Wireshark Network Traffic Analysis

Title: Wireshark Network Traffic Analysis — Ankit Jaiswal

Objective: Capture and analyze DNS, HTTP and ARP traffic to understand host resolution, web requests, and local network mapping.

Environment: Laptop (windows), Wireshark (with Npcap). Local network 192.168.56.1.

Steps Taken:

1. Started capture on interface `Wi-Fi` for ~5 minutes.
2. Generated traffic: visited `www.iana.org`, pinged router 10.10.223.254, ran a local HTTP server.
3. Applied display filters for `dns`, `http`, `arp` and inspected packets.

Observations:

- **DNS:** `www.iana.org`→ Standard query and response. Answer section returned IP `192.0.33.8` (See screenshot 01_dns_query.png)
- **HTTP:** Observed HTTP GET and 200 OK response from test server. Headers include `Host`, `User-Agent`, and `Content-Length`. (See screenshot 02_http_get_follow_stream.png)
- **ARP:** ARP request: `Who has 192.168.56.1? Tell 10.10.223.254` and ARP reply with MAC `a6:0a:ec:6f:e3:91`. (See screenshot 03_arp_request_reply.png)

Conclusion / Security Notes:

- DNS queries reveal the domains visited (clear text) and resolve to IP addresses — useful to observe for privacy concerns.
- Most modern web traffic is encrypted (HTTPS) — we can still observe TLS handshake and SNI.
- ARP traffic is local and unauthenticated — ARP spoofing is a possible local attack vector (mitigate with static ARP or network security controls).