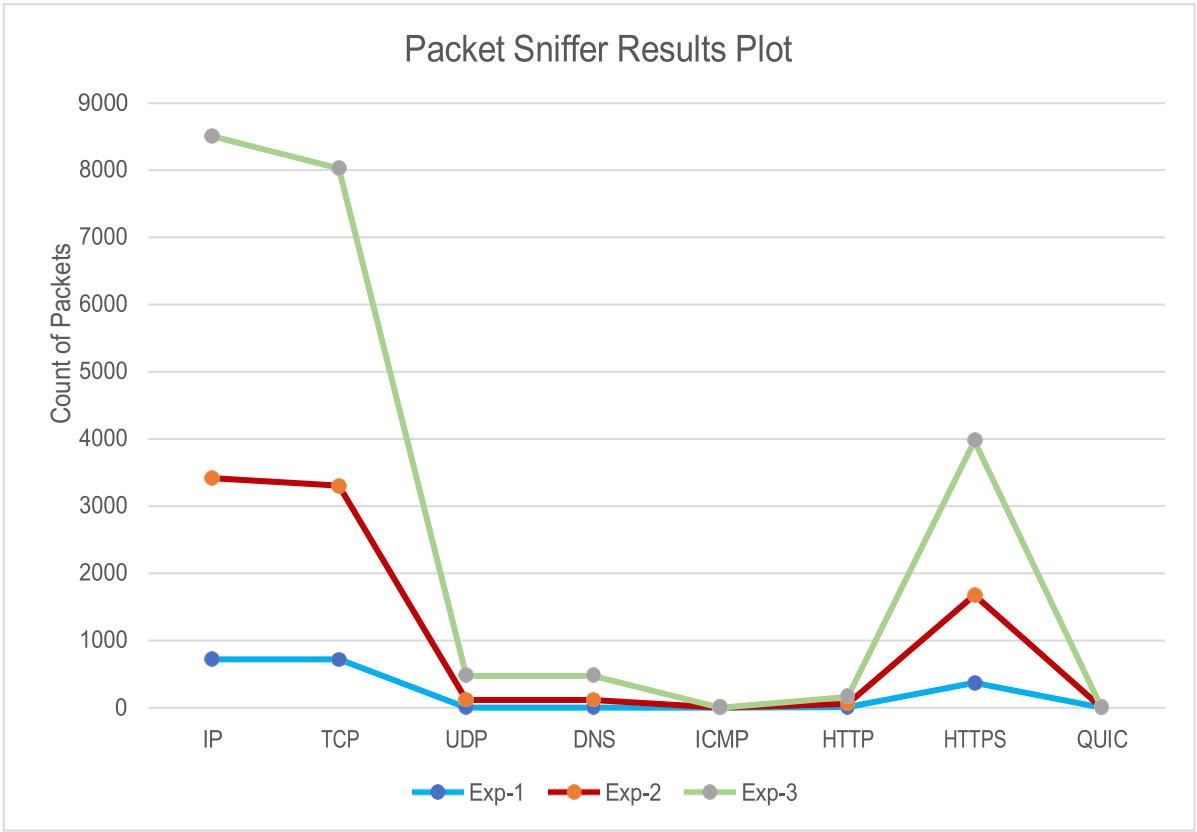
Packet Sniffer Analysis

Plot of packet counts:

Results of three experiments are plotted below.

- x-axis has different protocols for which we are counting packets.
- y-axis has the number of packets.
- Blue → Exp-1, Red → Exp-2, Green → Exp-3, represents the graph line plot.



Analysis:

Exp -1: In this experiment, we played a YouTube video at highest resolution possible (720P) in a browser. Once the video started playing, we ran the packet sniffer tool. After 30 seconds, the results were captured in a .csv file. As a result, we observed IP, TCP, HTTP and HTTPS packet counts. Whereas UDP, DNS, ICMP and QUIC protocols were not involved in the process while running the packet sniffer tool on an already playing video, therefore their count remains zero. DNS and QUIC are UDP based protocols, and since the count of both did not incremented, therefore UDP count also remained un-incremented.

Exp -2: In this experiment, first we ran our packet sniffer tool. Then we opened a browser, opened YouTube and played a random video for 30 seconds until the tool exits. A .csv file is generated with the packet counts. The results show that except ICMP and QUIC, all other protocols (IP, TCP, UDP, DNS, HTTP, HTTPS) were involved in the process with a significant increase in packet count as compared to Exp-1. The observation here is, as the tool was already running and YouTube website query was made, it triggered DNS (a lookup protocol) and in-turn increases the UDP packet count. UDP and TCP count incremented the IP protocol count.

Exp -3: In this experiment, first we ran our packet sniffer tool. Then we opened a browser and randomly opened different websites like Amazon, YouTube, Facebook, Wikipedia, NS-3, etc. until the tool exits after 30 seconds. A .csv file is generated. The results show that except ICMP and QUIC, all other protocols (IP, TCP, UDP, DNS, HTTP, HTTPS) were involved in the process with a significant increase in the packet count as compared to Exp-2 and Exp-1. The observation here is, as the tool was already running, and by making multi-faceted queries, including YouTube video, shopping website, and general google query, it resulted in a good packet capture count.

Note: The ICMP protocol count remained zero throughout all the experiments as it is a ping protocol, and no ping query was involved in any of the experiments.