

NetResident®

Руководство пользователя

Copyright © 2006-2011 TamoSoft

Введение

О программе NetResident

NetResident - это программа сетевого мониторинга, предназначенная для перехвата, хранения, анализа и восстановления различных сетевых событий: сообщений электронной почты, веб-страниц, загруженных файлов и сообщений коммуникационных программ. Для перехвата данных из сети NetResident использует продвинутую технологию мониторинга. После перехвата программа записывает их в базу данных, восстанавливает информацию и отображает ее в форме, понятной пользователю.

Во многих аспектах NetResident похож на сетевой анализатор, но у программы есть отличительная особенность - ориентация на протоколы высокого уровня, которые используются для передачи данных через Интернет или локальную сеть. Работая с NetResident, вам не потребуется глубокое понимание сетевых технологий, а также не придется пользоваться сложными программами или исследовать содержимое пакета для восстановления исходных данных. NetResident выполняет всю эту работу за вас, предоставляя на выходе веб-страницы, сообщения электронной почты и коммуникационных программ или загруженные файлы. Программа предназначена для сетевых администраторов, которые действуют в области обеспечения информационной безопасности, для родителей, которые хотят быть в курсе того, чем их дети заняты в Интернете, а также для судебных экспертов.

Если вы являетесь одним из профессионалов в области сетевых технологий, которые пользуются решениями для сетевого мониторинга от TamoSoft (CommView или CommView for WiFi), NetResident поможет вам обработать лог-файлы, созданные этими программами мониторинга и восстановить сообщения электронной почты, содержимое веб-страниц и другие виды данных из сети для их быстрого анализа.

ЧТО НОВОГО

Версия 2.0

- Добавлен перехват передачи файлов во всех поддерживаемых IM.
- Поддержка новых версий Live Messenger.
- Добавлен фильтр перехвата для FTP.
- Исправлено несколько ошибок.

Версия 1.9

- Улучшена работа с ICQ.
- Улучшена работа с HTTP прокси.
- Улучшена работа с SOCKS 4 и SOCKS 5 прокси.
- Добавлена поддержка вебпочт Mail.Ru, Яндекс.Почта и AOL Mail.
- Улучшена обработка Gmail, Hotmail и Yahoo! Mail (в связи с последними изменениями этих сервисов).
- Исправлено несколько ошибок.

Версия 1.8

- Многочисленные обновления обработчиков протоколов, позволяющие корректно обрабатывать сообщения мгновенного обмена и Web-почты с использованием самых последних протоколов.
- Поддержка вложений в исходящих почтовых сообщениях Web-почты.
- Обновлен сетевой драйвер, что улучшило производительность программы в нагруженном LAN-окружении.
- Исправлено несколько ошибок, улучшен интерфейс программы.

Версия 1.7

- Поддержка протокола IPv6
- Улучшена производительность программы при работе с многоядерными процессорами
- Расширены настройки оповещений
- Добавлены настройки HTTP- и почтовых фильтров для работы в режиме реального времени
- Поддержка Windows 7
- Добавлена возможность сворачивания программы в область системного трея
- Возможность архивации старых записей базы данных
- Улучшена обработка Gmail и Yahoo! Mail (в связи с последними изменениями этих сервисов)
- Исправлено несколько ошибок

Версия 1.6

- Поддержка Web-почты (Gmail, Hotmail, Yahoo! Mail, Mail.ru)
- Поддержка протокола Mail.ru agent
- Автоматический импорт log-файлов
- Улучшено управление событиями (уровни приоритетов и комментарии)
- Настраиваемый путь к базе данных NetResident
- Исправлено несколько ошибок

Версия 1.5

- Возможность поиска по базе данных событий
- Установка предупреждений на основе ключевых слов
- Улучшена производительность базы данных
- Исправлено несколько ошибок

Версия 1.4

- Новый, улучшенный процессор базы данных
- Улучшена работа с VoIP
- Улучшена работа с ICQ
- Дополнительный инструмент PromiSwitch для мониторинга в коммутируемых сетях
- Новые виды лицензий: Pro и Lite
- Исправлено несколько ошибок

Версия 1.3

- Улучшена работа с VoIP

- Поддержка удаленных подключений к сервису NetResident
- Дополнительные сведения о событиях (номера портов и временные отметки)
- Поддержка Windows Vista
- Исправлено несколько ошибок

Версия 1.2

- Поддержка протокола IRC (Internet Relay Chat)
- Поддержка протокола Telnet
- Поддержка протокола VoIP (Voice over IP)
- Импорт и экспорт базы данных
- Исправлено несколько ошибок

Версия 1.1

- Поддержка протоколов Yahoo и Jabber
- Импортирование лог-файлов различных форматов
- Настраиваемый размер базы данных, что позволяет автоматически удалять старые записи.
- Исправлено несколько ошибок

Работа с программой

Перед началом работы: “прозрачность” вашей сети

Ключом к успешному мониторингу является т. н. “прозрачность” сетевого трафика. Если вам требуется наблюдать лишь один компьютер в сети, то просто установите NetResident на данной машине. Однако, если вы хотите осуществлять мониторинг сразу нескольких компьютеров в рамках локальной сети, важно понять, каким образом достичь “прозрачности” сети, т. е. способности “видеть” трафик с разных машин из одной точки наблюдения.

В целом, для мониторинга других компьютеров в вашей локальной сети вам потребуется либо установить NetResident на шлюзе, либо использовать коммутатор (switch) с функцией “зеркалирования портов”, либо работать с хабом. Существует множество конфигураций сети, так что если вы – новичок в области сетевого мониторинга, мы советуем прочитать подробную статью с поясняющими иллюстрациями, которая называется [Мониторинг сетей Ethernet и Wi-Fi в режиме “promiscuous”](#) (статья также доступна в формате [PDF](#)).

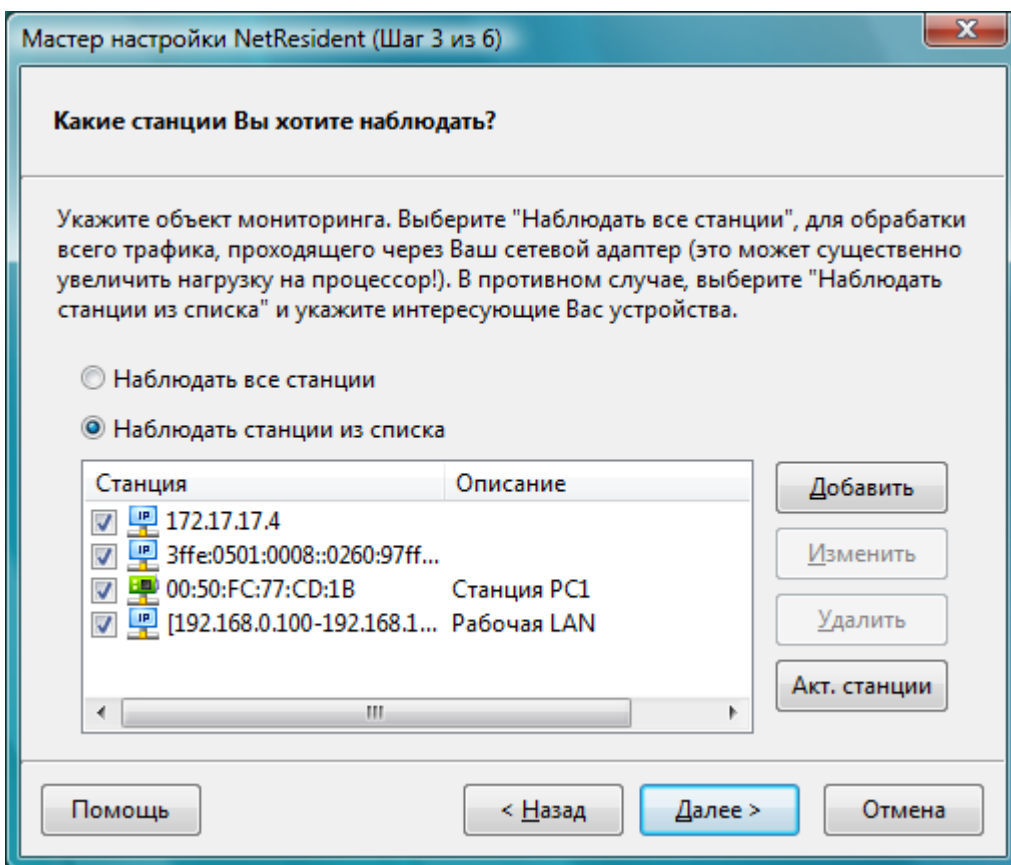
В настоящее время доступна специальная утилита для мониторинга коммутируемых сетей Ethernet. Для более подробной информации обратитесь к главе [Утилита PromiSwitch](#).

Мастер настройки

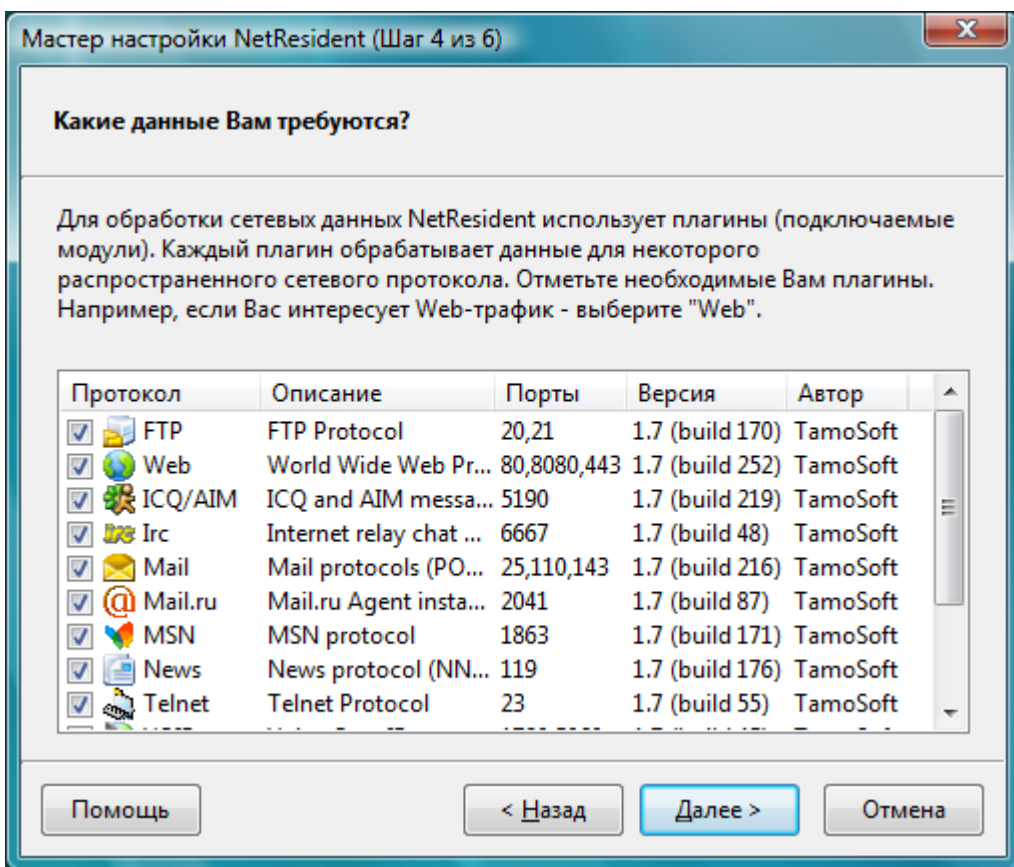
Прежде чем начать мониторинг вашей сети, вам потребуется настроить NetResident с помощью Мастера. Если вы не запустили Мастер при первом открытии программы, вы всегда сможете это сделать, выбрав в меню **Инструменты => Мастер установки**.

Для перехода к странице выбора адаптера нажмите **Далее**. На этой странице вы увидите выпадающий список, в котором можно будет выбрать адаптер для мониторинга. Если у вас dial-up-соединение или вы подключены к локальной сети через Ethernet-адаптер, в меню будет лишь один адаптер. Выберите его. Если ваш компьютер является Интернет-шлюзом для локальной сети или на нем установлено несколько сетевых адаптеров, выберите, какой адаптер вы хотите наблюдать с помощью NetResident. Некоторые сетевые адаптеры не могут работать в режиме "promiscuous" (состояние, в котором сетевой адаптер обнаруживает в сети все пакеты вне зависимости от их конечного адреса). Если вы работаете с таким адаптером, выберите опцию **Использовать режим "non-promiscuous"**. Для беспроводных (802.11) адаптеров эта опция должна быть всегда активна. Для работы с dial-up- или VPN-адаптерами выберите адаптер **WAN miniport**. Для перехода к странице выбора станций нажмите **Далее**.

Программа попытается обнаружить рабочие станции вашей сети и предоставит список компьютеров, которые, возможно, вы захотите наблюдать. Самый простой способ определить рабочие станции – выбрать опцию **Наблюдать все станции**. Этим самым вы дадите указание NetResident собирать все данные в сети. Вы всегда можете изменить эту настройку и выбрать отдельные станции для мониторинга. За более подробной информацией обратитесь к главе [Наблюдаемые станции](#).



Для перехода к странице выбора плагинов нажмите **Далее**. NetResident обрабатывает сетевой трафик с использованием специальных модулей-плагинов для каждого протокола. Если данные, передаваемые по определенному протоколу, не представляют для вас интереса, вы можете отключить соответствующий протокол, сняв метку возле его названия. За более подробной информацией обратитесь к главе [Плагины](#).



На следующей странице вы сможете настроить опции сетевого мониторинга. Если вы хотите начинать мониторинг сразу при старте Windows, выберите опцию **При запуске Windows**. Если вы хотите вести мониторинг лишь при запущенной программе NetResident, выберите опцию **При запуске NetResident**. Для сохранения введенных настроек нажмите **Далее**, а затем **Завершить**.

Обзор интерфейса

NetResident может отображать текущую информацию в разных видах, которые можно менять в меню **События => Просмотр** или из панели инструментов. Внешний вид приложения можно изменять, но в целом, главное окно приложения разделено на 3 секции, в каждой из которых представлены структурированные данные. В каждой секции можно производить сортировку и фильтрацию сетевых событий и получать к ним быстрый доступ.

Важно: в зависимости от [настроек поиска](#) главное окно программы может содержать несколько закладок: закладку **Все данные**, в которой отображается вся перехваченная информация, а также все другие закладки, соответствующие вашим [Группам поиска](#). Структура данных в закладках описана ниже.

