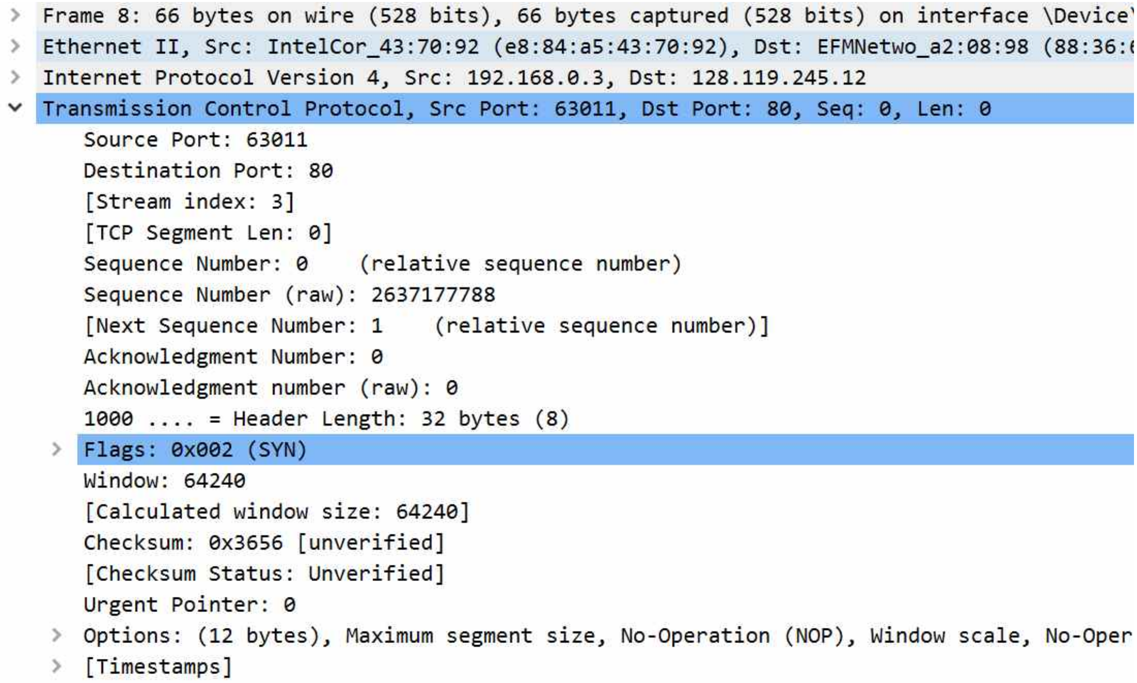
Network

(Lab Assignment 2)

Wireshark

컴퓨터소프트웨어 학부
2018008559
신상윤

1. A first look at the captured trace

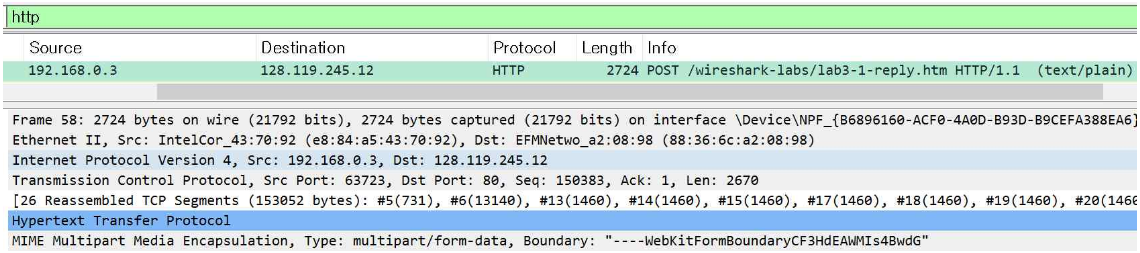


```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device
> Ethernet II, Src: IntelCor_43:70:92 (e8:84:a5:43:70:92), Dst: EFMNetwo_a2:08:98 (88:36:6
> Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 63011, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 63011
     Destination Port: 80
     [Stream index: 3]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 2637177788
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
     1000 .... = Header Length: 32 bytes (8)
   > Flags: 0x002 (SYN)
     Window: 64240
     [Calculated window size: 64240]
     Checksum: 0x3656 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Oper
   > [Timestamps]
```

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?
source의 ip 주소는 192.168.0.3이고, 포트 번호는 63011이다.

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 주소는 128.119.245.12이고, 포트 번호는 80이다.

