ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

Д. И. Полухин
М. М. Жуков

АНАЛИЗ И ВОССТАНОВЛЕНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Практикум

Воронеж

2024

ББК 32.972
П53

Рецензенты:

Г. К. Усков – заведующий кафедрой электроники физического факультета ВГУ, доктор физико-математических наук, профессор;

А. С. Бовкун – заместитель начальника отдела специальных и физико-химических экспертиз ЭКЦ ГУ МВД России по Воронежской области, подполковник полиции.

Полухин Д. И.

П53 Анализ и восстановление криминалистически значимой информации с помощью специализированного программного обеспечения : практикум / Д. И. Полухин, М. М. Жуков. – Воронеж : Воронежский институт МВД России, 2024. – 265 с.

ISBN 978-5-00229-138-0

Издание подготовлено в соответствии с требованиями нормативных правовых актов и официальных документов, регламентирующих учебный процесс в образовательных организациях, подведомственных МВД России.

В практикуме изложены требования по выполнению практических и лабораторных работ с различными программными и аппаратными комплексами, приведены краткие теоретические сведения по соответствующим темам, описана методика выполнения заданий, а также дан перечень вопросов, обязательных для изучения.

ISBN 978-5-00229-138-0

П-46-41(1)-24 **ББК 32.972**

ISBN 978-5-00229-138-0

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА № 1

ПОЛУЧЕНИЕ СВЕДЕНИЙ ОБ ОПЕРАЦИОННОЙ СИСТЕМЕ

Цель работы: Получение практических навыков обнаружения информации об операционной системе.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Получение сведений об операционной системе

Для осмотра активной системы можно использовать как штатные средства операционной системы, так и набор специализированных утилит. В ряде случаев применение специализированных средств может быть недоступно, например, при отсутствии возможности подключения внешних носителей или ограничения, связанные с запуском программного обеспечения. Поэтому сначала рассмотрим штатные средства операционной системы.

При осмотре средств вычислительной техники при активной системе, штатными средствами операционной системы семейства Windows NT следует выполнить следующие действия.

Для определения данных об операционной системе целесообразно воспользоваться данными командной строки – SYSTEMINFO. При этом можно как выполнить копирование информации из выводимого окна, так и сразу вывести информацию в файл. В этом случае префикс команды будет следующим:

SYSTEMINFO > [путь куда где будет создан файл]:\[имя файла].txt – например SYSTEMINFO > D:\systeminfo.txt будет осуществлять вывод информации о системе на локальном компьютере в текстовый файл systeminfo.txt, расположенный в корневой директории диска D. Аналогичные действия, по копированию информации в файл, можно

применять и к остальным командам приведенным ниже.

Также информацию о системе можно получит из приложения «Сведения о системе», для запуска которого можно использовать команду msinfo32.

Кроме того сведения о системе содержатся в реестре. Данные реестра, содержащие сведения об операционной системе хранятся в ветви: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

В данном ключе содержатся сведения о наименовании операционной системы и дате инсталяции InstallDate.

Дата инсталляции хранится в шестнадцатеричном и десятичном виде. Параметр InstallDate показывает количество секунд, прошедших с 1 января 1970 г. до момента установки операционной системы. Идентификационные номера продукта и пути установки.

Для получения сведений об использовании операционной системы, необходимо просмотреть данные из журнала событий Windows (рис. 1).

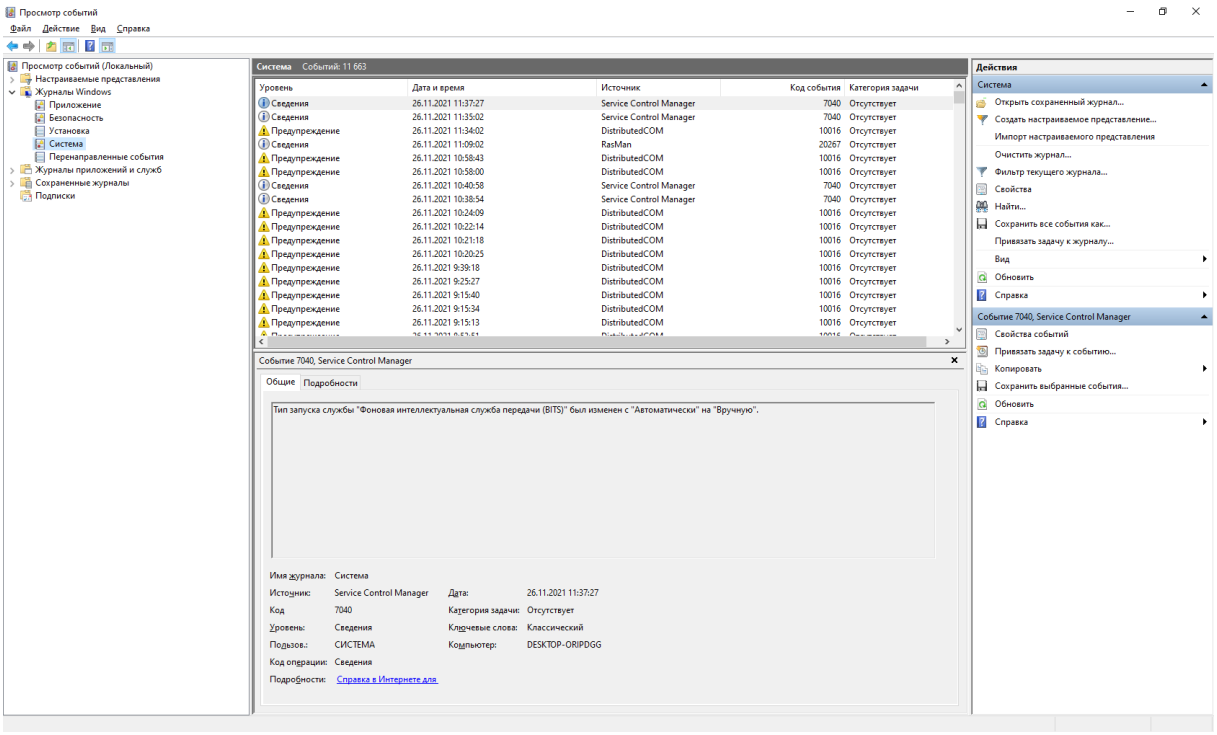


Рис. 1. Окно журнала событий Windows

Ниже приведены некоторые коды, отображающие работу системы для операционных систем Windows 7 и выше.

Код 1. Отображает системное время изменения времени операционной системы (отображает информацию и при смене часового пояса).

Код 12. Отображает системное время запуска операционной системы.

Код 13. Отображает системное время завершения работы операционной системы.

Код 26 (источник Application Popup). Отображает информацию об

использовании компьютера другими пользователями. Позволяет выявить работу иных пользователей с системой. Завершение работы Windows может привести к потере данных, открытых этим пользователем.

Код 36 (источник Time-Service). Отображает информацию об использовании компьютера другими пользователями. Завершение работы Windows может привести к потере данных, открытых этим пользователем.

Код 41 (источник Kernel-Power). Сообщает о перезагрузке системы в результате критического сбоя, или неожиданного отключения питания.

Код 6008. Отображает сообщение об аварийном завершении работы системы.

На рисунке 2 приведены данные из журнала «Система» о времени запуска операционной системы.