Группы показывают события, объединенные по датам их наступления, сетевым протоколам и хостам, задействованным в обмене информацией. События, принадлежащие группе, можно вносить или удалять из списка **Событий**. Хосты сгруппированы по **Сторонам**, участвующим в процессе обмена информацией. **Сторона А** включает в себя все IP-адреса/имена хостов, участвующих в обмене на локальной стороне. Если для выхода в Интернет вы используете только один сетевой интерфейс, то **Сторона А** будет содержать одну запись. Если, к примеру, вы используете ваш сетевой адаптер как основной источник подключения к Интернету, а dial-up-подключением пользуетесь лишь изредка, и при каждом подключении вам выделяется динамический IP-адрес, то в этом случае вы увидите несколько записей. **Сторона В** содержит записи обо всех удаленных хостах, к которым подключались локальные хосты. За более подробной информацией обратитесь к главе [Систематизация данных](#)

Проводник во всем похож на группы, кроме того, что события группируются только по протоколам. Мы советуем пользоваться **Проводником** в том случае, если вы хотите просмотреть события, связанные с заданным протоколом, например, сообщения ICQ за определенный промежуток времени. Чтобы открыть узлы и просмотреть события, нажмите кнопку "+". За более подробной информацией обратитесь к главе [Систематизация данных](#)

Список **Событий** состоит из следующих колонок:

Дата – дата, когда произошло событие

Протокол – протокол, который был использован для передачи информации

Сторона А, Сторона В – хосты, которые передавали и принимали данные

Порт А, Порт В – порты, которые были использованы для передачи данных

Обновление – дата и время последнего обновления события

Описание – общие сведения о событии

ID – идентификатор события (скрыто по умолчанию)

Приоритет – пользовательский приоритет события (скрыто по умолчанию)

Комментарий – пользовательский комментарий к событию (скрыто по умолчанию)

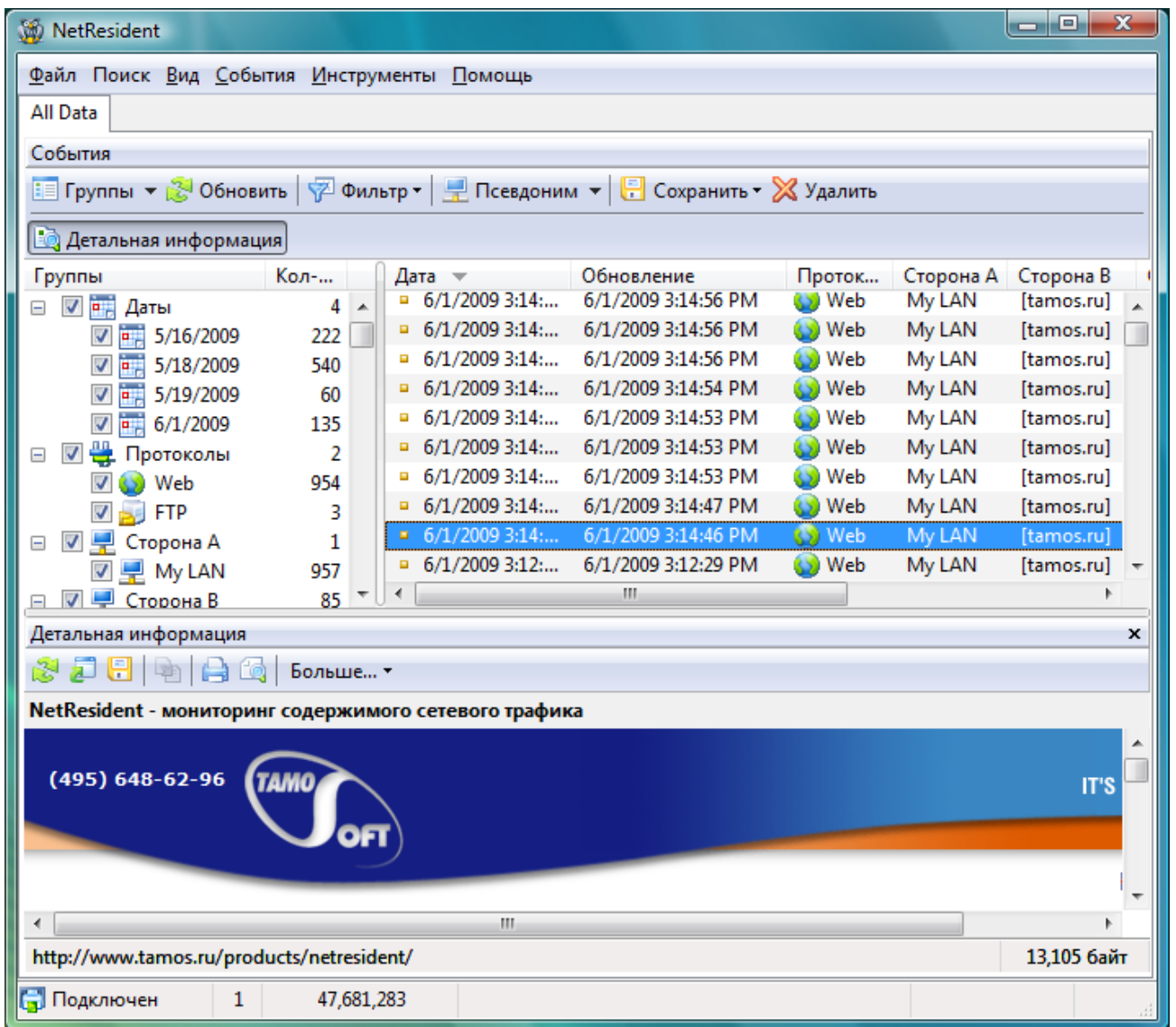
Флаги – флаги события (скрыто по умолчанию)

В секции **Детальная информация** показано реальное содержимое, соответствующее выбранному событию из списка **Событий**. В секции **Детальная информация** может быть показана информация только по одному выбранному событию.

В **Окне состояния** показаны системные сообщения программы.

NetResident состоит из двух частей: консоль подключается к сервису, обрабатывает данные, группирует их и предоставляет их пользователю. Сервис осуществляет мониторинг сети, перехват информации и ее сохранение в [базе данных](#) для последующей обработки и просмотра.

Для обработки собранной информации NetResident использует плагины. Чтобы просматривать только нужную вам информацию, отключите или включите соответствующие плагины.



Главное меню	
Файл	
Подключиться	Подключиться к сервису NetResident
Отключиться	Отключиться от сервиса NetResident
Управление базой данных	Запустить Мастер управления базой данных
Импорт трафика	Запустить мастер импортирования лог-файлов
Выход	Закреть программу
Поиск	
Найти	Поиск в событиях по заданной строке
Найти снова	Повторить поиск
Новая Группа Поиска	Запустить Мастер Группы Поиска

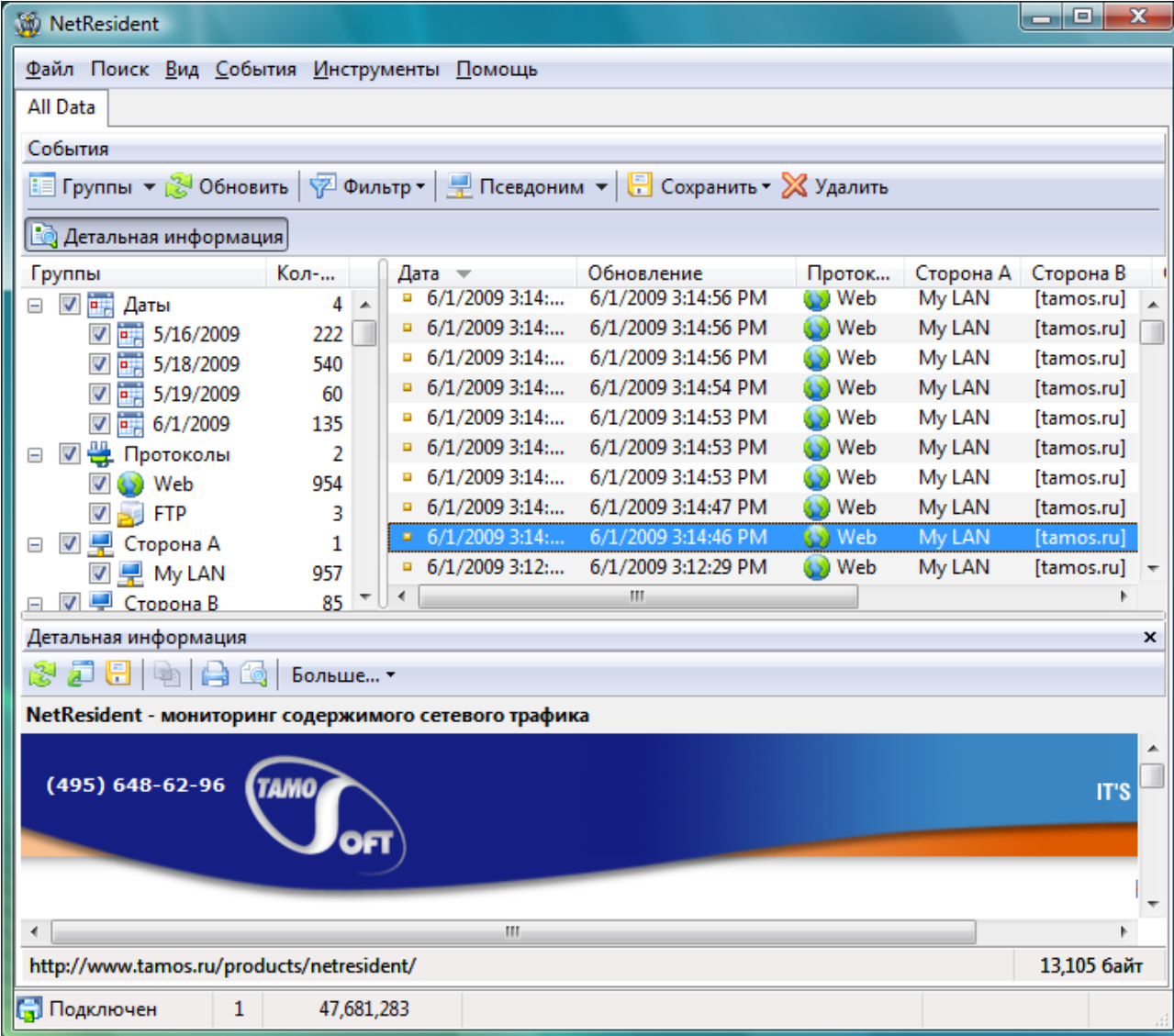
Удалить Группу Поиска	Удалить текущую активную Группу Поиска
Изменить Группу Поиска	Редактировать текущую Группу Поиска
Вид	
Окно состояния	Показать/скрыть окно состояния
Строка состояния	Показать/скрыть строку состояния
События	
Обновить	Обновить события/остановить обновление
Фильтр	Задать фильтры для событий
Сохранить	Сохранить список текущих событий или дополнительных данных в файл
Удалить	Удалить выбранные события из базы данных
Детальная информация	Показать/скрыть секцию Детальной информации
Просмотр	Переключить виды главного окна
Режим отображения хоста	Изменить режим отображения хостов в Группках и Событиях
Инструменты	
Псевдонимы	Показать диалог Псевдонимов
Настройки	Показать диалог Настроек
Мастер установки	Запустить Мастер установки
Anti-Switch Tool	Запустить утилиту PromiSwitch
Language	Выбрать язык интерфейса
Помощь	
Содержание	Открыть файл-справку
Искать в справке	Открыть форму поиска по справке
Обновления через Web	Проверить обновления на сайте TamoSoft
О программе	Показать информацию о программе

Систематизация данных

NetResident, являясь мощной программой сетевого мониторинга, предлагает вам полную картину всех событий, происходящих в сети. В нагруженной сети вы можете наблюдать сотни тысяч событий, таких как сообщения электронной почты, веб-страницы, сообщения и т. д. Таким образом, чтобы сразу просмотреть нужные вам события, потребуется упорядочить данные – это важный аспект при работе с NetResident. Мы предлагаем вам несколько возможностей для фильтрации данных.

Переключаемые виды **Проводник** и **Группы** позволяют вам по-разному взглянуть на события в сети. Мы советуем выбрать тот, который покажется вам наиболее удобным.

В секции **Группы**, расположенной в левой части главного окна программы, у вас будет возможность отфильтровать события по дате, сторонам, участвующим в обмене или по хостам.



The screenshot shows the NetResident application window. The menu bar includes 'Файл', 'Поиск', 'Вид', 'События', 'Инструменты', and 'Помощь'. The main area is titled 'События' and contains a toolbar with 'Обновить', 'Фильтр', 'Псевдоним', 'Сохранить', and 'Удалить'. Below the toolbar is a 'Детальная информация' section. The main display is a table with columns: 'Группы', 'Кол-...', 'Дата', 'Обновление', 'Проток...', 'Сторона А', and 'Сторона В'. The table lists events for various dates and protocols, with the selected row showing a Web event on 6/1/2009 at 3:14:46 PM from My LAN to [tamos.ru]. Below the table is another 'Детальная информация' section with a 'Больше...' button. At the bottom, there is a banner for TAMOSOFT and a status bar showing 'Подключен', '1', '47,681,283', and '13,105 байт'.

Группы	Кол-...	Дата	Обновление	Проток...	Сторона А	Сторона В
Даты	4	6/1/2009 3:14:...	6/1/2009 3:14:56 PM	Web	My LAN	[tamos.ru]
5/16/2009	222	6/1/2009 3:14:...	6/1/2009 3:14:56 PM	Web	My LAN	[tamos.ru]
5/18/2009	540	6/1/2009 3:14:...	6/1/2009 3:14:56 PM	Web	My LAN	[tamos.ru]
5/19/2009	60	6/1/2009 3:14:...	6/1/2009 3:14:54 PM	Web	My LAN	[tamos.ru]
6/1/2009	135	6/1/2009 3:14:...	6/1/2009 3:14:53 PM	Web	My LAN	[tamos.ru]
Протоколы	2	6/1/2009 3:14:...	6/1/2009 3:14:53 PM	Web	My LAN	[tamos.ru]
Web	954	6/1/2009 3:14:...	6/1/2009 3:14:53 PM	Web	My LAN	[tamos.ru]
FTP	3	6/1/2009 3:14:...	6/1/2009 3:14:47 PM	Web	My LAN	[tamos.ru]
Сторона А	1	6/1/2009 3:14:...	6/1/2009 3:14:46 PM	Web	My LAN	[tamos.ru]
My LAN	957	6/1/2009 3:12:...	6/1/2009 3:12:29 PM	Web	My LAN	[tamos.ru]
Сторона В	85					

- **Даты** – укажите интересующие вас даты. Все события, которые произойдут в другое время, будут проигнорированы и не будут показаны в списке **Событий**. Помните, что удаление дат из секции **Группы** не приведет к их удалению из базы данных. Вы можете изменить настройки **Групп** и показывать те события, которые не были запротоколированы программой.
- **Протоколы** – укажите интересующие вас протоколы. Например, если вы хотите просмотреть сообщения электронной почты, выберите протокол **Mail**.
- **Сторона А / Сторона В** – фильтрация событий по сторонам, участвующим в обмене информацией. Вы найдете эти хосты в узлах **Сторона А** и **Сторона В**. Укажите те хосты, события с которых вы хотите наблюдать.

Вы можете комбинировать фильтры. Например, если требуется просмотреть только веб-страницы, загруженные с определенного сервера в определенный день, выберите дату в секции **Даты**, выберите **Web** в секции **Протоколы** и укажите хост в секции **Сторона В**. Все события, не подпадающие под этот комбинированный критерий, будут проигнорированы.

