Computer Networks Lab Report

Topic: Network Traffic Capture and Protocol Analysis using Wireshark
Date: October 17, 2025
File Analyzed: `task-1.pcapng`

1. Objective

The goal of this task was to analyze captured network traffic using Wireshark, identify active network protocols, observe packet size distribution, and interpret communication patterns using protocol hierarchy and I/O graphs.

2. Summary of Capture

- **Total Packets Captured:** 1608
- **Displayed/Filtered Packets:** 458 (based on source IP filter and TCP ports 80/443)
- **Duration:** ~70 seconds
- **Capture Source:** Wi-Fi interface (system IP: 10.21.17.119)

3. Protocol Analysis

From the **Protocol Hierarchy Statistics** (see screenshot `task-5-protocol-hierarchy.png`):

Protocol	Percent Packets	Percent Bytes	Description
Ethernet	100%	100%	Data link layer encapsulation
IPv4	100%	11.5%	Network layer for routing packets
TCP	100%	80.4%	Transport layer (connection-oriented communication)
TLS	25.1%	57.9%	Encrypted HTTPS sessions

Protocol	Percent Packets	Percent Bytes	Description
HTTP	1.5%	2.4%	Unencrypted web traffic
Data (payload)	0.7%	0.1%	Miscellaneous payload packets

Observation:
The majority of the packets belong to **TCP** and **TLS**, indicating encrypted HTTPS communication. A small fraction of **HTTP** packets suggests initial handshakes or non-secure requests. The presence of **ICMP** and **DNS** packets was minimal in this filtered dataset, as the filter primarily focused on web traffic.

4. Packet Length Distribution

From the **Packet Length Statistics** (see screenshot `task-5-packet-length.png`):

Range (bytes)	Count	Percent
40–79	790	49.13%
80–159	456	28.36%
160–319	100	6.22%
1280–2559	157	9.76%
2560–5119	1	0.06%

Insights:

- Most packets are **small (40–159 bytes)**, likely TCP acknowledgments or control packets.
- Larger packets (1280–2559 bytes) represent **data transfer segments** during HTTPS communication.
- The single large packet (2641 bytes) likely corresponds to a **TLS record or data burst**.

5. I/O Graph Analysis

From the **I/O Graph** (see screenshot `task-5-io-graph.png`):

- **Traffic pattern:** Bursty, with high activity spikes around **10s, 15s, and 65s**.
- **Peak rate:** ~160 packets/sec.
- **Overall rate:** ~0.022 packets/ms (22 packets/sec average).
- **Interpretation:** These spikes correspond to web page loads or TLS session establishment, typical of browsing behavior.

6. Key Insights

- The capture shows **typical HTTPS traffic behavior**, dominated by **TLS-encrypted packets** over **TCP**.
- **No suspicious or abnormal traffic** (e.g., excessive ICMP or non-standard ports) was detected.
- The **burst transmission** pattern aligns with standard HTTP/TLS sessions initiated by visiting websites.
- Small packets (ACKs, control frames) dominate in count, while large packets dominate in byte volume — a characteristic of efficient TCP data flow.

7. Conclusion

The network traffic captured and analyzed reflects normal web browsing activity involving encrypted HTTPS communication. Wireshark successfully revealed the distribution of protocols, packet sizes, and transmission patterns. The analysis confirms stable, non-anomalous traffic behavior consistent with regular user browsing and data exchange over secure channels.

Attachments:

- `filteredpackets.pcap`
- `task-5-packet-length.png`
- `task-5-protocol-hierarchy.png`
- `task-5-io-graph.png`