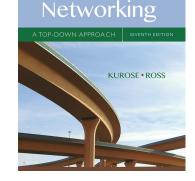
CS 447: Network and Data Communication

Wireshark Lab #02: TCP

© 2005-2017, J.F Kurose and K.W. Ross, All Rights Reserved

Note:

- Make sure you produce your answers and any packet prints in PDF. Moodle will only accept PDF files.
- Provide a screenshot with each answer wherever applicable or possible as proof of your work.



Computer

In this lab, we'll investigate the behavior of the celebrated TCP protocol in detail. We'll do so by analyzing a trace of the TCP segments sent and received in transferring a 380KB file (containing the text of Robert Louis Stevenson's *Treasure Island*) from your computer to a remote server. We'll study TCP's use of sequence and acknowledgement numbers for providing reliable data transfer; we'll see TCP's congestion control algorithm – slow start and congestion avoidance – in action; and we'll look at TCP's receiver-advertised flow control mechanism. We'll also briefly consider TCP connection setup and we'll investigate the performance (throughput and round-trip time) of the TCP connection between your computer and the server.

Before beginning this lab, you'll probably want to review sections 3.5 and 3.7 in the text¹.

• Capturing a bulk TCP transfer from your computer to a remote server

Before beginning our exploration of TCP, we'll need to use Wireshark to obtain a packet trace of the TCP transfer of a file from your computer to a remote server. You'll do so by accessing a Web page that will allow you to enter the name of a file stored on your computer (which contains the ASCII text of *Treasure Island*), and then transfer the file to a Web server using the HTTP POST method (see section 2.2.3 in the text). We're using the POST method rather than the GET method as we'd like to transfer a large amount of data *from* your computer to another computer. Of course, we'll be running Wireshark during this time to obtain the trace of the TCP segments sent and received from your computer.

Do the following:

- Start up your web browser. Go the <u>http://www.gutenberg.org/cache/epub/120/pg120.txt</u> and retrieve an ASCII copy of *Treasure Island*. Store this file somewhere on your computer.
- Next go to <u>http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html</u>.
- You should see a screen that looks like similar to Figure 01 below.
- Use the *Browse* button in this form to enter the name of the file (full path name) on your computer containing *Treasure Island* (or do so manually). Don't yet press the "*Upload alice.txt file*" button.
- Now start up Wireshark and begin packet capture (*Capture->Start*) and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).

¹ References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down* Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.



Figure 1

- Returning to your browser, press the "*Upload alice.txt file*" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture. Your Wireshark window should look similar to the window shown below.

