**Task 5 : Capture and Analyze Network Traffic Using Wireshark.**

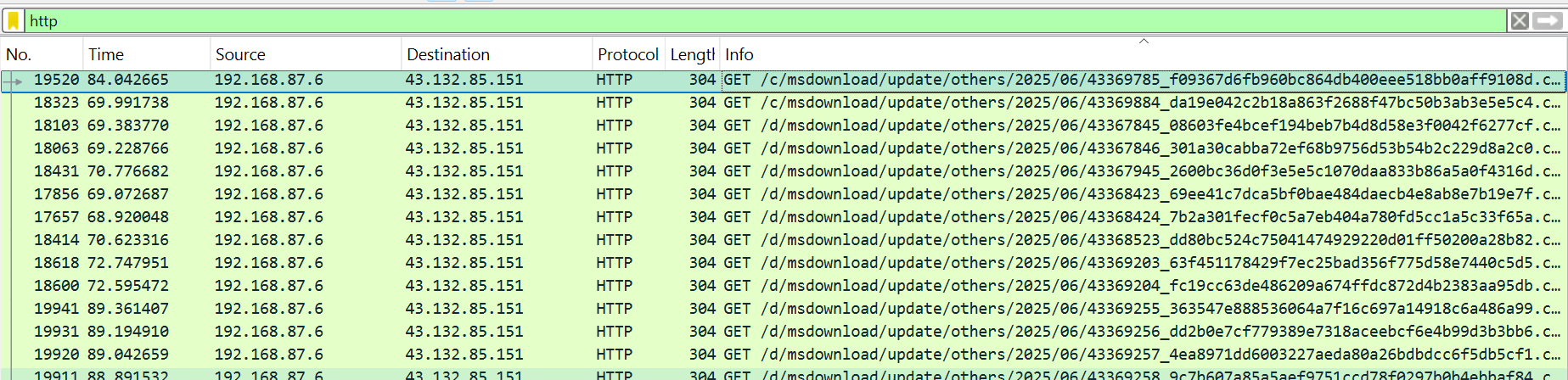
**Objective:** Capture live network packets and identify basic protocols and traffic types.

