Essential NetTools

Руководство пользователя
Версия 4.4

Содержание

Введение

О программе Essential NetTools

Essential NetTools - это набор сетевых утилит для диагностики сетей и мониторинга сетевых соединений вашего компьютера. Это незаменимый инструмент для каждого, кому нужен набор мощных сетевых инструментов для ежедневного использования. Он включает в себя:

- **NetStat**: отображает список входящих и исходящих соединений вашего компьютера, включая информацию по открытым TCP- и UDP-портам, IP-адресам и состоянию соединений. От других утилит NetStat отличает способность привязывать открытые порты к приложениям, владеющим ими. Возможна настройка системы предупреждений на входящие и исходящие соединения.
- **ProcMon**: отображает список активных процессов с полной информацией о нахождении программы, производителе, идентификаторе процесса, загруженных модулях. С этим инструментом вы можете просмотреть статистику по потреблению процессорного времени, распознавать скрытые приложения, останавливать текущие процессы и эффективнее управлять использованием ресурсов компьютера.
- **TraceRoute** и **Ping**: знакомые всем утилиты, которые снабжены множеством функций и наглядным представлением результатов, позволят вам исследовать Интернет и выявлять проблемы соединений.
- **PortScan**: сканер TCP-портов с расширенными возможностями, позволяющий сканировать сеть на предмет активных портов. Этот инструмент сканирует как в обычном (полносвязном), так и в скрытом (half-open) режимах.
- **HostAlive**: модуль мониторинга сети, периодически проверяющий, активен ли хост и работают ли на нем сетевые сервисы, например HTTP- или FTP-сервер.
- **EmailVerify**: проверяет, существует ли адрес электронной почты, связываясь по SMTP с сооветствующим почтовым сервером.
- **NSLookup**: позволяет переводить адреса IP в имена хостов и наоборот, получать алиасы и выполнять расширенные DNS-запросы, такие как MX или CNAME.
- **IPBlackList**: проверяет, включен ли IP-адрес в различные черные списки IP-адресов: базы адресов спамеров, открытые прокси и рилеи электронной почты. Этот инструмент даст вам ответ на вопрос, почему проверяемый IP-адрес отвергается некоторыми сетевыми ресурсами, такими как почтовые сервера.
- **NBScan**: сканер NetBIOS, мощный и быстрый инструмент для исследования сетей. NBScan может сканировать сеть в заданном диапазоне IP-адресов и составлять список компьютеров, имеющих службу NetBIOS разделяемых ресурсов и таблицу их имен. В отличие от стандартной утилиты, поставляемой с Windows, NBScan обеспечивает дружественный графический интерфейс и легкое управление файлами lmhosts, а также параллельное сканирование, что позволяет проверить сеть класса C менее, чем за минуту. NBScan может облегчить выполнение ежедневных задач системными интеграторами, администраторами и аналитиками.
- **RawSocket**: наделяет вас возможностью устанавливать низкоуровневые соединения TCP для выявления проблем с различными сетевыми службами. Представление данных разными цветами, а также удобный интерфейс делают его отличным инструментом для ежедневной работы и администратора, и программиста.

- **WiFiMan**: показывает информацию об установленных в компьютере беспроводных адаптерах, доступных беспроводных сетях, позволяет редактировать соответствующие профили подключения.
- **Shares**: контролирует и ведет отчет внешних подключений к разделяемым ресурсам вашего компьютера, а также предоставляет быстрый и легкий путь подключения к удаленным ресурсам.
- **NetAudit** (NetBIOS Auditing Tool): позволяет вам проводить различные проверки безопасности сети и/или отдельных компьютеров, на которых запущена служба доступа к разделяемым ресурсам по NetBIOS. Этот инструмент поможет вам идентифицировать потенциальные бреши в безопасности.
- **SNMPAudit**: продвинутый сканер SNMP-устройств. Позволяет быстро локализовать SNMP-устройства в выбранном сетевом диапазоне и получить настраиваемую выборку данных от каждого из них. Для более детального изучения устройства пользователь может использовать SNMP-браузер.
- **SysFiles**: удобный редактор для пяти важных системных файлов: services, protocol, networks, hosts и lmhosts.

Другие возможности: создание отчета в HTML, текстовом и CSV-форматах, быстрая обмен IP-адресами в разных инструментах; геолокация IP-адресоов, подробная информация о системе, настраиваемый интерфейс и многое другое.

Что нового

Версия 4.4

- Программа Essential NetTools теперь стала бесплатным ПО.

Версия 4.3

- WiFiMan: новый инструмент для работы с беспроводными сетями: доступны сканирование сетей, управление профилями, слежение за уровнем сигнала и многое другое.
- Поддержка Windows 7.
- Улучшена генерация отчетов инструментов NetStat и ProcMon.
- Обновлена карта распределения IP-адресов.
- Другие улучшения.

Версия 4.2

- Добавлены новые сетевые инструменты: HostAlive для мониторинга работоспособности сетевых служб, EmailVerify для проверки существования e-mail адресов с помощью связи с соответствующим почтовым сервером, IPBlackList для проверки нахождения IP-адресов в различных черных списках IP-адресов.
- Все инструменты поддерживают геолокацию в реальном времени, т. е. для всех IP-адресов определяется страна и рядом с IP-адресом показывается соответствующая страна и флаг.
- Исправлено несколько ошибок.

Версия 4.1

- Поддержка Windows Vista.

Версия 4.0

- Улучшен модуль NetStat: добавлена новая, настраиваемая система предупреждений для входящих и исходящих соединений. Также добавлены иконки, иллюстрирующие процессы соединений. Различные виды соединений, включая прекращенные, отмечены разными цветами.
- SNMPAudit – новый модуль для работы с SNMP-устройствами. Для подробного исследования устройств добавлен SNMP-браузер.
- Исправлен NetAudit: улучшены быстродействие и совместимость с современными сетевыми стандартами. Доработан интерфейс с целью повышения удобства и простоты работы.
- В модуле ProcMon теперь показано распределение процессорного времени по отдельным процессам.
- Автоматические обновления через Web.
- Некоторые улучшения интерфейса, включая настраиваемую панель инструментов.
- Модуль RawSocket теперь позволяет отсылать любую информацию, включая непечатаемые символы.
- Распознавание DNS в модуле TraceRoute теперь ведется в фоновом режиме, тем самым повышая качество работы самого модуля.
- Исправлены некоторые ошибки, допущенные в предыдущей версии.

Версия 3.2

- Новое окно общей информации о системе, в котором представлена самая подробная информация о вашем компьютере.
- Улучшенная система отчетов, которая позволяет вести записи только новых соединений или тех, которые были обработаны модулями NetStat и ProcMon.
- Теперь можно осуществлять пинг целой области IP-адресов.
- Новые подпункты меню Быстрый запуск и Инструменты, которые позволяют вам запускать ваши любимые программы и получать доступ к часто используемым инструментам Windows.
- В дополнение к TCP теперь поддерживаются прямые UDP-соединения.
- В модуле NetStat отмечены новые соединения.
- Локальные разделяемые ресурсы перечислены в модуле Shares.
- SysFiles – новый модуль, предназначенный для редактирования пяти важнейших системных файлов: services, protocol, networks, hosts и lmhosts.
- Многоязычный интерфейс.

Версия 3.1

- PortScan – новый модуль для сканирования TCP-портов.
- Пользовательсикие фильтры в NetStat.
- Возможность прерывания TCP-соединений, созданных через другие программы.
- Автоматическая генерация отчетов NetStat и ProcMon.
- Другие улучшения.

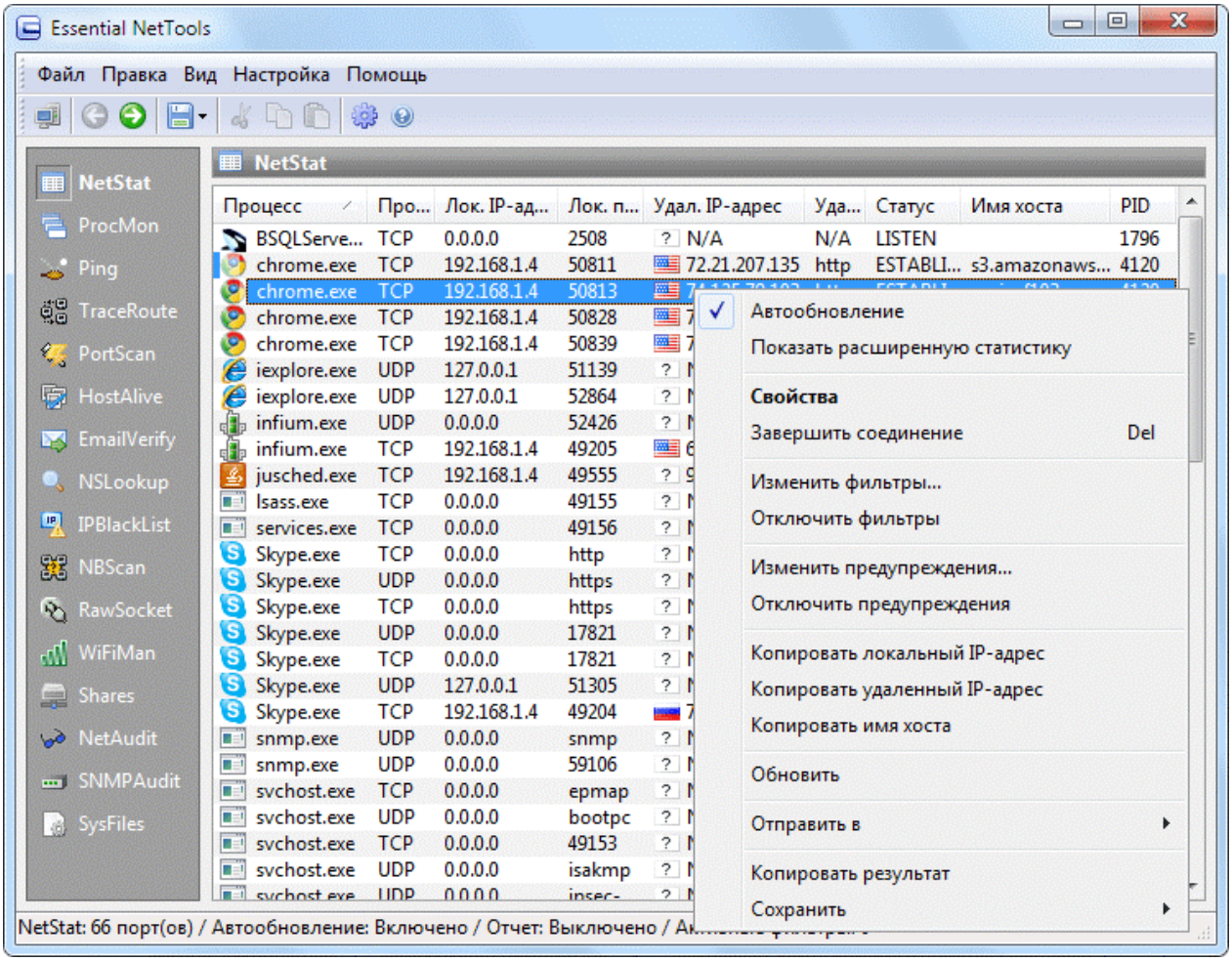
Версия 3.0

- Новый, улучшенный интерфейс.
- Поддержка Windows XP.
- NetStat делает доступными (отображает) открытые порты и соединения для приложения-собственника (только для Windows NT/2000/XP).
- Новые модули: TraceRoute, Ping, NSLookup и Process Monitor.

Работа с программой

Обзор интерфейса

Главное окно программы состоит из панели с изменяемым размером слева, где вы можете выбрать инструмент, с которым хотите работать, а также главная панель, которая показывает рабочую область выбранного сетевого инструмента. В строке состояния, показанной ниже, сообщается информация о рабочем состоянии модуля (например, включен или выключен). Для более детального описания каждого модуля обратитесь к соответствующей главе этого руководства.



Главное меню

Файл

- **Общая информация о системе** – показать окно с подробной информацией о вашем компьютере.
- **Приложения Windows** – быстрый доступ к часто используемым утилитам Windows.
- **Быстрый запуск** – запустить другие сетевые инструменты от TamoSoft, если они установлены на вашем компьютере, а также настроить программу для запуска других приложений.
- **Выполнить** – открыть стандартный диалог Windows "Выполнить...".
- **Сохранить отчет** – сохранить вывод модуля в файл.
- **Отчет** – открыть диалог создания отчетов.

- **Выход** – закрыть программу.

Правка

- **Вырезать, Копировать, Вставить** – выполнить стандартные операции с текстом.

Вид

- **Панель инструментов** – показать/скрыть панель инструментов.
- **Панель состояния** – показать/скрыть панель состояния.
- **Боковая панель** – показать/скрыть боковую панель.
- **Настроить боковую панель** – добавить/изменить кнопки на боковой панели.
- **Локальный IP-адрес(а)** – показать IP-адрес компьютера.
- **Назад, Вперед** – переключиться между модулями.
- **NetStat, NBScan и т. д.** – выбрать модуль.

Настройка

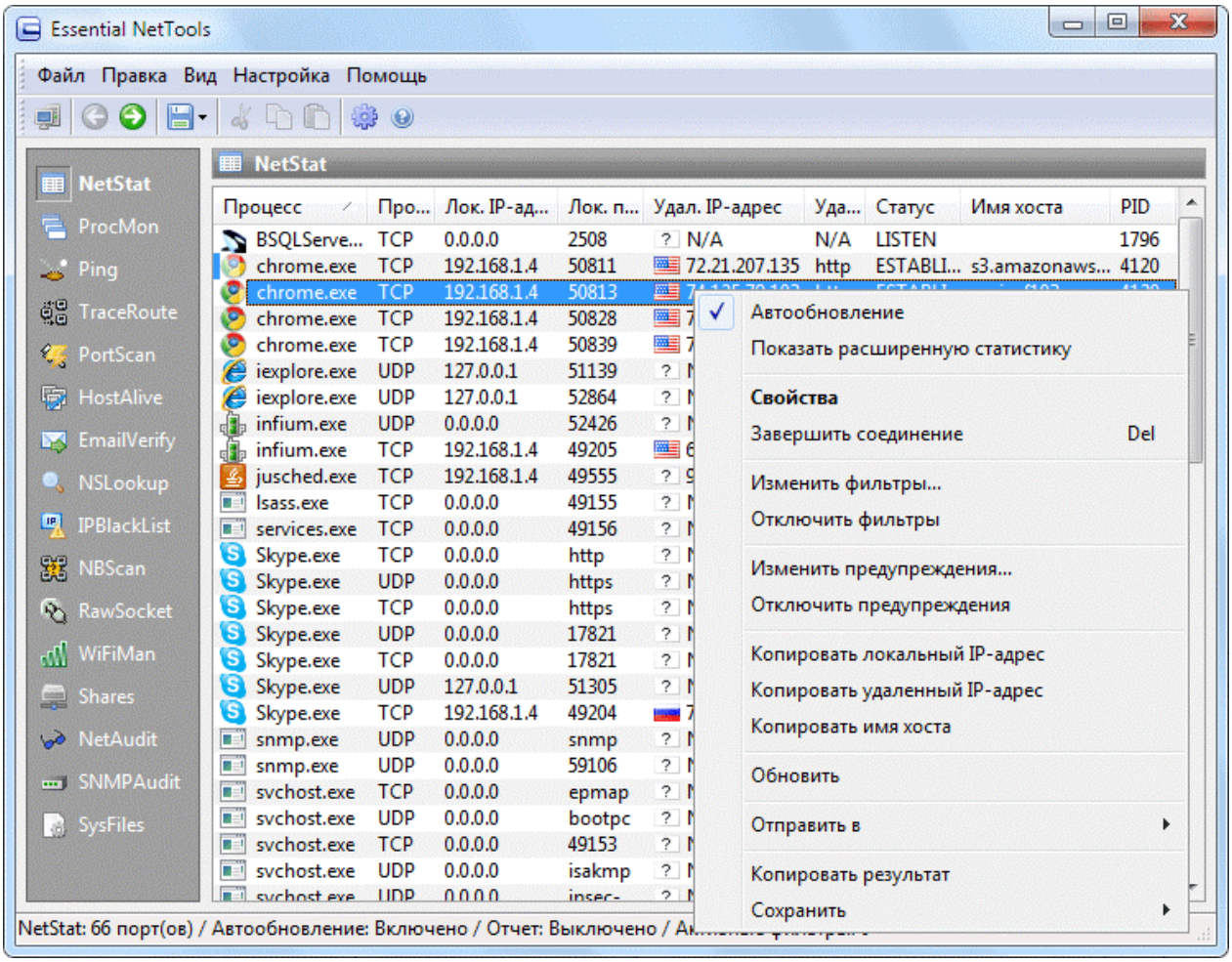
- **Шрифт** – выбрать шрифт интерфейса и шрифт с фиксированной (такие шрифты используются в некоторых окнах программы, например, в NetAudit или NSLookup).
- **Установки** – открыть диалог Установок.
- **Язык интерфейса** – выбрать язык интерфейса программы.

Помощь

- **Содержание** – открыть файл-справку.
- **Найти в справке** – открыть форму поиска по справке Essential NetTools.
- **Проверить обновления программы на сайте TamoSoft** – открыть диалог загрузки обновлений. Для загрузки и установки обновлений следуйте инструкциям Мастера обновлений.
- **О программе** – показать информацию о программе.

NetStat

Этот модуль является заменой стандартной утилите Windows, запускаемой из командной строки – netstat. В данном окне указаны все входящие и исходящие соединения вашего компьютера, а также все открытые порты. NetStat отображает открытые порты и соединения на приложение-собственника.



Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Автоообновление** – включить/отключить автоматическое обновление списка. Период обновления можно изменить - см. Установки.
- **Показать расширенную статистику** – показать дополнительную панель с расширенной статистикой по протоколам.
- **Свойства** – показать свойства файла процесса, которому принадлежит соединение.
- **Завершить соединение** – завершить выбранное TCP-соединение.
- **Изменить фильтры –** открыть диалог настройки фильтров.
- **Отключить фильтры** – включить/отключить текущие фильтры.
- **Изменить предупреждения** – открыть диалог настройки предупреждений.
- **Отключить предупреждения** – включить/отключить текущие предупреждения.
- **Копировать локальный IP-адрес** – копировать в буфер обмена локальный IP-адрес.
- **Копировать удаленный IP-адрес** – копировать в буфер обмена удаленный IP-адрес.

- **Копировать имя хоста** – копировать имя удаленного хоста в буфер обмена.
- **Обновить** – обновить список.
- **Отправить в** – передать выбранный IP-адрес в другие модули или SmartWhois.
- **Копировать результат** – копировать таблицу NetStat в буфер обмена.
- **Сохранить** – сохранить таблицу NetStat в файл.

Можно настроить программу таким образом, чтобы она не отображала все соединения, преобразовывала номера портов в имена сервисов, преобразовывала IP-адреса в имена хостов и т. д. Новые и завершенные соединения автоматически выделяются в течение 5 секунд. За более подробной информацией обратитесь к главе Установки.

