Homework #2

✓ This homework aims at knowing about real TCP behaviors through Wireshark.

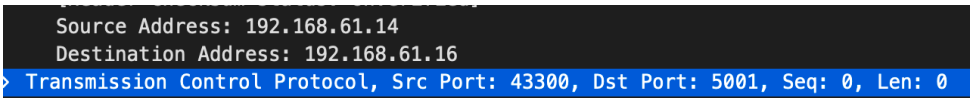
✓ Please upload your answer sheet in LMS. The uploading file must be PDF.

✓ You must show the screen capture for your answer.

✓ Due date: 11pm, 11/1 (Mon)

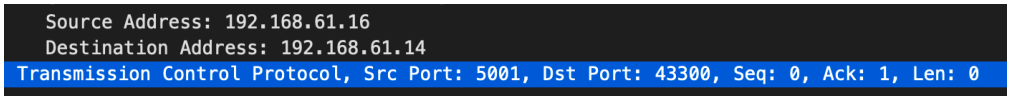
Let's analyze the *tcp.pcapng* file. This trace file contains TCP packets captured at TCP sender. The TCP sender transmits large file to the receiver for 10 seconds. Answer the following questions.

1. What is the IP address and TCP port number used by TCP sender? (10points)



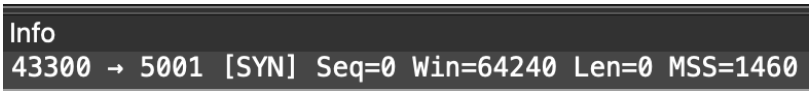
3-way-handshake 할 때의 ACK 을 보내는 첫번째 packet 은 sender 가 보내는 packet 이다. 따라서 그 packet 의 정보를 보면 source address 는 192.168.61.14 이고 src port 는 43300 이다.

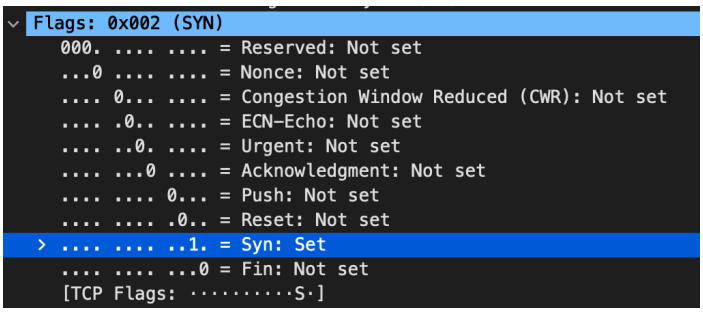
2. What is the IP address and TCP port number used by TCP receiver? (10points)



3-way-handshake 할 때의 SYN 과 ACK 을 보내는 두번째 packet 은 receiver 에서 보내는 packet 이다. 따라서 그 packet 의 정보를 보면 source address 는 192.168.61.16 이고 src port 는 5001 이다.

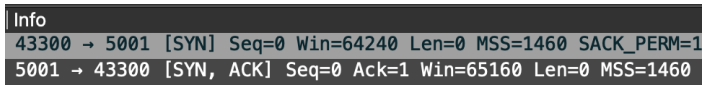
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the sender and receiver? What is it in the segment that identifies the segment as a SYN segment? (10points)

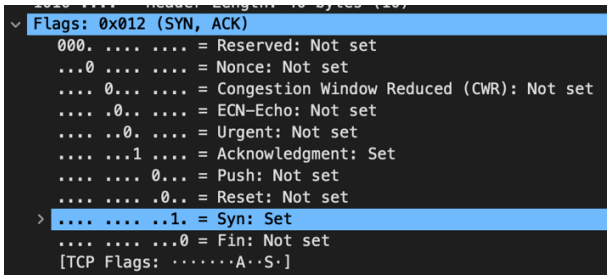




Seq#는 0 이고, TCP 의 Flags 를 보면 Syn 이 set 인걸 알 수 있다.