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?



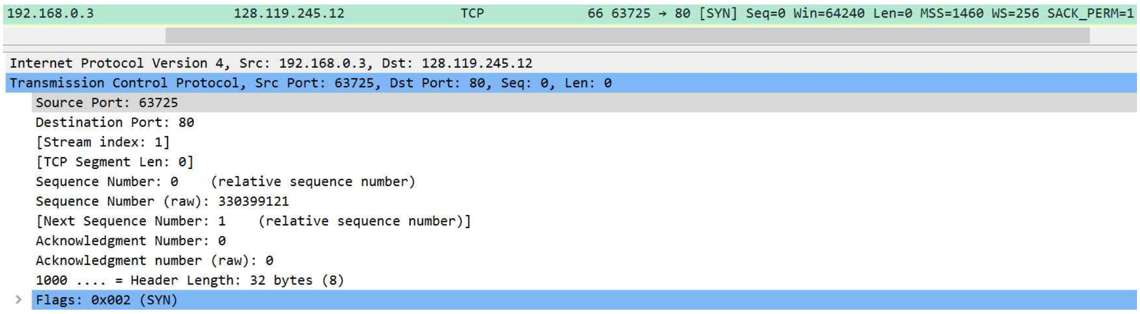
```
http

Source           Destination       Protocol  Length  Info
192.168.0.3      128.119.245.12    HTTP        2724  POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)

Frame 58: 2724 bytes on wire (21792 bits), 2724 bytes captured (21792 bits) on interface \Device\NPF_{B6896160-ACF0-4A0D-B93D-B9CEFA388EA6}
Ethernet II, Src: IntelCor_43:70:92 (e8:84:a5:43:70:92), Dst: EFMNetwo_a2:08:98 (88:36:6c:a2:08:98)
Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63723, Dst Port: 80, Seq: 150383, Ack: 1, Len: 2670
[26 Reassembled TCP Segments (153052 bytes): #5(731), #6(13140), #13(1460), #14(1460), #15(1460), #17(1460), #18(1460), #19(1460), #20(146
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryCF3HdEAWMIs4BwdG"
```

ip 주소는 : 192.168.0.3이고, 포트 번호는 63723이다.

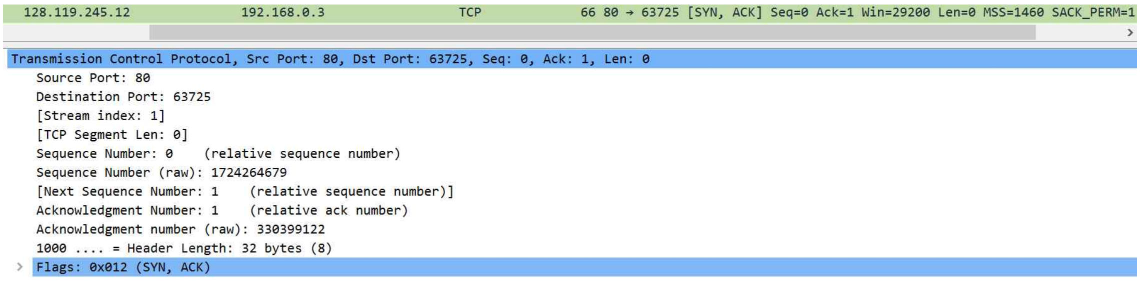
2. TCP Basics



```
192.168.0.3            128.119.245.12            TCP            66 63725 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63725, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 63725
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 330399121
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
```

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? initiate connection에 사용된 sequence number는 0이다. flags를 통해 SYN을 식별할 수 있다.

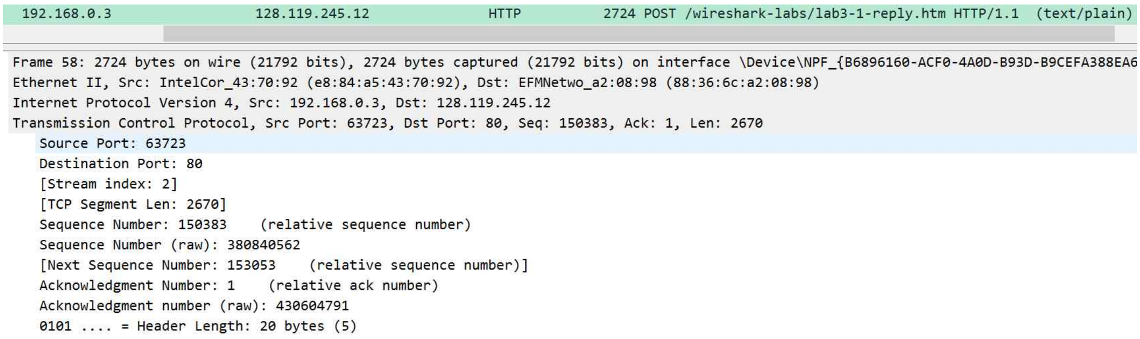


```
   128.119.245.12            192.168.0.3            TCP            66 80 → 63725 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1

Transmission Control Protocol, Src Port: 80, Dst Port: 63725, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 63725
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1724264679
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 330399122
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
```

