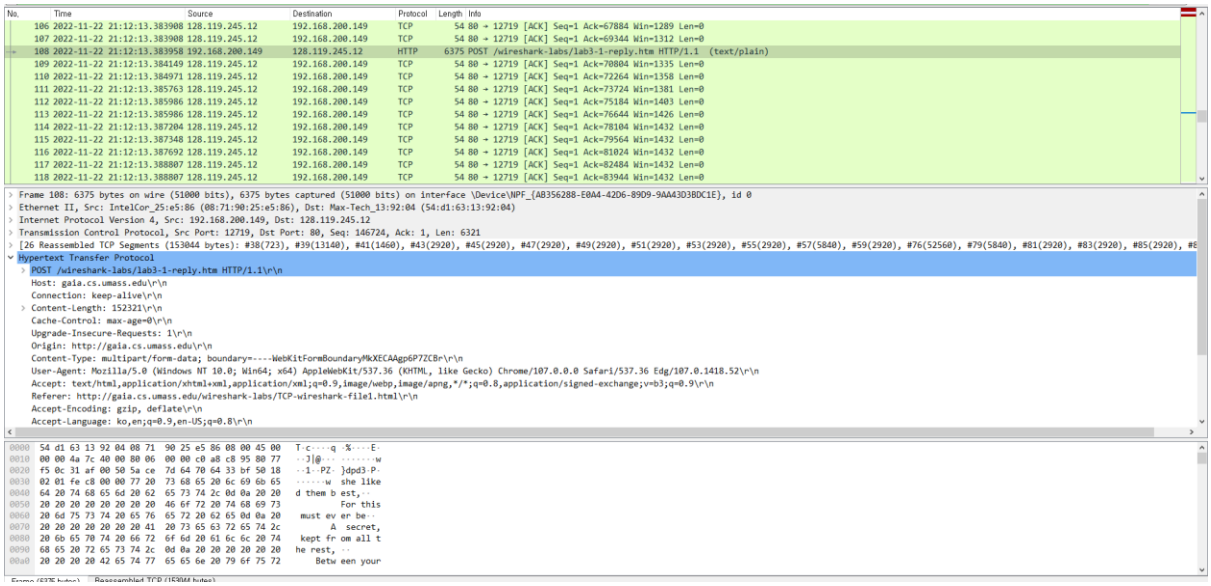
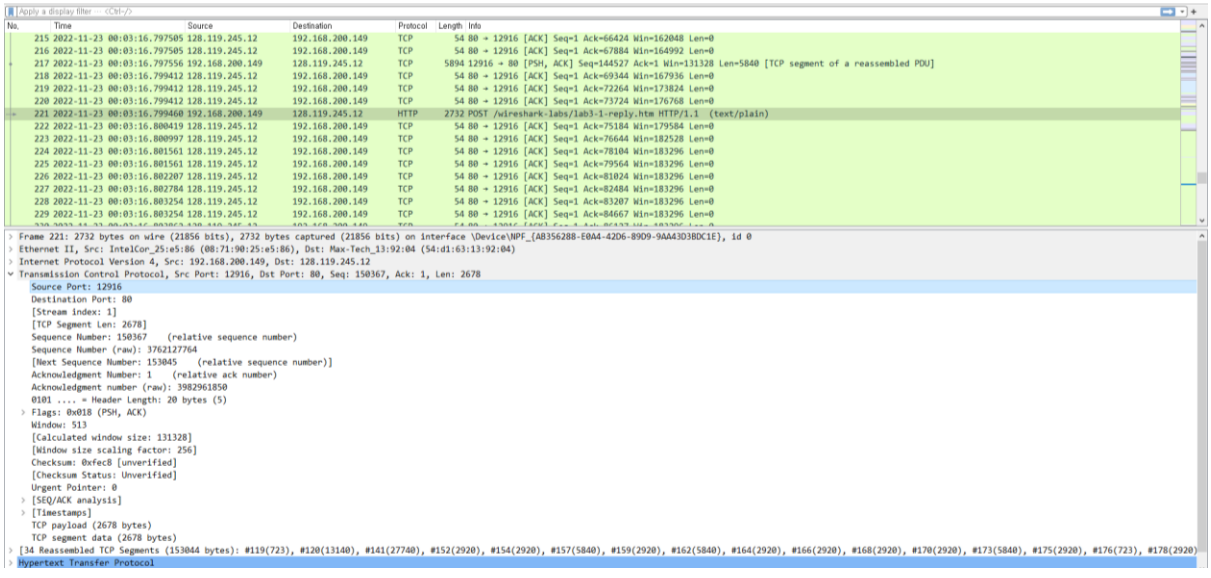
Wireshark Lab 3

