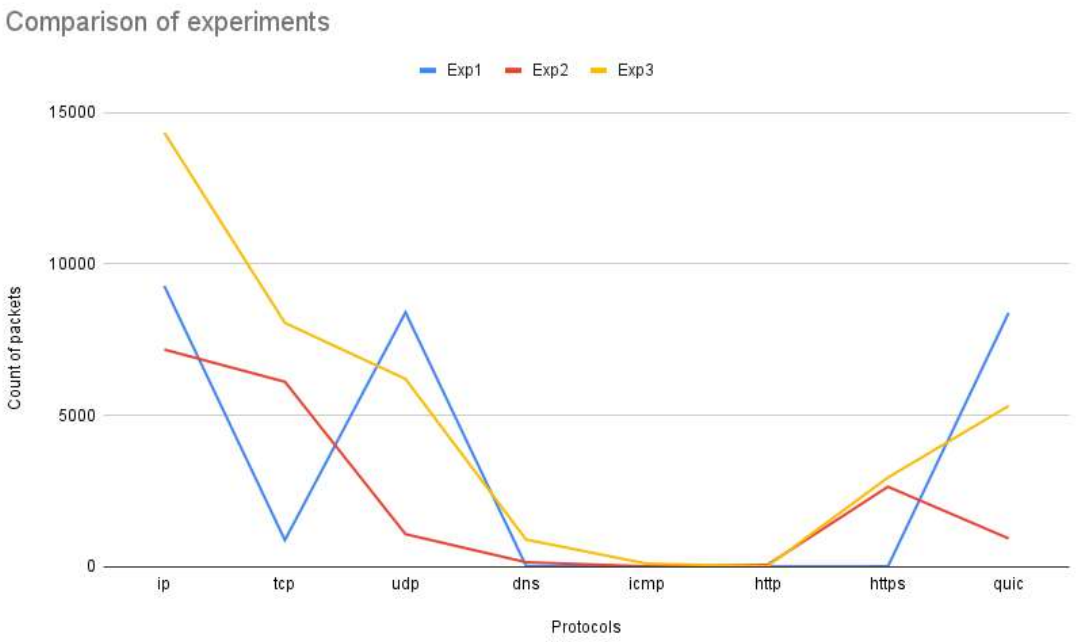
CSC/ECE 573: Homework 3 Report

Team:
Swetha Sairamakrishnan: ssairam
Naveen Jayanna: njayann

Packet Sniffer:

A plot of packet counts:



Analysis:

In experiment 1, we open Youtube and start the video before sampling the outgoing/incoming packet. Hence, the TCP connection was already established before initiating the experiment which resulted in the number of DNS, HTTP, HTTPS, and ICMP packets being negligible. Currently, YouTube uses Google's QUIC protocol when available and switches to TCP as a backup. Hence, about 85% of the total packets (IPv4) received were using QUIC (UDP) and the rest were TCP.

In experiment 2, as we establish a TCP connection with Youtube after the sampling begins, we see a relatively higher number of packets for HTTPS, DNS, and HTTP compared to the previous experiment. Further, as we are playing a YouTube video, a large number of IPv4 packets received were QUIC(UDP) while the rest remains to be TCP.

In experiment 3, we open Google and make some random searches and access multiple links across websites. Hence, we make HTTPS/HTTP (TCP) connections with multiple websites resulting in a large number of HTTPS, DNS, and ICMP packets, and the rest of the IPv4 packets received are related to the links which were opened.