**Tools:** Wireshark (free).

**Deliverables:** A packet capture (.pcap) file and a short report of protocols identified.

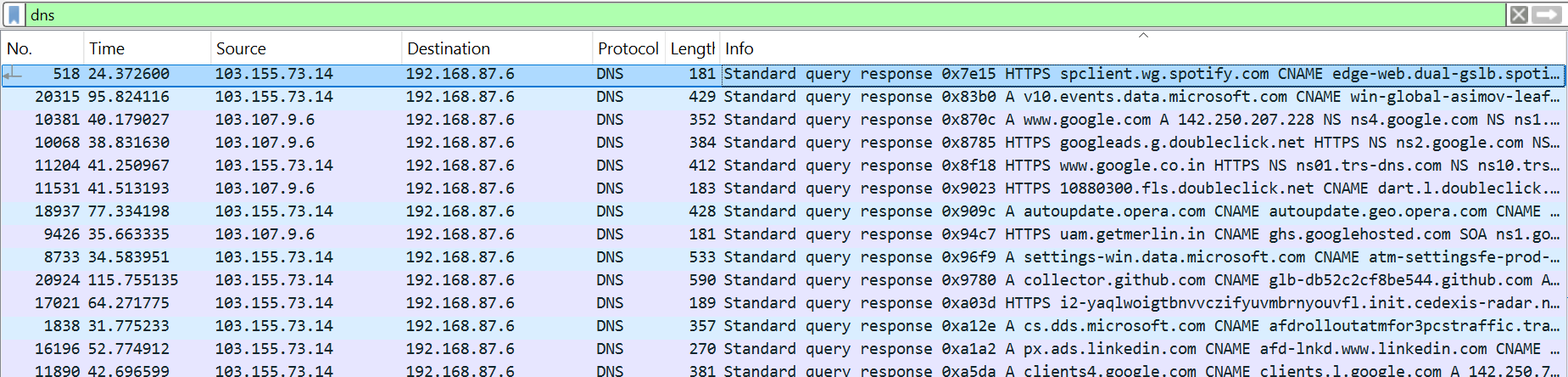
**Report of protocols identified:**

**HTTP:**



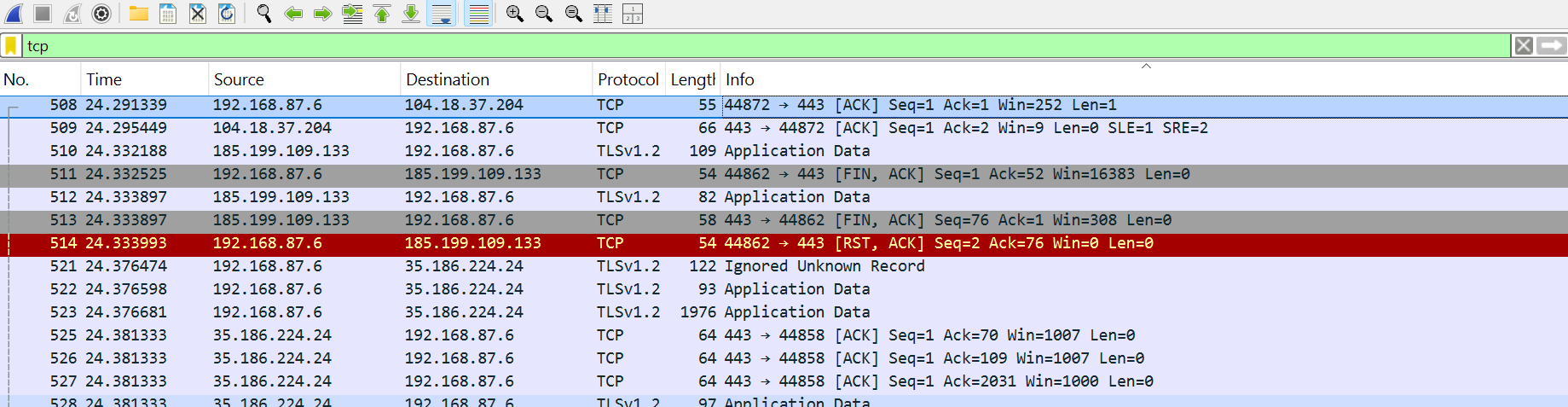
The Hypertext Transfer Protocol (HTTP) is a foundation of the World Wide Web, allowing clients and servers to communicate and exchange data. It's used to load webpages and transfer information between networked devices.

**DNS:**



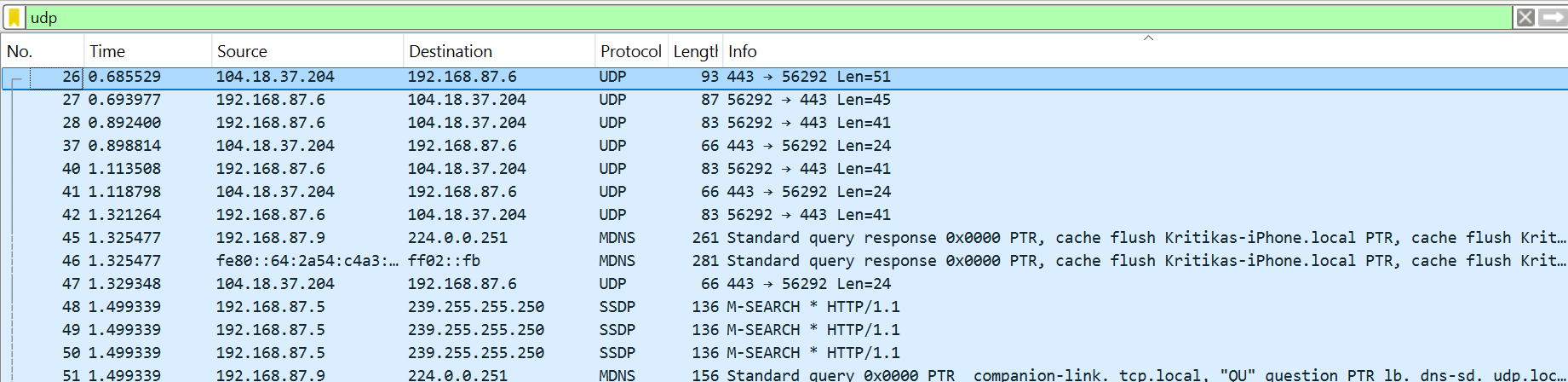
The Domain Name System (DNS) is a hierarchical and distributed naming system that translates human-readable domain names (like www.example.com) into machine-readable IP addresses (like 192.168.1.1).