ComputerSoftware

2020001658 이유민





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

   ➔ IP Address: 192.168.200.149

   ➔ port: 12916

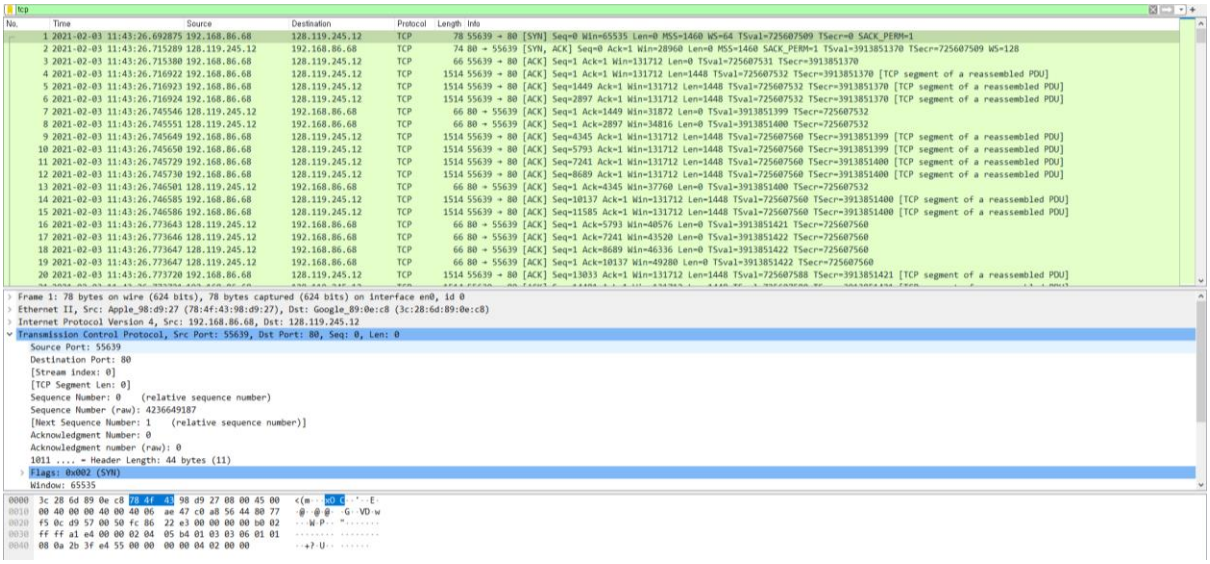
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