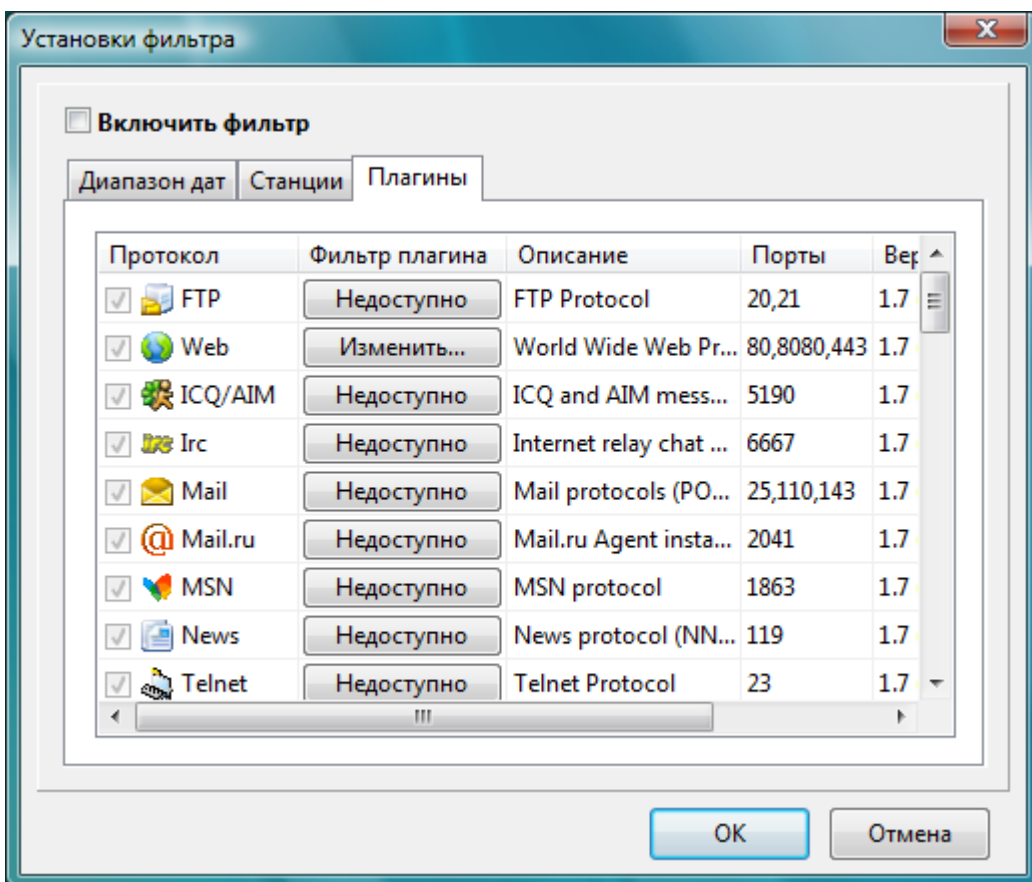
Более гибкий фильтр можно найти в меню **События => Фильтр** или выбрав в панели инструментов **Фильтр**. Здесь вы можете задать предопределенный период:

- **Сегодня** – показать все события в сети за сегодня
- **Последние 2 дня** – показать все события в сети за последние два дня
- **Последняя неделя** – показать все события в сети за последнюю неделю
- **Последний месяц** – показать все события в сети за последний месяц

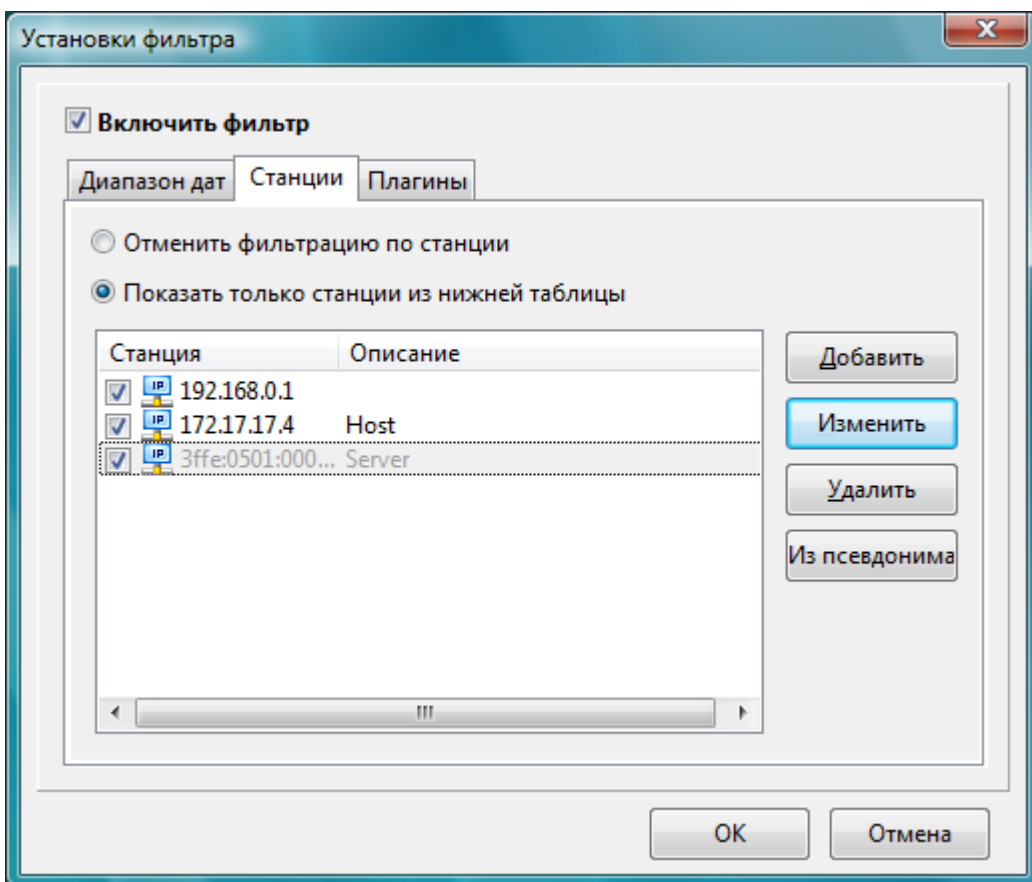
Выбрав **Все дни**, вы увидите все события, которые произошли в сети за весь период мониторинга. Можно выбрать **Свой период**, указав дату начала и окончания мониторинга в выпадающих списках **С:** и **По:**.

The screenshot shows a software interface with a toolbar at the top containing icons for 'Фильтр' (Filter), 'Псевдоним' (Alias), 'Сохранить' (Save), and 'Удалить' (Delete). A dropdown menu is open under 'Фильтр', showing options: 'Фильтр включен', 'Сегодня', 'Последние 2 дня', 'Последняя неделя', 'Последний месяц', 'Свой период...' (highlighted), 'Все дни' (checked), and 'Дополнительно...'. A sub-menu for 'Свой период...' is also open, showing 'Задать даты...' and a date range '13.05.2009 - 14.05.2009'. In the background, a table of network events is visible with columns: 'Обновление', 'Проток...', 'Сторона А', and 'Сторона В'. The table contains several rows of data, including timestamps, protocols (Web), and IP addresses (My LAN).

Дополнительные возможности фильтрации доступны через меню **События => Фильтр => Дополнительно**. Вы также можете отфильтровать события по плагинам сетевых протоколов или по станциям.



На странице **Плагины** отображается список всех установленных плагинов. Напротив активных плагинов стоят метки. Если вам нужны только определенные плагины (например, требуется лишь просмотреть сообщения электронной почты и содержимое веб-страниц), снимите метки напротив ненужных плагинов. Если в плагине предусмотрены дополнительные возможности фильтрации, нажмите **Изменить** для настройки этого плагина. За более подробной информацией обратитесь к главе [Плагины](#).



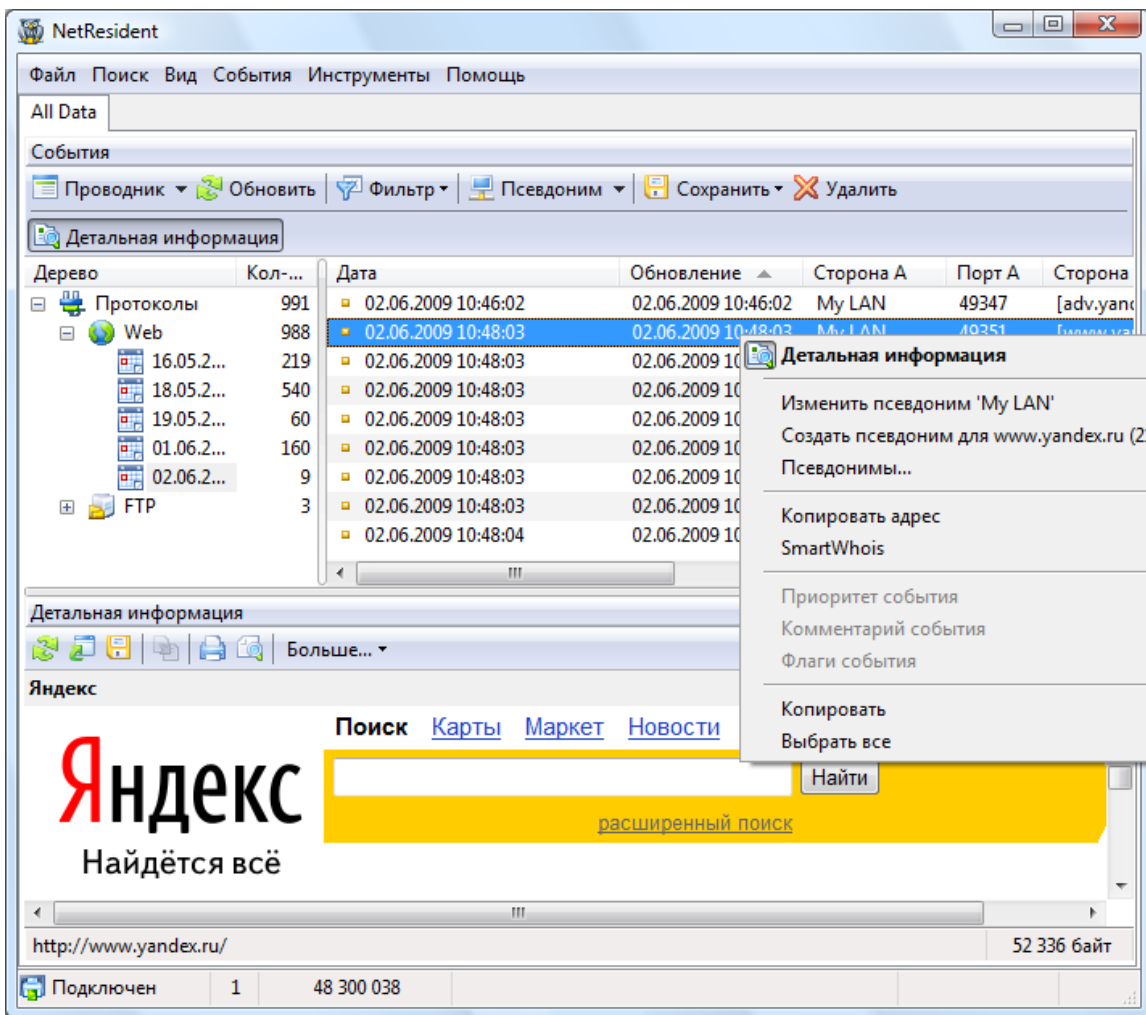
В NetResident можно показывать лишь те данные, которые поступили от выбранных станций (компьютеров, маршрутизаторов и других устройств, подключенных к вашей локальной сети). В этом случае NetResident покажет только исходящую/входящую информацию для станций, указанных в таблице закладки **Станции**. Вы можете добавить другие станции, выбрав опцию **Показать только станции из нижней таблицы**, нажав **Добавить** и указав IP-адрес, диапазон IP-адресов или MAC-адрес станции. Если вы заранее определили псевдонимы для хостов, нажмите **Из псевдонима** и выберите вашу станцию из списка псевдонимов. Для каждой новой станции можно указать описание, но это необязательно. Чтобы редактировать станцию, выберите ее и нажмите **Изменить**. Чтобы удалить станцию, выберите ее и нажмите **Удалить**.

Для сохранения настроек фильтрации нажмите **OK**. Для отмены введенных установок нажмите кнопку **Отмена**.

Чтобы временно отключить фильтр без сброса установок, снимите метку **Включить фильтр**.

Важное замечание: установки фильтрации будут применяться только к тем данным, которые отображаются в главном окне программы. Настройки фильтрации не повлияют на процесс сбора и сохранения информации. Процесс сбора информации описан в главе [Настройка NetResident](#), а хранение – в главе [Управление базой данных](#).

В **Проводнике** можно отфильтровать события по сетевым протоколам.



Откройте требуемые узлы, нажав на знак (+). Если вы хотите просмотреть веб-страницы, откройте узел Web. Открыв узел, вы увидите события, относящиеся к определенному протоколу, сгруппированные по датам. Если вы хотите просмотреть события, которые произошли в определенный день, выберите слева нужную группу и справа будут показаны сами сообщения. Виды **Проводник** и **Группы** схожи во всем кроме группировки событий.

Просмотр сетевых событий

Процесс обмена информацией представлен в виде сетевых событий. Такими событиями могут быть сообщения электронной почты, файлы, загруженные с FTP, веб-страницы или сообщения ICQ. После настройки фильтрации в список **События** будут занесены сетевые события, которые отображены программой из базы данных.

Каждая строка в таблице **Событий** соответствует отдельному событию в сети.

Дата	Обновление	Протокол	Сторона А	Сторона В	Описание
02.06.2009 10:...	02.06.2009 10:48:03	Web	My LAN	[img.yand...	img.yandex.net:G
02.06.2009 10:...	02.06.2009 10:48:03	Web	My LAN	[www.yan...	www.yandex.ru:G
02.06.2009 10:...	02.06.2009 10:46:02	Web	My LAN	[adv.yand...	crls.yandex.ru:GE
01.06.2009 16:...	01.06.2009 16:08:14	Web	My LAN	[tamos.ru]	www.tamos.ru:GE

Детальная информация

Изменить псевдоним 'My LAN'
Создать псевдоним для tamos.ru (216.92.210.111)
Псевдонимы...

Копировать адрес ▶
SmartWhois ▶

Приоритет события
Комментарий события
Флаги события

Копировать
Выбрать все

Таблица содержит следующие колонки:

- **Дата** – дата и время начала события.
- **Протокол** – протокол, который был использован для передачи данных. Название протокола соответствует названию плагина, который отвечает за обработку данного события.
- **Сторона А / Сторона В** – стороны, участвующие в обмене данными в сети. Примером стороны может быть компьютер, на котором просматривается веб-страница или компьютер, получающий электронную почту, а также сам почтовый сервер.
- **Описание** – краткое описание события, которое включает в себя размер переданного или полученного фрагмента данных.
- **Порт А / Порт В** – порты, которые были использованы для передачи данных.
- **Обновление** – дата и время последнего обновления события.
- **ID** – идентификатор события (скрыто по умолчанию)
- **Приоритет** – пользовательский приоритет события (скрыто по умолчанию)
- **Комментарий** – пользовательский комментарий к событию (скрыто по умолчанию)
- **Флаги** – флаги события (скрыто по умолчанию)

Стороны А и В, участвующие в обмене, могут быть представлены как IP- или MAC-адресами, так и именами хостов. Настройки отображения можно поменять в **События => Режим отображения хоста**.

IP- или MAC-адреса можно заменить [псевдонимами](#). Нажмите правой кнопкой мыши на любом сетевом событии и в появившемся меню выберите адрес, для которого надо создать псевдоним, или откройте список псевдонимов.

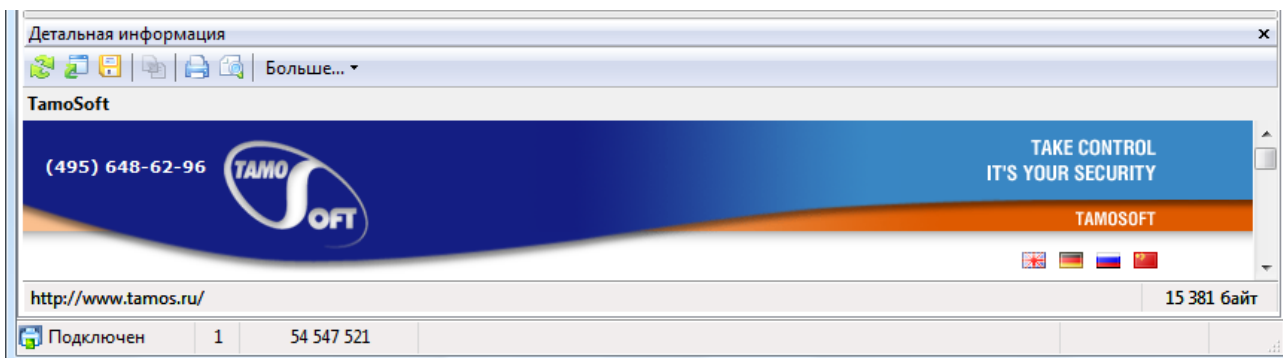
Чтобы сохранить список в HTML-файл, выберите **События => Сохранить** или нажмите соответствующую кнопку в панели инструментов.

Чтобы просмотреть дополнительную информацию о событии, выберите это событие в списке и кликните правой кнопкой мыши, затем в меню выберите **Детальная информация**.

Важное замечание: в режиме "Проводник" некоторых колонок может не быть. Например, если выбран протокол, то колонка с протоколами показана не будет.

