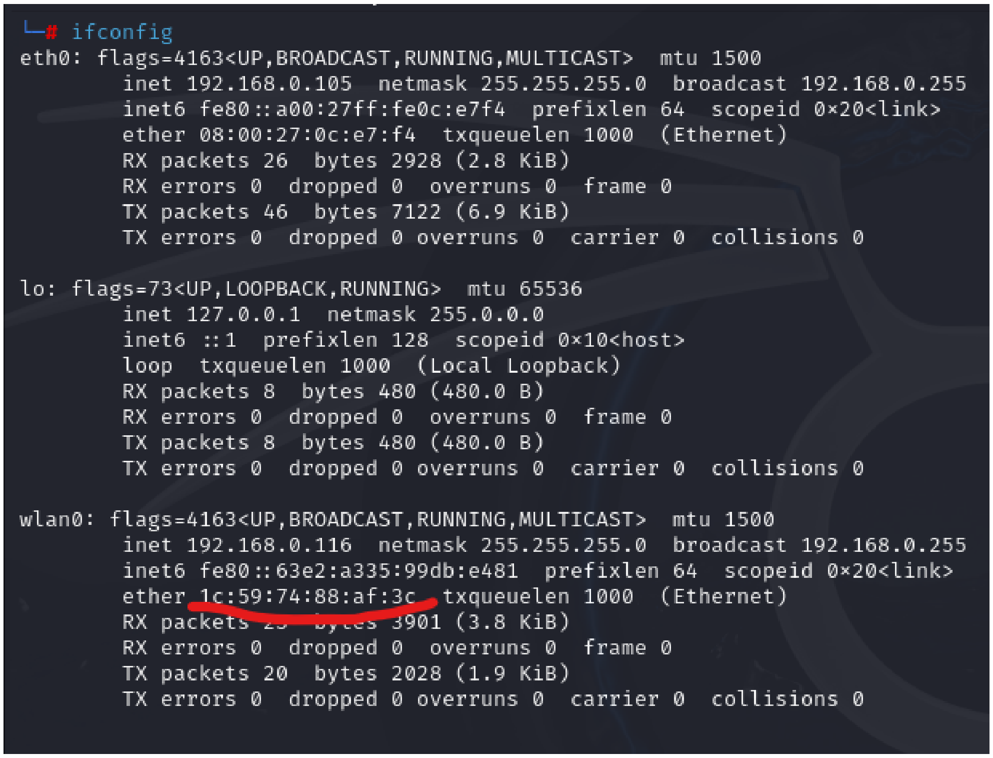
Pre Connection Att@ck

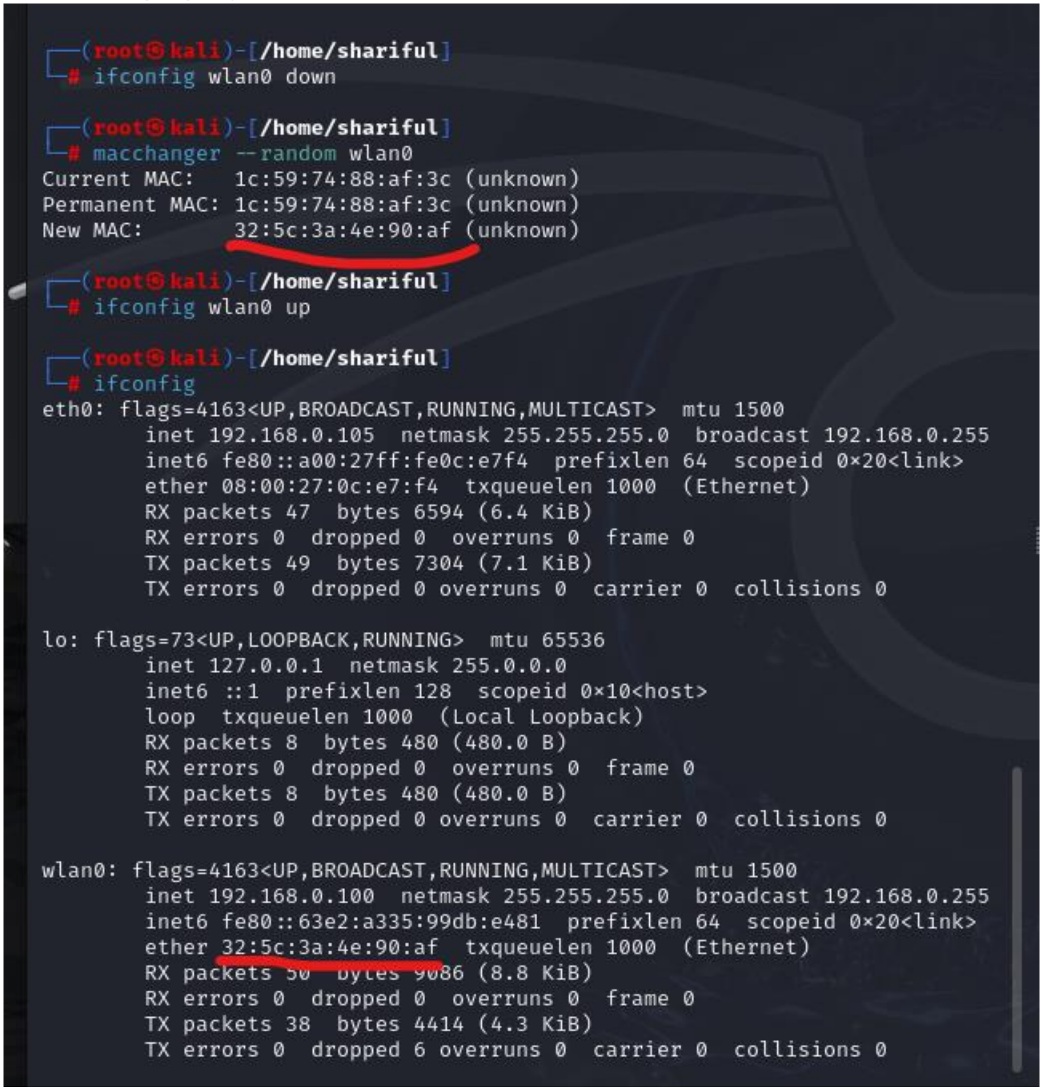
Change MAC Address: Because MAC and IP address is the way to trace you.

