**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

**EXPERIMENT 8**

**Aim:-** Study of packet sniffer tools Wireshark: - a. Observer performance in promiscuous as well as non-promiscuous mode. b. Show the packets can be traced based on different filters.

**Theory:-**

**Promiscuous Mode:**

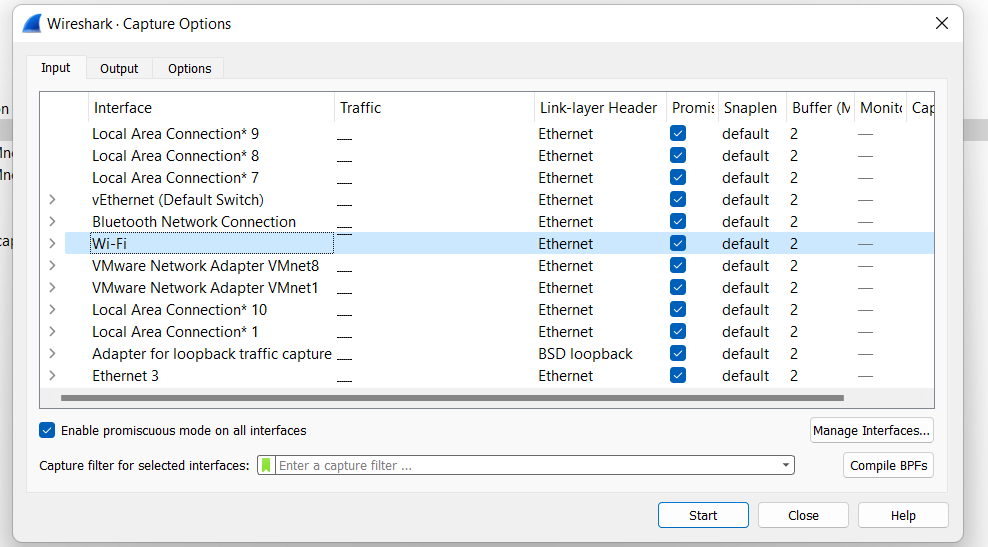
Promiscuous mode is a network interface mode that allows a network card to capture and inspect all network traffic on a shared network segment, regardless of whether the packets are addressed to that specific network card or not. Here's some theory related to promiscuous mode:

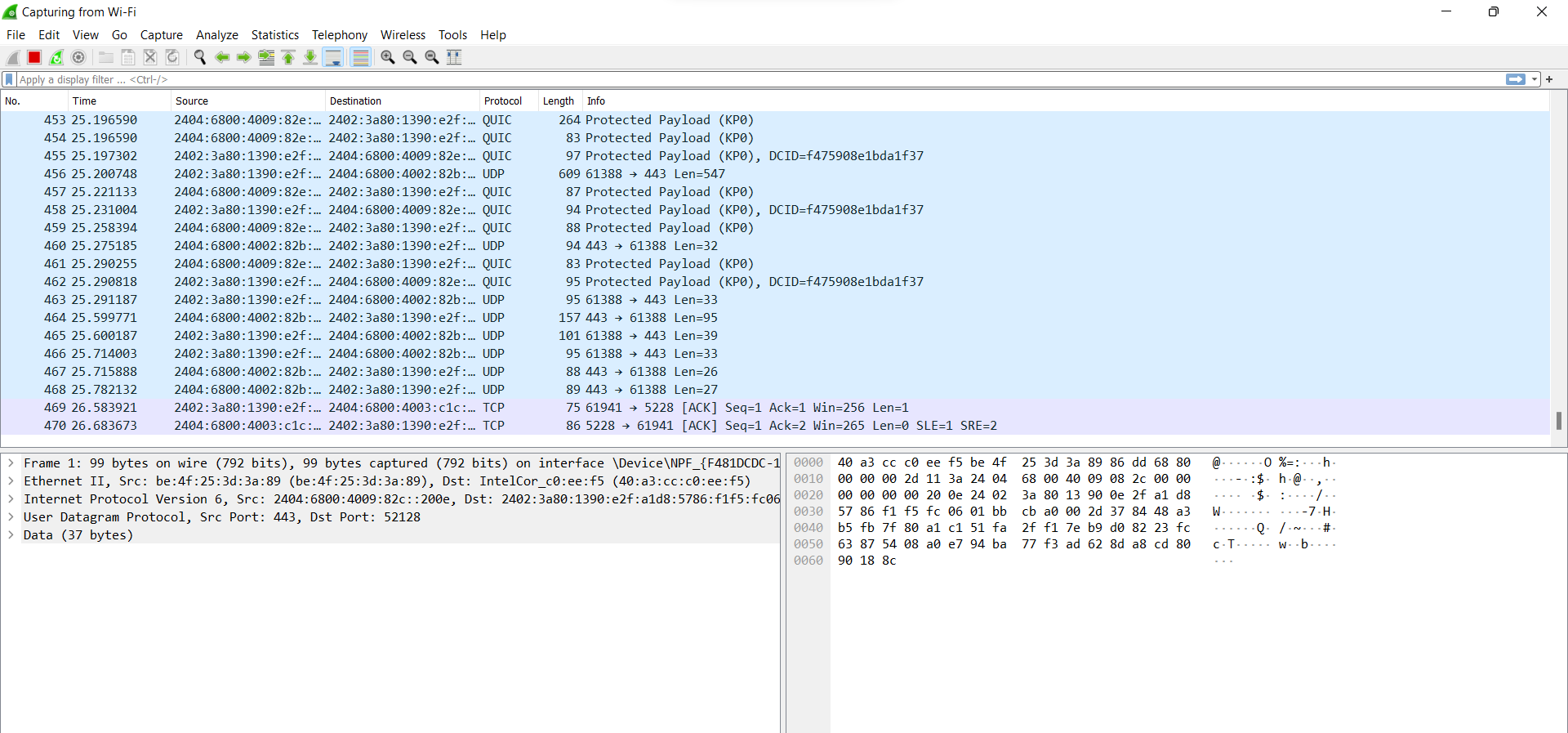
* **Purpose of Promiscuous Mode:**
  + Promiscuous mode is often used for network monitoring and analysis. It enables tools like packet sniffers to capture all network traffic passing through the network segment, including packets intended for other devices.
* Packet Capture in Promiscuous Mode:
  + When a network card is in promiscuous mode, it captures all network frames or packets on the network segment, even if they are not specifically addressed to that network card's MAC address.
  + This mode is useful for diagnosing network issues, security monitoring, and analyzing network protocols.
* Security Implications:
  + Promiscuous mode can potentially raise security concerns as it allows a device to eavesdrop on network traffic not intended for it.
  + In some environments, enabling promiscuous mode may be prohibited due to security policies.