**TCP:**



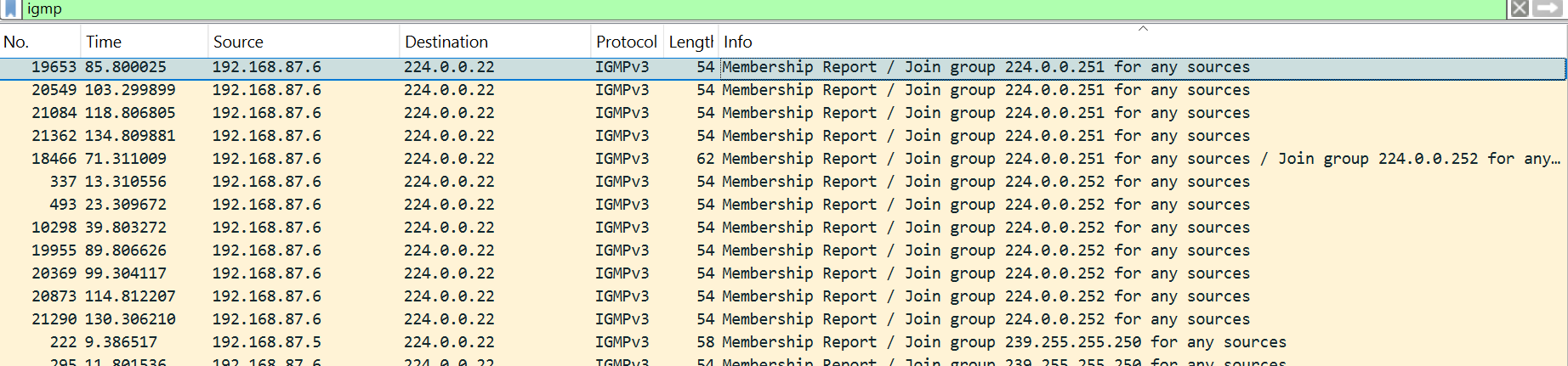
The Transmission Control Protocol (TCP) is a fundamental part of the internet protocol suite, working alongside the Internet Protocol (IP). It ensures reliable and ordered delivery of data between devices on a network by establishing a connection, managing data flow, and checking for errors.

**UDP:**



The User Datagram Protocol (UDP) is a connectionless transport layer protocol used for transmitting data over a network. Unlike TCP, UDP does not establish a connection before sending data, making it faster but less reliable. It's commonly used in applications where speed and efficiency are prioritized over guaranteed data delivery, such as streaming, online gaming, etc.

**IGMPv3:**



IGMPv3 (Internet Group Management Protocol version 3) is an extension of IGMPv2, used for IPv4 networks to manage multicast group membership.

It offers improved functionality, including: Enhanced multicast routing and forwarding, Better handling of multicast groups with multiple sources, Ability to filter out unwanted traffic.