Here is my original MAC address.



```
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.105  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe0c:e7f4  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:0c:e7:f4  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 2928 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 7122 (6.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.116  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::63e2:a335:99db:e481  prefixlen 64  scopeid 0×20<link>
        ether 1c:59:74:88:af:3c  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 3901 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2028 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

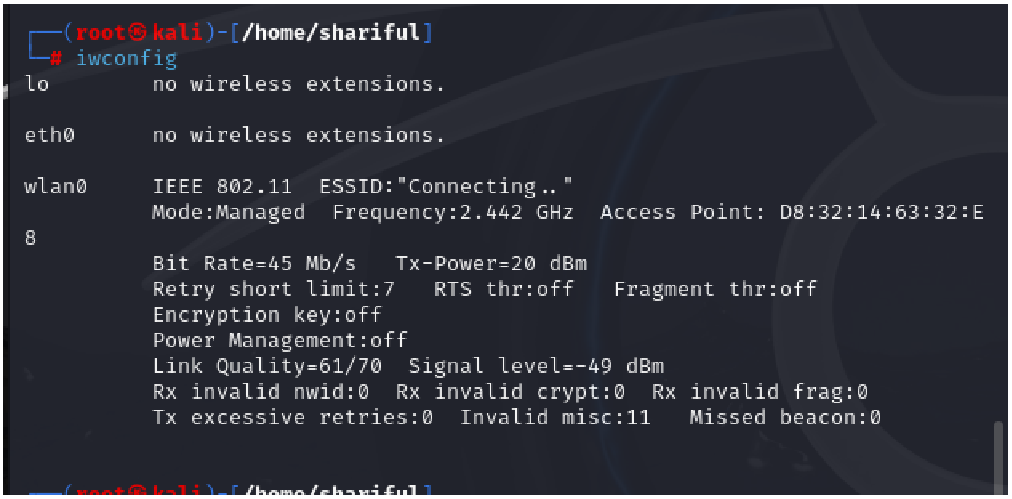
After changing my MAC address:



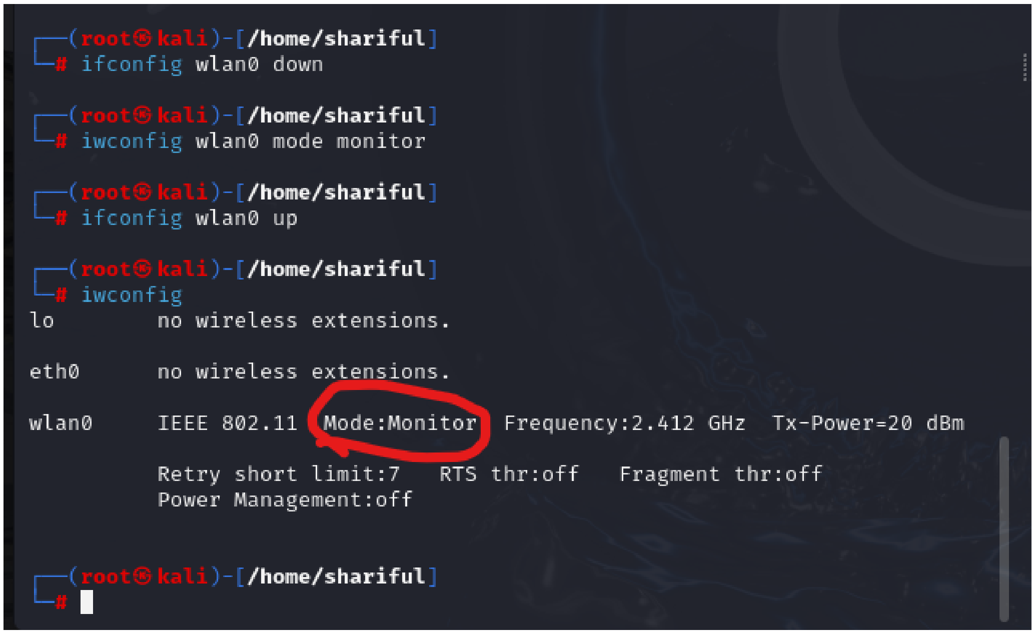
```
┌──(root㉿kali)-[/home/shariful]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[/home/shariful]
└─# macchanger --random wlan0
Current MAC:   1c:59:74:88:af:3c (unknown)
Permanent MAC: 1c:59:74:88:af:3c (unknown)
New MAC:       32:5c:3a:4e:90:af (unknown)

