# Week-6 Lab Assignment

---

**1. Aim:** Study of packet sniffer tools like Wireshark, ethereal, tcpdump etc.

**2. Objectives**: To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

## ➢ Steps for Installing Wireshark on Windows:

**Steps for Installing Wireshark on Windows:**

- **Download the Installer:**
  Visit the Wireshark website and select the appropriate installer for your system (either 32-bit or 64-bit).
- **Launch the Installer:**
  After the download, double-click the .exe file to open the installer. The setup wizard will guide you through the process. Click Next to continue.
- **Choose Installation Components:**
  Select the components you wish to install. The default options are sufficient for most users. Ensure that Npcap (or WinPcap) is selected, as it's necessary for capturing packets.
- **Install Npcap:**
  If prompted, agree to install Npcap (or WinPcap). This tool is required for Wireshark to capture network traffic.
- **Finish Installation:**
  After selecting the desired options, click Install and wait for the process to complete. Once done, click Finish to exit the setup.
- **Open Wireshark:**
  You can launch Wireshark from the Start Menu or desktop shortcut. For full packet capturing capabilities, you may need to run Wireshark as an administrator.

## ➢ Captured Packets and their details:

- Source and destination IP addresses.
- Packet size.
- Protocols used (TCP, UDP, HTTP, DNS, etc.).
- Flags such as SYN, ACK (in TCP packets).
- Payload (actual data being transmitted)

## ➢ Promiscuous Mode vs. Non-Promiscuous Mode:

In **Promiscuous Mode**, the network interface card (NIC) is configured to capture all traffic on the network, even if the data is not intended for the specific device. This mode is frequently used by network administrators or security experts for tasks such as monitoring, packet analysis, and troubleshooting. Tools like Wireshark often operate in this mode to collect data from all devices within a network.

**Example:** If your computer is connected to a Wi-Fi network, it can capture the communication between other devices on the same network, even though the packets are not intended for your computer.

In contrast, in **Non-Promiscuous Mode**, the NIC only captures and processes traffic that is specifically directed to its own IP or MAC address. This is the default mode for most devices, ensuring they only handle relevant traffic, which reduces unnecessary processing and helps maintain network privacy.

**Example:** Your computer will only capture data packets that are directed to your IP or MAC address, ignoring any unrelated traffic.

