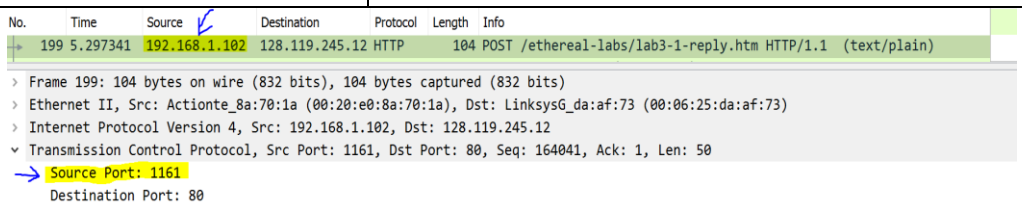
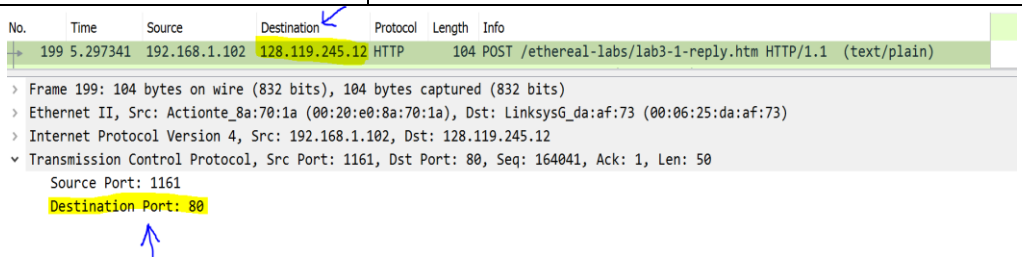
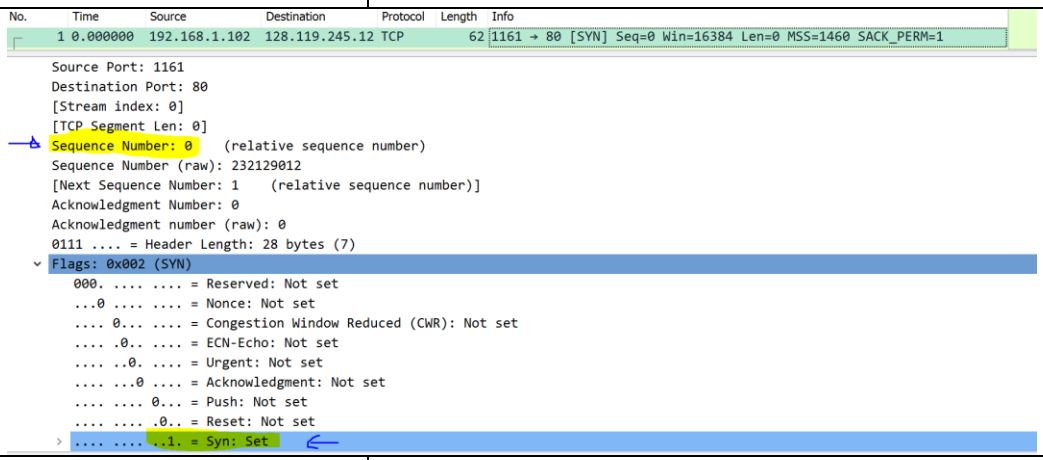
Wireshark Lab 3: TCP

