Оригинал: http://www.lissyara.su/articles/freebsd/programms/aimsniff/
Постановка задачи
Необходимо создать систему, позволяющую перехватывать, хранить и отображать в удобной форме ICQ-переписку сотрудников компании. Судя по диалогам на соответствующих форумах, рассматриваемая задача периодически возникает, поэтому я описал один из способов ее решения, примененный в нашей Компании.

Исходные данные
Имеется сервер с FreeBSD, через который сотрудники компании тем или иным способом (NAT, прокси-сервер и т.п.) выходят в Интернет. Для установки системы не требуется какая-либо перенастройка этого сервера. Самое главное - Вы должны тем или иным способом ограничить список портов, которые могут использовать клиенты ICQ, чтобы продвинутые пользователи не смогли "обмануть" сниффер.
В качестве сниффера мы будем использовать AimSniff, для хранения перехваченныйх сообщений - сервер MySQL (процесс настройки сервера MySQL не расматривается в данной статье за исключением создания базы данных и пользователя aimsniff), для просмотра отчетов - Web Aim Sniff (WAS) и Web-сервер Apache (процесс настройки сервера Apache не рассматривается в данной статье за исключением добавления возможности отображения необходимых отчетов). Почти все перечисленное программное обеспечение будет устанавливаться из портов, поэтому я настоятельно рекомендую Вам обновить их перед выполнением действий, описанных ниже (лично я использовал FreeBSD 7.0 и последние на конец 2008 года версии портов для нее). Ссылки на источники информации будут приводиться применительно к конкретным разделам статьи.

Установка и настройка AimSniff
Установку AimSniff необходимо выполнить из портов:cd /usr/ports/security/aimsniff
make install clean

Сразу после завершения установки необходимо выполнить команду: aimsniff -d=bge1 --nodb

Естественно, bge1 необходимо заменить на имя внутреннего интерфейса. Данная команда запускает мониторинг пакетов ICQ, проходящих через заданный интерфейс, и отображение содержимого декодированных пакетов на экране без записи в базу данных. Если после выполнения команды вместо сообщений "INCOMINMG MESSAGE..." и "OUTGOING MESSAGE..." выдается сообщение: "Can't locate GDBM_File.pm in @INC (…) at /usr/local/bin/aimsniff line 47. BEGIN failed--compilation aborted at /usr/local/bin/aimsniff line 47., следует пересобрать Perl с поддержкой GDBM: cd /usr/ports/lang/perl5.8
make deinstall
make WITH_GDBM=yes reinstall

По умолчанию AimSniff "не понимает" интересующие нас сообщения в кодировке UTF-8. Для исправления такого поведения необходимо загрузить пропатченную версию скрипта AimSniff и установить порт p5-Unicode-Map8 (если он не был установлен ранее):
fetch http://www.aimsniff.com/releases/aimSniff.Cyr-005.tar.gz
tar -xf aimSniff.Cyr-005.tar.gz
chmod 555 aimSniff.Cyr-005.pl
mv aimSniff.Cyr-005.pl /usr/local/bin
cd /usr/ports/converters/p5-Unicode-Map8
make install clean

Для проверки работоспособности руссифицированного AimSniff необходимо выполнить команду: aimSniff.Cyr-005.pl -d=bge1 --nodb

После того, как первичная настройка будет завершена, необходимо создать базу данных aimsniff и пользователя aimsniff для работы с этой базой данных. Для этого нужно запустить клиент MySQL командой: mysql -u <имя пользователя-администратора> -p

ввести пароль и выполнить три SQL-запроса: CREATE DATABASE aimsniff;
GRANT ALL ON aimsniff.* TO aimsniff@localhost IDENTIFIED BY 'aimsniff';
FLUSH PRIVILEGES;

После завершения работы клиента MySQL необходимо создать таблицы базы данных aimsniff: mysql -u <имя пользователя-администратора> -p aimsniff
< /usr/local/share/doc/aimsniff/table.struct

После завершения подготовки базы данных необходимо создать файл конфигурации AimSniff. В моем случае он называется aimSniff.cfg, находится в папке /usr/local/etc и имеет следующее содержимое: dev=bge1
filter='tcp and port 3128'
daemon=1
host=localhost
database=aimsniff
user=aimsniff
password=aimsniff
useSyslog=1

В данном файле заданы следующие значения параметров: dev - имя интерфейса; filter - фильтр, определяющий какие пакеты следует "вылавливать" (зависит от способа выхода клиентов ICQ в Интернет, в моем случае для выхода клиентов ICQ в Интернет используется прокси-сервер, "слушающий" порт 3128); daemon - признак работы в