	Capture Analyze Statisti	cs Telephony W		
			* 🖃 🗏	
Apply a display filter <ct< th=""><th>rl-/></th><th></th><th></th><th>Expression</th></ct<>	rl-/>			Expression
				ngt Info
1 0.000000000	24.37.243.70	255.255.255.255	UDP	215 44688 → 7437 Len=173
2 1.993634405	24.37.243.78	128.119.245.12	TCP	66 52676 → 80 [FIN, ACK] Seq=1 Ack=1 Win=229 Len=0 TSval=476468575 TSecr=40451053
3 1.993705570	24.37.243.78 1	128.119.245.12	TCP	66 52674 → 80 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0 TSval=476468575 TSecr=40457928
4 1.998102025	24.37.243.78	128.119.245.12	TCP	74 52688 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=476468579 TSecr=0 WS=128
5 2.040153609	128.119.245.12	24.37.243.78	TCP	66 80 → 52674 [ACK] Seq=1 Ack=2 Win=235 Len=0 TSval=40464209 TSecr=476468575
6 2.040157206	128.119.245.12	24.37.243.78	TCP	66 80 → 52676 [FIN, ACK] Seq=1 Ack=2 Win=227 Len=0 TSval=40464209 TSecr=476468575
7 2.040201838	24.37.243.78	28.119.245.12	TCP	66 52676 → 80 [ACK] Seq=2 Ack=2 Win=229 Len=0 TSval=476468622 TSecr=40464209
8 2.044458954	128.119.245.12	24.37.243.78	TCP	74 80 → 52680 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=40464213 TSecr=476468579 WS=128
9 2.044505412	24.37.243.78	128.119.245.12	TCP	66 52680 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=476468626 TSecr=48464213
10 2.044830243		128.119.245.12		734 52688 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=668 TSval=476468626 TSecr=40464213 [TCP segment of a reassembled PDU]
11 2.044886694	24.37.243.78 1	128.119.245.12	TCP 1	514 52688 → 80 [ACK] Seq-669 Ack-1 Min-29312 Len-1448 TSval-476468626 TSecr-40464213 [TCP segment of a reassembled PDU]
 <u>[Frame: 18, payloa</u> <u>[Frame: 11, payloa</u> <u>[Frame: 12, payloa</u> <u>[Frame: 13, payloa</u> <u>[Frame: 14, payloa</u> <u>[Frame: 15, payloa</u> <u>[Frame: 16, payloa</u> 	d: 0-667 (668 bytes)) d: 668-2115 (1448 bytes d: 2116-3563 (1448 bytes d: 3564-5011 (1448 byte d: 5612-6459 (1448 byte d: 6460-7907 (1448 byte d: 7908-9355 (1448 byte	511 5211 5211 5211 5211 5211 5211 5211		939(1448), #13(1448), #13(1448), #13(1448), #17(1448), #18(1448), #19(1448), #21(1448), #22(1448), #23(1448), #25(1448), #27(1448), #29(1448),
1011 05 5e 8f cd 48 02 1020 f5 0c cd cd 02 6e 02 50 00	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3 4e 88 77 6 02 88 18 6 8f 02 69 d 0a 0d 0a p5a 6 74 68 65 P1a 6 66 67 72 rg 1 74 69 6f c e 64 28 61 74 69 6 66 174 dd1 5 78 74 65 ior 2 28 6f 66 d 1	<pre>8 E e e \$ % N w P 11 st aff. ease c hack the roject Gutenbe Web p ages for urrent donatio metho ds and a resses . Donat ns are accepte in a n umber of ther ways inc ding c hecks, a</pre>	
Frame (1388 bytes) Reasse				- Packets: 480 - Displayed: 480 (100.0%) - Dropped: 0 (0.0%) Profile: Defa

If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's computers. You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, when you explore the questions below. • A first look at the captured trace

Before analyzing the behavior of the TCP connection in detail, let's take a high-level view of the trace.

• First, filter the packets displayed in the Wireshark window by entering "tcp" (lowercase, no quotes, and don't forget to press return after entering!) into the display filter specification window towards the top of the Wireshark window.

What you should see is series of TCP and HTTP messages between your computer and gaia.cs.umass.edu. You should see the initial three-way handshake containing a SYN message. You should see an HTTP POST message. Depending on the version of Wireshark you are using, you might see a series of "HTTP Continuation" messages being sent from your computer to gaia.cs.umass.edu. Recall from our discussion in the earlier HTTP Wireshark lab, that is no such thing as an HTTP Continuation message – this is Wireshark's way of indicating that there are multiple TCP segments being used to carry a single HTTP message. In more recent versions of Wireshark, you'll see "[TCP segment of a reassembled PDU]" in the Info column of the Wireshark display to indicate that this TCP segment contained data that belonged to an upper layer protocol message (in our case here, HTTP). You should also see TCP ACK segments being returned from gaia.cs.umass.edu to your computer.

Answer the following questions, based on your capture. Whenever possible, when answering a question, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout² to explain your answer. To print a packet, use *File*-*Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

- 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? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.
- 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?

Since this lab is about TCP rather than HTTP, let's change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages. To have Wireshark do this, select *Analyze-*>*Enabled Protocols*. Then uncheck the HTTP box and select *OK*. You should now see a Wireshark window that looks like:

² What do we mean by "annotate"? If you hand in a paper copy, please highlight where in the printout you've found the answer and add some text (preferably with a colored pen) noting what you found in what you 've highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

