**TITLE**

**Wireshark Network Traffic Analysis Report**

**Objective**

To capture live network traffic and identify at least three different network protocols using Wireshark.

**Step 1: Setup and Traffic Generation**

1. Installed Wireshark on Windows.
2. Selected the active network interface (Wi-Fi).
3. Started the capture.
4. Generated traffic by:
   * Visiting websites
   * Running the command ping google.com
   * Using the Spotify app
5. Let the capture run for about 1 minute and then stopped it.

**Step 2: Protocol Identification**

After applying filters like tcp, tls, and mdns, several protocols were identified:

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

* **Description:** Reliable, connection-based transport protocol.
* **Observation:** Seen in packets with SYN, ACK, and Keep-Alive flags.
* **Use Case:** Web traffic, Spotify app communication.

**2. TLSv1.2 (Transport Layer Security)**

* **Description:** Provides encrypted communication over HTTPS.
* **Observation:** TLS handshake packets such as Server Hello and Change Cipher Spec.
* **Use Case:** Secure web browsing, app security.

**3. MDNS (Multicast DNS)**

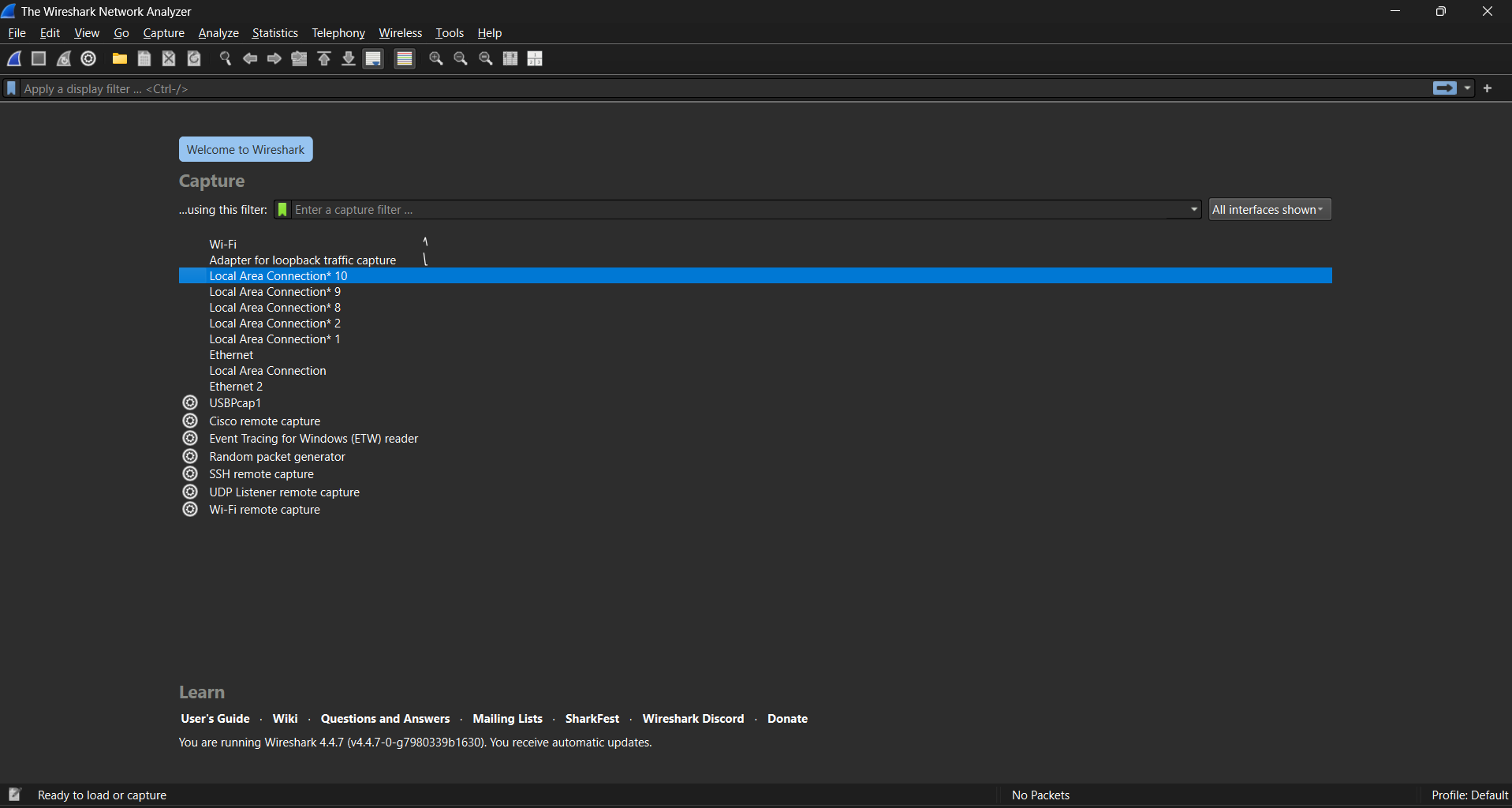
* **Description:** Resolves hostnames to IP addresses within local networks.
* **Observation:** Queries for services like \_Spotify-connect.\_tcp.local.
* **Use Case:** Spotify device discovery on the same network.