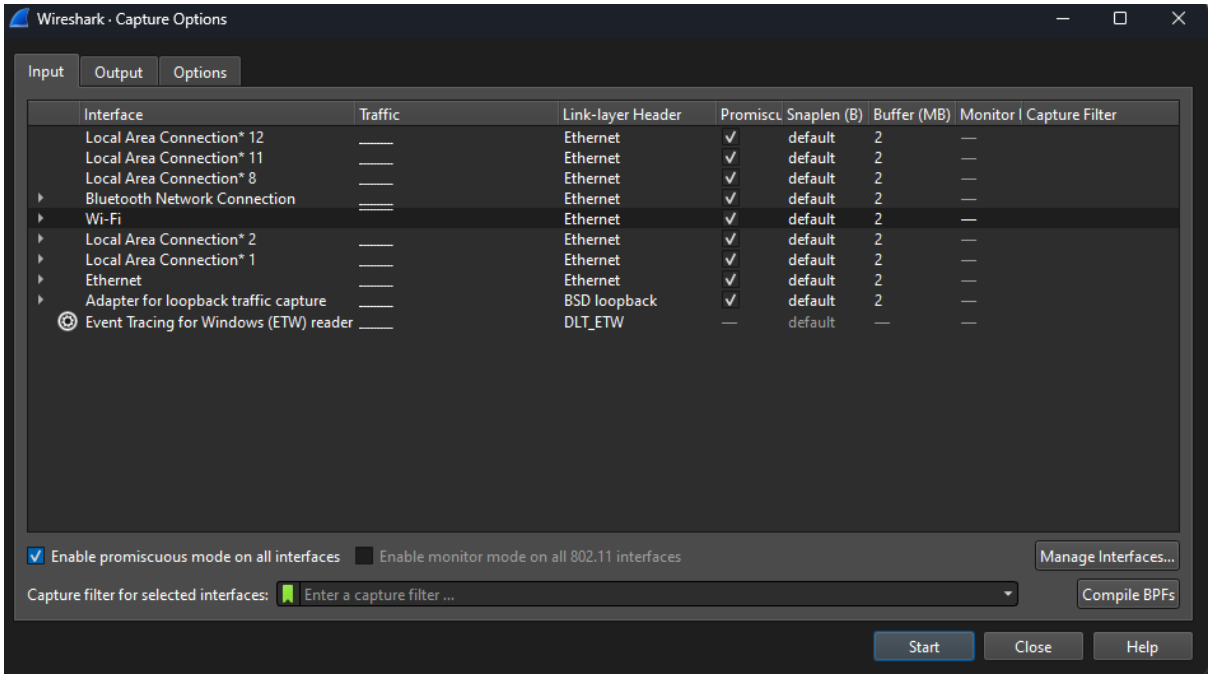


*Fig_1 - Changing_modes*

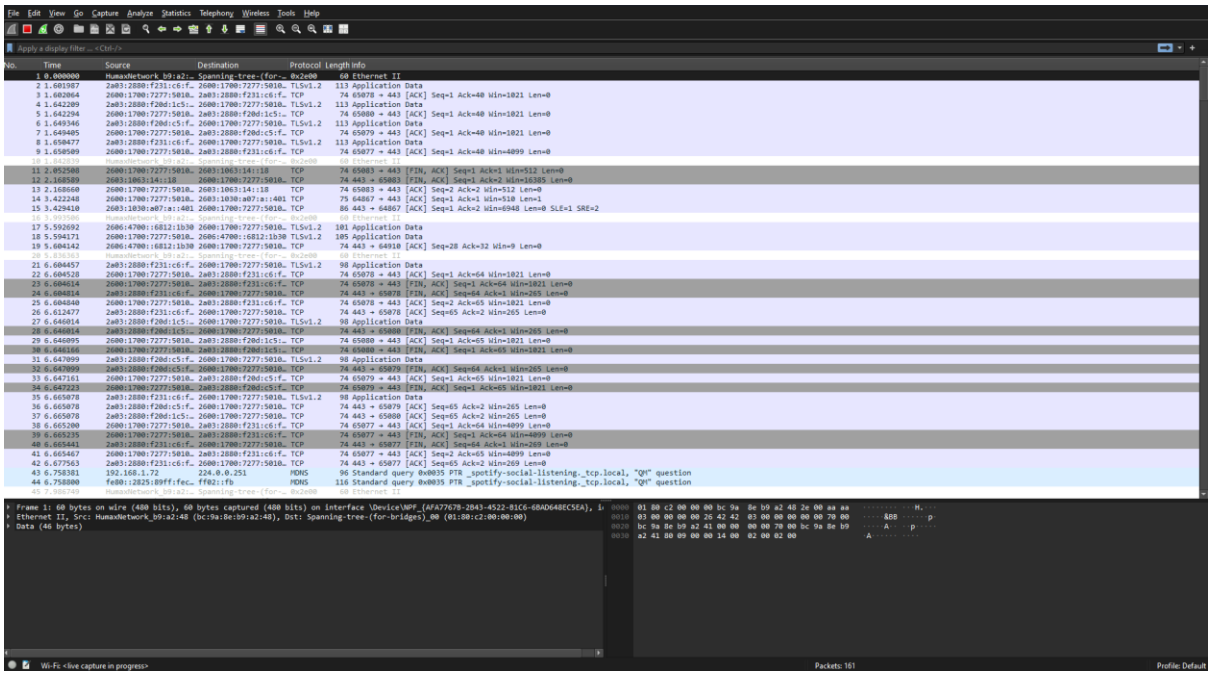

*Fig_2 - Captured_packets (Promiscuous_mode)*

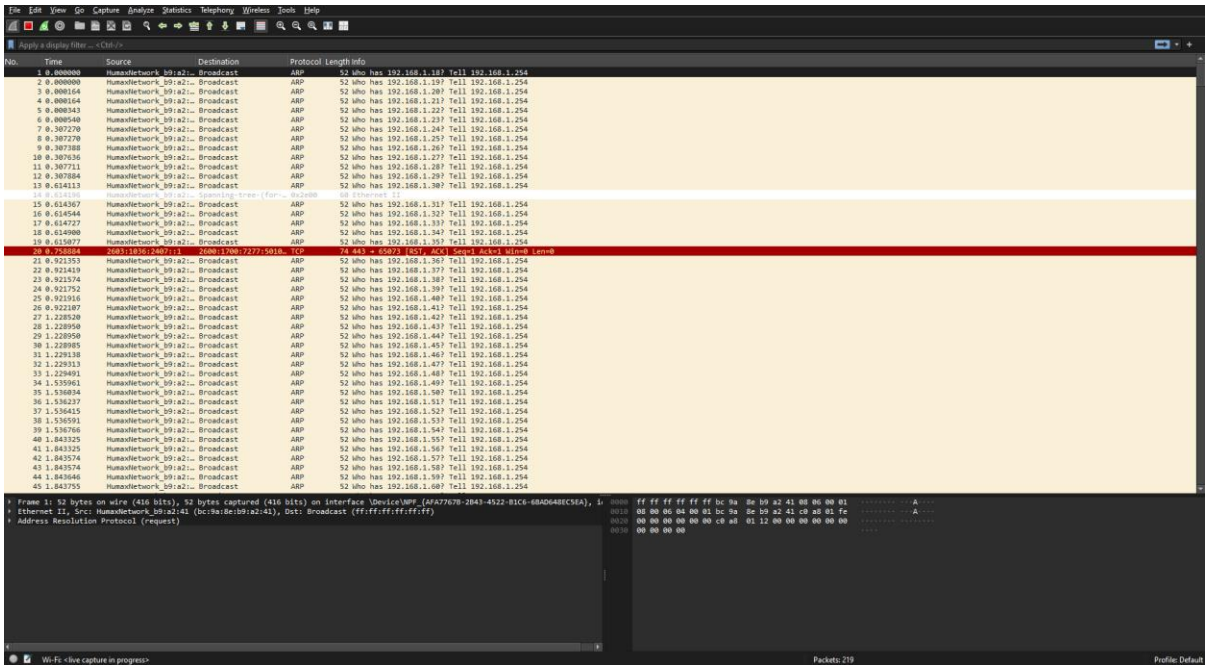

