Тема: **Изучение функционального назначения прикладного программного обеспечения «НИРСОФТ».**

NirSoft – это уникальная коллекция маленьких и полезных программ, разработанные Nir Sofer'ом.

У данных программ специфическое предназначение – они извлекают информацию (с постоянных носителей, из сетевых потоков, реестра и т.д.) из компьютеров на Windows. С их помощью вы можете восстановить потерянные пароли, мониторить вашу сеть для просмотра и извлечения кукиз, кэша и другой информации, хранимой веб-браузерами, искать по файлам в вашей системе, мониторить изменения в файловой системе и в системном Реестре и многое другое.

Программы являются бесплатными, не требуют установки, не содержат каких-либо вредоносных или рекламных компонентов. У программ присутствует графический интерфейс, многие программы также поддерживают работу в командной строке. У всех программ имеется поддержка многих языков и практически для всех сделан перевод на русский язык. Во время своей работы программы ничего не записывают в реестр Windows, т.е. при использовании с USB носителя не оставляют следов своего присутствия.

Познакомившись с программами NirSoft вы сможете извлекать забытые пароли и другую информацию, а также сможете оценить, что хранится на компьютере и что из него могут получить злоумышленники.

Программы регулярно обновляются, также постоянно добавляются новые инструменты.

В полном списке программы разделены на следующие разделы:

- восстановление паролей
- мониторинг сети
- извлечение информации из веб-браузеров
- работа с видео/аудио
- работа с Интернет
- утилиты командной строки
- настольные
- работа с Outlook/Office
- программерские инструменты
- дисковые утилиты
- системные утилиты
- прочие утилиты

Отдельные программы автор выделяет в разделы «Программное обеспечение для компьютерной криминалистики на Windows» и «Инструменты для работы с паролями», начнём знакомство с них.

Программное обеспечение для компьютерной криминалистики на Windows

InstalledPackagesView

InstalledPackagesView — это инструмент для Windows, который отображает список всех пакетов программного обеспечения, установленных в вашей системе с помощью установщика Windows, и перечисляет связанные с ними файлы, ключи реестра и сборки .NET. Для каждого установленного программного обеспечения отображается следующая информация: отображаемое имя, отображаемая версия, дата установки, время реестра, расчётный размер, место установки, источник установки, имя файла MSI (в C:\Windows\Installer) и многое другое…
Вы можете просматривать информацию об установленных пакетах программного обеспечения из вашей локальной системы или из другой системы на внешнем жёстком диске.
Информация об установленном программном обеспечении загружается из следующих ключей реестра:

- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Products*
- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Components*

Имейте в виду, что этот инструмент перечисляет только программное обеспечение, установленное установщиком Windows (MSI), он не перечисляет какое-либо программное обеспечение, установленное другими установщиками.

SpecialFoldersView

Этот инструмент показывает системные папки в Windows, которые обычно очень полезны в различных ситуациях. Вы можете просто дважды щелкнуть на папку в списке, чтобы открыть ее в Windows. Некоторые из папок включают данные приложения, историю Windows, административные инструменты, автозагрузку, меню «Пуск», временную папку, папку последних элементов и многое другое.

ExifDataView

ExifDataView — это небольшая утилита, которая считывает и отображает данные Exif, хранящиеся в файлах изображений .jpg, созданных цифровыми камерами. Данные EXIF включают название компании, создавшей камеру, модель камеры, дату и время, когда была сделана фотография, время экспозиции, скорость ISO, информацию GPS (для цифровых камер с GPS) и многое другое.