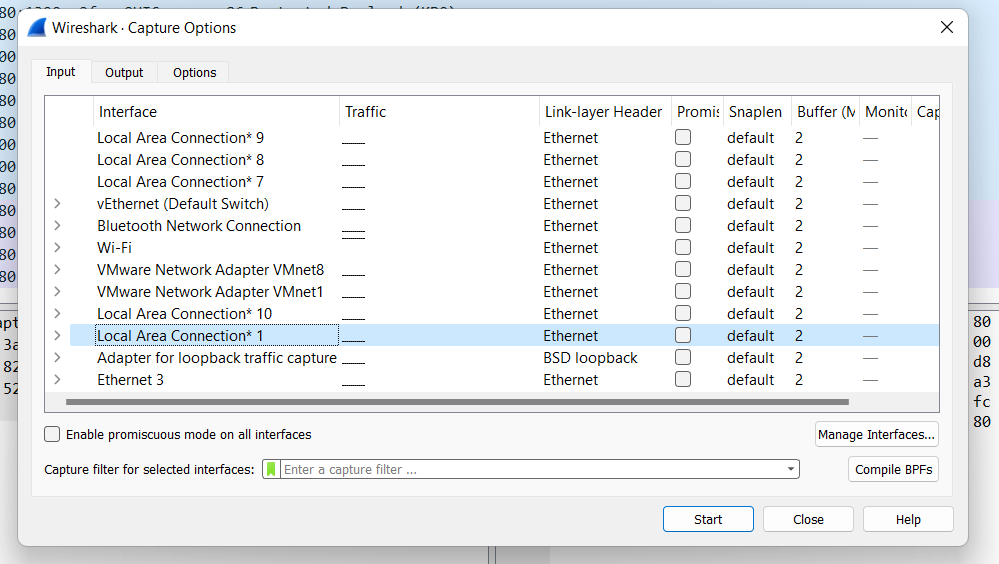
**Non-Promiscuous Mode:**

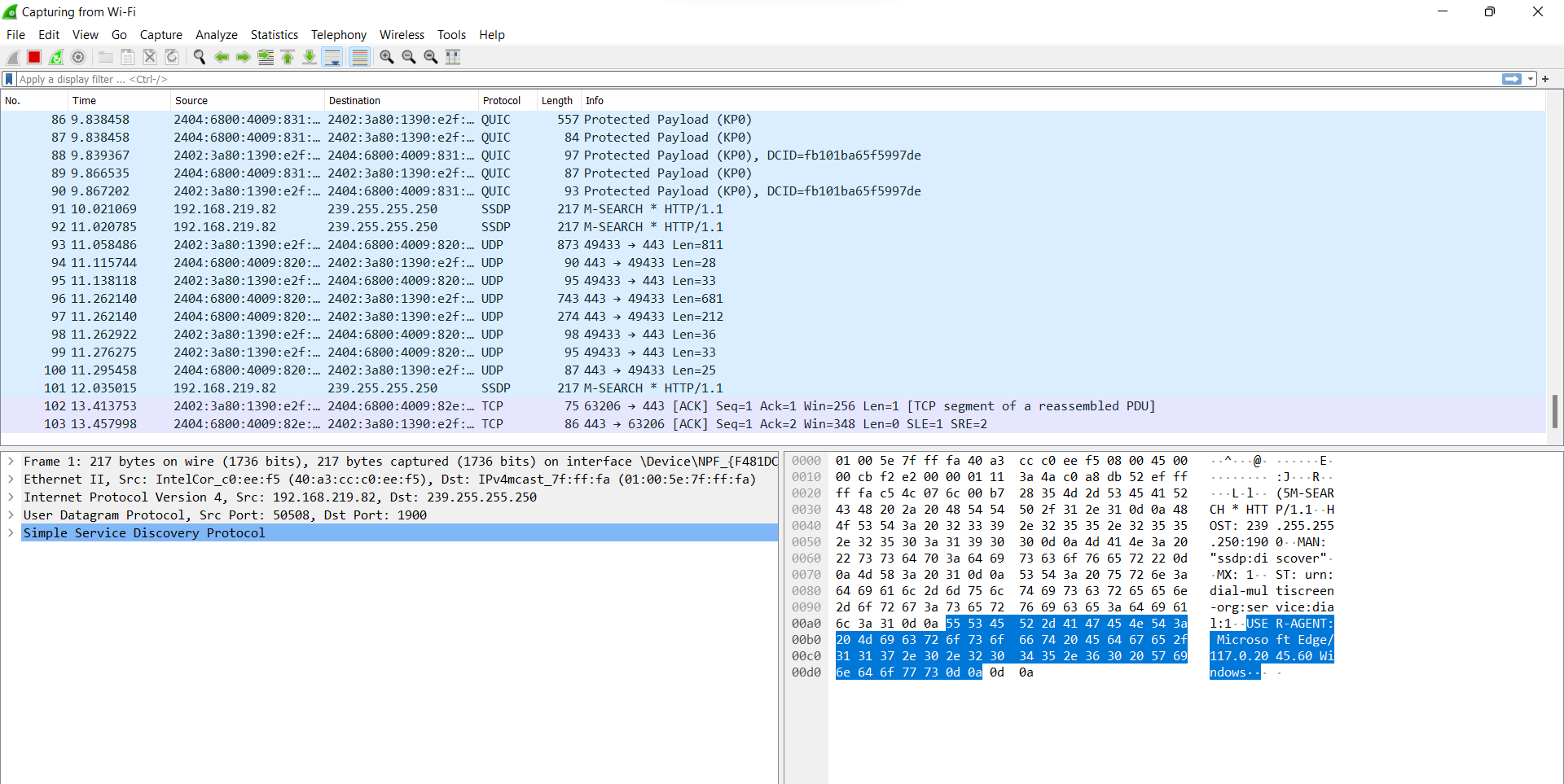
Non-promiscuous mode is the default operating mode for network interfaces. In this mode, the network card only captures packets specifically addressed to its MAC address. Here's some theory related to non-promiscuous mode:

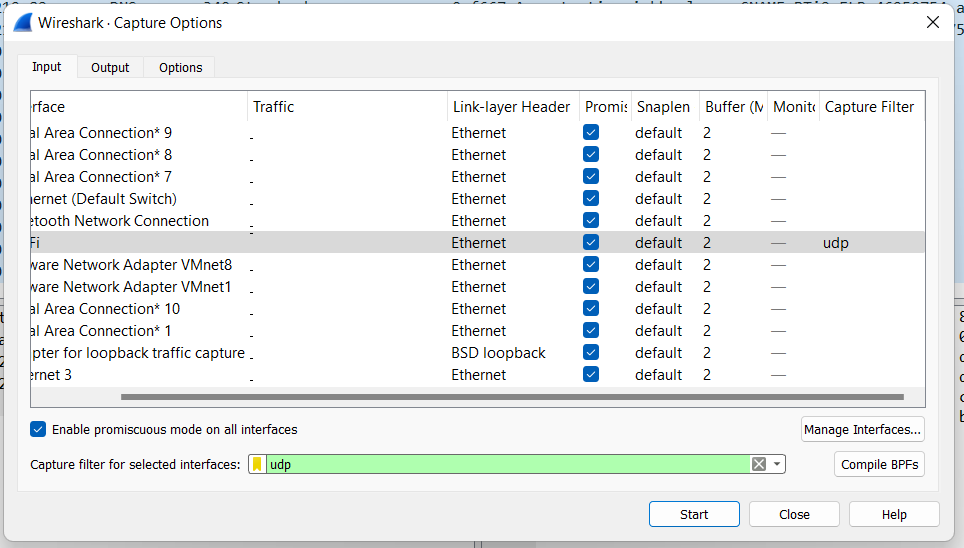
* Normal Operation:
  + In non-promiscuous mode, a network card will typically only process and pass up to the operating system the packets that are addressed to its unique MAC address.
  + Packets not intended for the specific network card are typically ignored.
* Limitations for Packet Analysis:
  + Non-promiscuous mode is less suitable for packet analysis and monitoring tasks because it only captures packets intended for the specific device.
  + It may not provide a comprehensive view of network activity.

