## NAME

airodump-ng - a wireless packet capture tool for aircrack-ng

## SYNOPSIS

**airodump-ng** [options] <interface name>

## DESCRIPTION

**airodump-ng** is used for packet capturing of raw 802.11 frames for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points. Additionally, airodump-ng writes out a text file containing the details of all access points and clients seen.

## OPTIONS

*-H, --help*
Shows the help screen.

*-i, --ivs* It only saves IVs (only useful for cracking). If this option is specified, you have to give a dump prefix (−−write option)

*-g, --gpsd*
Indicate that airodump-ng should try to use GPSd to get coordinates.

*-w <prefix>, --write <prefix>*
Is the dump file prefix to use. If this option is not given, it will only show data on the screen. Beside this file a CSV file with the same filename as the capture will be created.

*-e, --beacons*
It will record all beacons into the cap file. By default it only records one beacon for each network.

*-u <secs>, --update <secs>*
Delay <secs> seconds delay between display updates (default: 1 second). Useful for slow CPU.

*--showack*
Prints ACK/CTS/RTS statistics. Helps in debugging and general injection optimization. It is indication if you inject, inject too fast, reach the AP, the frames are valid encrypted frames. Allows one to detect "hidden" stations, which are too far away to capture high bitrate frames, as ACK frames are sent at 1Mbps.

*-h* Hides known stations for −−showack.

*--berlin <secs>*
Time before removing the AP/client from the screen when no more packets are received (Default: 120 seconds). See airodump-ng source for the history behind this option ;).

*-c <channel>[,<channel>[,...]], --channel <channel>[,<channel>[,...]]*
Indicate the channel(s) to listen to. By default airodump-ng hops on all 2.4GHz channels.

*-C <freq>[,<freq>[,...]]*
Indicates the frequencies to listen to. By default airodump-ng hops on all 2.4GHz channels.

*-b <abg>, --band <abg>*
Indicate the band on which airodump-ng should hop. It can be a combination of 'a', 'b' and 'g' letters ('b' and 'g' uses 2.4GHz and 'a' uses 5GHz). Incompatible with --channel option.

*-s <method>, --cswitch <method>*
Defines the way airodump-ng sets the channels when using more than one card. Valid values: 0 (FIFO, default value), 1 (Round Robin) or 2 (Hop on last).

*-2, --ht20*
Set the channel to be in HT20 (802.11n).

*-3, --ht40+*
Set the channel to be in HT40+ (802.11n). It requires the frequency 20MHz above to be available (4 channels above) and thus some channels are not usable in HT40+. Only channels up to 7 are available in HT40+ in the US (and 9 in most of Europe).

*-5, --ht40-*
Set the channel to be in HT40- (802.11n). It requires the frequency 20MHz below to be available (4 channels be)low and thus some channels are not usable in HT40-. In 2.4GHz, HT40- channels start at channel 5.

*-r <file>*
Reads packet from a file.

*-T, --real-time*
While reading packets from a file specified with '-r <file>', simulate the arrival rate of them, as if they were "live".

*-x <msecs>*
Active Scanning Simulation (send probe requests and parse the probe responses).

*-M, --manufacturer*
Display a manufacturer column with the information obtained from the IEEE OUI list. See airodump-ng-oui-update(8)

*-U, --uptime*
Display APs uptime obtained from its beacon timestamp.

*-W, --wps*
Display a WPS column with WPS version, config method(s), AP Setup Locked obtained from APs beacon or probe response (if any).

*--output-format <formats>*
Define the formats to use (separated by a comma). Possible values are: pcap, ivs, csv, gps, kismet, netxml. The default values are: pcap, csv, kismet, kismet-newcore. 'pcap' is for recording a capture in pcap format, 'ivs' is for ivs format (it is a shortcut for --ivs). 'csv' will create an airodump-ng CSV file, 'kismet' will create a kismet csv file and 'kismet-newcore' will create the kismet netxml file. 'gps' is a shortcut for --gps.
Theses values can be combined with the exception of ivs and pcap.

*-I <seconds>, --write-interval <seconds>*
Output file(s) write interval for CSV, Kismet CSV and Kismet NetXML in seconds (minimum: 1 second). By default: 5 seconds. Note that an interval too small might slow down airodump−ng.