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?

sequence number는 0이다. ACKnowledgement는 1이고, initial sequence number에서 1을 더한 값이다. 마찬가지로 flags를 통해 SYNACK를 식별할 수 있다.



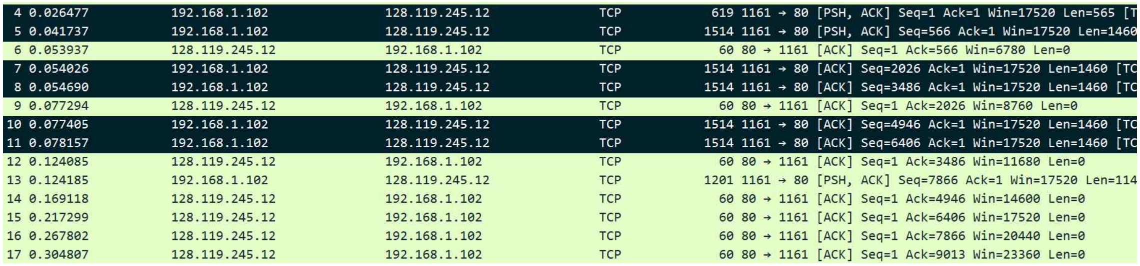
```
 192.168.0.3                  128.119.245.12              HTTP          2724 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)

Frame 58: 2724 bytes on wire (21792 bits), 2724 bytes captured (21792 bits) on interface \Device\NPF_{B6896160-ACF0-4A0D-B93D-B9CEFA388EA6
Ethernet II, Src: IntelCor_43:70:92 (e8:84:a5:43:70:92), Dst: EFMNetwo_a2:08:98 (88:36:6c:a2:08:98)
Internet Protocol Version 4, Src: 192.168.0.3, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63723, Dst Port: 80, Seq: 150383, Ack: 1, Len: 2670
    Source Port: 63723
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 2670]
    Sequence Number: 150383    (relative sequence number)
    Sequence Number (raw): 380840562
    [Next Sequence Number: 153053    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 430604791
    0101 .... = Header Length: 20 bytes (5)
```

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 number는 150383이다.

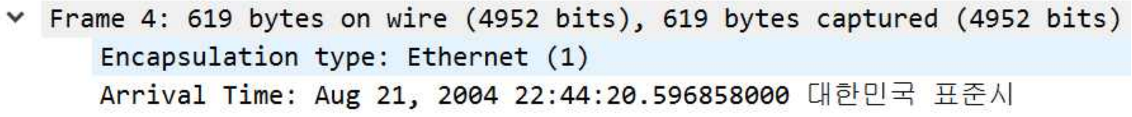
7번부터 wireshark-traces를 사용했습니다.

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 page 249 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 249 for all subsequent segments.



```
 4 0.026477      192.168.1.102       128.119.245.12      TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [T
 5 0.041737      192.168.1.102       128.119.245.12      TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
 6 0.053937      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
 7 0.054026      192.168.1.102       128.119.245.12      TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TC
 8 0.054690      192.168.1.102       128.119.245.12      TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TC
 9 0.077294      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10 0.077405      192.168.1.102       128.119.245.12      TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TC
11 0.078157      192.168.1.102       128.119.245.12      TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TC
12 0.124085      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13 0.124185      192.168.1.102       128.119.245.12      TCP      1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=114
14 0.169118      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15 0.217299      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16 0.267802      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17 0.304807      128.119.245.12      192.168.1.102       TCP        60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
```

