Wireshark Lab 1: TCP

Group Details:
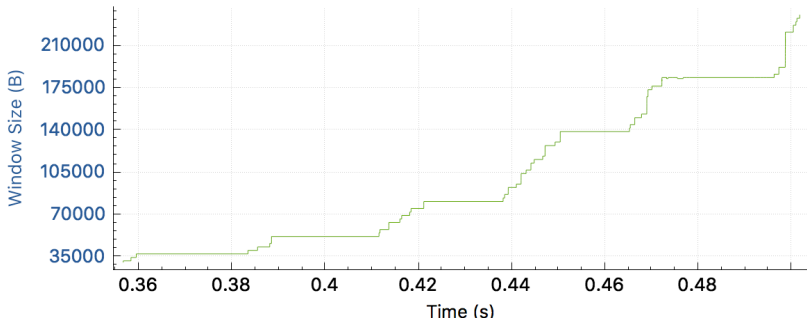**Zhaoning Kong**   **1004654288**
Qianhao Zhang   **1004654377**

Mark:

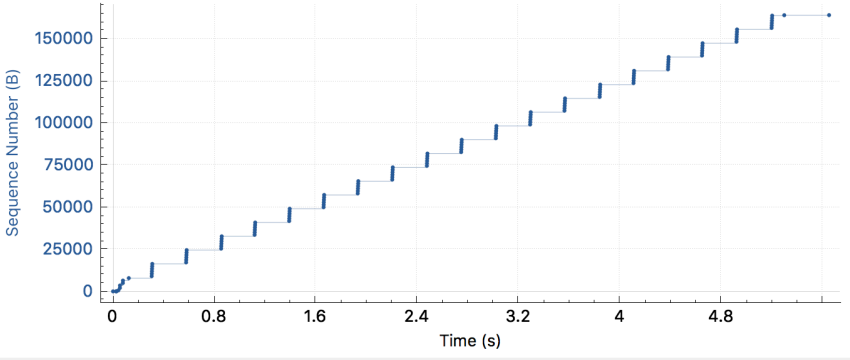|	Question	Answer
1	What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?	192.168.1.102 Port number: 1161
2	What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?	128.119.245.12 Port number: 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?	Souce IP: 100.64.203.116 Source Port: 49461
4	What is the sequence number of the TCP SYN segment that is	Sequence Number: 555386525 The SYN flag is set to 1.

	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?	Sequence number: 555386525
		Acknowledgment number: 0
		1011 .... = Header Length: 44 bytes (11)
		▼ Flags: 0x002 (SYN)
		    .... .0.. = Reset: Not set
		  ▶ ....1. = Syn: Set
		     0 = Fin: Not set

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 number: 2787860960
		ACK number: 555386526
		For the SYN-ACK packets, the sequence number is always set to the sequence number of SYN-packet plus 1.
		Both SYN and ACK flags are set to 1.
		
		Sequence number: 2787860960
		Acknowledgment number: 555386526
		1010 .... = Header Length: 40 bytes (10)
		▼ Flags: 0x012 (SYN, ACK)
		    000. .... = Reserved: Not set
		    ...0 .... = Nonce: Not set
		    .... 0... .... = Congestion Window Redu
		    .... .0.. .... = ECN-Echo: Not set
		    .... ..0. .... = Urgent: Not set
		    ....1 .... = Acknowledgment: Set
		    .... 0... = Push: Not set
		    .... .0.. = Reset: Not set
		  ▶ ....1. = Syn: Set

6	What is the sequence number of the TCP segment containing the HTTP POST command?	Sequence number: 555386526
		▶ Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555386526,
		▼ Hypertext Transfer Protocol
		  ▶ POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\n
		    Host: gaia.cs.umass.edu\r\n

7	Consider the TCP segment containing the HTTP POST as the first segment in	Sequence number: 555386526, 555387132, 555387269, 555388673, 555390077, 555391481 Time sent:

	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?	**Time** 7 0.329748 8 0.330312 9 0.330566 10 0.330567 13 0.356749 15 0.358374 Receive at: 0.356657, 0.356662, 0.358324, 0.359451, 0.383415, 0.385476 Time Info 0.356657 80 → 49461 [ACK] Seq=2787860961 Ack=555387132 0.356662 80 → 49461 [ACK] Seq=2787860961 Ack=555387269 0.356749 Continuation 0.358324 80 → 49461 [ACK] Seq=2787860961 Ack=555388673 0.358374 Continuation 0.358374 Continuation 0.359451 80 → 49461 [ACK] Seq=2787860961 Ack=555390077 0.359498 Continuation 0.359498 Continuation 0.383415 80 → 49461 [ACK] Seq=2787860961 Ack=555391481 0.383490 Continuation 0.383491 Continuation 0.385476 80 → 49461 [ACK] Seq=2787860961 Ack=555392885 RTT: 0.026909, 0.02635 , 0.027758, 0.028884, 0.026666, 0.027102 Estimated RTT after each receipt: 0.026909, 0.026839, 0.026953, 0.027195, 0.027129, 0.027125
8	What is the length of each of the first six TCP segments?	606, 137, 1404, 1404, 1404, 1404 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555386526, Ack: 2787860961, Len: 606 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555387132, Ack: 2787860961, Len: 137 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555387269, Ack: 2787860961, Len: 1404 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555388673, Ack: 2787860961, Len: 1404 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555390077, Ack: 2787860961, Len: 1404 Transmission Control Protocol, Src Port: 49461, Dst Port: 80, Seq: 555391481, Ack: 2787860961, Len: 1404

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?	Minimal advertised window size: 28960 The lack of receiver buffer did not throttle the sender. **Window Scaling for 100.64.203.116:49461 → 128.119.245.12:80** Wi-Fi: en0 _(Chart: Window Size (B) vs Time (s); y-axis 35000 to 210000, x-axis 0.36 to 0.48)_
10	Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?	Yes. The first (SYN) packet is being retransmitted, because they have the same sequence number. | Time	Source	Destination	Protocol	Length	Info
1 0.000000	100.64.203.116	128.119.245.12	TCP	78	49461 → 80 [SYN] Seq=555386525 Win=65535 Len=0 MSS=
2 0.259129	100.64.203.116	128.119.245.12	TCP	78	[TCP Retransmission] 49461 → 80 [SYN] Seq=555386525	
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	1404 or 2808 bytes. Typically, one HTTP frame should be of size 1404 bytes. Upon the arrival of in-order segment with expected sequence number, and all data up to expected sequence number already acknowledged, TCP sends ACK for every other packet. If one other in-order segment waiting for ACK transmission, TCP immediately send single cumulative ACK for both in-order segments. Ack=555488357 Ack=555491165 Ack=555493973 Ack=555496781 Ack=555499589 Ack=555502397 Ack=555505205 Ack=555508013 Ack=555510821
12	What is the throughput (bytes transferred per unit	We calculated throughput by dividing the size of the file by the time it takes to be transmitted by TCP, which can be deduced from the traces. We calculate the number of bytes transmitted by taking the relative

	time) for the TCP connection? Explain how you calculated this value.	ACK number of the last packet. 149329 * 8 / 0.501845 = 2380911 (bit/s)
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.	In the first few hundred milliseconds, TCP is in slow start state, and then enters congestion avoidance. After that, the rate is constant, sending 6 packets each time, which differs from what we've studied, which is different from the linearly increasing rate as described in the textbook. This is probably enforced by HTTP server. **Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80** tcp-ethereal-trace-1.pcapng *[Plot: Sequence Number (B) vs Time (s), values from 0 to 150000 on y-axis, 0 to 4.8 on x-axis, showing a roughly linear staircase increase]*
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	The TCP remains in slow start state during the entire transmission. This is what we expected. **Sequence Numbers (Stevens) for 100.64.203.116:49461 → 128.119.245.12:80** traces.pcapng *[Plot: Sequence Number (B) vs Time (s), values from 0 to 150000 on y-axis, 0 to 0.48 on x-axis, showing slow start with increasing steep rise near the end]*