┌──(root㉿kali)-[/home/shariful]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[/home/shariful]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.105  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe0c:e7f4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0c:e7:f4  txqueuelen 1000  (Ethernet)
        RX packets 47  bytes 6594 (6.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49  bytes 7304 (7.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.100  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::63e2:a335:99db:e481  prefixlen 64  scopeid 0x20<link>
        ether 32:5c:3a:4e:90:af  txqueuelen 1000  (Ethernet)
        RX packets 50  bytes 9086 (8.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 4414 (4.3 KiB)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0
```

Enable Monitor Mode

First need to down the wlan0(wifi):

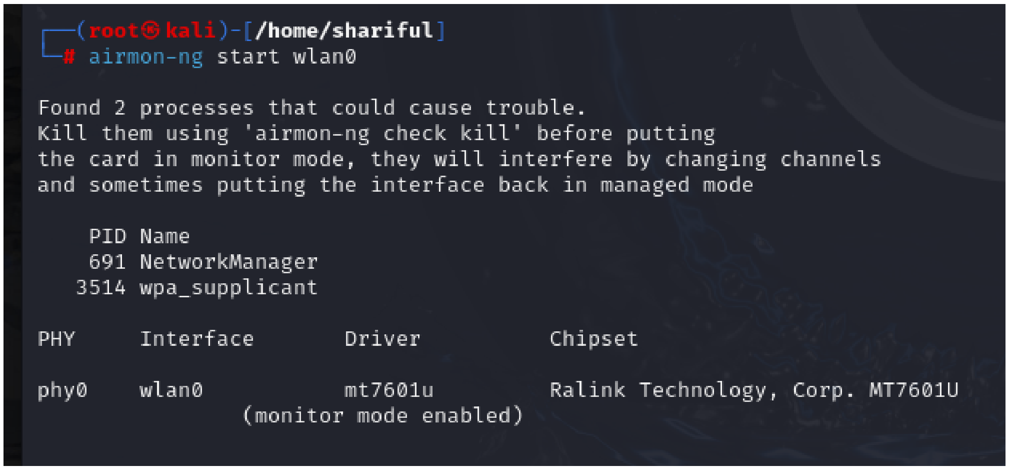


```
