Assignment 3

Full Marks-22

Q1. Use tshark or tcpdump to capture tcp packets for 30 seconds:[1+2+3+2+2+3+3]

a) Give the screenshot of the tshark command used.

b) Use wireshark to analyze the packet trace. How many TCP connections are there and who are the communicating peers? Put a screenshot.

c) How much data has been transferred for both upstream and downstream for all the connections? Compute and put a screenshot.

d) Take a TCP connection which has transferred the maximum number of bytes. Study the sequence number progress for this connection. Check TCP stream graph. Put a screenshot.

e) Check RTT graph for the same connection. Put a screenshot.

f) Are there any timeout instances for this connection, if yes, how did you find that out, what is the value of the congestion window at that time? If not, look for instances from other TCP connections that you captured. Can you highlight this from the TCP stream graph?

g) How many fast retransmissions are there? Compute and put a screenshot.

Q2. When you collected the packet trace, at the end of 30 sec use Netstat to validate the numbers you got from the above analysis [2 + 2 + 2]

a) Compute the number of TCP connections, are they matching with the above numbers? Put a screenshot.

b) How many are in Timed-wait state, how many are in established state and how many are in fin-wait-1 state. Put a screenshot.

c) Put your network interface down, could you see any changes of the TCP connections as compared to b)? Put a screenshot.