Image Secure Description Proceeding large labor 10 4.15334555 24.37 24.07.1 121 12.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque029 Active Library 200506 Secure 44775856 12 4.151345655 24.37 24.07.1 121 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque029 Active Library 200506 Secure 44775826 12 4.1513526 24.37 24.07.1 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque039 Active Library 200506 Secure 44775826 14 4.1513526 24.37 24.07.1 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque039 Active Library 200506 Secure 477882 14 4.1513526 24.37 24.07.1 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque039 Active Library 200506 Secure 477882 14 4.1513526 24.37 24.0.7 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque039 Active Library 200506 Secure 477882 14 4.1513527 24.37 24.0.7 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque139 Active Library 200506 Secure 477882 14 4.151228 24.37 24.0.7 122 11.152.25.1.2 TCP 131 42.2714 + 10 (AG) Seque139 Active Library 200 Active Library 200506 Secure 4777882 <th>🔲 🗟 🕲 🖄 🖄 🔘</th> <th></th> <th></th> <th></th> <th></th>	🔲 🗟 🕲 🖄 🖄 🔘				
14 4 1154455 24 47 24 47 7 22 112 42 112 24 112 17 12 14 21152 45 12 17 12 14 212 15 24 12 17 12 14 12 15 24 17 12 14 12 15 24 17 12 14 12					Expressi
14 4 11970 4 4 4 7 2 4 7 1 2 1 1 2 4 5 1 2 1 7 0 13 4 272 1 1 7 0 13 4 272 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1				Lengt Info	
12 4 0.11 4 0.11 0.4 0.7 0.7 0.7 10.2 0.1 0.2 0.7 10 10.2 0.1 0.2 0.7 0.0 0.0 0.0 0.2 0.0 0.2 0.0 0.2 0.0 0.2 0.0 0.2 0.0 0.2 0.0 0.0	10 4.813034565 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=669 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
11 4 411224 4 477 40.7 121 19 24.1 2 17 0 13 4 271 4 4 7 1 4 2 10 1 4 271 4 4 7 1 40. 2 40. 2 49-2 13 4 1 - 1 411 - 22 1 4 - 4771805 1 5 - 477182 13 4 411224 4 3 7 241 7 1 13 4 411225 4 2 4 3 7 241 7 1 14 4 11225 4 2 1 1 2 2 11 9 25 1 2 17 1 2 11 9 25 1 2 17 1 1 2 1 4 271 4 4 1 (A1) 3 9 - 979 7 Act 1 411 - 22 1 ent 441 15 - 14778586 1 5 e c - 477182 14 4 11224 7 4 1 7 2 1 1 2 1 1 9 25 1 2 17 1 2 1 1 9 25 1 2 17 1 1 7 1 3 4 271 4 4 1 (A1) 3 9 - 979 7 Act 1 411 - 22 1 ent 441 15 - 21 - 4778586 1 5 e c - 477182 14 4 11224 7 4 1 7 2 1 1 1 2 1 1 9 2 1 1 9 2 1 1 9 2 1 1 2 1 1 9 2 1 1 7 1 2 1 1 9 2 1 1 2 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2 1 1 7 1 2 1 1 9 2 1 1 7 2	11 4.813076360 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=2117 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
14 4.8115214 24.37 24.77 123.19.24.72 17 123.19.24.72 17 12 1314 2271 4 40 24.07 Sep-904 64.5 14.5 14.912-29 14-772845 1560-772842 13 4.312528 24.37 24.77 123.19.25.12 17 134 5271 4 40 24.07 Sep-904 64.7 14.5 12.5 14.4778586 1560-477882 13 4.3125298 24.37 24.78 123.19.25.12 17 134 5271 4 40 24.07 Sep-904 64.5 14.5 14.29 14-7728586 1560-477882 13 4.3125298 24.37 24.78 123.19.25.12 17 15 134 5271 4 40 24.07 Sep-108 64.5 14.5 14.29 14-778586 1560-477882 13 4.3125298 24.37 24.78 123.19.25.12 17 15 134 5271 4 40 24.07 Sep-108 64.5 14.5 14.29 14-778586 1560-477882 13 4.3125298 24.37 24.78 12 12.19.25.12 17 15 134 5271 4 40 24.07 Sep-108 64.5 14.5 14.29 14-778586 1560-477882 13 4.3125298 24.37 24.78 12 12.19.25.12 17 15 134 5271 4 40 24.07 Sep-108 64.5 14.5 14.29 14.0 14.78 15.5 14.5 14.5 14.5 14.5 14.5 14.5 14.5	12 4.813104778 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=3565 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
