Wireshark Network Traffic Analysis Report

# 1. Capture Details

|  |  |
| --- | --- |
| Interface | wlan0 |
| Capture Duration | 1 minute |
| File Name | network\_traffic\_analysis.pcap |

# 2. Protocols Identified

|  |  |  |
| --- | --- | --- |
| Protocol | Description | Notes |
| DNS | Domain lookups | Requests to google.com, cloudflare.com |
| HTTP | Web browsing | Unencrypted traffic captured |
| TCP | Transport Layer | Base layer for other protocols |

# 3. Observations

* HTTP traffic is visible in plain text.
* DNS requests reveal visited domain names.
* TCP sessions were established normally.
* HTTPS sessions appeared as encrypted TLS traffic.
* No suspicious or malformed packets observed.

# 4. Conclusion

Wireshark successfully captured real-time traffic across multiple protocols. The capture reveals how various common protocols like DNS, HTTP, and TCP operate in a live network. Such analysis is critical for understanding normal vs. malicious traffic patterns.