ProcMon

ProcMon – это модуль, который отображает список процессов (приложений и сервисов), запущенных в данный момент на вашем компьютере. В колонке **Программа** указано имя программы, **PID** – уникальный идентификатор процесса, **Путь** – указывает полный путь к исполняемому файлу программы, **Производитель** – имя производителя, **Модули** – количество модулей, используемых данным процессом. ProcMon является удобным средством для выявления скрытых программ, завершения процессов и эффективного управления ресурсами вашего компьютера.

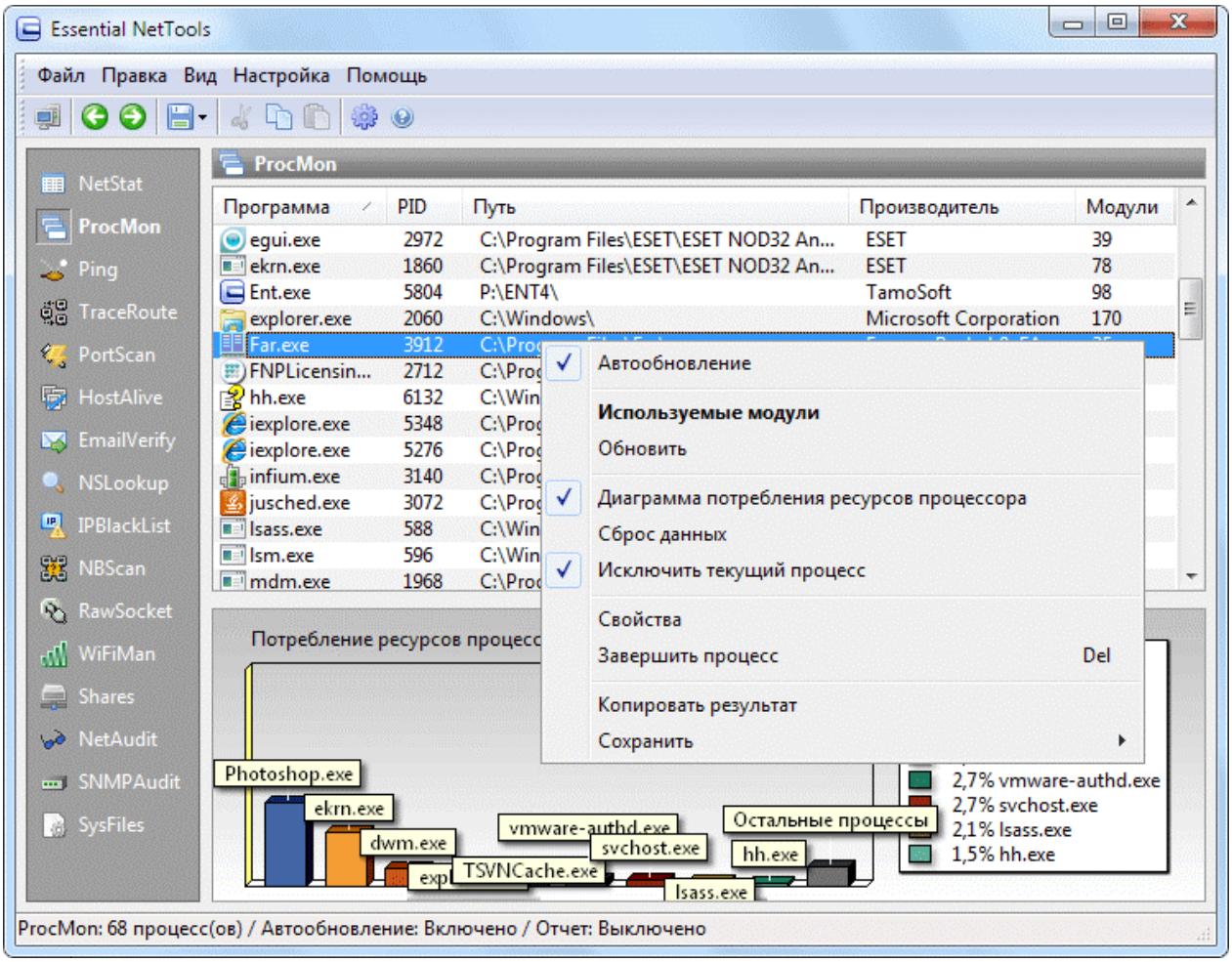


Диаграмма загрузки процессора показывает распределение ресурсов между процессами за последние несколько минут. Показаны 10 самых активных в плане потребления процессорного времени процесса, в том числе включая скрытые процессы. Период обновления диаграммы можно настроить (см. главу Настройки).

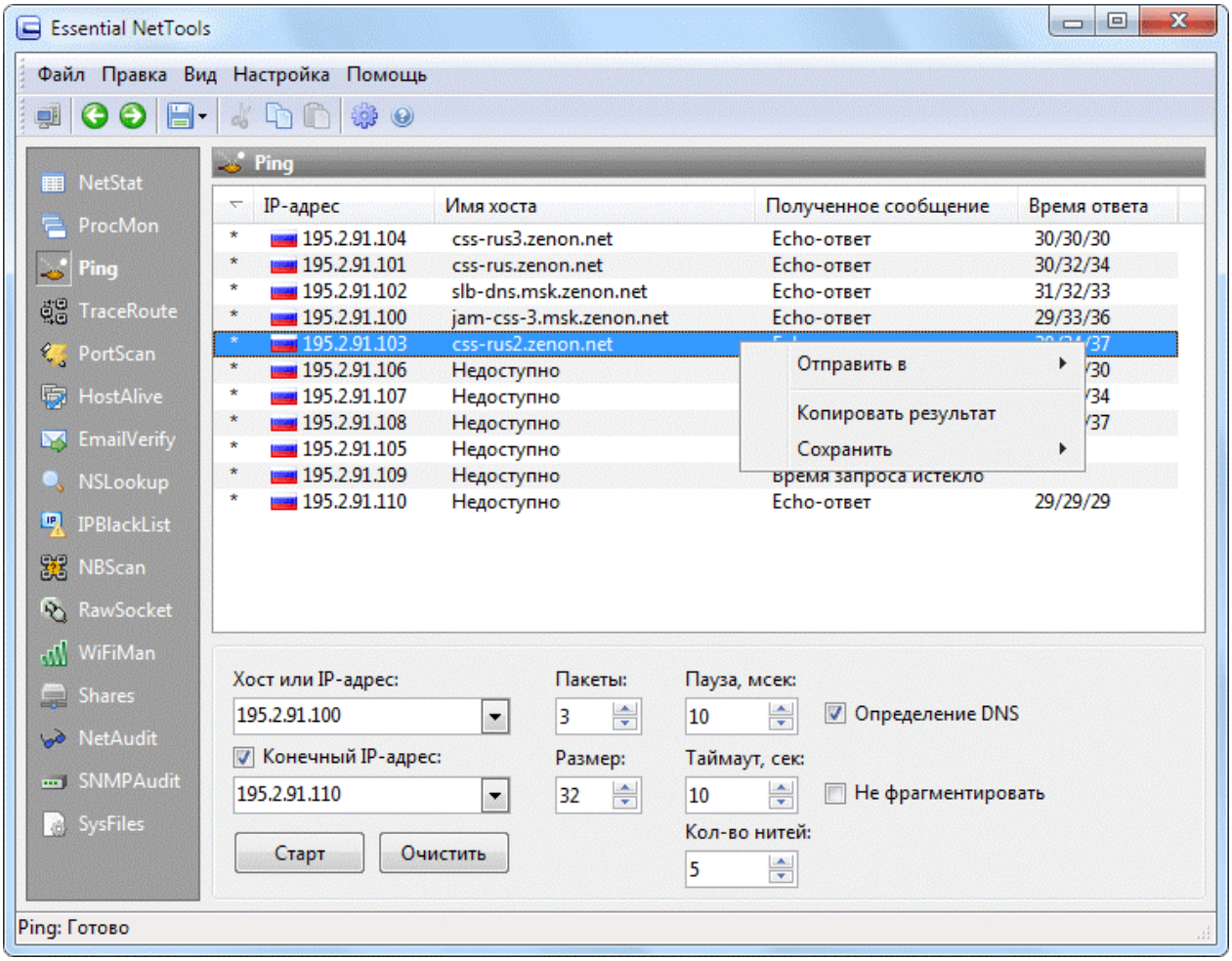
Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Автообновление** – включить/отключить автоматическое обновление списка. Период обновления можно изменить – см. Настройки.
- **Используемые модули** – показать окно со списком модулей (файлов DLL), которые использует выбранный процесс.
- **Обновить** – обновить список.

- **Диаграмма потребления ресурсов процессора** – показать/скрыть диаграмму.
- **Сброс данных** – сбросить всю накопленную статистику и начать сбор данных заново.
- **Исключить текущий процесс** – исключить из статистики процесс Essential NetTools.
- **Свойства** – показать свойства файла процесса.
- **Завершить процесс** – завершить выбранный процесс (пользуйтесь этой функцией осторожно!).
- **Копировать результат** – копировать таблицу ProcMon в буфер обмена.
- **Сохранить** – сохранить таблицу ProcMon в файл.

Ping

С помощью этого модуля вы можете убедиться, что данный IP-адрес существует и может отвечать на запросы, отправляя отклик по протоколу ICMP. Пинг используется в целях диагностики – чтобы выяснить, работает ли компьютер, с которым вы пытаетесь соединиться. Если, к примеру, вы не можете пропинговать хост, то вы не сможете воспользоваться протоколом FTP для передачи файлов этому хосту. Пинг может быть также отправлен на рабочий хост с целью выяснить время отклика. Если компьютер работает, то обычно он присылает обратно *Echo-ответ*.



Этот модуль может работать в двух режимах. Если вы снимите метку **Конечный IP-адрес**, модуль будет пинговать лишь один IP-адрес, при этом каждый адрес будет показан в отдельной строке. Если вы установите метку **Конечный IP-адрес**, модуль пропингует диапазон IP-адресов, при этом каждый адрес также будет показан в отдельной строке. В последнем случае в колонке **Время ответа** будет показано минимальное, среднее и максимальное время, отделенное символами "/".

Для начала работы с модулем введите IP-адрес или имя хоста и нажмите **Старт**. После этого будут доступны следующие характеристики:

- **Пакеты** – задать количество пакетов, которые будут переданы удаленному хосту.
- **Пауза, мсек** – установить интервал между пингами в миллисекундах.
- **Размер** – задать размер ICMP-пакета в байтах.
- **Таймаут, сек** – установить максимальной время ожидания ответа от хоста в секундах.

- **Определение DNS** – установите эту опцию, если хотите, чтобы модуль TraceRoute преобразовывал IP-адреса в имена хостов.
- **Не фрагментировать** – установить в пакете флаг "*Don't fragment* ".
- **Кол-во нитей** – установить количество заданий, выполняемых одновременно при опросе многих IP-адресов. Если на вашем компьютере не очень много оперативной памяти, рекомендуется не водить больших чисел во избежание перегрузки системы.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

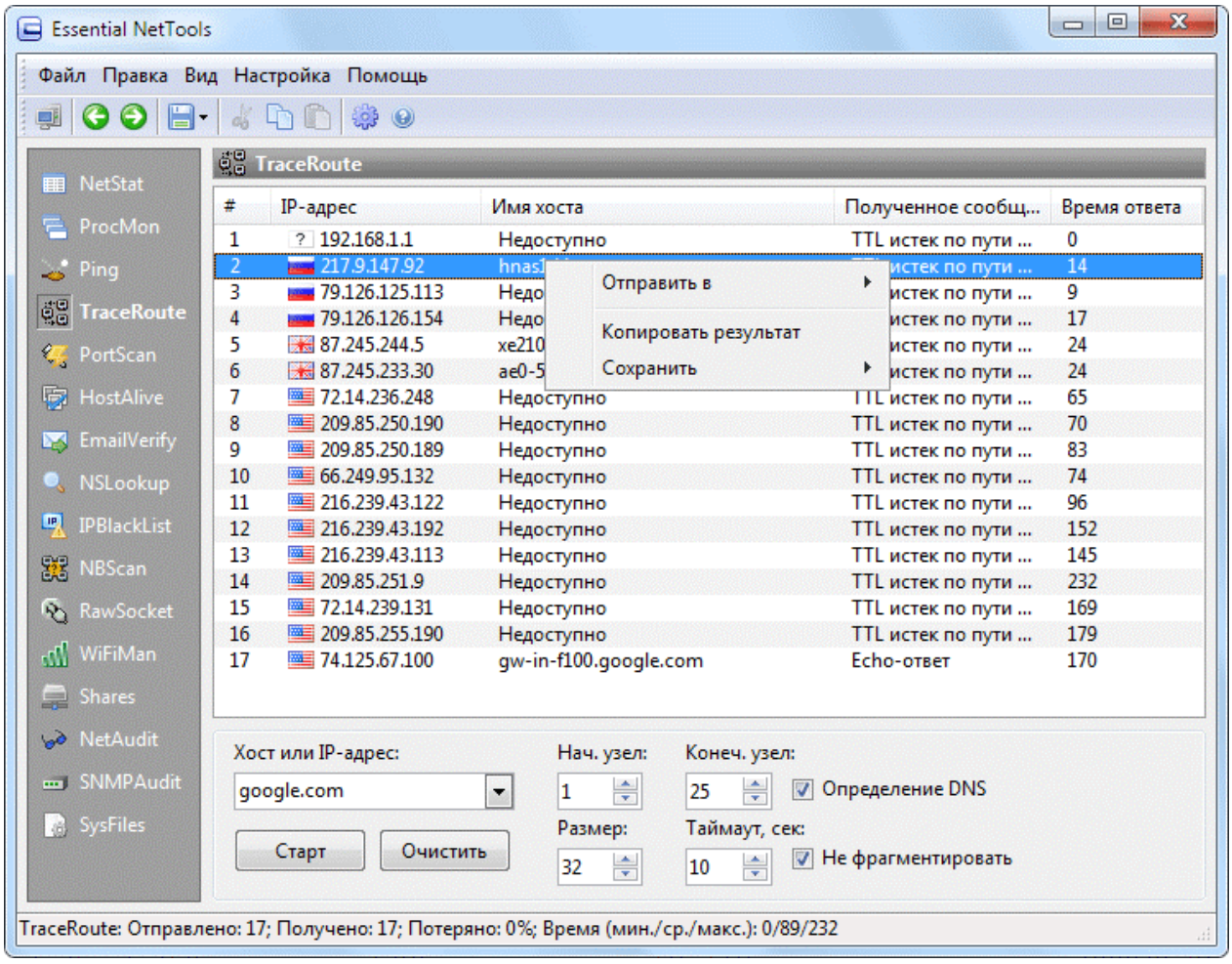
- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать результат** – копировать таблицу Ping в буфер обмена.
- **Сохранить** – сохранить таблицу Ping в файл.

TraceRoute

TraceRoute – это модуль, который отслеживает путь (т. е. шлюзы на каждом участке) от компьютера-клиента до удаленного хоста, сообщая все IP-адреса маршрутизаторов. Модуль также ведет подсчет и отображает время, затраченное на каждый шаг. TraceRoute является удобным инструментом для определения этапа, на котором возникла проблема.

TraceRoute получает ICMP-пакеты от каждого маршрутизатора. Пакет IP содержит значение "времени жизни" (Time-to-Live, TTL), которое определяет, как долго шел пакет до места назначения. Каждый раз при прохождении пакетом маршрутизатора значение TTL уменьшается на единицу; при достижении нулевого значения пакет считается потерянным и отправителю возвращается сообщение об истечении TTL.

TraceRoute отсылает первую группу пакетов с TTL, равным 1. Первый маршрутизатор в пути отменит этот пакет (его TTL станет равным нулю) и вернет ошибку об истечении TTL. Таким образом мы нашли первый маршрутизатор в пути. Можно отправлять пакеты с TTL, равным 2, 3 и т. д., каждый раз идентифицируя маршрутизатор, получая от него сообщение об ошибке. Некоторые маршрутизаторы "молча" отбрасывают пакет с TTL, равным нулю – в этом случае вы получите сообщение Время запроса истекло. В конечном счете либо будет достигнут конец цепи передачи, либо будет достигнуто максимальное значение и TraceRoute прекратит свою работу. В конечной точке TraceRoute отправит ICMP-пакет (пинг) и, если удаленный компьютер доступен, то в колонке полученных сообщений появится сообщение *Эхо-ответ*.



Для начала работы с модулем введите IP-адрес или имя хоста и нажмите **Старт**. После этого будут доступны следующие характеристики:

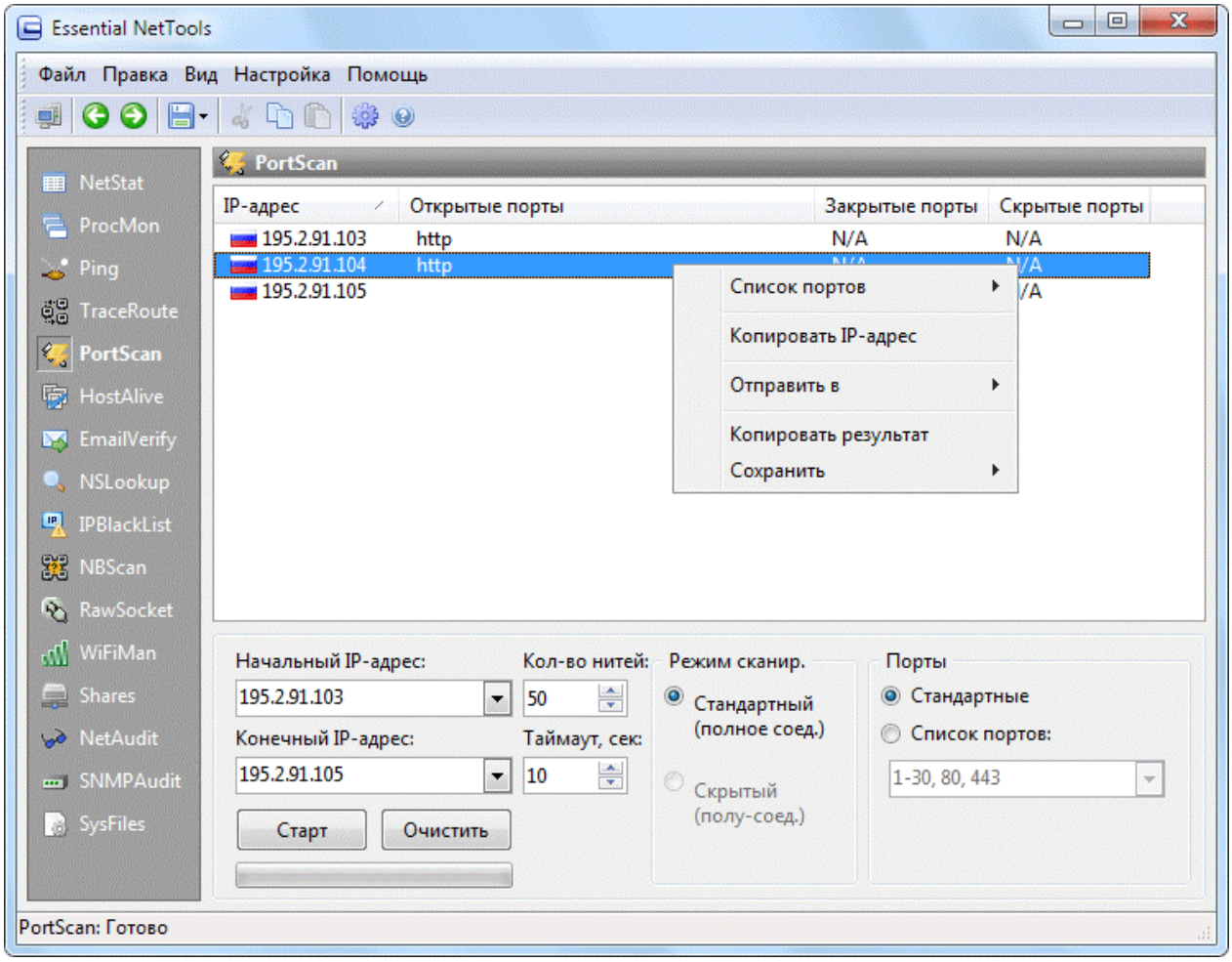
- **Нач. узел** – установить узел, с которого требуется начать трассировку. Бывает полезно установить значение больше 1, поскольку первые узлы часто бывают одинаковы; тем самым вы сэкономите некоторое время.
- **Конеч. узел** – ограничить количество трассируемых узлов.
- **Размер** – задать размер ICMP-пакета в байтах.
- **Таймаут, сек** – установить максимальной время ожидания ответа от хоста в секундах.
- **Определение DNS** – установите эту опцию, если хотите, чтобы модуль TraceRoute преобразовывал IP-адреса в имена хостов.
- **Не фрагментировать** – установить в пакете флаг "*Don't fragment* ".