FullEventLogView

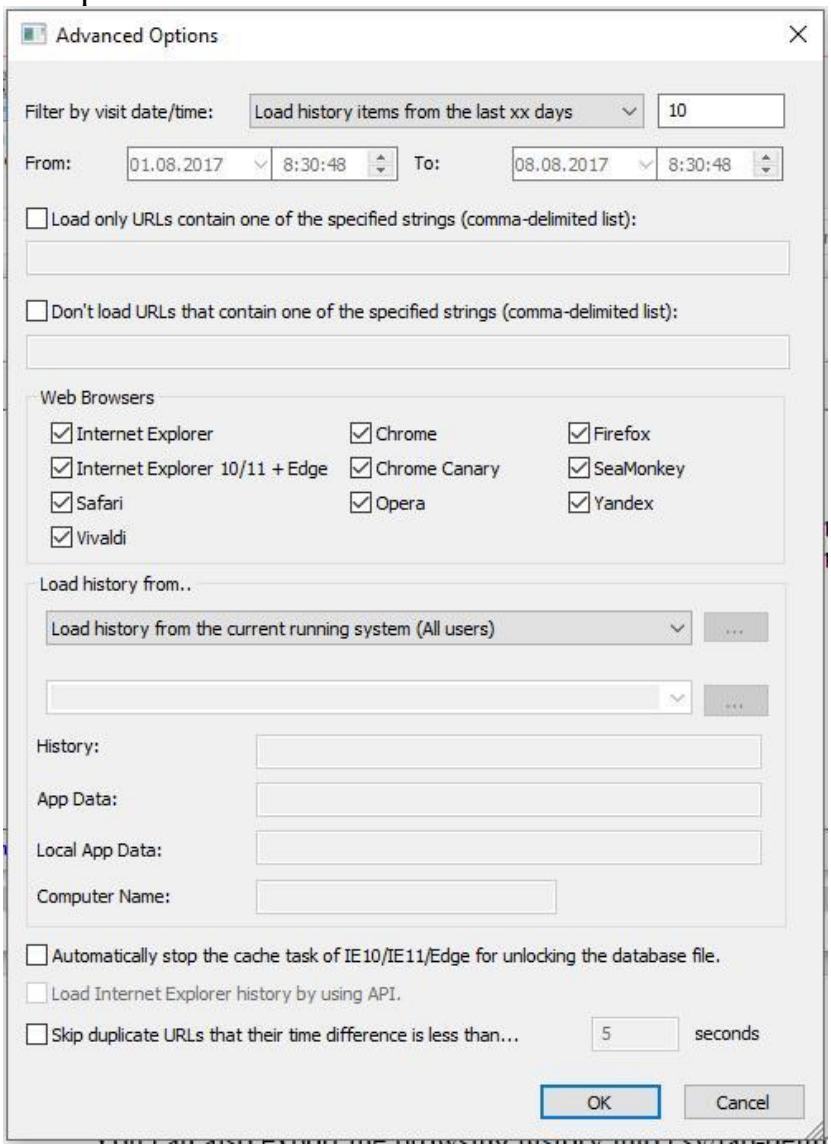
FullEventLogView — это простой инструмент для Windows 10/8/7/Vista, который отображает в таблице сведения обо всех событиях из журналов событий Windows, включая описание события. Он позволяет вам просматривать события

вашего локального компьютера, события удалённого компьютера в вашей сети, а также события, хранящиеся в файлах .evtx. Он также позволяет экспортировать список событий в файл форматы текст/csv/с TAB разделителями/html/xml из графического интерфейса пользователя и из командной строки.

BrowsingHistoryView

BrowsingHistoryView считывает и показывает информацию о посещённых сайтах для всех популярных браузеров. Кроме адреса посещённых страниц, показывается её имя, время посещения, счётчик визитов и прочее. Можно извлечь информацию из всех профилей пользователей системы, а также из внешнего диска. Присутствует возможность сохранения результатов.

Настройки:



MyLastSearch

MyLastSearch сканирует кэш и файлы историй вашего веб-браузера и определяет все пользовательские запросы, которые вы сделали в самых популярных поисковых системах (Google, Yahoo и MSN), на самых популярных сайтах социальных сетей (Twitter, Facebook, MySpace), а также на других популярных сайтах (YouTube, Wikipedia, Friendster, hi5).

