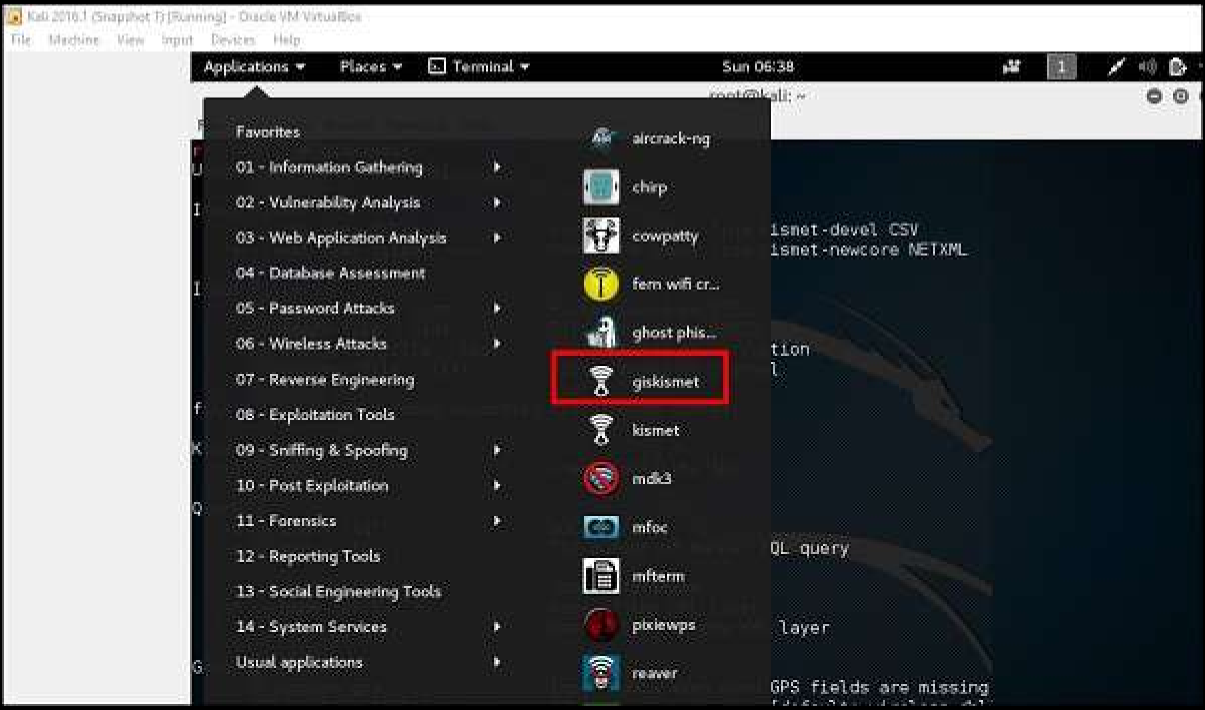
Wireless Attacks-GISKismet

GISKismet is a wireless visualization tool to represent data gathered using Kismet in a practical way. GISKismet stores the information in a database so we can query data and generate graphs using SQL. GISKismet currently uses SQLite for the database and GoogleEarth / KML files for graphing.

Let’s learn how to use this tool.

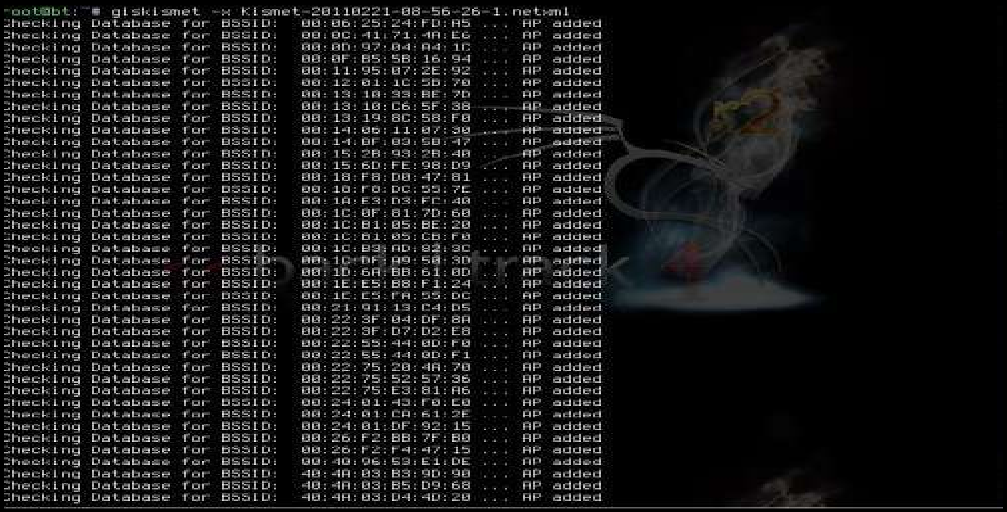
Step 1 – To open GISKismet, go to: Applications → Click “Wireless Attacks” → giskismet.



```
ismet-devel CSV
ismet-newcore NETXML

tion
l

QL query

 layer

GPS fields are missing
```

