Darrel Chang

Professor Ibrahhim

CS 3800

3/24/24

Homework 5 Wireshark Lab 4

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt 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).

**Source IP: 172.20.8.99**

**TCP Port: 64075**

1. What is the IP address of gaia.cs.umass.edu? On what port number is it sending

and receiving TCP segments for this connection?

**Destination IP: 128.119.245.12**

**TCP Port: 80**

1. 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?

**Sequence number 0**

1. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?

**Sequence number 0**

1. What is the sequence number of the TCP segment containing the header of the HTTP POST command?

**Sequence number 1**

Note that in order to find the POST message header, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text “POST” within its DATA field4,5.

How many bytes of data are contained in the payload (data) field of this TCP segment?

**612 bytes**

Did all of the data in the transferred file alice.txt fit into this single segment?

**No**

1. Consider the TCP segment containing the HTTP “POST” as the first segment in the data transfer part of the TCP connection.

At what time was the first segment (the one containing the HTTP POST) in

the data-transfer part of the TCP connection sent?

**At time 1.817566**

At what time was the ACK for this first data-containing segment received?

**At t = 1.894785**

What is the RTT for this first data-containing segment?

**1.894785 - 1.817566 = 0.077219**

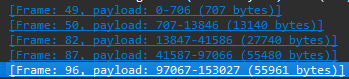
What is the RTT value for the second data-carrying TCP segment and its ACK?

**Sent at t1 = 1.894959 and ACKed at t2 = 1.971789. So the RTT = t2 - t1 = 0.07693 seconds**

What is the EstimatedRTT value (see Section 3.5.3, in the text) after the

ACK for the second data-carrying segment is received?

1. What is the length (header plus payload) of each of the first four data-carrying TCP segments?

****

1. What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments7? Does the lack of receiver buffer space ever throttle the sender for these first four data-carrying segments?

**The minimum amount of available buffer space is 131328 bytes. The lack of receiver buffer space never throttles the sender for the first four data-carrying segments**

1. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

**There are no retransmitted segments in the trace file. I checked for packets with the same sequence number sent at different times.**

1. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu?

**The receiver typically ACKs 7300 bytes in each ACK**

1. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value

**The average throughput is 95155 bytes per second. I found this by taking the total number of bytes transferred and dividing it by the total time between the last and the first segment sent was. 153028 / (2.055678 - 1.894859)**

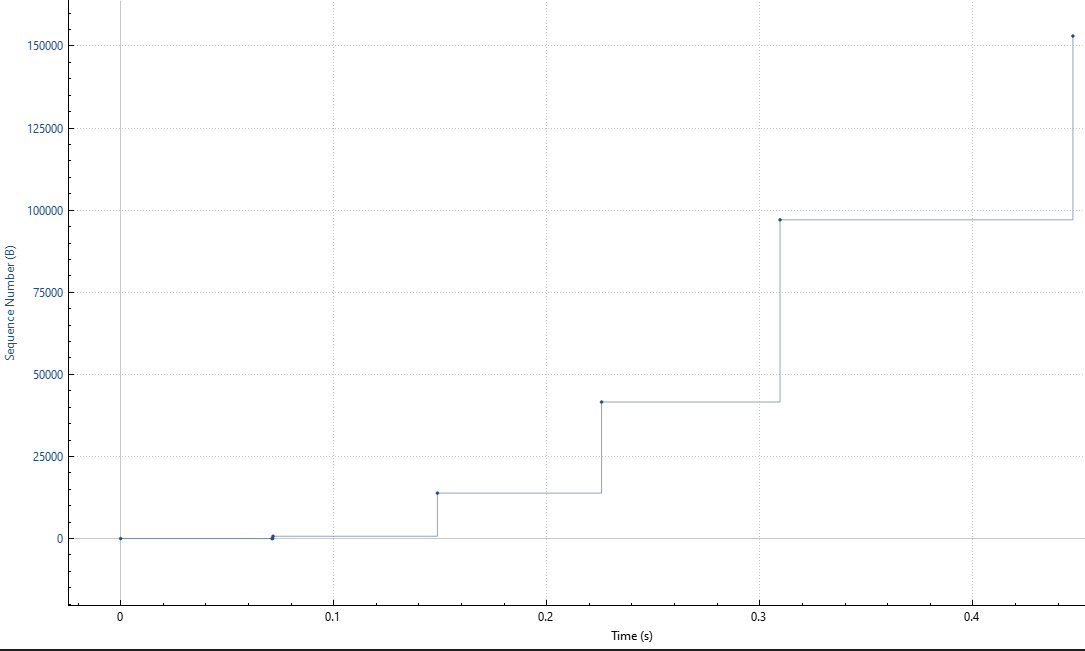
1. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the “fleets” of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase. Figure 6 shows a slightly different view of this data.

**It looks like its in it slow start phase until around the t = 0.1 second mark and then there are periods of congestions and starting again**

1. These “fleets” of segments appear to have some periodicity. What can you say about the period?

**I think the period is used to avoid congestion. The number of packets sent never changes so it doesn’t appear to be a flow control method, but rather a rate limit.**

1. 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



**For the file alice.txt I uploaded to the gaia website, it looks like the slow start occurs between the first and second segments, where the sequence number doesn’t increase much. After that point the segment sizes increase exponentially which is why the sequence number also increases exponentially.**