Lab-5: TCP Congestion Window: Wireshark based
Siri N Shetty – PES2UG22CS556 (Semester 4 Section J)

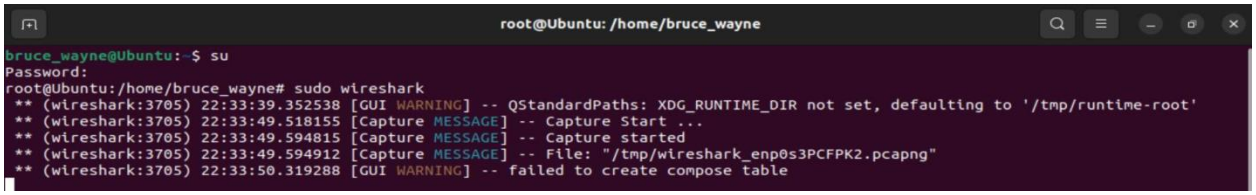
The aim of this experiment is to understand the TCP congestion control mechanisms. When will the Congestion Window grow and when will it shrink? Who dictates the size of the Congestion Window? How does the client and server exchange this information? What causes Fast Retransmit? We will try to understand and answer these questions in this experiment.
We will use Wireshark tool to do the following,

a. Capture TCP traffic and plot the Congestion Windo
b. Use a PCAP and try to analyze the Congestion Window graph.

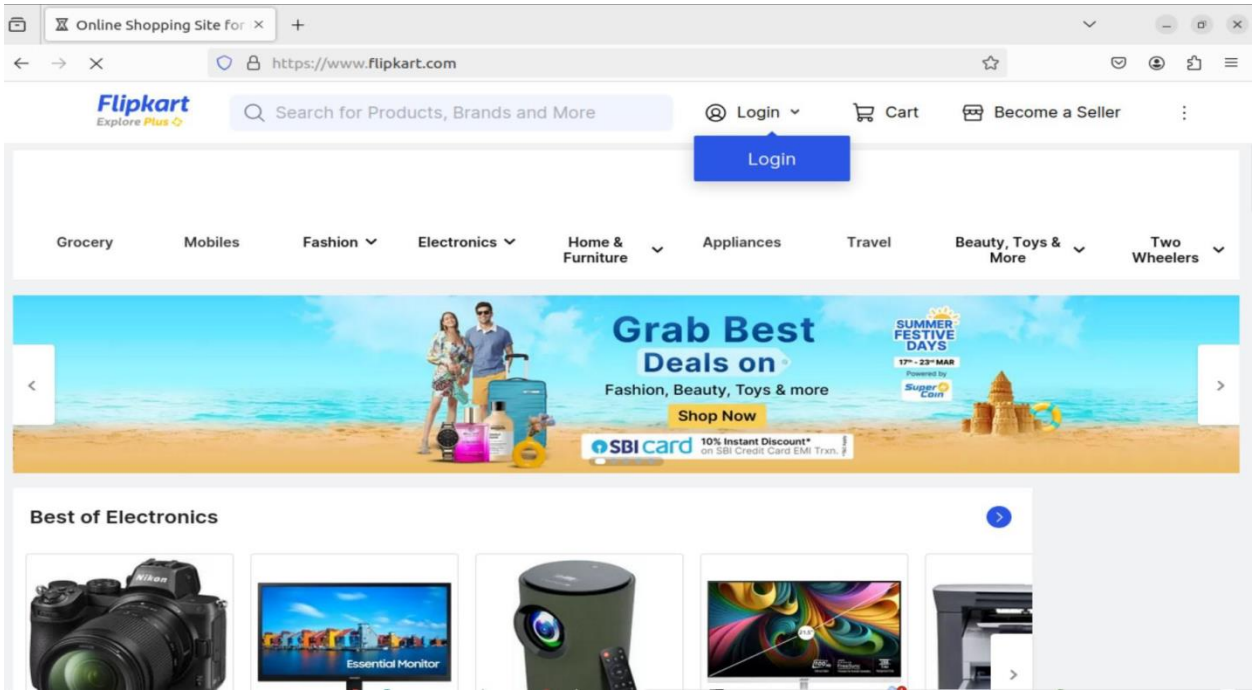
Follow the procedure below.