┌──(root㉿kali)-[/home/shariful]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"Connecting.."
          Mode:Managed  Frequency:2.442 GHz  Access Point: D8:32:14:63:32:E
8
          Bit Rate=45 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=61/70  Signal level=-49 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:11   Missed beacon:0

┌──(root㉿kali)-[/home/shariful]
```



```
┌──(root㉿kali)-[/home/shariful]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[/home/shariful]
└─# iwconfig wlan0 mode monitor

┌──(root㉿kali)-[/home/shariful]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[/home/shariful]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm

          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(root㉿kali)-[/home/shariful]
└─# █
```

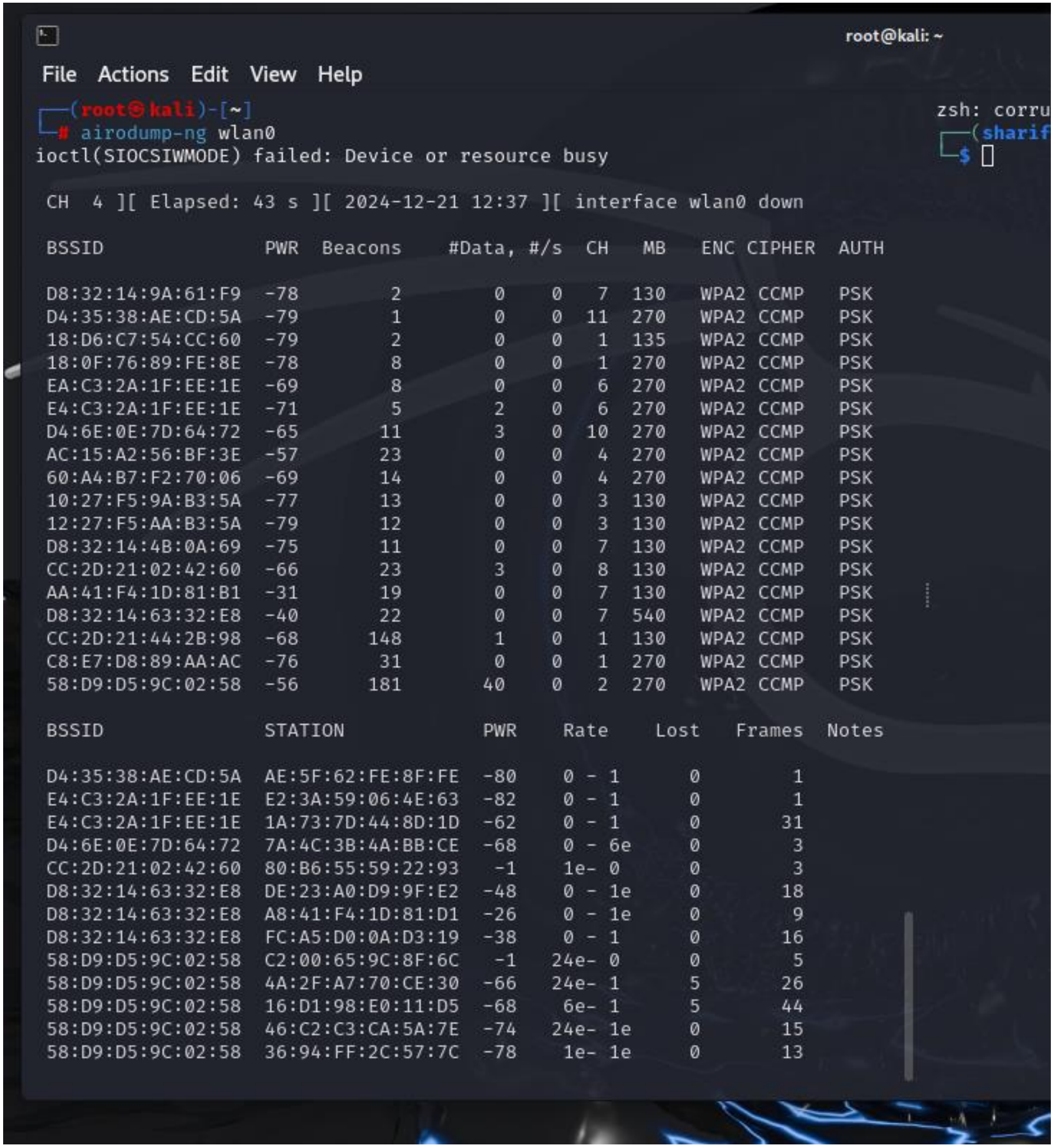
Here is the another way to start monitor mode just type **airmon-ng start wlan0**



