**Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

This project introduces the student to Wireshark, which is a free software for network protocol analysis. We’ll look into the behavior of the TCP protocol. We’ll see TCP’s basics such as sequence numbering and acknowledgement. The name of the input file is **tcp-trace.**

**Instructions**

1. **A first look at Wireshark**

First, let’s take a high-level view of the trace. We can filter the packets by entering “tcp” into the display filter specification window.

A screenshot of a computer

Description automatically generated

What you should see is a rich set of information like a series of messages exchanged between source and destination, in which there are three-way handshake messages and normal data messages.

Moreover, you may want to change Wireshark’s “listing of captured packets” window. In this way, it only shows information about the TCP segments containing the upper-layer messages. To have Wireshark do this, select *Analyze->Enabled Protocols*. Then uncheck the HTTP box and select OK.

Answer the following questions, by opening the file **tcp-trace.**

1. **Submission guide**

Put your answer directly in this document following each question. Submit this document (in PDF) to Canvas electronically.

**Answer Sheet**

1. What is the IP address and TCP port number used by the client (source)?
2. What is the IP address and TCP port number of the server (destination)?
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client and server?
4. What is the sequence number of the SYNACK segment sent by sever to the client in reply to the SYN?
5. What is the sequence number of the TCP segment containing the HTTP POST command? *Hint: you need to dig into the packet content field looking for a segment with a “POST” within its DATA field.*
6. What is the length of each of the first six TCP segments? Note that the first segment of these six segments starts from the one after completion of TCP handshake.
7. What is the minimum advertised window size at the receiver for the entire trace? Does this flow control condition ever throttle the sender?
8. Are there any retransmitted segments in the trace file? If there are any, indicate their sequence number(s).
9. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the RTT value for each of the six segments? *(Hint: Use the difference in time of sending data and receiving ACK.)*

What is the EstimatedRTT value after the receipt of each ACK? Use the original algorithm with alpha = 0.125. *(refer to my lecture slides for the right formula)*

*Note:* Wireshark has the feature to plot the RTT. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the server. Then select: *Statistics->TCP Stream Graph->Round Trip Time Graph.*