a. Capture TCP traffic and plot the CW:

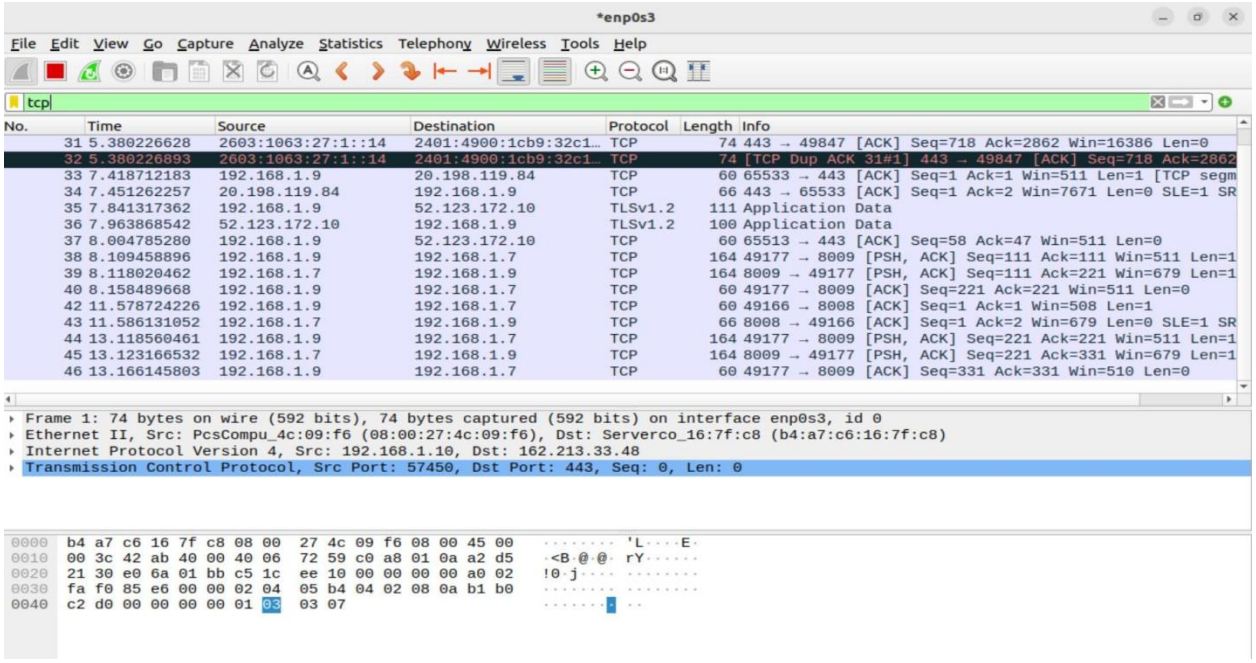
> Open Wireshark in admin/sudo mode.



> Start the Capture on the live interface.
> Open a browser and visit a site of your choice (ex: www.news18.com)