```
┌──(root㉿kali)-[/home/shariful]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    691 NetworkManager
   3514 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Ralink Technology, Corp. MT7601U
                (monitor mode enabled)
```

Now monitor mode is on.

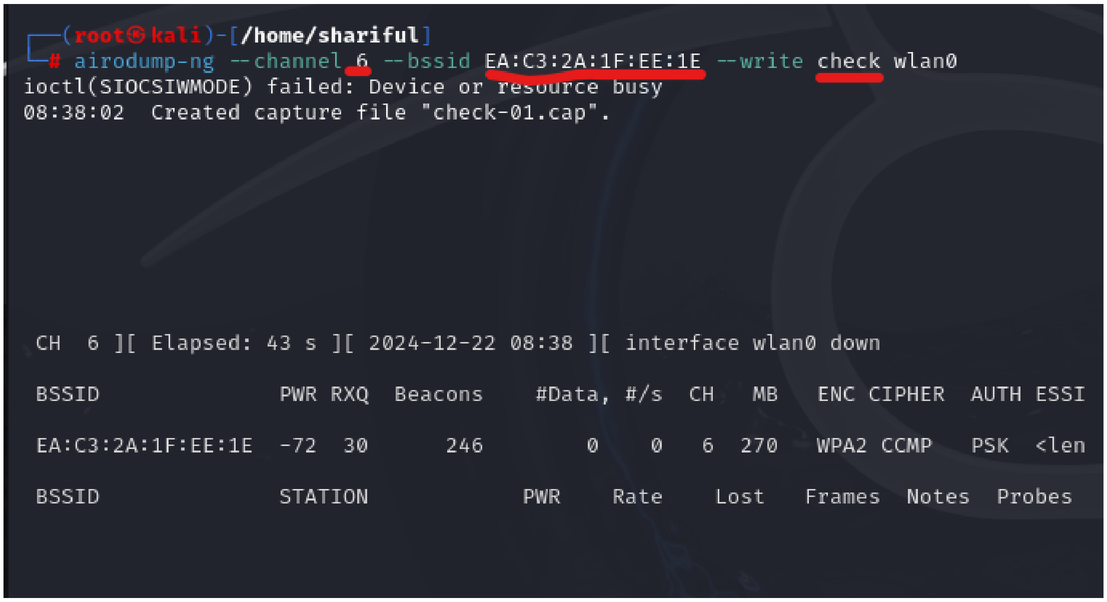
Here is the different type of network around me.



