

WiFi Training Program 2025

Name: Aswath S

University: VIT Vellore

Reg.No: 21BEC2188

Question-6:

Whats the difference between Sniffer and monitor mode , use case for each mode.

Aspect	Sniffer Mode	Monitor Mode
Purpose	Capturing network traffic for analysis.	Capturing all wireless traffic in a specific channel.
Frame Types Captured	Only frames meant for the device (unicast, broadcast, multicast).	All frames, including management, control, and data frames.
Filtering	Filters applied at the driver level (e.g., only TCP traffic).	No filtering at the hardware level, captures everything.
Usage Layer	Usually operates at Layer 3 (Network Layer) and above.	Operates at Layer 2 (Data Link Layer).
Promiscuous Mode	Enabled to capture traffic not directly addressed to the device.	Doesn't require promiscuous mode; captures raw frames from the air.
Encryption Handling	Can only capture encrypted packets unless configured with keys.	Captures packets regardless of encryption, but requires decryption for analysis.
Supported Devices	Typically implemented via software tools (e.g., Wireshark, tcpdump).	Requires hardware support (e.g., Wi-Fi adapters that support Monitor Mode).
Use Cases	Network troubleshooting, packet analysis, intrusion detection.	Wireless security auditing, channel scanning, network reconnaissance.
Example Tools	Wireshark, tcpdump.	Aircrack-ng, Kismet.