

# **AIM Sniff**

## User Manual

# Table of Contents

## **Disclaimer**

This is provided as a public service to experienced systems administrators who wish to protect their users from harassment while using AIM and to demonstrate the need for encryption in instant messaging programs. No technical support will be given to users attempting to use this software for malicious purposes.

## Licensing

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the:

Free Software Foundation, Inc.

59 Temple Place, Suite 330

Boston, MA 02111-1307 USA

You may also contact me directly with any questions at:

[grimesh@users.sourceforge.net](mailto:grimesh@users.sourceforge.net)

## **Description**

AIM Sniff is a utility for monitoring and archiving AOL Instant Messenger messages across a network. You can either do a live dump (actively sniff the network) or read a PCAP file and parse the file for IM messages. You also have the option of dumping the information to a MySQL database, a flat file, STDOUT, or any combination of the three. AIM Sniff allows administrators to see how often users are chatting to monitor for abuse and you can also use AIM Sniff to monitor for cases of harassment or pirated software trading. It has been tested on FreeBSD, Linux, and OS X.

## Command Line Switches

- C=filename <-Get AIM Sniff options from a configuration file
- r=filename <-Read a PCAP file instead of doing a live capture
- O=filename <-Output to the specified filename
- c=integer <-The number of packets to read before quitting
- d=dev <-The device to capture packets from
- f='filter string' <-String to filter on enclosed in single quotes  
(DEFAULT: 'tcp and port 5190') -- Should only have to be specified if you think AIM is running on a different port
- p <-Place the device into promiscuous mode
- to=integer <-Read timeout of packets in milliseconds
- SMB <-Turn SMB lookups 'on' to get NT domain usernames with AIM logins, Off by default
- nodb <-Do not dump to a DB, only dump to STDOUT
- quiet <-Do not print anything but errors to STDOUT
- D <-Run as a daemon
- getHandles <-Does not do anything with PCAP but will populate the fromHandle field in the logs table (Can be used with -C switch above)

Defaults:

“-d=eth0 -f='tcp and port 5190' -p -to=1000”

## Sample Configuration File

Lines that begin with a '#' are viewed as comments and are ignored.

```
dumpfile=/home/aimsniiff/aim.dump
```

```
packetCount=10
```

```
dev=eth0
```

```
filter='tcp and port 5190'
```

```
promisc=1
```

```
timeout=1000
```

```
SMB=1
```

```
#daemon=1
```

```
#nodb=1
```

```
#quiet=1
```

```
##Database information
```

```
host=mysql.server.com
```

```
user=aimuser
```

```
password=password
```

## Dependencies

The following software is necessary for in order for AIM Sniff to run correctly:

Samba to perform SMB lookup features, available at [www.samba.org](http://www.samba.org)

Libpcap, available at [www.tcpdump.org](http://www.tcpdump.org)

The following Perl modules, available at [www.cpan.org](http://www.cpan.org):

Net::Pcap

NetPacket::Ethernet

NetPacket::IP

NetPacket::TCP

Unicode::String

DBI

DBD::mysql

Proc::Daemon

FileHandle

## Installation Procedure

The first step is to install the necessary dependencies. The Perl modules can be installed using the CPAN tool. This tool can be run from a linux console by issuing the command 'perl -MCPAN -e shell'. Once you are running CPAN, use the command 'install NetPacket::Ethernet' to install a module (replace NetPacket::Ethernet with the name of the module to install). Various problems were experienced when using CPAN to install Net::Pcap. It is highly recommended that you download the source code of this module from the CPAN website ([www.cpan.org](http://www.cpan.org)) and install it manually.

After all of the dependencies have been installed, configure the port on the switch that the computer running AIM Sniff is plugged into is set as a monitor port. Now run 'aimSniff.pl -nodb' to ensure that everything is linked correctly and running. Send a few AIM messages from a computer on the same switch to ensure everything is working properly.

If you plan to use the database dump feature, you'll have to load the included table.struct file into MySQL. To do this run the following command 'mysql < table.struct'. This will create a database named "aim" with all the tables that AIM Sniff will report to. Now you can create a user that has rights to this database by running mysql and issuing: 'GRANT ALL ON aim.\* TO username@hostname IDENTIFIED BY 'password';'. For more info on granting access to a user please see the MySQL documentation.