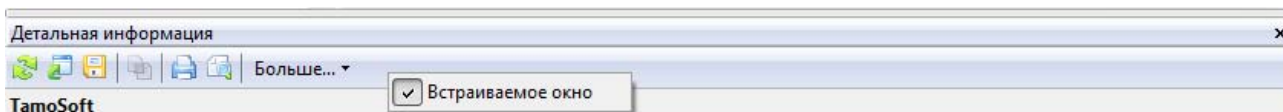
Просмотр детальной информации о событии

В секции **Дополнительная информация** главного окна приложения будет показано восстановленное сетевое событие. Чтобы показать эту секцию, выберите в меню **События => Детальная информация** или нажмите правой кнопкой мыши на самом событии в списке и в появившемся меню выберите **Детальная информация**. Плагины NetResident обработают информацию и предоставят восстановленную веб-страницу, сообщение электронной почты, сообщение ICQ и т. п.



Как только из списка будет выбрано событие, NetResident создаст запрос к базе данных, восстановит данное событие и отобразит результаты в секции **Детальная информация**. Помимо отображения самого события, программа покажет полезную техническую информацию о событии, такую, как HTTP-заголовки веб-страниц, заголовки сообщений электронной почты и протоколы ftp-подключений при загрузке файлов.

У секции **Детальная информация** есть панель инструментов, вид которой зависит от типа выбранного события.



Эту панель можно перемещать мышью по главному окну программы. Чтобы вернуть ее обратно, перемещайте ее по главному окну до тех пор, пока она не "приклеится" к одной из сторон окна. Чтобы впоследствии свободно перемещать это окно, кликните по заголовку окна правой кнопкой мыши и уберите опцию **Встраиваемое окно**.

В данном окне можно вызвать контекстное меню со следующими пунктами:

- Настройки интерфейса** – настроить шрифты для выбранного события
- Копировать** – копировать выделенный фрагмент данных в буфер обмена
- Выделить все** – выделить все данные, которые относятся к событию

В дополнение к основным опциям, в зависимости от типа события, каждый плагин добавляет в меню свои пункты. Например, **Показать логин/пароль** показывает логин и пароль, которые использовались для сеанса связи (только для входящих сообщений); **Показать заголовки** – отобразить заголовки HTTP-сессий (только для веб-страниц) и т. д.

Настройка NetResident

Настройки программы доступны в меню **Инструменты => Настройки**. Если вы не очень хорошо знакомы с организацией и работой в сети, то для настройки программы мы советуем воспользоваться Мастером.

Все необходимые настройки можно задать в окне **Настройки**. Для этого выберите слева нужную вам категорию.

Интерфейс: Общие установки

Здесь можно выбрать шрифт интерфейса и настроить условия обновления программы через Web.

Для работы программы в фоновом режиме выберите опцию **Показывать значок в трее**. Кроме этого, вы можете включить опцию **Убирать из панели задач при сворачивании**, в случае, если вы не хотите, чтобы окно программы отображалось на панели задач при сворачивании в трей.

Чтобы активировать обновления, установите флаг **Включить автоматические обновления**. Вы также можете указать интервал между проверками в поле **Интервал между проверками, дни**. Чтобы проверить обновления немедленно, нажмите кнопку **Проверить сейчас**.

Сеть: Запуск

Здесь можно настроить параметры сетевого мониторинга, которые выполняются [Сервисом NetResident](#).

Если требуется постоянный мониторинг сети, выберите опцию **При запуске Windows**. Когда выбрана эта опция, сервис NetResident будет загружен при старте операционной системы и сразу же начнет мониторинг. Вы можете в любой момент открыть программу NetResident и просмотреть результаты мониторинга.

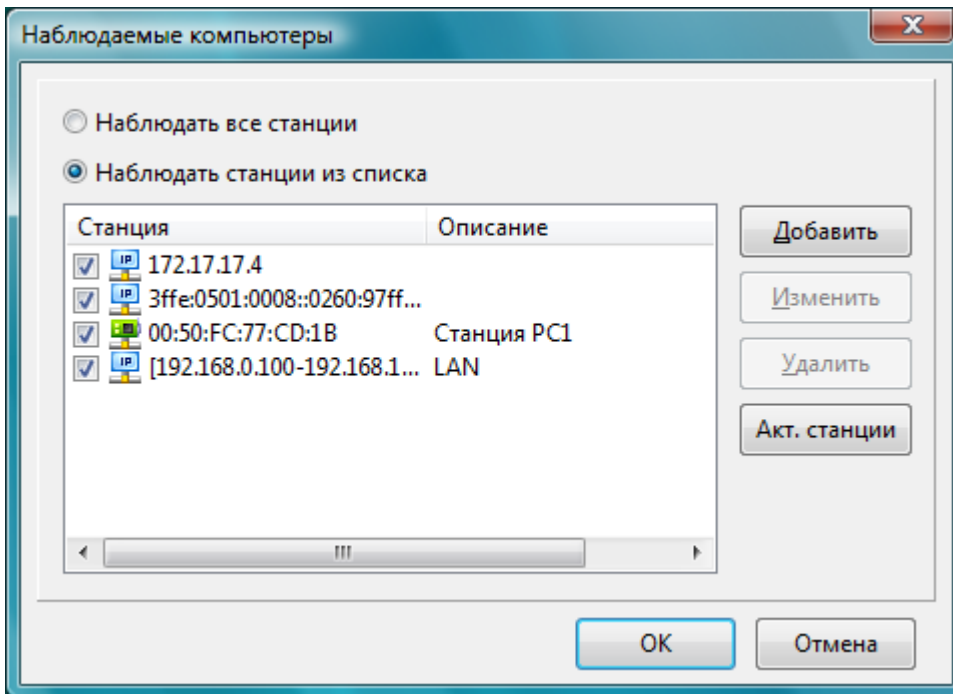
Если вы пользуетесь программой периодически и вам не требуется постоянный мониторинг, выберите опцию **При запуске NetResident**. Это позволит снизить нагрузку на процессор и уменьшить загрузку жесткого диска. В данном случае сервис NetResident будет начинать работу одновременно с программой и будет остановлен при ее закрытии.

Сеть: Цели

В подпункте **Цели** вы увидите выпадающий список, из которого следует выбрать адаптер для мониторинга. Если у вас dial-up-соединение или вы подключены к локальной сети через Ethernet-адаптер, в меню будет лишь один адаптер. Выберите его. Если ваш компьютер является Интернет-шлюзом для локальной сети или на нем установлено несколько сетевых адаптеров, выберите из списка именно тот, который вы хотите наблюдать с помощью NetResident. Некоторые сетевые адаптеры не могут работать в режиме "promiscuous" (состояние, в котором сетевой адаптер обнаруживает в сети все пакеты вне зависимости от их конечного адреса). Если вы работаете с таким адаптером, выберите опцию **Использовать режим "non-promiscuous"**. Для беспроводных (802.11) адаптеров эта опция должна быть активна всегда. Для работы с dial-up- или VPN-адаптерами выберите адаптер **WAN miniport**.

Для анализа данных со всех компьютеров вашей сети выберите **Наблюдать все станции**. Если активность вашей сети достаточно высока, возможно, вы захотите сузить список наблюдаемых станций. Нажмите **Дополнительно** и выберите **Наблюдать станции из списка**. Отметьте станции для мониторинга. Если кнопка **Дополнительно** недоступна, отключите опцию **Наблюдать все станции** и кнопка станет доступна.

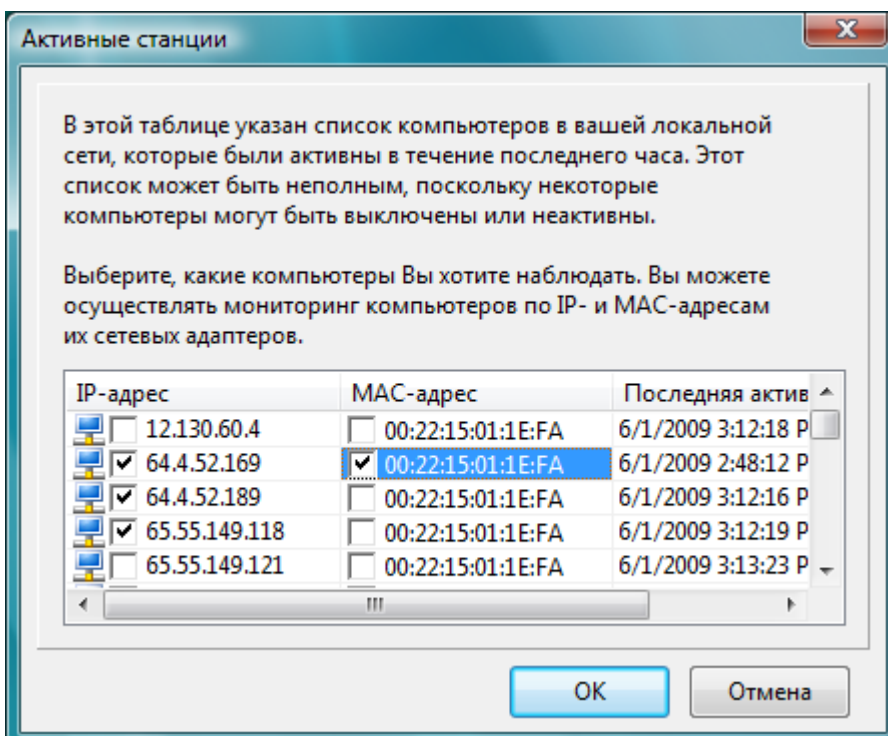
Наблюдаемые станции



Чтобы добавить новую станцию, нажмите **Добавить** и введите IP-адрес, MAC-адрес или группу IP-адресов. В поле **Описание** можно ввести любую информацию о добавляемой станции. Это поле необязательно для заполнения.

Чтобы сохранить изменения, нажмите **OK**. Чтобы отменить сохранение введенных данных, нажмите **Отмена**. Чтобы изменить или удалить какую-либо запись, воспользуйтесь кнопками **Изменить** и **Удалить**. Если требуется временно отключить мониторинг какой-либо станции без удаления из списка, снимите соответствующую метку слева от станции.

Вы также можете добавить активные станции, нажав на кнопку **Акт. станции** и выбрав активные станции, обнаруженные программой NetResident:



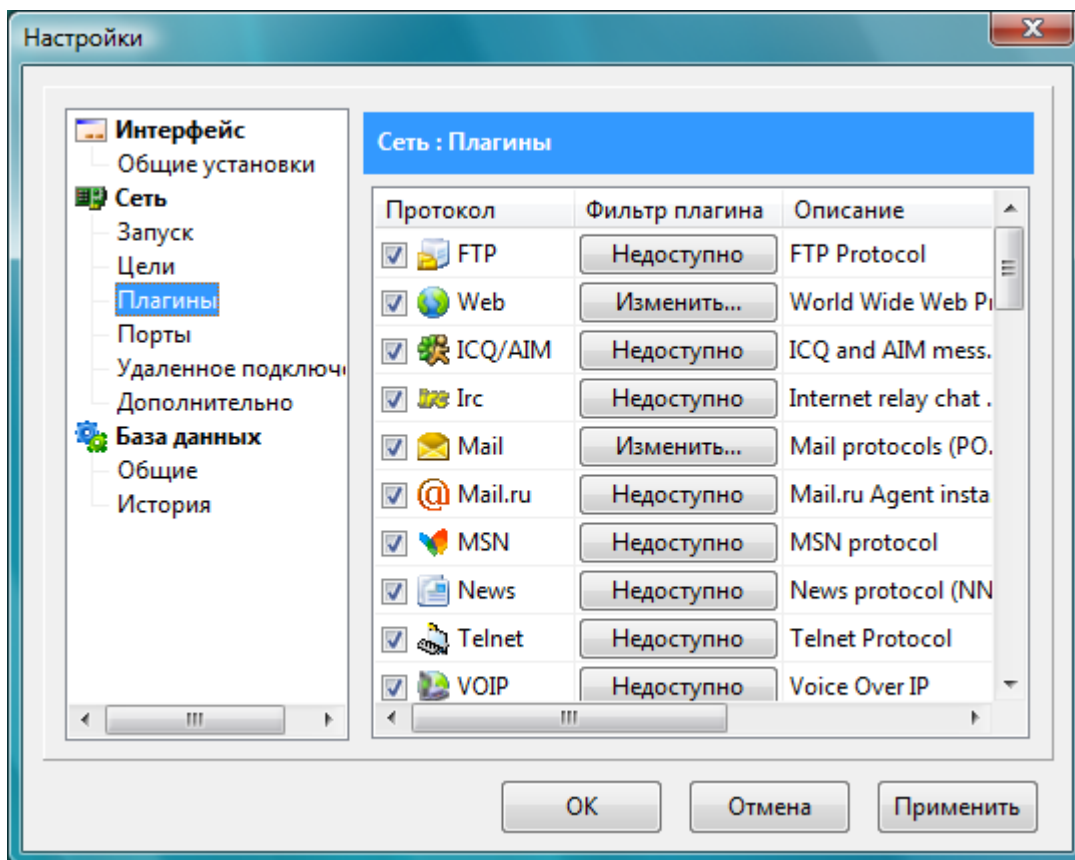
Выберите нужный адрес и нажмите **ОК**. Выбранный адрес будет добавлен в список станций для мониторинга.

Помните, что список станций может быть неполным, поскольку некоторые станции могут быть отключены или изменить свои адреса. К тому же, некоторые станции могут быть "спрятаны" за файрволлы. Поэтому мы советуем относиться к этому списку как приблизительному.

Если вы не уверены, какой адрес вам нужно использовать для идентификации наблюдаемой станции (MAC или IP), обратитесь к разделу [Ответов на вопросы](#).

Сеть: Плагины

На этой странице отображены плагины, установленные в настоящее время. Если какие-либо плагины вам не требуются, мы советуем их отключить для снижения нагрузки на процессор или для экономии места на диске.



Вы также можете использовать собственные фильтры плагинов для указания дополнительных критериев фильтрации. Дополнительная фильтрация сообщений уменьшает количество перехваченных событий и, как следствие, объем использованной дисковой памяти, требуемый для работы. Для изменения настроек фильтра, нажмите на кнопку **Изменить** желаемого плагина. Более подробная информация доступна в разделе [Плагины](#) настоящего руководства.

Замечание: в настоящий момент собственные фильтры имеют только плагины Web и Mail.

Сеть: Порты

На этой странице вы можете настроить порты, которые используются NetResident для мониторинга.

По умолчанию сервис NetResident настроен на мониторинг трафика со всех возможных портов (1-65535). В этом случае вы можете быть уверены, что будет перехвачена вся информация в сети. Тем не менее, обработка всех сетевых пакетов может сопровождаться значительными нагрузками на процессор. Если у вас возникают проблемы с производительностью вашей системы, попробуйте уменьшить количество портов для мониторинга. Например, если вы хотите наблюдать трафик в вашей локальной офисной сети, где большинство трафика генерируется при передаче файлов с одной машины на другую посредством Microsoft Windows, вы можете исключить этот трафик из наблюдения, введя следующую строку:

В этой строке порты 139 и 145 исключаются из процесса мониторинга. Если вы не знаете, что такое сетевые порты или не испытываете каких-либо затруднений, связанных с понижением производительности вашего компьютера, не меняйте никаких значений на этой странице.

Вы можете указать один, несколько или область портов, разделяя эти значения запятыми. Пожалуйста, помните, что исключение портов будет справедливо как для портов-источников, так и для портов назначения.

Сеть: Удаленное подключение

На этой странице вы можете настроить удаленные подключения к сервису NetResident. Подробности в главе [Удаленные подключения к сервису NetResident](#).

Сеть: Дополнительно

На этой странице можно настроить работу системы протоколирования. Опция **Включить протоколирование для сервиса** включена по умолчанию и установлен уровень **Минимальное**. В случае возникновения каких-либо проблем с NetResident, служба поддержки TamoSoft может попросить вас изменить уровень ведения протокола в том случае, если понадобится дополнительная информация. Служебные сообщения NetResident записываются в файл DebugCWS.log, который находится в той же папке, что и программа. Служба поддержки TamoSoft может попросить вас выслать этот файл по электронной почте. Помните, что лог-файл может достигать значительных размеров при выбранной опции **Подробное**. Поэтому перед отправкой лог-файла желательно его заархивировать.

