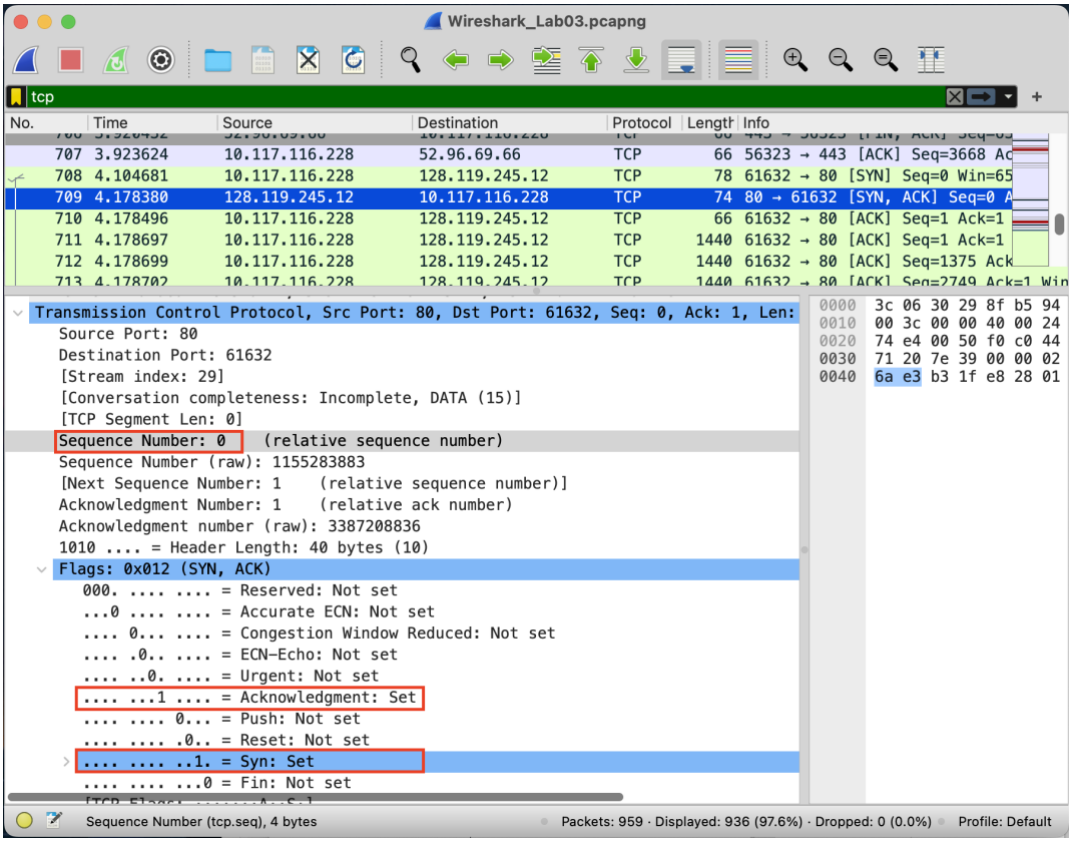
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

    - The sequence number of the TCP SYN segment is 0. The segment that identifies the segment as a SYN segment is where the Syn flag is set to one that is shown in the figure.



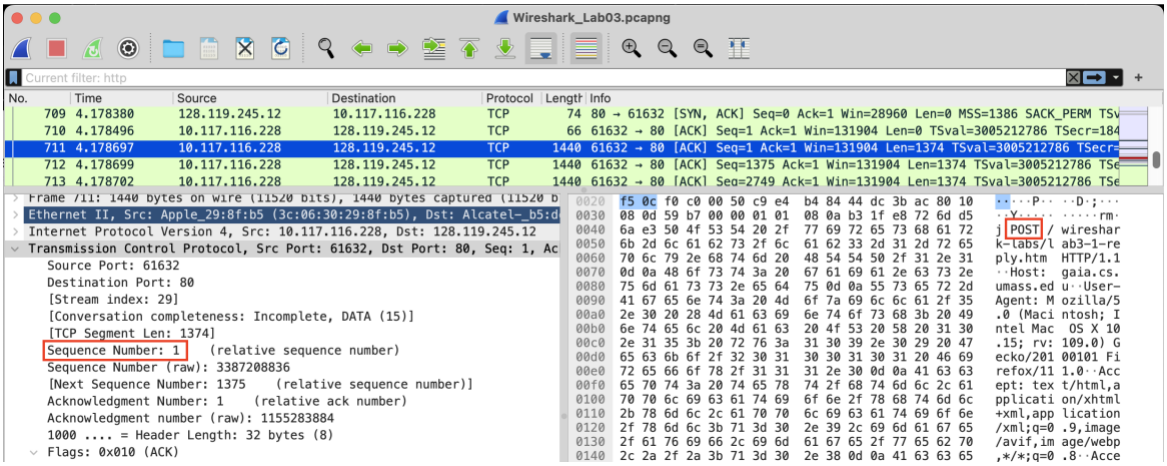
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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

    - The sequence number of the SYNACK segment is 0.
    - The value of the Acknowledgement field in the SYNACK segment is 1.
    - The segment that identifies the segment as a SYNACK segment is where the Syn flag and Acknowledgement are set to 1.