   ➔ IP Address: 128.119.245.12

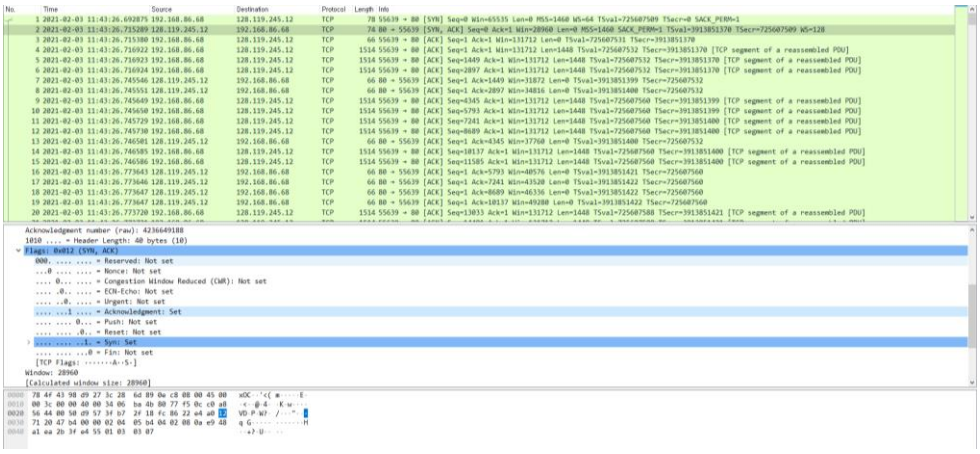
   ➔ Port: 80

3. 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?

   ➔ the sequence number: 0 in the trace



4. What is the sequence number of the SYN ACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?



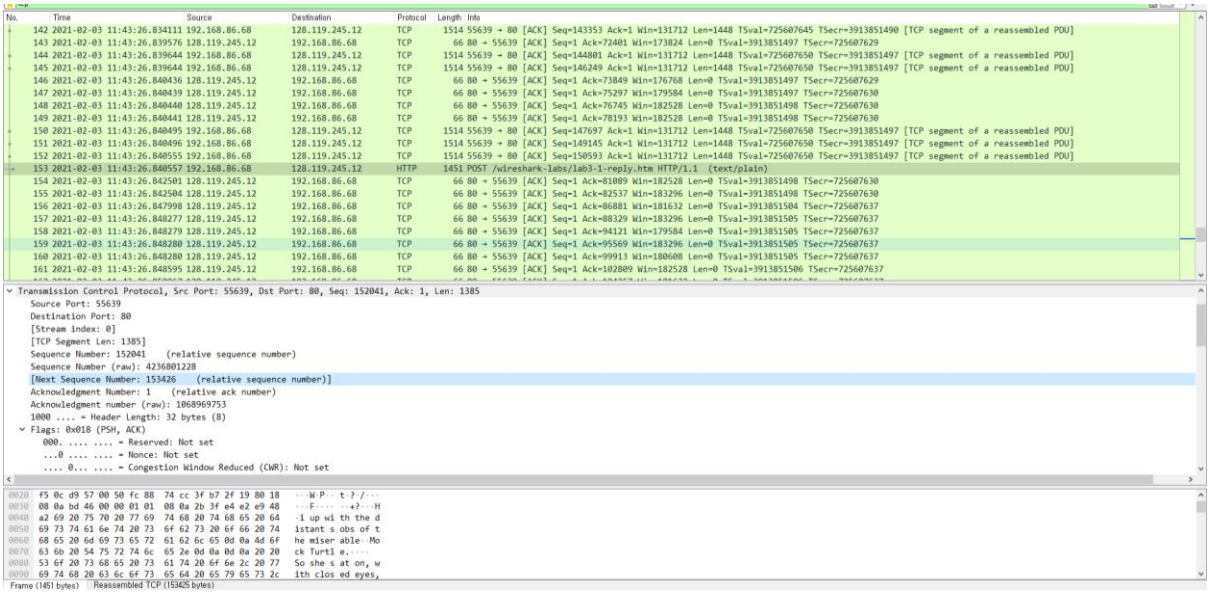
What is it in the segment that identifies the segment as a SYN ACK segment?

➔ the sequence number: 0

What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

➔ 1

5. What is the sequence number of the TCP segment containing the header of the HTTP POST command? Note that in order to find the POST message header, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text "POST" within its DATA field4,5 . How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?



➔ the sequence number: 153426

➔ 1451bytes

6. Consider the TCP segment containing the HTTP "POST" as the first segment in the data transfer part of the TCP connection.

• At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent?

➔ 12:20:26.175345

• At what time was the ACK for this first data-containing segment received?

➔ 12:20.26.194966

• What is the RTT for this first data-containing segment?