As you remember in the previous section, we used Kismet tool to explore data about wireless networks and all this data Kismet packs in netXML files.

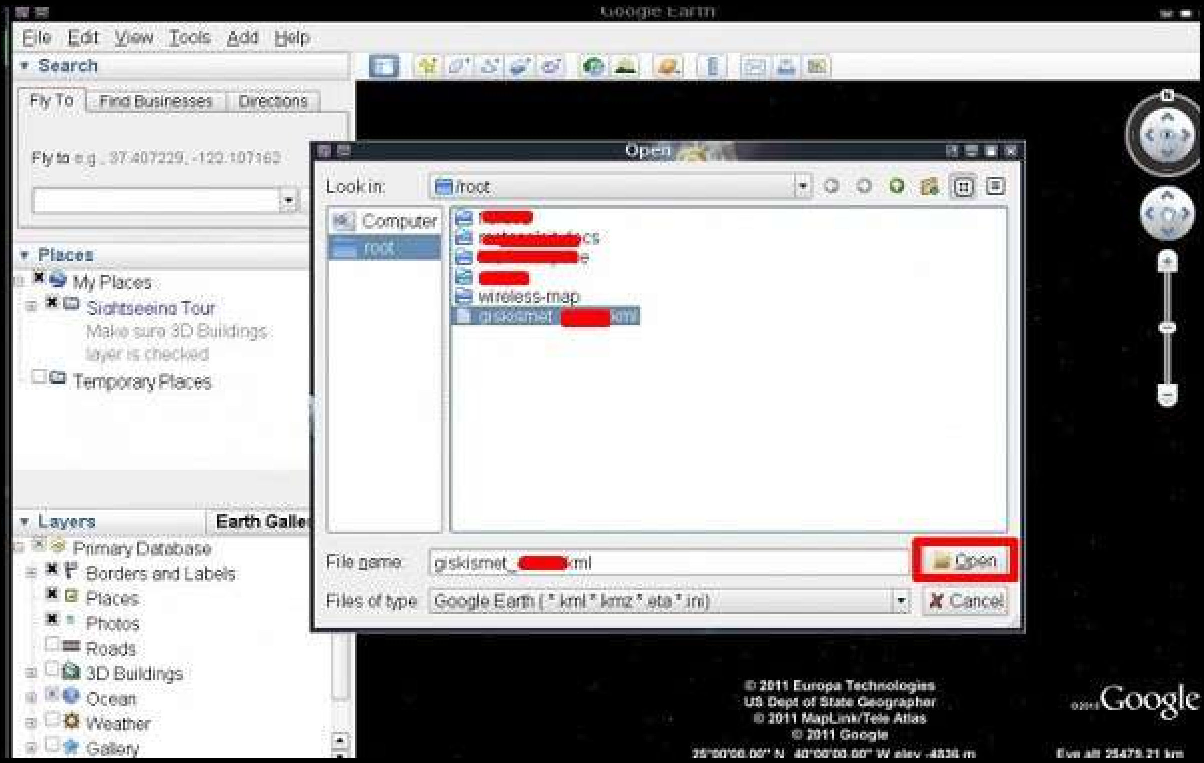
Step 2 – To import this file into Giskismet, type “root@kali:~# giskismet -x Kismetfilename.netxml” and it will start importing the files.



```
root@bt:~# giskismet -x Kismet-20110221-08-56-26-1.netxml
Checking Database for BSSID:  00:06:25:24:FD:A5 ... AP added
Checking Database for BSSID:  00:0C:41:71:4A:E6 ... AP added
Checking Database for BSSID:  00:0D:97:04:A4:1C ... AP added
Checking Database for BSSID:  00:0F:B5:5B:16:94 ... AP added
Checking Database for BSSID:  00:11:95:07:2E:92 ... AP added
Checking Database for BSSID:  00:12:01:1C:5D:70 ... AP added
Checking Database for BSSID:  00:13:10:33:BE:7D ... AP added
Checking Database for BSSID:  00:13:10:C6:5F:38 ... AP added
Checking Database for BSSID:  00:13:19:8C:58:F0 ... AP added
Checking Database for BSSID:  00:14:06:11:07:30 ... AP added
Checking Database for BSSID:  00:14:BF:03:5B:47 ... AP added
Checking Database for BSSID:  00:15:2B:93:2B:40 ... AP added
Checking Database for BSSID:  00:15:6D:FE:98:D9 ... AP added
Checking Database for BSSID:  00:18:F8:D0:47:81 ... AP added
Checking Database for BSSID:  00:18:F0:DC:55:7E ... AP added
Checking Database for BSSID:  00:1A:E3:D3:FC:40 ... AP added
Checking Database for BSSID:  00:1C:0F:81:7D:60 ... AP added
Checking Database for BSSID:  00:1C:B1:05:BE:20 ... AP added
Checking Database for BSSID:  00:1C:B1:05:C6:F0 ... AP added
Checking Database for BSSID:  00:1C:B3:AD:82:3C ... AP added
Checking Database for BSSID:  00:1C:DF:A9:58:3D ... AP added
Checking Database for BSSID:  00:1D:6A:BB:61:0D ... AP added
Checking Database for BSSID:  00:1E:E5:B8:F1:24 ... AP added
Checking Database for BSSID:  00:1E:E5:FA:55:DC ... AP added
Checking Database for BSSID:  00:21:91:13:C4:D5 ... AP added
Checking Database for BSSID:  00:22:3F:04:DF:8A ... AP added
Checking Database for BSSID:  00:22:3F:D7:D2:E8 ... AP added
Checking Database for BSSID:  00:22:55:44:0D:F0 ... AP added
Checking Database for BSSID:  00:22:55:44:0D:F1 ... AP added
Checking Database for BSSID:  00:22:75:20:4A:70 ... AP added
Checking Database for BSSID:  00:22:75:52:57:36 ... AP added
Checking Database for BSSID:  00:22:75:E3:81:A6 ... AP added
Checking Database for BSSID:  00:24:01:43:F0:E0 ... AP added
Checking Database for BSSID:  00:24:01:CA:61:2E ... AP added
Checking Database for BSSID:  00:24:01:DF:92:15 ... AP added
Checking Database for BSSID:  00:26:F2:BB:7F:B0 ... AP added
Checking Database for BSSID:  00:26:F2:F4:47:15 ... AP added
Checking Database for BSSID:  00:40:96:53:E1:DE ... AP added
Checking Database for BSSID:  40:4A:03:B3:9D:98 ... AP added
Checking Database for BSSID:  40:4A:03:B5:D9:68 ... AP added
Checking Database for BSSID:  40:4A:03:D4:4D:20 ... AP added
```