4. What is the sequence number of the SYNACK segment sent by receiver to the sender in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did the receiver determine that value? What is it in the segment that identifies the segment as a SYNACK segment? (10points)

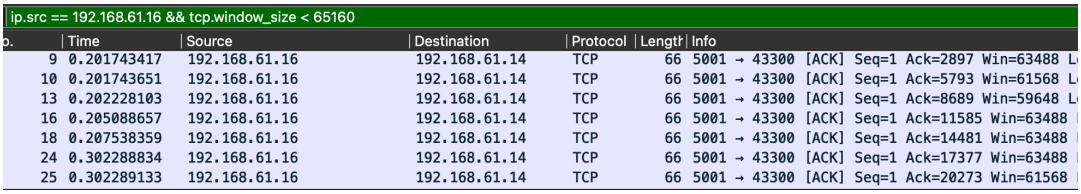


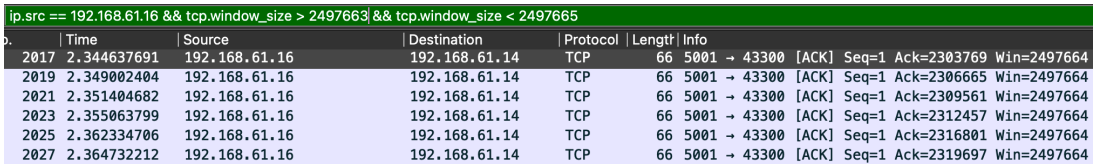


SYNACK 의 Seq#는 0 이고, Flags 를 보면 Acknowledgment field 가 set 인걸 알 수 있다. 그리고 sender 로부터 Syn# 0 을 받았기 때문에 다음으로 받아야 할 Seq#을 Ack 으로 보낸다. 따라서 Ack1 이 간다. Flags 를 보면 Syn 과 Acknowledgment 가 Set 으로 되어 있기 때문에 SYNACK segment 인걸 알 수 있다.

5. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? What is the maximum amount of available buffer space advertised at the receiver for the entire trace? What does mean window size scaling factor in Wireshark? (10points)

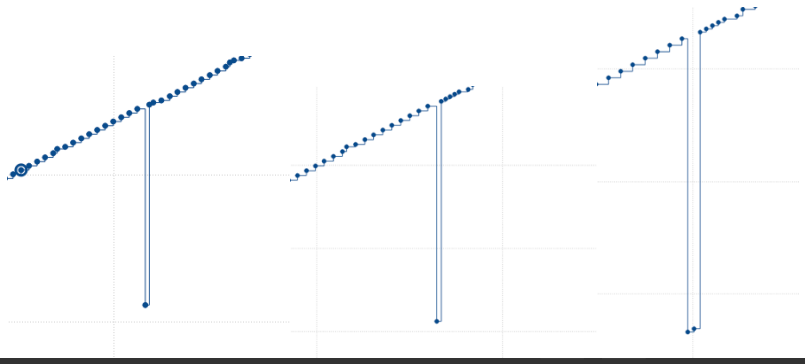
(Hint 1: Click menu, Statistics > TCP Stream Graphs > Windows Scaling → Click 'Switch Direction' → Enable 'Rcv Win' only)





Receiver 의 buffer 크기를 알기 위해선 receiver 에서 오는 packet 을 분석하면 된다. 따라서 ip.src 가 server 일 때, window size 가 제일 작은 것은 59648bytes 이다. 또한 maximum 의 크기는 2497664bytes 인걸 알 수 있는데, 그 이유는 2497664bytes 보다 큰 window 를 검색했을 때 결과가 나오지 않기 때문이다. Window size scaling factor 가 필요한 이유는 bit shift 를 통해서 훨씬 큰 버퍼 사이즈를 사용하기 위해서이다.

