Hayden Townley, Noah Verdeyen
Cis 457
Section 102
Lab #9

Part I: TCP Basics

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" (0.5Pt)
    a. **35.39.165.120:50064**
2. What is the IP address of gaia.cs.umass.edu? (0.5Pt)
    a. **128.119.245.12:80**
3. On what port number is it sending and receiving TCP segments for this connection? (0.5Pt)
    a. **80**
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? (1Pt)
    a. **0, the flag has 0x002 on every SYN message**
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? (2Pts)
    a. **0, this one has 0x012 on the flag, and the ACK message needs to start at 1**
6. 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. (1Pt)
    a. **164041**
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) that are sent by the same host? 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 observed RTT value for each of the six segments? What is the EstimatedRTT value after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the "*observed RTT for Segment 1" for the first segment, and then is computed using the EstimatedRTT equation developed by Jacobson algorithm for all subsequent segments. (5Pts)
    a. **164041, 1, 1, 1, 1, 164091**

   b. **5.297, 5.389, 5.448, 5.456, 5.461, 5.651**
   c. **observedRTT:0.0232, 0.023265, 0.0245863, 0.0158489, 0.023265, 0.023265**

8. What is the length of each of the first six TCP segments? (1Pt)
   a. **50, 0, 0, 0, 730, 0**
9. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question? (1Pt)
   a. **No, we looked at the sequence numbers**
10. Approximately, what is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value. (2Pts)
    a. **1521388 bytes / 7.595557 sec = 20029.867 bytes per second**

Part II: TCP congestion control in action

11. 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 slow start phase begins and ends? (1.5Pt)
    a. **0.03, 0.03 this is where the graph goes straight up, then levels off.**
12. What is the value of the Window scale factor for the server side as well as its effective window size? (1Pt)
    a. **8192, scale is 1**
13. Compare the 3-way handshake messages in this trace (TCP-2) to your trace that you captured from your local machine in the beginning of the lab (TCP-mine). Note any differences and explain why there are differences? (1Pt)
    a. **The TCP-mine is much shorter in terms of messages, the 3-way handshake is faster though.**