Once imported, we can import them to Google Earth the Hotspots that we found before.

Step 3 – Assuming that we have already installed Google Earth, we click File → Open File that Giskismet created → Click "Open".



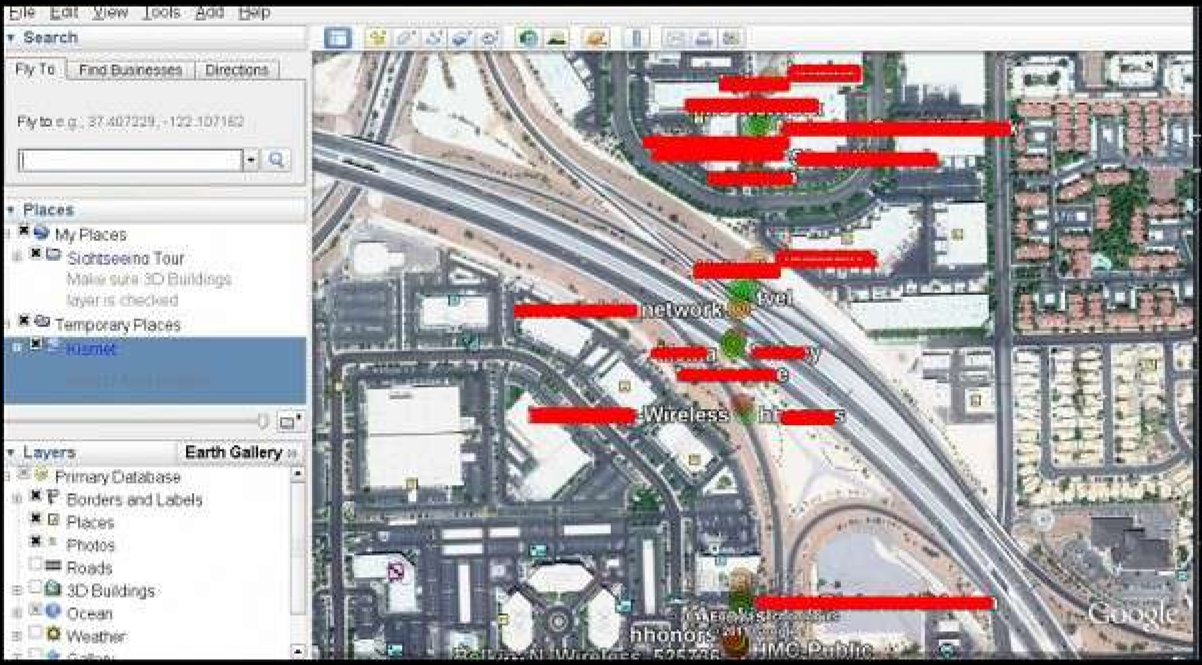
