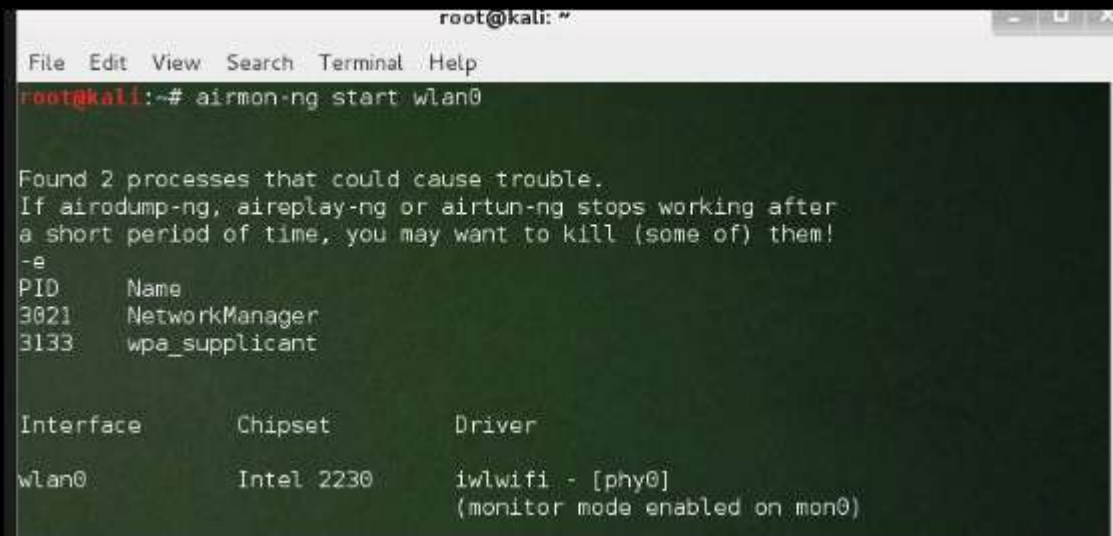


Wireless Attacks-Kismet

Kismet is a WIFI network analyzing tool. It is a 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11a/b/g/n traffic. It identifies the networks by collecting packets and also hidden networks.

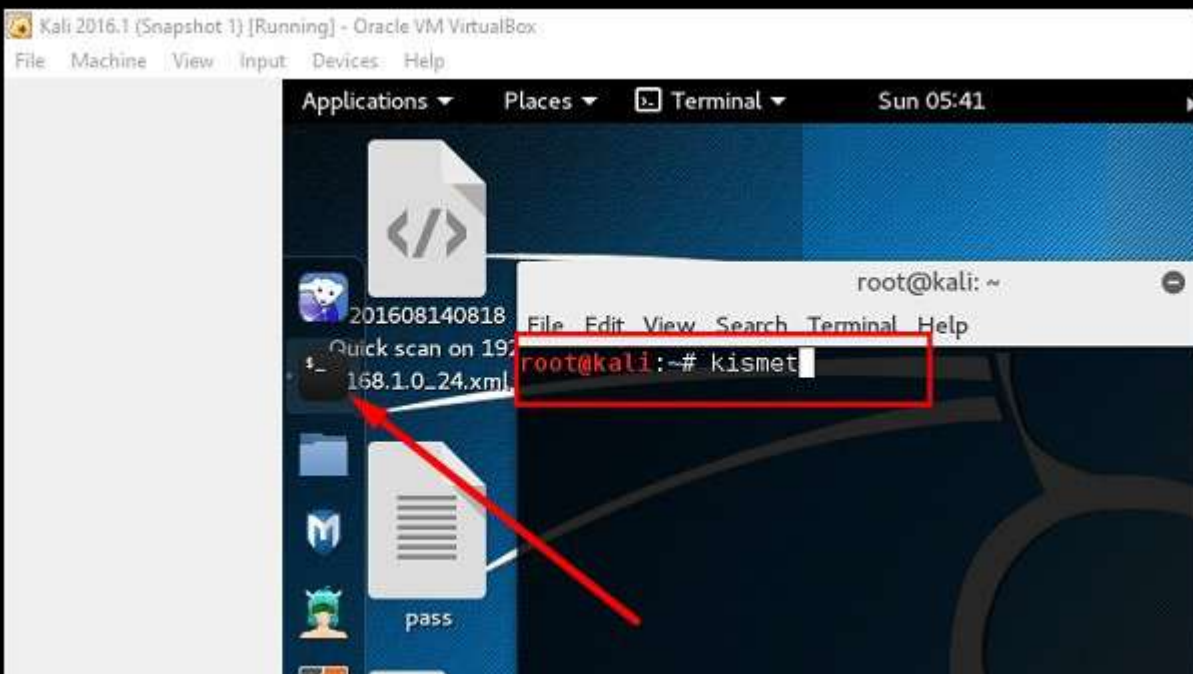
To use it, turn the wireless card into monitoring mode and to do this, type “airmon-ng start wlan0” in the terminal.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng start wlan0  
  
