Usage

```
aircrack-ng [options] <capture file(s)>
```

You can specify multiple input files (either in .cap or .ivs format) or use file name wildcarding. See Other Tips for examples. Also, you can run both airodump-ng and aircrack-ng at the same time: aircrack-ng will auto-update when new IVs are available.

Here's a summary of all available options:

Option	Param.	Description
-a	amode	Force attack mode (1 = static WEP, 2 = WPA/WPA2-PSK).
-b	bssid	Long version –bssid. Select the target network based on the access point's MAC address.
-e	essid	If set, all IVs from networks with the same ESSID will be used. This option is also required for WPA/WPA2-PSK cracking if the ESSID is not broadcasted (hidden).
-p	nbcpu	On SMP systems: # of CPU to use. This option is invalid on non-SMP systems.
-q	*none*	Enable quiet mode (no status output until the key is found, or not).
-c	*none*	(WEP cracking) Restrict the search space to alpha-numeric characters only (0x20 - 0x7F).
-t	*none*	(WEP cracking) Restrict the search space to binary coded decimal hex characters.
-h	*none*	(WEP cracking) Restrict the search space to numeric characters (0x30-0x39) These keys are used by default in most Fritz!BOXes.
-d	start	(WEP cracking) Long version –debug. Set the beginning of the WEP key (in hex), for debugging purposes.
-m	maddr	(WEP cracking) MAC address to filter WEP data packets. Alternatively, specify -m ff:ff:ff:ff:ff:ff to use all and every IVs, regardless of the network.
-M	number	(WEP cracking) Sets the maximum number of ivs to use.
-n	nbits	(WEP cracking) Specify the length of the key: 64 for 40-bit WEP, 128 for 104-bit WEP, etc. The default value is 128.
-i	index	(WEP cracking) Only keep the IVs that have this key index (1 to 4). The default behaviour is to ignore the key index.
-f	fudge	(WEP cracking) By default, this parameter is set to 2 for 104-bit WEP and to 5 for 40-bit WEP. Specify a higher value to increase the bruteforce level: cracking will take more time, but with a higher likelyhood of success.
-H	*none*	Long version –help. Output help information.
-l	file name	(Lowercase L, ell) logs the key to the file specified.
-K	*none*	Invokes the Korek WEP cracking method. (Default in v0.x)
-k	korek	(WEP cracking) There are 17 korek statistical attacks. Sometimes one attack creates a huge false positive that prevents the key from being found, even with lots of IVs. Try -k 1, -k 2, … -k 17 to disable each attack selectively.

-p	threads	Allow the number of threads for cracking even if you have a non-SMP computer.
-r	database	Utilizes a database generated by airolib-ng as input to determine the WPA key. Outputs an error message if aircrack-ng has not been compiled with sqlite support.
-x/-x0	*none*	(WEP cracking) Disable last keybytes brutforce.
-x1	*none*	(WEP cracking) Enable last keybyte bruteforcing (default).
-x2	*none*	(WEP cracking) Enable last two keybytes bruteforcing.
-X	*none*	(WEP cracking) Disable bruteforce multithreading (SMP only).
-y	*none*	(WEP cracking) Experimental single bruteforce attack which should only be used when the standard attack mode fails with more than one million IVs
-u	*none*	Long form –cpu-detect. Provide information on the number of CPUs and MMX support. Example responses to “aircrack-ng –cpu-detect” are “Nb CPU detected: 2” or “Nb CPU detected: 1 (MMX available)”.
-w	words	(WPA cracking) Path to a wordlist or ”-” without the quotes for standard in (stdin).
-z	*none*	Invokes the PTW WEP cracking method. (Default in v1.x)
-P	*none*	Long version –ptw-debug. Invokes the PTW debug mode.
-C	MACs	Long version –combine. Merge the given APs to a virtual one.
-D	*none*	Long version –wep-decloak. Run in WEP decloak mode.
-V	*none*	Long version –visual-inspection. Run in visual inspection mode.
-1	*none*	Long version –oneshot. Run in oneshot mode.
-S	*none*	WPA cracking speed test.