14 4.000 4.07 4.07 4.07 10.0000 10.0000 10.000 10.000 10.000 10.000 10.000 10.0	13 4.813127964 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq-5013 Ack-1 Win-229 Len-1448 TSval-476785866 TSecr-40773082	
14 4.1529489 2.4 37 2.4 77 1 22.1 10.245 1.2 10 1 10 114 5271 4 10 (AL) Sep-103 7 Abr 1 10:229 2.02-1447 15361 5362-4477882 13 4.13228479 2.4 37 2.4 77 1 22.1 10.245 1.2 10 1 10 114 5271 4 10 (AL) Sep-1037 Abr 1 10:229 2.02-1447 15361 5362-1477882 13 4.3228479 2.4 37 2.4 77 1 22.1 10.245 1.2 10 1 10 114 5271 4 10 (AL) Sep-1037 Abr 1 10:229 2.02-1447 15361 5362 1562-4077882 13 4.3228479 2.4 37 2.4 77 1 22.1 10.245 1.2 10 1 10 114 5271 4 10 (AL) Sep-1037 Abr 1 10:229 2.02-1447 15361 5361 5562-4077882 14 4.32847744 2.8 10.2 7.4 77 1 22.1 10.2 45 1.2 10 1 10 11 10	14 4.813153234 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=6461 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
11 4 11272185 2 41 77 41 77 10 22 119 245 12 10 10 134 571 4 10 (AG) (speched 55 Adv-1 kin-22 (sm-144 TSval-4777882 Tser-4777882 18 4 3122407 24 37 24 77 12 21 19 24 51 2 51 10 10 134 571 4 10 (AG) (speched 55 Adv-1 kin-22 (sm-144 TSval-4777882 Tser-4777882 24 4 3128277 24 37 72 47 71 12 119 245 12 10 10 154 571 4 10 (AG) (speched 55 Adv-1 kin-22 (sm-144 TSval-4778868 Tser-4777882 24 4 3128277 24 37 72 47 71 12 119 245 12 10 10 154 571 4 10 (AG) (speched 55 Adv-1 kin-22 (sm-144 TSval-4778868 Tser-4777882 24 4 3128277 24 37 72 47 71 12 119 245 12 10 10 154 571 4 10 (AG) (speched 5 Adv-1 kin-22 (sm-144 TSval-47787868 Tser-4777882 24 4 3128277 34 37 72 47 71 12 119 245 12 10 10 1457 21 (sm-144 TSval-47787868 Tser-4777882 24 4 3128277 34 77 40 77 71 10 17 10 12 119 24 12 110 24 110 24 12 110 24 110 24 110 24 110 11 110 12 110 12 110 12 110 110 110	15 4.813166578 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq-7909 Ack-1 Win-229 Len-1448 TSval-476785866 TSecr-40773082	
14 4.122407 2.4277.2077 2.427.207	16 4.813255405 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=9357 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
10 4 6579247 12 47.72 657.71 12 12 10 22 5.12 17 10 12 10 22 5.12 11 5274 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 42 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 574 4 6 10 4 10 4 10 4 10 4 10 4 10 4 10 4	17 4.813272105 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=10805 Ack=1 Win=229 Len=1448 TSval=476785866 TSecr=40773082	
24.4 359227 24.27 24.77 24.77 24.79 24.77 24.19 24.19 24.17 24 24.	18 4.813284767 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seq=12253 Ack=1 Win=229 Len=1448 T5val=476785866 TSecr=40773082	