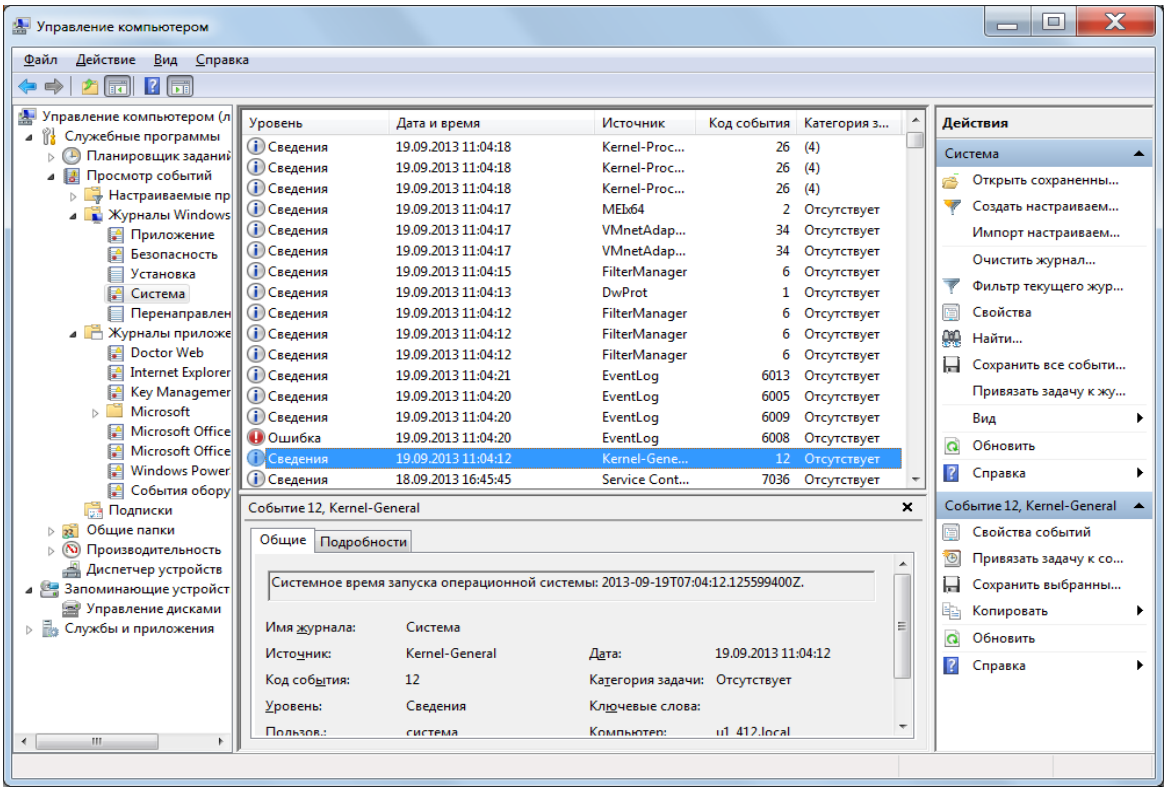


Рис. 2. Данные из журнала «Система» о времени запуска операционной системы

Для определения подключенных в системе логических томов и дисков необходимо просмотреть подменю меню «Управление дисками», входящее в состав меню «Управление» на вкладке «Компьютер».

Далее необходимо просмотреть меню «свойства» каждого из дисков, либо наличие логических томов и дисков, определяемых как устройство. На рисунке 3 приведены данные о подключении логических томов и дисков в меню «Управление дисками».

При этом обозначенный на рисунке «Диск 3» является виртуальным диском подключенным (смонтированным) из файла образа Acronis, что видно при просмотре меню «Свойства» данного диска. Содержание меню приведено на рисунке 4.

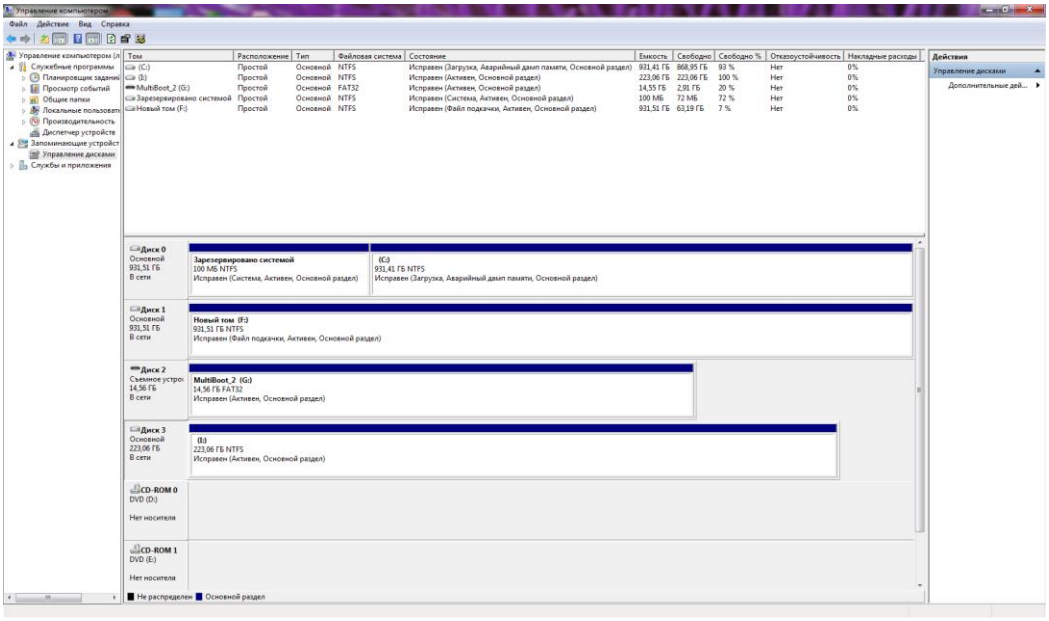


Рис. 3. Данные о подключении логических томов и дисков

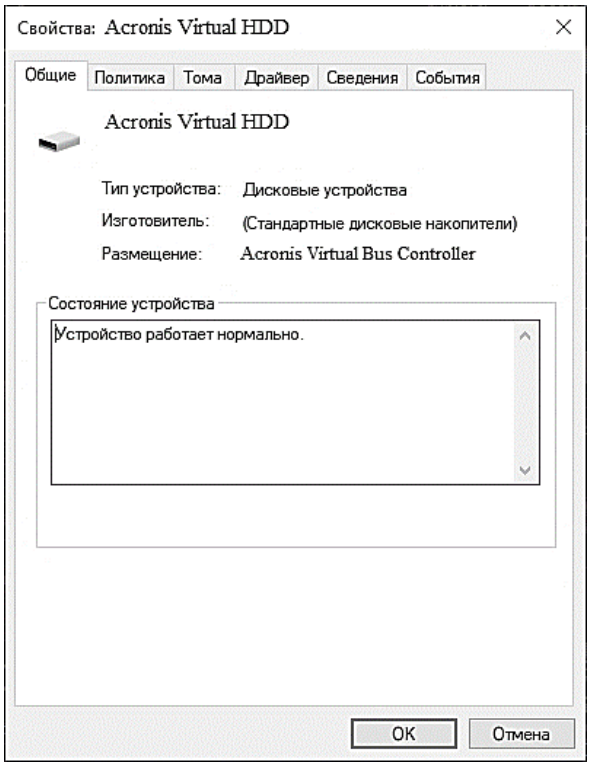
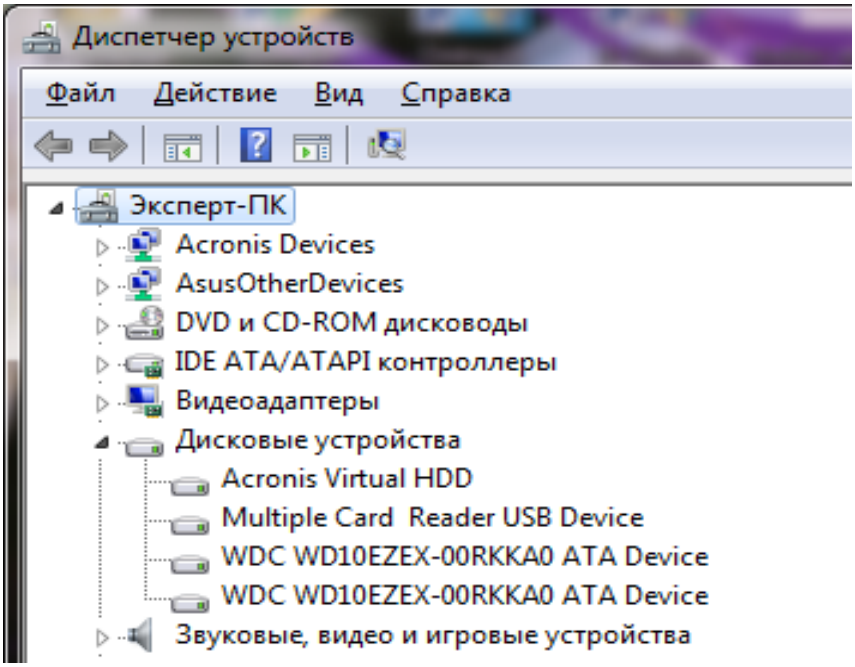


Рис. 4. Содержание меню «Свойства» виртуального раздела Acronis

Также информация о подключении виртуального раздела Acronis будет содержаться в разделе «Дисковые устройства» диспетчера устройств, операционной системы семейства Windows NT. Содержание диспетчера устройств, при подключенном виртуальном разделе Acronis приведено на рисунке 5.



.

Рис. 5. Содержание панели диспетчер устройств,
при подключенном виртуальном разделе Acronis

Однако не всегда данные о подключении виртуальных разделов отражается в разделе «Управление дисками». Это не происходит в случаях подключения криптоконтейнеров или в ряде случаев, файлов образов, как логических разделов.

Порядок выполнения работы

1. Получить сведения об операционной системе. Результаты привести в форме отчета.

1.1. Включить персональный компьютер и загрузить ОС Windows.

1.2. Для открытия командной строки нажать сочетание клавиш WIN+R. В открывшемся окне запуска приложений написать имя программы – cmd. Нажать Ok.

1.3. В командной строке ввести – SYSTEMINFO.

И фиксируем следующие параметры:

– версия ОС;
– изготовитель ОС;
– код продукта;
– дата установки;
– время загрузки системы;
– модель системы;
– версия BIOS;
– часовой пояс;
– полный объем физической памяти;

– доступная физическая память;

– виртуальная память;

– расположение файла подкачки.

