Matt Kennedy CIS 457
Brent Thompson Section 101
Lab 09

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"
35.39.165.136, port 50064

2. What is the IP address of gaia.cs.umass.edu?
128.119.245.12

3. On what port number is it sending and receiving TCP segments for this connection?
port 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?
The sequence number is 0, there is a bit in the flags section of the SYN packet that sets SYN: Set to 1, which is enabled.

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?
The sequence number is 0, acknowledgement is 1. Additionally, SYN is 1, which identifies this packet as a SYNACK packet.

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.
152041 is the sequence number.

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 3 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.

The first six sequence number 152041, 1, 1, 1, 1, 1.
The times are 0.111, 0.14066, 0.14067, 0.14068, 0.14069, 0.14072
The RTT values are 0.0217, 0.0218, 0.0230, 0.0165, 0.0217, 0.02175

8. What is the length of each of the first six TCP segments?

864, 0, 0, 0, 0, 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?

There don't appear to be any; we used the tcp.analysis.retransmission filter.

10. Approximately, what is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

There are 1521388 bytes in the file. This file took 7.36249 seconds to upload.
1521388 / 7.36249 = 206640.41648953 bytes/second

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 slowstart phase begins and ends?

According to the Time-Sequence-Graph, the slow-start phase appears to begin right around 0.05 seconds. It ends shortly after.

12. What is the value of the Window scale factor for the server side as well as its effective window size?

The value is 8192, the 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?

In this trace, the overall message quantity is significantly less compared to the trace captured on our local machines. Additionally, the handshake took place faster. This could be due to differences in computer used on the network, connection destination, and speeds along the path.