Опция **Автоматический импорт** предназначена для автоматического импорта лог-файлов, в которых содержится перехваченный сетевой трафик. Чтобы воспользоваться этой возможностью, активируйте метку **Включить автоматический импорт** и выберите директорию, в которой находятся требуемые лог-файлы.

Замечание: директория, содержащая лог-файлы для импорта, должна быть локальной, т. е. находиться на том же самом компьютере, где работает сервис NetResident.

База данных: Общие

В NetResident предусмотрена своя собственная база данных, в которой хранится вся перехваченная и проанализированная информация. По умолчанию файлы базы данных находятся в директории программы. На данной странице вы сможете изменить местоположение базы данных, если возникнет такая необходимость. Для этого выберите директорию, где должна находиться база данных и нажмите **Применить**.

База данных: История

Поскольку база данных содержит все события, перехваченные NetResident, то ее размер со временем увеличивается. Чтобы уменьшить объем памяти, занимаемой этими событиями и увеличить производительность программы, вы можете установить ограничение на размер базы данных. Для этого установите соответствующий флаг. Вы также можете удалить события, которые старше определенного количества дней.

При выходе из программы содержимое базы данных можно очистить – для этого отметьте опцию **Очищать базу данных при выходе**.

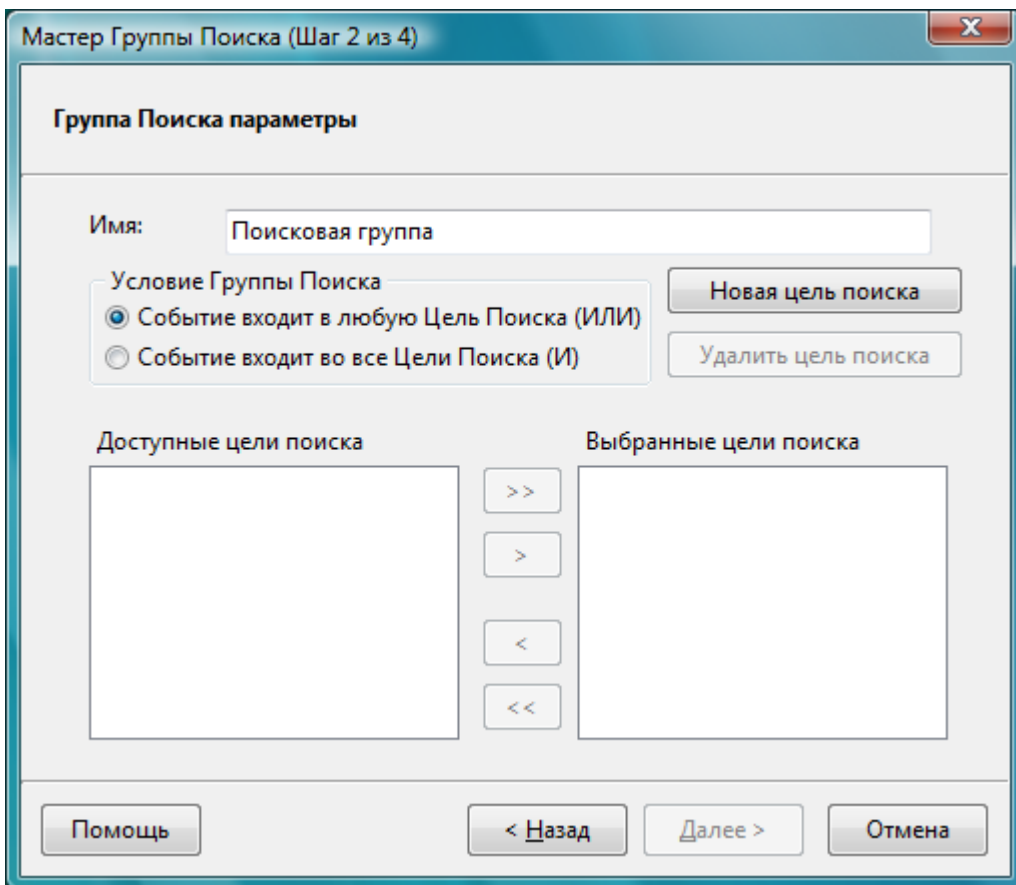
Также вы можете архивировать старые записи вместо их удаления. Для архивации записей, выберите опцию **Создать архивную копию** и укажите путь для сохранения записей. Используйте [Мастер управления базой данных](#) для последующего восстановления архивных записей.

Расширенный поиск

Расширенный поиск позволяет вам найти практически любую информацию в базе данных NetResident, упрощая анализ перехваченных сетевых событий. В базе предусмотрен поиск определенных типов данных, таких как содержимое веб-страниц, текст URL, заголовки сообщений электронной почты и т. п. Для каждого [плагина](#) NetResident предусмотрены свои поля поиска. Вы можете искать и создавать предупреждения для уже перехваченных данных или для данных, которые будут перехвачены в будущем. При этом используются два типа данных: **Цель Поиска** и **Группа Поиска**.

Цель Поиска является простым критерием поиска, который используется программой NetResident при обработке базы данных. Это может быть ключевым словом в коде HTML, сообщении электронной почты, тексте URL и т. п. **Цели Поиска** варьируются в зависимости от плагина. **Группа Поиска** состоит из одной или многих **Целей Поиска**, что позволяет использовать комбинации критериев при выполнении поискового запроса.

Для создания новой поисковой группы выберите **Поиск => Новая Группа Поиска**. С помощью **Мастера Группы Поиска** вы сможете создать новый поисковый фильтр буквально за несколько кликов. На начальной странице Мастера нажмите **Далее** и перейдите к окну Параметров Группы Поиска.



Для создания группы вам потребуется ввести уникальное название, выбрать **Условие Группы Поиска** и **Доступные цели поиска**, которые вы хотите включить в группу. Обратите внимание, что для активации всех элементов данной формы необходимо задать **Имя** группы поиска. Для создания новой цели нажмите кнопку **Новая Цель Поиска** и в появившемся диалоге нажмите **Далее**. Для создания Цели Поиска введите уникальное название (имя), выберите необходимый плагин, поле плагина, которое нужно использовать при поиске, а также значение этого поля. Например, если вы хотите выполнить поиск в Web-страницах по слову "бомба", задайте уникальное имя Цели Поиска (например, "Бомба"), выберите плагин Web, поле "Text" и введите одно или несколько ключевых слов (например, "бомба" или "бомба, взрывчатка").

Подсказка: вы можете ввести несколько значений одновременно, разделив их запятыми.

Мастер Цели Поиска (Шаг 2 из 3)

Цель Поиска параметры

Имя:

Плагин:

Поле:

Значение:

Учитывать регистр символов

Только слово целиком

Применить только к будущим событиям

Доступны следующие дополнительные опции:

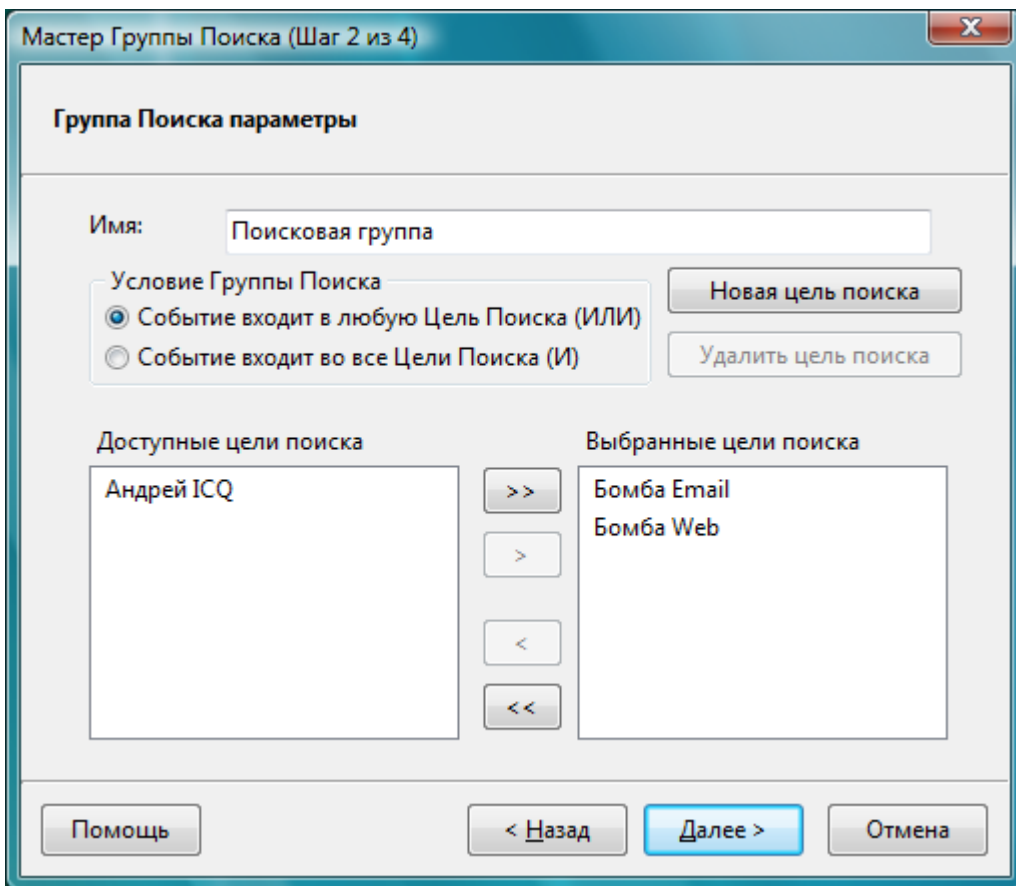
Учитывать регистр символов – если опция активна, то регистр введенной поисковой фразы должен соответствовать регистру символов в событии, где производится поиск.

Только слово целиком – если опция активна, то все подстроки будут игнорироваться.

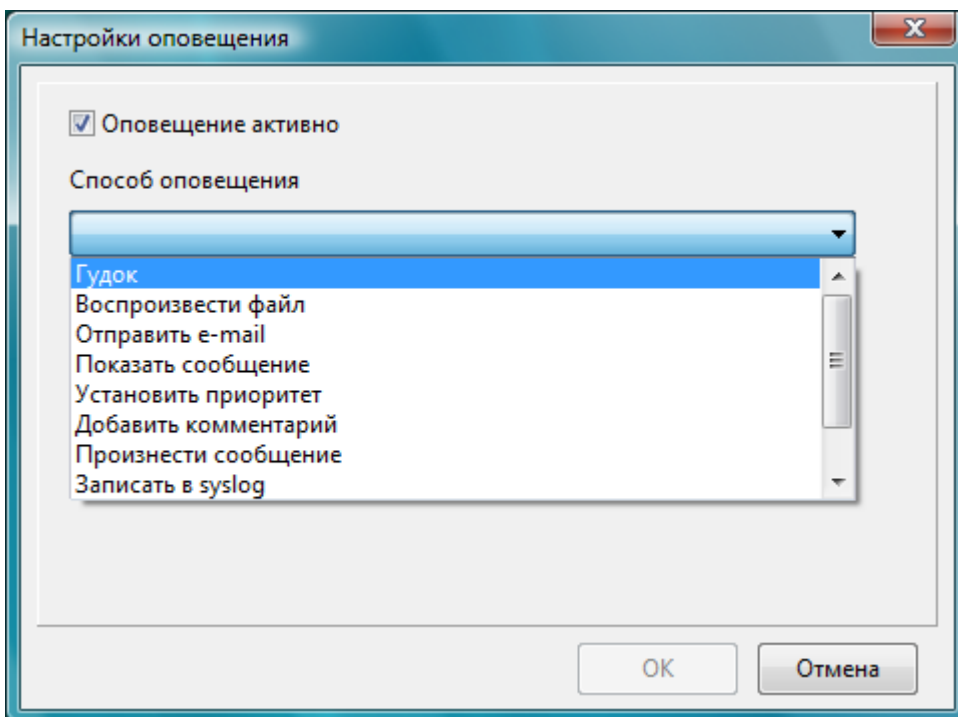
Применить только к будущим событиям – если опция активна, поиск будет выполняться только для новых записей. В противном случае будут обработаны все записи в базе данных, включая созданные в прошлом.

Замечание: каждая Цель Поиска требует дополнительных операций с базой данных, поэтому мы советуем минимизировать количество целей для снижения потребления ресурсов компьютера. Для этого просто удалите ненужные Цели Поиска.

Нажмите **Далее**, потом **Завершить**. Мастер Цели Поиска будет закрыт.



Поместите цели в список **Выбранных целей поиска**. Нажмите **Далее** и выберите способ оповещения.



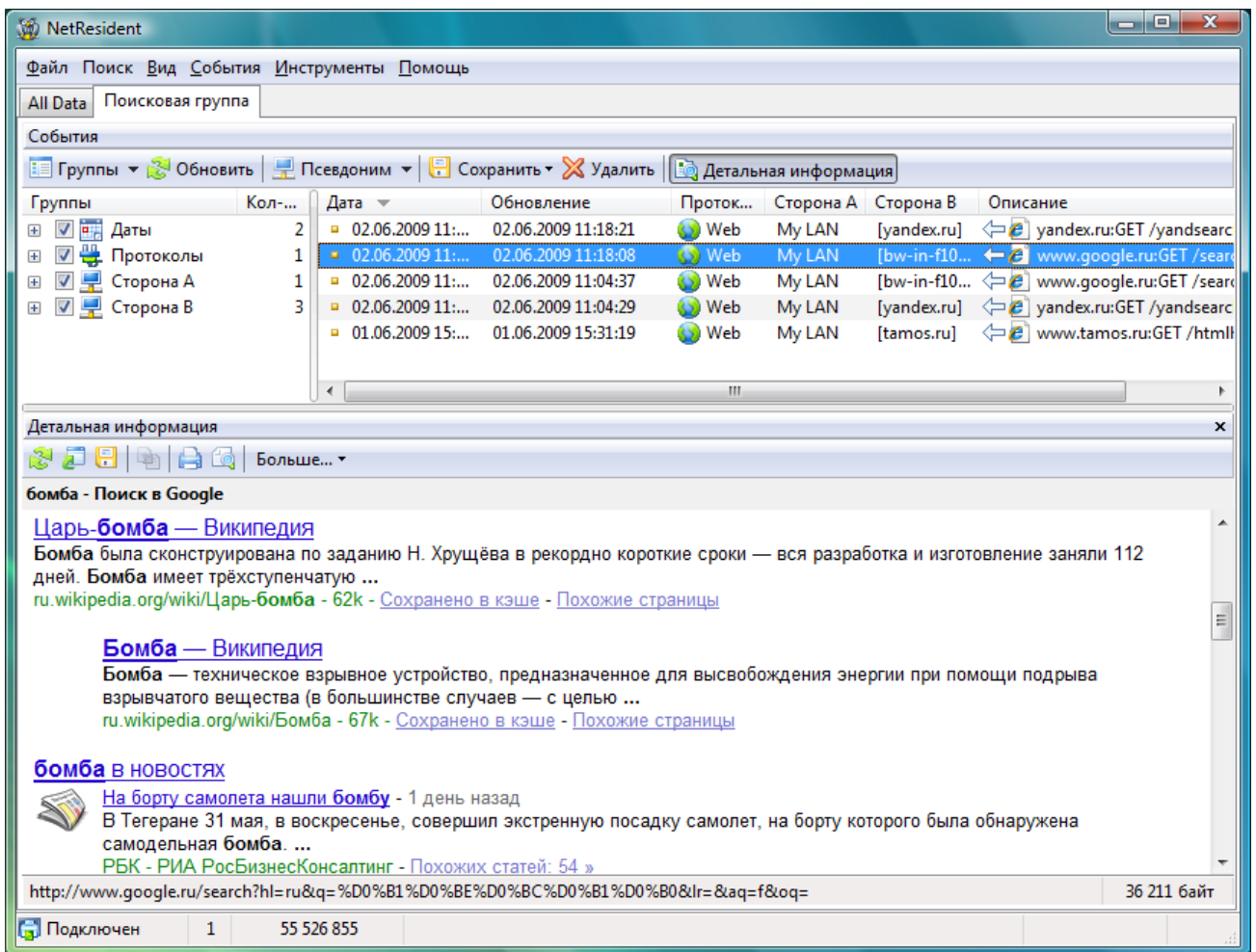
В окне выбора **Способа оповещения** вы можете указать действие, которое будет выполнено при совпадении содержания Группы Поиска и вашего критерия. Варианты действий могут быть следующими:

