CS 453: Lab 3

Using Wireshark [100 Points]

Due: Tuesday Dec 4 2018 before class

I. Using Wireshark to analyze HTTP packets

Read the Wireshark_HTTP.pdf file uploaded on e-campus (only part 1 and part 2). Answer questions 1-6 from part 1 and questions 8-11 of part 2.

Please use http-etheral-trace-1 and http-ethereal-trace-2 for answering these questions: simply download these files on to your computer from e-campus and open them using "Open" in wireshark.

II. Using Wireshark to analyze TCP segments

Download the file tcp-thereal-trace-1 from ecampus under Lab3. This is a trace file that has been generated by uploading a large file to the website http://gaia.cs.umass.edu, using the HTTP POST command. Start Wireshark, open the trace file and answer the following questions based on the trace file.

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?

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?

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 TCP segment containing the HTTP POST command? Note that in order to find the POST command you will 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.

5. 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?

6. 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 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 shown below for all subsequent segments.

   *EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT*

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