режиме демона; host / database / user / password - параметры доступа к базе данных; useSyslog - признак использования syslog'а для записи служебных сообщений.
Самым последним этапом настройки AimSniff является доработка скрипта автозапуска, выполняемого при запуске операционной системы. Образец такого скрипта поставляется в составе AimSniff (файл rc.aimsniff в папке /usr/local/share/doc/aimsniff), однако его нужно немного адаптировать. Во-первых, нужно указать корректный интерпретатор shell в первой строке (в моем случае это /bin/sh), а во вторых заменить имя скрипта и файла конфигурации в шестой строке на: /usr/local/bin/aimSniff.Cyr-005.pl -C=/usr/local/etc/aimSniff.cfg

После этого необходимо сделать скрипт исполняемым и скопировать его в папку usr/local/etc/rc.d: cd /usr/local/share/doc/aimsniff
chmod 555 rc.aimsniff
cp rc.aimsniff /usr/local/etc/rc.d/aimsniff.sh

На этом настройка AimSniff заканчивается. Перезагрузите сервер, и после запуска операционной системы демон AimSniff начнет "вылавливать", декодировать и записывать перехваченные сообщения ICQ в базу данных.

Установка и настройка WAS
WAS (Web Aim Sniff) - Web-интерфейс для доступа к базе данных AimSniff, написанный на языке PHP. К сожалению, пока он не добавлен в коллекцию портов FreeBSD, в связи с чем придется ставить его из исходных тестов. Перед началом установки WAS необходимо добавить в файл конфигурации необходимого виртуального хоста Apache следующие строки:Alias /was "/usr/local/www/was/"
<Directory "/usr/local/www/was">
 AuthName "This server require authorization!"
 AuthUserFile /usr/local/etc/apache/htpasswd
 AuthType Basic
 Require user <Список пользователей, которым разрешен доступ>
 Order deny,allow
 Deny from all
 Allow from ...
 Allow from ...
</Directory>

Как видно из фрагмента файла конфигурации для установки WAS была выбрана папка /usr/local/www/was, доступ к которой разрешен только с определенных IP-адресов и только после прохождения процедуры Basic-аутентификации. Вам нужно подставить реальные IP-адреса в директивы Allow from и добавить необходимых пользователей в файл htpasswd и директиву Require user. О том, как это сделать, подробно написано в разделе Authentication, Authorization, and Access Control официальной документации Apache. Не забудьте перезапустить Web-сервер после внесения изменений в его

конфигурацию.
Когда Web-сервер будет подготовлен, необходимо загрузить, распаковать и переместить WAS в нужную папку, удалить все лишнее и сделать владельцем файлов WAS пользователя, от имени которого работает Web-сервер:mkdir /usr/local/www/was
cd /usr/local/www/was
fetch http://aimsniff.com/releases/was-0.1.2b.tar.gz
tar -xf was-0.1.2b.tar.gz
mv was-0.1.2b/* was-0.1.2b/.[a-zA-Z]* .
rm -Rf was-0.1.2b was-0.1.2b.tar.gz
chown -R www:www * .[a-zA-Z]*

После этого необходимо слегка подкорректировать файлы WAS. Во-первых, в файлах .header.php и index.html неоходимо исправить charset=iso-8859-1 на charset=koi8-r (это приведет к корректному выбору кодировки браузером и, соответственно, корректному отображению русских символов). Во-вторых, в файле index.php необходимо исправить img src=./typesGraph.php на img src=./images/typesGraph.php (это исправит ошибку, допущенную разработчиком WAS). В третьих, мне показалось более удобным видеть в списке сообщений не IP-адреса, а имена компьютеров локальной сети. Если Вы согласны со мной, исправьте в файле .global.php <td><B>IP</td> на <td><B>Computer</td>, а также исправьте в теле функции printMessages $rs["ip"] на ucwords(gethostbyaddr($rs["ip"])). Вообще, следует заметить, что WAS - очень "сырой" пакет. К сожалению, у меня нет времени на его адаптацию, да и PHP я знаю лишь поверхностно, поэтому в настоящий момент приходится довольствоваться тем, что есть. Все работает, хотя за эргономику я бы не поставил больше тройки.
После доработки файлов WAS необходимо открыть в браузере URL http://host.company.com/was/admin.php, естественно, изменив host.company.com на имя используемого Вами виртуального хоста. В браузер будет загружена страница, на которой можно задать параметры WAS. В первую очередь необходимо изменить параметры Database User / Database Password и нажать кнопку Submit. Остальные параметры могут быть изменены или не изменены, исходя из личных предпочтений. На этом настройка WAS заканчивается.

Заключение
С учетом простоты рассмотренной системы с одной стороны и огромной популярностью ICQ с другой Вам скорее всего удастся выявить не один и не два эпизода неправильного использования рабочего времени, а возможно и "слива" конфиденциальной информации. Бесспорно, система не является панацеей, однако даже несколько выявленных случаев с лихвой окупят время, потраченное на ее настройку.