*Fig_3 - Captured_packets (Non_Promiscuous_mode)*

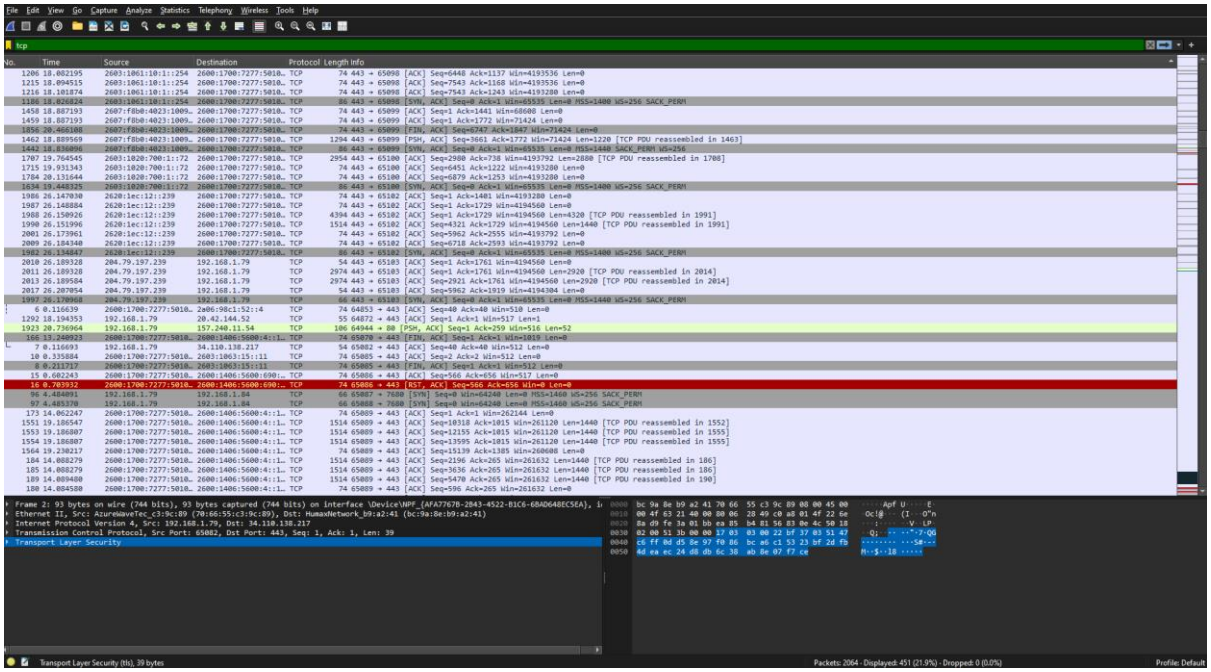

*Fig_4 - Applying filter to display the packets using TCP protocol.*

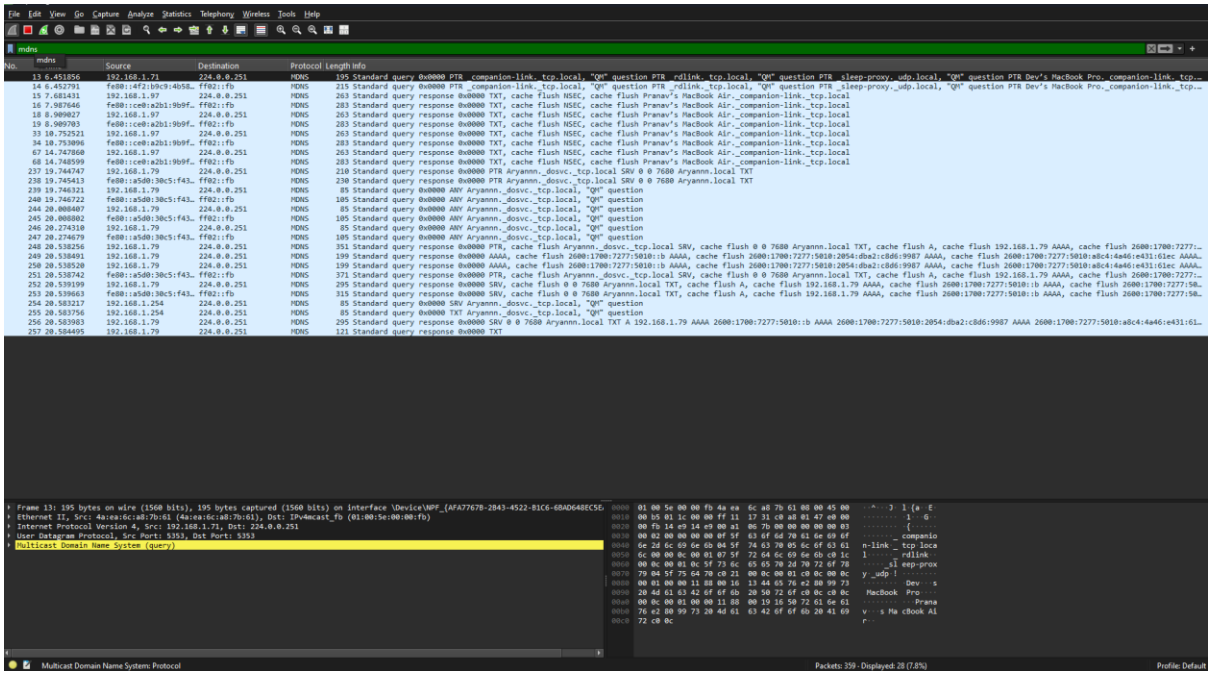

