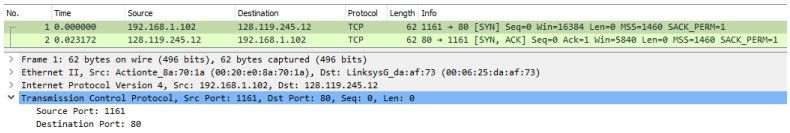
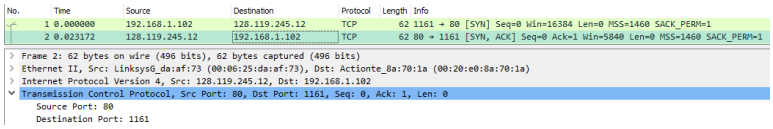
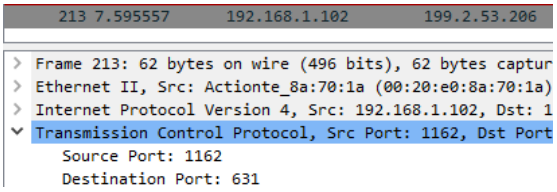
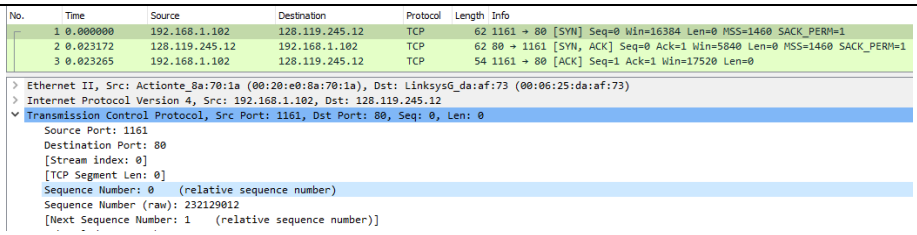
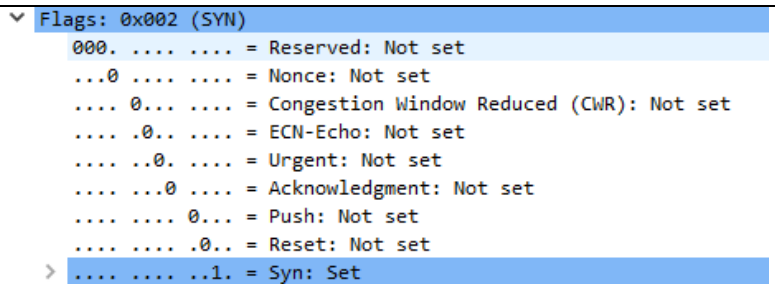
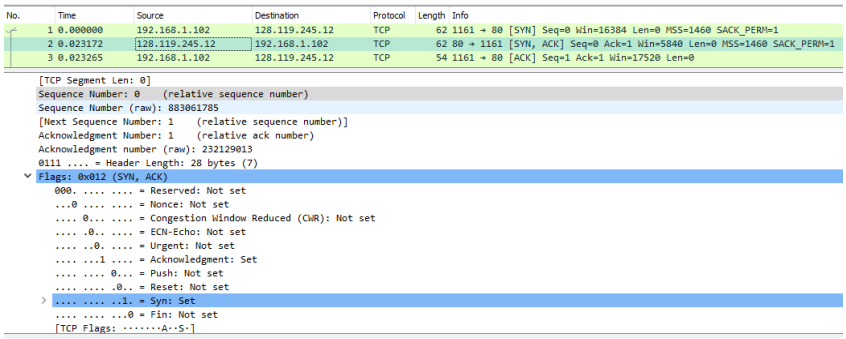
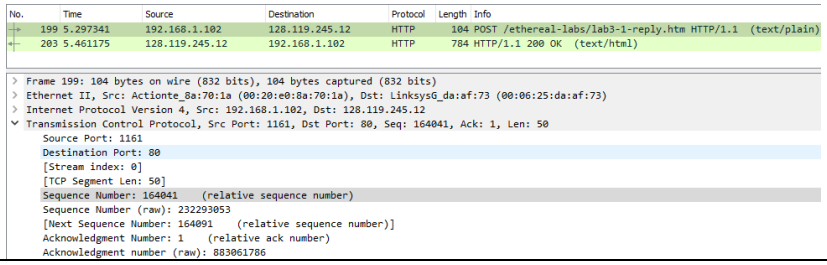
Wireshark Lab 3: TCP