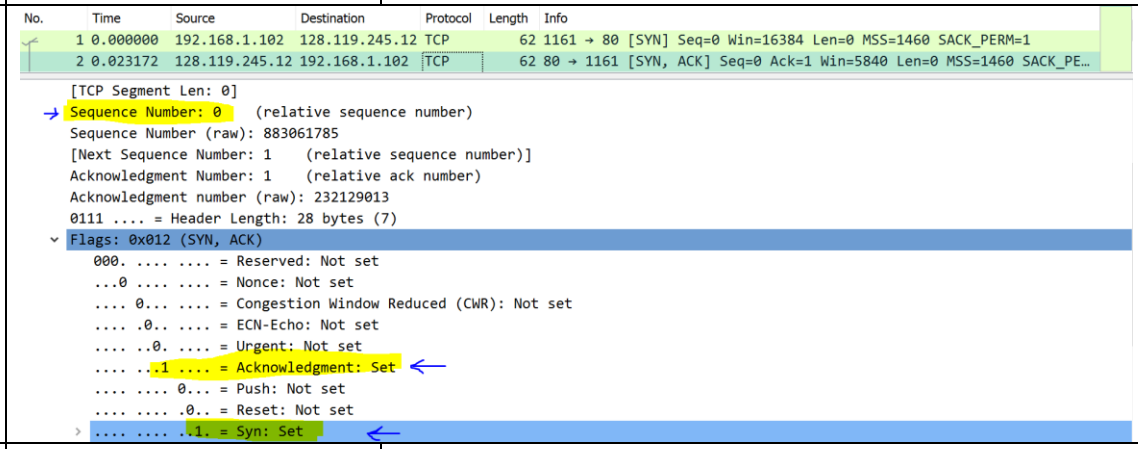
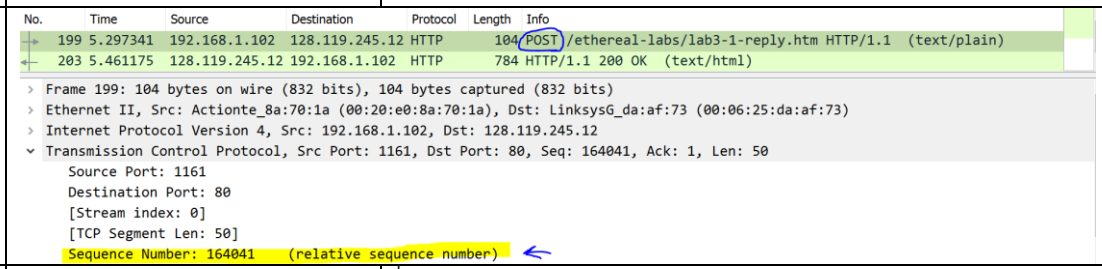
Group Details:

Muhammad Zaheer Hashmi - 1004299056
Hairan Zhang - 1004957601

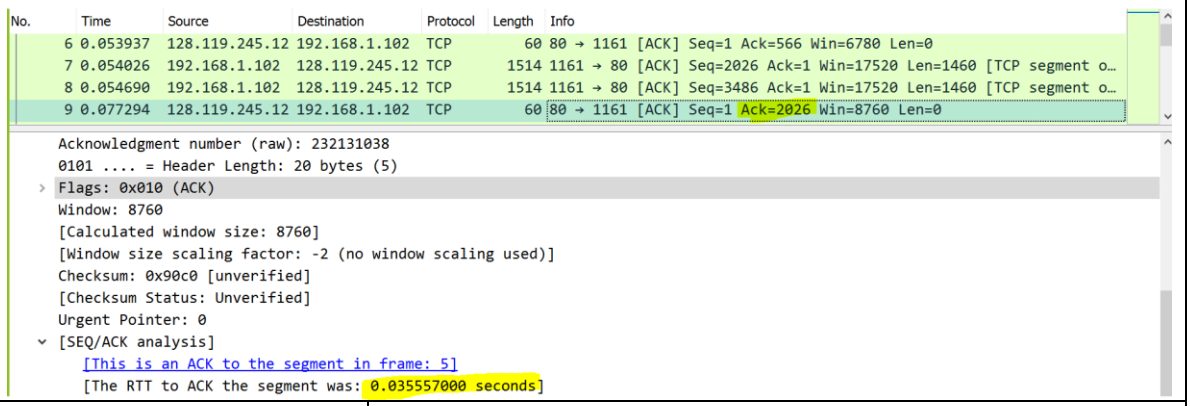
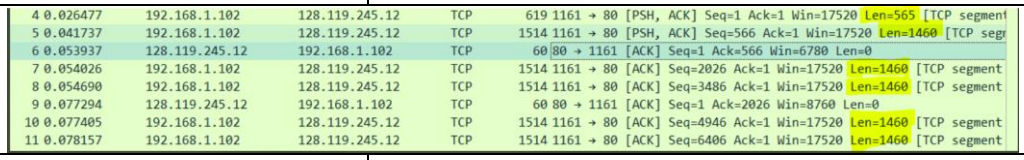
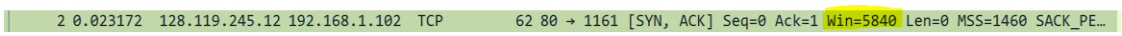
Mark:

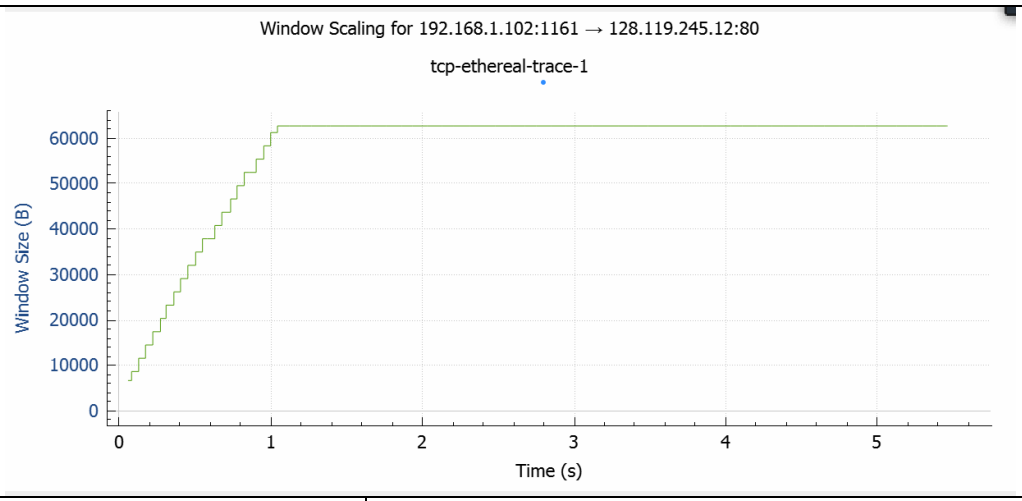
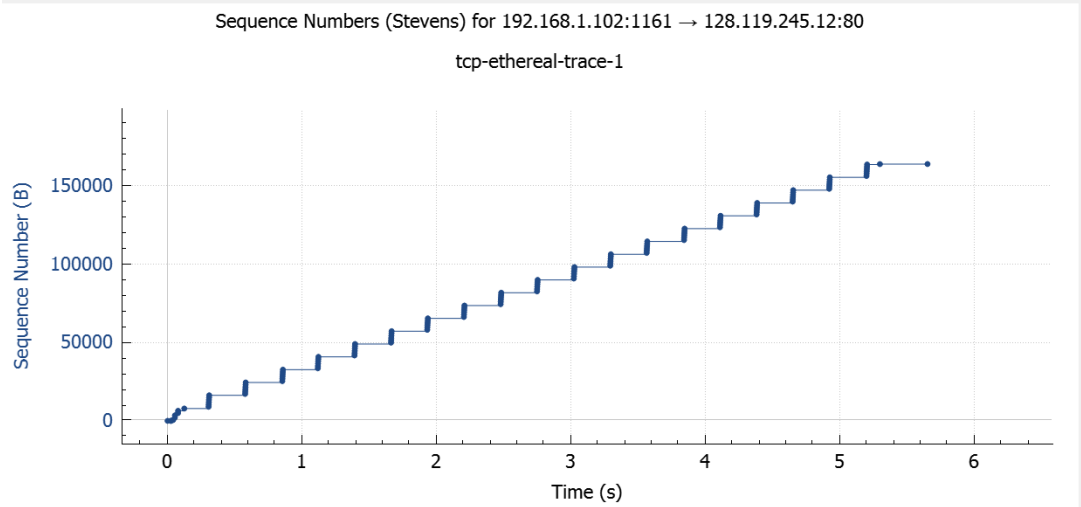
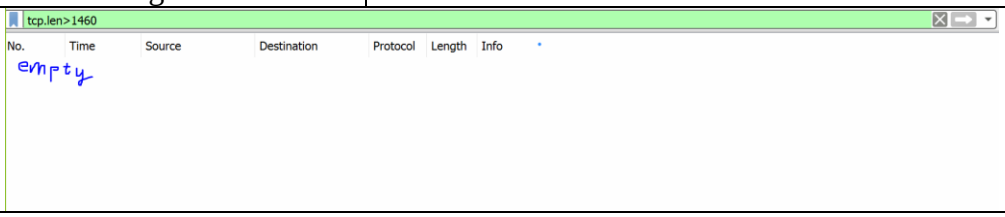
	Question	Answer
1	What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?	IP: 192.168.1.102 Source Port: 1161
Annotated Screenshots (if needed)		
2	What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?	IP: 128.119.245.12 Port: 80
Annotated Screenshots (if needed)		
3	What is the IP address and	

