# Wireshark Network Analysis Report

Here is a summary of what I found after capturing and analyzing the network traffic for the lab. This analysis is based on the Protocol Hierarchy statistics from my capture file.

## 1. Most Active Protocols

When I looked at the stats, it was clear that almost all the traffic (**98.7%**) was **Internet Protocol Version 4 (IPv4)**.

Inside IPv4, the traffic was split between two main protocols:

- **User Datagram Protocol (UDP): 74.5%**
    - This was the most active protocol by far.
    - The main reason for this was the **QUIC IETF protocol (43.2%)**, which I learned is used by Google and other big sites.
    - A lot of "Data" packets (28.4%) also showed up, which I assume is the encrypted info being sent inside those QUIC packets.
    - Regular **DNS** (1.3%) and **Multicast DNS** (1.4%) queries made up a small, expected part of the traffic.
- **Transmission Control Protocol (TCP): 23.9%**
    - This was the second busiest protocol.
    - Almost all the TCP traffic was **Transport Layer Security (TLS) (8.2%)**. This is the encrypted HTTPS traffic from when I visited the secure websites for the assignment.

Other important protocols like **Address Resolution Protocol (ARP) (1.1%)** (for devices to find each other) and **Internet Control Message Protocol (ICMP) (0.2%)** (from my `ping` command) were there but didn't make up much of the total traffic.

## 2. Suspicious or Unusual Traffic

**I didn't find any suspicious or malicious traffic** during my analysis. Everything I saw seemed directly related to the tasks I was performing (browsing websites and running a `ping`).

One thing I thought was unusual at first was seeing so much UDP (74.5%) instead of TCP (23.9%), since I thought TCP was used for most web browsing. But I found out this isn't suspicious. It's because of all the **QUIC** traffic (43.2%), which is a newer protocol that uses UDP to make websites load faster.

## 3. Key Insights about Network Communication

This capture showed me a few key things about how my network communicates:

1. **The Web is Shifting to UDP:** The biggest thing I learned is that a lot of web traffic doesn't use TCP anymore. The high amount of QUIC traffic shows that the industry is using UDP to make things faster.
2. **Encryption is Standard:** I barely saw any packets with the `http` filter, but I saw a lot of **TLS** traffic. This confirms that pretty much all websites use secure, encrypted (HTTPS) connections now, which keeps data safe.
3. **Background "Chatter" is Essential:** Protocols like **DNS** (to find a website's IP), **ARP** (for my computer to find other devices), and **ICMP** (for my `ping` test) are critical. They don't create a lot of packets, but the network can't work without them.