Look in: /root

[redacted]
[redacted]cs
[redacted]e
[redacted]
wireless-map
giskismet_[redacted]kml

File name: giskismet_[redacted]kml

Files of type: Google Earth (*.kml *.kmz *.eta *.ini)

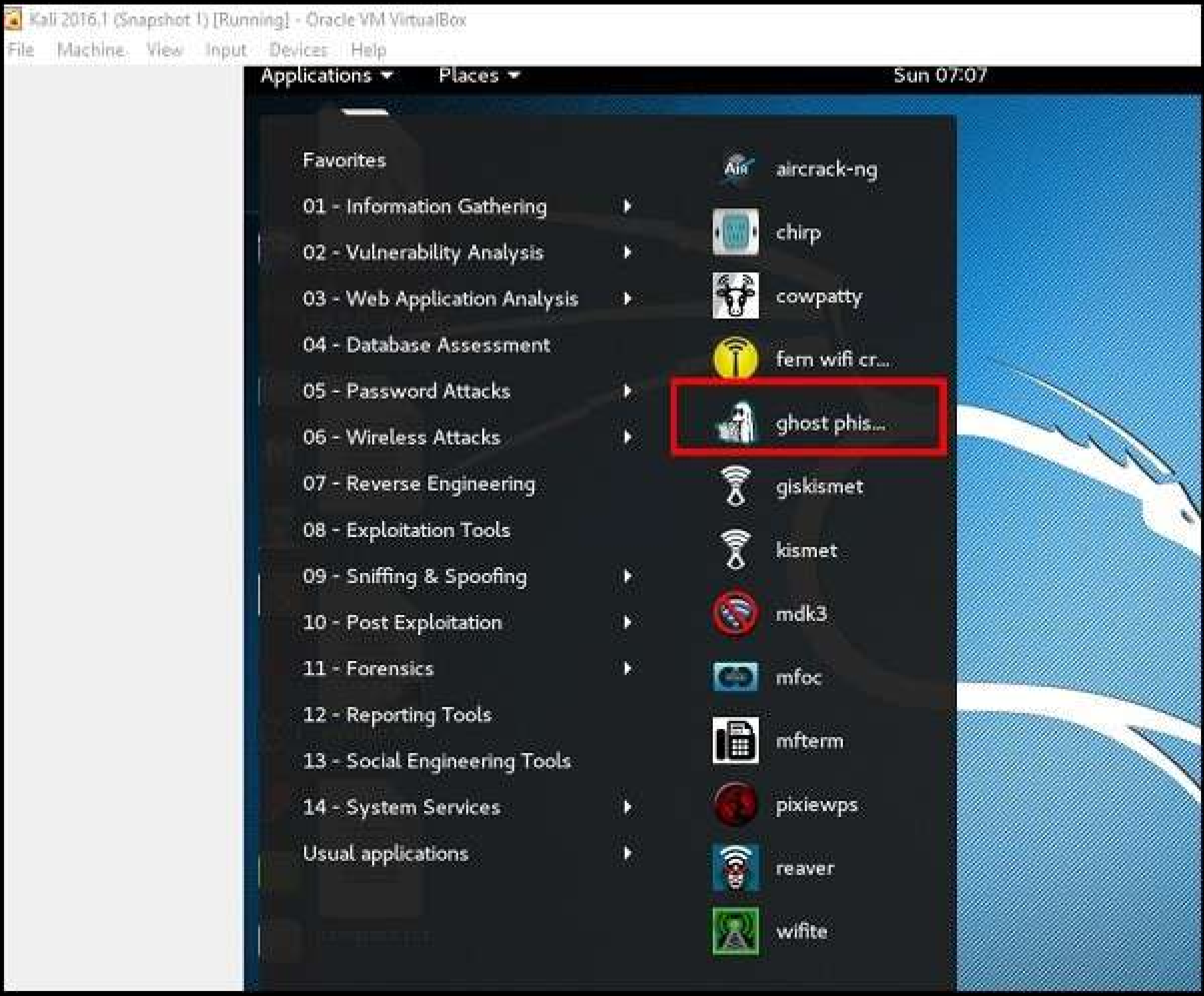
The following map will be displayed.