1.4. Выполнить копирование информации из выводимого окна в файл.

- Создать на диске D папку с номером группы.

- Набрать в командной строке: SYSTEMINFO > [путь куда где будет создан файл]:\[имя файла].txt, например SYSTEMINFO > D:\systeminfo.txt будет осуществлять вывод информации о системе на локальном компьютере в текстовый файл systeminfo.txt.

- Продемонстрировать файл и его содержимое преподавателю.

1.5. Набрать в командной строке: msinfo32. Запустится приложение «Сведения о системе».

Сравнить параметры с ранее полученными и сделать отметку о соответствии.

1.6. Набрать в командной строке: regedit. Запустится «Редактор реестра». Данные реестра содержащие сведения об операционной системе хранятся в ветви: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion.

В конечной папке находятся ключи, по значению которых можно узнать информацию о системе. Сравнить параметры с ранее полученными и сделать отметку о соответствии.

2. Соответствие системного времени текущему, в случае активной машины. Результаты привести в форме отчета.

2.1. Набрать в командной строке: compmgmt/s. Откроется окно «Управление компьютером».

2.2. Перейти: /Просмотр событий/Журналы Windows/Система. В окне «Действия» в подменю «Фильтр текущего журнала» ввести код события – 1 (Отображает системное время изменения времени операционной). Определить соответствие системного времени текущему, данные о переводе системного времени, системное время запуска операционной системы (код 12), системное время завершения работы операционной системы (код 13), данные о перезагрузке системы в результате критического сбоя, или неожиданного отключения питания (код 41, источник Kernel-Power); данные об аварийном завершении работы системы (код 6008).

3. Данные о машинных носителях информации, установленных в системе.

3.1. Набрать в командной строке: compmgmt/s. Откроется окно «Управление компьютером».

3.2. Перейти в раздел «Управление дисками». Сделать вывод о количестве Дисков и Томов, имеющихся на исследуемом компьютере. Отразить их основные параметры.

Контрольные вопросы

1. Как получить сведения об операционной системе?
2. Как получить сведения о системном времени?
3. Как получить сведения об изменения времени в операционной системе?
4. Как получить сведения о системном времени завершения работы операционной системы?
5. Как получить сведения о перезагрузке системы в результате критического сбоя?
6. Как получить данные о машинных носителях информации, установленных в системе?

ЛАБОРАТОРНАЯ РАБОТА № 2

ПОЛУЧЕНИЕ СВЕДЕНИЙ О СЕТЕВЫХ СОЕДИНЕНИЯХ

Цель работы: Получение практических навыков обнаружения данных о сетевых соединениях.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения и формулы, ход выполнения работы и выводы.

Основные теоретические сведения

Из данных командной строки: SYSTEMINFO можно получить сведения о сетевых адаптерах и подключениях. Более подробные сведения о сети можно получить с помощью командной строки IPCONFIG /ALL. Здесь будут содержаться следующие сведения:

- настройка протокола IP для Windows;
- сетевое имя компьютера;
- физические адреса адаптеров.

Если в системе имеется виртуальная машина, то она будет отражаться так же, как сетевой адаптер.

Следует обратить внимание, что если в системе используется несколько сетевых адаптеров, то для адаптеров, которые в данный момент неактивны в строе «состояние среды» будет обозначение «среда передачи недоступна»! Ниже приведены сведения, полученные с помощью данной команды выгруженные в файл.

```
Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : DESKTOP-ORIPDGG
   Основной DNS-суффикс  . . . . . . :
   Тип узла. . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . : Нет
   WINS-прокси включен . . . . . . . : Нет
   Порядок просмотра суффиксов DNS . : local.vimvd.ru
```

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Realtek RTL8188SU Wireless
LAN 802.11n USB 2.0 Network Adapter
   Физический адрес. . . . . . . . . : 00-14-D1-D1-50-86
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Microsoft Hosted Network
Virtual Adapter
   Физический адрес. . . . . . . . . : 00-14-D1-D1-50-86
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . : local.vimvd.ru
   Описание. . . . . . . . . . . . . : Intel(R) 82579V Gigabit
Network Connection
   Физический адрес. . . . . . . . . : 50-46-5D-74-0E-2B
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . :
fe80::f90e:9d63:3960:e405%10(Основной)
   IPv4-адрес. . . . . . . . . . . . : 192.168.238.236(Основной)
   Маска подсети . . . . . . . . . . : 255.255.192.0
   Аренда получена. . . . . . . . . . : 26 ноября 2021 г. 8:53:48
   Срок аренды истекает. . . . . . . . . . : 27 ноября 2021 г.
8:53:47
   Основной шлюз. . . . . . . . . : 192.168.252.50
   DHCP-сервер. . . . . . . . . . . : 192.168.252.3
   IAID DHCPv6 . . . . . . . . . . . : 105924189
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-28-4B-7B-23-50-
46-5D-74-0E-2B
   DNS-серверы. . . . . . . . . . . : 192.168.252.3
   NetBios через TCP/IP. . . . . . . . : Включен