<pre></pre>	19 4.858857484 128.119.245.12	24.37.243.78	TCP	66 80 → 52714 [ACK] Seq=1 Ack=669 Win=237 Len=0 TSval=40781501 TSecr=476785866	
Enert II. Sp:: Legra.(J2:60:0) (00:07-60:0-02:00), DD:: Dp::ID:02:00:00) met Functorial Version 6. Sp:: 23 27:20 370, DD:: 123 119:20:512 mainsion control Protocol, Sp:: Port: Sp714, DD: Port: 0: 50:0 (000 bytes) cf: 40 84 97 80 69 89 47 80 42 60: 90 80 69 55 80 control Bore E cf: 40 84 97 80 69 89 47 80 42 60: 90 80 69 55 80 control Bore E cf: 40 84 97 80 69 49 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 49 60 42 60: 103 51 54 40 877 control Bore E cf: 40 84 97 80 69 49 60 42 60: 103 51 54 40 877 control Bore E cf: 40 84 97 80 69 49 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 40 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 40 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 40 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 40 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 84 97 80 69 40 60 42 60: 103 51 54 40 80 7 control Bore E cf: 40 70 80 70 70 70 70 70 70 70 70 70 70 70 70 70	20 4.858902247 24.37.243.78	128.119.245.12	TCP	1514 52714 → 80 [ACK] Seg=13701 Ack=1 Win=229 Len=1448 TSval=476785912 TSecr=40781501	
22 05 24 05 04 46 05 44 05 12 57 13 48 07 12 57 13 48 07 1 45 07 1 4 0 4 12 57 13 48 07 1 4 0 5 12 57 13 4 0 5 12 50 10 5 10 5 0 5 10 5 0 5 10 5 0 5 10 5 0 5					
15 % C c d0 x a 80 5 8 c 7 6d d i c 3 39 a 1 a ac 29 0 118					
000 000 <td>, (668 bytes) c4 e7 84 97 86 82 80 87 0e 42 0c</td> <td>:: 52714, Dst Port: 84</td> <td></td> <td></td> <td></td>	, (668 bytes) c4 e7 84 97 86 82 80 87 0e 42 0c	:: 52714, Dst Port: 84			
06 a0 6 c 16 27 37 47 6c 61 22 33 24 31 a0 72 c 65 k-labs71 abs-i-cree Te C 70 26 66 77 37 4 a 24 6 71 30 4 a 26 37 13 26 i k-labs71 abs-i-cree Te C 70 26 66 77 37 4 a 24 6 71 30 74 i k-labs71 abs-i-cree Te C 70 26 66 77 37 4 a 24 6 71 30 74 i k-labs71 abs-i-cree Te C 70 26 66 77 5 74 a 24 6 71 50 74 i k-labs71 abs-i-cree Te C 70 26 66 74 50 74 20 41 61 60 76 7 i k-labs71 abs-i-cree Te C 70 26 66 74 50 74 20 41 61 60 76 7 i k-labs71 abs-i-cree Te C 70 26 76 76 abs-i-cree a	(668 bytes) c4 e9 84 97 85 89 98 97 98 42 90 22 d9 74 93 46 89 48 69 49 91 18	95 08 00 45 00 25 13 46 80 7	18, Seq: 1, A	я <u>.</u> Ям	
The C: 70 26 67 26 42 9 44 54 54 50 27 11 26 11 [b], hts HTTP/L1 64 64 64 76 77 77 75 64 30 41 54 56 77 67 16 78 67 26 78 75 66 16 77 77 72 26 65 67 75 68 30 41 37 66 66 57 67 68 74 66 67 66 30 28 66 55 57 76 26 16 65 77 68 75 68 16 38 37 66 74 50 74 50 16 66 77 68 74 50 76 68 37 66 74 20 44 55 16 69 77 68 74 50 76 68 39 76 69 74 20 44 55 16 97 76 8 74 50 76 78 78 78 78 78 78 78 78 78 78 78 78 78	(668 bytes) c.f. e0 84 07 bh 85 80 07 00 42 06 20 68 74 05 44 0 69 42 06 41 95 11 15 0 c. for ea 80 59 c? dd dd c3 39	95 08 00 45 00 25 73 46 80 7 t al ac 29 80 18	18, Seq: 1, A tere B tere B P 	€. R w) - n	