> Apply the TCP filter in Wireshark

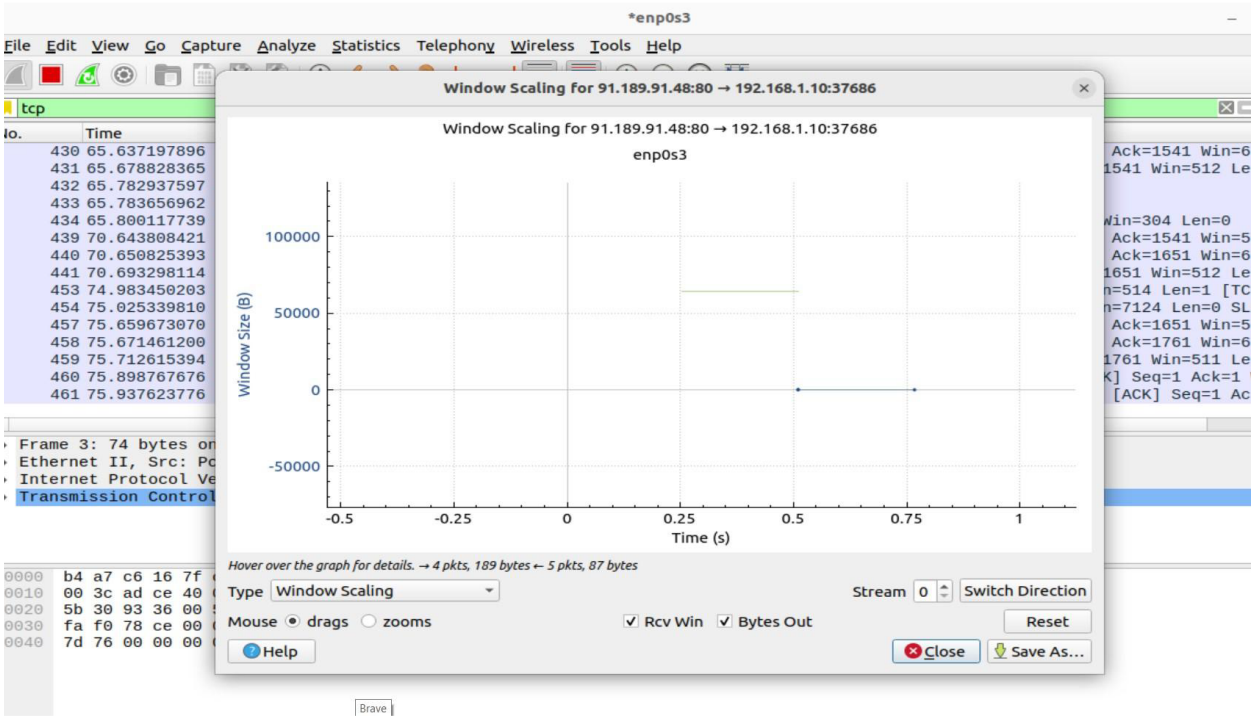


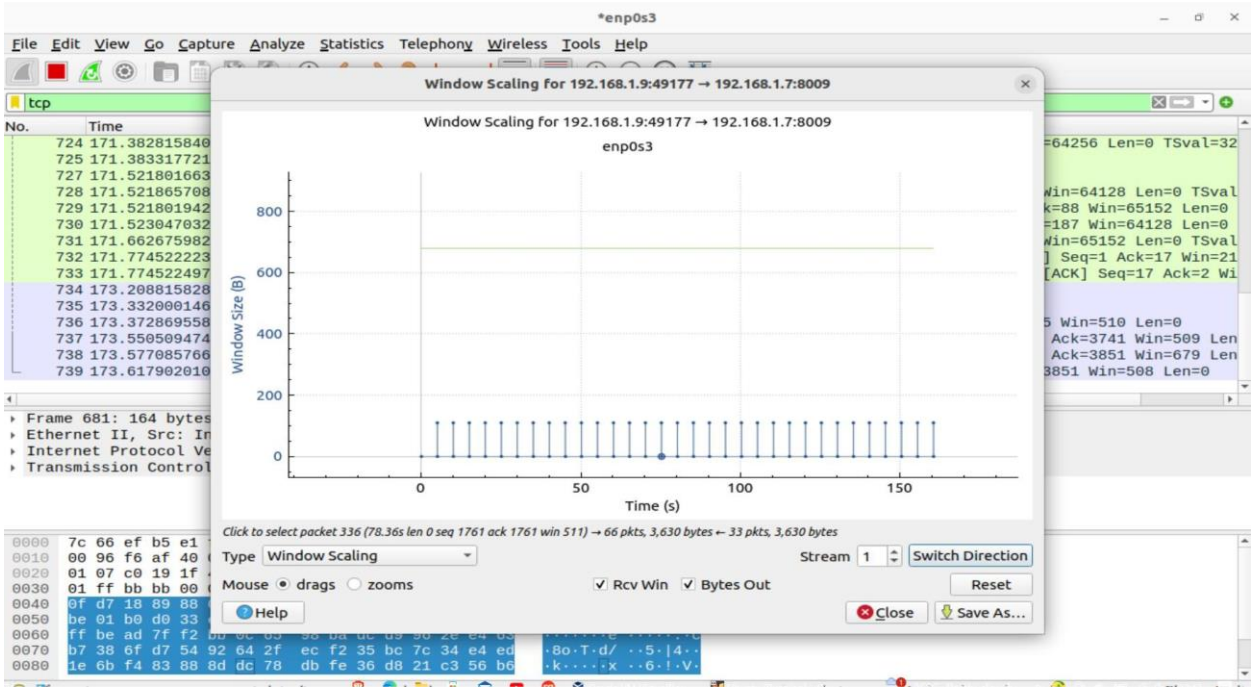
> Choose the very first TCP-SYN packet from your system to the server.

