

# Examine Pass-codes in PCAPs' - Using aircrack-ng (Wi-Fi Forensic)

## Aircrack-ng

Aircrack-ng includes a set of tools to perform Wi-Fi network hacking.

**Monitoring:** Packet capture and export of data to text files for further processing by third-party tools.

**Attacking:** Replay attacks, deauthentication, fake access points and others via packet injection.

**Testing:** Checking Wi-Fi cards and driver capabilities (capture and injection).

**Cracking:** WEP and WPA PSK (WPA 1 and 2).

## Some Important Terminology:

Bssid :- Mac Address of The Access Point

Essid :- Name of The Access Point

Ch :- Channel Number of Access Point

Data :- Data Packets Transferred

Beacons :- Advertisement Packets Sent by Access Point

Pwr :- Signal Strength of Access Point

Auth :- Encryption Used by The Access Point

Cipher :- Encryption Cipher Used by The Access Point

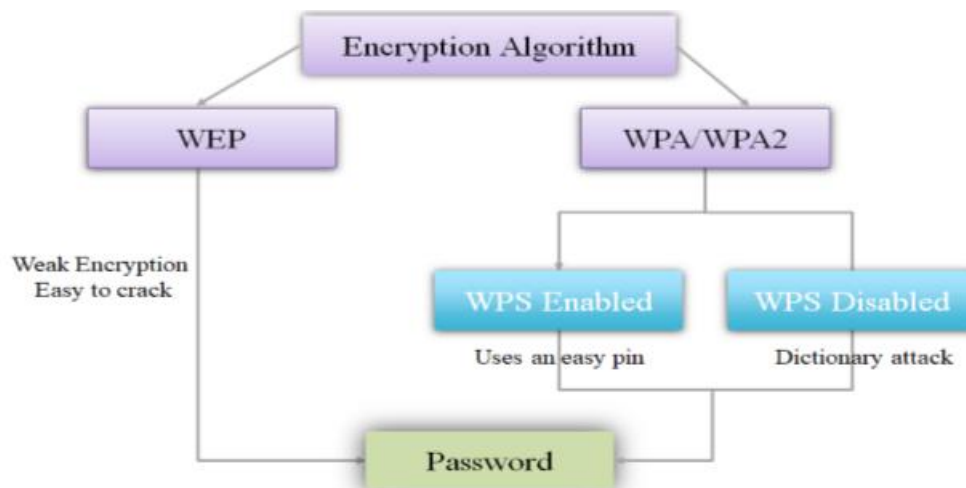
## Examine PCAP for Pass-code:

Capturing WPA packets is not useful as they do not contain any info that can be used to examine the pass-code. The only packet that contains info that helps us examine the pass-code is the handshake packets.

Every time a client connects to that AP a four-way handshake occurs between the client and the Access Point. By capturing the handshake, we can use aircrack-ng to launch a word list attack

against the handshake to determine the Pass-code. To crack a WPA/WPA2 AP with WPS disabled, we need two things:

1. Capture the Handshake
2. A word-list / Expression for Password try



## Procedure:

We have captured handshake and it is stored in .pcap file. This .pcap file can we examine for pass-code with or without word-list.

The word-list is a list of numerous combinations of words created using characters, numbers and special characters.