odd to 4 d6 r7 37 r6 3a 20 f0 r6 00 f1 20 61 37 20 r2 - Most:	(468 bytes) cl or Add ST BL 00 00 00 00 42 0c; 01 00 74 01 04 00 00 01 00 42 0c; 02 00 74 01 04 00 00 00 01 01 01 01 00 00 50 74 00 00 00 01 01 01 01 00 00 50 74 00 00 00 01 01 01 01 00 01 00 00 00 00 01 01 01 01 00 01 00 00 00 00 01 01 01 01 00 01 00 01 00 00 01 01 01 01 00 01 00 01 01 01 01 01 00 01 01 01 01 01 00 01 01 01 01 01 00 01 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 00 01 01 00 01 01 00 01 01 00	95 08 00 45 00 25 14 50 25 13 45 00 25 13 45 50 25 15 26 15 27 36 50 28 15 20		E R N J D D D D	
63 74 69 67 66 23 26 69 67 65 77 62 45 61 67 67 ction: keep-alia 68 28 49 67 66 74 65 66 74 24 65 66 77 7 ction: keep-alia 68 28 28 33 93 13 73 4 3 68 48 44 51 68 66 5 h: 39774 6 Cache 24 38 67 66 74 72 67 66 58 23 46 61 72 26 15 67 - Contral : asarag 63 28 49 64 28 47 72 69 67 89 66 3a 28 66 74 74 e eet Origin: htt 78 3a 27 47 67 61 66 13 28 76 77 67 67 77 69 78 79 77 69 13 79 . Transa	(464 bytes) cc or 2 do 9f lb 0a 08 of 09 of 20 cc or 2 do 9f lb 0a 08 of 09 of 20 cc or 2 do 40 of 20 cc or 2 do 50 of 2 cc or 2 cc or 2 do 50 of 2 cc or 2 cc	90 08 00 45 00 25 73 40 05 00 25 73 40 00 77 t al m 29 50 18 05 22 c 8 00 57 26 66 17 2 % P		t n n haz - re	
65 68 8 48 3 67 66 74 65 6 67 72 64 65 66 67 76 e Contentententente 68 3a 28 33 93 31 37 34 36 68 48 48 16 16 36 86 5 h: 30174 6 Cache 28 34 57 66 74 72 65 66 5 3a 28 66 61 78 23 65 16 7 - Control : max-ag 65 36 38 68 38 47 72 65 67 49 56 3a 28 66 17 74 74 e emě Drigin: htt 73 3a 27 47 67 61 66 12 68 37 28 75 66 17 37 9: //gana c.s.umans	(464 hytes) cf en 84 97 hb en 40 ef 40 ef 20 20 dh 20 s 40 ef 20 20 d	50 60 60 55 00 25 12 40 65 00 25 12 40 60 77 25 12 40 60 77 25 10 40 60 77 25 10 40 60 25 10 61 72 50 26 50 26 50 26 51 26 51 50 27 55 50 27 51 26 51 50 27 51 50 20 51 50 50 50 50 500		б. Ям - Л - Л - Л - Л - Л - Л - Л - Л - Л - Л	
66 3a 26 3 39 3 13 73 4 5 6 6 d à 4 3 6 (6 5 6 6 5 h : 307 74 6 Cache 20 4 3 6 6 6 6 7 2 7 6 6 6 5 a 2 6 6 1 7 2 2 6 1 6 7 . Contral : max-ag 6 3 2 6 3 6 6 7 2 7 6 6 6 1 a 2 6 6 7 2 7 6 6 6 1 3 7 9 1 7 7 1 7 1 7 1 7 1 7 1 7 1 7 1 7 1	(466 bytes) Cc 4 e9 84 97 Bb 89 89 07 89 42 86 22 09 74 93 46 89 89 67 89 42 86 22 09 74 93 46 89 49 60 42 95 18 15 8c Cc 49 84 9 60 42 95 18 25 4b 24 46 43 34 92 27 70 97 29 25 4b 24 45 35 94 29 27 70 97 29 26 45 94 45 35 94 29 27 70 97 29 26 45 94 45 35 94 29 27 70 97 29 26 45 94 45 35 94 29 27 70 97 29 26 45 94 45 35 94 29 27 70 97 29 26 45 94 45 35 94 29 27 70 97 29 26 45 95 46 77 37 74 39 28 67 56 46 26 46 77 37 74 39 28 67 56 46	50 88 68 65 68 23 73 46 88 77 t 30 62 62 86 76 t 25 73 46 88 77 t 31 36 26 87 98 18 20 32 62 68 79 78 23 31 27 51 79 78 19 32 37 31 73 78 19 10 15 26 37 28 11 11 15 16 26 37 28 11 11 16 12 16 26 37 28 11 11 15 16 26 37 28 11 11 15 16 16 26 37 12 13 16 16 16 26 30 16 16 36 16 16 16	i8, Seq: 1, A t & B F P P S T V Mines T B S T V Mines T S T V Mines T S T V Mines T S S C Mines T S S C Mines T S C S C Mines T S C Mines T S C Mines T S S C Mines T S C S C S C S C S C S C S C S C S C S	я; Ки)- ла Ла 14 14 15 15 15 15 15 15 15 15 15 15 15 15 15	