Ghost Phisher

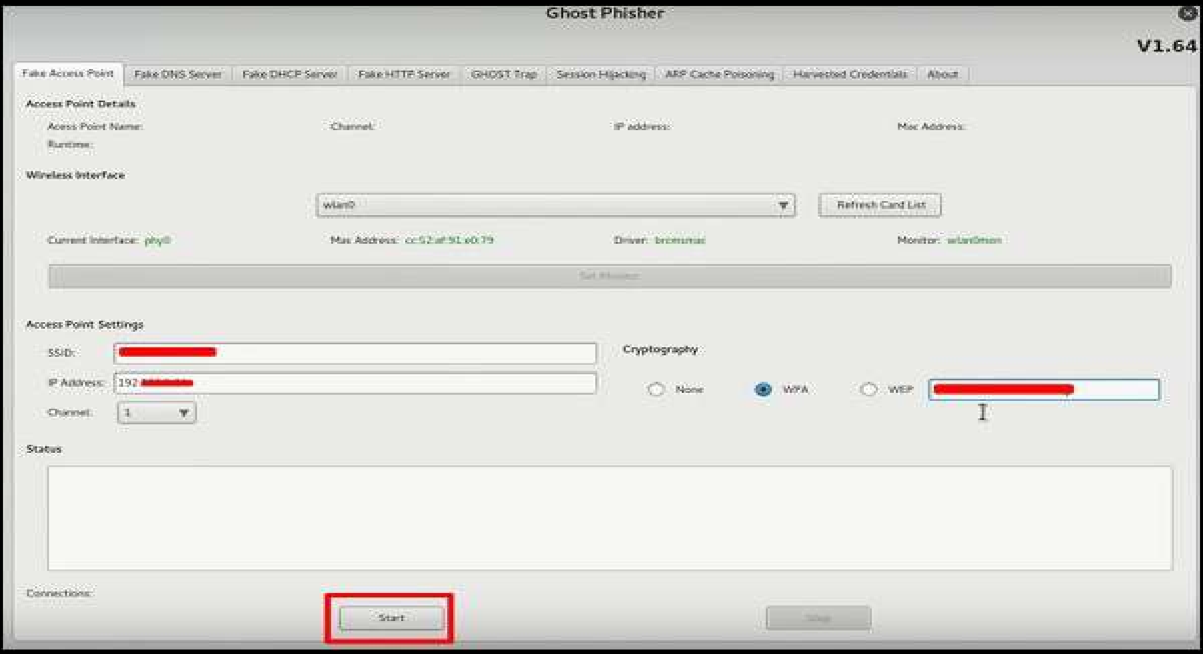
Ghost Phisher is a popular tool that helps to create fake wireless access points and then later to create Man-in-The-Middle-Attack.