*-K <enable>, --background <enable>*
Override automatic background detection. Use "0" to force foreground settings and "1" to force background settings. It will not make airodump-ng run as a daemon, it will skip background autodetection and force enable/disable of interactive mode and display updates.

*--ignore-negative-one*
Removes the message that says 'fixed channel <interface>: -1'.

**Filter options:**

*-t <OPN|WEP|WPA|WPA1|WPA2|WPA3|OWE>, --encrypt <OPN|WEP|WPA|WPA1|WPA2|WPA3|OWE>*
It will only show networks matching the given encryption. Note that WPA is a shortcut for WPA1, WPA2 and WPA3. May be specified more than once: '−t OPN −t WPA2'

*-d <bssid>, --bssid <bssid>*
It will only show networks, matching the given bssid.

*-m <mask>, --netmask <mask>*
It will only show networks, matching the given bssid ^ netmask combination. Need −−bssid (or −d) to be specified.

*-a* It will only show associated clients.

*-n <int>, --min-packets <int>*
The minimum number of packets received by an AP before displaying it.

*-N, --essid*
Filter APs by ESSID. Can be used several times to match a set of ESSID.

*-R, --essid-regex*
Filter APs by ESSID using a regular expression.

## INTERACTION

**airodump-ng** can receive and interpret key strokes while running. The following list describes the currently assigned keys and supposed actions:

*a* Select active areas by cycling through these display options: AP+STA; AP+STA+ACK; AP only; STA only

*d* Reset sorting to defaults (Power)

*i* Invert sorting algorithm

*m* Mark the selected AP or cycle through different colors if the selected AP is already marked

*o* Enable colored display of APs and their stations.

*p* Disable colored display.

*q* Quit program.

*r* (De-)Activate realtime sorting - applies sorting algorithm every time the display will be redrawn

*s* Change column to sort by, which currently includes: First seen; BSSID; PWR level; Beacons; Data packets; Packet rate; Channel; Max. data rate; Encryption; Strongest Ciphersuite; Strongest Authentication; ESSID

*SPACE* Pause display redrawing/ Resume redrawing

*TAB* Enable/Disable scrolling through AP list

*UP* Select the AP prior to the currently marked AP in the displayed list if available

*DOWN* Select the AP after the currently marked AP if available

If an AP is selected or marked, all the connected stations will also be selected or marked with the same color as the corresponding Access Point.

## EXAMPLES

**airodump-ng** −c 9 wlan0mon

Here is an example screenshot:

```
---------------------------------------------------------------------------
CH  9 ][ Elapsed: 1 min ][ 2007-04-26  17:41 ][ BAT: 2 hours 10 mins ][ WPA handshake: 00:14:6C:7E:40:80

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

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              <length: 7>
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   11-11     2        14         bigbear
(not associated)   00:14:A4:3F:8D:13   19   11-11     0         4         mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   −1   11-2      0         5         bigbear
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   36-24     0        99         teddy
---------------------------------------------------------------------------
```

*BSSID* MAC address of the access point. In the Client section, a BSSID of "(not associated)" means that the client is not associated with any AP. In this unassociated state, it is searching for an AP to connect with.

*PWR* Signal level reported by the card. Its signification depends on the driver, but as the signal gets higher you get closer to the AP or the station. If the BSSID PWR is -1, then the driver doesn't support signal level reporting. If the PWR is -1 for a limited number of stations then this is for a packet which came from the AP to the client but the client transmissions are out of range for your card. Meaning you are hearing only 1/2 of the communication. If all clients have PWR as -1 then the driver doesn't support signal level reporting.

*RXQ* Only shown when on a fixed channel. Receive Quality as measured by the percentage of packets (management and data frames) successfully received over the last 10 seconds. It's measured over all management and data frames. That's the clue, this allows you to read more things out of this value. Lets say you got 100 percent RXQ and all 10 (or whatever the rate) beacons per second coming in. Now all of a sudden the RXQ drops below 90, but you still capture all sent beacons. Thus you know that the AP is sending frames to a client but you can't hear the client nor the AP sending to the client (need to get closer). Another thing would be, that you got a 11MB card to monitor and capture frames (say a prism2.5) and you have a very good position to the AP. The AP is set to 54MBit and then again the RXQ drops, so you know that there is at least one 54MBit client connected to the AP.