> Plot the Congestion Window:

> Statistics -> TCP Stream Graphs -> Window Scaling

> Look at the Congestion Window and the byte going out and coming in



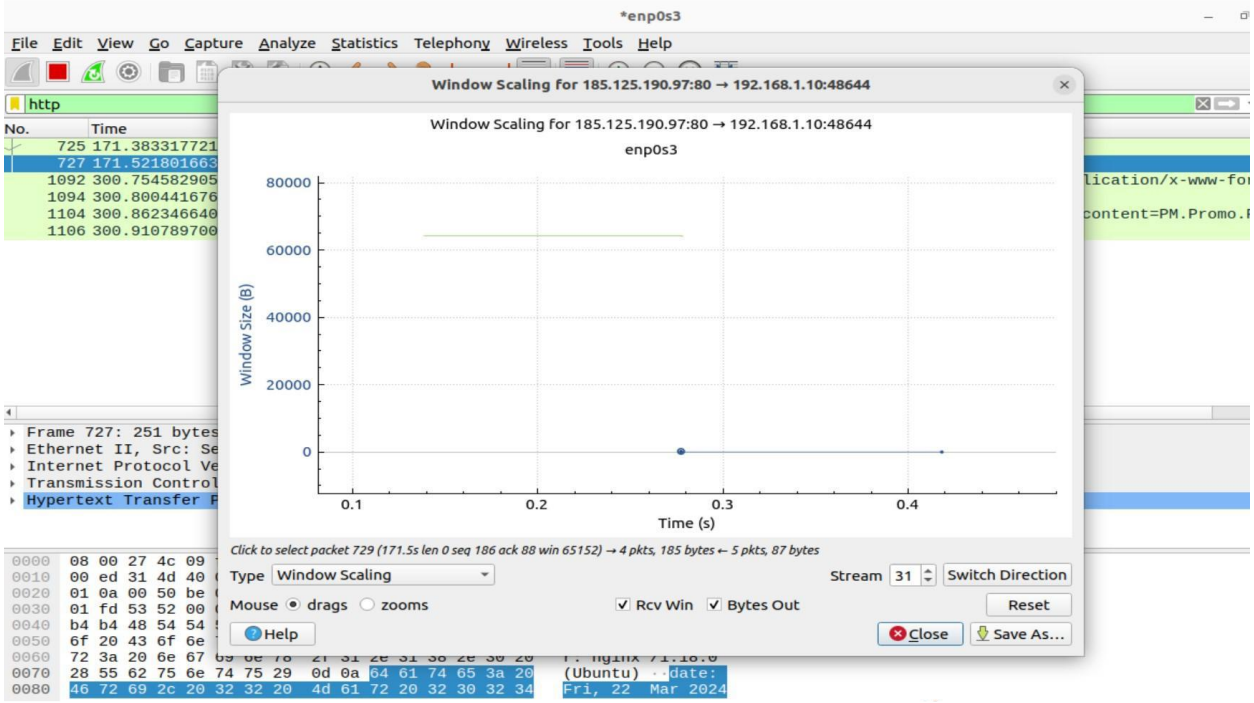


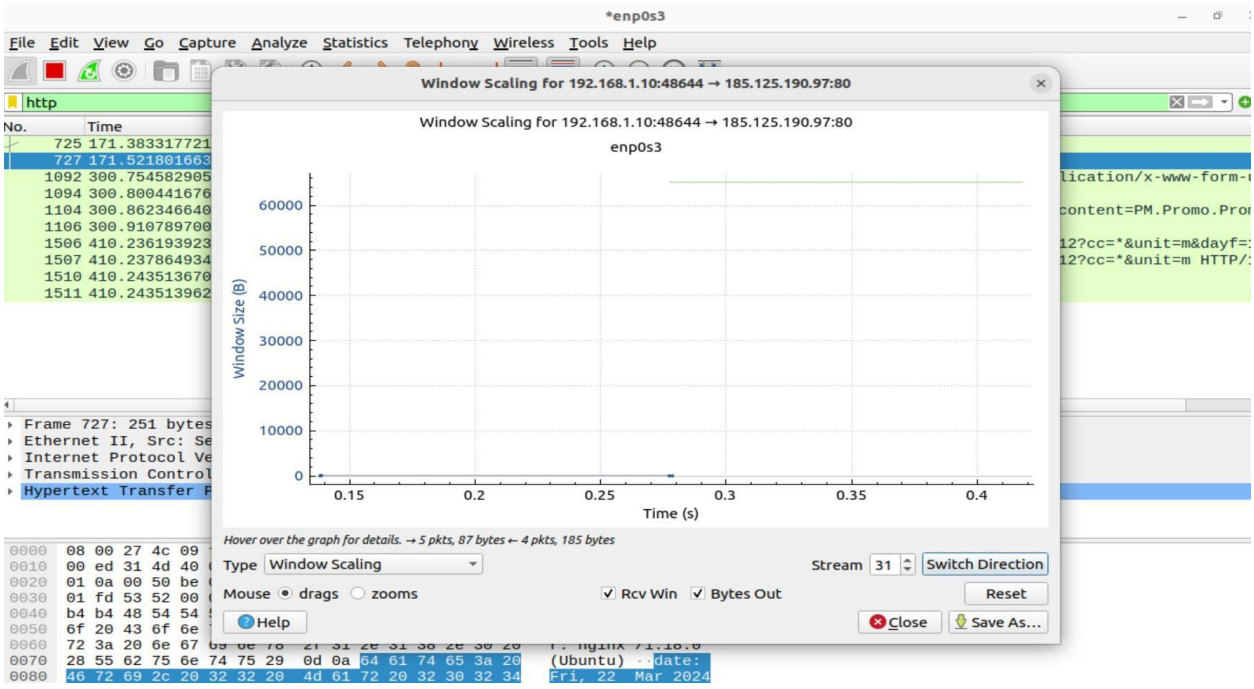
> Now, try to plot the window for multiple other TCP traffic types.