*Fig_5 - Applying filter to display the packets using MDNS protocol.*

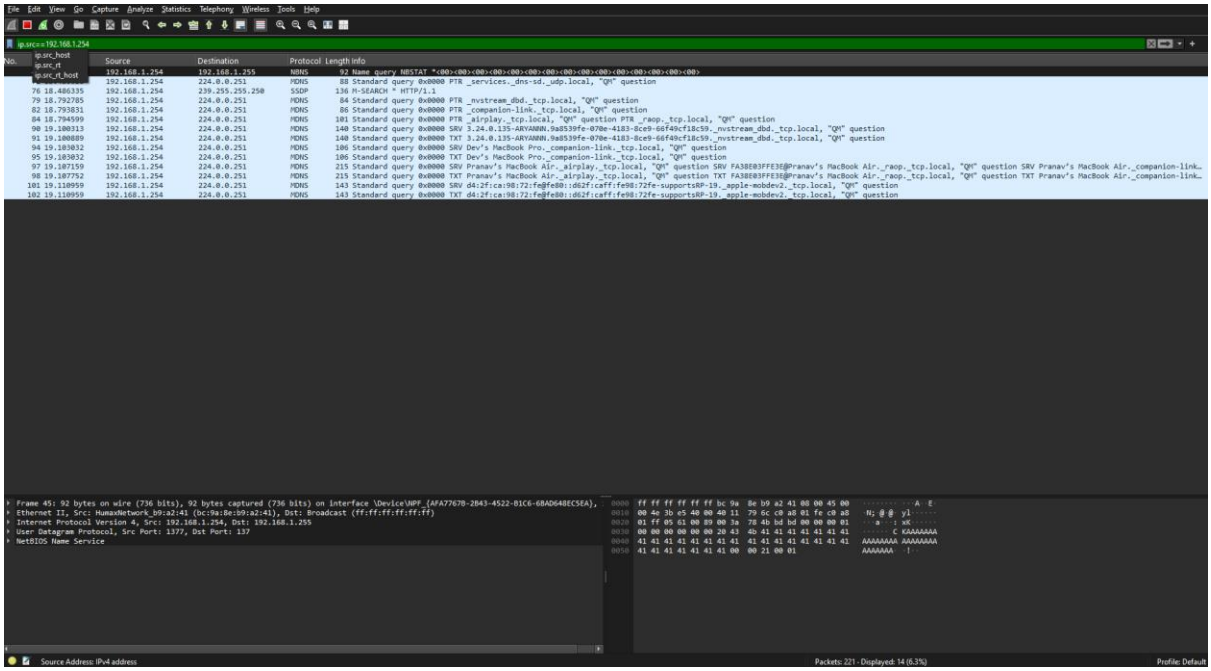

*Fig_6 - Applying filter to display the packets having IP address 192.168.1.254*