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать результат** – копировать таблицу TraceRoute в буфер обмена.
- **Сохранить** – сохранить таблицу TraceRoute в файл.

PortScan

TCP-сканер PortScan показывает, какие TCP-порты открыты и могут участвовать в соединениях. Обычно TCP-сканеры используются для проверки того, работают ли на удаленном компьютере определенные сервисы (например, Telnet или FTP), а также для анализа безопасности. Сканирование порта в модуле PortScan - это отправка данных в порты из пользовательского списка портов и анализ ответов (открыт или закрыт данный порт).



Важная информация для пользователей Windows XP SP2 и Vista

В Windows XP Service Pack 2 и в более новых версиях Windows для каждой программы установлено ограничение в 10 незавершенных одновременных исходящих подключений. По достижении этого лимита все последующие попытки подключений будут помещены в очередь, где со временем будут обработаны с фиксированной скоростью. Это может существенно замедлить работу программы, в которой происходит большое количество попыток соединений. Примером такой программы является Essential NetTools в режиме сканирования портов (модуль PortScan).

В настоящее время не существует официальных решений для этой проблемы. Однако существует неофициальная программа, которая модифицирует системные файлы и устраняет это ограничение. Если вы работаете Windows XP Service Pack 2 и недовольны скоростью либо качеством работы работы модуля PortScan (например, многие открытые порты остались необнаруженными), попробуйте установить одну из неофициальных программ, доступных на сайте http://www.lvllord.de/ .

Предупреждение: эта программа работает только с Windows XP Service Pack 2 и не поддерживается компанией Microsoft.

К тому же, в Windows XP Service Pack 2 и в более новых версиях Windows убрана поддержка raw sockets, что делает невозможной работу модуля PortScan в скрытом режиме Stealth. Неофициальных программ-решений этой проблемы в настоящий момент неизвестно.

Перед началом сканирования введите начальный и конечный IP-адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес**, как показано выше. Вы также можете задать количество одновременных подключений и таймаут соединения в полях **Кол-во нитей** и **Таймаут, сек** соответственно. Затем следует выбрать режим сканирования: **Стандартный** или **Скрытый**. В стандартном режиме устанавливается TCP-соединение между вашим компьютером и тем компьютером, который вы сканируете. В скрытом режиме соединение создается, но не завершается. Эта технология сканирования известна как полуоткрытая (half-open) или *SYN*: программа отсылает SYN-пакет (как будто мы хотим установить соединение), а удаленный хост отвечает пакетом SYN ACK (это означает, что порт готов к обмену) или RST ACK (порт не готов к обмену). Удаленный хост не может обнаружить скрытое сканирование на уровне TCP, хотя системы обнаружения вторжений могут это обнаружить на уровне пакетов. Этот режим может вам пригодиться при тестировании и оценки эффективности настроек системы обнаружения вторжений. Скрытый режим работает только в **Windows 2000/XP**, требует административных привилегий и не может быть использован для сканирования ваших собственных IP-адресов (чтобы просканировать собственные IP-адреса, используйте обычный режим или зайдите в модуль NetStat и просмотрите список открытых портов). Также учтите, что работающий **на вашем** компьютере файрволл может повлиять на результаты сканирования в скрытом режиме, поэтому рекомендуется закрыть подобные программы на время сканирования.

В завершение вам следует определиться со списком портов для сканирования. **Стандартный** список включает в себя следующие порты: 7, 9, 11, 13, 17, 19, 21, 23, 25, 43, 53, 70, 79, 80, 88, 110, 111, 113, 119, 135, 139, 143, 389, 443, 445, 512, 513, 1080, 1512, 3128, 6667 и 8080. Если вы хотите создать свой собственный список, выберите **Список портов**. Синтаксис для ввода номеров портов достаточно прост: вы можете вводить как отдельные порты, так и области портов, отделяя эти записи запятыми. Ниже показаны примеры списков:

1-1024

1-30, 80, 443

21, 22, 25, 80-88, 1000-1024, 6666

После того, как заданы все настройки, нажмите кнопку **Старт**. Скорость сканирования можно задать через меню **Настройка** => **Установки** (см. главу Установки).

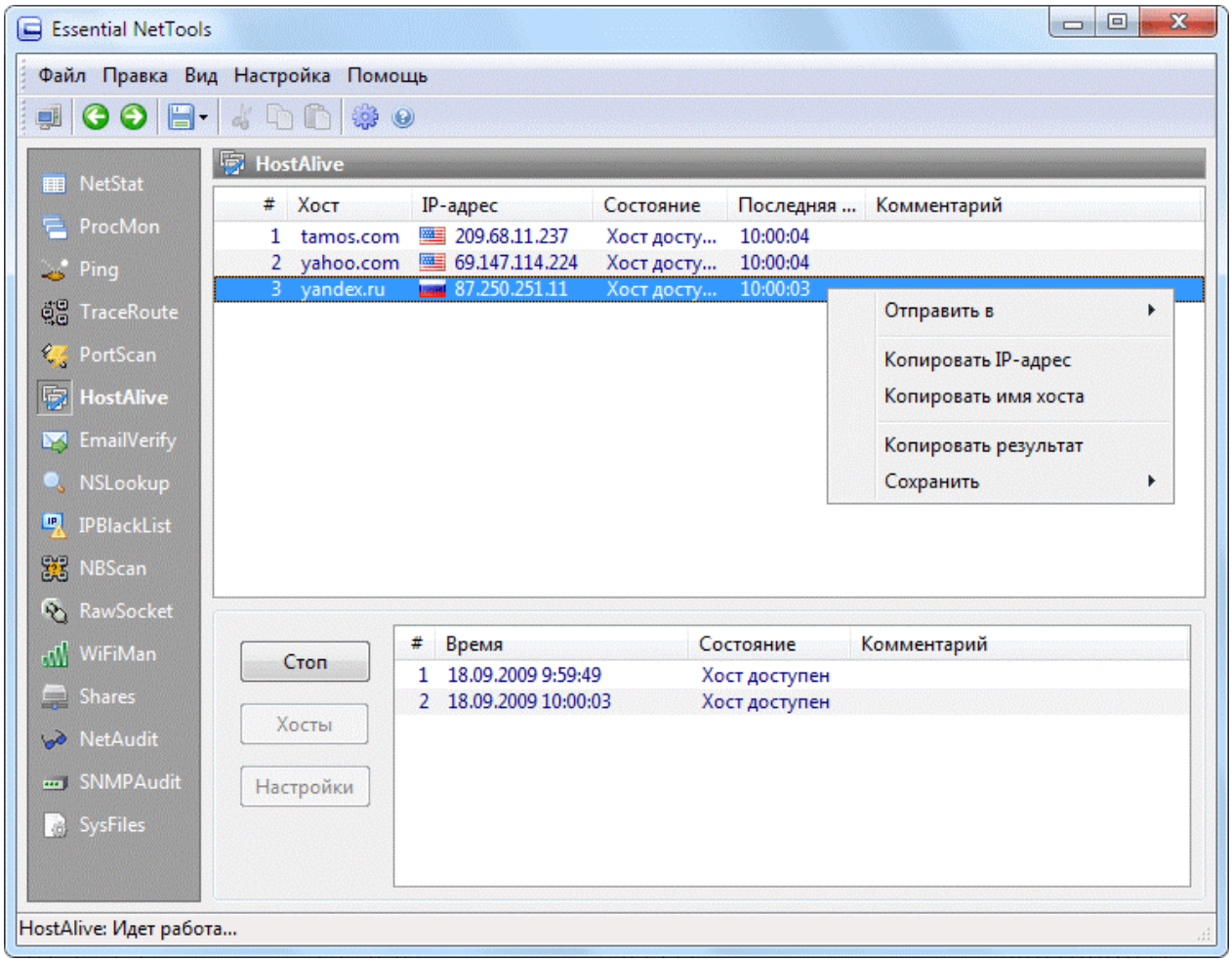
В процессе сканирования информация о портах заносится в список. В колонке **Открытые порты** указаны порты, которые подтвердили соединение. В колонке **Закрытые порты** указано количество портов, которые отказали в соединении, а в колонке **Скрытые порты** указано количество портов, которые проигнорировали попытки соединения. В обычном режиме последние две колонки пусты, поскольку в этом режиме можно лишь определять открытые порты, но не определять разницы между закрытыми и скрытыми портами. Другими словами, в обычном режиме все неоткрытые порты считаются закрытыми. В скрытом режиме порты, которые отвечают пакетами RST ACK считаются закрытыми, а порты, которые проигнорировали наши SYN-пакеты считаются скрытыми. В последнем случае вполне вероятно, что эти порты защищены файрволлом.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

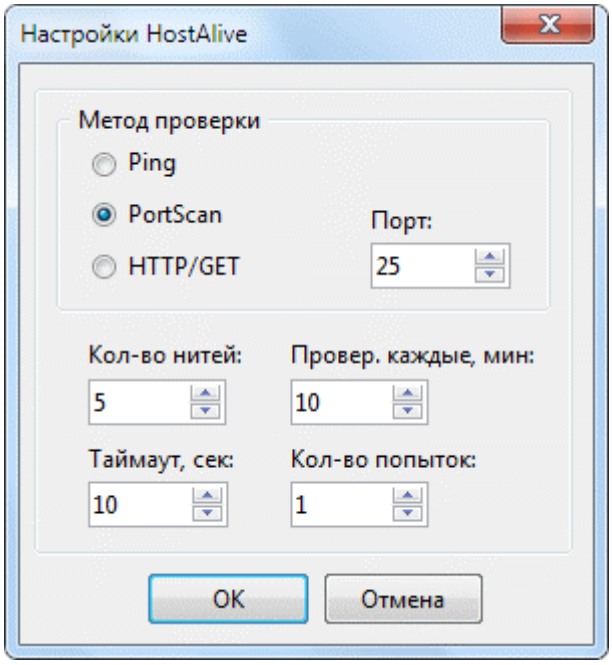
- **Список портов** – показать полный список открытых, закрытых и скрытых портов. Поскольку списки портов обычно длинные, эта команда как раз создана для показа таких длинных списков.
- **Копировать IP-адрес** – копировать IP-адрес выбранного компьютера в буфер обмена.
- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать результат** – копировать таблицу PortScan в буфер обмена.
- **Сохранить** – сохранить таблицу PortScan в файл.

HostAlive

HostAlive – это модуль, который периодически проверяет доступность удаленного хоста или группы хостов. Работа HostAlive основана на простом принципе: он отправляет сетевой пакет на хост назначений и ждет ответа. Например, с его помощью можно проверить, работает ли на удаленном хосте сервис HTTP. Метод проверки и интервал настраиваются пользователем.



Для проверки списка хостов нажмите кнопку **Хосты**. Введите имена или IP-адреса хостов, которые вы хотите проверить. Для настройки метода проверки нажмите кнопку **Настройки**:



Существует три метода проверки:

- **Ping:** стандартная проверка с использованием ping-пакетов ICMP. Это наиболее общий метод проверки, который сообщит вам, подключен ли хост к сети и работает ли операционная система. При этом не будет информации, работает ли какой-то определенный сетевой сервис, такой как HTTP или POP3. Нужно иметь ввиду, что хосты, находящиеся за брандмауэром, могут не отвечать на ping-пакеты.
- **PortScan**: проверка, основанная на способности хоста принимать входящие TCP-соединения. Например, просканировав TCP-порт 110, вы узнаете, работает ли сервис POP3.
- **HTTP/GET**: проверка веб-сервера на предмет того, принимает ли удаленный хост подключения по стандартному HTTP-порту и возвращает ли корректный HTTP-отклик. Стандартный HTTP-порт имеет номер 80, но вы можете ввести и другое значение.

Также доступны следующие настройки:

- **Кол-во нитей** – указать количество одновременно выполняемых заданий, которые может запустить модуль.
- **Провер. каждые, мин** – указать интервал между проверками в минутах.
- **Таймаут, сек** – указать, сколько времени модуль будет ждать отклика от хоста.
- **Кол-во попыток** – указать количество попыток.

После того, как вы ввели список хостов для проверки и выполнили настройку, нажмите **Старт** для начала процесса. Модуль будет периодически проверять хосты до тех пор, пока вы не нажмете **Стоп** или не выйдите из программы.

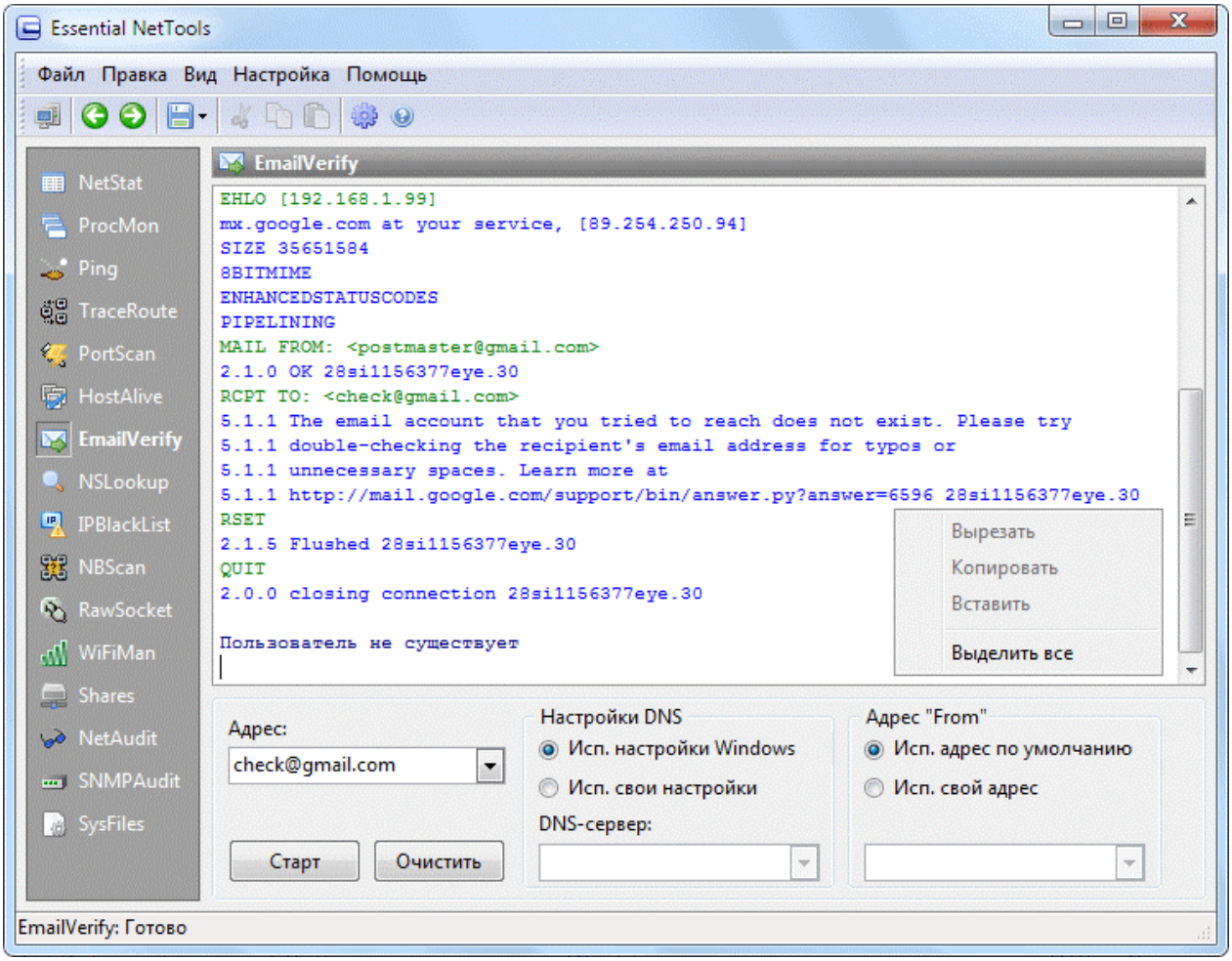
Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать IP-адрес** – копировать IP-адрес выбранного компьютера в буфер обмена.
- **Копировать имя хоста** – копировать имя хоста выбранного компьютера в буфер обмена.

- **Копировать результат** – копировать таблицу HostAlive в буфер обмена.
- **Сохранить** – сохранить таблицу HostAlive в файл.

EmailVerify

EmailVerify – это модуль, который проверят, существует ли адрес электронной почты и может ли этот адрес принимать почту. Модуль проверяет записи MX почтового адреса (другими словами, определяет, какой почтовый сервер обрабатывает почту для данного адреса) и затем пробует подключиться к почтовому серверу и доставить почту. В процессе этой проверки реально сообщения не отправляются.



Для проверки адреса электронной почты введите его в соответствующее поле и нажмите **Старт**. Результаты проверки будут отображены в главном окне.

Для обнаружения почтового сервера EmailVerify должен выполнить несколько DNS-запросов. По умолчанию, модуль будет пытаться работать с DNS-серверами, используемыми Windows. В некоторых нестандартных ситуациях вы можете обойти эти настройки, выбрав **Исп. свои настройки** и введя свой адрес сервера.

В процессе верификации электронной почты EmailVerify должен предоставить адрес отправителя. По умолчанию используется адрес *postmaster@domain*, где *domain* – часть почтового адреса. Например, если вы проверяете адрес *user1@gmail.com*, EmailVerify в качестве адреса "From" использует адрес *postmaster@gmail.com*. Этот адрес можно изменить и ввести свой, выбрав пункт **Исп. свой адрес**.