Found 2 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
-e  
PID      Name  
3021     NetworkManager  
3133     wpa_supplicant  
  
Interface      Chipset      Driver  
wlan0          Intel 2230    iwlwifi - [phy0]  
              (monitor mode enabled on mon0)
```

Let's learn how to use this tool.

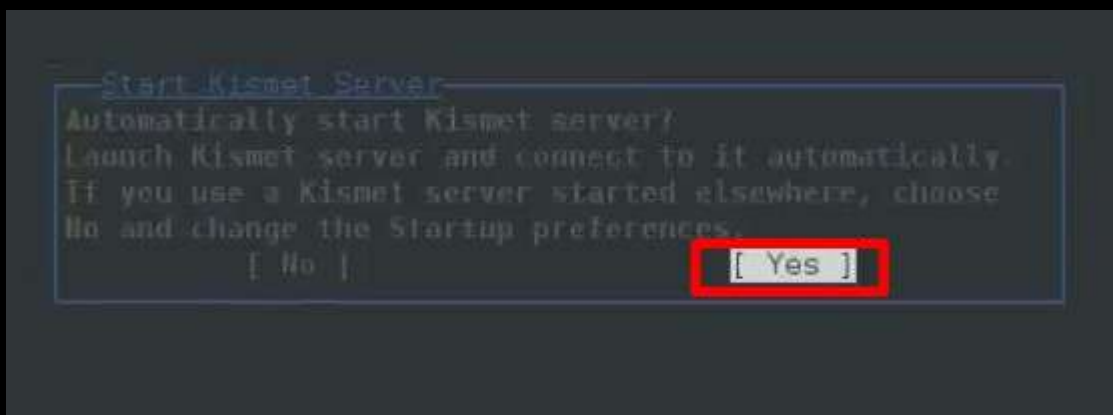
Step 1 – To launch it, open terminal and type “kismet”.



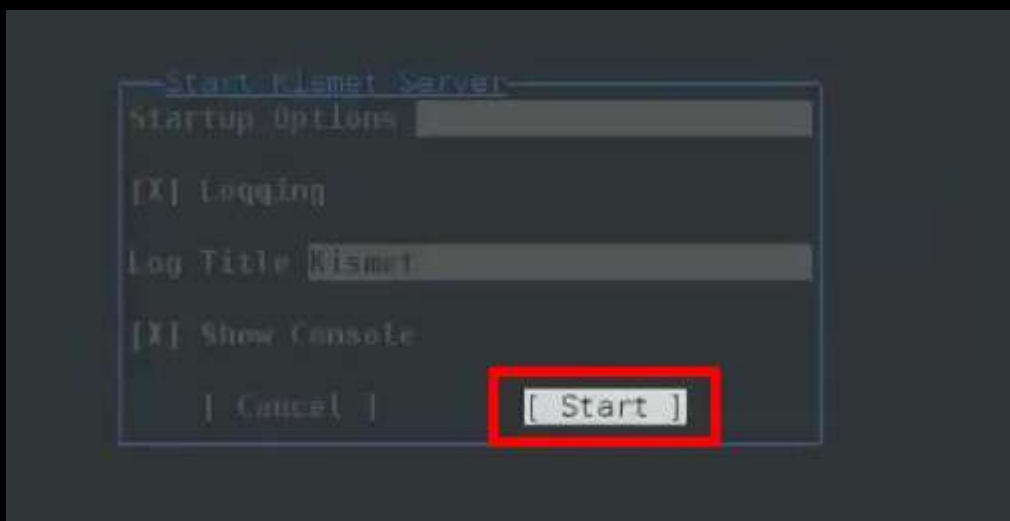
Step 2 – Click “OK”.



Step 3 – Click “Yes” when it asks to start Kismet Server. Otherwise it will stop functioning.



Step 4 – Startup Options, leave as default. Click “Start”.



Step 5 – Now it will show a table asking you to define the wireless card. In such case, click Yes.