Адаптер PPP VPN:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : VPN
   Физический адрес. . . . . . . . . :
   DHCP включен. . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . : Да
   IPv4-адрес. . . . . . . . . . . . : 172.30.3.111(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.255
   Основной шлюз. . . . . . . . . : 0.0.0.0
   DNS-серверы. . . . . . . . . . . : 172.30.0.2
   NetBios через TCP/IP. . . . . . . . : Включен
```

Далее необходимо определить активные подключения, для чего используется команда NETSTAT. Команда выводит сведения о TCP и UDP -соединений, таблицы маршрутизации, слушаемых портов, статистических данных.

Команда NBTSTAT–n отображает таблицу NetBIOS-имен на локальном компьютере. Таблица содержит следующие сведения: «Имя», «тип», «Состояние». Состояние «Зарегистрирован» означает, что имя зарегистрировано с использованием широковещательного запроса или с помощью сервера WINS. Так же отражается количество локальных подключений.

Команда NET USE – отображает список сетевых дисков, подключенных в системе.

Команда NET SHARE – отображает список ресурсов, к которым открыт общий доступ.

Команда NET LOCALGROUP Администраторы – отображает список пользователей локальной группы «Администраторы» системы.

Команда NET USER – отображает список пользователей.

Данные о настройке Dialupass сетевых соединений, в том числе VPN хранятся в файле:

%SystemDrive%\Users\[имя пользователя]\AppData\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk

Фрагмент содержимого файла:

DEVICE=vpn

PhoneNumber=vpn.local.vimvd.ru

Если для данных подключений сохранен пароль, то для его просмотра необходимо специализированное программное обеспечение, например входящий в комплект NirLauncher - Nirsoft, утилитой Dialupass.

Данные о беспроводном подключении Wi-Fi можно получить командой NETSH WLAN SHOW PROFILES

Профили Wi-Fi хранятся в каталоге %ProgramData%\Microsoft\Wlansvc\Profiles\Interfaces в виде файлов *.xml.

Если для данных подключений сохранен пароль, то для его просмотра в явном виде, возможно использовать специализированное программное обеспечение, например входящий в комплект NirLauncher - Nirsoft, утилитой WirelessKeyView.

Информация о всех сетевых подключениях, в том числе о подключениях по локальной сети хранится в журнале Приложений и служб Microsoft-Windows-NetworkProfile/Operational (выполняется).

Файл данного журнала расположен по адресу: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx.

Данным о подключении соответствует код события 1000.

Ниже приведены примеры из журнала для различных подключений.

Из данных представлений можно получить информацию, как о времени подключения, так и об устройствах, с помощью которых данное подключение осуществлялось. В частности, для рассматриваемого Wi-Fi подключения можно определить источник предоставляющий доступ к сети - AndroidAPfc89.

Следует обратить внимание, что в журнале WLAN-AutoConfig, содержится более подробная информация о Wi-Fi подключениях. Данные о подключениях – код событий 8001, и об отключениях, код – событий 8003, от Wi-Fi сети.

Порядок выполнения работы

1. Получение данных о сетевых соединениях.

1.1. Набрать в командной строке: SYSTEMINFO. Отобразить основные сетевые параметры.

1.2. Набрать в командной строке IPCONFIG /ALL. Отобразить в отчете следующие сведения:

- настройка протокола IP для Windows;
- сетевое имя компьютера;
- физические адреса адаптеров.

Следует обратить внимание, что если в системе используется несколько сетевых адаптеров, то для адаптеров, которые в данный момент неактивны в строе «состояние среды», будет обозначение «среда передачи недоступна»!

1.3. Набрать в командной строке: NETSTA. Определить активные подключения и сведения о TCP и UDP-соединений, таблицы маршрутизации слушаемых портов.

1.4. Набрать в командной строке: NBTSTAT –n. Получить таблицу NetBIOS-имен на локальном компьютере.

Таблица содержит следующие сведения: «Имя», «тип», «Состояние». Состояние «Зарегистрирован» означает, что имя зарегистрировано с использованием широковещательного запроса или с помощью сервера WINS. Также отражается количество локальных подключений.

1.5. Набрать в командной строке: NET USE. Зафиксировать список сетевых дисков, подключенных в системе.

1.6. Набрать в командной строке: NET USE. Зафиксировать список пользователей.

1.7. Набрать в командной строке: NETSH WLAN SHOW PROFILES. Зафиксировать данные о беспроводном подключении Wi-Fi.

1.8. Перейти к файлу %SystemRoot%\System32\Winevt\Logs\ Microsoft-Windows-NetworkProfile%4Operational.evtx. В нем содержится информация о всех сетевых подключениях, в том числе о подключениях по локальной сети хранится в журнале. Осуществить двойной клик по файлу и зафиксировать данные о сетевом подключении (соответствует код события 1000).

Контрольные вопросы

1. Какие разделы реестра просматриваются для определения данных о сетевых подключениях?
2. Какое программное обеспечение позволит получить информацию о сетевых подключениях на персональном компьютере?
3. В каком файле на персональном компьютере содержится информация о всех сетевых подключениях, в том числе о подключениях по локальной сети?
4. Что такое IP-адрес?
5. Что такое MAC-адрес?
6. Что такое маска сети?
7. Что такое DHCP-сервер?
8. Что такое DNS-сервер?

ЛАБОРАТОРНАЯ РАБОТА № 3