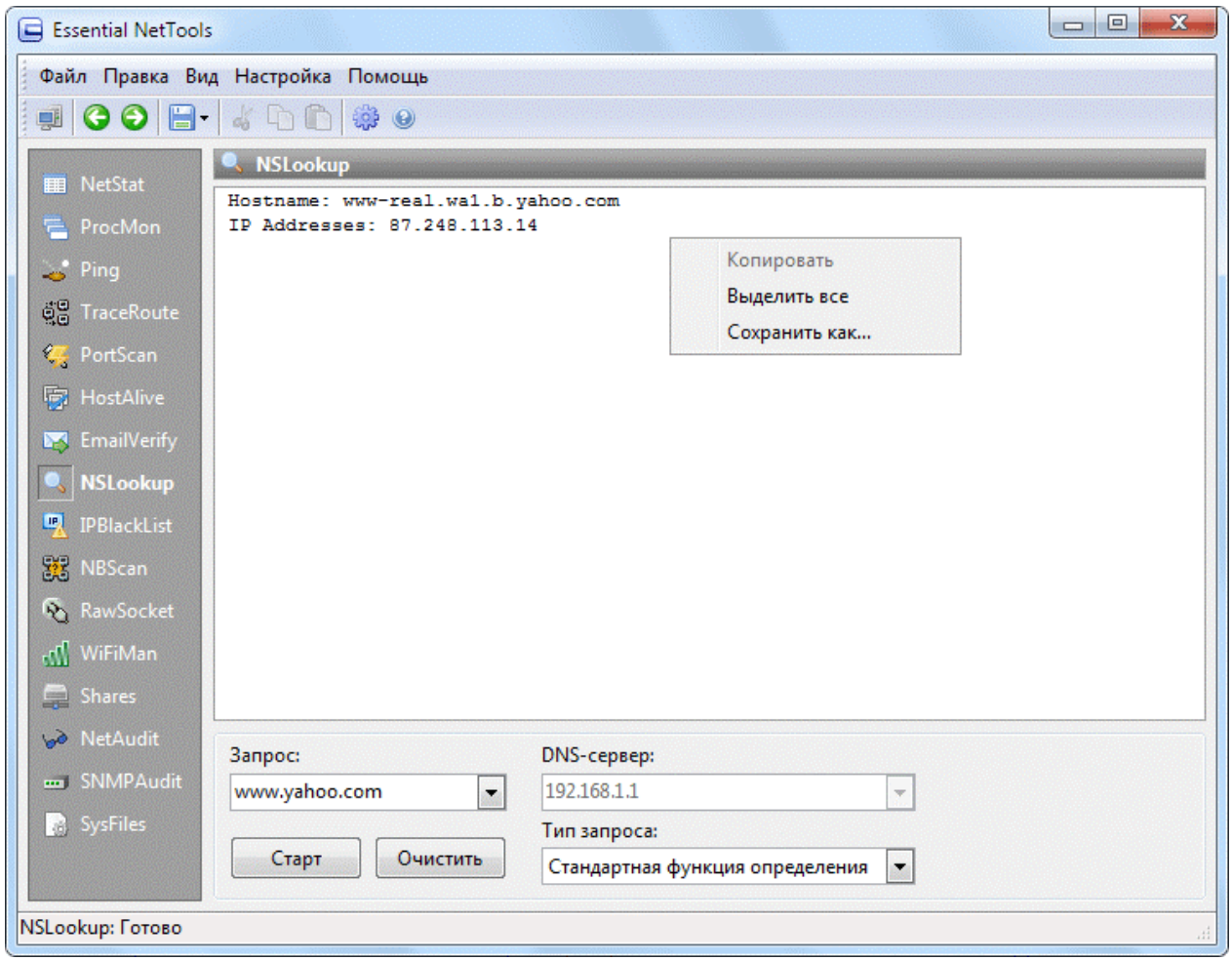
Важно помнить, что результаты этого теста могут зависеть от того, с какого IP-адреса вы подключаетесь, а также от используемого адреса "From". Почтовый сервер может отвергнуть почту с

определенных IP-адресов или со всех динамических IP-адресов. Он также может отказать в обработке почты с определенных доменов или учетных записей (аккаунтов).

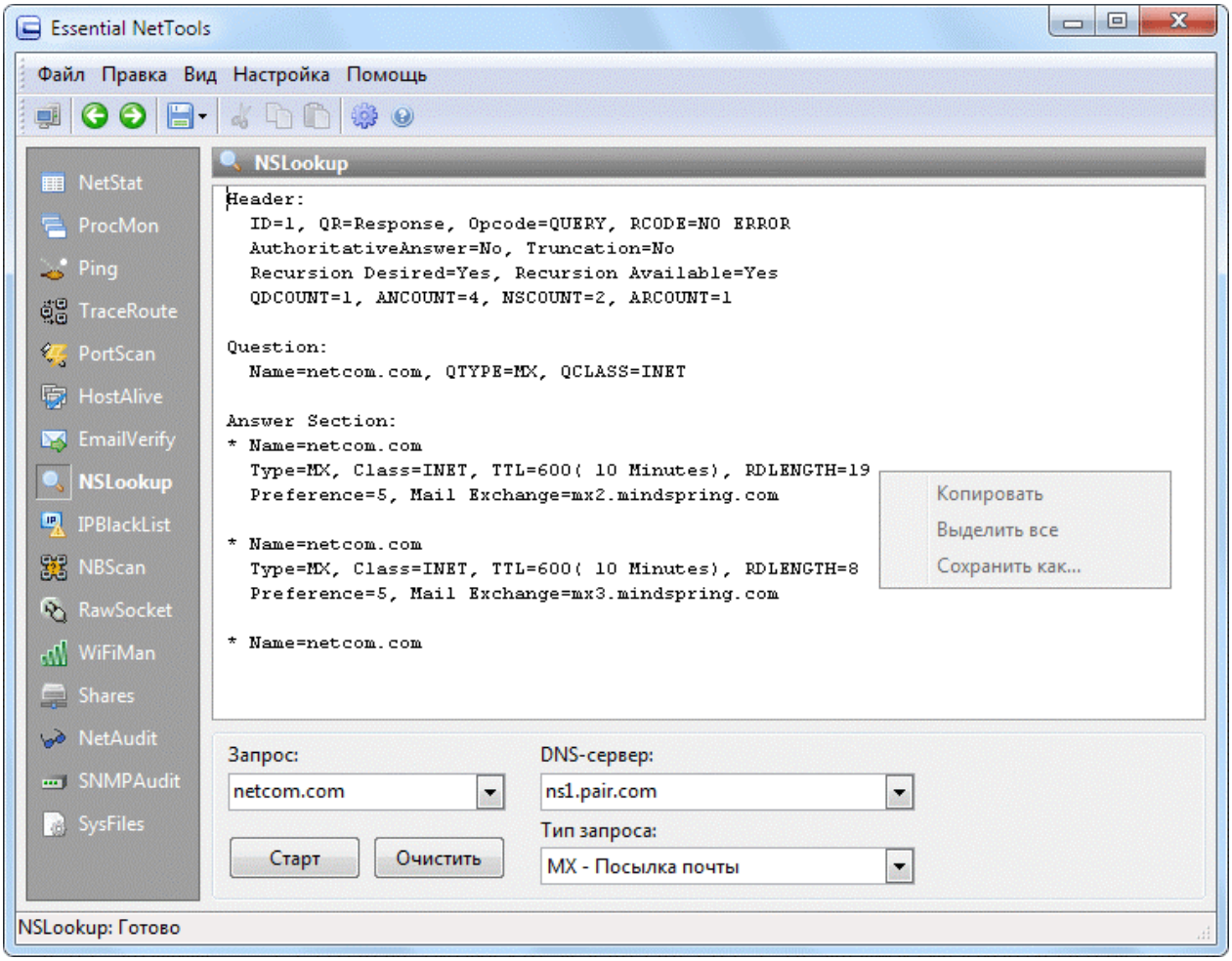
NSLookup

Модуль NSLookup позволяет получить IP-адрес по имени хоста (например, www.yahoo.com). Здесь также можно выполнить обратный поиск по имени и узнать имя хоста по IP-адресу. Выполнение таких преобразований является основной функцией NSLookup; тем не менее, опытные пользователи могут создавать более сложный запросы, например, для записей Mail Exchange (MX). NSLookup работает путем посылки запроса на ваш DNS-сервер по умолчанию (в случае **Стандартной функции определения**) или на любой другой указанный вами DNS-сервер (если в выпадающем списке **Тип запроса** выбран какой-либо другой тип, отличный от стандартного).

Для выполнения стандартного запроса в списке **Тип запроса** выберите **Стандартная функция определения**, в поле **Запрос** введите IP-адрес или имя хоста и нажмите **Старт**. Программа выдаст результат в течение нескольких секунд. В случае стандартного запроса программа свяжется с вашим DNS-сервером по умолчанию, так что поле **DNS-сервер** будет недоступно для ввода.



Для выполнения нестандартных запросов выберите **Тип запроса**, введите сам запрос в поле **Запрос** и в поле **DNS-сервер** укажите адрес DNS-сервера. При первом запуске программы выпадающий список серверов будет содержать ваши DNS-сервера по умолчанию; вам следует выбрать один из списка либо ввести любой другой, например, "ns1.pair.com".



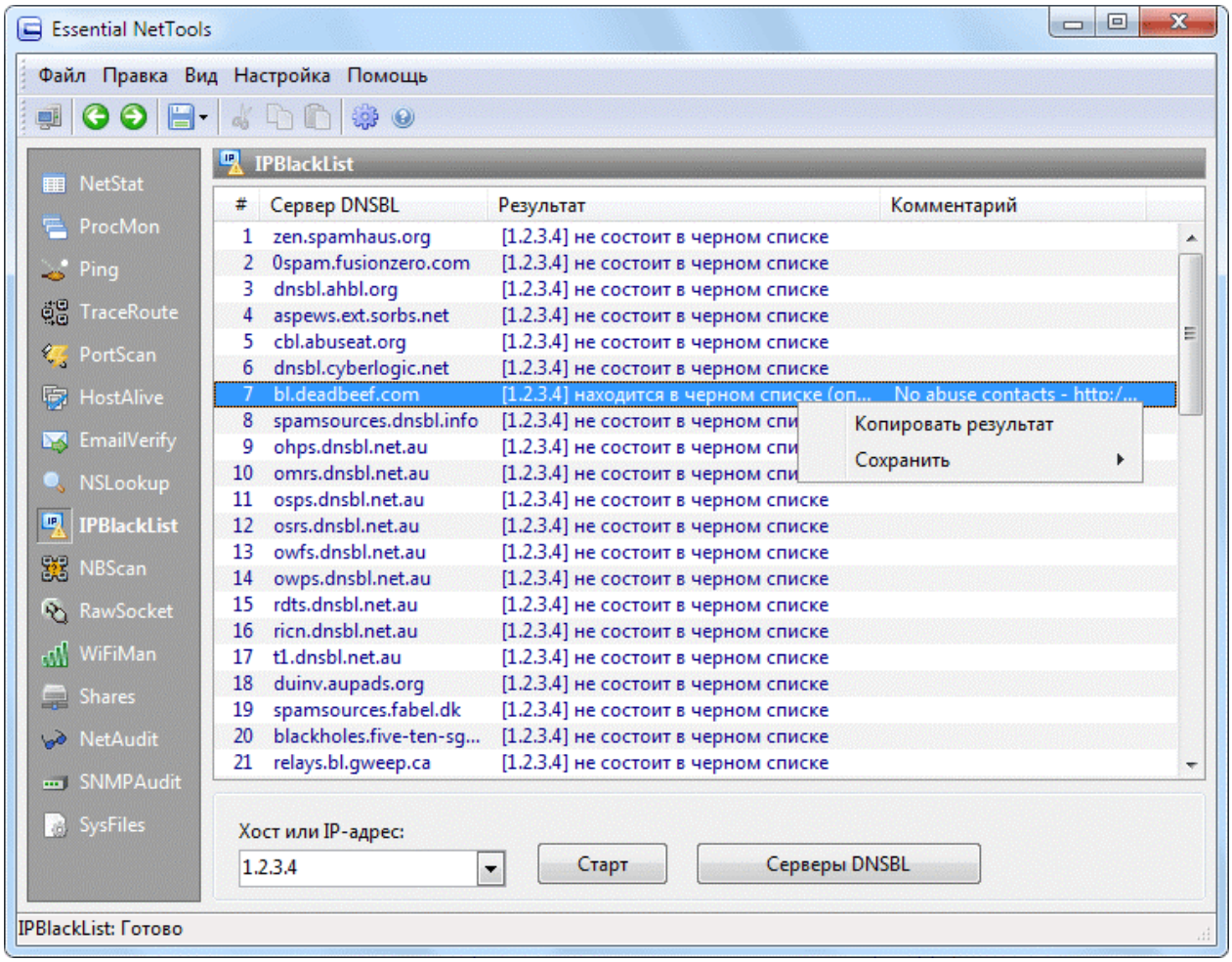
В NSLookup предлагается множество вариантов запросов, поэтому требуется некоторое понимание Интернет-технологий для выполнения запросов, отличных от стандартного. Если вы новичок и хотите побольше узнать о различных типах запросов, мы советуем вам почитать RFC 1034 и RFC 1035 или поискать в Интернете по названиям самих запросов.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Копировать** – копировать выделенный текст в буфер обмена.
- **Выделить все** – выделить весь текст в окне.
- **Сохранить как** – сохранить отчет в файл.

IPBlackList

IPBlackList – это модуль для проверки IP-адресов на предмет их нахождения в различных черных списках, таких как базы данных адресов спамеров, открытые прокси, рилеи электронной почты и т. п. Этот модуль полезен при определении причины, почему данный IP-адрес отвергается определенными сетевыми ресурсами, такими как почтовые сервера.



IPBlackList проверяет введенный IP-адрес на предмет его нахождения в базах данных, поддерживаемых DNSBL-серверами (за более подробной информацией об этой технологии обратитесь сюда). Вкратце, модуль работает следующим образом. К примеру, вы хотите проверить, не находится ли адрес 1.2.3.4 в черном списке сервера *antispam.somedomain.com*. IPBlackList посылает DNS-запрос, который выглядит как *4.3.2.1.antispam.somedomain.com*, на ваш DNS-сервер. Если такая DNS-запись существует, т. е. данный адрес хоста может быть преобразован в IP-адрес (согласно спецификациям DNSBL, такой IP-адрес должен принадлежать к области локальных IP-адресов, т. е. 127.x.x.x), то проверяемый IP-адрес 1.2.3.4 действительно занесен в черный список.

Обратите внимание, что мы не поддерживаем черные списки DNSBL-серверов, и по этой причине мы не можем удалить вас оттуда.

Модуль IPBlackList позволяет провести проверку IP-адреса по многим DNSBL-серверам одновременно. Essential NetTools содержит список известных DNSBL-серверов, но вы можете ввести свой список, нажав на кнопку **Сервера DNSBL**.

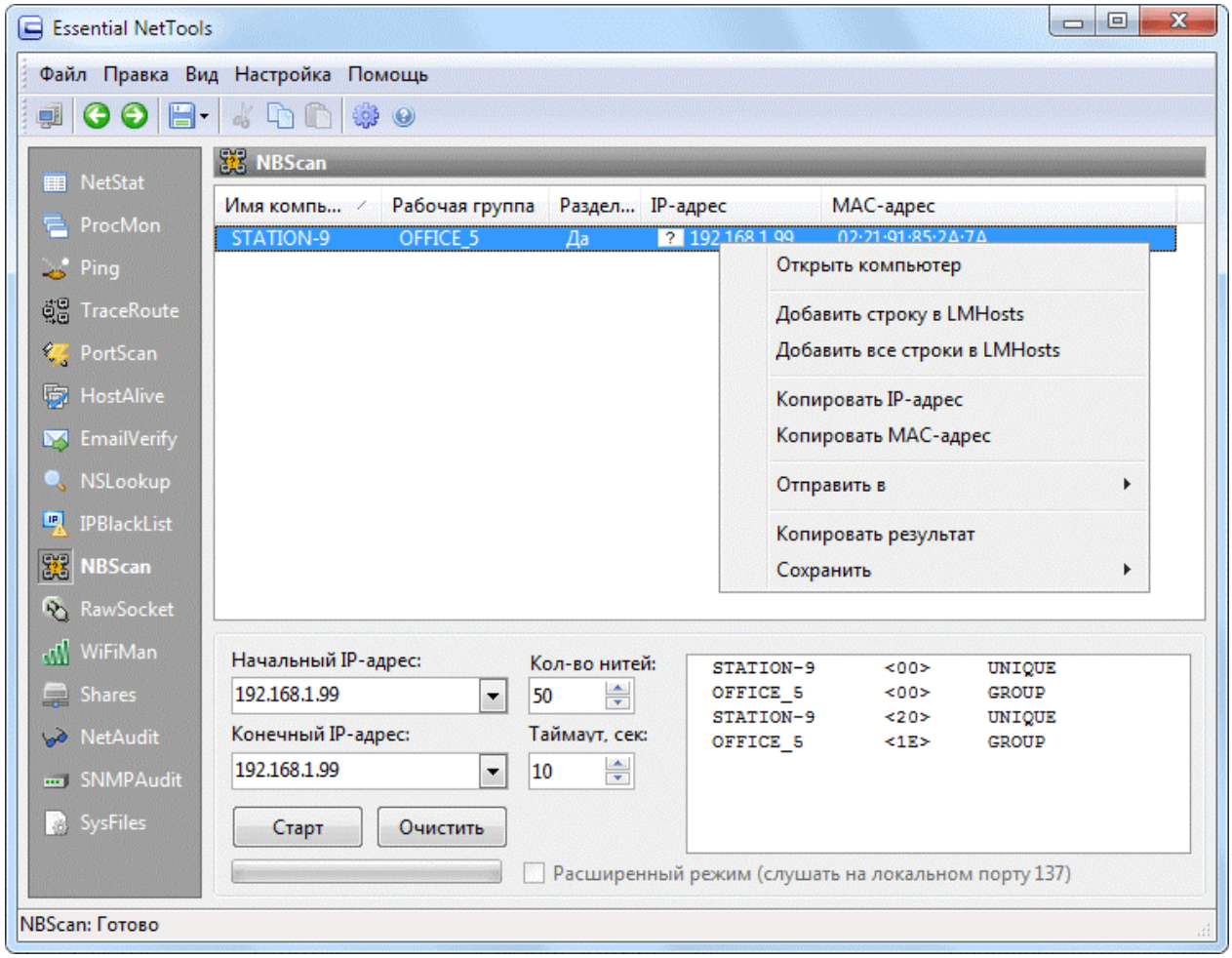
Свежий список функционирующих DNSBL-серверов доступен по адресу http://www.declude.com/Articles.asp?ID=97.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Копировать результат** – копировать таблицу IPBlackList в буфер обмена.
- **Сохранить** – сохранить таблицу IPBlackList в файл.

NBScan

NBScan – это мощный и быстрый сканер NetBIOS, который используется для исследования сетей. NBScan может просканировать сеть в заданном диапазоне IP-адресов и показать список компьютеров с разделяемыми ресурсами NetBIOS, а также таблицы их имен. В отличие от стандартной Windows-утилиты nbtstat данный модуль располагает удобным графическим интерфейсом и удобной системой управления файлом lmhosts, а также возможностью параллельного сканирования, которое позволяет проверить сеть класса C менее, чем за одну минуту. Можно сканировать сети класса B и C. NBScan существенно облегчает рутинную работу системных проектировщиков, администраторов и аналитиков.