> HTTP(s)

> FTP

> File Downloads etc

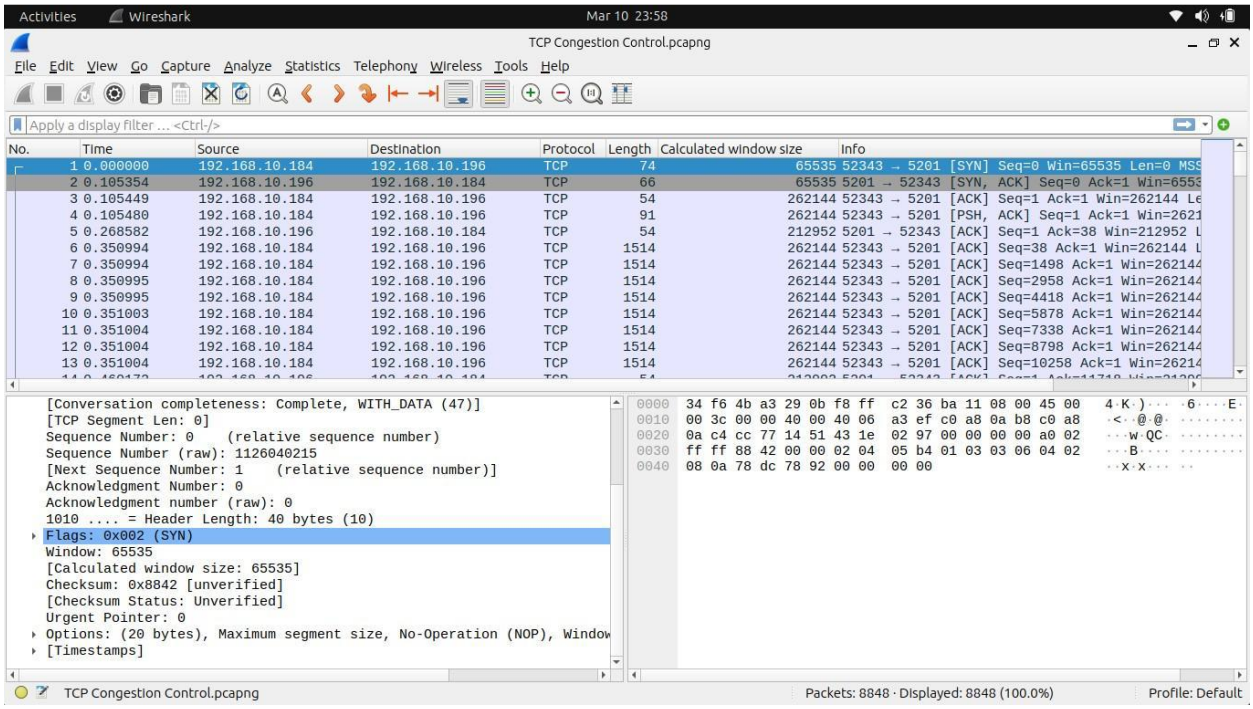




b. Use a PCAP and try to analyze the Congestion Window graph.