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 of the TCP segment containing the HTTP POST command is 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 239 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 239 for all subsequent segments.

711	4.178697	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=1 Ack=1 Win=131904 Len=1374 TSval=3005212786 TSe
712	4.178699	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=1375 Ack=1 Win=131904 Len=1374 TSval=3005212786
713	4.178702	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=2749 Ack=1 Win=131904 Len=1374 TSval=3005212786
714	4.178704	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=4123 Ack=1 Win=131904 Len=1374 TSval=3005212786
715	4.178706	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=5497 Ack=1 Win=131904 Len=1374 TSval=3005212786
716	4.178708	10.117.116.228	128.119.245.12	TCP	1440 61632 → 80 [ACK] Seq=6871 Ack=1 Win=131904 Len=1374 TSval=3005212786

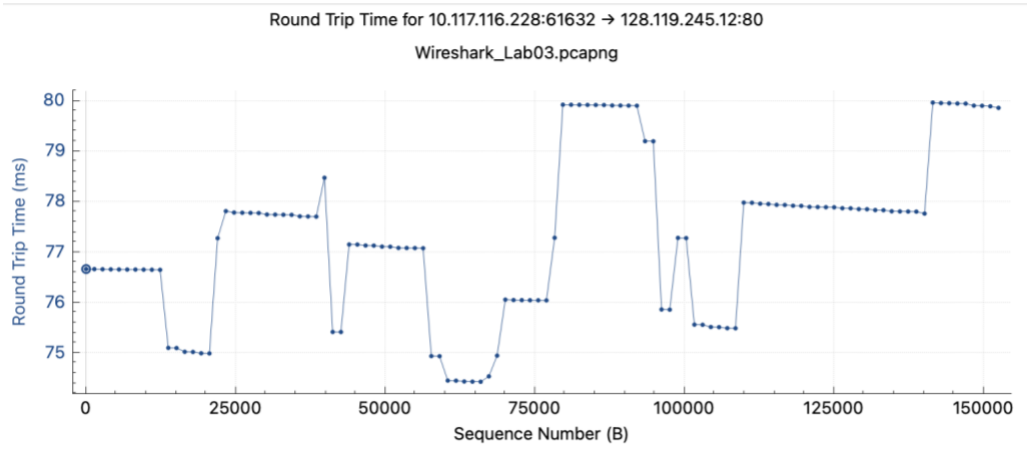
- The first six segments including the HTTP POST are in no. 711, 712, 713, 714, 715, 716 and their sequence number are 1, 1375, 2749, 4123, 5497, 6871, respectively.

721	4.255355	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=1375 Win=31872 Len=0 TSval=1842703152 T
722	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=2749 Win=34816 Len=0 TSval=1842703152 T
723	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=5497 Win=40320 Len=0 TSval=1842703152 T
724	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=8245 Win=45824 Len=0 TSval=1842703152 T
725	4.255357	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=10993 Win=51328 Len=0 TSval=1842703152
726	4.255357	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=13741 Win=56832 Len=0 TSval=1842703152

- The ACK of segments are no. 721, 722, 723, 724, 725, 726

SEGMENT	SENT TIME	ACK RECEIVED TIME	RTT
1	4.178697	4.255355	0.073815
2	4.178699	4.255356	0.076657
3	4.178702	4.255356	0.076652
4	4.178704	4.255356	0.076648
5	4.178706	4.255357	0.076646
6	4.178708	4.255357	0.076642

`Formula: EstimatedRTT` = 0.875 * `EstimatedRTT` + 0.125 * `SampleRTT`



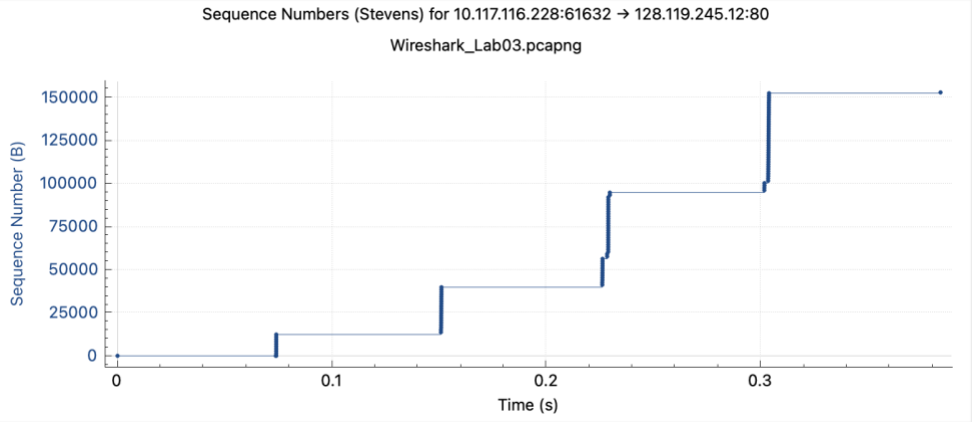
8. What is the length of each of the first six TCP segments?

