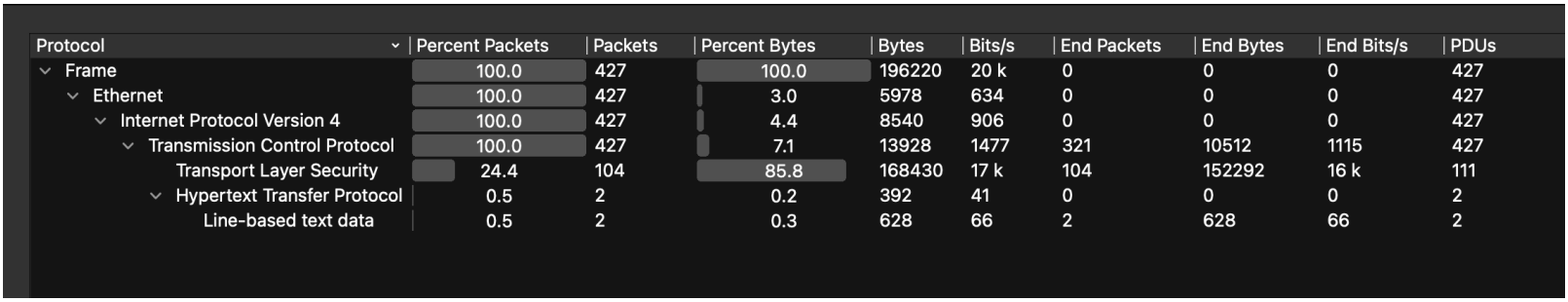
Findings Report

1. Protocol Summary

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



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	427	100.0	196220	20 k	0	0	0	427
Ethernet	100.0	427	3.0	5978	634	0	0	0	427
Internet Protocol Version 4	100.0	427	4.4	8540	906	0	0	0	427
Transmission Control Protocol	100.0	427	7.1	13928	1477	321	10512	1115	427
Transport Layer Security	24.4	104	85.8	168430	17 k	104	152292	16 k	111
Hypertext Transfer Protocol	0.5	2	0.2	392	41	0	0	0	2
Line-based text data	0.5	2	0.3	628	66	2	628	66	2

Observation:

- The traffic is **dominated by TCP**, showing most communication is over reliable, connection-based sessions.
- A small percentage (0.5%) 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 (85.8% 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).