```
┌──(root㉿kali)-[~]
└─# airodump-ng wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy

 CH  4 ][ Elapsed: 43 s ][ 2024-12-21 12:37 ][ interface wlan0 down

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

 D8:32:14:9A:61:F9  -78        2        0    0   7  130   WPA2 CCMP   PSK
 D4:35:38:AE:CD:5A  -79        1        0    0  11  270   WPA2 CCMP   PSK
 18:D6:C7:54:CC:60  -79        2        0    0   1  135   WPA2 CCMP   PSK
 18:0F:76:89:FE:8E  -78        8        0    0   1  270   WPA2 CCMP   PSK
 EA:C3:2A:1F:EE:1E  -69        8        0    0   6  270   WPA2 CCMP   PSK
 E4:C3:2A:1F:EE:1E  -71        5        2    0   6  270   WPA2 CCMP   PSK
 D4:6E:0E:7D:64:72  -65       11        3    0  10  270   WPA2 CCMP   PSK
 AC:15:A2:56:BF:3E  -57       23        0    0   4  270   WPA2 CCMP   PSK
 60:A4:B7:F2:70:06  -69       14        0    0   4  270   WPA2 CCMP   PSK
 10:27:F5:9A:B3:5A  -77       13        0    0   3  130   WPA2 CCMP   PSK
 12:27:F5:AA:B3:5A  -79       12        0    0   3  130   WPA2 CCMP   PSK
 D8:32:14:4B:0A:69  -75       11        0    0   7  130   WPA2 CCMP   PSK
 CC:2D:21:02:42:60  -66       23        3    0   8  130   WPA2 CCMP   PSK
 AA:41:F4:1D:81:B1  -31       19        0    0   7  130   WPA2 CCMP   PSK
 D8:32:14:63:32:E8  -40       22        0    0   7  540   WPA2 CCMP   PSK
 CC:2D:21:44:2B:98  -68      148        1    0   1  130   WPA2 CCMP   PSK
 C8:E7:D8:89:AA:AC  -76       31        0    0   1  270   WPA2 CCMP   PSK
 58:D9:D5:9C:02:58  -56      181       40    0   2  270   WPA2 CCMP   PSK

 BSSID              STATION            PWR    Rate    Lost   Frames  Notes

 D4:35:38:AE:CD:5A  AE:5F:62:FE:8F:FE  -80    0 - 1      0        1
 E4:C3:2A:1F:EE:1E  E2:3A:59:06:4E:63  -82    0 - 1      0        1
 E4:C3:2A:1F:EE:1E  1A:73:7D:44:8D:1D  -62    0 - 1      0       31
 D4:6E:0E:7D:64:72  7A:4C:3B:4A:BB:CE  -68    0 - 6e     0        3
 CC:2D:21:02:42:60  80:B6:55:59:22:93   -1    1e- 0      0        3
 D8:32:14:63:32:E8  DE:23:A0:D9:9F:E2  -48    0 - 1e     0       18
 D8:32:14:63:32:E8  A8:41:F4:1D:81:D1  -26    0 - 1e     0        9
 D8:32:14:63:32:E8  FC:A5:D0:0A:D3:19  -38    0 - 1      0       16
 58:D9:D5:9C:02:58  C2:00:65:9C:8F:6C   -1   24e- 0      0        5
 58:D9:D5:9C:02:58  4A:2F:A7:70:CE:30  -66   24e- 1      5       26
 58:D9:D5:9C:02:58  16:D1:98:E0:11:D5  -68    6e- 1      5       44
 58:D9:D5:9C:02:58  46:C2:C3:CA:5A:7E  -74   24e- 1e     0       15
 58:D9:D5:9C:02:58  36:94:FF:2C:57:7C  -78    1e- 1e     0       13
```

