Sniffer Mode

Sniffer Mode is a feature supported by some Wi-Fi adapters that allows them to capture packets while still being associated with a specific network (like your home Wi-Fi). It’s essentially a "lite" version of packet capturing, working within the bounds of the network you’re connected to.

Works:

In Sniffer Mode, the Wi-Fi card operates in a managed mode but with the ability to grab all the data frames it sees on the channel it’s connected to. It doesn’t hop between channels or capture everything in the air—it’s tied to the access point (AP) you’re associated with.

Points :

- Stays connected to a specific network.
- Captures packets only on the channel of the associated AP.
- Typically captures data frames, not the full spectrum of management or control frames unless the hardware/software explicitly supports it.

Use Case:

Troubleshooting network issues: If you’re debugging your own Wi-Fi network (e.g., slow speeds, dropped connections), Sniffer Mode lets you analyze the traffic between your device and the AP.

Basic packet analysis: Useful for developers or network admins who want to inspect application-layer data (like HTTP requests) without needing to go full-on rogue.

Learning: Great for beginners who want to dip their toes into packet sniffing without messing with advanced setups.

Limitations: You’re locked to one channel, and you might miss traffic from nearby networks or devices not associated with your AP.

Monitor Mode

Monitor Mode (sometimes called RFMON or Radio Frequency Monitor Mode) is the full-on packet-capturing beast. It turns your Wi-Fi adapter into a passive listener that captures all wireless traffic in range, regardless of whether it’s part of your network or not.

Works:

In Monitor Mode, the Wi-Fi card doesn’t associate with any network. Instead, it listens promiscuously to the airwaves, capturing raw 802.11 frames (data, management, and control frames) on a specific channel—or hops between channels if supported by the tool.

Points :

- Not tied to any network; it’s a passive observer.
- Captures everything: beacons, probes, authentication frames, and more—not just data packets.
- Requires compatible hardware (not all Wi-Fi cards support it) and often a specific driver (e.g., in Linux with tools like aircrack-ng or Wireshark).

Use Case:

Security auditing: Ethical hackers and penetration testers use Monitor Mode to analyze Wi-Fi networks for vulnerabilities—like spotting weak encryption or capturing handshakes for cracking attempts (e.g., WPA2-PSK).

Deep network analysis: Ideal for studying how devices communicate in a given area, including rogue APs or interference from overlapping networks.

Forensic investigations: Capturing all traffic in a specific location to reconstruct events or detect unauthorized activity.

Real-World Example

Sniffer Mode: At home, when Netflix keeps buffering, by firing up Sniffer Mode with a tool like Wireshark to see if packets are dropping between our laptop and router.

Monitor Mode: A security pro at a coffee shop, wants to check if someone’s running a fake hotspot. By switching to Monitor Mode with airodump-ng to scan all nearby APs and devices.