- **Гудок:** компьютер издает звуковой сигнал.
- **Воспроизвести файл:** компьютер воспроизведет указанный звуковой файл WAV.
- **Отправить e-mail:** компьютер отправит сообщение на указанный адрес электронной почты. Перед отправкой сообщений вам **ОБЯЗАТЕЛЬНО** потребуется настроить NetResident для работы с вашим SMTP-сервером. Для ввода параметров SMTP воспользуйтесь кнопкой **Настройка e-mail**. Сообщения электронной почты часто используются для отправки уведомлений на сервисы мгновенных сообщений, сотовые телефоны или пейджеры. Так, для отправки сообщения пользователю ICQ введите адрес в виде ICQ_USER_UIN@pager.icq.com, где ICQ_USER_UIN – уникальный номер пользователя ICQ и активизируйте возможность использования EmailExpress в настройках клиента ICQ. За более подробной информацией обратитесь к документации программы мгновенных сообщений или к оператору сотовой связи. Для ввода произвольного тела письма воспользуйтесь полем **Текст сообщения e-mail**.
- **Показать сообщение:** компьютер отобразит предупреждение с указанным вами текстом.
- **Установить приоритет:** установка приоритета события.
- **Добавить комментарий:** добавление комментария.
- **Произнести сообщение:** произнести указанный текст посредством встроенного движка Windows. По умолчанию Windows поставляется только с английскими компьютерными голосами, поэтому возможна ситуация, когда произнесение сообщений с текстом отличным от английского невозможно.
- **Записать в syslog:** отправить сообщение по указанному адресу посредством протокола syslog.
- **Отправить SNMP trap:** отправить сообщение на указанный IP-адрес по протоколу SNMP. MIB-файл, содержащий описания OID, может быть предоставлен по запросу.
- **Запустить приложение:** запускает указанное приложение (доступны опции командной строки).

Если вам требуется временно отключить какие-либо из вышеуказанных опций, это можно сделать снятием соответствующих меток.

Замечание: такие действия, как **Гудок**, **Воспроизвести файл**, **Показать сообщение**, **Воспроизвести сообщение** или **Запустить приложение** будут работать только при открытом клиентском приложении NetResident.

Выберите соответствующие действия и нажмите **Далее**. Созданная вами Группа Поиска будет сохранена в базе данных, а в главном окне программы появится закладка с соответствующим названием. Все записи, удовлетворяющие критериям поиска (Целям Поиска), будут отображены в этой закладке.



Если вы хотите изменить или удалить Группу Поиска, воспользуйтесь соответствующими пунктами меню **Поиск**.

Псевдонимы

Псевдонимы – это легко запоминаемые названия, заменяющие собой MAC- и IP-адреса, которые показаны в **Группах** и в секции **События** главного окна программы. Таким образом, псевдонимы существенно облегчают распознавание и анализ событий в сети.

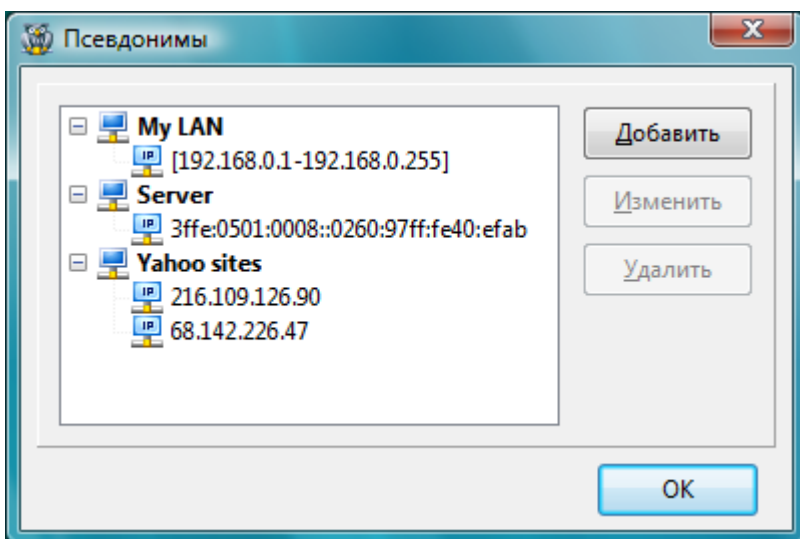
После того, как IP- или MAC-адресу будет назначен псевдоним, он заменит собой соответствующие адреса в **Группах** и в секции **События**. Вы можете выбрать, как именно будут показаны хосты: по IP-адресу, MAC-адресу или псевдониму. Эти настройки доступны в меню **События => Режим отображения хоста**.

В программе есть возможность преобразования IP-адресов в имена хостов. Для этого в меню **События => Режим отображения хоста** установите опцию **Преобразовывать численные IP-адреса в имена хостов**.

Псевдоним может быть также присвоен сразу целой области IP-адресов. Это очень удобно, поскольку по одному имени можно обращаться сразу к целой группе устройств, например, ко всем компьютерам в локальной сети.

Каждый псевдоним уникален. Тем не менее, вы можете назначить один и тот же псевдоним разным MAC- и IP-адресам, тем самым сформировав группу. Это может быть полезным, если у компьютера несколько сетевых адресов, и вы хотите свести все эти адреса в одно название.

Псевдонимы можно добавлять, редактировать или удалять, вызвав редактор псевдонимов в меню **Инструменты => Псевдонимы**.



Чтобы добавить станцию, нажмите **Добавить**. Введите название псевдонима и нажмите **Добавить**. Откроется диалог, в котором нужно будет ввести адрес и указать его тип: **IP-адрес**, **Диапазон IP-адресов** или **MAC-адрес**. Если вы хотите ввести диапазон IP-адресов, выберите опцию **Диапазон IP-адресов** и введите в соответствующие поля начальный и конечный IP-адреса.

Чтобы внести изменения в список псевдонимов, нажмите **OK**. Для отмены изменений нажмите **Отмена**.

Псевдонимы можно назначать и хостам, нажав правой кнопкой мыши на событии в списке и выбрав соответствующий пункт из появившегося меню.

Импортирование лог-файлов с пакетами

Для визуального представления и анализа данных в NetResident реализованы мониторинг и ведение лог-файлов. У вас также есть возможность импортировать файлы с перехваченными пакетами, которые были созданы при помощи других наших программ: CommView и CommView for WiFi, а также некоторыми другими.

Для запуска Мастера импортирования лог-файлов, выберите **Файл => Импорт трафика**. Далее выберите файл для импортирования и задайте необходимые настройки. Импортированный файл мог быть создан уже давно и, возможно, вы захотите импортировать события вместе с фактическими датами их возникновения. В противном случае вся информация будет импортирована с использованием оригинальных дат в соответствии со временем последнего обновления лог-файла.

Помните: эта возможность доступна не для всех видов лог-файлов.

Важно: некоторые или все события в лог-файле могут быть удалены из базы данных сразу после импортирования, потому что программа может быть сконфигурирована на удаление старых событий. Если записи в лог-файле старше, чем установленный в программе показатель, то для импортирования лог-файла используйте текущую дату или увеличьте число дней на странице Database: История в настройках программы.

Вы можете импортировать только те события, которые представляют интерес. Установите опцию **Использовать текущие фильтры сервиса при импорте данных**. Теперь в работе сервиса Мастер будет использовать текущие настройки фильтрации.

Убедитесь, что настройки групп и [фильтров](#) позволяют программе корректно отображать импортированные данные. В противном случае, вы не увидите эти данные в главном окне приложения, даже если данные были успешно импортированы.

Чтобы импортировать выбранный файл, нажмите **Далее**. Вы можете либо дождаться окончания процесса импортирования, либо нажать кнопку **Завершить** и продолжить процесс в фоновом режиме. В последнем случае программа уведомит вас об окончании импортирования. Этот процесс может быть прерван в любой момент нажатием кнопки **Остановить**.

NetResident поддерживает импорт лог-файлов из командной строки. Для этого вам следует запустить приложение NetResident с именем лог-файла в качестве первого параметра командой строки. Учтите, что имя лог-файла должно включать в себя полный путь к этому файлу.

Важно: если имя файла содержит пробелы, его необходимо взять в кавычки (" ").

Примеры:

```
NETRESIDENT.EXE C:\mylog.ncf
```

```
NETRESIDENT.EXE "D:\DATA\October 12.cap"
```

```
NETRESIDENT.EXE "D:\Captured data\log file.pkt"
```

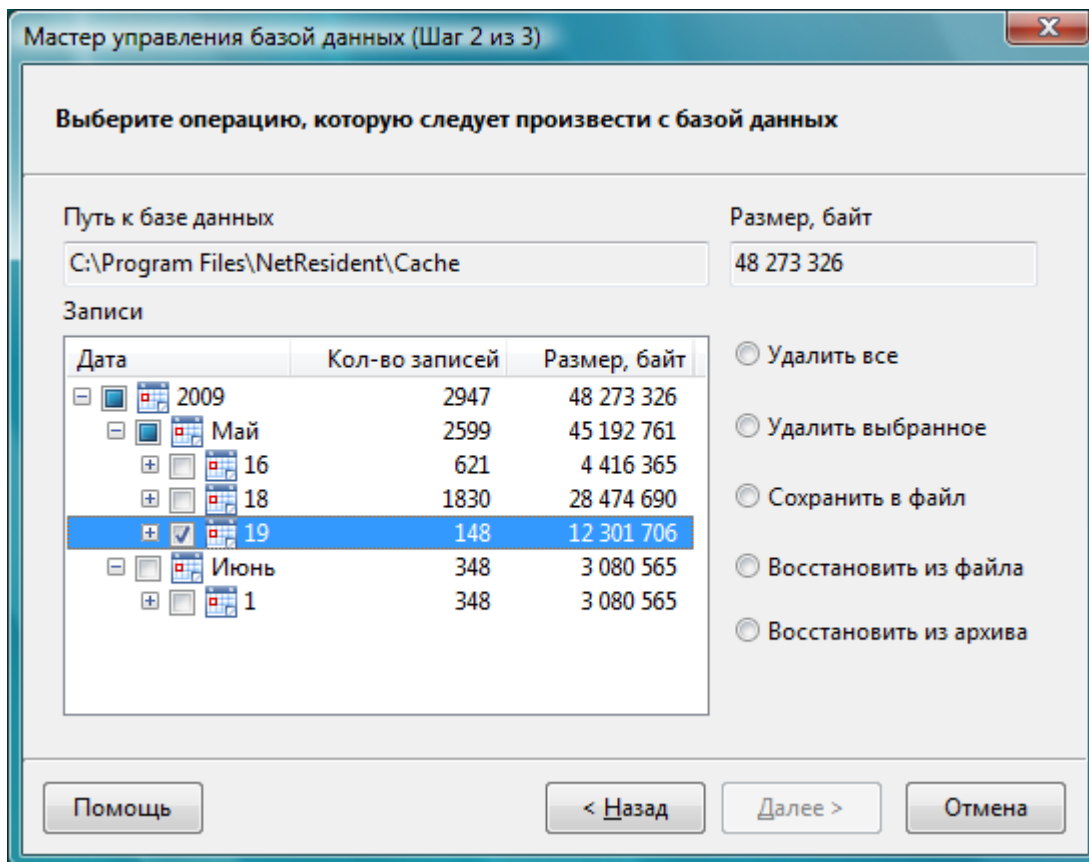
Важно: импорт лог-файлов с пакетами недоступен для пользователей с лицензией Lite.

Управление базой данных

Вся перехваченная для анализа информация сохраняется в базе данных NetResident. Иногда база может достигать столь значительных размеров, что это начинает сказываться на общей производительности программы. Записи, хранящиеся в базе, могут устаревать. В таких случаях мы советуем очищать базу от ненужных записей, запустив **Мастер управления базой данных**.

Это можно сделать из меню **Файл => Управление базой данных**.

Для просмотра текущего состояния базы данных, ее размера и количества записей, нажмите **Далее**. Здесь же выберите операцию с базой данных.



На этой странице вы увидите список сетевых событий, которые хранятся в базе. В колонке **Дата** можно найти события по датам их появления (год, месяц, день). В колонке **Кол-во записей** показано количество сетевых событий, произошедших за период времени, выбранный в колонке **Дата**. Для удаления всех событий из базы данных выберите опцию **Удалить все**. Для удаления записей за определенный период времени, выберите в таблице этот период и установите опцию **Удалить выбранное**.

Замечание: восстановить записи после удаления будет невозможно!

Если вы хотите сохранить базу данных для последующей работы с ней на другом компьютере, выберите **Сохранить в файл**. NetResident сохранит базу данных в файл, который потом можно просмотреть, выбрав команду **Восстановить из файла**.

Замечание: при сохранении, все события в базе данных записываются в файл. При восстановлении базы данных, все записи в текущей базе данных удаляются!

Если вы хотите восстановить данные из архива, выберите опцию **Восстановить из архива**. Обратите внимание, что даты событий также импортируются из архива, поэтому, возможно, вам потребуется изменить настройки фильтров для отображения записей. Если включена опция ограничения размера базы, записи событий автоматически архивируются в конце дня и, возможно, архив будет содержать дубликаты записей. Для предотвращения подобного рода ситуаций, вам потребуется или отключить опцию ограничения размера базы данных, или удалить соответствующие записи вручную.

Выберите требуемую операцию и нажмите кнопку **Далее**. При сохранении и восстановлении вам потребуется ввести имя файла базы данных. Если выбрана опция **Восстановить из архива**, вам потребуется указать папку (в архиве), содержащую записи событий за требуемый период времени. Работа с базой данных может потребовать достаточно много времени. Во время внесения изменений в базу данных мониторинг и запись данных будут приостановлены.

Сервис NetResident

Сервис NetResident перехватывает сетевой трафик, анализирует и вносит его в базу данных. Сервис работает в фоновом режиме. Сервис запускается автоматически при старте Windows и постоянно активен. В зависимости от настроек программы, он перехватывает трафик все время либо только тогда, когда запущен сам NetResident. Эти настройки можно изменить через меню **Инструменты => Настройки, Сеть => Запуск**. За более подробной информацией обратитесь к разделу [Сеть: Запуск](#).

Обычно вам не придется запускать или останавливать сервис NetResident вручную. Если это все же потребуется, сервис доступен в группе программ NetResident (**Stop / Start NetResident Service**) или в панели управления (**Control Panel => Administrative Tools => Services**).

Удаленные подключения к сервису NetResident

Замечание: за более подробной информацией о лицензировании сервиса и консоли NetResident, работающих на разных компьютерах, обратитесь к разделу [FAQ](#).

Как упоминалось ранее, NetResident состоит из двух частей: консоли, которая подключается к сервису NetResident, обрабатывает данные, группирует и предлагает их пользователю, а также сервиса, который осуществляет мониторинг сети, перехватывает информацию и сохраняет ее в [базе данных](#) для обработки и просмотра. Связь между сервисом и консолью происходит по протоколу TCP/IP. Это означает, что вы можете подключиться к сервису NetResident, запущенному на любом компьютере при условии, если к этому компьютеру в принципе возможно подключение по TCP/IP и вы знаете пароль.