6. How many segments were retransmitted in the trace file? Show the packet numbers. Why were the segments retransmitted? (10points)

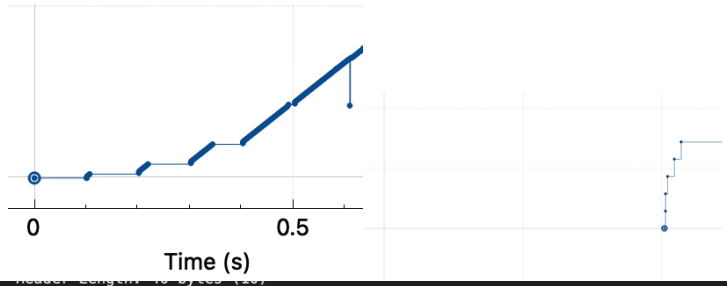


tcp.analysis.retransmission

o.	Time	Source	Destination	Protocol	Length	Info
220	0.609248057	192.168.61.14	192.168.61.16	TCP	2962	[TCP Fast Retransmission] 43300 → 5001
1921	2.232311824	192.168.61.14	192.168.61.16	TCP	2962	[TCP Fast Retransmission] 43300 → 5001
4359	5.198891922	192.168.61.14	192.168.61.16	TCP	1514	[TCP Fast Retransmission] 43300 → 5001

No.220(TCP Fast Retransmission), No.1921(TCP Fast Retransmission), No.4359(TCP Fast Retransmission)으로 총 3 번의 retransmission 이 일어난다.

7. Use the Time-Sequence-Graph (Stevens) plotting tool to view the sequence number versus time. Can you identify where TCP's slow start phase? What is the initial congestion window size? (10points)



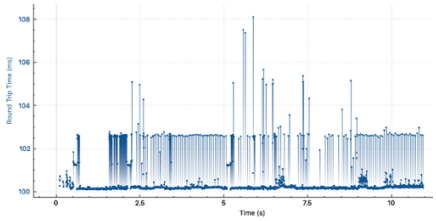

```
> Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0xfb9d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
v Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  v TCP Option - Maximum segment size: 1460 bytes
      Kind: Maximum Segment Size (2)
      Length: 4
      MSS Value: 1460
```

약 0.4s 까지 segment 가 두배 씩 늘어나므로 slow start 가 일어나고, 그 이후부턴 Seq#가 꾸준히 2896 만큼 linear 하게 증가하는 것을 볼 수 있다. 그리고 3-way-handshake 를 할 때 SYNpacket 을 보면 MSS 가 1460bytes 인 것을 확인할 수 있고, 처음에 5 개의 packet 을 보낸다.따라서 initial cwnd 는 5MSS(5*1460bytes)이다.

8. What is the average throughput of entire trace? Can you show RTT? (10points)

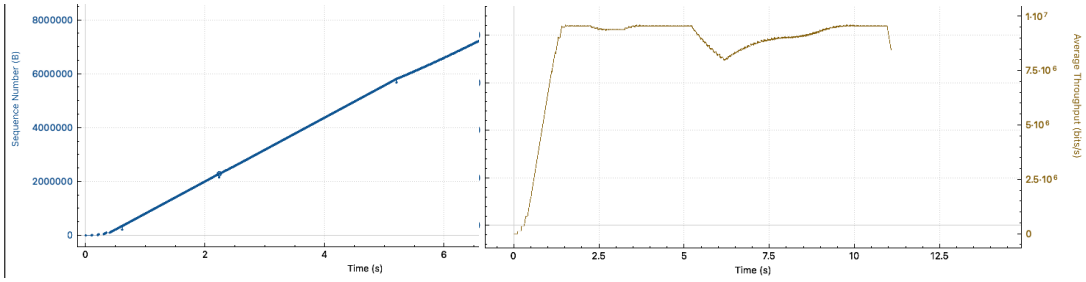
   (Hint: Wireshark can show an average throughput and RTTs)

Statistics	
Measurement	Captured
Packets	8772
Time span, s	11.065
Average pps	792.8
Average packet size, B	1471
Bytes	12901476
Average bytes/s	1165 k
Average bits/s	9327 k



