Network Packet Analysis Report

Captured Protocols:

- **DNS (Domain Name System)** – Handles domain resolution.
- **TCP (Transmission Control Protocol)** – Manages reliable communication between client and server.
- **HTTP (Hypertext Transfer Protocol, port 80)** – Handles web browsing and data requests.

1. DNS Analysis

Overview:

- DNS packets reveal **queries and responses** for domain name resolutions. Your device requested IP addresses for multiple services.

  Key Findings:

  ✅ **Queried Domains:**

  1) googleusercontent.com
  2) ssl.gstatic.com

  ✅ **Successful Responses:** Most queries received valid IP mappings.

  ⚠️ **Potential Repeated Queries:** If multiple lookups for the same domain occurred, this may indicate connectivity or latency issues.

2. TCP Analysis

Overview:

- TCP packets display **connection establishment, data transfer, and session termination** between your local device and remote servers.

  Key Observations:

  ✅ **Connection Handshake Detected:**

  - SYN (Start connection)
  - SYN-ACK (Server response)
  - ACK (Final confirmation)

  ✅ **Data Exchange:** TCP packets confirm reliable communication between endpoints.

3. HTTP (Port 80) Analysis

Overview:

HTTP packets show **unsecured web browsing** interactions between your device and external servers.

Key Findings:

✅ **Request-Response Communication:**

- Your device sent HTTP requests to servers.
- The responses contained website data (HTML, images, etc.).
-

✅ **Traffic on Port 80:** This confirms unencrypted HTTP communication rather than HTTPS (port 443).

⚠️ **No Encryption:** Since this traffic isn't secured via TLS/SSL, data could be intercepted if transferred over an untrusted network.

Performance Insights:

📌 Latency Metrics: TCP timestamps reveal round-trip times impacting network speed.

📌 Packet Loss Indicators: If retransmissions appear in TCP, they may signal network instability.

📌 Encryption Consideration: While TLS packets were seen, HTTP traffic over port 80 wasn't secured.

✅ **DNS shows domain resolution success**
✅ **TCP confirms active data exchanges**
✅ **HTTP traffic exists, but without encryption**