*Beacons*
Number of beacons sent by the AP. Each access point sends about ten beacons per second at the lowest rate (1M), so they can usually be picked up from very far.

*#Data* Number of captured data packets (if WEP, unique IV count), including data broadcast packets.

*#/s* Number of data packets per second measure over the last 10 seconds.

*CH* Channel number (taken from beacon packets). Note: sometimes packets from other channels are captured even if airodump-ng is not hopping, because of radio interference.

*MB* Maximum speed supported by the AP. If MB = 11, it's 802.11b, if MB = 22 it's 802.11b+ and higher rates are 802.11g. The dot (after 54 above) indicates short preamble is supported. 'e' indicates that the network has QoS (802.11e) enabled.

*ENC* Encryption algorithm in use. OPN = no encryption,"WEP?" = WEP or higher (not enough data to choose between WEP and WPA/WPA2), WEP (without the question mark) indicates static or dynamic WEP, and WPA or WPA2 if TKIP or CCMP or MGT is present.

*CIPHER*
The cipher detected. One of CCMP, WRAP, TKIP, WEP, WEP40, or WEP104. Not mandatory, but TKIP is typically used with WPA and CCMP is typically used with WPA2. WEP40 is displayed when the key index is greater than 0. The standard states that the index can be 0-3 for 40bit and should be 0 for 104 bit.

*AUTH* The authentication protocol used. One of MGT (WPA/WPA2 using a separate authentication server), SKA (shared key for WEP), PSK (pre-shared key for WPA/WPA2), or OPN (open for WEP).

*WPS* This is only displayed when --wps (or -W) is specified. If the AP supports WPS, the first field of the column indicates version supported. The second field indicates WPS config methods (can be more than one method, separated by comma): USB = USB method, ETHER = Ethernet, LAB = Label, DISP = Display, EXTNFC = External NFC, INTNFC = Internal NFC, NFCINTF = NFC Interface, PBC = Push Button, KPAD = Keypad. Locked is displayed when AP setup is locked.

*ESSID* The so-called "SSID", which can be empty if SSID hiding is activated. In this case, airodump-ng will try to recover the SSID from probe responses and association requests.

*STATION*
MAC address of each associated station or stations searching for an AP to connect with. Clients not currently associated with an AP have a BSSID of "(not associated)".

*Rate* This is only displayed when using a single channel. The first number is the last data rate from the AP (BSSID) to the Client (STATION). The second number is the last data rate from Client

(STATION) to the AP (BSSID).

*Lost* It means lost packets coming from the client. To determine the number of packets lost, there is a sequence field on every non-control frame, so you can subtract the second last sequence number from the last sequence number and you know how many packets you have lost.

*Notes* Additional information about the client, such as captured EAPOL or PMKID.

*Frames* The number of data packets sent by the client.

*Probes* The ESSIDs probed by the client. These are the networks the client is trying to connect to if it is not currently connected.

The first part is the detected access points. The second part is a list of detected wireless clients, stations. By relying on the signal power, one can even physically pinpoint the location of a given station.

## AUTHOR

This manual page was written by Adam Cecile <gandalf@le-vert.net> for the Debian system (but may be used by others). Permission is granted to copy, distribute and/or modify this document under the terms of the GNU General Public License, Version 2 or any later version published by the Free Software Foundation On Debian systems, the complete text of the GNU General Public License can be found in /usr/share/common-licenses/GPL.

## SEE ALSO

**airbase-ng(8)**
**aireplay-ng(8)**
**airmon-ng(8)**
**airodump-ng-oui-update(8)**
**airserv-ng(8)**
**airtun-ng(8)**
**besside-ng(8)**
**easside-ng(8)**
**tkiptun-ng(8)**
**wesside-ng(8)**
**aircrack-ng(1)**
**airdecap-ng(1)**
**airdecloak-ng(1)**
**airolib-ng(1)**
**besside-ng-crawler(1)**
**buddy-ng(1)**
**ivstools(1)**
**kstats(1)**
**makeivs-ng(1)**
**packetforge-ng(1)**
**wpaclean(1)**
**airventriloquist(8)**