65 3d 3m 6d 8a 4f 72 60 57 65 6e 3a 38 6d 74 74 ere 0 ori gin: htt 78 3a 2f 2f 67 61 60 61 2e 637 22 07 5 6d 61 51 p.//gaia.cc.umas	(466 bytes)	50 60 60 45 60 25 50 60 45 60 25 51 60 60 7 25 51 60 60 7 26 60 10 60 20 60 10 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	18, Seq: 1, A 18, Seq: 1, A 18, Seq: 1, A 18, Seq: 1, A 18, Seq: 1, A 19, Seq: 10, Seq:	E N N N N N N T T S S S S S S S S S S S S	
76 3a 2f 2f 67 61 69 61 2e 63 73 2e 75 6d 61 73 p://gaia_cs.umas	<pre>cc ev 84 0 yr 80 0a 00 0f 00 42 0c 22 0a 74 53 44 0b 44 05 14 00 42 34 0c 74 53 44 0b 44 05 44 05 13 36 0c 74 53 44 0b 44 05 44 05 13 36 0c 74 53 44 0b 44 05 44 05 13 36 0c 74 53 44 0b 44 05 44 05 13 36 0c 74 53 44 0b 44 05 44 05 13 36 0c 74 53 44 0b 44 05 45 45 14 36 0c 74 53 44 0b 44 05 45 45 14 36 0c 74 53 44 0b 44 05 45 45 14 36 0c 74 53 44 0b 44 05 45 14 36 0c 74 53 44 0b 44 05 45 14 36 0c 74 54 0c 74 73 74 32 45 05 16 36 0c 74 54 25 74 75 74 32 45 05 16 36 0c 74 54 25 74 75 74 32 45 05 16 36 0c 74 54 25 74 75 74 15 45 16 16 75 16 36 0c 74 54 25 76 75 74 15 16 16 16 16 16 16 16 16 16 16 16 16 16</pre>	90 60 60 65 60 23 15 46 67 76 24 16 46 77 16 30 76 86 77 76 16 30 73 16 17 7 7 24 30 73 16 17 7 7 24 31 21 7 31 16 35 31 16 35 31 16 32 31 16 32 31 16 32 32 31 16 32 32 31 16 32 32 31 16 32 32 31 16 32 32 31 16 36	ie, seq: 1, А в в в t е е в ъ P 9 b k, P 9 kost: gala, ass.ed и Со ion: k еера- Conte nt-Lei 30174 6 СТС	Е Ки)) л л л л сте 1.1 ст. ст. ст. ст. ст. ст. ст. ст. ст. ст.	
	cf dd hytes) cf dr hytes) cf dr hytes) df hytes) cf dr hytes) df hytes) dr hytes) df hytes) <td>Spatial Spatial <t< td=""><td>ie, Seq: 1, A E & Seq: 1, A E & S E & S & S & S E & S &</td><td>б А м - D - D - D - D - D - D - D - D - D - D</td><td></td></t<></td>	Spatial Spatial <t< td=""><td>ie, Seq: 1, A E & Seq: 1, A E & S E & S & S & S E & S &</td><td>б А м - D - D - D - D - D - D - D - D - D - D</td><td></td></t<>	ie, Seq: 1, A E & Seq: 1, A E & S E & S & S & S E & S & S & S & S & S & S & S & S & S &	б А м - D - D - D - D - D - D - D - D - D - D	
73 2e 65 64 75 0d 0a 55 70 67 72 61 64 65 2d 49 s.eduU pgrade-I	c (4 4 9 bytes) c 4 4 0 bytes) c 4 4 bytes c 4 5 bytes) c 4 5 bytes c 4 5 bytes) c	90 00 00 50 00 31 02214, Dat Port B 32 00 00 50 00 33 15 00 00 34 00 00 35	ie, Seq: 1, A t @ E \$ 1 t @ E \$ 1 P 9 b \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	я: Я и). п ла ла ла ла ла ла ла ла ла ла ла ла ла	
	a (666 bytes) c4 60 B 5 91 Bb 6a 80 07 60 4 2 0c c5 60 4 2 0c 60 4 2 0c c6 60 4 2 0c 60 4 2 0c c7 60 4 2 0c 60 4 2 0c c7 60 4 2 0c 60 4 2 0c c8 60 c 10 0c 70 7 00 c9 c9 10 c 80 00 00 10 00 80 1 00 c9 c9 10 c 80 00 00 10 00 80 1 00 80 1 00 c9 c9 10 c 80 00 00 10 00 80 1 00 80 1 00 80 1 00 c9 c9 10 c 80 00 00 10 00 80 1 00 80 1 00 80 1 00 c9 c9 10 c 60 00 00 73 2 c 60 2 40 7 50 60 2 40 c9 60 10 00 17 7 72 c 60 00 00 00 80 00 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00	Sp. 88 68 65 88 7 8 Sp. 88 68 65 88 7 1 Sp. 88 68 7 1	<pre>18, Seq: 1, A 18, Seq: 1,</pre>	# N w n 10 11 12 13 14 15 16 17 18 19 11 12 13 14 15 16 17 18 181	

