



AirSnort Homepage



This software is OLD

It is no longer maintained or supported. Besides, there are much better tools out there. You really should be trying something like [aircrack-ng](#).

Download

[Download Airsnort here.](#)
[Snax's GPG key](#)

Help Forums

Sourceforge help [forums](#)

News

- **12/31/04** - Cisco users on Windows should choose the DWL-650 card type
- **12/25/04** - Released version 0.2.7c. Bug fixes and support for DWL-650 card in Windows
- **12/20/04** - Released version 0.2.7b. Bug fixes and improved handling of Korek/Aircrack attack initiation/execution
- **12/18/04** - Released airsnort-0.2.7. Incorporates aircrack style cracking in real time.
- **09/22/04** - Released airsnort-0.2.6. Greatly improved Windows stability along with other stability improvements as well.
- **09/05/04** - Released airsnort-0.2.5. This release includes a compiled Windows binary (tested on XP only). See [Windows information](#) for more details. Make sure you read README.win
- **02/19/04** - Pavel Roskin just let me know that the CVS version of the [orinoco drivers](#) now supports monitor mode via the iwconfig interface! Airsnort in CVS supports these latest changes to the orinoco drivers.
- **02/17/04** - [Adrian Woodley](#) has ported the orinoco patch for use with kernel 2.6.2. Get it from the [orinoco info page](#)
- **01/15/04** - Posted my libnids-1.18 patch to enable recognition of DLT_PRISM_HEADER (the data link type used by prism cards). This is a better fix to allow dsniffing in monitor mode as DLT_IEEE802_11 has been supported since version 1.16. Download patch and build libnids-1.18, then rebuild a stock version of dsniff to make use of it. You no longer need to use the dsniff below. Get the libnids patch here: [libnids-1.18-snax-prism-modified.diff](#).

- **12/09/03** - GUI updated to gtk+-2.2
- [Old news](#)

Introduction

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

802.11b, using the Wired Equivalent Protocol (WEP), is crippled with numerous security flaws. Most damning of these is the weakness described in "[Weaknesses in the Key Scheduling Algorithm of RC4](#)" by Scott Fluhrer, Itsik Mantin and Adi Shamir. [Adam Stubblefield](#) was the first to implement this attack, but he has not made his software public. AirSnort, along with [WEPCrack](#), which was released about the same time as AirSnort, are the first publicly available implementations of this attack.

AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.

AirSnort 0.2.6 Requirements

AirSnort runs under Windows or Linux, and requires that your wireless nic be capable of rf monitor mode, and that it pass monitor mode packets up via the PF_PACKET interface. Cards known to do this are:

- Cisco Aironet
- Prism2 based cards using wlan-ng drivers or Host-AP drivers
- Orinoco cards and clones using [patched](#) orinoco_cs drivers
- Orinoco cards using the latest Orinoco drivers >= 0.15 with built in monitor mode support
- And many others.
- **Windows:** Any(?) card supported by Airopeek.

For Linux users, the best resources for finding out if your card can do monitor mode and what drivers you will need are those maintained at the [Kismet](#) site.

To compile AirSnort, do the following:

- Get your drivers working! To do this you may need one or more of the following
 - [Kernel source](#)
 - [PCMCIA CS package](#)
 - [wlan-ng package](#)
 - [Orinoco driver patches](#)
 - [Host AP drivers](#)
- Install the LATEST version of [libpcap](#). Please make sure that you have removed any old version of pcap that may be resident on your system. (**not required for Windows users.**)
- Make sure you have [gtk+-2.2](#) installed as AirSnort is a gui application. You will also need

[gtk+-devel](#)

- Linux users perform the following steps

```
# tar -xzf airsnort-0.2.6.tar.gz
# cd airsnort-0.2.6
# ./configure
# make
# make install          (optional)
```

- Poof you're done. The airsnort executable is in the airsnort-0.2.6/src subdirectory, do with it what you will. There are some man pages in airsnort-0.2.6/man
- **Windows users:** see the [Windows info](#) page.

Orinoco Notes: The latest patches seem to smooth things out for all versions of Orinoco firmware. Please make sure you are using the latest patches. If you do not see a patch for your version of pcmcia-cs, then PLEASE determine what version of the orinoco drivers are included with your version of pcmcia-cs and get the appropriate orinoco-0.XX patches. To do this look in pcmcia-cs-X.Y.Z/wireless/orinoco_cs.c which will list the version number in the first couple of lines.