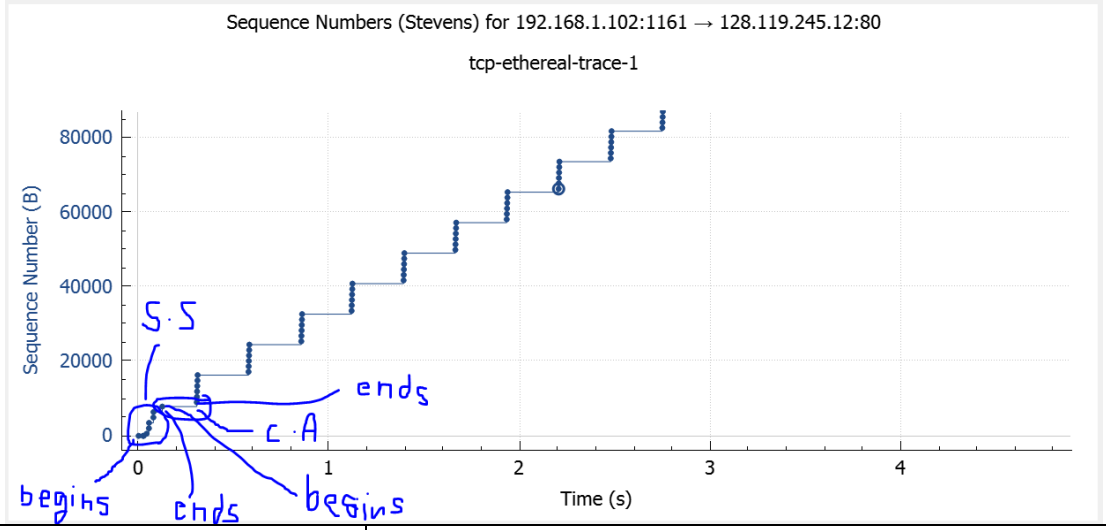
	TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?	
Annotated Screenshots (if needed)		
4	What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?	Seq NO: 0 The SYN segment is identified by setting the SYN flag as 0 in the TCP header.
Annotated Screenshots (if needed)		
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	Seq No: 0 Ack field Value: 1 - The value is determined by the SEQ No of the SYN segment. - The SYNACK segment is identified by setting the SYN and ACK flag to 1 in the TCP header.

	that identifies the segment as a SYNACK segment?	
Annotated Screenshots (if needed)		
6	What is the sequence number of the TCP segment containing the HTTP POST command?	Seq NO: 164041
Annotated Screenshots (if needed)		
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	Sequence numbers: 0, 565, 2025, 3485, 4945, 6405 Note: Annotation work is shown for the second segment. This can be repeated for the remaining segments.

Seg. No.	RTT (s)	Estimated Time (s)
1	0.02746	0.02746
2	0.035557	0.028472
3	0.070059	0.03367
4	0.114428	0.043765
5	0.139894	0.055781
6	0.189645	0.072514

	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?	
Annotated Screenshots (if needed)	2nd seg  No. Time Source Destination Protocol Length Info 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 [TCP segment o… 8 0.054690 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment o… 9 0.077294 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0 Acknowledgment number (raw): 232131038 0101 .... = Header Length: 20 bytes (5) Flags: 0x010 (ACK) Window: 8760 [Calculated window size: 8760] [Window size scaling factor: -2 (no window scaling used)] Checksum: 0x90c0 [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 [SEQ/ACK analysis] [This is an ACK to the segment in frame: 5] [The RTT to ACK the segment was: 0.035557000 seconds]	
8	What is the length of each of the first six TCP segments?	565 bytes, 1460 bytes ,1460 bytes ,1460 bytes ,1460 bytes ,1460 bytes respectively.
Annotated Screenshots (if needed)	 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 [TCP segment 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 [TCP segr 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 [TCP segment 8 0.054690 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment 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 [TCP segment 11 0.078157 192.168.1.102 128.119.245.12 TCP 1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment	
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?	5840 Bytes. We do not observe any time out as demonstrated by the windows time graph below (it is increasing linearly with time).
Annotated Screenshots (if needed)	 2 0.023172 128.119.245.12 192.168.1.102 TCP 62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PE…	

		
10	Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?	Observing the graph below we note that each segment has a unique SEG NO, therefore there were no retransmitted segments.
Annotated Screenshots (if needed)		
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	The receiver acknowledges 1460 bytes of data on average. There were no cases where the receiver was ACKing every other received segment. There were no cases where we had a length greater than 1460. Had there been a case of ACK for every other received segment this would be included in the trace below.
Annotated Screenshots (if needed)		

12	What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.	The throughput depends on the time across which we consider the data transfer. We can consider the whole process which took 5.651141 seconds. The last packet acknowledged was 164091. This means total byte transfer is 164090. We can do the ratio 164090/(5.455830 – 0.026477) to obtain through-put. This is 30222.71 bytes / sec.
Annotated Screenshots (if needed)	202 5.455830 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0	
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.	Slow start begins at 0 seconds ; ends at around 0.25 seconds. Congestion Avoidance takes over around 0.25 seconds (SEQ NO. 7866). The difference is that the slope of the graph in the congestion avoidance phase is rather flat.
Annotated Screenshots (if needed)		
14	Answer each of two questions above for the trace that you have gathered when you	Sequence number seems to increase quadratically throughout the entire graph, so thus it seems to be in slow start region all the time congestion avoidance never takes over. We are not sure because the transfer happens so quickly

	transferred a file from your computer to gaia.cs.umass.edu	
Annotated Screenshots (if needed)