К сожалению, программа не знает про google.ru (с google.com всё в порядке) и не знает про yandex.ru – т.е. поиски по этим сайтам она не видит.
UPD: Начиная с версии 1.65 добавлена поддержка для поисков в Yandex, DuckDuckGo и google.ru.

Программы для просмотра кэша браузеров (IECacheView, MozillaCacheView, ChromeCacheView, MZCacheView)

Работа программ IECacheView, MozillaCacheView, ChromeCacheView, MZCacheView напоминает работу **BrowsingHistoryView**, но просмотр кэша позволяет видеть каждый индивидуальный файл (скаченные ссылки, изображения и т.д.), а не только адреса посещённых страниц.

Программы для просмотра кукиз (ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView)

Как вы уже поняли, ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView используются для просмотра кукиз в различных веб-браузерах.

На самом деле, выделение раздела программ для IT криминалистики, на мой взгляд, довольно условно – там все программы в той или иной мере предназначены для цифровой криминалистики. Особенно это касается программ для извлечения сохранённых на компьютер паролей – кстати, перейдём теперь к ним.

EdgeCookiesView — это инструмент для Windows, который отображает файлы cookie, хранящиеся в более новых версиях веб-браузера Microsoft Edge и IE11 (начиная с Fall Creators Update 1709 для Windows 10). Он также позволяет вам выбрать один или несколько файлов cookie, а затем экспортировать их в файл с разделителями табуляции, файл csv, файл html или файл в формате cookie.txt. Вы можете прочитать файлы cookie из текущей работающей системы или из базы данных WebCacheV01.dat на внешнем жёстком диске.

Примечание. Новая версия Edge теперь основана на Chromium, поэтому вы можете использовать инструмент ChromeCookiesView для просмотра файлов cookie этого нового веб-браузера Edge.

EdgeCookiesView и **IECookiesView**

IECookiesView — очень старый инструмент, изначально разработанный в 2002 году (!), И он до сих пор работает с более ранними версиями веб-браузера Edge, которые хранят файлы cookie в текстовых файлах, точно так же, как Internet Explorer. Но начиная с Fall Creators Update 1709 для Windows 10 файлы cookie веб-браузера Microsoft Edge хранятся в базе данных WebCacheV01.dat вместе с историей и информацией кеша, поэтому IECookiesView больше не может читать файлы cookie Edge.

EdgeCookiesView — это новый инструмент, предназначенный для чтения файлов cookie из базы данных WebCacheV01.dat.

Программы для мониторинга сети

Wireless Network Watcher

Wireless Network Watcher – это небольшая программа, которая сканирует вашу беспроводную сеть и отображает список всех компьютеров и устройств, которые в данный момент подключены к ней.

Для каждого компьютера или устройства, подключённого к вашей сети, отображается следующая информация: IP адрес, MAC адрес, компания-производитель сетевой карты и, опционально, имя компьютера.

WifiInfoView

WifiInfoView сканирует беспроводные сети в вашей области и отображает расширенную информацию о них, включая: имя сети (SSID), MAC адрес, тип PHY (802.11g или 802.11n), RSSI, качество сигнала, частоту, номер канала, максимальную скорость, имя компании, модель роутера и имя роутера (только для роутеров, которые предоставляют эту информацию) и другое.

При выделении элемента, внизу отображает информация об этом устройстве в шестнадцатеричном формате.

CountryTraceRoute

CountryTraceRoute утилита построения маршрута (Traceroute), похожа на tracert для Windows, но с графическим пользовательским интерфейсом, а также намного быстрее tracert из Windows. CountryTraceRoute также отображает страну-владельца каждого IP адреса, найденного в маршруте.

Программы для извлечения информации из веб-браузеров и почтовых клиентов

ChromePass

ChromePass — это небольшой инструмент для восстановления пароля для Windows, который позволяет просматривать имена пользователей и пароли, хранящиеся в веб-браузере Google Chrome. Для каждой записи пароля отображается следующая информация: URL-адрес источника, URL-адрес действия, поле имени пользователя, поле пароля, имя пользователя, пароль и время создания. Программа позволяет вам получить пароли из вашей текущей работающей системы или из профиля пользователя, хранящегося на внешнем диске.