Перед началом сканирования введите начальный и конечный IP-адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес** как показано выше. Вы также можете указать число одновременных подключений и таймаут подключения в поля **Кол-во нитей** и **Таймаут, сек** соответственно. Иногда можно пользоваться **Расширенным режимом** (описание см. ниже). В колонке **Разделяемые ресурсы** указывается, предлагает ли данный компьютер какие-либо ресурсы: некоторые компьютеры могут быть не настроены на разделение ресурсов; тем не менее, они отвечают на NetBIOS-запросы и попадают в список.

Кликнув по компьютеру в списке, вы увидите его имя в нижнем окне. Если вы не понимаете значений из таблицы имен NetBIOS, то рекомендуем ее просмотреть.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Открыть компьютер** – попытаться открыть выбранный компьютер. Если компьютер доступен, откроется новое окно Проводника Windows с ресурсами удаленного компьютера.
- **Добавить строку в LMHosts** – добавить запись по выбранному компьютеру в файл lmhosts в требуемом формате.
- **Добавить все строки в LMHosts** - добавить записи по выбранным компьютерам в файл lmhosts в требуемом формате.
- (компьютеры, не имеющие разделяемых ресурсов, добавлены не будут).
- **Копировать IP-адрес** – копировать IP-адрес выбранного компьютера в буфер обмена.
- **Копировать MAC-адрес** – копировать MAC-адрес выбранного компьютера в буфер обмена.
- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать результат** – копировать таблицу NBScan в буфер обмена.
- **Сохранить** – сохранить таблицу NBScan в файл.

Расширенный режим

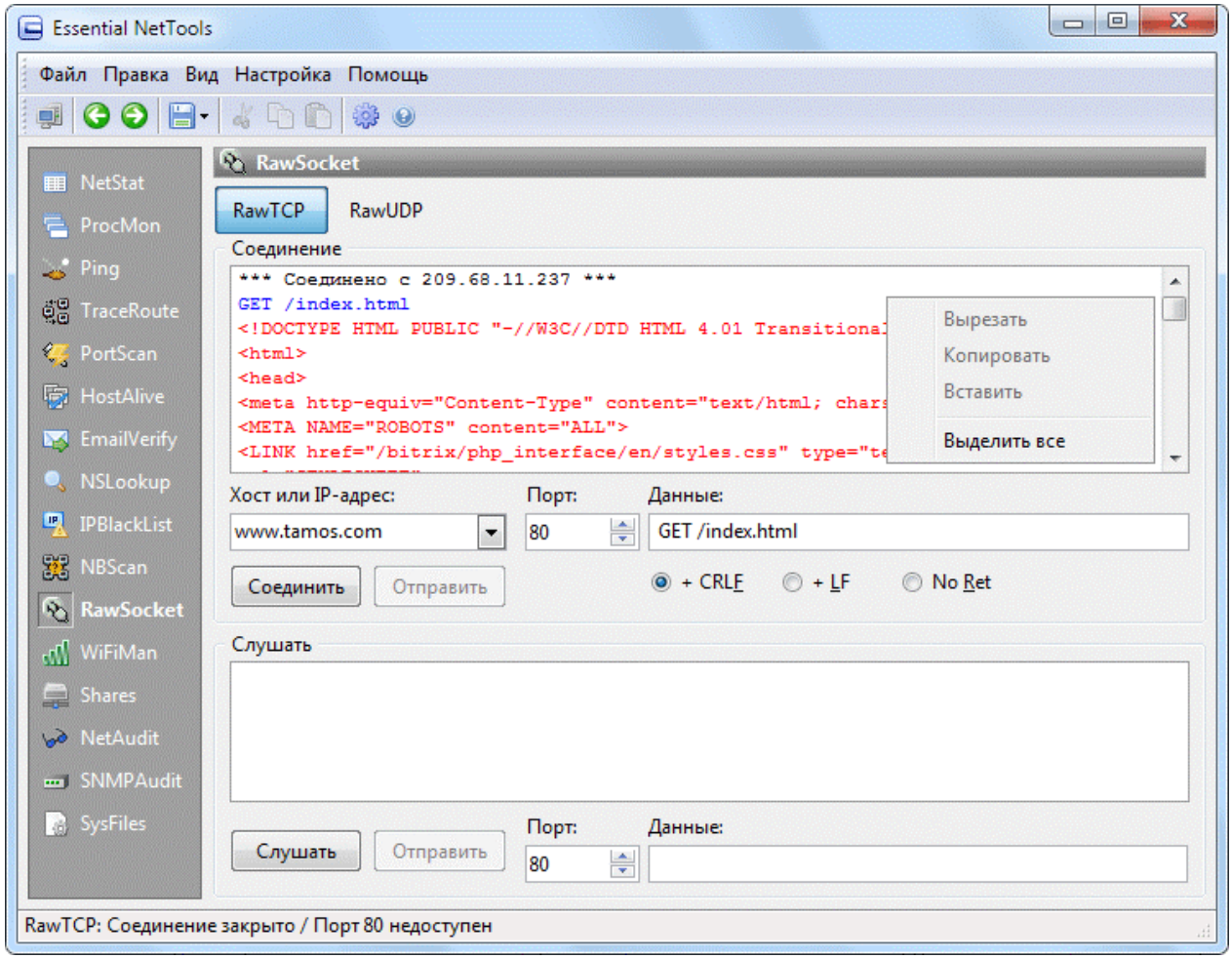
По причине некоторых особенностей в обработке NetBIOS-соединений, небольшой процент компьютеров может посылать ответы на NetBIOS-запросы только на порт 137, в независимости от того, с какого порта этот запрос был отправлен. Расширенный режим позволяет вам включить прием ответов, посланных на порт 137. Для перехода в этот режим установите флаг **Расширенный режим (слушать на локальном порту 137)**. В том случае, если компьютер уже вошел в сеть, расширенный режим может быть недоступен. Если компьютер уже в сети, этот пункт меню недоступен. Если вы хотите воспользоваться этим режимом, то установите флаг ДО ТОГО, как компьютер войдет в сеть. Например, если вы работаете с dial-up, то следует сначала запустить программу, установить флаг и уже после этого устанавливать соединение с провайдером.

Важно: работа в расширенном режиме может привести к неработоспособности сетевых сервисов Windows, привязанных к порту 137, например, модуля nbtstat. Вы также можете потерять возможность подключаться к удаленным компьютерам. Для восстановления нормальной работоспособности этих сервисов выключите расширенный режим, выйдите из сети и зайдите в нее снова.

Причина этих ограничений проста: в любой системе только один порт 137 и он "принадлежит" тому процессу, который заявил на его свои права первым. Если первым заявку подаст Essential NetTools, то программа сможет работать в расширенном режиме, но он будет недоступен операционной системе. Если операционная система "захватит" его первым, вы не сможете работать в расширенном режиме. Помните, что этот режим всего лишь дополнительная опция, и вам она может не понадобиться. Вполне вероятно, что вы не заметите разницы в результатах, полученных в обычном и расширенном режимах.

RawSocket

Модуль **RawSocket** предоставляет вам возможность передавать и принимать "сырую" информацию на/от IP-адрес, а также принимать входящие TCP- или UDP-соединения на любом локальном порту. Эти функции могут пригодиться при выявлении неисправностей в работе некоторых сетевых сервисов или для понимания сути процессов, происходящих в протоколах уровня приложения, таких как POP, SMTP или DAYTIME. Ниже на скриншоте показан пример HTTP-соединения, которое вы можете создать с помощью данного модуля:



Соединить

Для подключения к удаленному хосту введите его IP-адрес или имя, выберите порт и нажмите **Соединить**. Как только соединение будет установлено, вы сможете вводить любые данные в поле ввода **Данные**. Чтобы отправить эти данные на удаленный хост, нажмите **Отправить**. При пересылке данных вы можете изменять символы-разделители строк: LF (перенос строки, 0x0A), Перенос строки + возврат каретки (CRLF, 0x0D0A) или вообще не использовать разделитель. Для передачи произвольных символов, включая непечатаемые, используйте структуру [xx], где xx – шестнадцатеричный код отправляемого символа. Например, структура вида [48]ELLO будет преобразована в HELLO, поскольку ASCII-кодом "H" является 0x48. Передаваемые данные показаны синим цветом, а принимаемые – красным.

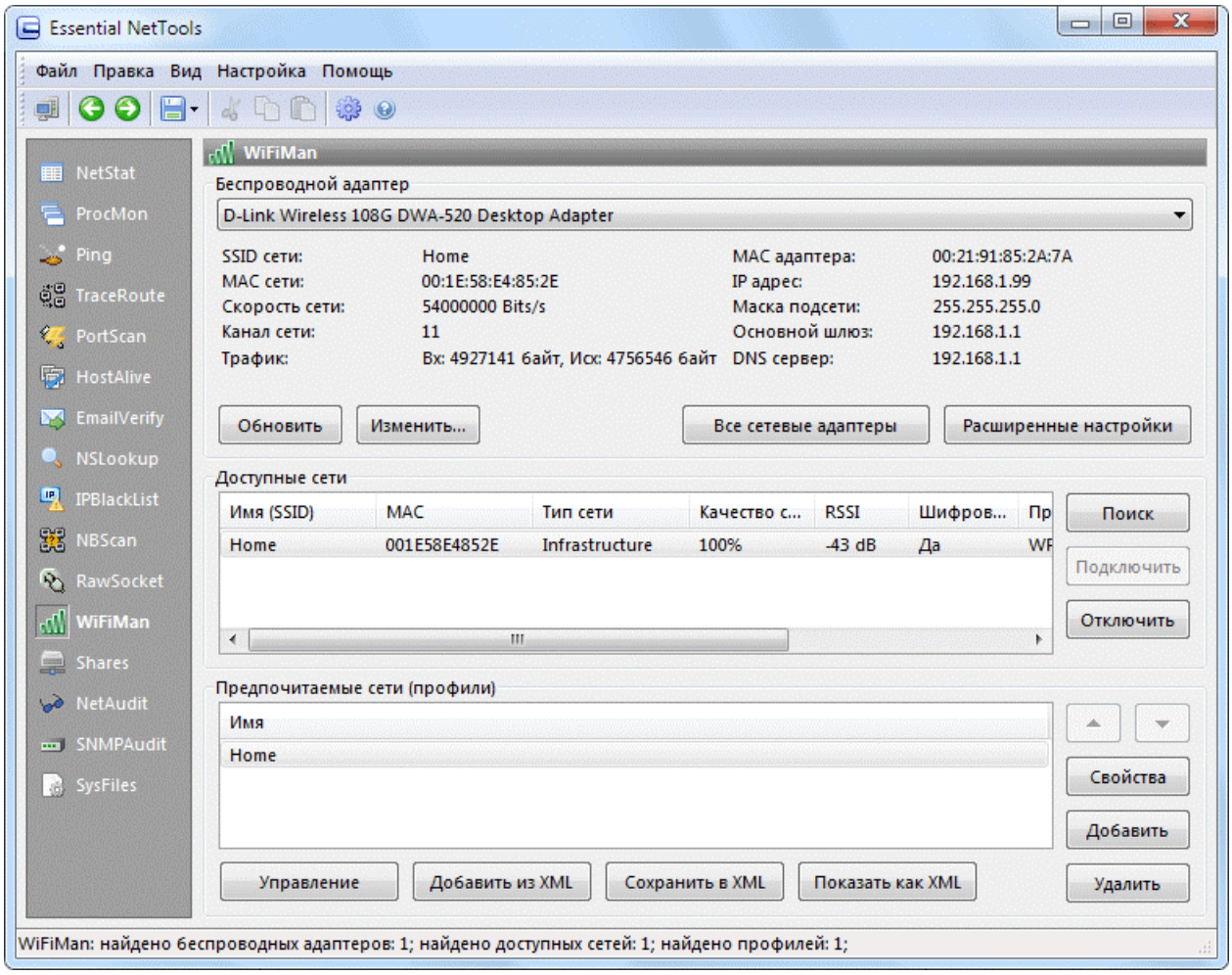
Слушать

Для прослушивания входящих соединений выберите локальный порт и нажмите **Слушать**. При подключении к вашему компьютеру удаленного хоста информация об этом подключении появится в окне. Если удаленный хост передает данные в локальный порт, то переданные данные будут показаны красным цветом. Процесс передачи данных удаленному хосту описан выше. Ваша информация будет показана синим цветом. Чтобы закрыть локальный порт, нажмите **Отключить**.

Все инструкции, описанные выше, относятся к **RawTCP** и **RawUDP** за одним исключением: так как протокол UDP не поддерживает соединений, для **RawUDP** нет кнопки **Соединить**. Для отправки UDP-данных вам не нужно устанавливать соединения. Т. е. вы должны только отправить эти данные.

WiFiMan

Модуль **WiFiMan** показывает установленные в системе беспроводные адаптеры, доступные беспроводные сети и позволяет вам редактировать профили подключения к ним. Данный модуль доступен только в Windows XP SP2 и в более поздних версиях Windows.



Интерфейс модуля логически разбит на три группы: **Беспроводной адаптер**, **Доступные сети** и **Предпочитаемые сети (Профили)**.

Группа **Беспроводной адаптер** позволяет просмотреть информацию о параметрах выбранного адаптера. Если в системе установлено несколько адаптеров, вы можете выбрать нужный из выпадающего списка. По каждому адаптеру представлена информация о его основных параметрах и параметрах сети, к которой он подключен. Кроме информации в этой же группе вы можете выполнить следующие команды:

- **Обновить** – обновляет информацию о количестве и параметрах установленных в системе беспроводных адаптеров.
- **Изменить…** – показывает диалог, в котором вы можете изменить следующие параметры беспроводного адаптера: **IP адрес**, **Маска подсети**, **Шлюз по умолчанию**, **DNS сервер** и **MAC адаптера**.
- **Все сетевые адаптеры** – показывает диалог со списком всех сетевых адаптеров установленных в системе и информацию о них. В этом диалоге вы можете включить,

отключить или перезапустить выбранный из списка адаптер, нажав на соответствующую кнопку.

- **Расширенные настройки** – показывает диалог для редактирования настроек. Диалог позволяет выбрать тип сетей для соединения, указать, нужно ли использовать Windows для управления адаптером и выбрать режим автоматического подключения к любой сети. В диалоге доступны следующие опции:
  - **Доступные сети** – настройка поиска доступных сетей. Данная опция работает только в Windows Vista и более старших версиях. Для Windows XP выполняется поиск всех доступных сетей.
  - **Использовать Windows для настроек** – данная опция поддерживается только в Windows XP.
- **Автоматическое подключение к любой сети** – данная опция поддерживается только в Windows XP.

Группа **Доступные сети** показывает список доступных беспроводных сетей и их параметры. В этой группе доступны следующие команды:

- **Поиск** – выполняет поиск доступных беспроводных сетей.
- **Подключить** – выполняет подключение к выбранной сети.
- **Отключить** – отключиться от выбранной сети.

Дополнительно по клику правой кнопкой мыши в списке доступных сетей будет показано контекстное меню с командами **Подключить** и **Отключить**.

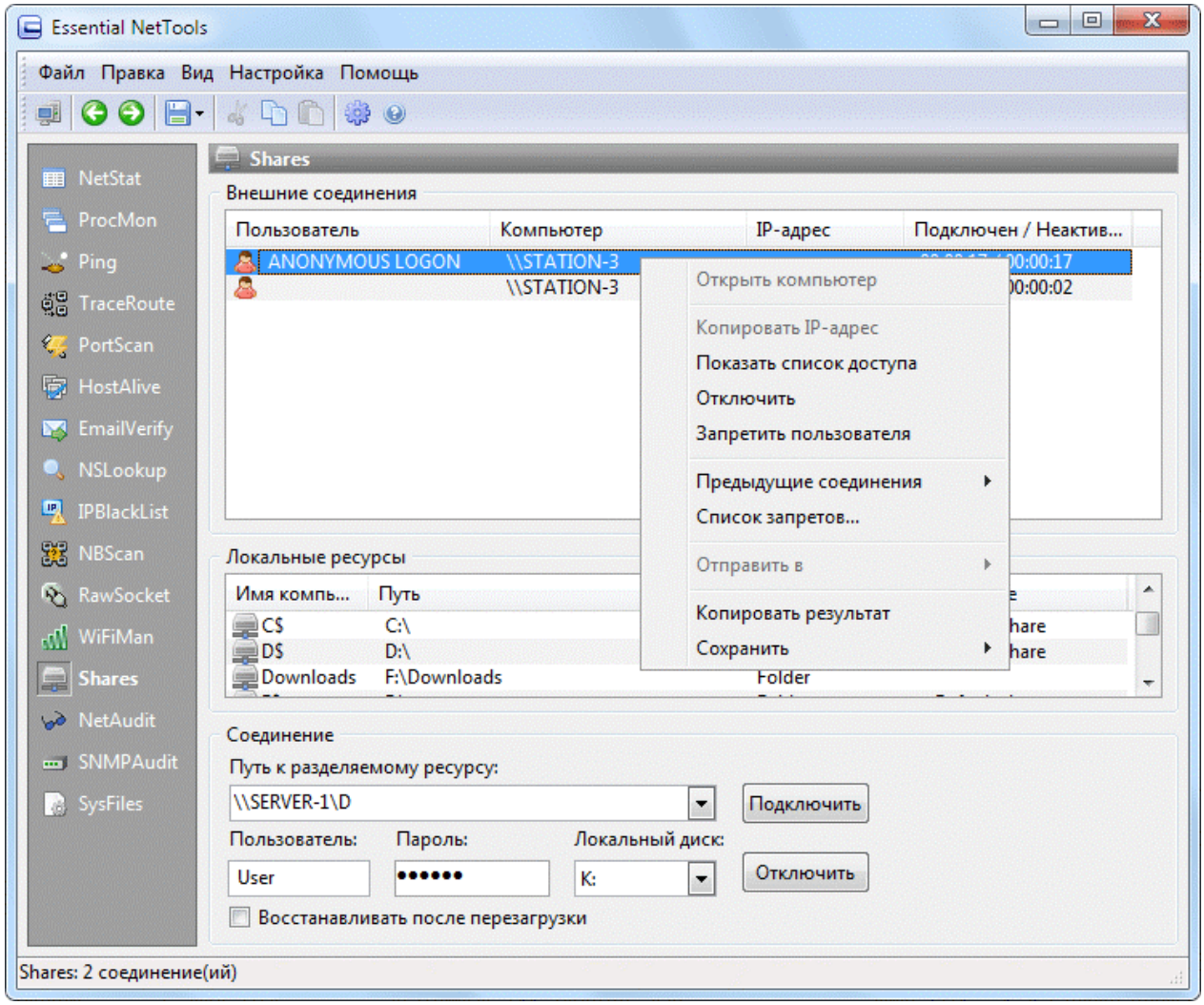
В группе **Предпочитаемые сети (Профили)** показан список настроенных профилей для подключения к беспроводным сетям. Здесь вы можете отредактировать профиль, добавить новый или удалить существующий, а так же экспортировать или импортировать профили в формате XML, что позволяет легко переносить настройки с компьютера на компьютер или распространять их среди группы пользователей. Вам доступны следующие команды:

- **Управление** – открывает стандартный диалог системы для управления беспроводными сетями. Данная опция доступна начиная с Windows Vista, в Windows XP опция недоступна.
- **Добавить из XML** – добавляет профиль сети из XML файла.
- **Сохранить в XML** – сохраняет профиль сети в XML файл.
- **Показать как XML** – открывает диалог показа профиля выбранной сети в формате XML.
- **Свойства** – показывает диалог настройки выбранного профиля сети. В этом диалоге вы можете настроить различные параметры сети, такие как аутентификация, шифрование и автоматическое подключение к сети при ее доступности.
- **Добавить** – открывает диалог добавления нового профиля сети и позволяет настроить параметры подключения.
- **Удалить** – удаляет выбранный профиль из списка предпочитаемых сетей.

