**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

SYN packet start something new that’s where

1. 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 len(app data)

495-66=429

SO basically subtract the one previous

Or the larger ACK -1

1. 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 is acknowledging. Seq# is 1 since it is beginning send window/ get request seq#+len=430 ack 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?

6 TCP segments are needed 6,7,8,9 13 and 14 7643 bytes LAST ACK -1

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

Seq#=seq# + app data length ack # stays the same because client does not send any more app data. Sequence number is increasing because tcp segments being sent from server to client.

1. In packets 10 and 11, how many TCP segments are being acknowledged 4 ack 2 packets each you can tell by the ack number

1 additional segments each

1. In packet 15 and 16, how many TCP segments are being acknowledged 2
2. What is the client’s initial advertised receive window in the trace 65535
3. What is the purpose of the receive window ?

The Receiver Window (rwnd) is a variable that advertises the amount of data that the destination side can receive (TELL HOW MANY PACKETS CAN BE SENT)

MEMORY SET ASIDE TO BUFFER INCOMING PACKETS

1. Does the client’s receive window change over time? Why or why not?

YES depending on how fast application can download info from the buffer