```

root@kali: ~
File Edit View Search Terminal Help
Kismet Server Console
ERROR: Could not open OUI file '/etc/manuf': No such file or directory
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
INFO: Creatin
INFO: Register
INFO: Pcap lo
INFO: Opened
INFO: Opened
INFO: Opened
INFO: Opened
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
(/etc/kismet/kismet.conf)
INFO: Kismet server accepted connection from 127.0.0.1

[ Kill Server ] [ Close Console Window ]

```

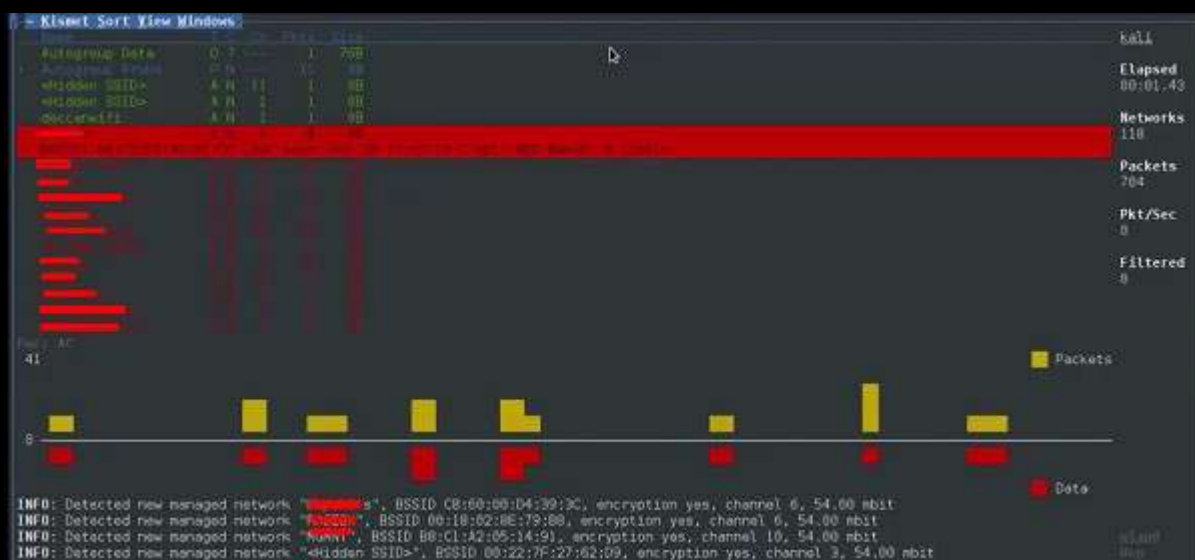
Step 6 – In this case, the wireless source is “wlan0”. It will have to be written in the section “Intf” → click “Add”.