sender			receiver			sender	
#	segment	time	#	ACK	time	RTT	estimated RTT
4	1	0.596858	6	566	0.624318	0.02746	0.02746
5	566	0.612118	9	2026	0.647675	0.035557	0.028472125
7	2026	0.624407	12	3486	0.694466	0.070059	0.0336704844
8	3486	0.625071	14	4946	0.739499	0.114428	0.0437651738
10	4946	0.647786	15	6406	0.78768	0.139894	0.0557812771
11	6406	0.648538	16	7866	0.838183	0.189645	0.0725142425



```
˅ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
      Encapsulation type: Ethernet (1)
      Arrival Time: Aug 21, 2004 22:44:20.596858000 대한민국 표준시
```

estimatedRTT = (0.875 * estimatedRTT) + (0.125 * sampleRTT)

segment1 : estRTT = RTT segment 1 = 0.02746

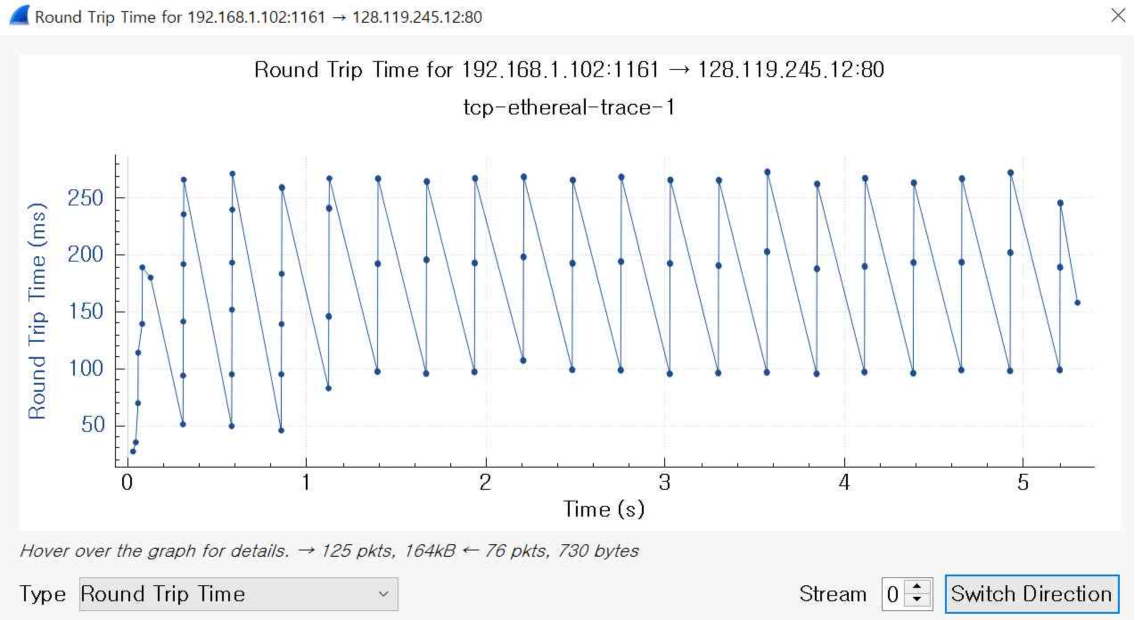
segment2 : 0.875 * 0.02746 + 0.125 * 0.035557 = 0.028472125

segment3 : 0.875 * 0.028472125 + 0.125 * 0.070059 = 0.0336704844

segment4 : 0.875 * 0.0336704844 + 0.125 * 0.114428 = 0.0437651738

segment5 : 0.875 * 0.0437651738 + 0.125 * 0.139894 = 0.0557812771

segment6 : 0.875 * 0.0557812771 + 0.125 * 0.189645 = 0.0725142425

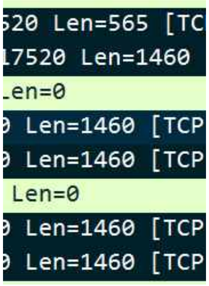


Hover over the graph for details. → 125 pkts, 164kB ← 76 pkts, 730 bytes

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

첫 번째 : 565(bytes)

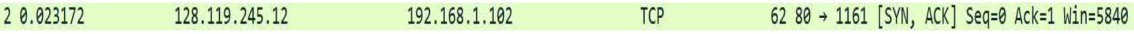
나머지 : 1460(bytes)



```
520 Len=565 [TC
17520 Len=1460
Len=0
0 Len=1460 [TCP
0 Len=1460 [TCP
 Len=0
0 Len=1460 [TCP
0 Len=1460 [TCP
```

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?

minimum은 서버의 첫 번째 승인에서 나타난다.