ОПРЕДЕЛЕНИЕ ДАННЫХ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНЫХ ПРОДУКТОВ

Цель работы: Выработка практических навыков получения данных об использовании программных продуктов с применением специального программного обеспечения.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения и формулы, ход выполнения работы и выводы.

Основные теоретические сведения

Определение данных об использовании программных продуктов

(на примере Microsoft Office)

Для определения данных об использовании программных продуктов просматривается следующая информация:

- данные из ветви реестра HKEY_CURRENT_USER\Software;
- данные из ветвей реестра, содержащих сведения об использовании программного обеспечения, например, данные из ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Office\XX.X\Word\File MRU содержат сведения об открытых в приложении файлах;
- данные из файлов журнал системы;
- данные из файлов Prefetch;
- данные из файлов гибернации – hiberfil.sys;
- данные из файлов подкачки – pagefile.sys;
- данные из оперативной памяти;
- данные из файлов журналирования;
- данные из файлов ссылок;
- данные из MFT (*Master File Table* – «Главная файловая таблица»);

- данные из директории %SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent;

- данные из файла реестра Amcache.hve расположенного %SYSTEMROOT% \appcompat\Programs\;

- данные из файлов переходов – Jump Lists.

Файлы списков переходов * .automaticDestinations-ms расположены по следующему пути:

%SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent \ AutomaticDestinations

Для просмотра файлов можно использовать утилиту JumpListsView входящий в комплект NirLauncher - Nirsoft.

Данные об использовании Microsoft Office (на примере Word) содержатся:

- в файле WINWORD.EXE-B9C5483D.pf директории Prefetch;

- в журнале приложений – Microsoft Office Alerts.

Для Windows 7 и выше в директории

%SYSTEMDRIVE%\Users\%USERNAME%\AppData\Roaming\Microsoft\ Office\ Последние файлы\

В реестре для каждого компонента Office:

HKEY_CURRENT_USER\Software\Microsoft\Office\XX.X\Word\File MRU

И ключе типа:

HKEY_USERS\S-1-5-21-3243842915-810645812-68586957-1000\Software\Microsoft\Office\XX.X\Word\File MRU

- в файлах гибернации - hiberfil.sys;

- в файлах подкачки- pagefile.sys;

- данные из оперативной памяти;

- в данных MFT;

- в данных из директории %SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent;

- в данных из файлов переходов – Jump Lists.

Причем частично содержимое файлов Microsoft Office сохраняется в

файлах гибернации – hiberfil.sys, файлах подкачки – pagefile.sys, в оперативной памяти.

Рассмотрим способ получения данных из MFT.

MFT (англ. Master File Table – «Главная файловая таблица») – база данных, в которой хранится информация о содержимом тома с файловой системой NTFS.

Для получения данных из MFT сначала необходимо скопировать сам файл $MFT на доступное специалисту пространство его машинного носителя, т.е. в директорию для исследования. Для этой цели воспользуемся программным продуктом AccessData FTK Imager. С его помощью возможно получать данные из служебных областей диска. После

запуска программы необходимо воспользоваться меню Add All Attached Devices  , с помощь которого открываем необходимый раздел диска. Для каждого раздела с файловой системой NTFS имеется свой файл $MFT. Далее открываем раздел root и получаем доступ к содержимому раздела. Для копирования файла активируем меню Export Files. После того как файл будет скопирован необходимо преобразовать его в табличный вид. Для это воспользуемся программой MFTDump. Программа работает из командной строки! После преобразования создается файл mftdump_localhost.txt, который необходимо открыть в табличном редакторе, например Exel. При этом для корректного отображения кириллицы необходимо выбрать формат 65001: юникод (UTF-8).

MFTDump предоставляет три формата отчетов; короткие, стандартные и длинные. Если не указать параметр / s (короткий) или / l (длинный) в командной строке, выходной отчет будет в стандартном формате. Пример поля отчета показан на рисунке 1.

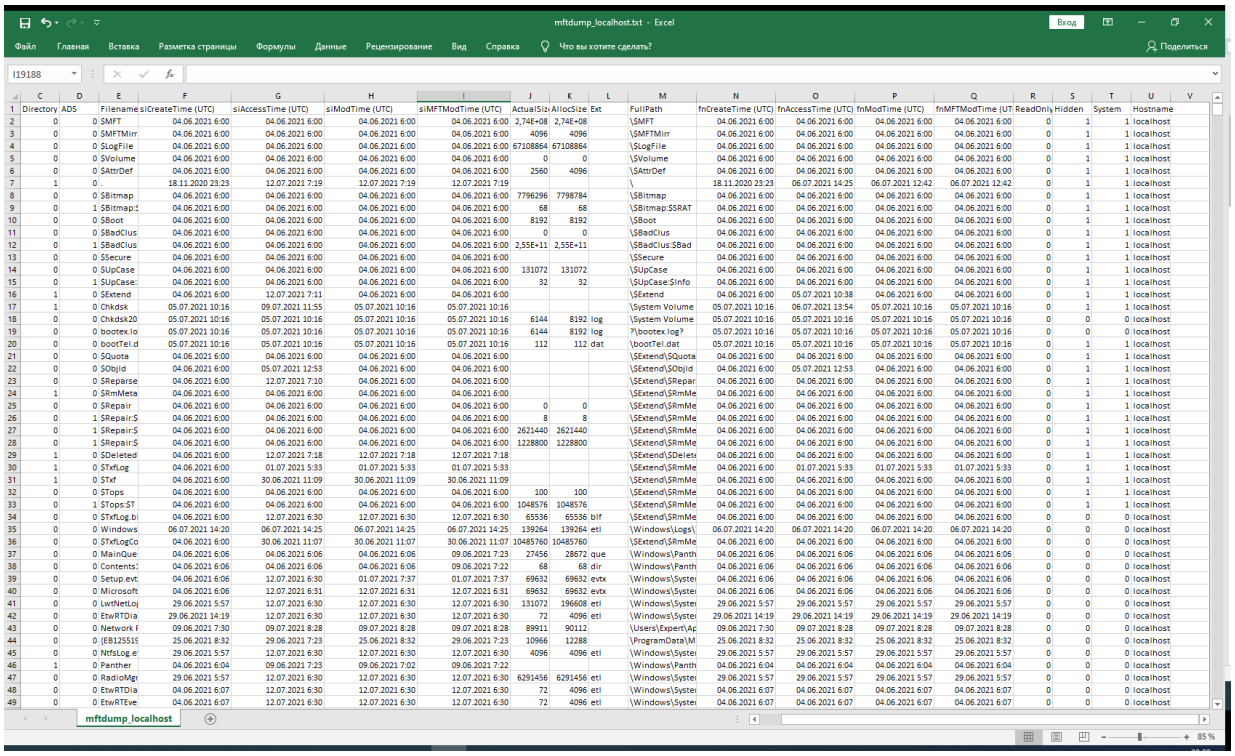


Рис. 1. Пример поля отчета

Названия столбцов обозначают следующее:

Rename – переименование файла;

Local Move – перемещение файла в пределах одной файловой системы;

Volume move – перемещение между файловыми системами;

Copy – копирование файла;

Create – создание файла;

Delete – удаление файла;
Open – открытие файла;
Properties – просмотр свойств файла;
Attributes – изменение атрибутов файла;
Modify – изменение файла.

Для работы с таблицей необходимо воспользоваться фильтрами. Так для поиска документов созданных в Word, в столбце Ext выбираем фильтр по расширению файлов doc и docx.

Данные об удалении файлов находятся в столбце Deleted, значение 1.

Следует обратить внимание, что изменения в файл $MFT сохраняются при любом подключении к соответствующему разделу диска. В том числе и при загрузке с внешнего носителя или подключении диска как внешнего!

Соответствующие данные о выявленных программных продуктах целесообразно привести в виде таблицы.

