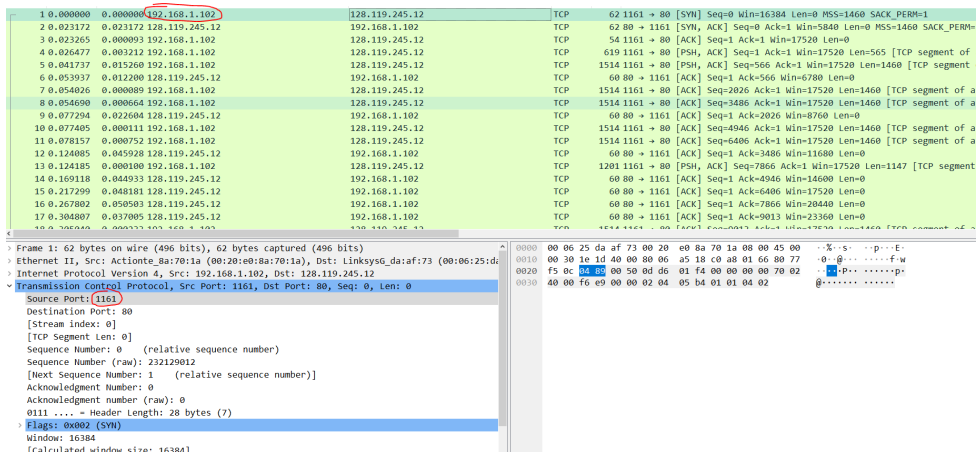


Wireshark Lab 3: TCP

Group Details:
Leo Hanxu 1006045067
Shaoyang Zhang 1005751660

Mark:

	Question	Answer
1	What is the IP address and TCP port number used by your client computer (source) that is transferring the file to gaia.cs.umass.edu?	The address of the client is IP: 192.168.1.102 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?	The IP address of server: 128.119.245.12 port:80

Annotated Screenshots (if needed)

1 0.000000 0.000000 192.168.1.102 128.119.245.12 TCP 62 1101 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

2 0.023172 0.023172 128.119.245.12 192.168.1.102 TCP 62 80 → 1101 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1

3 0.023265 0.000093 192.168.1.102 128.119.245.12 TCP 54 1101 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0

4 0.026477 0.003212 192.168.1.102 128.119.245.12 TCP 619 1101 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

5 0.041737 0.015260 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

6 0.053937 0.012280 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=566 Win=6780 Len=0

7 0.054026 0.000809 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

8 0.054690 0.000664 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

9 0.077294 0.022604 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=2026 Win=8760 Len=0

10 0.077405 0.000111 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

11 0.078157 0.000752 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

12 0.124085 0.045928 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=3486 Win=11680 Len=0

13 0.124185 0.000100 192.168.1.102 128.119.245.12 TCP 1201 1101 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

14 0.169118 0.044933 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=4946 Win=14600 Len=0

15 0.217299 0.048181 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=6406 Win=17520 Len=0

16 0.267802 0.050501 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=7866 Win=20440 Len=0

17 0.304807 0.037005 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=9013 Win=23360 Len=0

18 0.305045 0.000000 192.168.1.102 128.119.245.12 TCP 62 1101 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_daiaf:73 (00:06:25:d0:00:00)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1101, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1101
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment Number (raw): 0
0111 = header length: 28 bytes (7)
Flags: 0x0002 (SYN)
Window: 16384
[calculated window size: 16384]

Question 3 omitted

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?

sequence number is 0

syn flag is set to 1

Annotated Screenshots (if needed)

1 0.000000 0.000000 192.168.1.102 128.119.245.12 TCP 62 1101 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

2 0.023172 0.023172 128.119.245.12 192.168.1.102 TCP 62 80 → 1101 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1

3 0.023265 0.000093 192.168.1.102 128.119.245.12 TCP 54 1101 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0

4 0.026477 0.003212 192.168.1.102 128.119.245.12 TCP 619 1101 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

5 0.041737 0.015260 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

6 0.053937 0.012280 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=566 Win=6780 Len=0

7 0.054026 0.000809 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

8 0.054690 0.000664 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

9 0.077294 0.022604 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=2026 Win=8760 Len=0

10 0.077405 0.000111 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

11 0.078157 0.000752 192.168.1.102 128.119.245.12 TCP 1514 1101 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

12 0.124085 0.045928 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=3486 Win=11680 Len=0

13 0.124185 0.000100 192.168.1.102 128.119.245.12 TCP 1201 1101 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a stream already established: 1101→80 Seq=1 Win=17520 Len=565]