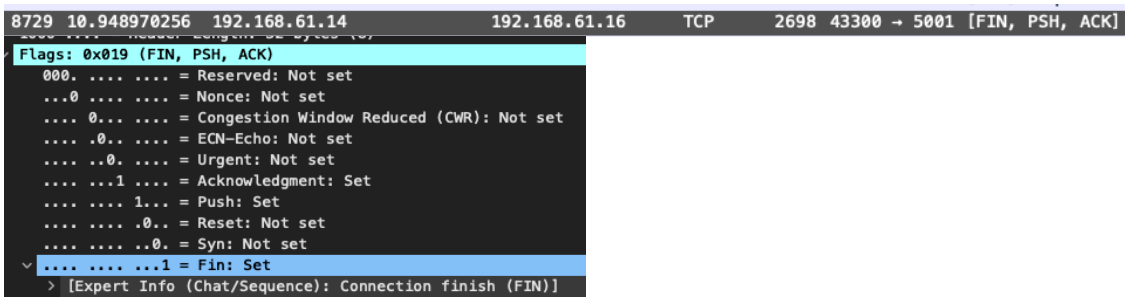
   Avg TCP throughput 은 9327kbps 이다.

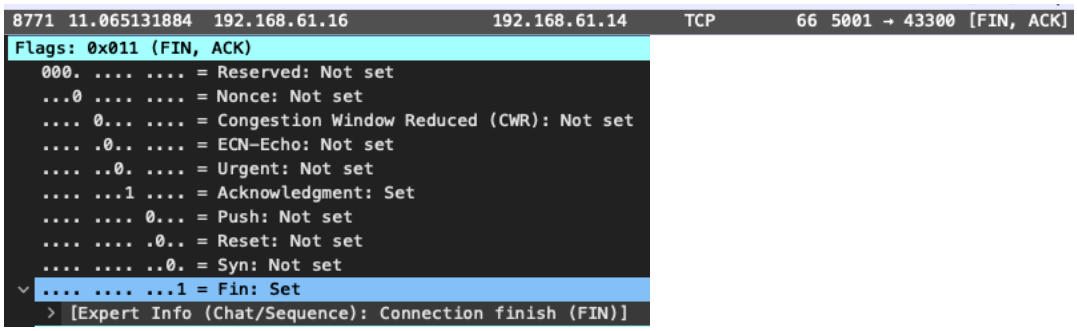
9. Show TCP throughput plot using TCP Stream Graphs menu (Statistics > TCP Stream Graphs > Throughput). What were the reason for decrease in throughput? (10points)

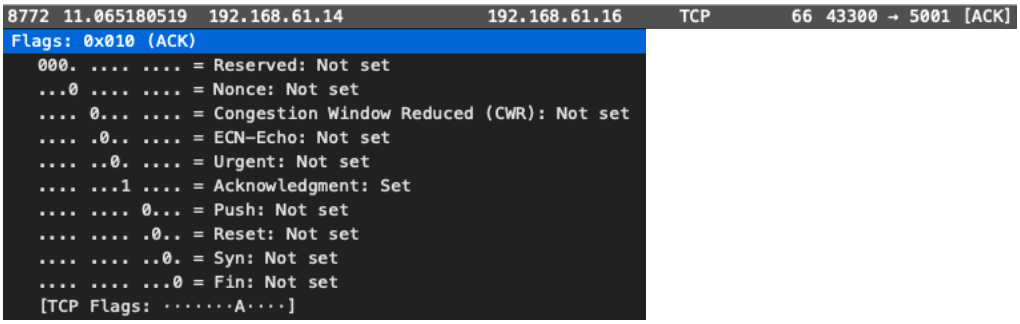


   두개의 그래프를 보면 Packet loss 로 인한 retransmission 으로 인해 throughput 이 감소된 것을 볼 수 있다.

10. Explain connection closing of the trace file, with TCP sequence number, acknowledgement number, and segment TYPE (FIN, ACK...) (10points)







먼저 8729 번째 packet 을 보면 sender 가 receiver 에게 FIN, PSH, ACK 을 한번에 보내고 있다. 이 뜻은 sender 는 receiver 에게 마지막 file data 를 전송(PSH)하면서 이전에 보냈던 seq#를 잘 받았다는 신호(ACK)를 보내면서 동시에 FIN 을 보내는 것이다. 그리고 이전에 보냈던 packet 에 대한 ACK 들을 receiver 로부터 받은 뒤에, 8771Packet 을 보면 receiver 로부터 FIN 과 ACK 을 동시에 받는 것을 알 수 있다. 그 뒤로 sender 로부터 ACK 을 받고 4-way handshake 를 마무리 짓게 된다.