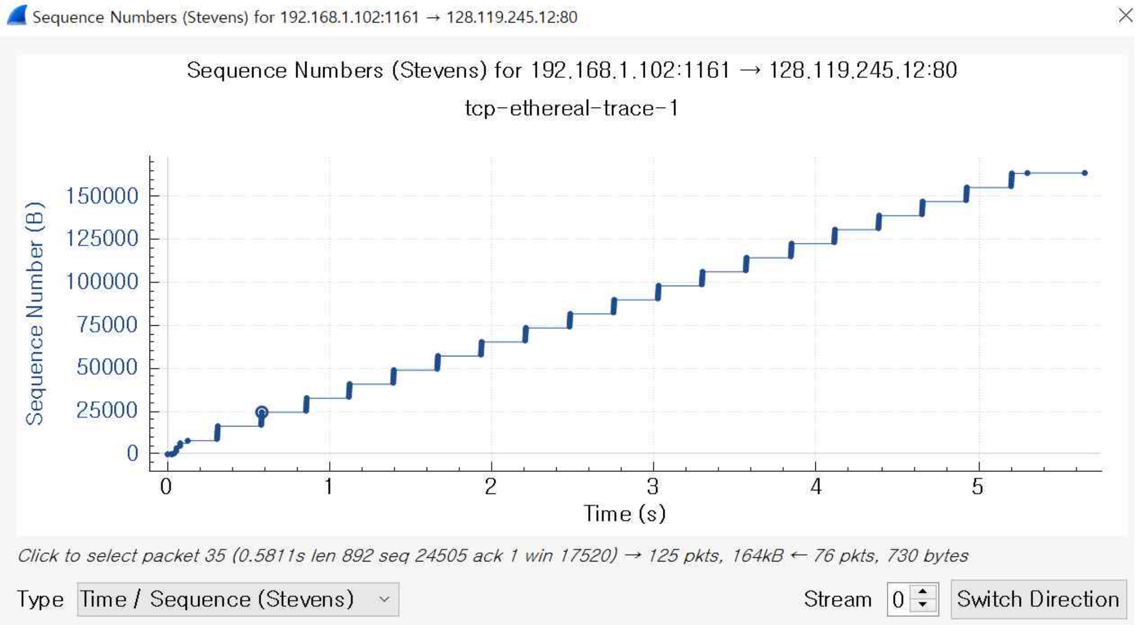


```
2 0.023172    128.119.245.12    192.168.1.102    TCP    62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840
```

minimum = 5840 bytes 이후 62780 bytes까지 커지고, 그동안 throttled 되지 않는다.

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

retransmitted segments는 없다. 이는 sequence number로 확인할 수 있는데, 만약 재전송된 segment가 있었다면 인접 segment의 sequence number보다 작아야 한다. 그러나 그래프는 계속 증가한다.



Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

tcp-ethereal-trace-1

Click to select packet 35 (0.5811s len 892 seq 24505 ack 1 win 17520) → 125 pkts, 164kB ← 76 pkts, 730 bytes

Type Time / Sequence (Stevens)

Stream 0

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 257 in the text).

ACK	acknowledged sequence #	acknowledged data
1	1	565
2	566	1460
3	2026	1460
4	3486	1460
5	4946	1460
6	6406	1460

