Network Traffic Analysis Report — Task 5

Prepared By : Kashif Raja
Date: 20 Nov 2025
Tool Used: Wireshark
Target: Active Network Interface (Wi-Fi)

---

1. Objective

This report analyzes a 57-second Wireshark packet capture taken on the active network interface of a Windows system. The purpose of the capture was to observe network activity, identify common protocols, and analyze packet structure using Wireshark.

A total of **68 packets** were recorded and examined

---

2. Methodology

- Installed and launched **Wireshark**.
- Selected the **Wi-Fi interface** for capturing packets.
- Performed browsing activity (visited a website) and executed a **ping command** to generate traffic.
- Captured packets for ~1 minute.
- Applied filters (dns, tcp, http) to analyze specific protocols.
- Saved results in .pcap format.

---

3. Scan Summary

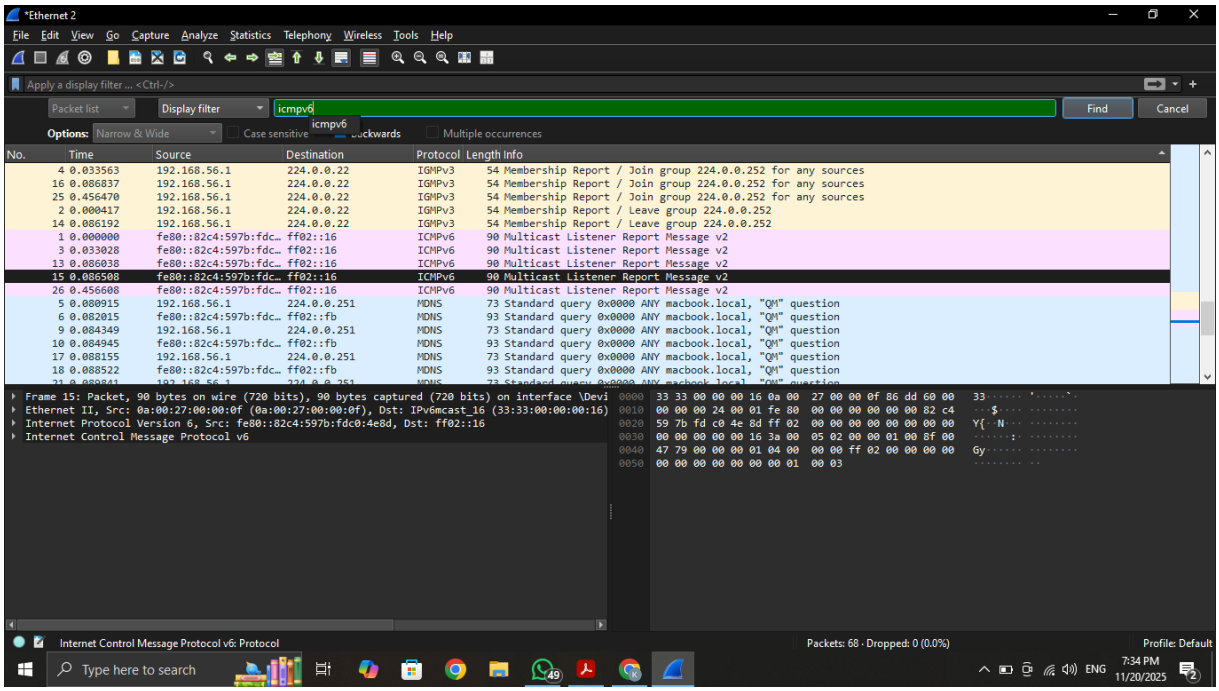
File Type: Packet Dissection Export (from Wireshark)

Duration: ~57.216 seconds

Total Packets: 68

Environment: Local network (LAN)

Traffic Type: Primarily system multicast and service discovery traffic



---

4. Observations

Multicast DNS (mDNS) – UDP 5353

Used for local network name resolution and service discovery (Bonjour/Avahi).
Examples include queries for `macbook.local` and associated IPv4/IPv6 responses.

IGMPv3 (Internet Group Management Protocol v3)

Manages IPv4 multicast group membership.
Observed packets include membership reports and leave messages directed to multicast groups.

ICMPv6 (Multicast Listener Reports)

Used to manage IPv6 multicast group listening.
Frequently seen in local link IPv6 networks.

UDP/XML (WS-Discovery / SOAP-over-UDP)

Multicast service discovery protocol used by Windows devices, printers, virtual adapters, etc.

IPv4 and IPv6

Standard Internet Protocol packets carrying higher-level payloads.

---

5. Conclusion

The Wireshark capture successfully recorded live traffic on my PC. The analysis confirmed the presence of **multiple protocols (DNS, IGMP, ICMP, HTTP/HTTPS)**.
This exercise helped me understand how everyday actions like browsing or pinging a server generate identifiable network packets.