➔ 20.26.194966 - 20:26.175345 = 0.019621

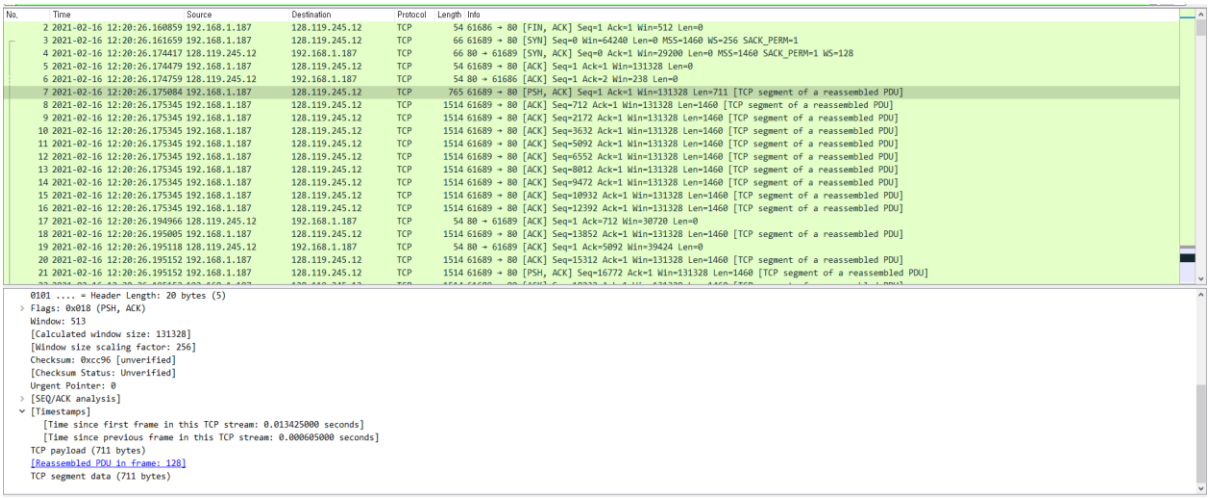
• What is the RTT value the second data-carrying TCP segment and its ACK?

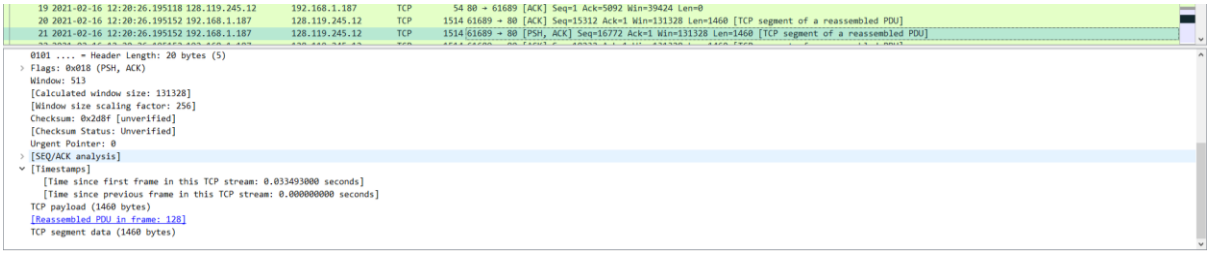
➔ 12:20:26.175345 - 12:20:26.175084 = 0.000261

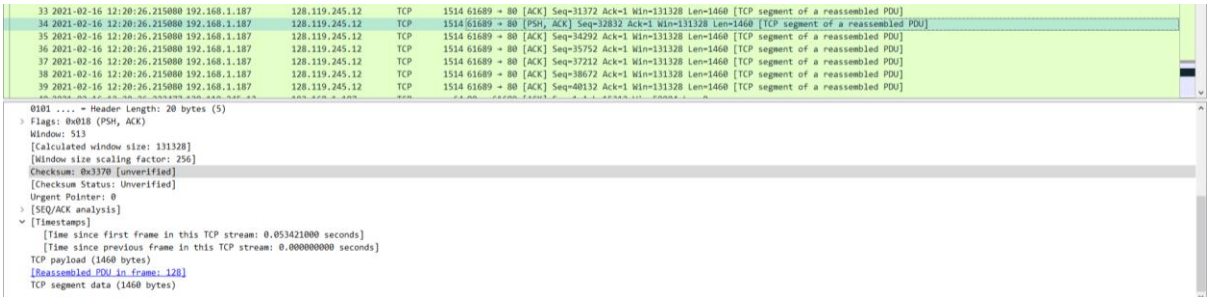
• What is the EstimatedRTT value (see Section 3.5.3, in the text) after the ACK for the second data-carrying segment is received? Assume that in making this calculation after the received of the ACK for the second segment, that the initial value of EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242, and a value of α = 0.125.