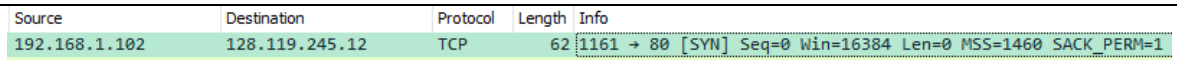
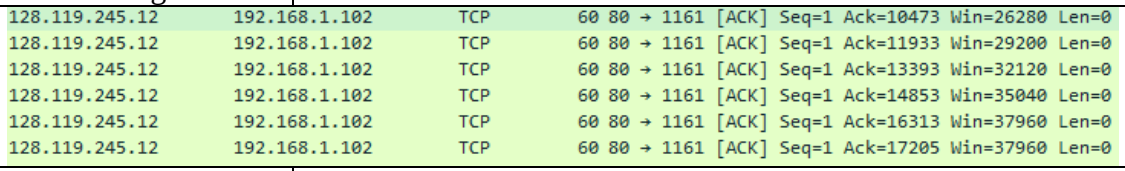
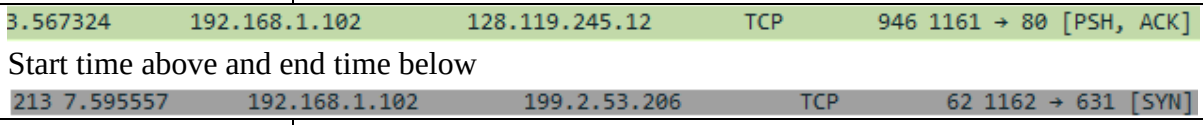
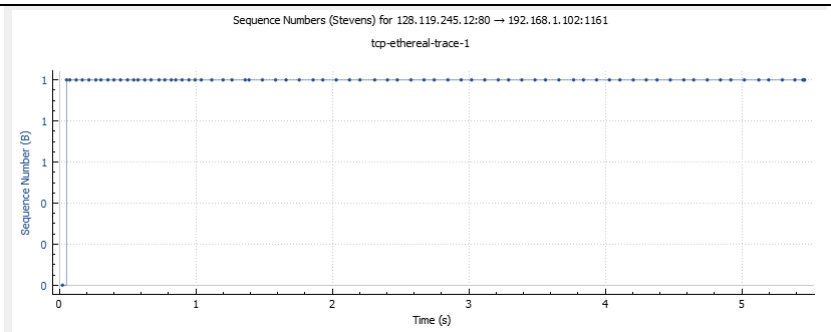
Group 31 Details: Bikramjit Narwal (1005242300), Chao Glen Xu (1004274634)

Mark:

	Question	Answer
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?	IP: 192.168.1.102 Port: 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?	IP: 128.119.245.12 Port: 80 
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?	IP: 192.168.1.102 Port: 1162 
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?	 Seq #: 0 The SYN flag is set to 1 as seen at the end of the 2nd screenshot.
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?	Seq #: 883061785 ACK #: 232129013 For the SYN-ACK packets, the seq # is set to the seq # of SYN-packet + 1. Both the SYN and the ACK flags are then set to 1. 
6	What is the sequence number of the TCP segment containing the HTTP POST command?	Seq #: 164041 
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 after the receipt of each ACK?	
8	What is the length of each of the first six TCP segments?	0, 0, 0, 565, 1460, 0
Annotated Screenshots (if needed)	Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0 Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0 Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 0 Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565 Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 566, Ack: 1, Len: 1460 Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 566, Len: 0	
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 of available buffer space is 16384. This is indicated by the win = 16384 in the screenshot below. The lack of receiver buffer space does not ever throttle the sender.

Annotated Screenshots (if needed)		
10	Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?	No there are not any retransmitted segments in the trace file. I checked the sequence numbers in the TCP segments in the trace file to confirm. Each sequence number is seen at a different 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	Below we can see the Ack value difference between the different packets is 1460 bytes.
Annotated Screenshots (if needed)		
12	What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.	How to calculate: Divide size of file by the time it takes to be transmitted by TCP. 184320 / (7.595557 – 3.567324) = 45757.03 KB/s
Annotated Screenshots (if needed)		
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 slow start phase appears to begin at 0.1 s and end near 0.2 s. Congestion avoidance appears to take over 0.8 s and it continues.

	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.