Вы можете выбрать один или несколько элементов, а затем сохранить их в файл text/html/xml или скопировать в буфер обмена.

Известные проблемы: в последних версиях веб-браузера Яндекса изменили шифрование паролей, и теперь оно отличается от шифрования паролей в Chrome, поэтому ChromePass больше не может расшифровывать пароли веб-браузера Яндекса.

BrowserAddonsView

BrowserAddonsView отображает подробности о всех дополнениях/плагинах веб-браузера, установленных в вашу систему. BrowserAddonsView может сканировать и определять дополнения большинства популярных браузеров: Chrome, Firefox и Internet Explorer. Для Chrome и Firefox, BrowserAddonsView сканирует все профили веб-браузера, если их несколько.

WebCookiesSniffer

WebCookiesSniffer захватывает все кукиз веб-сайтов, отправляемые между веб-браузером и веб-сервером и отображает их в простой таблице кукиз. Верхняя панель WebCookiesSniffer показывает строку куки и имя сайта/хоста, который отправил или принял это куки. При выборе строки куки в верхней панели, WebCookiesSniffer разбирает строку куки и отображает кукиз в нижней панели в формате имя-значение.

Утилиты, связанные с Интернетом, сетью и сетевым оборудованием

DomainHostingView

DomainHostingView – это программа для Windows, которая собирает обширную информацию о домене, используя серию DNS и WHOIS запросов и генерирует HTML отчёт, который можно открыть в веб-браузере.

Информация включает в себя: хостинг-компанию или дата центр, который хостит веб-сервер, почтовый сервер и сервер доменных имён (DNS) указанного домена, даты создания/изменения/истечения домена, владельца домена, регистратора домена, список всех DNS записей и другое.

IPNetInfo

IPNetInfo – это программка, которая позволяет вам с лёгкостью найти всю доступную информацию об IP адресе: владельца IP адреса, страну/штат, диапазон IP адресов, контактную информацию (адрес, телефон, факс и email) и другое.

IPNetInfo может извлекать все IP адреса из заголовков сообщения электронной почты – достаточно скопировать их в программу и она отобразит всю информацию об этих IP адресах.

MACAddressView

MACAddressView делает поиск по базе данных MAC адресов для поиска информации о компании (имя компании, адрес, страна), которая произвела данное сетевое устройство.

MACAddressView не посылает каких-либо запросов на удалённый сервер, он использует вшитую в .exe файл базу MAC адресов

PingInfoView

PingInfoView — это небольшая утилита, которая позволяет легко пинговать несколько имён хостов и IP-адресов и просматривать результат в одной таблице. Она автоматически проверяет связь со всеми хостами каждые указанное вами количество секунд и отображает количество успешных и неудачных проверок связи, а также среднее время проверки связи. Вы также можете сохранить результат ping в файл text/html/xml или скопировать его в буфер обмена.

Новая версия PingInfoView (2.00) позволяет использовать TCP ping для указанного номера порта вместо стандартного ICMP ping.