14 0.169118 0.044933 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=4946 Win=14600 Len=0

15 0.217299 0.048181 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=6406 Win=17520 Len=0

16 0.267802 0.050501 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=7866 Win=20440 Len=0

17 0.304807 0.037005 128.119.245.12 192.168.1.102 TCP 68 80 → 1101 [ACK] Seq=1 Ack=9013 Win=23360 Len=0

18 0.305045 0.000000 192.168.1.102 128.119.245.12 TCP 62 1101 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6_daiaf:73 (00:06:25:d0:00:00)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1101, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1101
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment Number (raw): 0
0111 = header length: 28 bytes (7)
Flags: 0x0002 (SYN)
Window: 16384
[calculated window size: 16384]

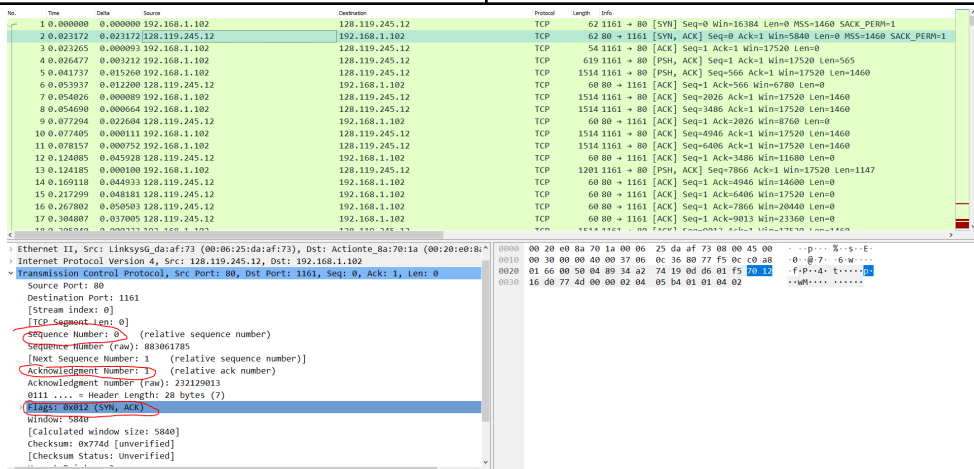
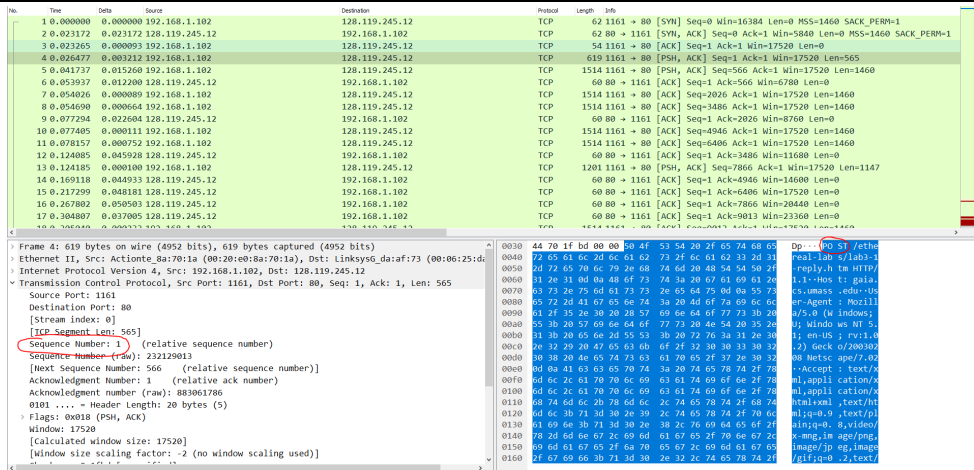
5

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

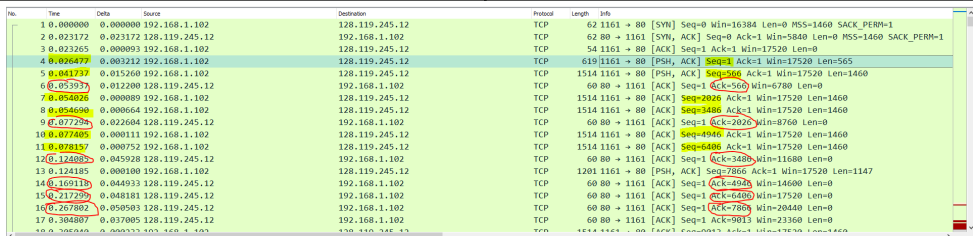
sequence number is 0

ACK number is 1, since the server received the sequence number from client is 0, it will send ACK=1 to request next segment