Справа от списка профилей расположены кнопки **Вверх** и **Вниз**, используя которые, вы можете менять порядок следования профилей в списке. По двойному клику в списке доступных сетей будет показано диалоговое окно редактирования свойств выбранного профиля.

Shares

Модуль **Shares** выполняет три функции: наблюдает за подключениями к вашим ресурсам, показывает локальные открытые ресурсы и подключается к удаленным ресурсам в сети.



Внешние соединения

Когда программа обнаруживает внешнее подключение к вашему компьютеру, она отображает информацию о пользователе (как показано выше). Программа сообщает о новом подключении звуковым сигналом или мигающей красной иконкой.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Открыть компьютер** – попытаться открыть выбранный компьютер. Если компьютер доступен, откроется новое окно Проводника Windows с ресурсами удаленного компьютера. Для этого вам потребуется установленный Client for Microsoft Networks.
- **Копировать IP-адрес** – копировать IP-адрес выбранного компьютера в буфер обмена.
- **Показать список доступа** – открыть окно со списком локальных файлов, к которым имеет доступ выбранный пользователь.
- **Отключить** – отключить выбранный компьютер.

- **Запретить пользователя** – добавить компьютер с выбранным именем в список запретов. Когда пользователь из этого списка попытается подключиться к вашему компьютеру, он будет автоматически отключен.
- **Предыдущие соединения** – показать отчеты о предыдущих соединениях. Здесь же можно их удалить.
- **Список запретов** – редактировать список запретов.
- **Отправить в** – передать выбранный IP-адрес в другие модули или в SmartWhois.
- **Копировать результат** – копировать таблицу соединений в буфер обмена.
- **Сохранить** – сохранить таблицу соединений в файл.

Важно: отключение или запрет пользователя не являются достаточными мерами безопасности. Отключая пользователя, вы даете указание операционной системе прервать текущее соединение, но этот пользователь может снова сделать попытку подключения через несколько секунд. Отключение лишь замедлит этот процесс. Если вы заметили несанкционированное подключение, советуем установить пароли на разделяемые ресурсы.

Локальные ресурсы

В этой области показаны локальные разделяемые ресурсы вашего компьютера.

Соединения

Данный модуль можно использовать для подключения к удаленным ресурсам сети. Для отображения удаленных ресурсов на ваш локальный жесткий диск введите правильный путь в поле **Путь к разделяемому ресурсу**. Правильным считается путь, который начинается с двух обратных слэшей ("\\"), после которых должно идти имя компьютера, затем еще один обратный слэш, а потом имя ресурса. Например, чтобы отобразить папку "COMMON" на компьютер "STATION1", введите следующую строку:

\\STATION1\COMMON

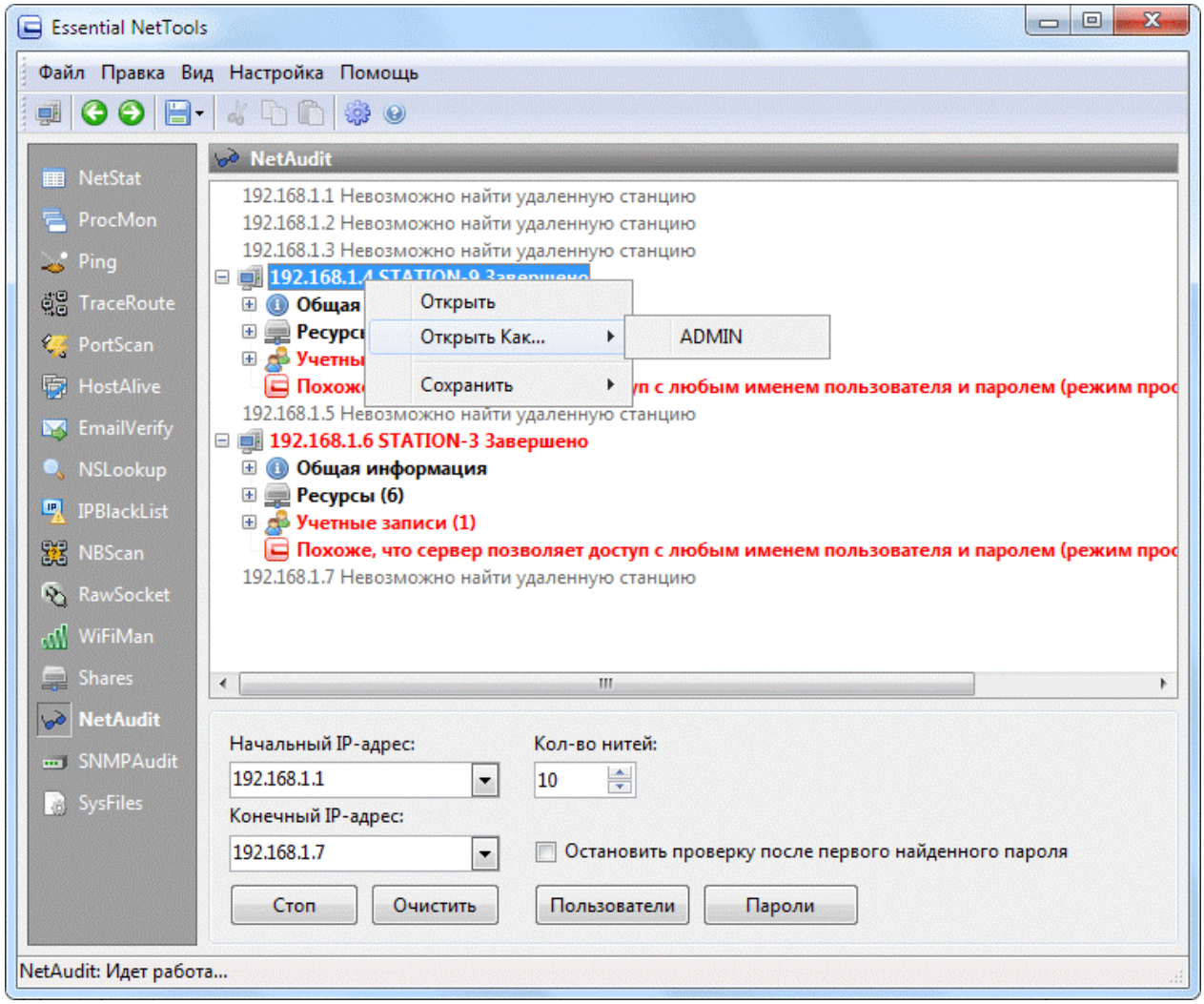
Вам также следует ввести в соответствующие поля имя пользователя и пароль и выбрать свободную букву из выпадающего списка **Локальный диск**. Учтите, что ваш компьютер должен быть способен преобразовывать имя удаленного компьютера в соответствующий IP-адрес. Обычно это означает, что пара IP-адрес/Имя компьютера должны всегда присутствовать в вашем файле lmhosts. Эту пару можно добавить через модуль SysFiles.

Чтобы отобразить разделяемый ресурс на локальный диск, нажмите **Подключить**. Если вы хотите, чтобы при повторной загрузке компьютер восстанавливал подключения к разделяемым ресурсам, установите флаг Восстанавливать после перезагрузки. Для отмены отображения нажмите Отключить. Учтите, что по команде Отключить программа попытается отключить диск, указанный в поле Локальный диск, так что если вы подключались ко многим ресурсам, вам следует выбрать соответствующую букву.

NetAudit

NetAudit (программа аудита NetBIOS) – это модуль для проверки сетей или отдельных компьютеров, на которых работает сервис NetBIOS File Sharing.

Несмотря на то, что существует масса мощных и дорогостоящих решений для нахождения уязвимостей в сети, большинство проблем безопасности берут свое начало от неверной настройки разделяемых ресурсов NetBIOS. С помощью данного модуля вы сможете легко и быстро проверить вашу сеть и/или отдельные компьютеры. Помните, что для такой проверки вы должны обладать административными правами.



Перед началом проверки введите начальный и конечный IP-адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес**. Помните, что три первые группы в начальном и конечном IP-адресах должны быть одинаковы. Имена пользователей и пароли можно настроить, нажав на кнопки **Пользователи** и **Пароли** соответственно. Эти списки служат для проверки возможности потенциального вторжения и вы можете их настроить на основании таблицы имен, полученных в модуле NBScan. Нулевой пароль всегда автоматически добавляется как первый пароль списка, поскольку его нельзя ввести, но такой пароль зачастую используется. Все введенные пароли будут опробованы для всех имен пользователей.

Количество одновременно проверяемых адресов можно изменить в поле **Кол-во нитей**. Вы также можете **Остановить проверку после первого найденного пароля** для любого хоста. Такая остановка

позволит прекратить поиск других паролей и программа незамедлительно перейдет к другим IP-адресам.

Чтобы начать проверку, нажмите **Старт**. Процесс можно прервать в любой момент, нажав **Стоп**. Помните, что проверка компьютера – это длительный процесс и зависит от множества факторов, так что будьте готовы к длительному ожиданию, особенно если вы задали большой диапазон IP-адресов. При обнаружении модулем NetAudit какой-либо уязвимости в безопасности, вы услышите звук и увидите мигающую иконку.

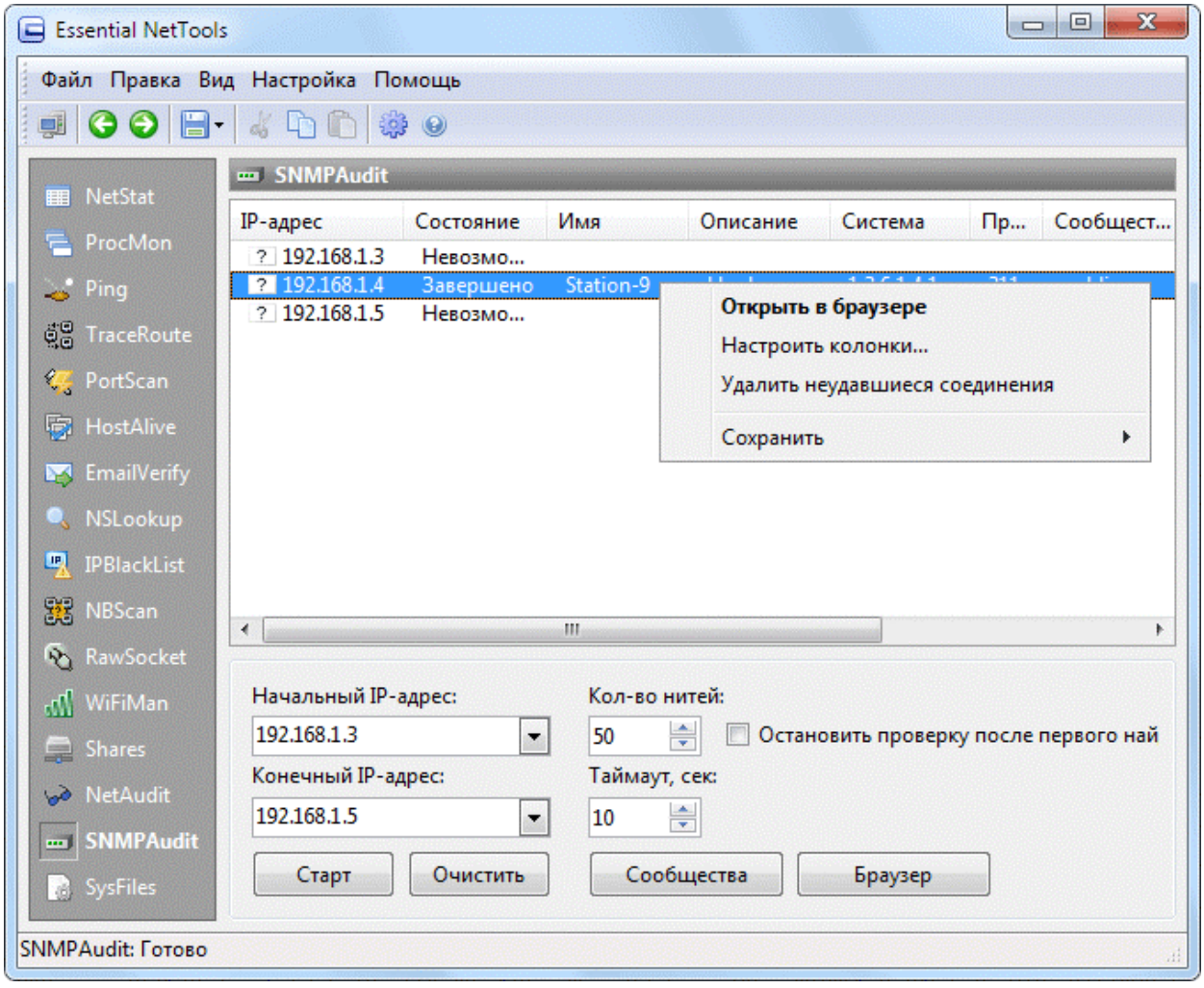
Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Копировать** – копировать выделенный текст в буфер обмена.
- **Выделить все** – выделить весь текст в окне.
- **Сохранить как** – сохранить отчет в файл.

SNMPAudit

SNMPAudit – это модуль для быстрого обнаружения SNMP-устройств и получения по ним выбранной информации. Этот модуль можно использовать для опроса устройств, которые находятся в заданном диапазоне адресов. Протокол SNMP используется для работы с различными сетевыми устройствами, такими как серверы, маршрутизаторы, коммутаторы и т. д. От SNMP-устройства можно получить много полезной информации о состоянии устройства и его характеристиках производительности.

Для обозначения класса SNMP-устройства по его функциональности и назначению в протоколе SNMP используется термин "Сообщества". SNMP-устройство может быть настроено на принадлежность к нескольким сообществам. Во время подключения в SNMP-устройству консоль (например, Essential NetTools) отображает название сообщества, к которому адресован запрос. Важно знать сообщество, к которому принадлежит устройство. Если сообщество указано неверно, то устройство просто проигнорирует запрос. Поэтому название сообщества используется для идентификации как своего рода пароль, который необходим для доступа и получения информации от SNMP-устройства.

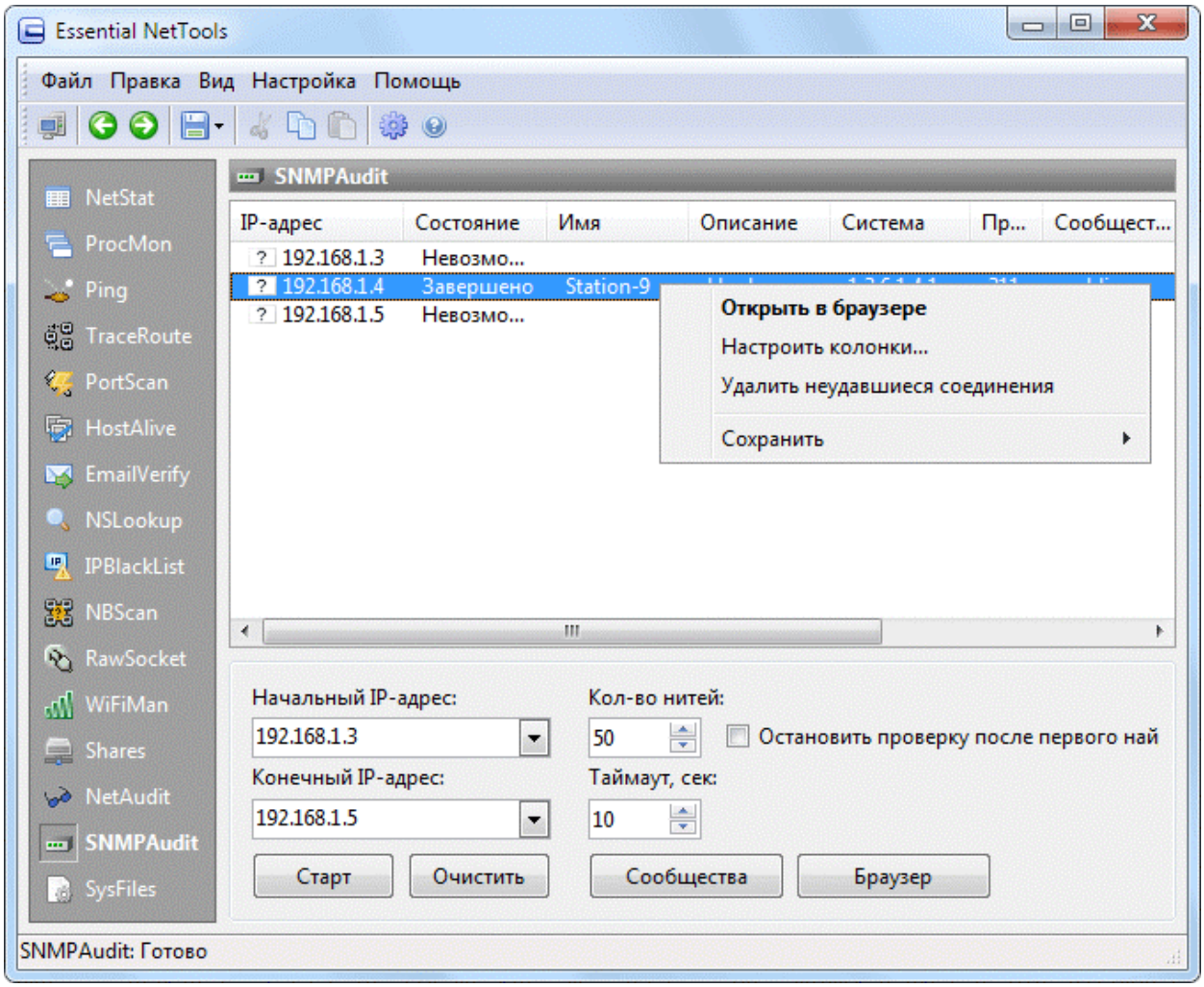


Наиболее часто используется имя Public. Кликнув по кнопке **Сообщества**, вы можете добавить свое сообщество в список опрашиваемых. Помните, что **SNMPAudit** всегда проверяет наличие сообщества Public, даже если его нет в списке сообществ. Для каждого адреса из заданного диапазона программа опробует каждое сообщество из списка. Если вас устраивает обнаруженное для данного хоста сообщество, установите флаг **Остановить проверку после первого найденного сообщества.** В этом случае модуль остановится после первого найденного сообщества и не будет проверять остальные

сообщества из списка. После этого программа продолжит опрос других IP-адресов из указанного диапазона.