Step 1 – To open it, click Applications → Wireless Attacks → “ghost phishing”.



Step 2 – After opening it, we will set up the fake AP using the following details.

- Wireless Interface Input: wlan0
- SSID: wireless AP name
- IP address: IP that the AP will have
- WAP: Password that will have this SSID to connect



Access Point Details

Acess Point Name: Channel: IP address: Mac Address:
Runtime:

Wireless Interface

wlan0

Current Interface: phy0 Mac Address: cc:52:af:91:e0:79 Driver: brcmsmac Monitor: wlan0mon

Access Point Settings

SSID: [redacted]

IP Address: 192 [redacted]

Channel: 1

Cryptography

○ None ● WPA ○ WEP [redacted]

Status

Connections:

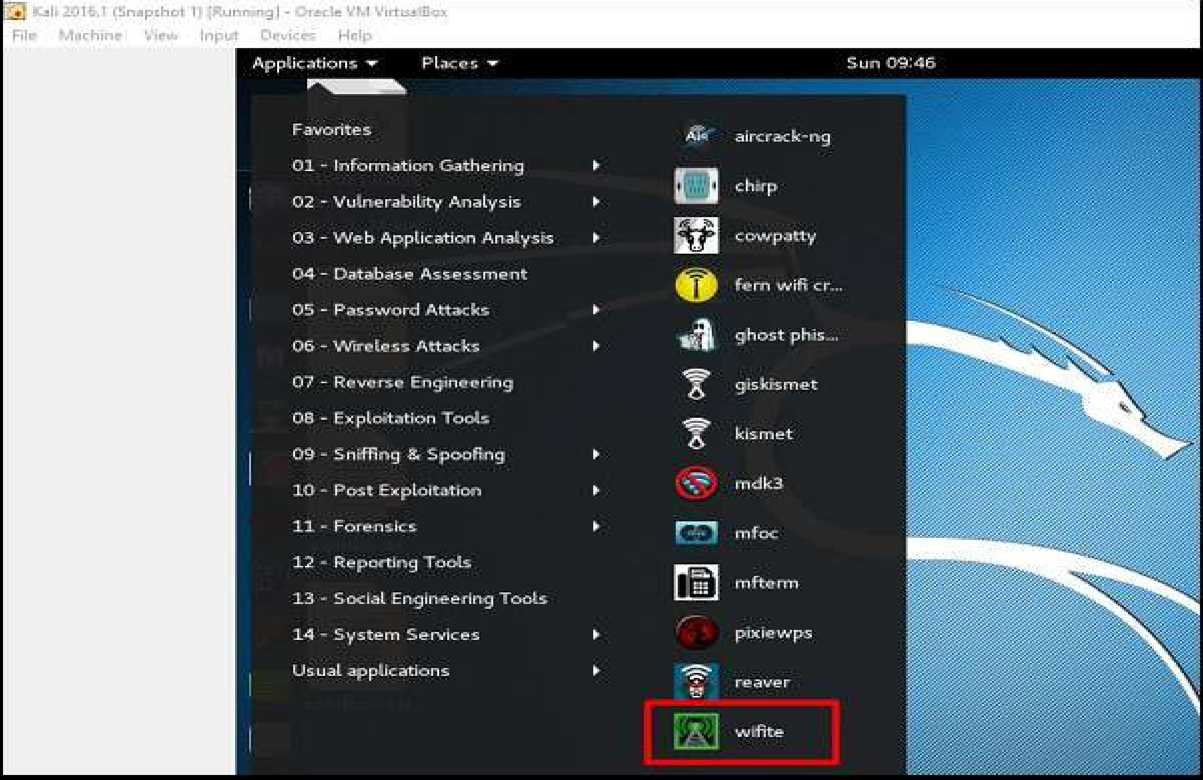
Step 3 – Click the **Start** button.

