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, 11/01 (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)
2. What is the IP address and TCP port number used by TCP receiver? (10points)
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)
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)
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)
6. How many segments were retransmitted in the trace file? Show the packet numbers. Why were the segments retransmitted? (10points)
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)
8. What is the average throughput of entire trace? Can you show RTT? (10points)

   (Hint: Wireshark can show an average throughput and RTTs)
9. Show TCP throughput plot using TCP Stream Graphs menu (Statistics > TCP Stream Graphs > Throughput). What were the reason for decrease in throughput? (10points)
10. Explain connection closing of the trace file, with TCP sequence number, acknowledgement number, and segment TYPE (FIN, ACK…) (10points)