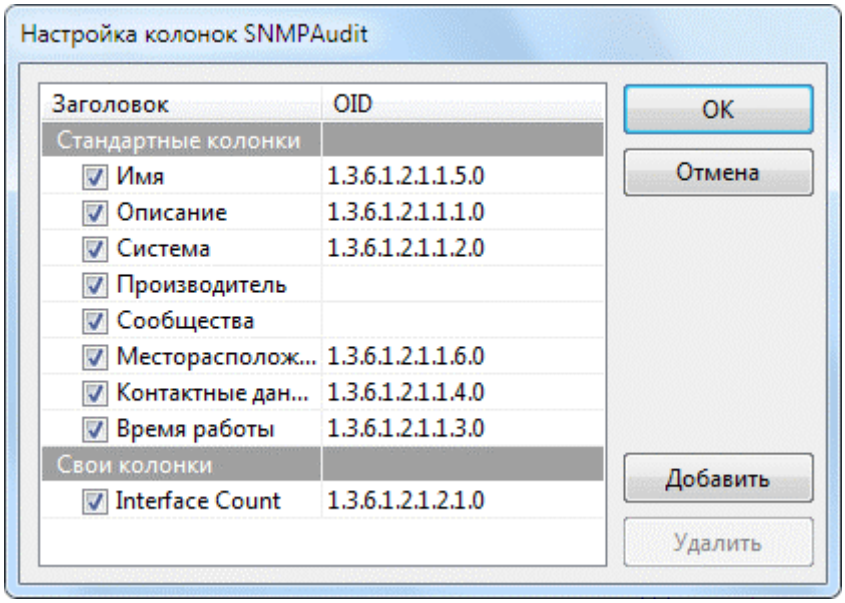
Перед началом проверки введите начальный и конечный IP-адреса в поля **Начальный IP-адрес** и **Конечный IP-адрес**. Количество одновременно проверяемых адресов можно изменить в поле **Кол-во нитей**, а таймаут соединения – в поле **Таймаут, сек**. Для начала сканирования нажмите **Старт**. IP-адреса и состояние опрошенных хостов будут появляться в главном окне модуля в процессе сканирования. Если хост не является SNMP-устройством, то в колонке **Состояние** вы увидите одно из двух сообщений: **Невозможно найти удаленную станцию** или **Удаленная сторона разорвала соединение** (при необходимости, можно очистить список от неудавшихся соединений, выбрав команду контекстного меню **Удалить неудавшиеся соединения**).

Для прекращения сканирования нажмите **Стоп**. Для очистки списка в главном окне модуля нажмите **Очистить**; однако ваши настройки, включая начальный и конечный IP-адреса, количество одновременных подключений и таймаут будут сохранены.

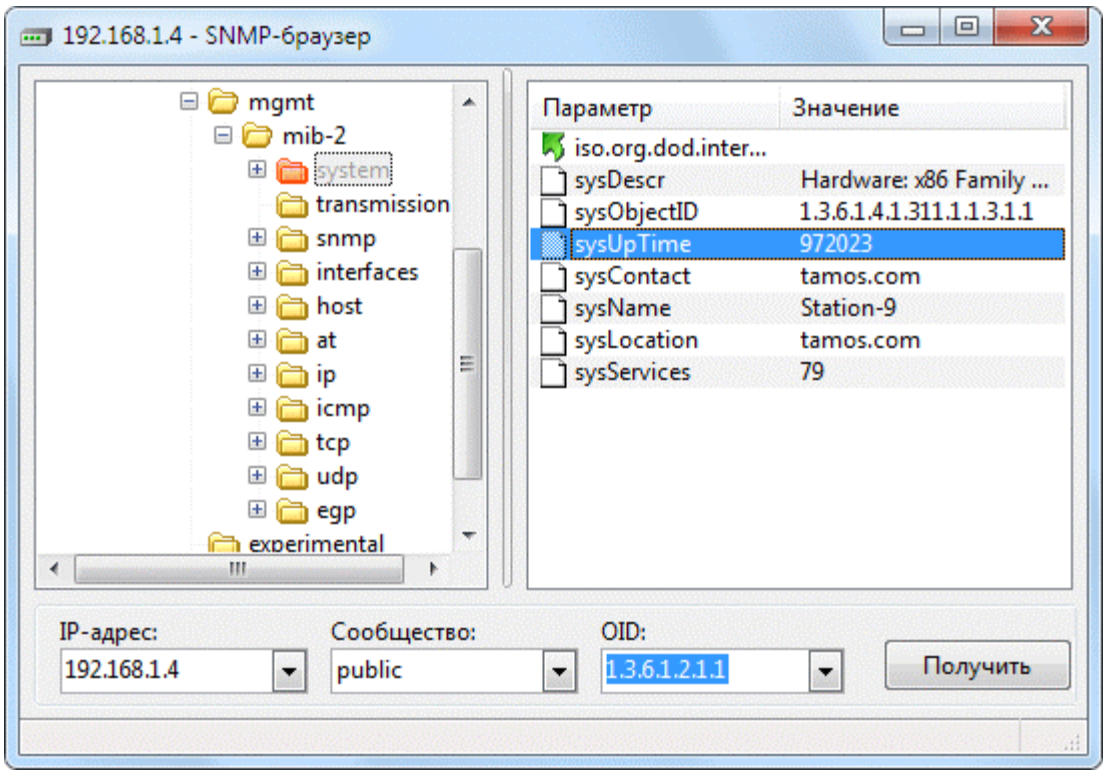


После обнаружения устройства, принадлежащего сообществу из списка **SNMPAudit** делает запрос на получение базовой информации об устройства и отображает полученный результат в список. Можно выбрать колонки, которые будут показаны в главном окне модуля: **Имя**, **Описание**, **Система**, **Производитель**, **Сообщества**, **Месторасположение**, **Контактные данные** и **Время работы**. Для этого кликните правой кнопкой мыши на окне модуля.

Вы не можете изменять установки **Стандартных колонок** или удалять их. При добавлении своих колонок вы должны указать правильный путь к SNMP-информации в колонке OID. Вы можете обратиться к выпадающему списку или найти OID в соответствующей базе данных MIB. Если вы хотите удалить колонку, нажмите **Удалить**.



Если вы хотите исследовать какое-либо SNMP-устройство из списка опрошенных устройств, дважды кликните или выберите его, а затем выберите опцию **Открыть в браузере**.



В **SNMP-браузере** вы можете просмотреть всю доступную информацию о данном сообществе, полученную от SNMP-устройства. Если в базе данных MIB существует нужное описание, то вы всегда сможете прочитать описание для полученных данных.

Введите в окне SNMP-браузера IP-адрес устройства, сообщество и начальный OID. Нажмите **Получить** или просто клавишу **Enter**. Программа извлечет все уровни данных, лежащие ниже указанного OID.

Полученная структура данных отобразится в левой панели. Если вы не уверены, с какого OID следует начать, выберите начальное значение из дерева слева. В этом случае в поле **OID** будет занесен полный путь к выбранному элементу дерева. Обычно вся информация относится к ветвям **iso.org** или **1.3** – для получения всей доступной информации о устройстве выберите OID **1** или **1.3.**

Реальные данные, полученные от устройства будут показаны на панели справа. Поля данных будут показаны на панели слева.

По умолчанию в правой панели будет показаны только данные о выбранном элементе (стиль Проводника Windows). Если вы хотите отображать всю информацию из последующих слоев, кликните по списку правой кнопкой мыши и в меню выберите **Показать все значения**.

Вы можете открыть столько окон SNMP-браузера, сколько хотите.

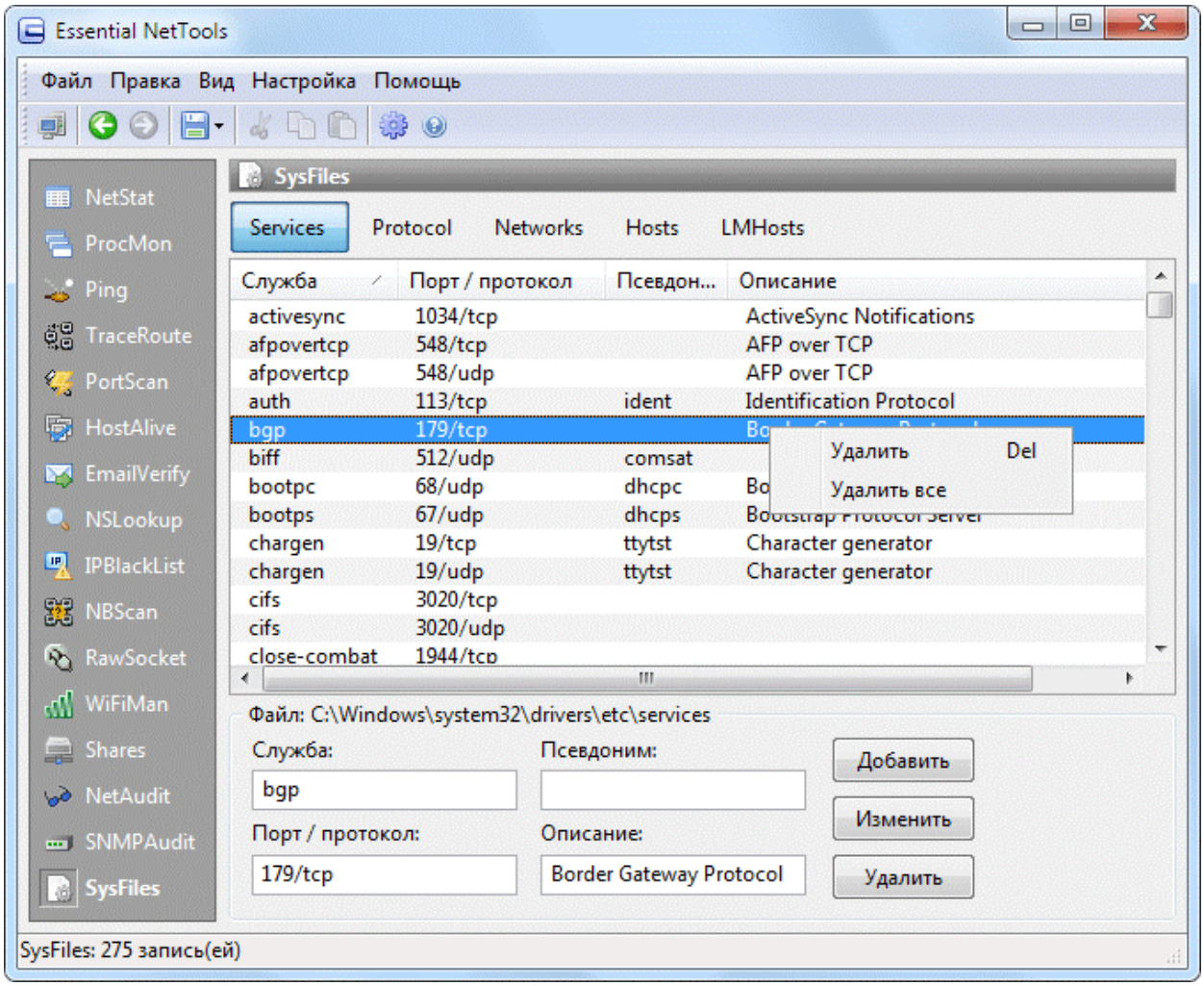
Базы данных MIB

При первом запуске браузера программа загрузит базы данных MIB из каталога (по умолчанию C:\Program Files\EssNetTools\SNMP\MIB) и покажет их в древовидной форме. Базы данных MIB содержат пути к различным данным SNMP-устройств (OID), а также описание этих данных. Вы можете получить описание элемента (если оно есть), подведя курсор мыши к соответствующему элементу. Описание будет показано в отдельном окне.

Базы данных MIB могут быть общими либо разными для отдельного производителя, модели или класса устройств. В дистрибутив Essential NetTools включен базовый набор MIB, достаточный для большинства устройств. Вы всегда можете скачать базы с сайта http://www.mibdepot.com/. Запишите их в каталог программы (по умолчанию C:\Program Files\EssNetTools\SNMP\MIB) и перезапустите программу. Помните, что даже если у вас нет необходимой базы MIB для вашего устройства, вы все равно можете получать данные об этом устройстве без всяких ограничений. В базах данных MIB содержатся только описания полученной информации и ее назначение.

SysFiles

Этот модуль можно использовать для редактирования пяти системных файлов: services, protocol, networks, hosts и lmhosts. При запуске программы этот модуль считывает записи из этих файлов как показано ниже:



Этот модуль предназначен в первую очередь для профессионалов, так что не редактируйте эти файлы, если точно не уверены что вы делаете.

Кликнув правой кнопкой мыши по окну модуля, вы увидите контекстное меню со следующими командами:

- **Удалить –** удалить выбранную запись (записи).
- **Удалить все** – удалить все записи.

Установки

Для задания установок программы перейдите в меню **Настройка** => **Установки**.

Инструменты

NetStat

- **Отображать полный путь процесса** – показывать полный путь к процессу, которому в данным момент "принадлежит" порт. (Например, "C:\Files\Program.exe" – полный путь, а "Program.exe" – короткий).
- **Конвертировать имена портов в имена сервисов** – показать в NetStat имена сервисов вместо цифр. Например, если эта опция установлена, порт 21 показан как ftp, а порт 23 как telnet. Программа преобразует численные значения в имена сервисов, используя файл SERVICES, установленный системой Windows. Этот файл можно редактировать в модуле SysFiles.
- **Отключить распознавание DNS** – не выполнять обратный DNS-поиск по IP-адресу. Если опция установлена, колонка Имя хоста в модуле NetStat будет пуста.

NBScan и PortScan

- **Исключать границы подсети** – пропускать IP-адресе, которые заканчиваются на .0 или .255.
- **Очищать список перед запуском –** очищать список NBScan или PortScan каждый раз перед сканированием нового диапазона IP-адресов. Если опция не установлена, программа будет хранить результаты всех предыдущих сканирований и будет автоматически сортировать новые записи по IP-адресам.

Интервал автообновления

Установить интервал автоообновления для модулей NetStat и ProcMon, если установлен режим автообновления. Для модуля ProcMon также можно указать интервал автообновления для сбора статистики по загрузке процессора.

Интерфейс

Звуковые сигналы

Обнаружение уязвимости в NetAudit, **Обнаружение внешнего соединения** – сопровождать некоторые события звуковыми сигналами. Чтобы изменить стандартные звуковые файлы, нажмите кнопку Обзор и выберите новый звуковой файл в формате .WAV. Чтобы проверить звуковой файл, нажмите на кнопку с изображением динамика.

Визуальные эффекты

- **Двухцв. раскраска** – показывать текст двумя цветами. Для настройки цветов выберите **Цвет 1** и **Цвет 2**.
- **Цвет новых соединений в NetStat** – настроить цвет для временной подсветки новых записей в окне модуля NetStat.
- **Цвет закрытых соединений в NetStat** – настроить цвет для подсветки записей, которые подготовлены для удаления в окне модуля NetStat.
- **Подсв. пунктов при движении мыши** – если опция установлена, то при движении мыши по элементам списка эти элементы будут подсвечены, и вы сможете их выбрать, остановив мышь.

- **Плоские полосы прокрутки** – сделать все полосы прокрутки плоскими (недоступно для Windows XP/Vista).

Геолокация

Геолокация – это определение страны по IP-адресу. Если опция включена, Essential NetTools извлечет из внутренней базы данных информацию о том, к какой стране принадлежит IP-адрес. Рядом с каждым IP-адресом вы можете показывать **ISO-код страны**, **Название страны** или **Флаг страны**. Вы также можете отключить геолокацию. Для некоторых IP-адресов (например, зарезервированных вида 192.168.*.* или 10.*.*.*) информация о стране предоставлена не будет. В этом случае имя страны показано не будет, а если вы установили опцию **Показывать флаг страны**, будет показан флаг со знаком вопроса.

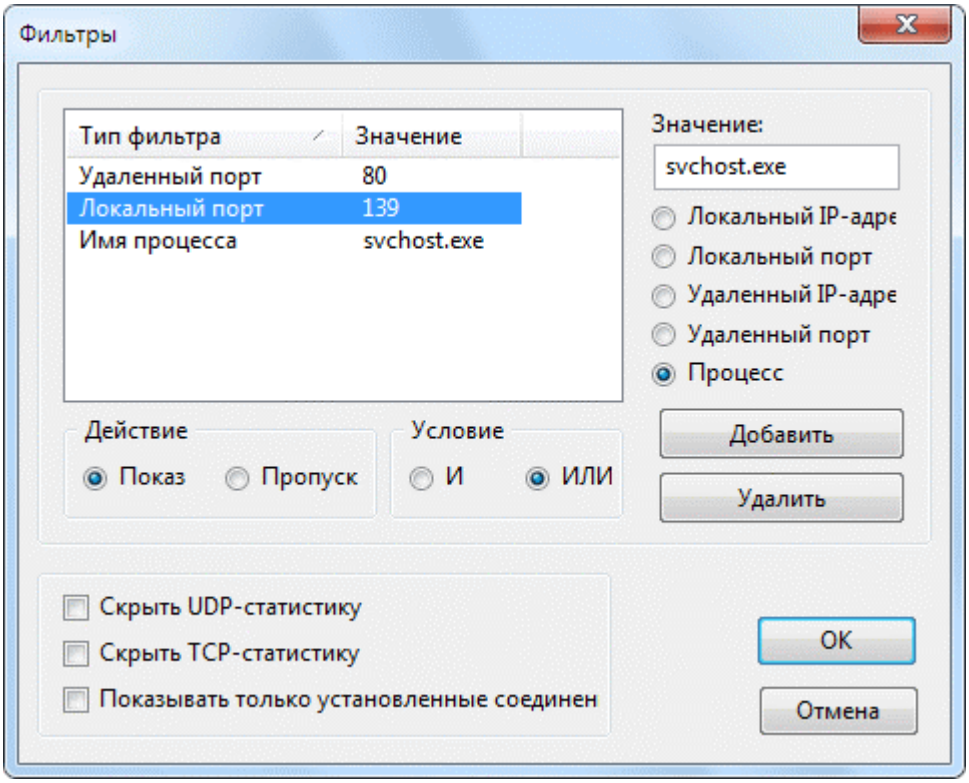
Поскольку местонахождение IP-адресов постоянно меняется, важно, чтобы у вас всегда была последняя версия Essential NetTools. Обновления базы данных включаются в каждую сборку Essential NetTools. Последняя версия базы данных имеет точность порядка 98%. Без обновлений показатель точности падает примерно на 15% каждый год.