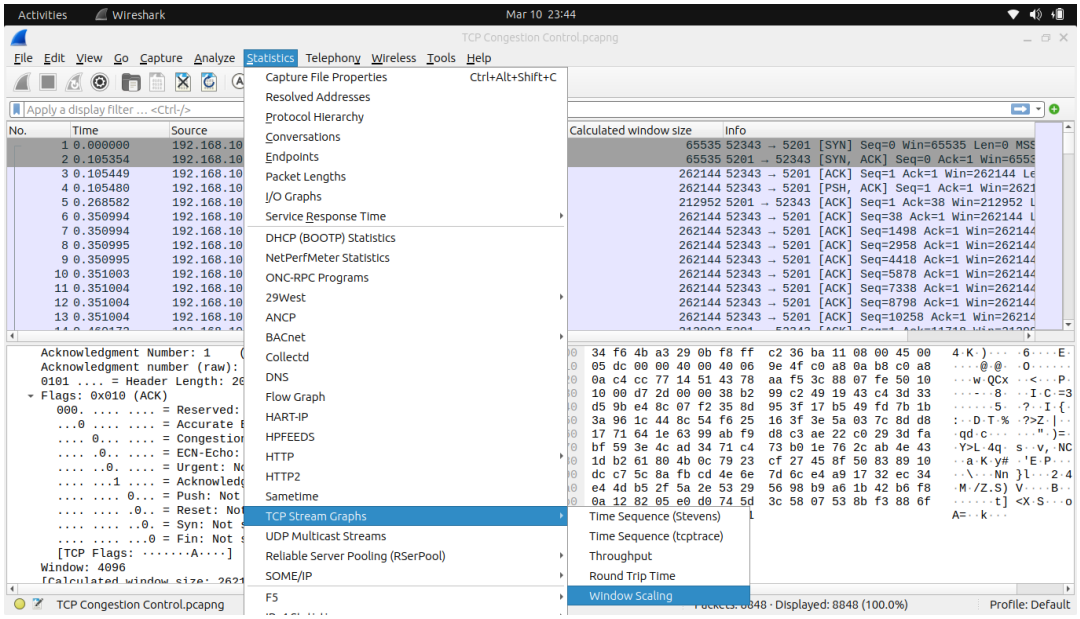
> Use the PCAP provided here to understand the TCP Congestion Control in case of 3 consecutive duplicate packets causing Fast Retransmit. (https://github.com/packetpioneer/youtube/blob/main/TCP%20Congestion%20Control.pcapng)

> Open the PCAP in Wireshark.