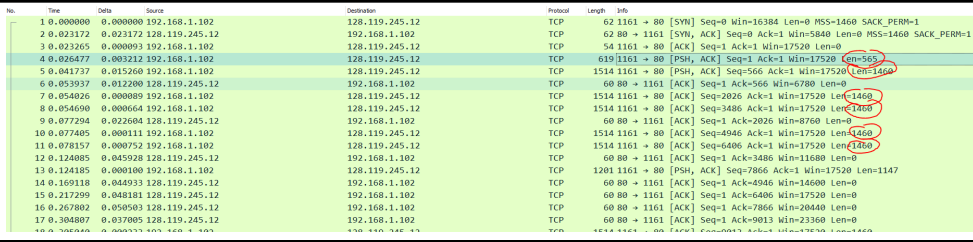
SYN & ACK flag is set to 1

	SYNACK segment?																		
Annotated Screenshots (if needed)																			
6	What is the sequence number of the TCP segment containing the HTTP POST command?	sequence number is 1																	
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 when its acknowledgement was	<table><tr><th>seg ment num ber</th><th>sequ ence num ber</th><th>time Sent</th><th>time AC K recei ved</th><th>Esti mate d RTT</th></tr><tr><td>1</td><td>1</td><td>0.02647</td><td>0.053937</td><td>0.027467</td></tr><tr><td>2</td><td>566</td><td>0.041737</td><td>0.077294</td><td>0.028467</td></tr></table>			seg ment num ber	sequ ence num ber	time Sent	time AC K recei ved	Esti mate d RTT	1	1	0.02647	0.053937	0.027467	2	566	0.041737	0.077294	0.028467
seg ment num ber	sequ ence num ber	time Sent	time AC K recei ved	Esti mate d RTT															
1	1	0.02647	0.053937	0.027467															
2	566	0.041737	0.077294	0.028467															

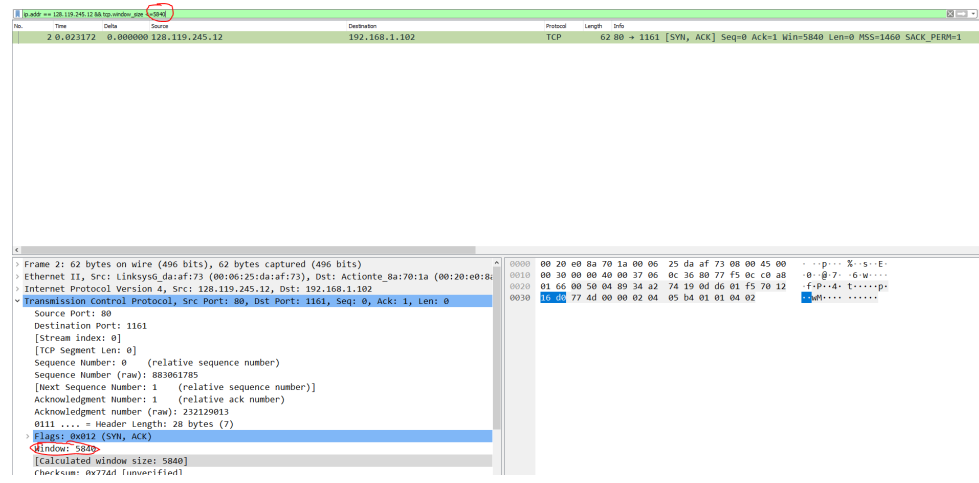
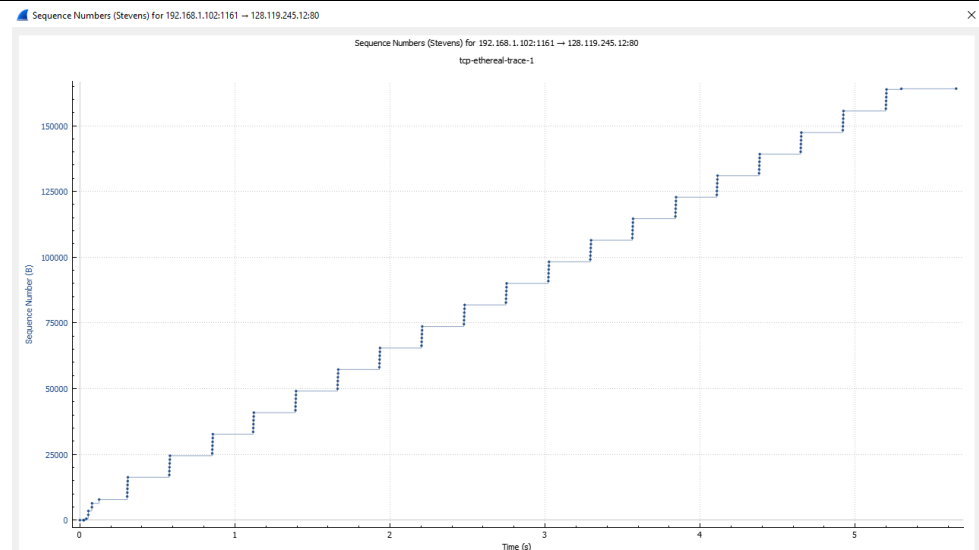
	received, what is the RTT value for each of the six segments? What is the EstimatedRTT value after the receipt of each ACK?	3	2026 4026	0.05 4026	0.12 4085	0.0336 7584
		4	3486 4690	0.05 4690	0.16 9118	0.0437 6986
		5	4946 7405	0.07 7405	0.21 7299	0.0557 8538
		6	6406 8157	0.07 8157	0.26 7802	0.0725 1783