Дополнительно

- **Автозагрузка с Windows** – автоматический запуск программы вместе с Windows.
- **Сворачивать окно в системный лоток при закрытии** – если опция установлена, то программа не закроется при нажатии на "x" в правом верхнем углу окна. Чтобы закрыть программу, выберите в меню Файл => Выход.
- **Скрывать из панели задач при свертывании** – установите эту опцию, если вы не хотите видеть кнопку программы в панели задач Windows, когда вы минимизируете саму программу. Если опция установлена, то для открытия программы после ее минимизации используйте иконку в трее.
- **Перемещать фокус на поле ввода при переключении** – автоматически устанавливать фокус ввода на области ввода при переключении с одного модуля на другой, например, на области IP-адресов.
- **Автозаполнение полей ввода IP-адресов** – если опция установлена, программа автоматически заполнит поле **Конечный IP-адрес** в модулях NBScan, PortScan и NetAudit в том случае, если вы заполнили поле **Начальный IP-адрес**.
- **Изменить заполнение для ping/traceroute** – изменить строку, которая содержится по умолчанию в пакетах ping и traceroute. Установите метку и введите ваше сообщение в поле ниже.
- **Разрешить автоматическое обновление** – если опция установлена, программа проверит наличие обновления для текущей версии и, если оно есть, предложит вам его скачать и установить.
- **Периодичность проверки, дней –** указать, как часто проверять наличие обновлений.
- **Проверить сейчас** – проверить наличие обновлений немедленно.

Фильтры

В данном диалоге можно настроить фильтры для отображения информации в окне модуля NetStat. По умолчанию в NetStat перечислены все соединения вашего компьютера. Обычно этот список очень длинный, и, возможно, вы захотите отфильтровать какие-то записи, которые не представляют интереса.



Чтобы создать новый фильтр, введите **Значение**, укажите тип фильтра (**Локальный IP-адрес**, **Локальный порт** и т. д.) и нажмите **Добавить**. Чтобы удалить фильтр, выберите его в списке и нажмите **Удалить**. После того, как вы создали один или несколько фильтров, выберите **Действие**. Если вы выберите **Показ**, NetStat отобразит только те соединения, которые удовлетворяют условиям фильтрации. Если вы выберите **Пропуск**, NetStat не покажет те соединения, которые удовлетворяют условиям фильтрации. Если вы создали много фильтров, то ими можно управлять с помощью булевых **Условий**: **И** (Фильтр 1 И Фильтр 2 И Фильтр 3, и т. д.) или **ИЛИ** (Фильтр 1 ИЛИ Фильтр 2 ИЛИ Фильтр 3, и т. д.). На скриншоте сверху показан набор правил, который дает указание модулю NetStat скрывать те соединения, у которых локальный порт 3128, удаленный порт 89 или же имя процесса *svchost.exe*.

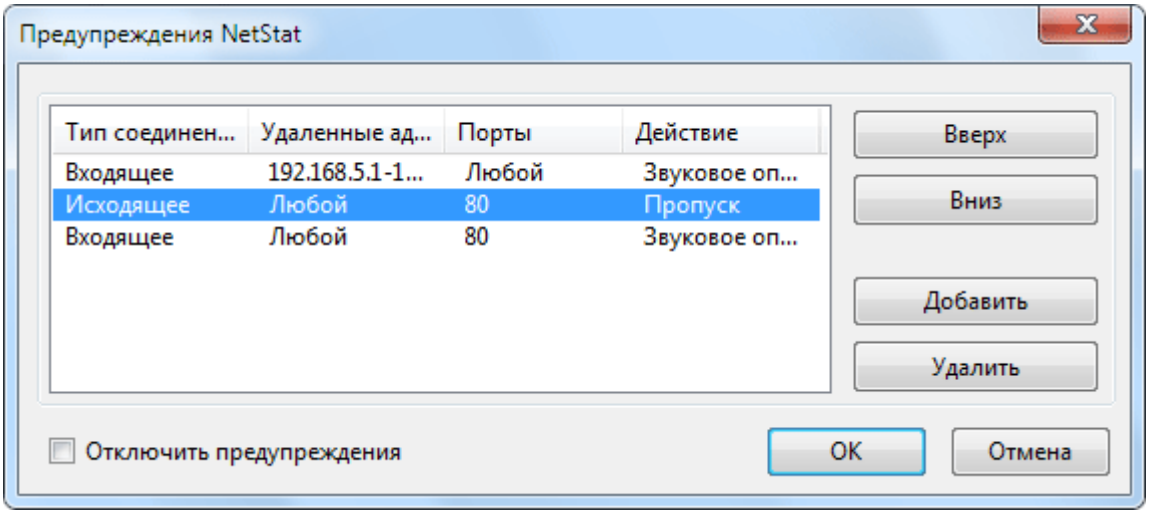
Вы также можете использовать эти базовые фильтры:

- **Скрыть UDP-статистику** – не показывать UDP-соединения в окне модуля NetStat.
- **Скрыть TCP-статистику** - не показывать TCP-соединения в окне модуля NetStat.
- **Показывать только установленные соединения** – все другие соединения, кроме установленных, перечислены не будут.

Фильтры можно временно отключить в контекстном меню NetStat – опция **Отключить фильтры**.

Предупреждения

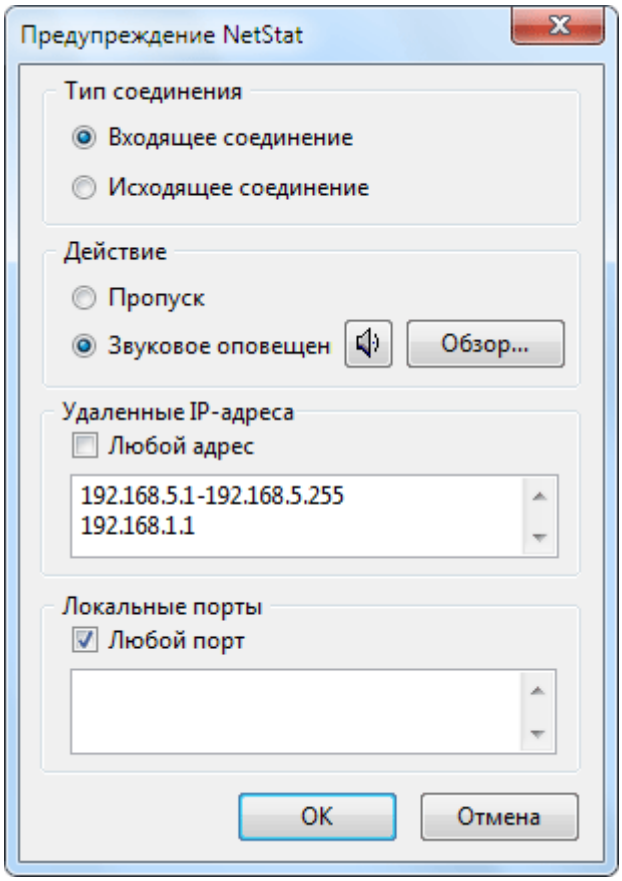
В данном диалоге можно настроить список предупреждений о различных входящих и исходящих соединениях.



Доступны следующие виды предупреждений:

- Входящее соединение с указанного IP-адреса или диапазона IP-адресов.
- Входящее соединение с указанного локального порта или диапазона локальных портов.
- Исходящее соединение на указанный IP-адрес или диапазон IP-адресов.
- Исходящее соединение на указанный удаленный порт или диапазон удаленных портов.

Чтобы создать новое предупреждение, нажмите **Добавить**.



Тип соединения – выберите тип соединения: входящее или исходящее.

Действие – выберите действие, которое будет выполнено при срабатывании предупреждения: **Звуковое оповещение** – проиграть звуковой файл. При выбранной опции **Пропуск** программа исключит этот вид соединения из списка предупреждений. Например, если вы хотите наблюдать все входящие соединения кроме тех, что идут с порта 80, укажите тип соединения – Входящий и локальный порт 80, затем выберите действие **Пропуск**. Учтите, что функция предупреждения ищет первое совпадение с критерием предупреждения, поэтому исключенное предупреждение должно быть первым в списке предупреждений, иначе оно не будет считано программой и все соединения с порта 80 вызовут срабатывание предупреждения.

Удаленные IP-адреса – несколько IP-адресов или диапазон адресов, соединение с которых вызовет срабатывание предупреждения. Если установлена опция **Любой адрес**, то срабатывание вызовет соединение с любого адреса.

Локальные порты – несколько локальных или удаленных портов, соединение с которых вызовет срабатывание предупреждения. Если установлена опция **Любой порт**, то срабатывание вызовет соединение с любого порта.

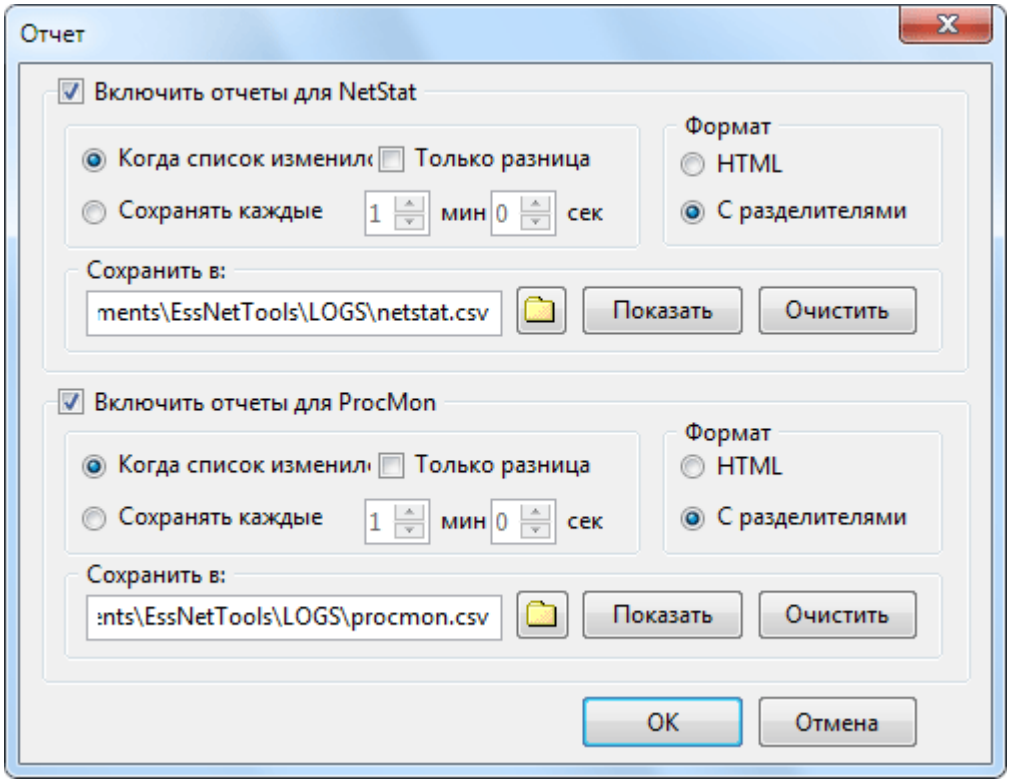
После того, как предупреждение создано, вы всегда сможете его отредактировать, дважды кликнув по нему в списке предупреждений. Используя кнопки **Вверх** и **Вниз**, вы можете изменить порядок, в котором предупреждения считываются программой.

Предупреждения считываются в убывающем порядке. Поиск останавливается при первом совпадении; все остальные предупреждения уже не учитываются.

Чтобы временно приостановить все предупреждения, выберите команду **Отключить предупреждения**.

Отчеты

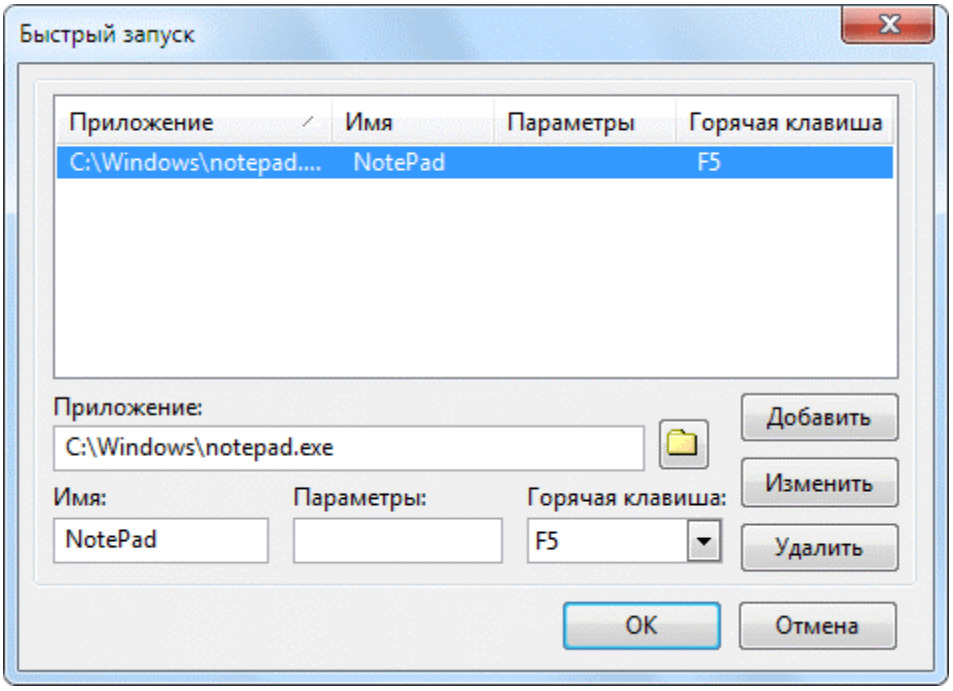
В этом диалоге можно включить и настроить систему отчетов для модулей NetStat и ProcMon.



Вы можете сохранять списки из модулей NetStat или ProcMon **Когда список изменился** или периодически, выбрав опцию **Сохранять каждые** и указав интервал. Если вы хотите минимизировать размер отчетов, выберите опцию **Только разница**. Таким образом вы дадите программе указание сохранять только те записи, которые были добавлены или удалены с момента последнего изменения списка. Вы также можете выбрать формат отчета, **HTML** или **С разделителями** и указать имя файла и путь, куда требуется сохранить отчет.

Быстрый запуск

В этом диалоге можно добавить программы для быстрого запуска в меню **Файл** => **Быстрый запуск**. Добавляя различные программы в меню, вы можете использовать данную программу как удобный инструмент для быстрого запуска.



Чтобы добавить программу, введите путь к исполняемому файлу в поле **Приложение** и произвольное название в поле **Имя**. Значение из поля **Имя** будет использовано в меню **Файл** => **Быстрый запуск**. Вы можете ввести **Параметры**, которые будут передаваться исполняемому файлу программы, а также назначить программе **Горячую клавишу**. После окончания ввода этой информации нажмите **Добавить**. В меню **Файл** => **Быстрый запуск** появится новая запись.

Поле **Приложение** необязательно должно содержать имя файла. Вы можете ввести путь не к исполняемому файлу, если данный файл уже связан с какой-то программой, например, файл MS Word. Интернет-адреса вроде http://www.yahoo.com также приемлемы (откроется ваш Интернет-браузер и будет загружен веб-сайт Yahoo).

Обзор системы

В этом диалоге представлена очень подробная информация о вашем компьютере, например, информация о процессоре, установленных программах, используемой памяти и т. д. Чтобы сохранить отчет в XML-формате, нажмите **Отчет**. Поскольку смысл практически всех элементов данного окна может утратиться при их переводе с английского, поэтому мы оставили всю информацию только на английском.

Справка

Таблица NetBIOS

Ниже вы найдете описание некоторых имен NetBIOS, которые используются на машинах с Windows.

Имя	Суффикс (16-р.)	Тип	Описание
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<..._MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCP/IP Service
<computername>	52	U	DEC Pathworks TCP/IP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser

<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	Internet Information Server
<IS~computername>	00	U	Internet Information Server

Часто задаваемые вопросы

В этой главе вы найдете ответы на наиболее часто встречающиеся вопросы. Свежий FAQ всегда доступен по адресу: http://www.tamos.ru/products/nettools/faq.php.

В. Мой брандмауэр, когда я пользуюсь Essential NetTools, сообщает, что программа "пытается получить доступ в Интернет". Я знаю, что некоторые фирмы могут отслеживать действия пользователей, собирая информацию, посылаемую их программами на сайт фирмы через Интернет. Зачем Essential NetTools пытается получить доступ в сеть?

О. Брандмауэр (firewall) реагирует на попытки преобразовать IP-адрес в имя хоста, что необходимо для отображения имен хостов в утилите NetStat. Так как Essential NetTools должен послать DNS-запрос на DNS-сервер, срабатывает тревога. Можно выключить данный сервис (Настройка => Установки => Отключить распознавание DNS), но в этом случае в таблице NetStat не будут показаны имена хостов.

В. Я пытаюсь заставить NBScan просканировать мой адрес IP, но я не вижу таблицу имен моего компьютера.

О. Скорее всего, это означает, что на вашем компьютере не запущен сервис разделяемых ресурсов, или на нем установлен Winsock версии 1, который распространялся с Windows 95. В последнем случае используйте команду nbtstat -A xxx.xxx.xxx.xxx или обновите вашу версию Winsock до версии 2. Это ограничение не касается ни просмотра таблиц имен других компьютеров (Winsock 1 работает так же хорошо, как и Winsock 2), ни NetAudit (вы можете проверять им свой компьютер).

В. Я проверяю адрес xxx.xxx.xxx.xxx при помощи NBScan и не получаю результатов, однако nbtstat показывает таблицу имен.

О. Возможны две причины. Либо у вас установлено слишком короткое время ожидания ответа на запрос и ваш компьютер не успевает его вовремя получить, либо вы не используете Advanced Mode (расширенный режим). В этом режиме программа отображает 100% компьютеров, которые в принципе может показать nbtstat. Пожалуйста, прочитайте раздел Advanced Mode в главе NBScan.

В. Я проверяю адрес xxx.xxx.xxx.xxx с помощью NBScan и NBStat, однако не получаю результатов. Человек, компьютеру которого принадлежит этот адрес, проверяет этот же адрес (свой собственный) и видит таблицу имен своего компьютера. Почему он видит ее, а я нет?

О. Между вашими компьютерами находится брандмауэр (firewall) или другое устройство, фильтрующее пакеты. Некоторые пакеты могут блокироваться из-за настроек брандмауэра. Кроме этого, некоторые Интернет-провайдеры фильтруют пакеты, не информируя своих клиентов. В этом случае вы сможете провести аудит сети, подключившись через другого Интернет- провайдера.

В. Когда я пробую подключить раздел, появляется сообщение об ошибке "The network is not present or not started", однако я подключен к сети!

О. Возможно, вы используете модемное подключение к сети (Dial-Up) и забыли выбрать опцию "Войти в сеть" в свойствах соединения.

В. Когда я пробую подключить раздел, появляется сообщение об ошибке "Shared Resource Not Found", однако уверен, что я правильно выбрал путь к удаленному разделу.

О. Убедитесь что имя компьютера прописано в файле lmhosts, и что оно уникально в этом файле. Одно и то же имя не может быть у двух или более компьютеров в файле lmhosts. Вы можете

проверить, "понимает" ли компьютер имя, набрав команду ping computername в командной строке. Если компьютер успешно пингуется, вы можете использовать Essential NetTools, чтобы присоединиться к нему.

В. Когда я выбираю команду Open Computer или пытаюсь подключить сетевой раздел, программа показывает курсор в виде песочных часов и в течение некоторого времени ничего не происходит.

О. Наберитесь терпения :-) Обычно на установление соединения требуется несколько секунд.

Контакты

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

http://www.tamos.ru/support/

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**) и другие важные подробности.