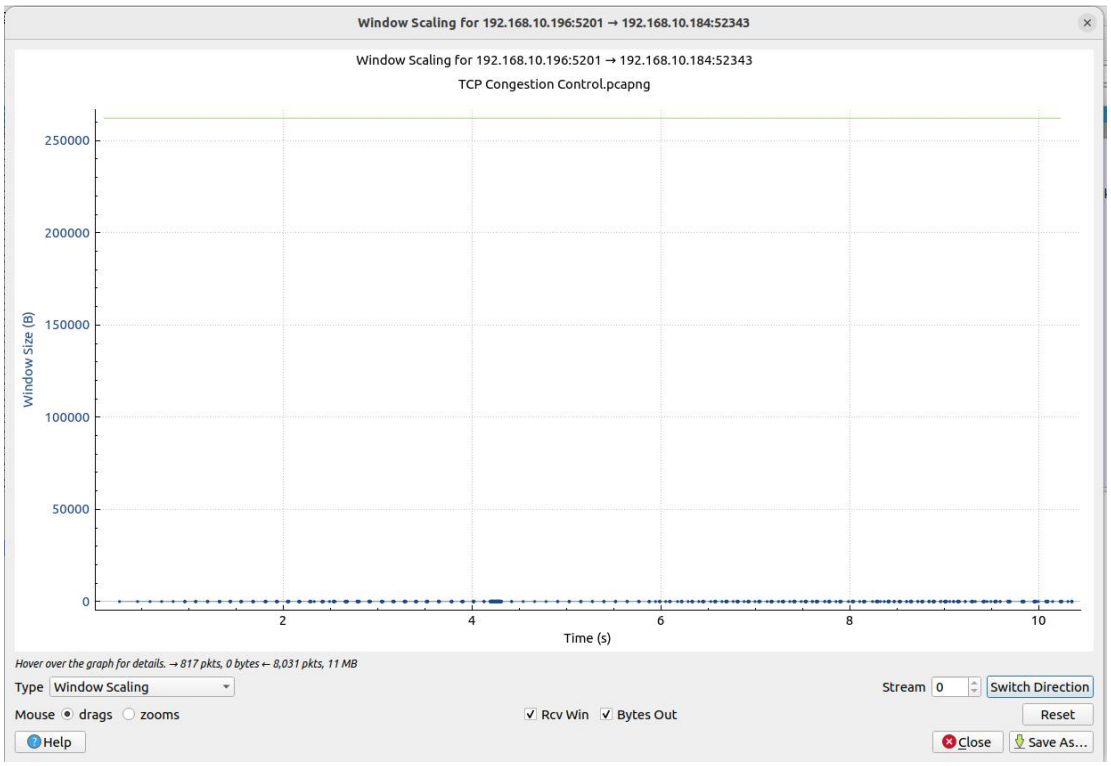


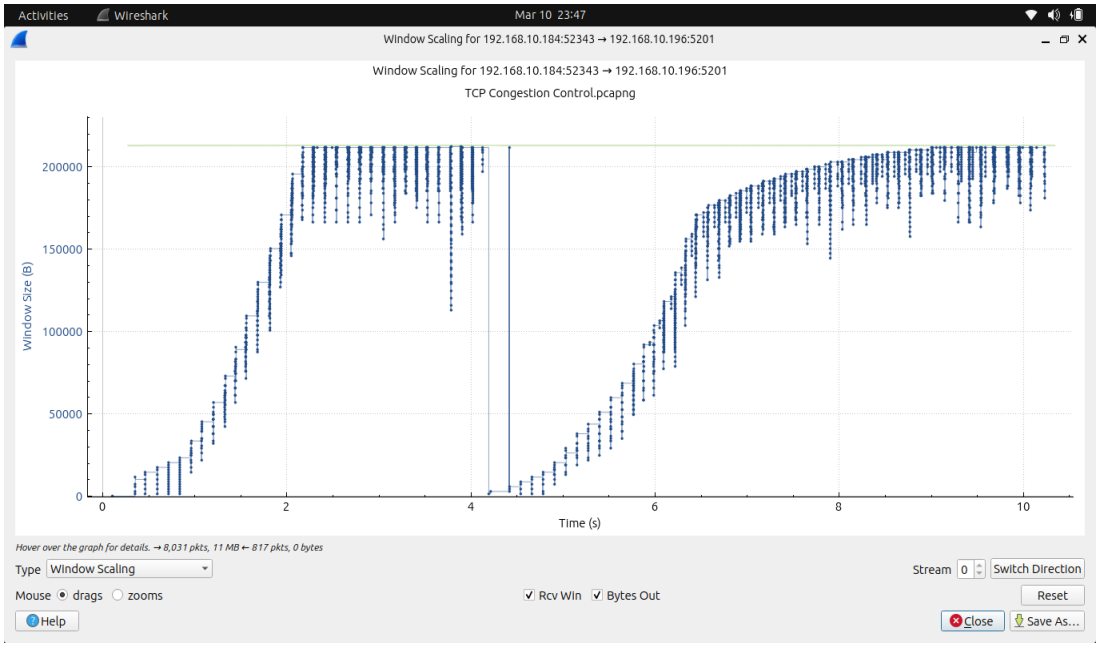
> Plot the Congestion Window through the same option as before

> Statistics -> TCP Stream Graphs -> Window Scaling



> Look at the graph and understand the Congestion Window. Switch the direction.





> Click on the fist dip in the graph to see the reason for it. There are 3 duplicate packets and TCP does Fast Retransmit and also reduces the window size to 1.

> Now, identify the following,

> Slow Start

> Congestion avoidance

> Timeout and other parameters

> TCP flavor in use.

Ref:

> *https://www.youtube.com/watch?v=IRXP1vJ6-vM*

> *https://www.youtube.com/watch?v=2PJVHvthrNU*

> *https://github.com/packetpioneer/youtube/blob/main/TCP%20Congestion%20Control.pcapng*

> *https://share.netresec.com/s/nF5zNcaXLgwdQFZ*

> *https://www.netresec.com/?page=PcapFiles*

> *https://tcpreplay.appneta.com/wiki/captures.html*

Compiled By:
Prof. Vadiraja Acharya
Dept. of CSE,
PESU-RR