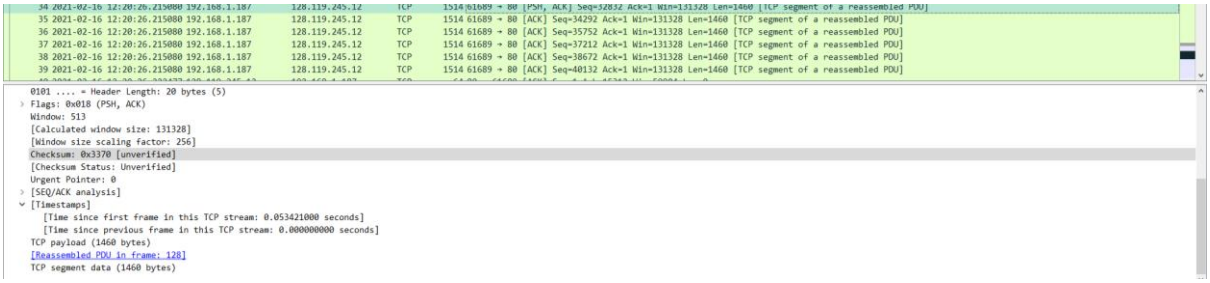
➔ (0.875*0.019621) + (0.125*0.000261) = 0.017168375 + 0.000032625 = 0.017201

7. What is the length (header plus payload) of each of the first four data-carrying TCP segments?









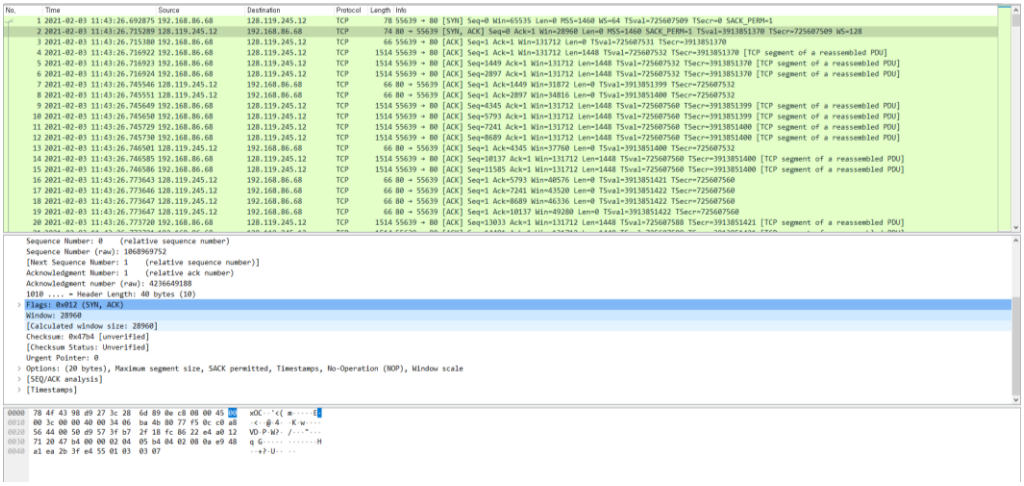
➔ 1th: 711 bytes

➔ 2th: 1460 bytes

➔ 3th: 1460 bytes

➔ 4th:1460bytes

8. What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments7 ? Does the lack of receiver buffer space ever throttle the sender for these first four datacarrying segments?