Когда вы запускаете NetResident, программа начинает подключение к тому сервису, к которому вы подключались последний раз (по умолчанию – локальный компьютер). Если вы хотите подключиться к другому сервису, выполните следующие шаги:

- Чтобы отключить сервис NetResident, выберите **Файл => Отключиться**.
- Выберите **Файл => Подключиться**.
- Выберите опцию **Подключиться к локальному сервису**, если вы хотите установить соединение с сервисом на вашем локальном компьютере. Если вы хотите подключиться к удаленному компьютеру с NetResident, выберите опцию **Подключиться к удаленному сервису**.
- Если вы выбрали опцию **Подключиться к удаленному сервису**, укажите IP-адрес удаленного компьютера и пароль в полях **IP-адрес удаленного сервиса** и **Пароль**.
- Нажмите **ОК**.

Учтите, что по умолчанию удаленное подключение к сервису NetResident в целях безопасности запрещено. Чтобы разрешить удаленное подключение, компьютер с NetResident, к которому вы хотите подключиться, должен быть правильно настроен. Для настройки выберите **Инструменты => Настройки => Сеть => Удаленное подключение**. **Установите опцию Разрешить удаленные подключения к сервису** и введите пароль. Нажмите **ОК**.

Замечание: у вас никогда не будет запрошен пароль при локальном подключении к сервису NetResident.

Плагины

Для обработки и отображения событий в NetResident используется система плагинов. Каждый плагин отвечает за обработку одного или нескольких протоколов. В дистрибутив NetResident включены следующие плагины:

- **Web** – обработка данных, которые были переданы через протокол HTTP. Этот протокол отвечает за отображение веб-страниц.
- **Mail** – обработка данных, которые были переданы через протоколы POP3, SMTP и IMAP. Эти протоколы используются как клиентом, так и сервером электронной почты для обмена сообщениями.
- **News** – обработка данных, которые были переданы через протокол NNTP. Этот протокол используется для отправки или просмотра сообщений групп новостей.
- **ICQ/AIM** – обработка данных, которые были переданы через протоколы [ICQ](#) и [AOL](#).
- **MSN** – обработка данных, которые были переданы через протокол [MSN](#) версии 8.
- **FTP** – обработка данных, которые были переданы через протокол FTP, который используется для загрузки файлов с/на FTP-серверы.
- **Yahoo** – обработка данных, которые были переданы через протокол [Yahoo](#).
- **Jabber** – обработка данных, которые были переданы через протокол XMPP. Этот протокол используется для отправки сообщений разными клиентами [Jabber](#), включая [Google Talk](#). Обращаем внимание, что данный плагин не может перехватывать зашифрованные сообщения SSL.
- **IRC** – обработка данных, которые были переданы через протокол Internet Relay Chat.
- **Telnet** – обработка данных, которые были переданы через протокол Telnet.
- **VoIP** – обработка данных, которые были переданы через протокол SIP с использованием голосовых потоков RTP.
- **WebMail** – обработка сообщений электронной почты, переданных или полученных через веб-интерфейсы почтовых сервисов (поддерживаются GMail, Hotmail и Yahoo! Mail).
Замечание: для корректной работы **WebMail** необходимо подключить плагин **Web**.
- **Mail.ru** – обработка данных, которые были переданы посредством Mail.ru Agent.

Замечание: воспроизведение перехваченных голосовых данных недоступно для пользователей с версией Lite.

Сами плагины находятся в папке, куда был установлен NetResident (папка Plugins). По умолчанию все плагины включены и активны, т. е. они обрабатывают данные из сети и записывают их в базу данных. Если вас не интересует обработка и хранение данных, переданных по определенному протоколу, вы можете [выключить](#) соответствующие плагины с целью уменьшения нагрузки на процессор и экономии места на диске.

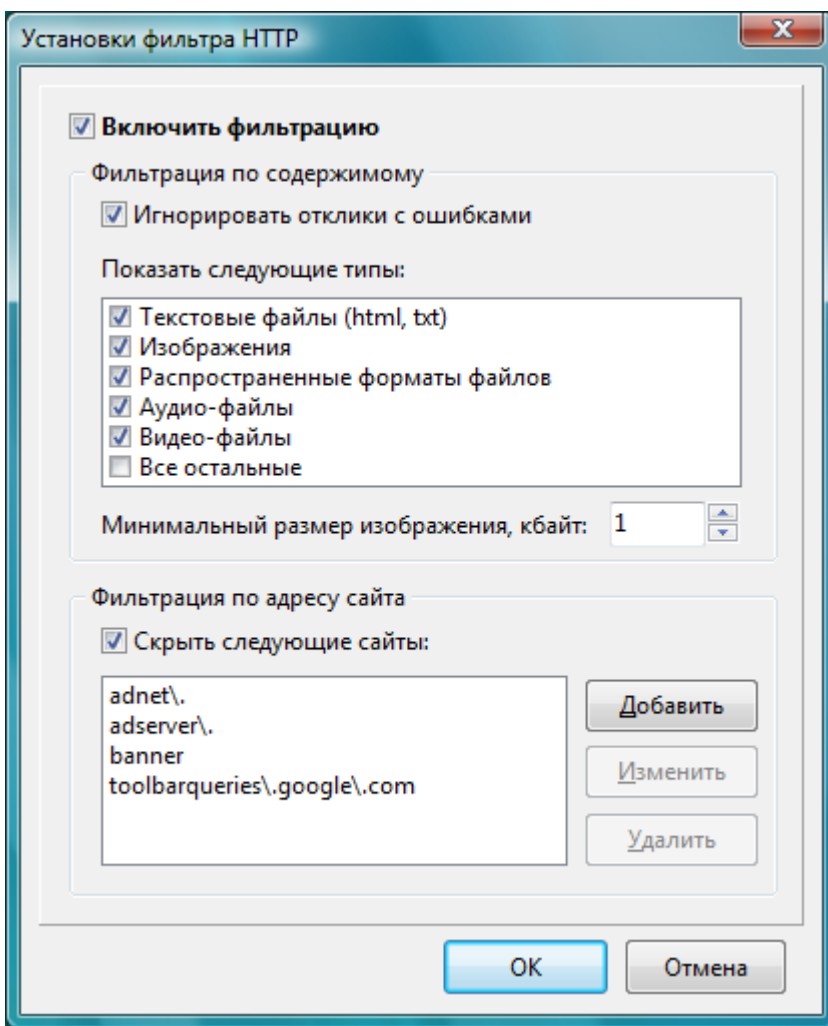
К NetResident можно подключать дополнительные плагины от [TamoSoft](#). Для этого поместите файл плагина в папку Plugins. После этого перезапустите программу. Чтобы перезапустить сервис NetResident, нажмите **Stop NetResident Service / Start NetResident Service**.

Некоторые плагины NetResident можно настроить таким образом, что перехваченные события будут скрыты (они не будут отображены в списке событий, но будут сохранены в базе данных), или же отфильтрованы во время перехвата (они не будут отображаться, и не будут сохранены в базе данных). Последний тип фильтров называется "фильтр перехвата".

Для нас **События => Фильтр => Дополнительно**. Выберите вкладку **Плагины**. Выберите желаемый плагин, и нажмите на кнопку **Изменить**. Для настройки фильтров перехвата выберите **Инструменты => Настройки**, и нажмите **Плагины**. Выберите плагин и нажмите на кнопку **Изменить** для изменения настроек. Доступны следующие опции:

Фильтр отображения HTTP

Отображение веб-страницы требует большого количества дополнительных файлов, которые автоматически подгружаются браузером при открытии данной страницы. Этот фильтр скрывает все дополнительные файлы, тем самым сокращая количество показанных записей.



Чтобы активировать фильтр HTTP, установите метку **Включить фильтр**. Если вы хотите временно отключить этот фильтр, просто снимите эту метку.

В списке **Показать следующие типы** вы можете указать, какие типы файлов будут или не будут (в зависимости от установок) показаны как сетевые события.

- **Текстовые файлы** – текстовые и гипертекстовые (веб-страницы)
- **Изображения**
- **Широко известные файлы** – архивы (.zip, .rar, .arj и т. д.), документы MS Office (.doc, .xls) и другие файлы известных форматов не будут показаны, если установлена эта опция.
- **Аудиофайлы**
- **Видеофайлы**
- **Все остальные**

При снятых метках NetResident уберет соответствующие файлы из списка событий. Например, если вы уберете метку с **Изображений**, то изображений в списке не будет. Если вы уберете все метки, то в списке не будет событий, связанных с HTTP.

Минимальный размер изображения, кбайт – установить минимальный размер изображения, которое будет показано. Большинство изображений в Интернете имеют достаточно небольшой размер (за исключением фотографий). Если требуется, чтобы NetResident показывал изображения, но вы не хотите видеть баннеры и некоторые элементы страницы, укажите в этом поле нужное значение.

Можно также пользоваться фильтрацией по адресу сайта. В этом случае в качестве критерия фильтрации вы можете указать конкретные сайты.

Скрыть следующие сайты – включить/выключить фильтрацию по сайтам.

Когда этот фильтр включен, программа скроет все сайты, удовлетворяющие критерию (см. список сайтов). Для определения новых критериев фильтрации используйте следующий основной синтаксис:

. – любой символ
\. – символ "точка"
\d – любая цифра (от 0 до 9)

Для фильтрации в NetResident используются стандартные регулярные выражения. Более подробную информацию о регулярных выражениях и их синтаксисе можно найти на сайте <http://www.regular-expressions.info/reference.html>.

Примеры критериев:

Google\.com – скрыть сайты, которые содержат в своем имени подстроку "google.com"

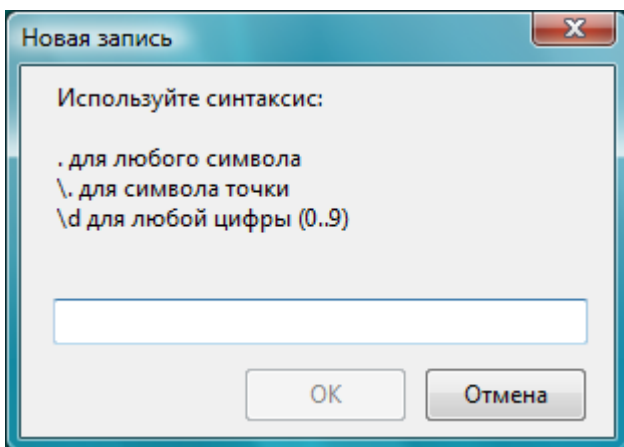
www\.google\.com – скрыть "www.google.com"

\.org\$ – скрыть все сайты с доменом .ORG

\d – скрыть все сайты, в названиях которых есть хоть одна цифра

Замечание: если в качестве критерия вы хотите указать какой-либо домен (.org, .com и т. д.), не забудьте в конце строки указать символ \$.

Для ввода нового критерия фильтрации нажмите кнопку **Добавить**, которая расположена в правой части окна.

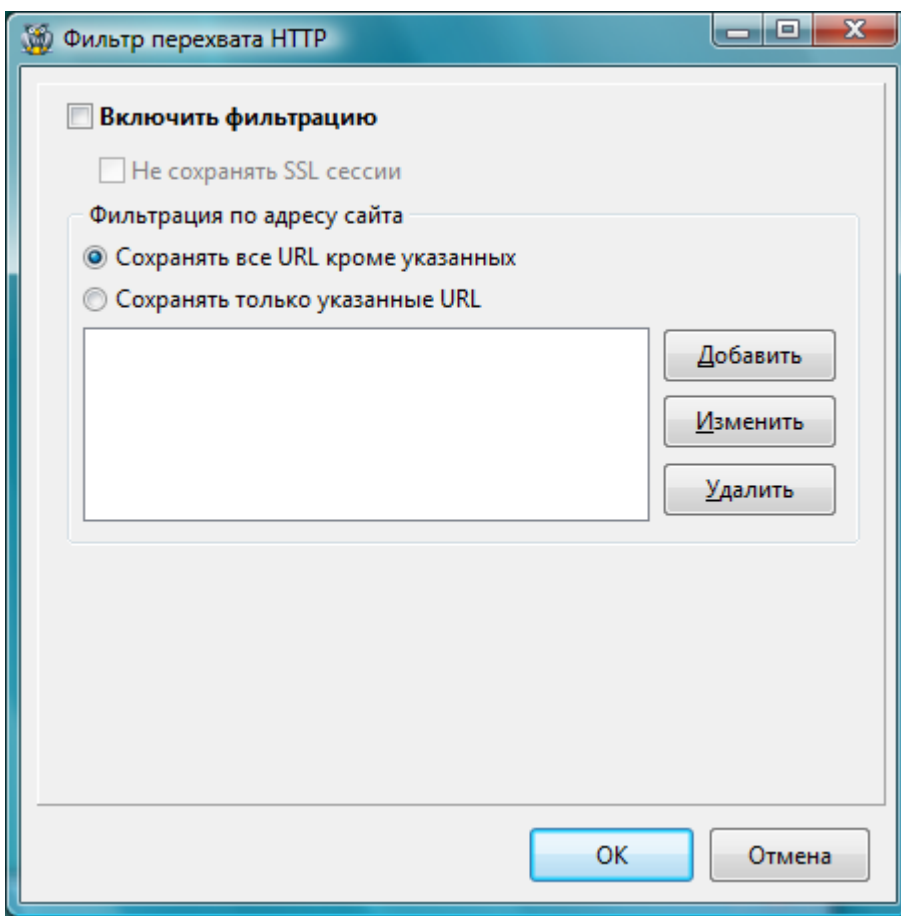


Появится диалог **Новая запись**. Укажите критерий и нажмите **ОК**. Окно будет закрыто, а новая запись добавлена в список критериев.

Чтобы удалить какую-либо запись, выберите ее в списке и нажмите **Удалить**. Чтобы редактировать какую-либо запись, выберите ее в списке и нажмите **Изменить**.

Фильтр перехвата HTTP

Этот фильтр во всем повторяет предыдущий фильтр HTTP, однако его назначение – это фильтрация событий до их сохранения в базу данных. Это уменьшает как требуемый объем дисковой памяти, так и нагрузку на процессор при работе с базой данных.



Выберите опцию **Включить фильтрацию** для активации фильтра. Если вы хотите временно отключить фильтр, снимите соответствующую метку.

Включите опцию **Не сохранять SSL-сессии** для отключения перехвата HTTPS-сессий.

В поле **Фильтрация по адресу сайта** вы можете задать список интересующих вас URL, которые требуется отфильтровать. Более подробная информация о синтаксисе определения критериев фильтрации (регулярные выражения) приведена выше. Доступны два режима работы: записываются только события, удовлетворяющие критериям фильтрации (опция **Сохранять только указанные URL**), либо записываются все события, кроме тех, которые удовлетворяют условиям фильтра (опция **Сохранять все URL, кроме указанных**).

Фильтр перехвата Почта

Функциональность этого фильтра, предназначенного для фильтрации e-mail сообщений, во всем повторяет предыдущий фильтр перехвата.

Включить фильтрацию

Сохранять все кроме указанного
 Сохранять только указанное

Адрес отправителя

ИЛИ

Адрес получателя

ИЛИ

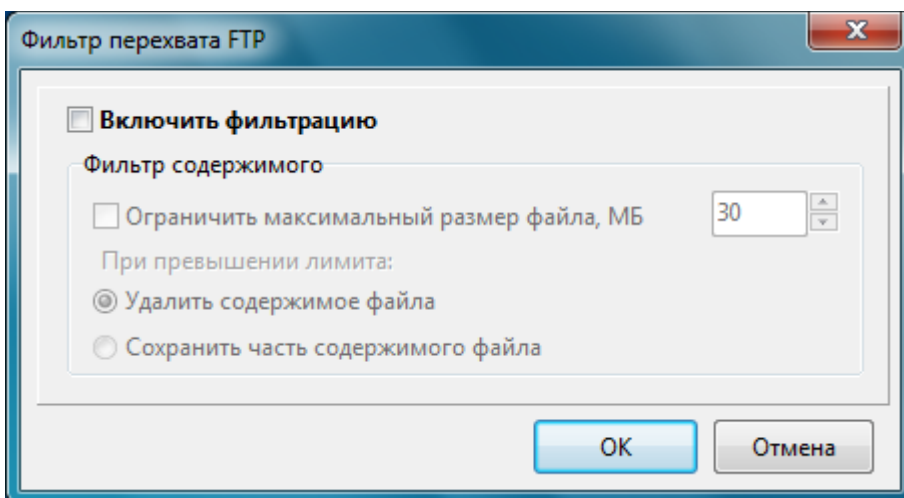
Текст сообщения

Выберите опцию **Включить фильтрацию** для активации фильтра. Если вы хотите временно отключить фильтр, снимите соответствующую метку.