```
zsh: corru
┌──(sharif
└─$
```

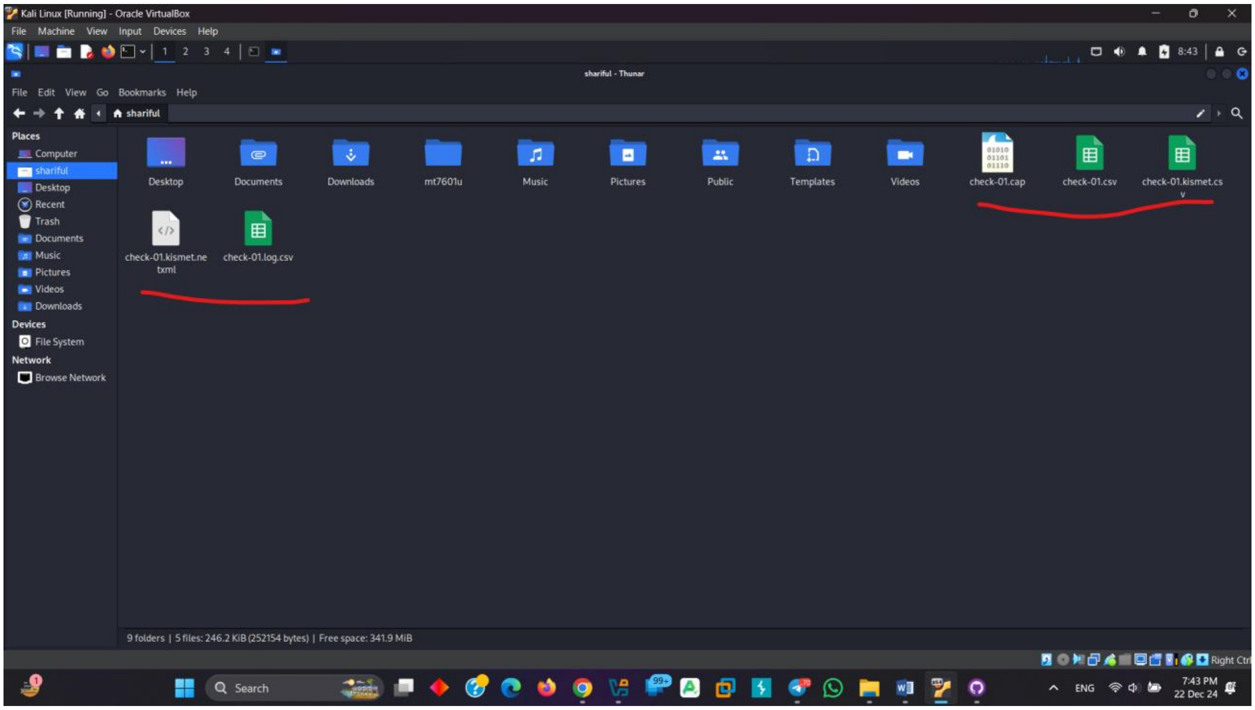
Gather information within a particular BSSID: **airodump-ng --channel 6 --bssid EA:C3:2A:1F:EE:1E --write check wlan0**



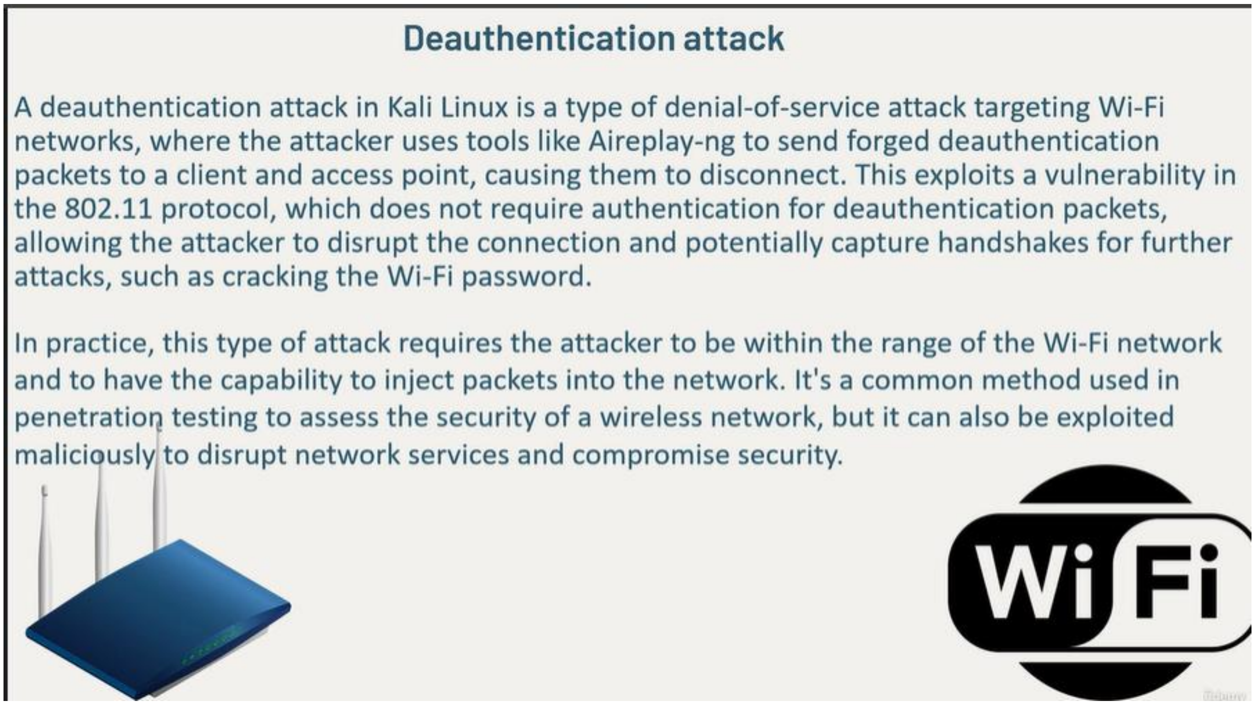
```
┌──(root㉿kali)-[/home/shariful]
└─# airodump-ng --channel 6 --bssid EA:C3:2A:1F:EE:1E --write check wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy
08:38:02  Created capture file "check-01.cap".