Annotated Screenshots (if needed)	
-----------------------------------	--

8	What is the length of each of the first six TCP segments?	segment number	Len
		1	565
		2	1460
		3	1460
		4	1460
		5	1460
		6	1460

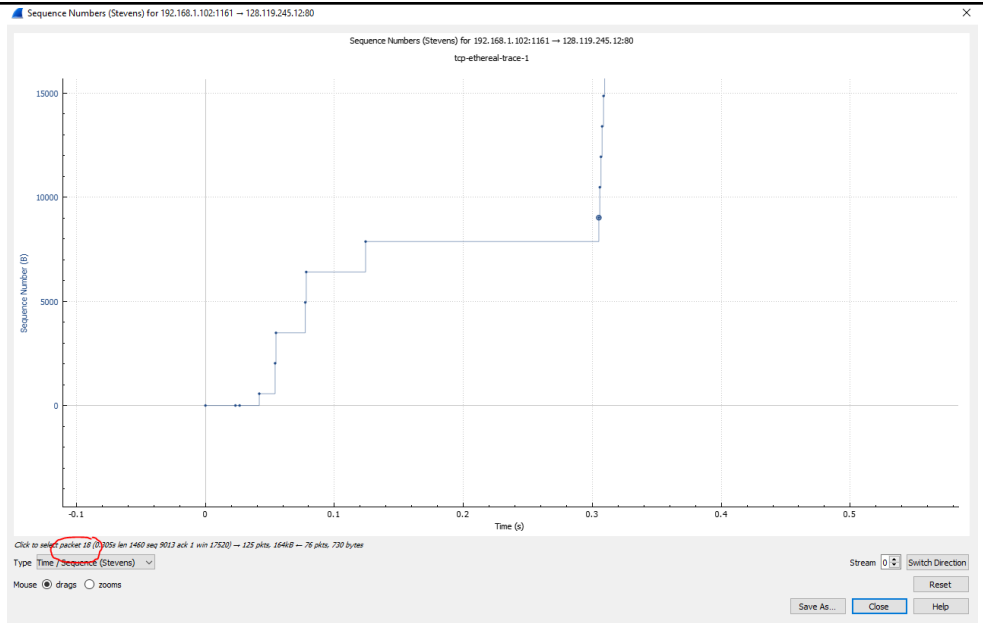
Annotated Screenshots (if needed)	
-----------------------------------	--

9	What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of	minimum available buffer is 5860 at the time when transferring start. No
---	--	---

	receiver buffer space 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 Check the duplicated sequence number, we can see that the graph is strictly increasing, so there is no duplicate sequence
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	MSS: 1460 Arrival of out-of order segments, the receiver send duplicate ACK to request the sender to retransmit the lost segment

Annotated Screenshots (if needed)		
12	<p>What is the throughput (bytes transferred per unit time) for the TCP connection?</p> <p>Explain how you calculated this value.</p>	<p>throughput = Total data/Total time it transfer=160490 bytes/5.46s=29394 byte/s</p>
Annotated Screenshots (if needed)		
13	<p>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.</p> <p>Tip: if your time sequence doesn't look like the one in the handout, try pressing the Switch Direction button.</p>	<p>At the 18th packet the TCP ends the slow start and enters the congestion avoidance.</p> <p>In the wireshark the number of segments stay the same when entering the congestion avoidance, but ideal, the number of segments will increase by one in congestion avoidance</p>

Annotated
Screenshots
(if needed)



Question 14 omitted