События могут быть отфильтрованы по адресу получателя/отправителя, а также ключевым словам в теле сообщения. Для объединения условий фильтра используется булева (AND/OR) логика. Более подробная информация о синтаксисе определения критериев фильтрации (регулярные выражения) дана выше. Этот фильтр позволяет записывать все e-mail сообщения, удовлетворяющие условиям фильтра (опция **Сохранять только указанное**), или же запись всех событий кроме тех, которые удовлетворяют критериям фильтра (опция **Сохранять все, кроме указанного**).

Фильтр перехвата FTP

При обмене данными посредством FTP-протокола количество перехваченных файлов и их объем могут быть достаточно большими. С помощью этого фильтра вы можете ограничить размер перехваченных файлов.



Выберите опцию **Включить фильтрацию** для активации фильтра. Если вы хотите временно отключить фильтр, снимите соответствующую метку.

Включите опцию **Ограничить максимальный размер файла** и укажите требуемый максимальный размер файла (в Мегабайтах) в соответствующем поле справа.

При превышении лимита размера файла, доступны следующие опции:

- **Удалить содержимое файла** – если выбрана эта опция, в базе данных будет отмечен факт получения файла, однако его размер будет нулевым.
- **Сохранить часть содержимого файла** – если выбрана эта опция, содержимое файла будет ограничено лимитом максимального размера файла.

Утилита PromiSwitch

Важно: используйте эту утилиту на свой страх и риск. Если вы не администратор сети, к которой вы подключены – не используйте эту утилиту. Это может привести к потере сетевого соединения. Для данного модуля мы не предлагаем технической поддержки.

Утилита PromiSwitch создана для обеспечения полной видимости сетевых процессов в коммутируемой сети. При этом предполагается, что у коммутаторов не предусмотрено функции зеркалирования портов. За более подробной информацией на эту тему обратитесь к нашей [статье](#). Данная утилита попытается обеспечить “прозрачность” сети, используя уязвимости протокола ARP. Мы советуем, где это возможно, использовать зеркалирование вместо данной утилиты.

Запустите PromiSwitch и выберите адаптер для мониторинга. В соответствующих полях задайте диапазон IP-адресов и начните сканирование. После завершения сканирования вы увидите список обнаруженных рабочих станций с их IP- и MAC-адресами.

Отметьте рабочие станции, которые вы хотите наблюдать и нажмите кнопку **Start**. Утилита будет периодически отсылать специальные сетевые пакеты на эти станции. Таким образом, на ваш компьютер будет переправляться трафик между выбранными рабочими станциями и шлюзом, чем и будет обеспечена прозрачность сети. Вы также можете получить доступ к трафику между двумя рабочими станциями, выбрав эти станции, а также опцию **Internal** в выпадающем списке **Traffic**.

В окне **Options** вы можете выбрать такие возможности, как сброс списка станций перед новым сканированием, автоматическую рассылку пакетов при запуске, а также задать временной интервал между пакетами.

Часто задаваемые вопросы (FAQ)

В этом разделе вы найдете ответы на часто задаваемые вопросы. Обновленный вариант FAQ всегда доступен на нашем сайте по адресу <http://www.tamos.ru/products/netresident/faq.php>.

Q. В чем разница между NetResident Lite и NetResident Pro?

A. Для NetResident предусмотрено два типа лицензий: Lite и Pro.

- Pro: доступны все функции.
- Lite: доступны все функции, кроме поддержки VoIP и возможности импортирования лог-файлов с пакетами из других приложений.

Q. Я хочу установить сервис NetResident на одном компьютере и затем подключиться к нему с помощью консоли на другом компьютере. Как мне при этом соблюсти лицензионное соглашение?

A. В соответствии с пользовательским соглашением, однопользовательская лицензия дает возможность работать с одной копией NetResident в рамках одной учетной записи операционной системы. Чтобы установить и работать с программой на нескольких компьютерах, независимо от способа установки или использования (сервис или консоль), вам следует приобрести количество лицензий, равное количеству установок программы.

Q. Мой HTTP-плагин не всегда верно отображает HTML-страницы. Например, некоторые изображения не показываются. Почему?

A. Обычная HTML-страница представляет собой набор независимых объектов – HTML-код, изображения, стили CSS и т. д. Каждый из этих объектов запрашивается браузером. Однако некоторые из объектов кэшируются (сохраняются на жесткий диск для последующего доступа к ним) и поэтому не запрашиваются из сети всякий раз, когда вы просматриваете веб-страницу. NetResident не имеет доступа к вашему кэшу, поэтому он не "видит" эти объекты. Это не проблема NetResident; вам следует перезагрузить страницу в вашем браузере (например, полная перезагрузка страницы в MSIE производится нажатием комбинации клавиш Shift+Refresh). Это позволит программе NetResident хранить все элементы веб-страницы.

Q. Какой из адресов (IP или MAC) мне использовать для того, чтобы указать, какой компьютер я хотел бы наблюдать?

A. Если в вашей сети включен DHCP, каждому компьютеру с уникальным MAC-адресом при каждой новой сессии всегда будет соответствовать новый IP-адрес. Для этого случая вам следует идентифицировать ваши компьютеры MAC-адресами. Этот шаг позволит программе связывать все события в сети с заданным для определенного компьютера MAC-адресом, что предотвратит перенасыщение списка рабочих станций. В некоторых случаях вы можете видеть разные MAC-адреса для одного хоста. Если у вас статический IP, то мы советуем его использовать для идентификации компьютера. Мы также рекомендуем использовать [псевдонимы](#) для MAC- и IP-адресов - это существенно упрощает анализ событий в сети.

Q. Когда я пытаюсь импортировать лог-файлы, созданные CommView или CommView for WiFi, я не вижу содержимого некоторых файлов. Я считаю, что все параметры фильтрации просмотра событий я выставил верно.

A. Важно понять, что у процедуры импортирования используется свой фильтр, а у системы отображения содержимого – свой. Когда вы импортировали файл, то вполне возможно, что на этой стадии файл уже был подвержен фильтрации. После окончания процесса импортирования программа использует другой фильтр для отображения информации. Весьма вероятно, что программа настроена на показ событий, которые произошли за последние 2 часа, а лог-файл содержит записи, которые выходят за эти временные рамки. Возможно, вам придется отключить фильтрацию.

Q. Почему программа пытается запустить сервис даже в том случае, если я хочу всего лишь просмотреть лог-файлы, а не включать мониторинг сети?

A. Сервис управляет работой с базой данных. Оболочка программы это всего лишь консоль для обмена информацией с сервисом. Весь процесс обработки и фильтрации информации осуществляется сервисом, так что он должен быть запущен.

Q. Я настроил NetResident таким образом, чтобы он осуществлял мониторинг сети только когда загружена сама программа, а не при старте Windows. Я заметил, что после того, как я закрыл NetResident, процесс "tfsnr.exe" все еще активен. Почему?

A. Необходимо разделять работу сервиса и процесс мониторинга. Для обмена с программой сервис должен быть активен все время. Это не означает, что сервис все время перехватывает данные в сети. Он осуществляет захват только по запросу. Теоретически, если программа настроена на перехват трафика только когда она запущена, можно запускать сервис при открытии программы и выгружать его при закрытии. Но запуск сервиса происходит не быстро, и, что самое важное – это невозможно сделать удаленно, когда сервис и программа выполняются на разных компьютерах. Мы планируем реализовать эту возможность в будущем. Но пусть сам факт работы сервиса в фоновом режиме вас не беспокоит – он не производит мониторинга сети и не потребляет значительных системных ресурсов.

Q. Можете ли вы предоставить некоторые численные данные о влиянии мониторинга сильно загруженной сети на производительность системы?

A. Производительность программы зависит от частоты процессора и объема памяти. Если вы используете все настройки мониторинга по умолчанию, т. е. когда включены все плагины и наблюдаются все порты, средний компьютер с процессором 3 ГГц и объемом памяти 512 Мбайт может осуществлять мониторинг полностью загруженной сети 100 Мбит. Чтобы наблюдать более быстрые сети, настройте [фильтрацию по станциям](#), ограничьте количество [портов](#) и отключите ненужные [плагины](#). Быстродействие также зависит от типа трафика, так что применяйте дополнительные фильтры лишь в том случае, если вы испытываете проблемы с производительностью.

Q. В некоторых сессиях ICQ и AIM один из номеров ID не определяется. Почему?

A. Это происходит, когда сессия ICQ/AIM (включая фазу авторизации) начинается до запуска перехвата программой NetResident. Если перехват начался уже в процессе сессии, то ID может быть найден, но этого нельзя гарантировать.

Q. Можно ли использовать модуль VoIP для записи разговоров по Skype?

A. Нет. В Skype используется надежное шифрование; расшифровать переговоры по Skype невозможно.

Q. Почему NetResident не отображает объем переданной информации в байтах?

A. NetResident не всегда хранит переданную информацию в ее исходном виде, а обрабатывает для более удобного представления. Обычным делом является разделение единой сетевой сессии на несколько отдельных событий или, наоборот, объединение нескольких сессий в одно событие. Кроме этого, некоторые передаваемые данные просто не могут быть обработаны существующими плагинами NetResident. Таким образом, не может быть использован и не предназначен для отображения достоверной сетевой статистики. Если вас интересует статистика сетевого трафика, то вы можете попробовать другой продукт от TamoSoft - [CommTraffic](#).

Q. При работе с WireShark я заметил, что после установки NetResident он перестал перехватывать пакеты.

A. Существует известный конфликт между драйвером, используемым в WireShark и многих схожих программах (WinPcap) и драйвером, используемым в NetResident. Проблема решается просто: начинайте перехват пакетов с помощью WireShark **до того**, как вы начнете перехват пакетов с помощью NetResident. В этом случае обе программы будут перехватывать данные одновременно. Если вы сначала начнете работать с NetResident, то WinPcap перестанет перехватывать пакеты по неизвестной нам причине.

Информация

Как купить NetResident

Работа демо-версии ограничена 30 днями. Если вы хотите пользоваться программой и дальше, вы должны будете ее купить. Для программы NetResident доступны два вида лицензий: Lite и Pro.

- Pro: доступны все функции.
- Lite: доступны все функции, кроме поддержки VoIP и импорта лог-файлов с пакетами из других приложений.

Как зарегистрированный пользователь вы получите:

- Бесплатные обновления, которые будут выпускаться в течение одного года со дня приобретения
- Информацию об обновлениях и новых продуктах
- Бесплатную техническую поддержку

Мы принимаем к оплате: кредитные карты, чеки, почтовые переводы и другие виды платежей. Цены и лицензионное соглашение могут быть изменены нами в одностороннем порядке. Пожалуйста, посетите наш сайт для получения последней информации о продуктах:

<http://www.tamos.ru/order/>

Свяжитесь с нами

У вас есть вопросы, предложения? Пожалуйста, свяжитесь с нами.

<http://www.tamos.ru/>

Описывая вашу проблему, постарайтесь быть как можно точнее. Детальное описание вопроса поможет нам быстрее в нем разобраться. Пожалуйста, не забудьте указать версию операционной системы, версию программы (**Справка => О программе**), тип адаптера и другие важные подробности.

Другие продукты TamoSoft

CommView

CommView – это программа для мониторинга активности в Интернете и локальной сети (LAN), способная перехватывать и анализировать сетевые пакеты. Программа собирает информацию о данных, проходящих по dial-up-соединению или через Ethernet-карту и декодирует проанализированную информацию. С помощью CommView вы сможете получить список сетевых подключений, важную IP-статистику и изучить отдельные пакеты. Пакеты декодируются вплоть до нижнего уровня с полным анализом наиболее распространенных протоколов. Также предоставляется доступ к необработанным данным в режиме реального времени. CommView будет полезным инструментом для сетевых администраторов, специалистов по безопасности, сетевых программистов и всех, кто хочет иметь перед глазами полную картину о трафике, проходящем через какой-либо компьютер или сегмент локальной сети.

[Подробнее](#)

CommView для WiFi

CommView для WiFi - это мощный инструмент для мониторинга и анализа беспроводных сетей 802.11 a/b/g/n. В программе сочетаются большой набор функций и простота их использования. CommView для WiFi перехватывает из эфира каждый пакет и сообщает такую информацию, как списки точек доступа и станций, статистику по узлам и каналам, уровень сигнала, списки пакетов и сетевых подключений, диаграммы распределения протоколов и т. д. Владея этой информацией, вы можете анализировать пакеты, идентифицировать проблемы в сетях, на сайтах, в программном и аппаратном обеспечении.

[Подробнее](#)

TamoGraph

TamoGraph – мощный и удобный инструмент для сбора, визуализации и анализа данных в сетях Wi-Fi стандарта 802.11 a/b/g/n. Программа предоставляет данные об уровне сигнала, шумов, помех, распределения каналов, скорости передачи данных, шифрования и других параметров. TamoGraph поможет существенно сократить время и расходы на планирование и обслуживание сети, увеличит ее производительность, расширит покрытие, возможно, даже без приобретения дополнительного оборудования.

[Подробнее](#)

SmartWhois

Удобная утилита для сбора информации о любом IP-адресе или имени хоста. В отличие от стандартной Whois-утилиты, SmartWhois автоматически предоставляет информацию, связанную с IP-адресом вне зависимости от географического места его регистрации. За несколько секунд вы можете узнать все, что вы хотите знать о пользователе: домен, сетевое имя, страну, штат или провинцию, город. Даже если по IP-адресу не может быть определено имя хоста, SmartWhois будет работать.

[Подробнее](#)

CountryWhois

CountryWhois – это утилита для определения географического местоположения IP-адреса. Утилита может быть использована для анализа лог-файлов сервера, проверки заголовков электронных писем, обнаружения фактов мошенничества с помощью кредитных карт и во многих других случаях, когда требуется быстро и точно определить страну по IP-адресу.

[Подробнее](#)

Essential NetTools

Полезный пакет для диагностики сетей и слежения за сетевыми соединениями вашего компьютера. Он включает быстрый, многопоточный NetBIOS-сканер, оболочку для NetBIOS Auditing Tool (NAT), утилиту netstat, которая отображает все сетевые соединения компьютера, монитор для слежения за внешними соединениями к открытым ресурсам вашего компьютера, удобную утилиту для быстрого подключения к удаленным ресурсам, которая дает пользователям Windows 95/98 возможности Windows NT при подключении на уровне пользователей, удобный редактор файла LMHosts и другие полезные утилиты. Программа проста в использовании и является заменой таких Windows-утилит, как nbtstat, netstat, NetWatcher. Она имеет много дополнительных возможностей по сравнению со стандартными утилитами Windows.

[Подробнее](#)

CommTraffic

CommTraffic – утилита для получения статистики использования сети, включая локальную сеть и удаленный доступ. Статистика

отображается по каждому узлу сети. Программа оснащена гибким, привлекательным интерфейсом, иконкой в панели извещений, показывающей общую сетевую статистику. Можно получать отчеты, отражающие объем сетевого трафика и стоимость подключения к Интернету (опция). CommTraffic можно настроить практически на любые особенности тарифных планов Интернет-провайдеров, такие как время активности, объем трафика, время суток и тому подобное. Есть настраиваемые предупреждения, срабатывающие по таким критериям, как достижение лимита по сумме оплаты или объему трафика. Мастер настройки поможет установить программу, автоматически распознает сетевую конфигурацию и параметры подключения.

[Подробнее](#)