Wifite

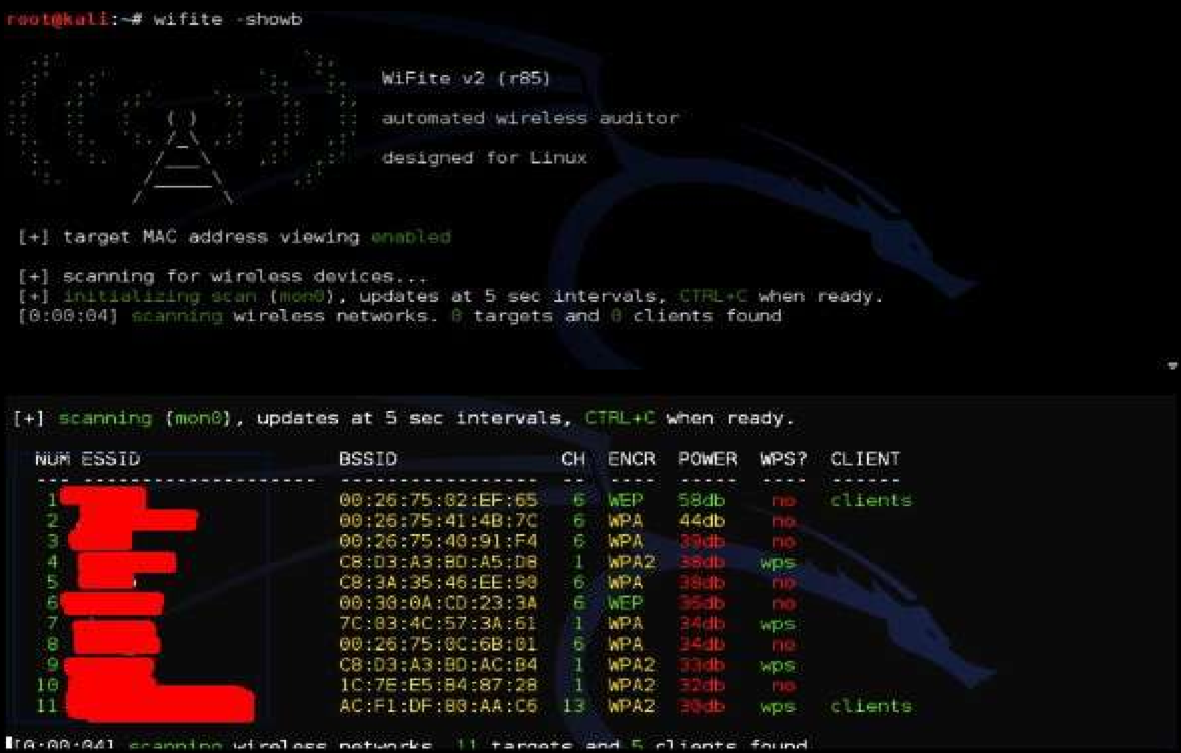
It is another wireless clacking tool, which attacks multiple WEP, WPA, and WPS encrypted networks in a row.

Firstly, the wireless card has to be in the monitoring mode.

Step 1 – To open it, go to Applications → Wireless Attack → Wifite.



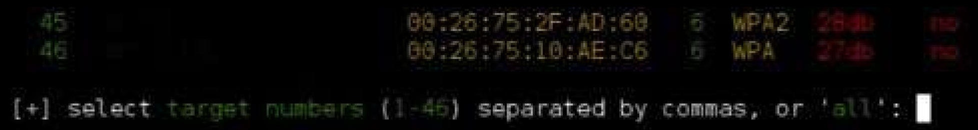
Step 2 – Type **"wifite –showb"**to scan for the networks.



```
root@kali:~# wifite -showb

                                    WiFite v2 (r85)

                                    automated wireless auditor

                                    designed for Linux

 [+] target MAC address viewing enabled

 [+] scanning for wireless devices...
 [+] initializing scan (mon0), updates at 5 sec intervals, CTRL+C when ready.
 [0:00:04] scanning wireless networks. 0 targets and 0 clients found
```