 CH  6 ][ Elapsed: 43 s ][ 2024-12-22 08:38 ][ interface wlan0 down

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

 EA:C3:2A:1F:EE:1E  -72  30      246        0    0   6  270   WPA2 CCMP   PSK  <len

 BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes
```

Here 6 is the channel 6, then target BSSID and check is the folder name.

Open the root directory and discover new file:



Deauthentication Att@ck:



Deauthentication attack

A deauthentication attack in Kali Linux is a type of denial-of-service attack targeting Wi-Fi networks, where the attacker uses tools like Aireplay-ng to send forged deauthentication packets to a client and access point, causing them to disconnect. This exploits a vulnerability in the 802.11 protocol, which does not require authentication for deauthentication packets, allowing the attacker to disrupt the connection and potentially capture handshakes for further attacks, such as cracking the Wi-Fi password.

In practice, this type of attack requires the attacker to be within the range of the Wi-Fi network and to have the capability to inject packets into the network. It's a common method used in penetration testing to assess the security of a wireless network, but it can also be exploited maliciously to disrupt network services and compromise security.

Important command

sudo chmod -R 777 /root →give the read write permission

ls example-upc* →find any file

airodump-ng --channel 6 --bssid E4:C3:2A:1F:EE:1E --write example-upc wlan0 →here wxample-upc is the file name.

airodump-ng wlan0 →show the available wifi around me