**Homework 7: TCP Wireshark Analysis**

The associated packet trace (TCP-Wireshark-Trace-HW6.pcapng), shows TCP packets between web browser and web server executing the download of a single web page. A web browser is using TCP to set up a connection to the web server, requesting a web page to be downloaded (packet 4), and the web server responds sending the contents of the web page in multiple subsequent TCP segments to the client. Ignore packets marked by [TCP Window Update].

*Note: To analyze the above packet trace for this homework, start with HTTP enabled (it should be on by default). To check some of the answers, you can temporarily disable HTTP processing in wireshark by going to* ***Analyze > Enabled Protocols*** *and unchecking all HTTP items.*

Examine the packet trace and answer the following questions:

1. Which packets correspond to the TCP three-way handshake \_\_\_\_1,2,3\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?
2. Packet 4 corresponds to the client sending a web request to the server. How many bytes are being sent in the above data request (excluding TCP and IP headers) \_\_\_\_\_\_\_\_\_429 bytes ethernet\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?
3. What packet is acknowledging the above client web request and why is the sequence number set to 1 and the acknowledgement number set to 430?

Packet 5 and the number is set to 430 because that is the sum of the bytes from previous plus the sequence number

1. How many TCP segments are needed to download the web page? What packet numbers does this correspond to? How large is the web page in bytes in total?

5363 bytes

1. Explain why the sequence number is increasing in the above packets, but the acknowledgement number stays the same

After acknowledging the last segment of data from the server, the client processes the HTTP response as a whole and decides no further communication is needed. So ACK stays the same

1. In packets 10 and 11, how many TCP segments are being acknowledged? 2
2. In packet 15 and 16, how many TCP segments are being acknowledged 2?
3. What is the client’s initial advertised receive window in the trace\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?
4. What is the purpose of the receive window ?
5. Does the client’s receive window change over time? Why or why not?