### With Word-list

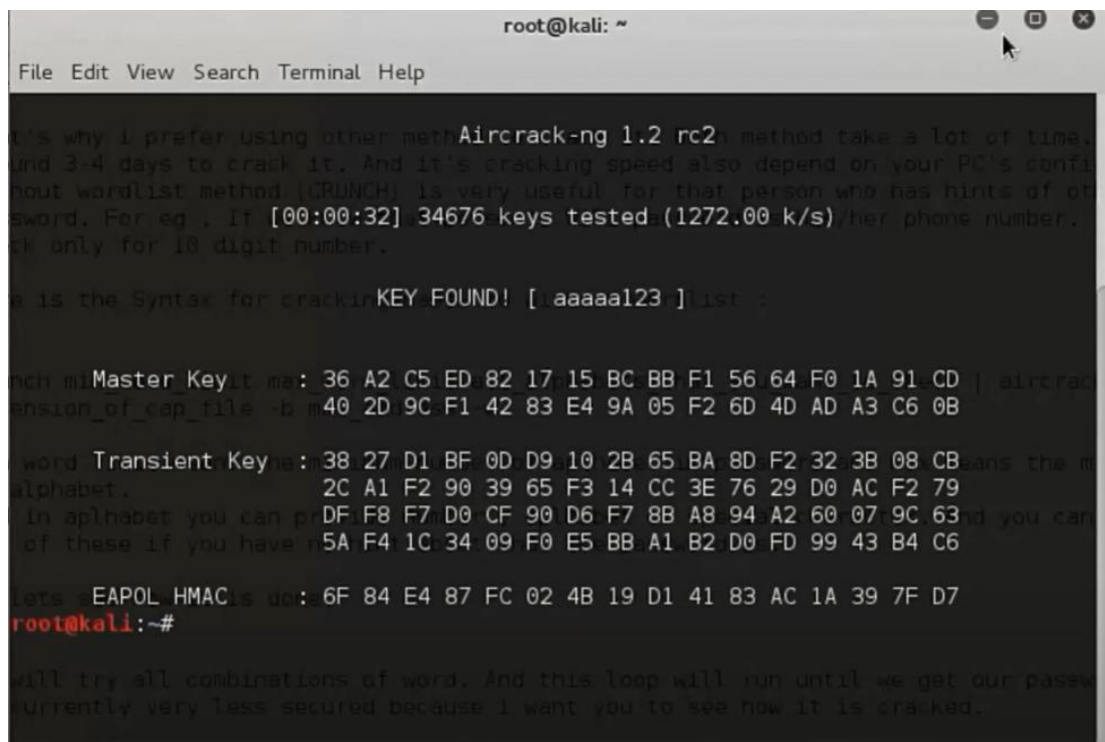
Syntax: `aircrack-ng pcap_file -w word_list`

The above command will try to match the list of words contain by word-list with the actual WIFI pass-code. If it will be matched then it will display that word on the screen as shown in figure-01.

**Without Word-list** (Using Crunch : Crunch is a word-list generator where you can specify a standard character set or a character set you specify. crunch can generate all possible combinations and permutations.)(Time saving method if we have some hint about pass-code)

Syntax: `crunch min_word_limit max_word_limit  
all_alphabets_that_you_want_to_check | aircrack-ng pcap_file -b  
mac_addr -w-`

The above command will try to match the list of words generated from mentioned criteria with the actual WIFI pass-code. If it will be matched then it will display that word on the screen as shown in figure-01.



```
root@kali: ~  
File Edit View Search Terminal Help  
It's why I prefer using other meth  
Aircrack-ng 1.2 rc2h method take a lot of time,  
and 3-4 days to crack it. And it's cracking speed also depend on your PC's confi  
out wordlist method (CRUNCH) is very useful for that person who has hints of et  
sword. For eg , If [00:00:32] 34676 keys tested (1272.00 k/s) her phone number.  
ok only for 10 digit number.  
is the Syntax for crackin  
KEY FOUND! [ aaaaa123 ]list :  
Master Keyit ma: 36 A2 C5 ED 82 17 15 BC BB F1 56 64 F0 1A 91 CD | aircrac  
nsion_of_cap_file -b m40 2D 9C F1 42 83 E4 9A 05 F2 6D 4D AD A3 C6 0B  
word Transient Key is: 38 27 D1 BF 0D D9 10 2B 65 BA 8D F2 32 3B 08 CB  
ans the m  
alphabet.  
2C A1 F2 90 39 65 F3 14 CC 3E 76 29 D0 AC F2 79  
in aplhabet you can pr  
DF F8 F7 D0 CF 90 D6 F7 8B A8 94 A2 60 07 9C 63  
nd you can  
of these if you have n  
5A F4 1C 34 09 F0 E5 BB A1 B2 D0 FD 99 43 B4 C6  
lets :EAPOL HMACis do: 6F 84 E4 87 FC 02 4B 19 D1 41 83 AC 1A 39 7F D7  
root@kali:~#  
will try all combinations of word. And this loop will run until we get our passw  
Currently very less secured because I want you to see how it is cracked.
```

Figure-01