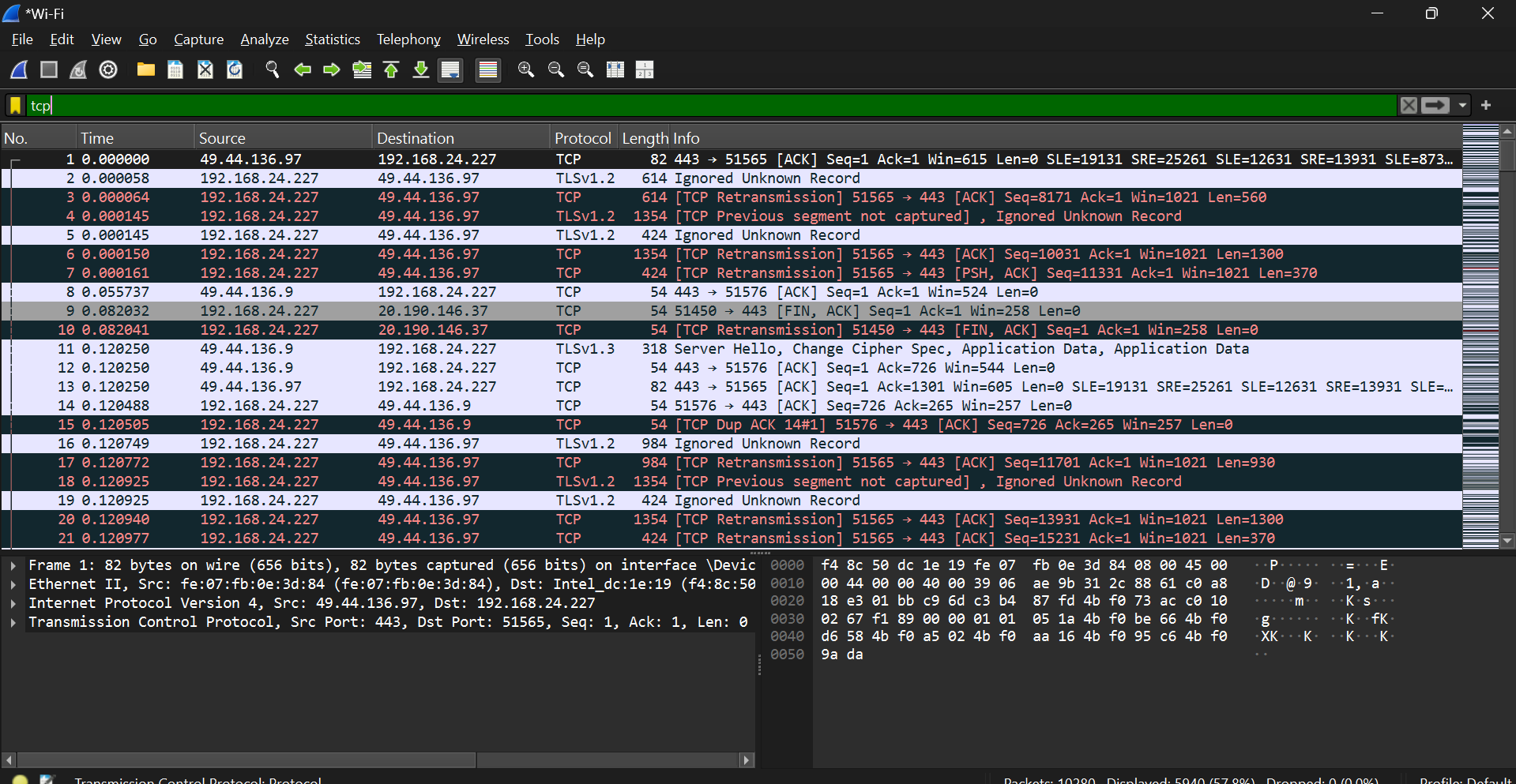
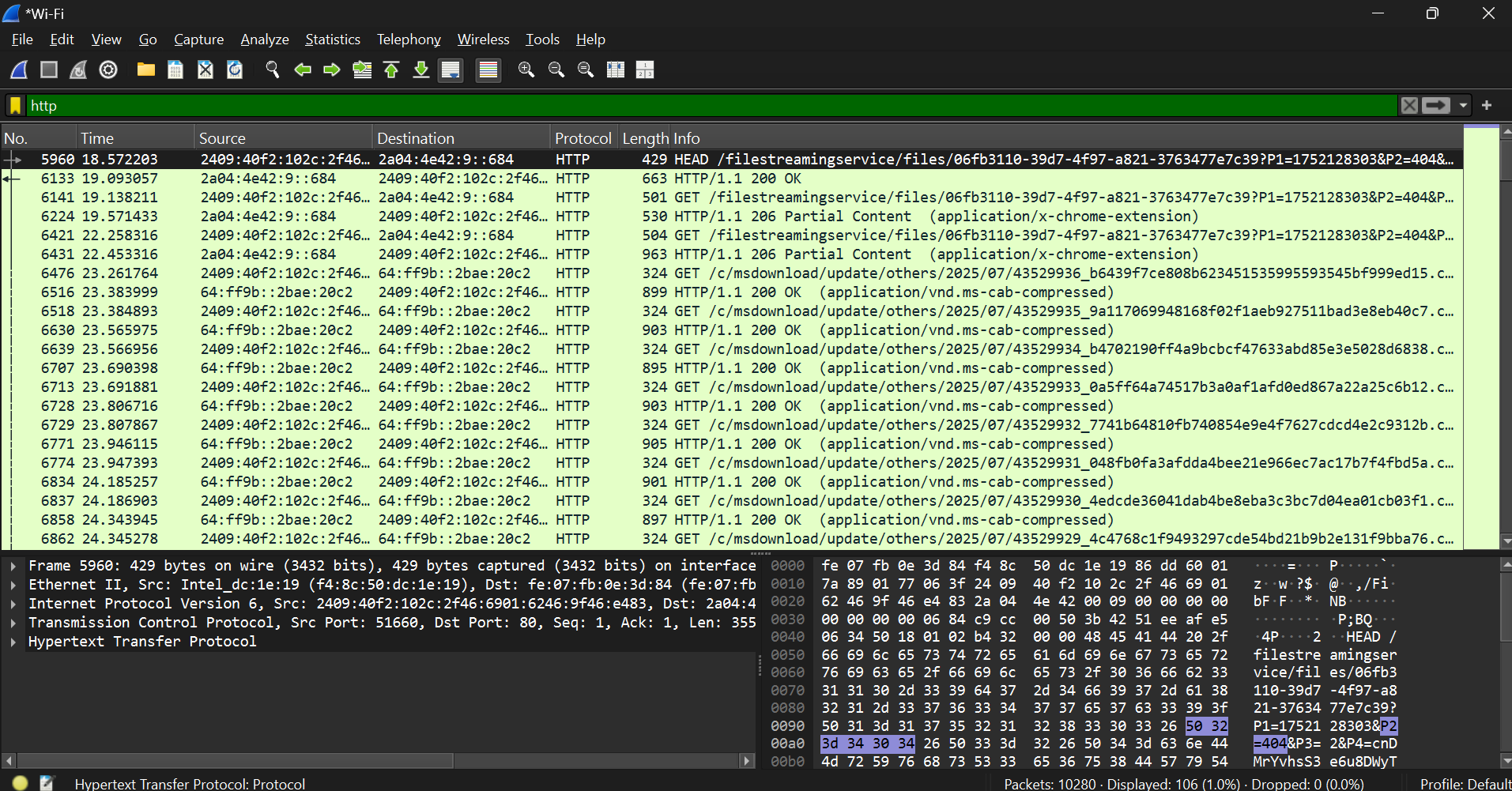
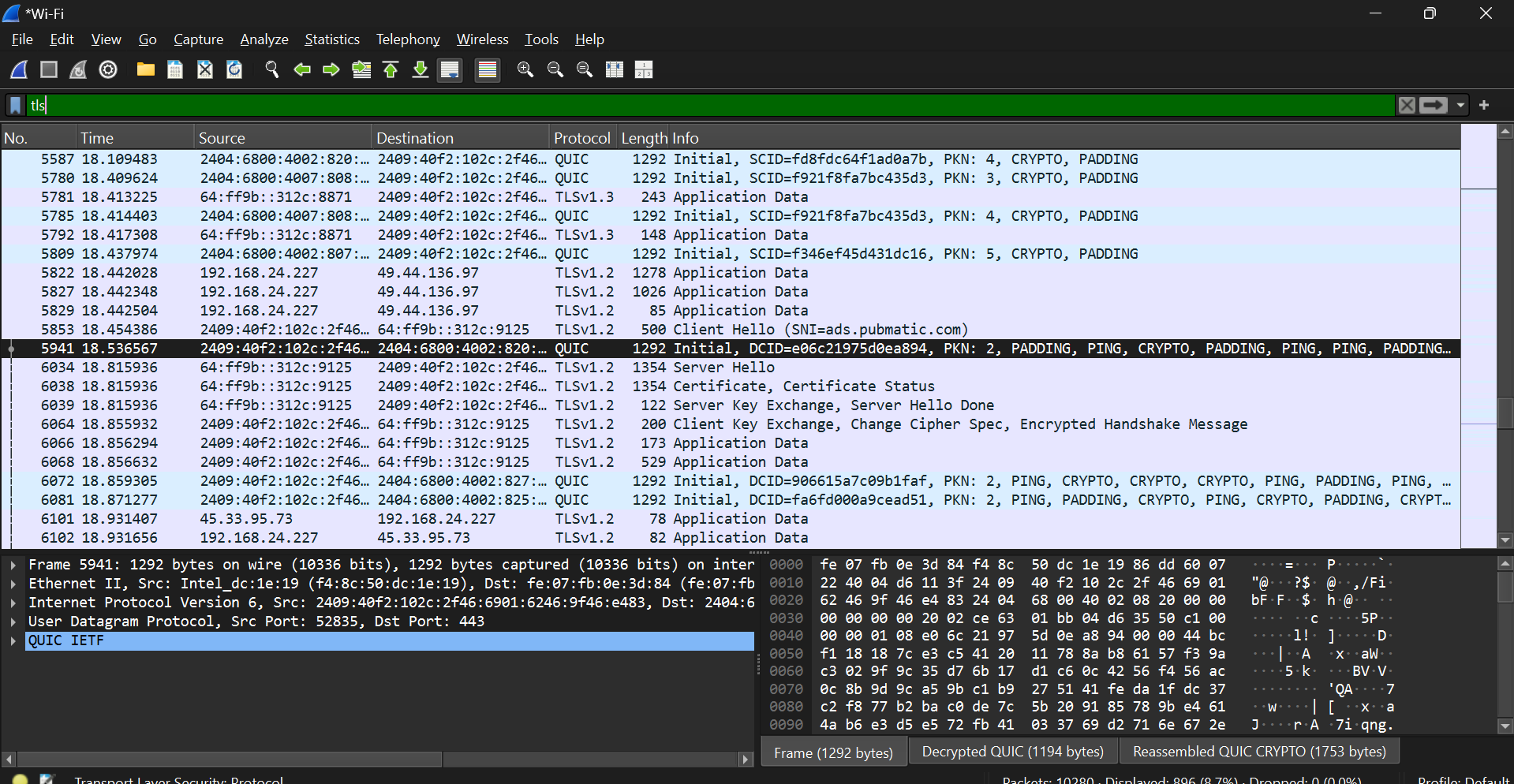
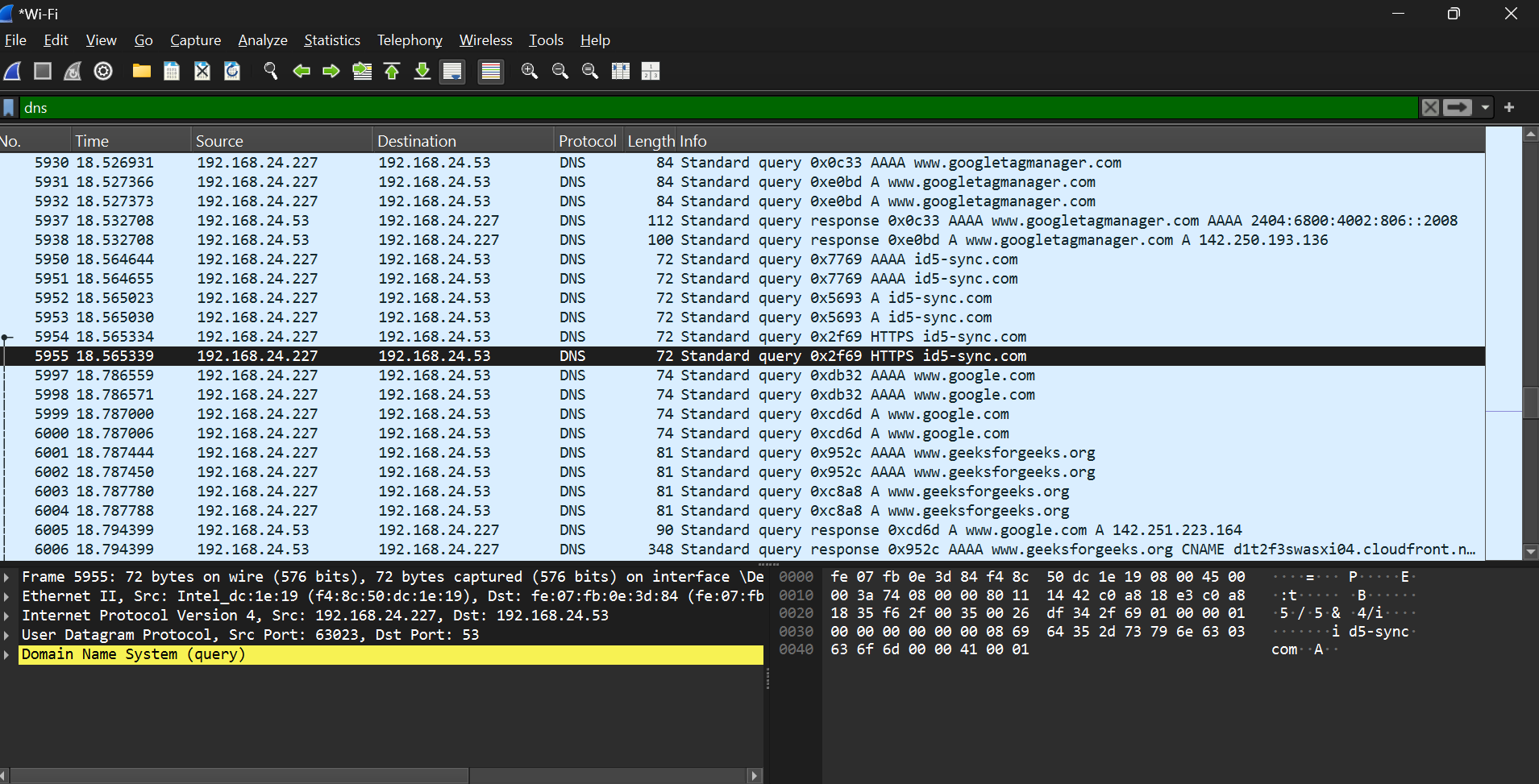
**Capture and Analyze Network Traffic using Wireshark**

Analyzing traffic of WIFI network









**Report of Protocals identified:**

| **Protocol** | **Approx. Count** | **Purpose** |
| --- | --- | --- |
| **TCP** | ~100+ | Transport layer for DNS, HTTP, TLS |
| **DNS** | ~20–30 | Domain name resolution |
| **HTTP** | ~10–50 | Unencrypted web traffic |
| **TLS** | ~30–60 | Secure HTTPS connections |

**Security Observations**

**1. HTTP**

* Plaintext communication detected
* Enforce HTTPS and disable HTTP

**2. DNS**

* DNS queries in plaintext
* Use **DNS over HTTPS (DoH)** or **DNS over TLS (DoT)** for privacy

**3. TLS**

* TLS 1.2/1.3 detected — good

**4. TCP**

* 3-way handshakes and normal data flow observed

**Recommended Actions**

* Migrate all HTTP services to **HTTPS** with valid certificates
* Implement **encrypted DNS** options to prevent MITM or DNS spoofing
* Monitor for unexpected external connections or IPs
* Review TLS configurations for only strong ciphers and protocols
* Re-analyze .pcapng after mitigation to verify results