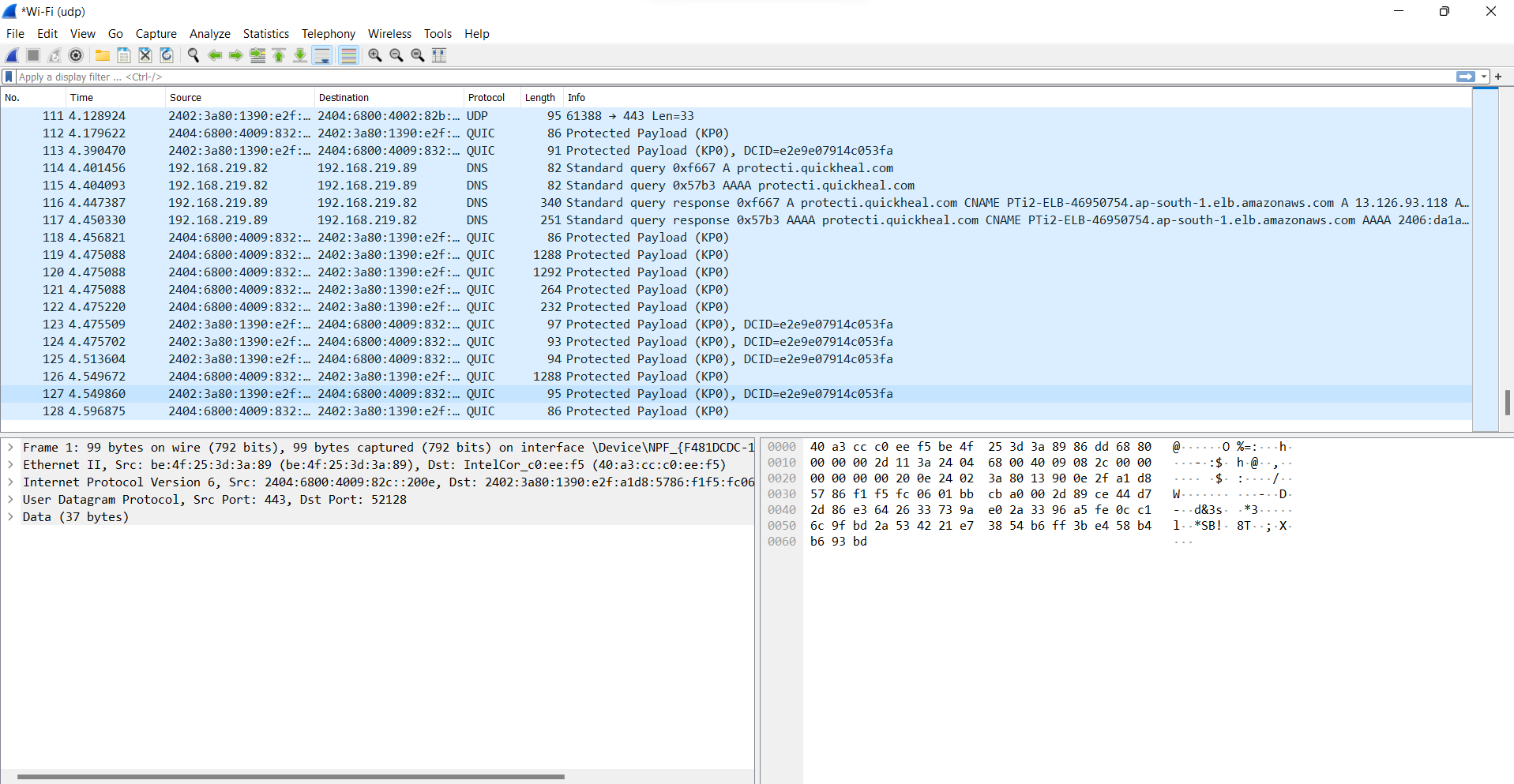












**Conclusion :-** Packet sniffer tools of Wireshark are studied including Promiscuous mode and non-promiscuous mode.