Findings Report

1. Protocol Summary

From the Wireshark *Protocol Hierarchy Statistics*, the following protocols were identified:

Protocol	Packets	Percent	Description
Ethernet II	286,840	100%	Data link layer protocol used for all network communication.
IPv4	286,840	100%	Network layer protocol carrying most traffic.
TCP	286,840	100%	Primary transport layer protocol used for reliable communication.
TLS (HTTPS)	435	0.2%	Encrypted web traffic on port 443.

Observation:

- The traffic is **dominated by TCP**, showing most communication is over reliable, connection-based sessions.
- A small percentage (0.2%) of **TLS (HTTPS)** packets were detected, indicating limited secure web traffic during the capture.

2. Most Active Protocols

The most active protocols in the capture were:

- **TCP** – carrying most of the data (over 46% of bytes).
- **IPv4** – used for addressing and routing across the network.
- **Ethernet II** – standard framing at the data link layer.

These indicate standard browsing and application communication patterns.

3. Suspicious or Unusual Traffic

No abnormal traffic detected.
All packets appear consistent with normal operations such as:

- ➢ HTTP/HTTPS web browsing
- ➢ ICMP ping traffic
- ➢ DNS lookups

There were no signs of port scans, broadcast floods, or malformed packets.

4. Key Insights

- ➢ TCP remains the backbone protocol for most communication.
- ➢ DNS queries always precede HTTP/HTTPS requests.
- ➢ The low percentage of TLS traffic suggests some sites accessed were still using HTTP.
- ➢ Network activity appeared typical of a user browsing and pinging known hosts (e.g., 8.8.8.8).