This is what we're looking for - a series of TCP segments sent between your computer and gaia.cs.umass.edu. We will use the packet trace that you have captured (and/or the packet trace *tcp-ethereal-trace-1* in <u>http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip</u>; see earlier footnote) to study TCP behavior in the rest of this lab.

• TCP Basics

Answer the following questions for the TCP segments:

- 3. 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?
- 4. 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?
- 5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.
- 6. 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 (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal

to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

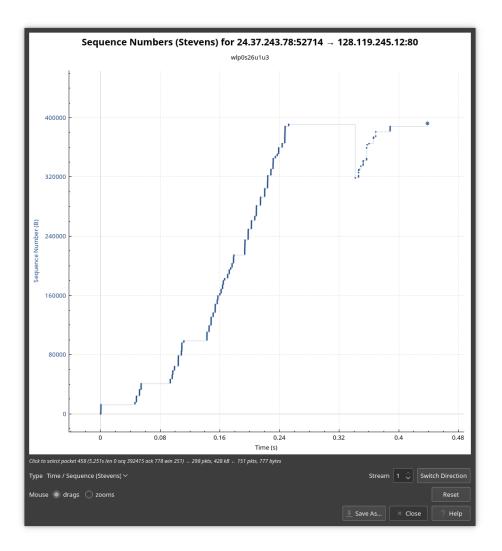
Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: *Statistics->TCP Stream Graph->Round Trip Time Graph.*

- 7. What is the length of each of the first six TCP segments?
- 8. 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?
- 9. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
- 10. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).
- 11. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.
- TCP congestion control in action

Let's now examine the amount of data sent per unit time from the client to the server. Rather than (tediously!) calculating this from the raw data in the Wireshark window, we'll use one of Wireshark's TCP graphing utilities - *Time-Sequence-Graph(Stevens)* - to plot out data.

• Select a TCP segment in the Wireshark's "listing of captured-packets" window. Then select the menu : *Statistics->TCP Stream Graph-> Time-Sequence-Graph(Stevens)*. You should see a plot that looks similar to the following plot.

Here, each dot represents a TCP segment sent, plotting the sequence number of the segment versus the time at which it was sent. Note that a set of dots stacked above each other represents a series of packets that were sent back-to-back by the sender.



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 during your file transfer earliers. Answer the following questions.

- 12. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over?
- 13. Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.