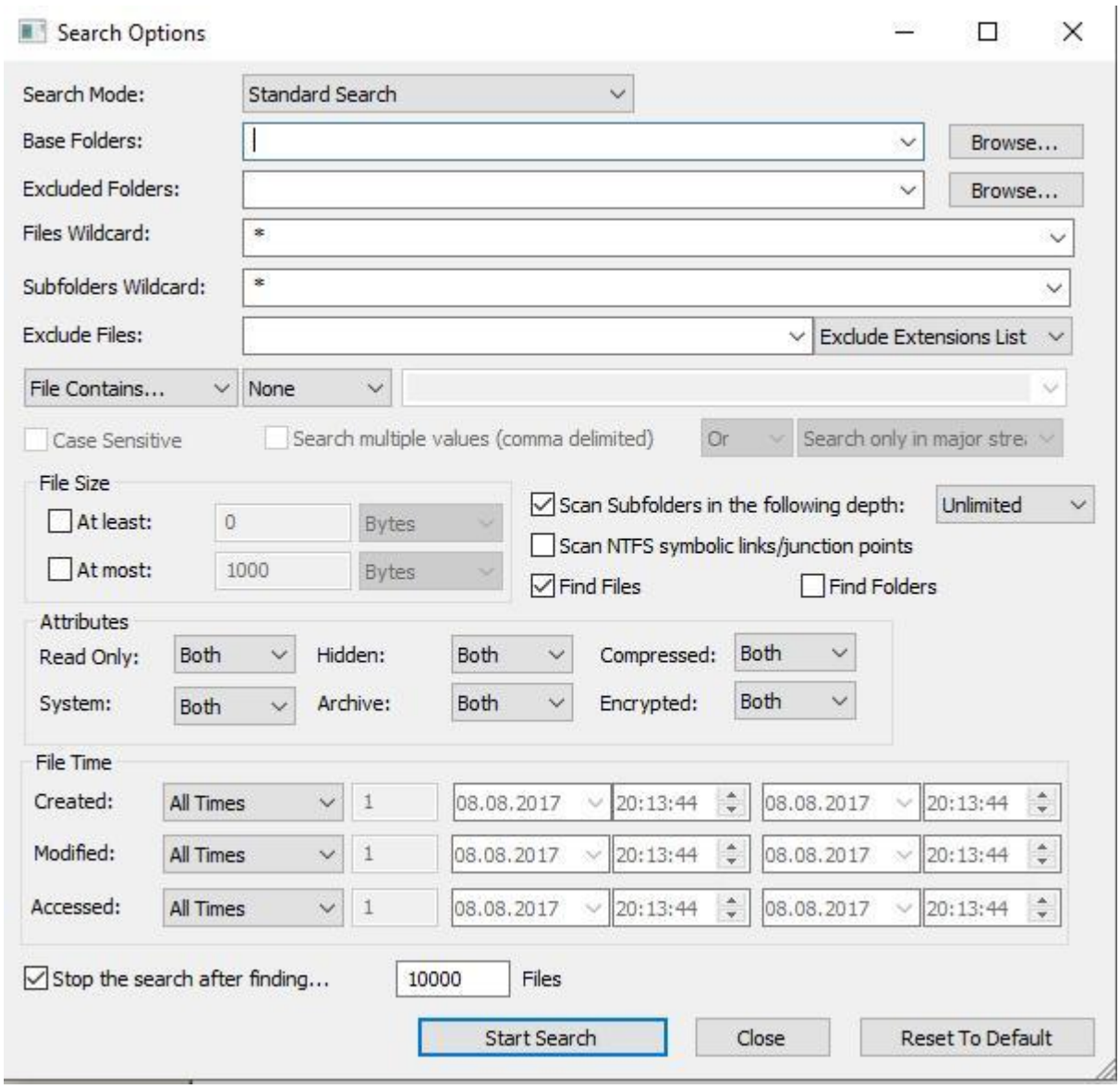
Чтобы использовать новую функцию TCP ping, просто укажите имя хоста или IP-адрес с номером TCP-порта, например: 10.0.0.10:21, 192.168.0.50:80, www.nirsoft.net:443

FastResolver

FastResolver переводит имена хостов в IP адреса и наоборот. Просто введите список IP адресов или имён хостов, которые вы хотите преобразовать. Также понимается ввод диапазонов IP, который вы хотите просканировать. Для локальной сети FastResolver также позволяет вам получить MAC адреса всех IP адресов, которые вы сканируете. FastResolver является многопоточным приложением, поэтому вы можете просканировать десятки адресов в считаные секунды.