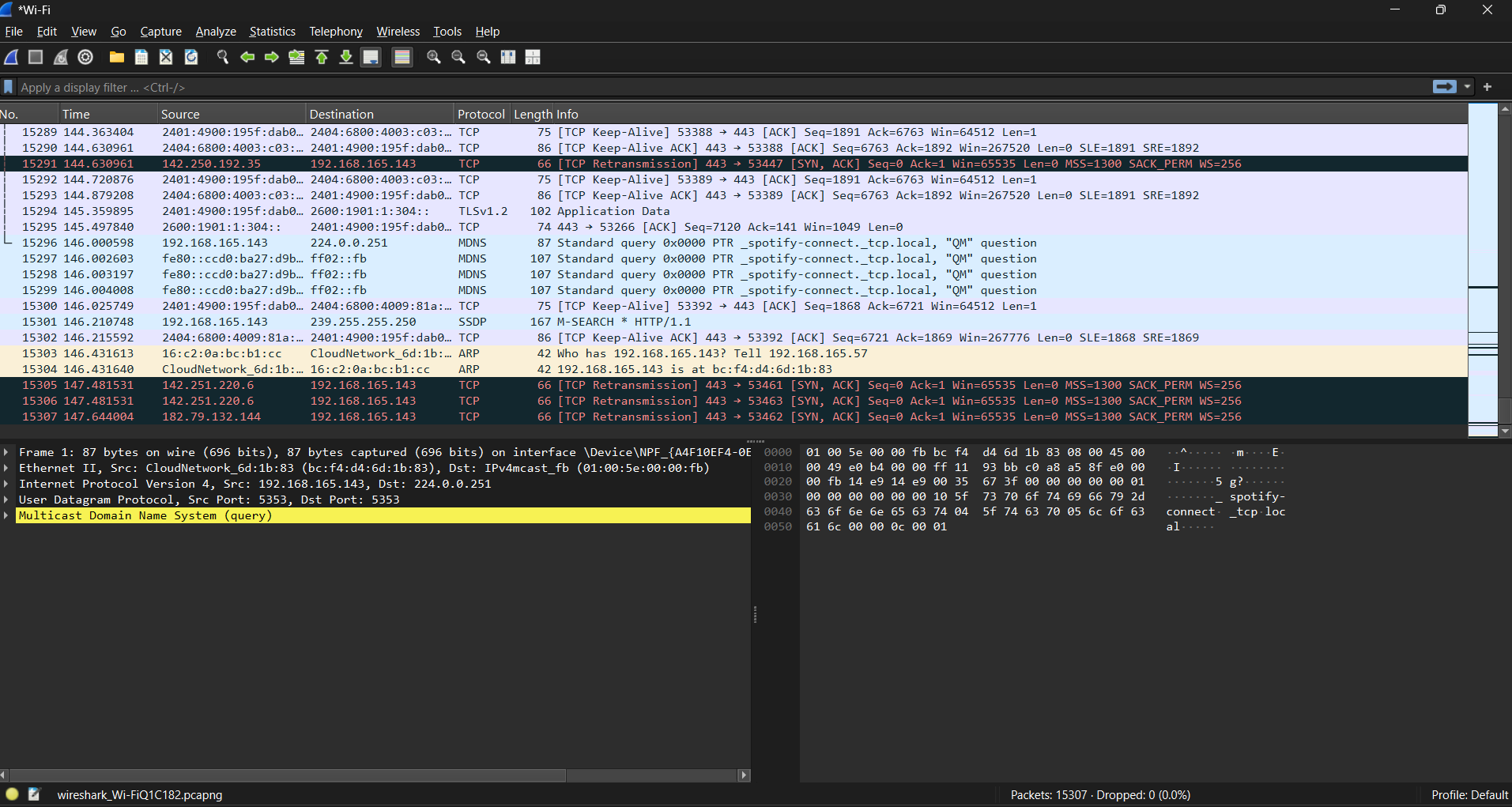
**4. ARP (Address Resolution Protocol)**