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

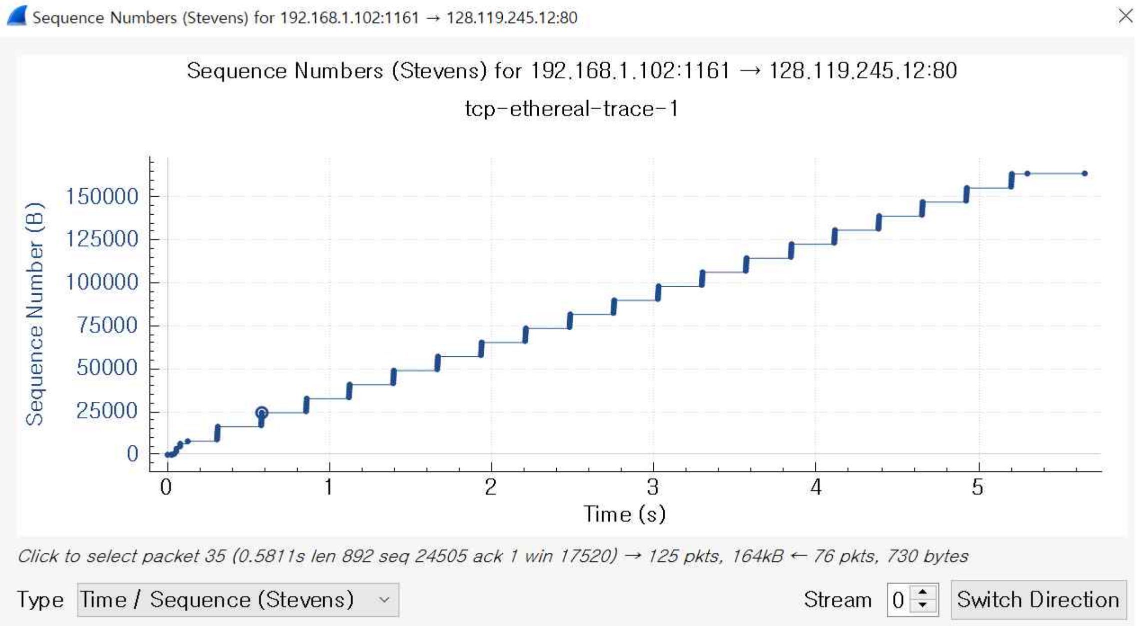
first ack : 1byte, time : 0.026477

last ack : 164091byte, time : 5.45583

throughput = data size / time = 164090/5.429353 = 30222.7539819201293 byte/sec

3. TCP congestion control in action

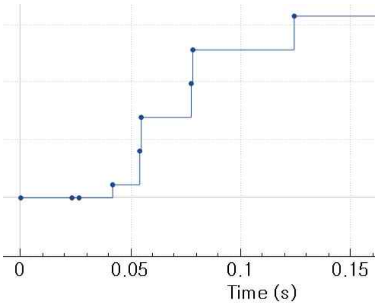
13. Use the *Time-Sequence-Graph(Stevens)* plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP’ s slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which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


Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

Click to select packet 35 (0.5811s len 892 seq 24505 ack 1 win 17520) → 125 pkts, 164kB ← 76 pkts, 730 bytes

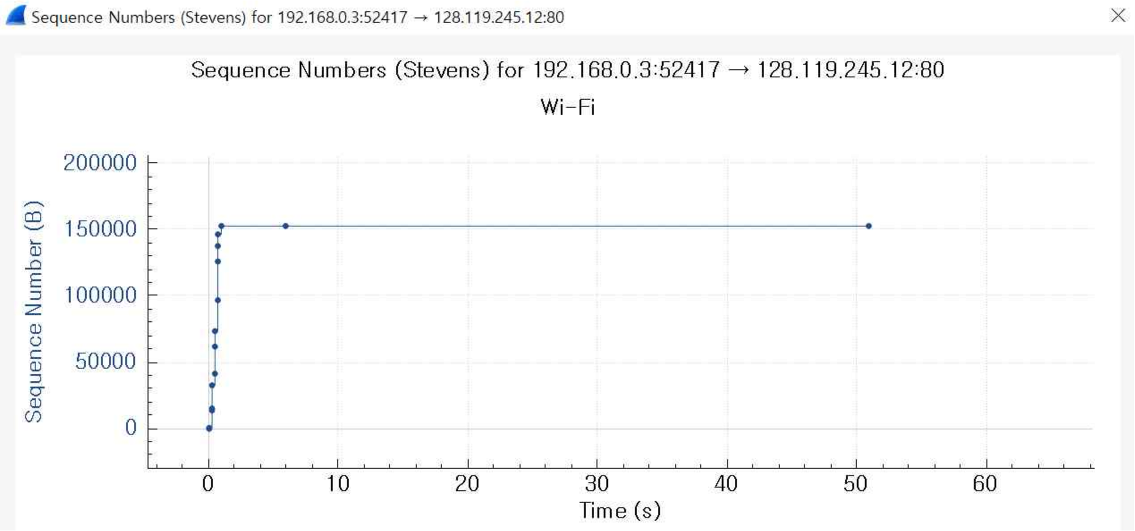
Type Time / Sequence (Stevens)

Stream 0



slow start는 0.05초쯤 시작해서 0.13초쯤 끝난다.
이후 측정된 데이터는 window size 일부만 사용한다.

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



직접 실행했을 때 증가가 한번 일어나고 이후 계속 일정하다.