```

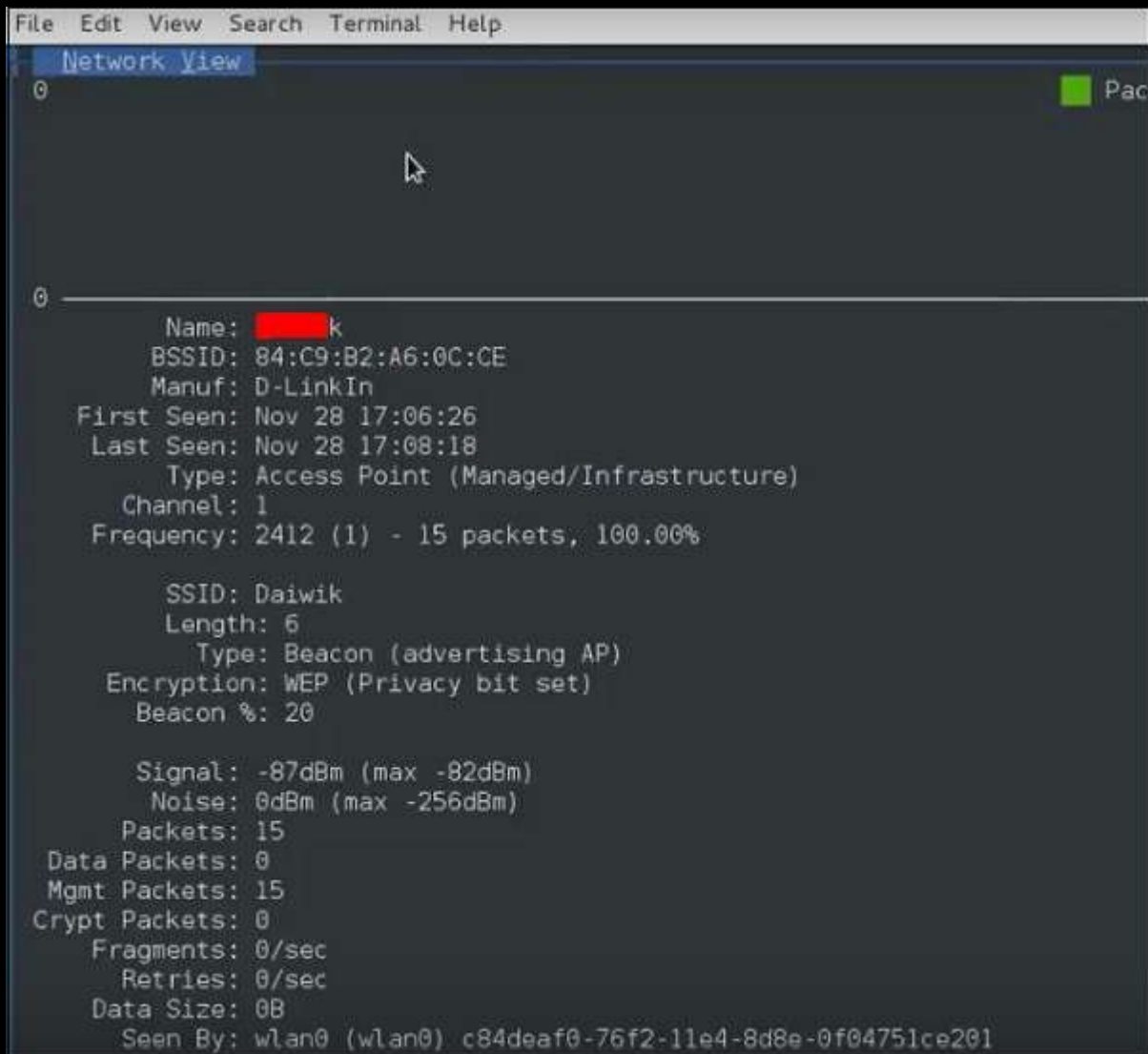
ng manufacturer db
ted indexing manufacturer db, 27350 lines 547 indexes
ng netw
ng chan
nering d
og in P
pcapdu
netxml
nettxt
gpsxml
alert
starti
ket sources defined. You MUST ADD SOME using the Kismet
, or by placing them in the Kismet config file
kismet/kismet.conf)

```

Step 7 – It will start sniffing the wifi networks as shown in the following screenshot.



Step 8 – Click on any network, it produces the wireless details as shown in the following screenshot.



The screenshot shows a window titled "Network View" with a menu bar (File, Edit, View, Search, Terminal, Help). The window displays details for a selected network. The details are as follows:

```
Name: [REDACTED]k
BSSID: 84:C9:B2:A6:0C:CE
Manuf: D-LinkIn
First Seen: Nov 28 17:06:26
Last Seen: Nov 28 17:08:18
Type: Access Point (Managed/Infrastructure)
Channel: 1
Frequency: 2412 (1) - 15 packets, 100.00%

SSID: Daiwik
Length: 6
Type: Beacon (advertising AP)
Encryption: WEP (Privacy bit set)
Beacon %: 20

Signal: -87dBm (max -82dBm)
Noise: 0dBm (max -256dBm)
Packets: 15
Data Packets: 0
Mgmt Packets: 15
Crypt Packets: 0
Fragments: 0/sec
Retries: 0/sec
Data Size: 0B
Seen By: wlan0 (wlan0) c84deaf0-76f2-11e4-8d8e-0f04751ce201
```