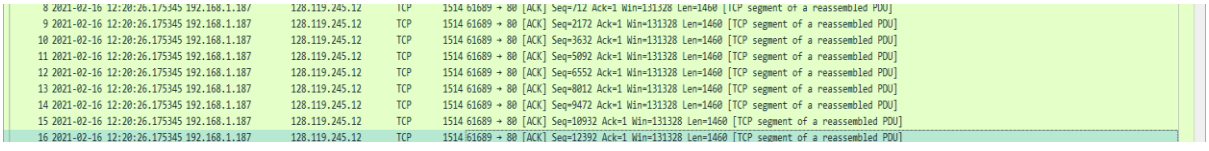


➔ 28960 bytes, not throttled.

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

➔ There are not.

10. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 in the text) among these first ten data-carrying segments?

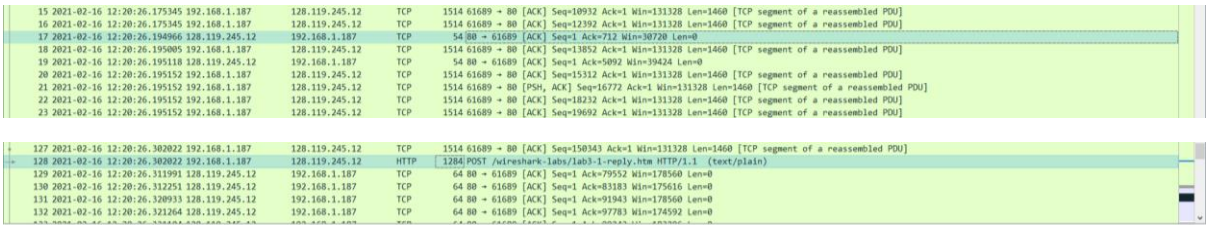


➔ ACK 숫자가 1460씩 증가.

➔ Receiver가 1460bytes씩 acknowledging.

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

    ➔ Throughput = Amount of data transmitted / time incurred.



    ➔ time incurred: 26.302022 – 26.194966 = 0.107056

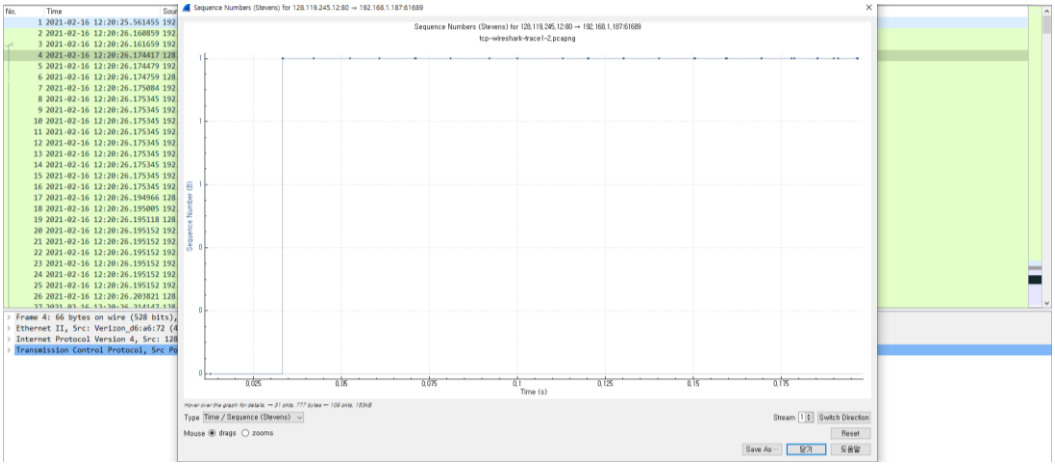
    ➔ 152,138 / 0.107056 =(대략) 142,111 (1,421,106.7105067)

12. 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. Consider the "fleets" of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase. Figure 6 shows a slightly different view of this data.

13. These "fleets" of segments appear to have some periodicity. What can you say about the period?

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.

    ➔ 12, 13, 14 answer.



➔ TCP slowstart: 0.037sec end.

➔ 선형 증가가 관찰되지 않는다.

➔ TCP transmit window가 선형적으로 증가하지 않는다.

➔ http의 속도제한 때문일 가능성이 있다.