# Capture and Analyze Network Traffic using Wireshark

**Date captured:** 2nd June 2025

**Network Interface used:** WiFi

**Duration of capture:** 00:01:04 (1min 4sec)

**Number of packets captured:** 6693

## Identified Protocols

1. **Domain Name System (DNS)**

* Usage: Resolves domain names to IP addresses.
* Example: Query to [www.google.com](http://www.google.com)

1. **Transmission Control Protocol (TCP)**

* Usage: Ensures reliable transmission of data
* Example: TCP handshake observed between local device and server (SYN, SYN-ACK, ACK)

1. **Transport Layer Security (TLS)**

* Usage: Encrypted communication (HTTPS)
* Example: Encrypted request to [www.google.com](http://www.google.com)

## Protocol Distribution:

|  |  |  |
| --- | --- | --- |
| **Protocol** | **Packet Count** | **Percentage (%)** |
| Ethernet | 6693 | 100 |
| IPv4 | 6623 | 99.0 |
| IPv6 | 15 | 0.2 |
| TCP | 6369 | 95.2 |
| UDP | 228 | 3.4 |
| TLS | 2411 | 36.0 |
| DNS | 212 | 3.2 |
| ICMP | 27 | ~0.4 |
| SSDP | 4 | 0.1 |
| Apache JServ Protocol v1.3 | 1 | ~0.0 |
| IGMP | 3 | ~0.0 |
| ARP | 55 | 0.8 |

## Key Observations:

* TLS traffic indicates encrypted sessions, possibly HTTPS.
* High TCP usage (95.2%) suggests reliable, connection-oriented communication.
* DNS traffic (3.2%) represents name resolution activity.
* UDP traffic (3.4%) likely includes DNS, SSDP, and mDNS.
* Minimal use of ICMP, ARP, and IGMP which are used for diagnostics and network operations.
* Only 1 packet using Apache JServ Protocol v1.3, indicating potential interaction with a specific Java-based web service.
* Very limited IPv6 usage (0.2%) indicates the network primarily uses IPv4.

## Conclusion:

The capture shows **normal, secure web usage behavior**, dominated by TLS-encrypted sessions. DNS queries and standard background protocols were also present. The analysis confirmed a secure and active internet session without visible signs of unencrypted web browsing or anomalies.