Packet Sniffing

- We now need a program that can capture these packets for us.
- use airodump-ng for this.
- enable monitor mode & then do:

(this is a dummy wireless adapter name)

```
# airodump-ng wlan0
```

→ ctrl + c to quit.

→ The output it shows is very useful.

↳
1. Essid shows all wifi networks around.
2. Other columns show more info about the network name we saw.
3. BSSID shows MAC Address of target.
4. PWR is power of network. (Higher the #, better the signal)
5. Beacons are frames sent by network to broadcast its existence.
6. #Data shows # of useful packets.
7. CH means channel.
8. ENC tells the encryption of the network.

Subject :

PAGE NO.:
DATE:

⑨ AUTH is the authentication used on that network.

★ Wifi Bands

→ decides frequency range that can be used
→ determines channels that can be used
→ most common: 2.4 ghz & 5ghz
★ → a: 5ghz only
→ airodump-ng only shows 2.4ghz networks.
→ use:

```
# airodump-ng --band a wlan0
```

→ now it'll discover 5ghz networks if your wireless network adapter supports it.
→ abg: captures both 2.4 & 5ghz at same time.

★ Targeted Packet Sniffing

→ now we can target a particular network.
→ do: ~~(specific)~~

```
# airodump-ng --{bssid} [bssid] --{channel} [ch]
  --write test wlan0
```

eg:

```
#airodump-ng --bssid F8:23:B2:B9:50:A8
  --channel 2 --write test wlan0
```

writes all data to test file.

→ Once this is done, you'll see one more section that shows the clients connected to that network.
→ STATION column shows client's MAC address.
→ The data is captured & stored locally.

Subject :

PAGE NO.:
DATE:

★ Since we have captured the packets, the only problem remains is encryption.

- test-01.cap file stores everything saved.

→ you can open the file in wireshark to view content but its not detailed. We need to break the encryption.

★ Deauthentication Attack

↳ we can disconnect any client from any network
↳ eg WEP, WPA & WPA2
↳ no need to know network key
↳ no need to connect to the network

```
# aireplay-ng --deauth 1000000000 -a {router MAC} -c {client MAC} mon0
```

1000000000 → no. of deauthentication packets we send

★ This will disconnect target client from the given network.