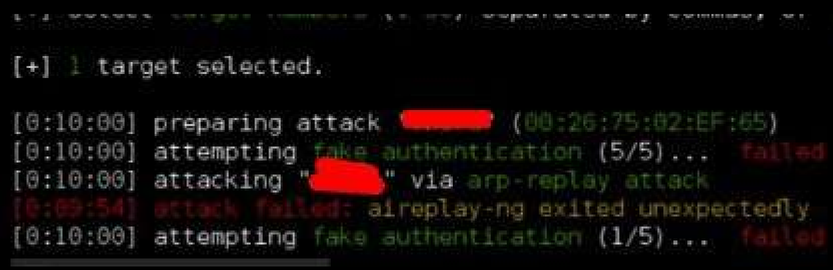
```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

  NUM ESSID                  BSSID              CH  ENCR  POWER  WPS?  CLIENT
  --- --------------------   -----------------  --  ----  -----  ----  ------
    1 [redacted]             00:26:75:02:EF:65   6  WEP   58db    no   clients
    2 [redacted]             00:26:75:41:4B:7C   6  WPA   44db    no
    3 [redacted]             00:26:75:40:91:F4   6  WPA   39db    no
    4 [redacted]             C8:D3:A3:BD:A5:D8   1  WPA2  38db   wps
    5 [redacted]             C8:3A:35:46:EE:90   6  WPA   38db    no
    6 [redacted]             00:30:0A:CD:23:3A   6  WEP   35db    no
    7 [redacted]             7C:03:4C:57:3A:61   1  WPA   34db   wps
    8 [redacted]             00:26:75:0C:6B:01   6  WPA   34db    no
    9 [redacted]             C8:D3:A3:BD:AC:B4   1  WPA2  33db   wps
   10 [redacted]             1C:7E:E5:84:87:28   1  WPA2  32db    no
   11 [redacted]             AC:F1:DF:B0:AA:C6  13  WPA2  30db   wps   clients
[0:00:04] scanning wireless networks. 11 targets and 5 clients found
```

Step 3 – To start attacking the wireless networks, click Ctrl + C.



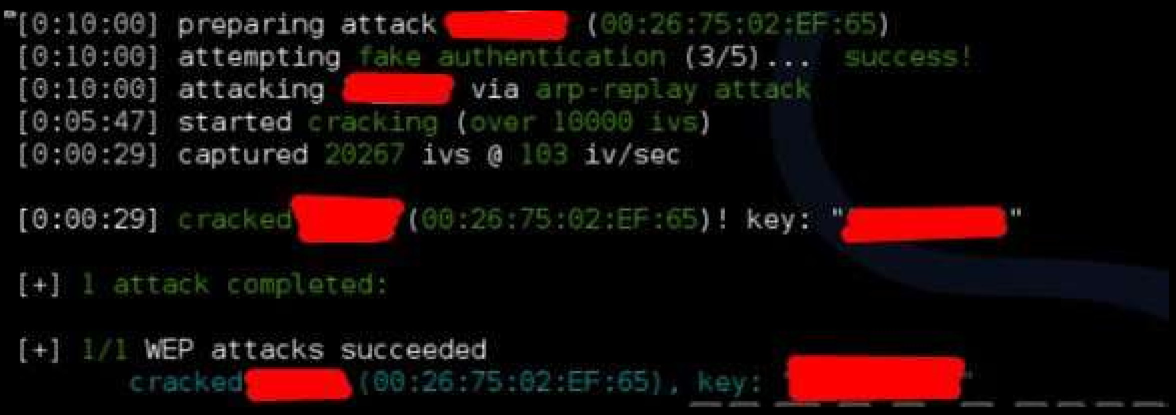
```
  45                          00:26:75:2F:AD:60   6  WPA2  28db   no
  46                          00:26:75:10:AE:C6   6  WPA   27db   no

 [+] select target numbers (1-46) separated by commas, or 'all': █
```

Step 4 – Type “1” to crack the first wireless.



```
 [+] select target numbers (1-46) separated by commas, or 'all': 1

 [+] 1 target selected.

 [0:10:00] preparing attack [redacted] (00:26:75:02:EF:65)
 [0:10:00] attempting fake authentication (5/5)...  failed
 [0:10:00] attacking "[redacted]" via arp-replay attack
 [0:09:54] attack failed: aireplay-ng exited unexpectedly
 [0:10:00] attempting fake authentication (1/5)...  failed
```

Step 5 – After attacking is complete, the key will be found.



```
 [0:10:00] preparing attack [redacted] (00:26:75:02:EF:65)
 [0:10:00] attempting fake authentication (3/5)...  success!
 [0:10:00] attacking [redacted] via arp-replay attack
 [0:05:47] started cracking (over 10000 ivs)
 [0:00:29] captured 20267 ivs @ 103 iv/sec

 [0:00:29] cracked [redacted] (00:26:75:02:EF:65)! key: "[redacted]"

 [+] 1 attack completed:

 [+] 1/1 WEP attacks succeeded
        cracked [redacted] (00:26:75:02:EF:65), key: "[redacted]"
```