Download

Anonymous CVS is at the CVSRROOT
:pserver:anonymous@cvs.airsnort.sourceforge.net:/cvsroot/airsnort . For more information, view our [SourceForge page](#).

Download the tarballs from [Sourceforge](#)

Apple iBook Info

See Erik Winkler's [iBook page](#) for more information.

Contact Us

Email [Snax](#) with questions, comments, suggestions and patches. Jeremy and Blake are semi-retired from the project.

Old News

- **08/08/03** - Posted my dsniiff patches to allow dsniiffing in monitor mode. Get it here [dsniiff-2.3-monitor-patch.tar.gz](#).
- **08/07/03** - Ported the orinoco patch to the orinoco-0.13d and 0.13e drivers. Get it from the [orinoco info](#) page.
- **02/22/03** - Monitor mode patch for orinoco-0.13b is available on [orinoco info](#) page.
- **02/19/03** - [Windows information](#) Some background information on the windows porting effort. Worth a read if you are going to attempt to build Airsnort on Windows.
- **02/15/03** - [Airsnort on Windows](#)? Its working in alpha, but requires some effort to install. If

patching the orinoco drivers is too much for you then this is probably not for you either. I hope to have more shortly. Most of the code is already in CVS, but the installation instruction instructions are not available yet.

- **02/07/03** - Ritchie@tipsybottle.com has a nice HOWTO on RedHat 8.0 + Orinoco + Kismet [here](#) Much of the info is applicable to airsnt as well.
- **09/25/02** - The problems with v8.10 firmware may have been solved thanks to the troubleshooting efforts of Ian Goldberg and Pat Swieskowski. Try the patch for pcmcia-cs-3.2.1 available on the [orinoco info](#) page. This patch should also apply to pcmcia-cs-3.2.0 though I have not tested it.
- **08/31/02** - Pat Swieskowski has also posted some info on using Airsnort on an Apple iBook. See the page - <http://www.swieskowski.net/code/wifi.php>
- **08/27/02** - Erik Winkler has posted some info on using Airsnort on an Apple iBook. See the page - <http://www.macunix.net:443/ibook.html>
- **08/17/02** - Released Airsnort-0.2.1b which fixes bug in gencases and decrypt.
- **08/16/02** - Ported the orinoco patch to the pcmcia-cs-3.2.0 drivers. Get it from the [orinoco info](#) page. David Gibson has declared the orinoco-0.12 series a failed experiment and I have removed the patch for 0.12 drivers.
- **06/20/02** - Ported the orinoco patch to the 0.12 drivers. Get it from the [orinoco info](#) page.
- **06/08/02** - Got off my butt and updated the orinoco driver capabilities. Posted a patch to the orinoco-0.11b drivers to enable monitor mode AND allow setting of your own MAC address via ifconfig. Get it from the [orinoco info](#) page.
- **06/07/02** - Released Airsnort-0.2.1a, primarily a maintenance release. This release fixes a bug in weak IV reporting and removes gnome dependencies. The decrypt tool is more like a dictionary based cracker now, but still has a way to go.
- **06/02/02** - Successful downgrade for Orinoco v8.10 firmware users. See the [Orinoco information](#) page for details.
- **05/03/02** - The project finally has a logo! It was derived with the permission of Marty Roesch over at the [Snort project](#) which you should certainly check out if you haven't already.
- **05/01/02** - Airsnort 0.2.1 released - requires libpcap. Limited support for Cisco cards. [Changes here](#)
- **04/17/02** - Updated the orinoco patches to correct a problem when receiving beacon packets (and perhaps others?) Thanks to jonp@chem.... !!
- **04/12/02** - Just released - [Decrypt](#) is a program to decrypt data packets in pcap style capture files.
- **04/10/02** - The faq has been [updated](#)
- **03/19/02** - New Patches available. See the new [Orinoco info page](#). Also see the [updated faq](#) for answers to questions about monitor mode, promiscuous mode, PF_NETLINK, and PF_PACKET.
- **03/14/02** - [patch-0.2.0-1](#) for Airsnort 2.0 posted. orinocoSniff.c updated to fix problems with SIOCIWFIRSTPRIV
- **03/07/02** - New Orinoco [patch](#) for pcmcia-3.1.33/orinoco-0.09b
- **02/28/02** - AirSnort 2.0 released. Read about [changes](#).
- **08/23/01** - [Frequently Asked Questions](#) we wrote in response to a bunch of our emails
- **08/20/01** - We got written up by [Wired News](#).