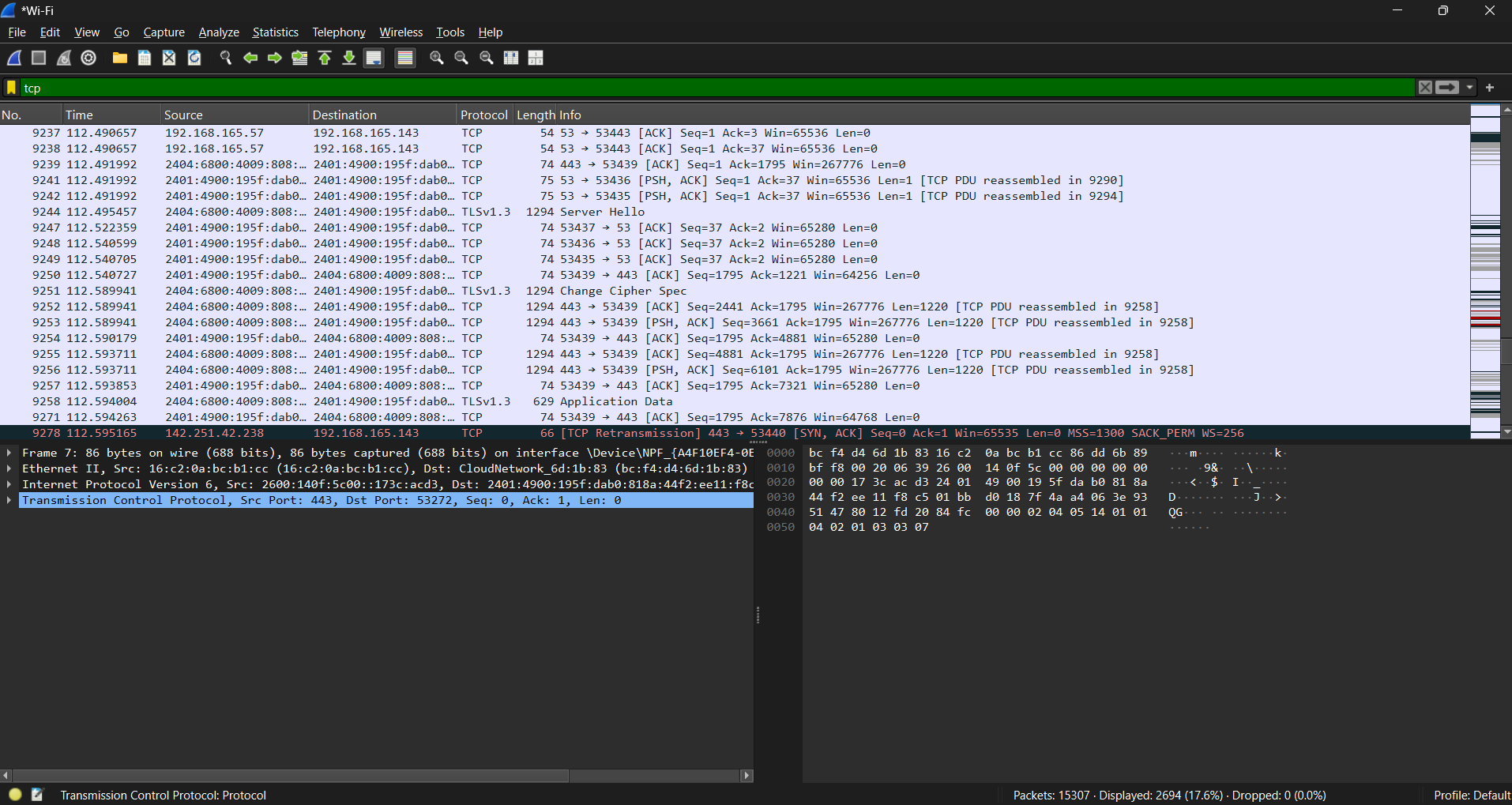
* **Description:** Resolves IP addresses to MAC addresses.
* **Observation:** Seen as "Who has 192.168.x.x?" requests.
* **Use Case:** Local network communication.