Также данные об использовании программных продуктов хранятся в файле Amcache.hve, расположенном по адресу %SystemRoot%\appcompat\Programs\. Данный файл является файлом реестра, о чем свидетельствует сигнатура файла 72 65 67 66 04 00 в HEX, и regf в ANSI кодировке. Для просмотра файла можно воспользоваться программой Windows Registry Recovery от компании MiTeC. Для копирования файла в активной системе так же можно воспользоваться программой AccessData FTK Imager. В файле Amcache.hve содержатся сведения о расположении и временных параметрах запуска программных продуктов. Так определения данных о программном продукте Word, достаточно произвести поиск по данному слову. Результаты приведены на рисунке 2.

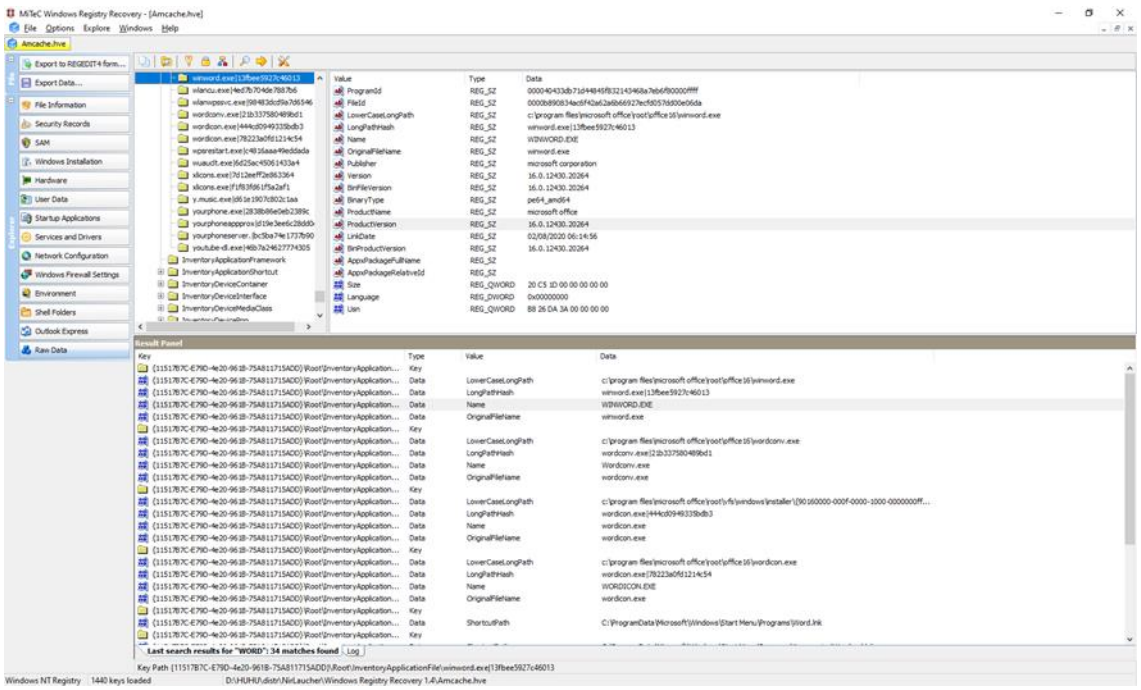


Рис. 2. Данные о программном продукте Word из файла Amcache.hve

Для получения сведений об использовании Microsoft Office из директории Prefetch, расположенной в директории Windows, целесообразно воспользоваться специализированными утилитами, например winprefetchview входящий в комплект NirLauncher - Nirsoft. Просмотром файла WINWORD, с помощью данной утилиты можно определить, какие последние файлы открывались в приложении Microsoft Office и расположение соответствующих временных файлов приложения.

Данные об установленном программном обеспечении Microsoft Office хранятся в ветвях реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\ (далее запись типа: 9140110900063D11C8EF10054038389C)\InstallProperties

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\ XX.0\Registration\ (далее запись типа: {90110419-6000-11D3-8CFE-0150048383C9})

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\XX.0\Registration\ (далее запись типа: {90120000-0016-0000-0000-0000000FF1CE})

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Installer\UserData\S-1-5-18\Products\ (далее запись типа: 00002109610000000000000000F01FEC)\InstallProperties,

где XX.0 код программного обеспечения Microsoft Office.

Ниже приведено соответствие кодов программного обеспечения Microsoft Office версии программы:

- Office 2003 Office11
- Office 2007 Office12
- Office 2010 Office14
- Office 2013 Office15
- Office 2016 Office15
- Office 2019 Office15

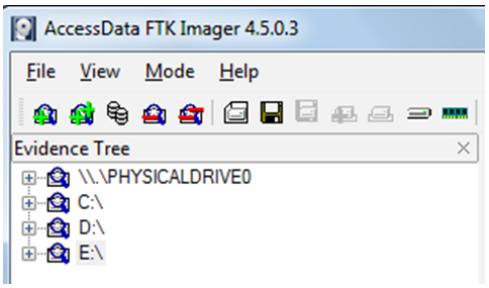
Порядок выполнения работы

1. Получить сведения о программном продукте Microsoft Word из MFT.

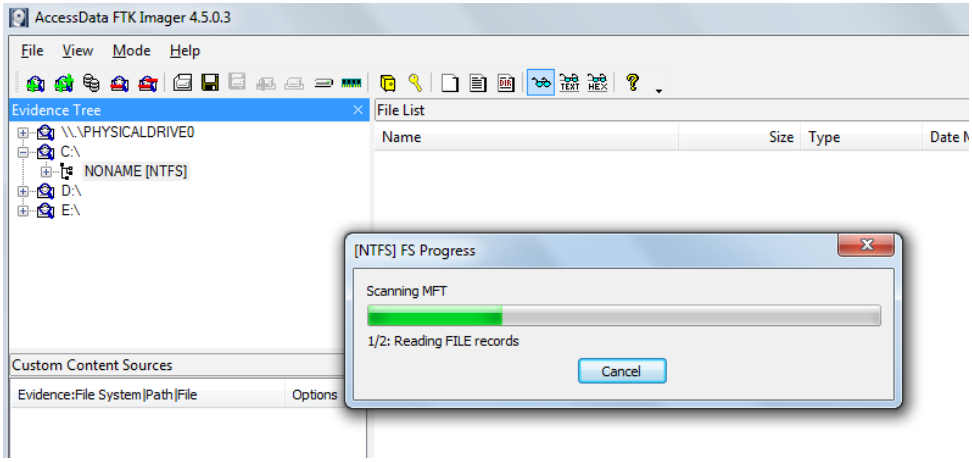
1.1. Включить персональный компьютер и загрузите ОС Windows.

1.2. Запустить программу **AccessData FTK Imager**.

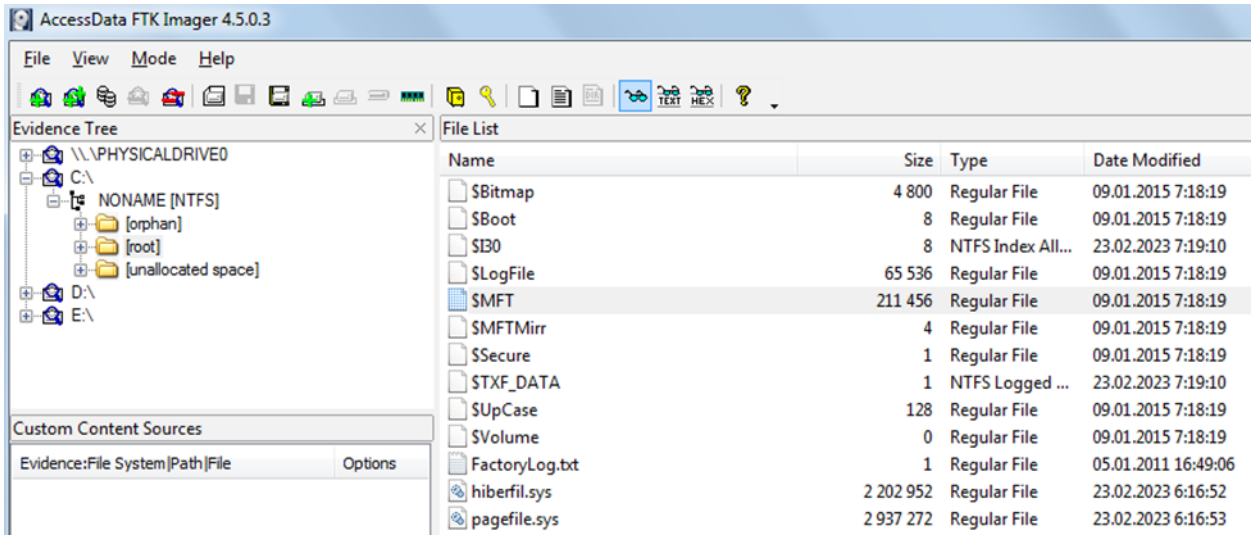
1.3. Запустить **Add All Attached Devices**  , выбрав в меню **File** либо кликнув соответствующую пиктограмму рабочего стола программы. В окне **Evidence Tree** отобразятся диски компьютера.



1.4. В окне **Evidence Tree** выбрать диск C и раздел **NONAME** и дождаться окончания сканирования.



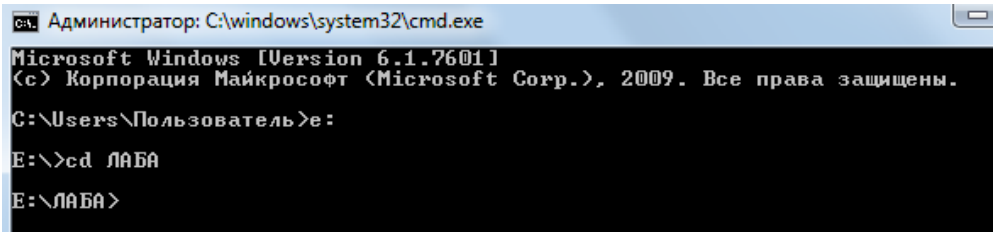
1.5. Далее открыть раздел **root** и получить доступ к содержимому раздела. Выбрать файл **$MFT** и, нажав правую кнопку мыши, выбрать **Export Files**. Экспорт файла осуществить в индивидуальную папку, созданную на прошлом занятии. Дождаться окончания копирования.



1.6. В индивидуальную папку копировать также файл **mftdump.exe**, полученный от преподавателя.

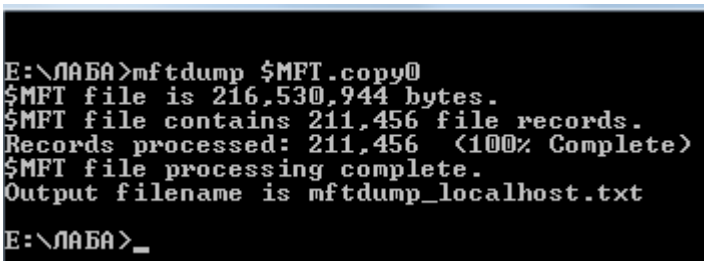
1.7. Преобразовать скаченный файл **MFT** в табличный вид с помощью программы MFTdump. Для этого запустить командную строку и перейти в

индивидуальную папку. Программа MFTDump работает из командной строки.



1.8. В командной строке набрать: **mftdump $MFT.copy0** и дождаться окончания процесса. MFTDump предоставляет три формата отчетов; короткие, стандартные и длинные. Если не указать параметр / s (короткий) или / l (длинный) в командной строке, выходной отчет будет в стандартном формате.

1.9. По окончании процесса будет создан файл **mftdump_localhost.txt**.



1.10. Открыть файл **mftdump_localhost.txt** с помощью **MS Excel** и сохранить его в формате XLS или XLSX.

1.11. В столбце Ext выбрать фильтр по расширению файлов doc и docx. Найти не менее 5 удаленных файлов и произвести их описание (Данные об удалении файлов находятся в столбце Deleted, значение 1).

1.12. Найти самый первый (по времени) и последний созданные файлы. Описать их.

1.13. Создать короткий и длинный отчеты с помощью команд **mftdump /s $MFT.copy0 и mftdump /l $MFT.copy0** (перед созданием нового отчета – старый удаляется). Провести сравнительный анализ таблиц.

2. Получить сведения о программном продукте Microsoft Word по данным из реестра.

2.1. Посмотреть содержимое SYSTEMDRIVE% \Users\ %USERNAME%\AppData\Roaming\Microsoft\ Office\ Последние файлы\. Сравнить полученную информацию с данными, полученными в 1 задании.

3. Определить, какие последние файлы открывались в приложении Microsoft Office на компьютере winprefetchview, входящем в комплект NirLauncher - Nirsoft.

3.1. Запустить winprefetchview, входящий в комплект NirLauncher - Nirsoft.

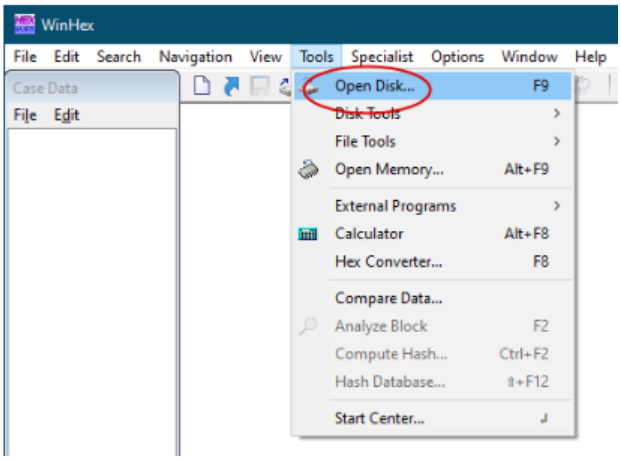
3.2. С помощью данной утилиты осуществить просмотр файла WINWORD.

3.3. Сравнить данные с ранее полученной информацией.

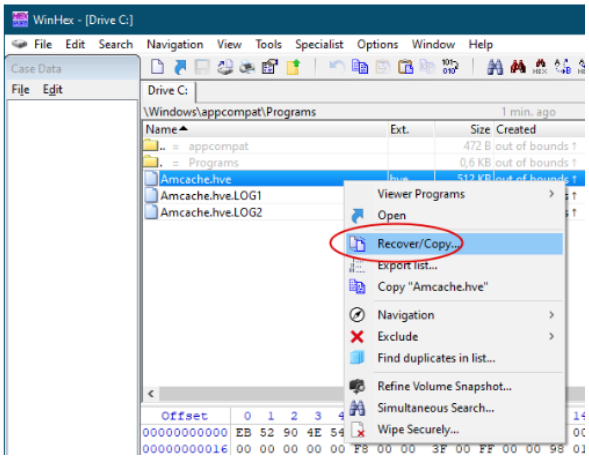
4. Получить список запускавшихся на компьютере программ с использованием файла **Amcache.hve**.

4.1. Запустить программу **WinHex (с правами администратора).**

4.2. В **WinHex** необходимо выбрать в меню **Tools** > **Open Disk.**



4.3. После того как программа создаст снапшот, перейти в **C:\Windows\AppCompat\Programs**, кликнуть по файлу **Amcache.hve** правой кнопкой мыши, выбрать **Recovery/Copy**. И указать путь сохранения файла (индивидуальную папку, созданную на прошлом занятии).