Дисковые утилиты

SearchMyFiles



SearchMyFiles – это альтернатива стандартному модулю поиска Windows. Эта программа позволяет вам с лёгкостью искать файлы в вашей системе с использованием подстановочных символов, по времени последней модификации/создания/последнего доступа, по атрибутам файла, по содержимому файла (текстовый или бинарный поиск) и по размеру файла. SearchMyFiles позволяет вам задать очень точный поиск, который не может быть выполнен с поиском Windows. Например, вы можете найти все файлы, созданные за последние 10 минут и с размером между 500 и 700 байт.

После нахождения файлов, вы можете выбрать один или несколько из них и сохранить список в текстовый/html/csv/xml файл или скопировать список в буфер обмена.

SearchMyFiles является портативной программой, вы можете использовать её с USB флэшки без оставления следов в реестре просканированного компьютера.

MobileFileSearch

MobileFileSearch — это инструмент для Windows, который позволяет вам искать файлы внутри мобильного устройства (смартфона или планшета), подключённого к USB-порту вашего компьютера, с помощью протокола передачи мультимедиа (MTP). Вы можете искать файлы по их размеру, времени создания, времени изменения или имени (используя подстановочный знак).

Найдя файлы на своём смартфоне/планшете, вы можете при желании удалить их, скопировать в папку на своём компьютере или экспортировать список файлов в файл csv/разделённый табуляцией/html/xml/JSON.

MobileFileSearch также позволяет активировать поиск из командной строки и затем экспортировать результат в файл или копировать найденные файлы в нужную папку на вашем компьютере.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.2»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

Задания по НИРСОФТ

1. С помощью утилиты InstalledPackagesView выполните просмотр информации об установленных пакетах программного обеспечения. Просмотрите информацию о приложениях, установленных компанией «Microsoft Corporation».
2. С помощью утилиты *SpecialFoldersView* выполните просмотр системных папок ОС Windows
3. С помощью утилиты ExifDataView выполните просмотр метаданных Exif, хранящиеся в файлах изображений .jpg, найденых на компьютере.
4. С помощью утилиты FullEventLogView выполните просмотр событий из журналов событий Windows. Экспортируйте полученные данный в файл формата csv с TAB разделителями/html/xml.
5. С помощью утилиты BrowsingHistoryView просмотрите информацию о посещенных сайтах различными браузерами на компьютере. Сохраните полученные результаты.

6. С помощью утилит MozillaCacheView, ChromeCacheView, MZCacheView выполните просмотр кэша браузеров.

7. С помощью утилит ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView выполните просмотр файлов кукиз различных браузеров.

8. В помощью утилиты ChromePass выполните восстановление пароля для Windows, который позволяет просматривать имена пользователей и пароли, хранящиеся в веб-браузере Google Chrome.

9. В помощью утилиты owserAddonsVie выполните просмотр и анализ плагинов браузеров.

10. С помощью утилиты WebCookiesSniffer выполните перехват кукиз веб-сайтов, отправляемых между веб-браузером и веб-сервером.

11. С помощью утилиты DomainHostingView выполните просмотр информации (сведения о хостинг-компании или дата центре, который хостит веб-сервер, почтовом сервере и сервере доменных имён (DNS) указанного домена, даты создания/изменения/истечения домена, владельца домена, регистратора домена, список всех DNS записей и др.) о любом известном вам домене.

12. С помощью утилиты IPNetInfo осуществите просмотр информации (сведения о владельце IP адреса, страна, диапазон IP адресов, контактная информация (адрес, телефон, факс и email) и др.) о любом известном вам IP-адресе.

13. С помощью утилиты IPNetInfo осуществите просмотр заголовков сообщения электронной почты (для этого скопируйте их в программу, и она отобразит всю информацию об этих IP адресах).

14. С помошью утилиты MACAddressView выполните поиск по базе данных MAC адресов. Установите информацию о компании (имя компании, адрес, страна), которая произвела ваше сетевое устройство.

15. С помощью FastResolver утилиты осуществите перевод IP-адресов (таблица 1) в имена хостов.

16. С помощью утилиты SearchMyFiles осуществите поиск на вашем компьютере файлов, созданных за последние 10 часов, с расширением *.dat и с размером между 10 и 100 байт.