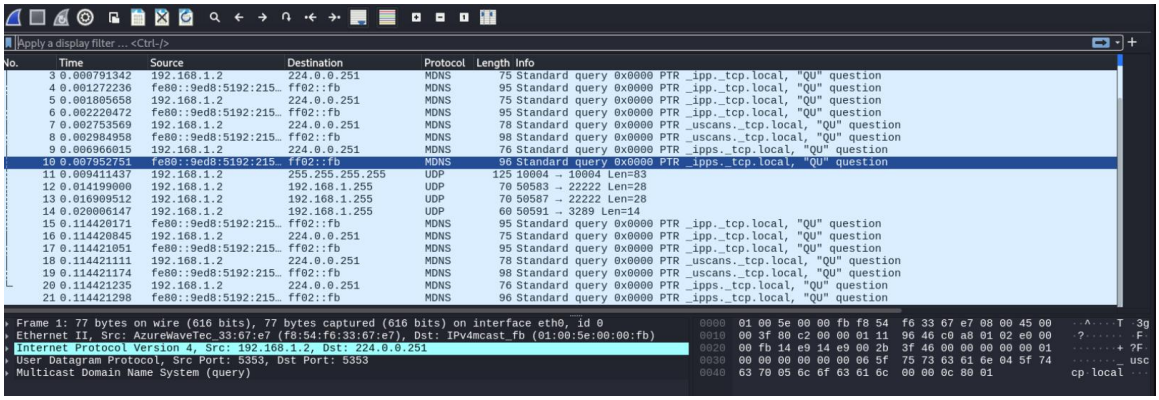
Task-5: Wireshark

Wireshark: It is the network traffic analyzing tool used to capture every network packet received on the given network interface.

➔ Here is the sample image of the home network pcap file:



Here are some of analyzing protocols:

1. MDNS (Multicast DNS)

Multicast DNS (mDNS) is used to resolve hostnames to IP addresses within small networks that do not include a local name server. It is commonly used for service discovery in local area networks, such as printers, smart devices, and IoT equipment.

2. UDP (User Datagram Protocol)

UDP is a transport layer protocol that provides a connectionless service for sending messages (datagrams). It is faster than TCP but does not guarantee delivery, ordering, or error correction. In the screenshot, UDP is the underlying protocol carrying the mDNS queries.

3. IPv4 and IPv6 (Internet Protocol)

Both IPv4 and IPv6 are present in the screenshot. IPv4 is the fourth version of the Internet Protocol and is still widely used. IPv6 is the newer version designed to replace IPv4 and provide a much larger address space. They are responsible for addressing and routing packets between devices across networks.

Other Common Protocols in Wireshark

1. TCP (Transmission Control Protocol)

TCP is a reliable, connection-oriented transport layer protocol. It ensures data delivery, error checking, and maintains the correct order of packets. It is used by applications like HTTP, HTTPS, FTP, and SMTP.

2. HTTP/HTTPS (Hypertext Transfer Protocol)

HTTP and HTTPS are application layer protocols used for communication between web browsers and servers. HTTPS adds security by using SSL/TLS encryption.

3. ARP (Address Resolution Protocol)

ARP is used to map IP addresses to physical MAC addresses in a local network. It is an essential protocol for LAN communication.

4. ICMP (Internet Control Message Protocol)

ICMP is mainly used for diagnostic and error reporting purposes. The most common use of ICMP is the 'ping' command, which tests connectivity between devices.

5. DNS (Domain Name System)

DNS translates human-readable domain names (like www.example.com) into IP addresses. It plays a critical role in enabling web browsing and other network services.