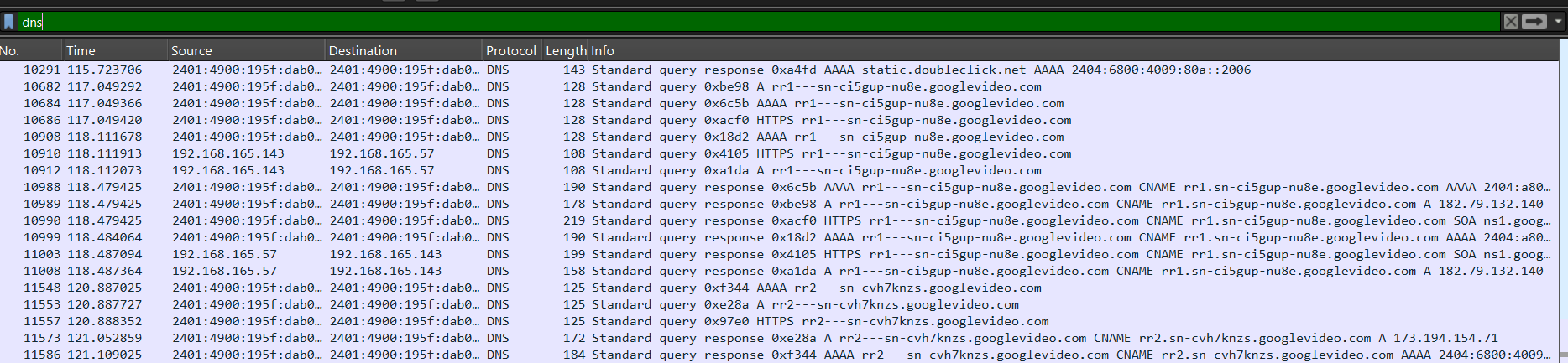
**5. SSDP (Simple Service Discovery Protocol)**

* **Description:** Used for discovering UPnP devices.
* **Observation:** M-SEARCH and NOTIFY packets.
* **Use Case:** Smart devices discovery (TVs, routers).









**Conclusion**

The Wireshark capture was successful in recording live traffic. At least five different protocols were identified, each serving different networking purposes:

* **TCP** for reliable transport
* **TLSv1.2** for encrypted communication
* **MDNS** and **SSDP** for device/service discovery
* **ARP** for internal IP-to-MAC resolution

This exercise provided valuable hands-on experience in using Wireshark and interpreting packet data across layers.