Once you have verified everything is working correctly, you may want to edit the included sample configuration file to reflect your system and the options you want to use.

Using a configuration file will shorten the command line that you need to run AIM Sniff.

It also prevents you from having to remember all the possible options and command line switches.

## Usage Information

In general, the default options will run AIM Sniff adequately but physical placement of AIM Sniff must be considered. Using Figure 1 as a reference, if the computer running AIM Sniff is placed on Switch B, it will only detect AIM traffic from the computers connected to Switch B. However, if we place AIM Sniff further up the network architecture at Switch A, we will be able to see all AIM traffic on both Switch B and Switch C.

If the computer running AIM Sniff has multiple network cards, be sure to specify which network interface you want to listen to traffic on by specifying the the ‘-d *interface*’ switch when running AIM Sniff. Replace *interface* with the name of the network interface card you want to listen on (fxpX on FreeBSD, ethX on Linux, where X is the number of your card).

## Technical Support

Thanks to Sourceforge.net, there are many ways to get technical support if you are having problems running AIM Sniff:

Website:

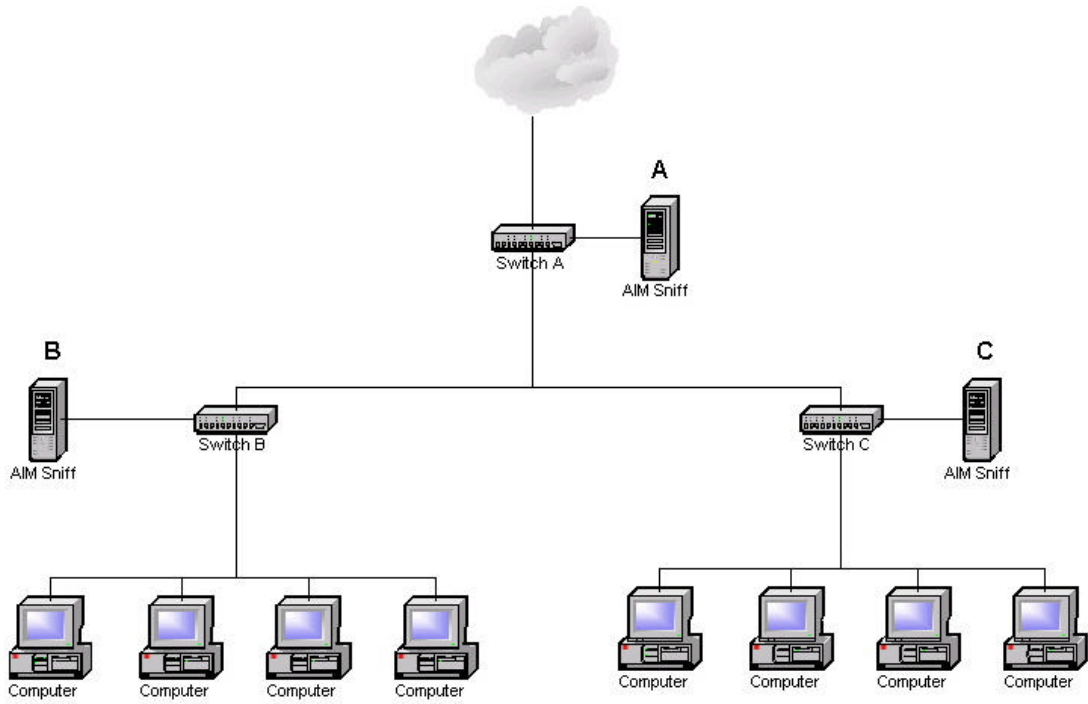
<http://aimsniiff.sourceforge.net> - The website provides several forums to posts questions, report bugs, and to request features.

Mailing Lists:

[Aimsniiff-devel@sourceforge.net](mailto:Aimsniiff-devel@sourceforge.net) - This mailing lists is another good place for technical support. You can also asks questions about the code of AIM Sniff, writing additional modules, volunteering for help and any other miscellaneous questions.

[Aimsniiff-announce@sourceforge.net](mailto:Aimsniiff-announce@sourceforge.net) - This mailing list is a low volume lists where new releases of AIM Sniff are sent to people who wish to run the most recent release.

# Figures



**Figure 1. Network Setup Diagram**