- The length of the first six TCP segments is 1440.

9. 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?

    - The minimum amount is 131904 from the first TCP segment.

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



    - I think there are no retransmitted segments. From the graph above, we can see that all the sequence numbers are increasing monotonically respect to time.

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 247 in the text).

    From the segment no 721, we can observe that the ACK numbers were 1375, 2749, 5497, 8245, and so on which showed below. From this, we can calculate that the data received 2748 bytes. However, the first segment and second segment only received 1375 and 1374 respectively.

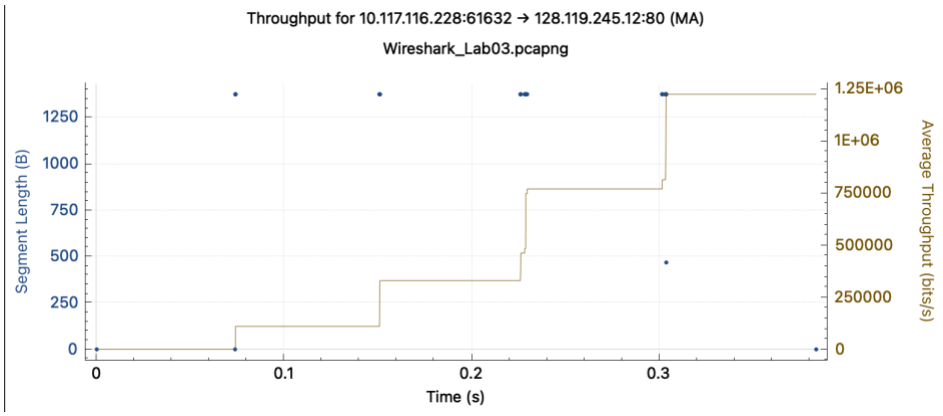
721	4.255355	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=1375 Win=31872 Len=0
722	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=2749 Win=34816 Len=0
723	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=5497 Win=40320 Len=0
724	4.255356	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=8245 Win=45824 Len=0
725	4.255357	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=10993 Win=51328 Len=0
726	4.255357	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=13741 Win=56832 Len=0

    Upon further investigation, I observed that the other ACK numbers that the data were received are also 1375 bytes. This shows that there are cases where the receiver is ACKing every other received segments as data who have 2758 bytes is equal to 1375 * 2.

747	4.330626	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=15115 Win=59648 Len=0
748	4.330627	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=16489 Win=62592 Len=0
749	4.330627	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=17863 Win=65536 Len=0
750	4.330627	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=19237 Win=68352 Len=0
751	4.330627	128.119.245.12	10.117.116.228	TCP	66 80 → 61632 [ACK] Seq=1 Ack=21985 Win=73856 Len=0

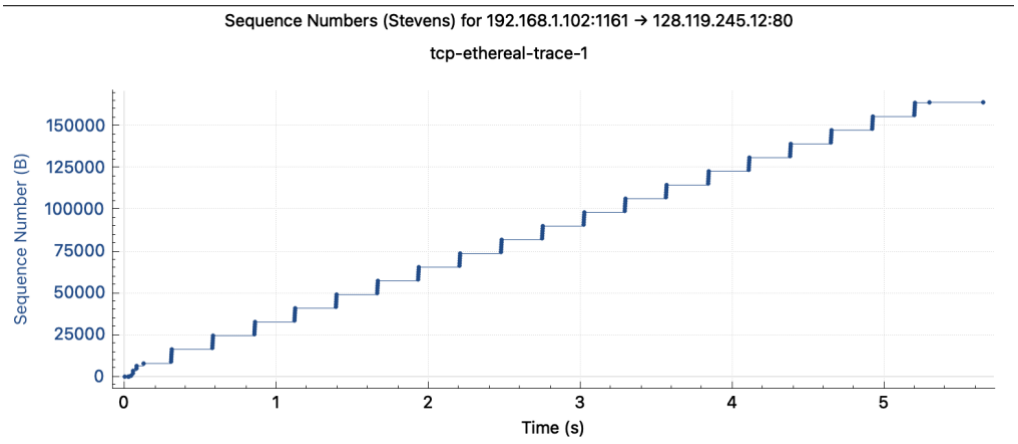
12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Throughput is ¾ W/RTT which W is the window size and RTT is round trip time. The window from the first segment is 2061 and the RTT will be 0.073815 in which the throughput I calculated is 20.940 Kb/s. Below is the full graph of throughput generated from the wireshark.



PART 4: TCP congestion control in action

13. Use the *Time-Sequence-Graph(Stevens*) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.



From the figure above, there's a slow start at the beginning till 0.1242s and I think the congestion avoidance already take over after the slow start at 0.1242s.

14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

The questions were already answered in the last number.