4.4. Для просмотра файла воспользуйтесь программой Windows Registry Recovery (рис.2). Провести анализ запускавшихся на компьютере программ.

Контрольные вопросы

1. Какие разделы реестра просматриваются для определения данных об использовании программных продуктов?
2. Назначение раздела Prefetch?
3. Где находится файл $MFT?
4. Какая информация содержится в файле $MFT?
5. С помощью каких программных продуктов возможно получение информации из файла $MFT?
6. Опишите алгоритм копирования файла $MFT.
7. Опишите алгоритм получения информации из $MFT в короткой стандартной и длинной формах.
8. Где находится информация об использовании программных продуктов на персональном компьютере?
9. Какие существуют способы обнаружения информации об использовании программных продуктов на персональном компьютере?
10. Какое программное обеспечение позволит получить информацию об использовании программных продуктов на персональном компьютере?

ЛАБОРАТОРНАЯ РАБОТА № 4

ОПРЕДЕЛЕНИЕ ДАННЫХ О ПОДКЛЮЧЕНИИ USB УСТРОЙСТВ

Цель работы: Получение практических навыков обнаружения данных о подключении USB устройств к исследуемому персональному компьютеру.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Информация о подключенных внешних устройствах хранится:
- в реестре операционных систем;
- журналах событий;
- в файлах журналирования;
- в файлах драйверов программного обеспечения.

Рассмотрим более подробно каждое из указанных мест.

Данные из реестра.

Сведения о подключении USB устройств содержатся в следующих ветвях реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

и

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR.

В данных ветвях содержится информация о типе и виде подключенных устройств, а так же их серийный номер и уникальный номер (Globally Unique Identifier – GUID), который идентифицирует устройство для системы.

Причем данные о серийном номере содержатся в имени ветви, например:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB\Vid_058f&Pid_6387\FKZ9XO6P, где FKZ9XO6P серийный номер устройства.

В ветви реестра USB устройства обозначаются идентификатором производителя и идентификатором устройства.

В ветви реестра USBSTOR устройства обозначаются по наименованию или типу.

Время о подключения устройств определяется из времени изменения соответствующей ветви реестра. Для получения данных о времени подключения можно использовать утилиту USBDeview входящий в комплект NirLauncher - Nirsoft. Если нет возможности использовать сторонне программное обеспечение, то можно произвести экспорт соответствующей ветви реестра в текстовый файл. При этом в файле будут указаны времена подключения соответствующих USB устройств.

На рисунке 1 приведены данные из реестра о подключении внешних устройств.

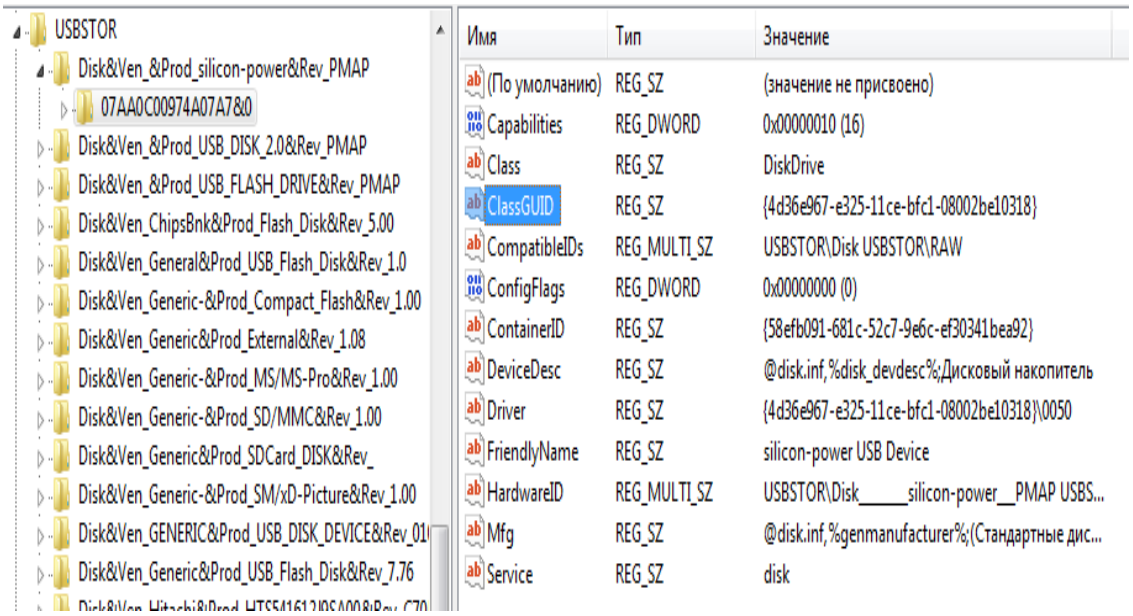


Рис. 1. Данные из реестра о подключении внешних устройств

Данные журналов событий

Данные о подключенных устройствах отражаются в журналах событий Windows, в частности в журнале «Система» и в журналах приложений и служб, в частности в журнале «Конфигурация устройств».

Для журнала «Система» Windows 7 и выше используют следующие коды событий, содержащих информацию о времени подключения внешних устройств:

- 10000 источник DriverFrameworks-UserMode содержит сведения о начале установки пакета драйверов;

- 20001, 20003 содержат сведения о завершении установки драйверов;

Данные коды событий можно задать в «фильтре» программы просмотра журналов. Следует помнить, что здесь содержатся данные об установке драйверов USB устройств и что указанное время напрямую зависит от системного времени.

Для просмотра файлов журналов событий можно использовать штатные средства операционной системы, в меню «Действия» программного обеспечения «Управление компьютером» открыв исследуемый файл. Или воспользоваться специализированным программным обеспечением, например Event Log Explorer.

На рисунке 2 приведено изображение окна просмотра журнала «Система» с выборкой фильтра 10000.

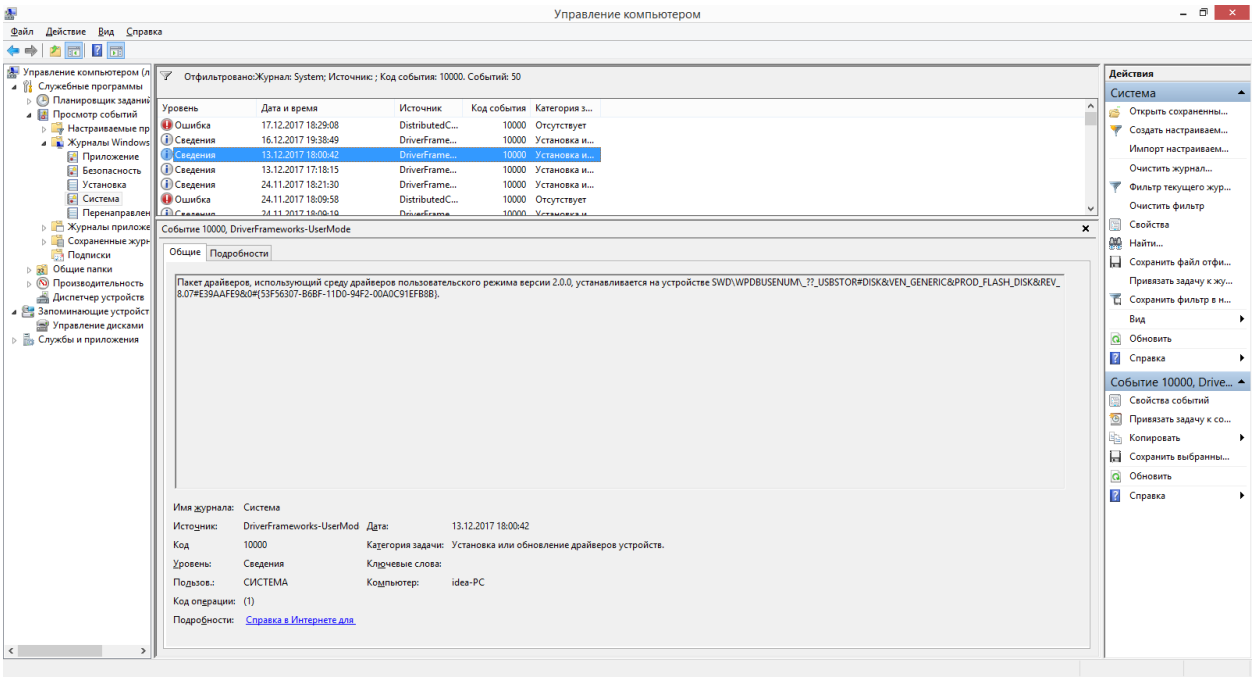


Рис. 2. Данные из журнала «Система» с выборкой фильтра 10000

На рисунке 3 приведены данные из журнала Microsoft-Windows-Kernel-PnP/Configuration (Конфигурация устройства), расположенного по следующему пути: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx.

Данный журнал содержит сведения об использовании USB устройств.

Следует помнить, что информация в журналах событий сохраняется только за время ведения журнала!

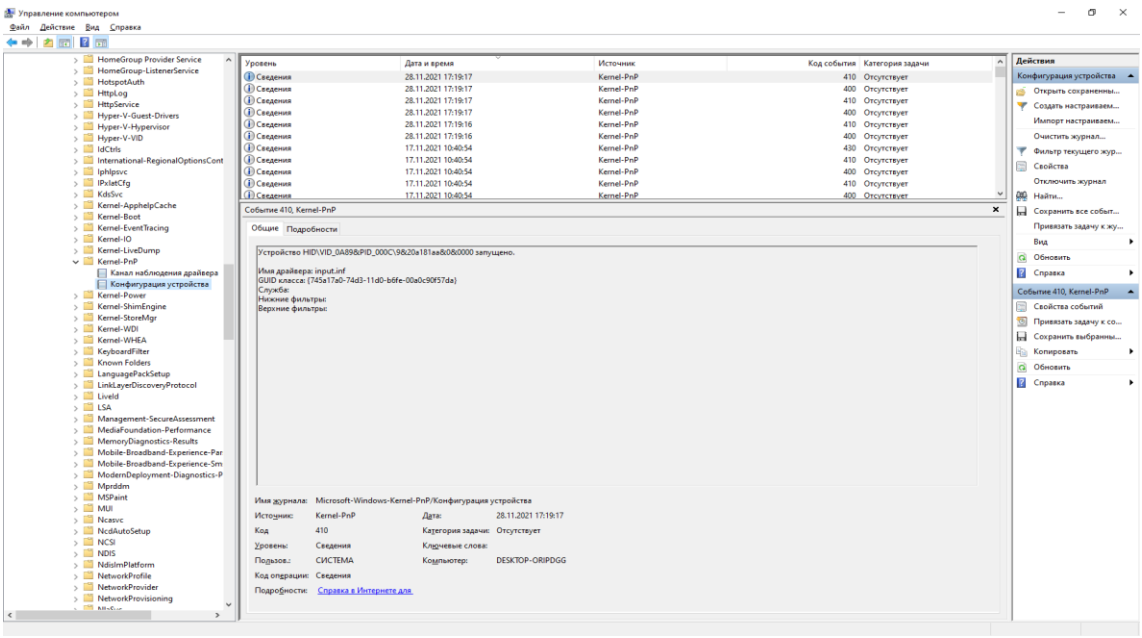


Рис. 3. Данные из журнала «Конфигурация устройства»

Файлы журналирования драйверов программного обеспечения

Данные об использовании USB устройств содержатся в файле setupapi.dev.log расположенном в директории \Windows\inf\ для Windows 7 и выше.

В файле setupapi.dev.log содержится информация следующего вида:

… [Device Install (Hardware initiated) - USB\VID_058F&PID_6366\058F63666438]

>>> Section start 2017/12/16 19:41:00.117 …

То есть имеется информация об идентификаторах производителя и устройства, а также серийный номер устройства. Эта информация содержится в ветви реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB.

В файлах usb.inf и usb.PNF расположенном в директории \Windows\inf\ содержится информация об установке драйверов для USB устройств.

В файле usb.inf содержится информация следующего вида:

```
[Version]
Signature=$Windows NT$
Class=USB
ClassGUID={36FC9E60-C465-11CF-8056-444553540000}
Provider=%Msft%
DriverVer=06/21/2006,6.3.9600.17238

[ControlFlags]
; Exclude USB\COMPOSITE from BasicDriverOK list
BasicDriverOk=USB\CLASS_09&SUBCLASS_01, USB\CLASS_09
ExcludeFromSelect=*
```

Получение информации из журналов операционной системы.

Для определения проведенных действий операционной системой семейства Windows производится просмотр журналов событий операционной системы.

Для Windows 7 данные файлы по умолчанию расположены в директории %SYSTEMROOT%\System32\Winevt\Logs\ и имеют расширение .Evtx.

Просмотром данного журнала возможно определить:

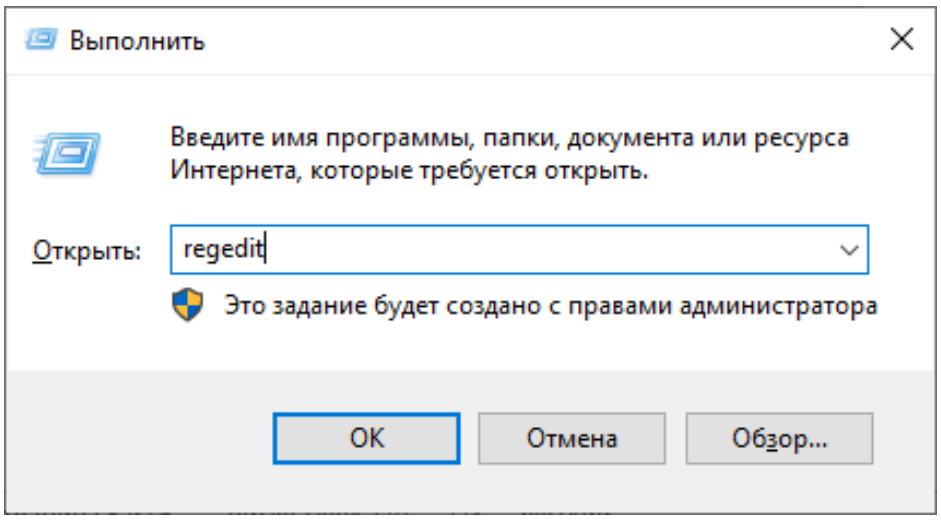
- временные рамки работы операционной системы;
- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы Windows;
- временные рамки подключения-отключения сетевых ресурсов (сетевого адаптера) запуск которых отображается в журнале событий операционной системы Windows, и ряд других параметров.

Порядок выполнения работы

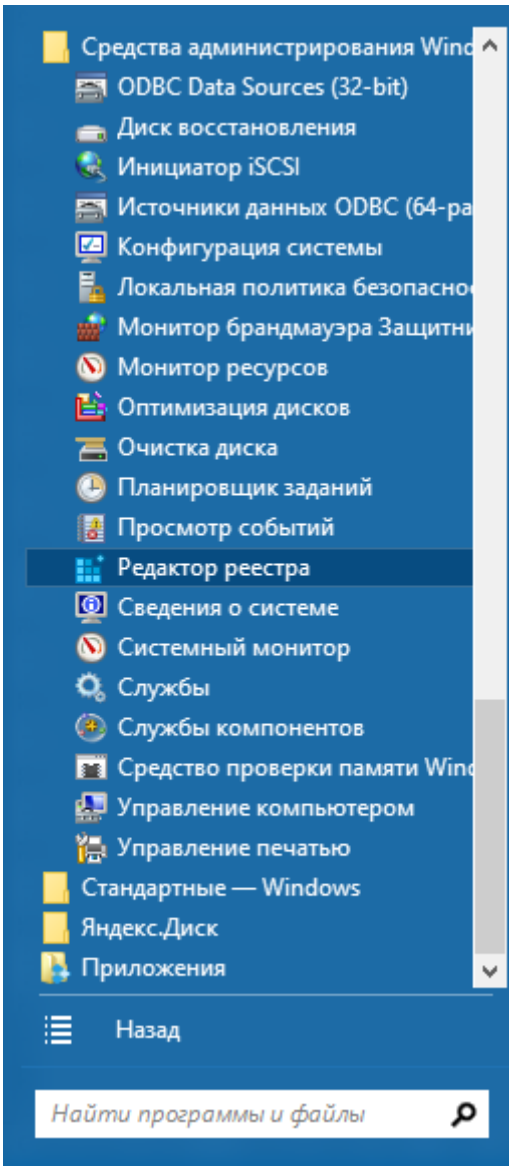
1. Исследование активной системы.

1.1 Запустить реестр исследуемого ПК несколькими способами.

1.1.1 Выполнить команду Пуск\Выполнить\regedit

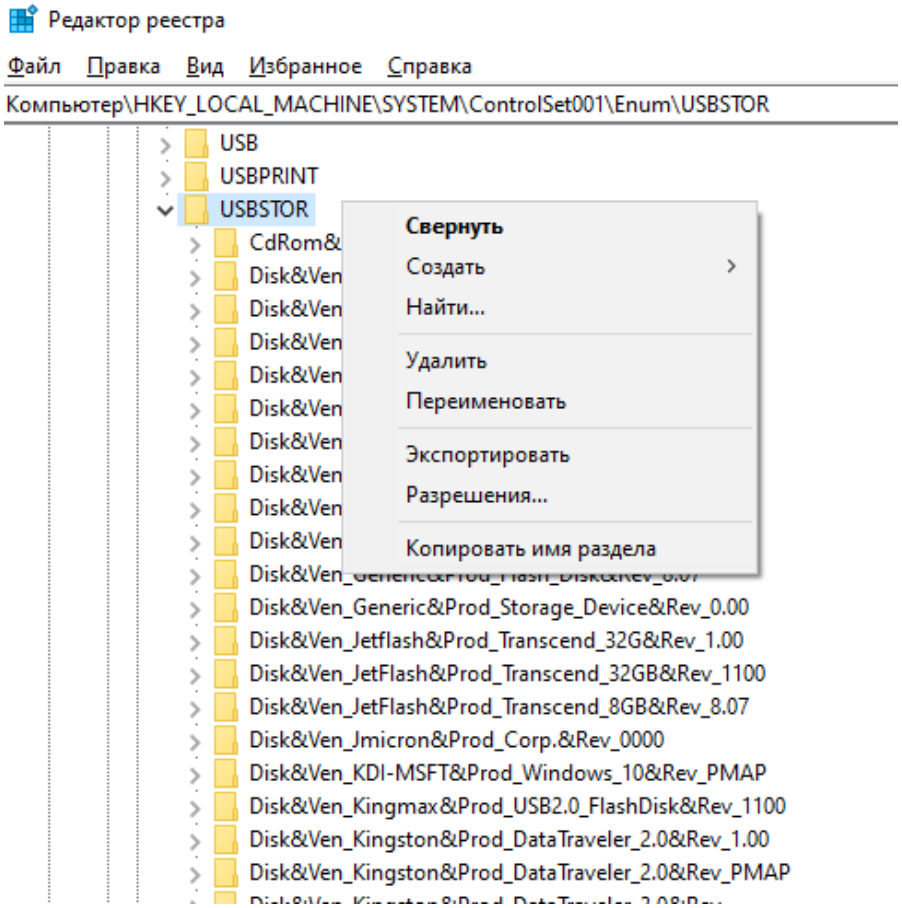


1.1.2 Выполнить команду «Пуск\Все программы\Средства администрирования Windows\Редактор реестра»



1.2 Обнаружить три ветви реестра
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB;
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB PRINT;
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB STOR.

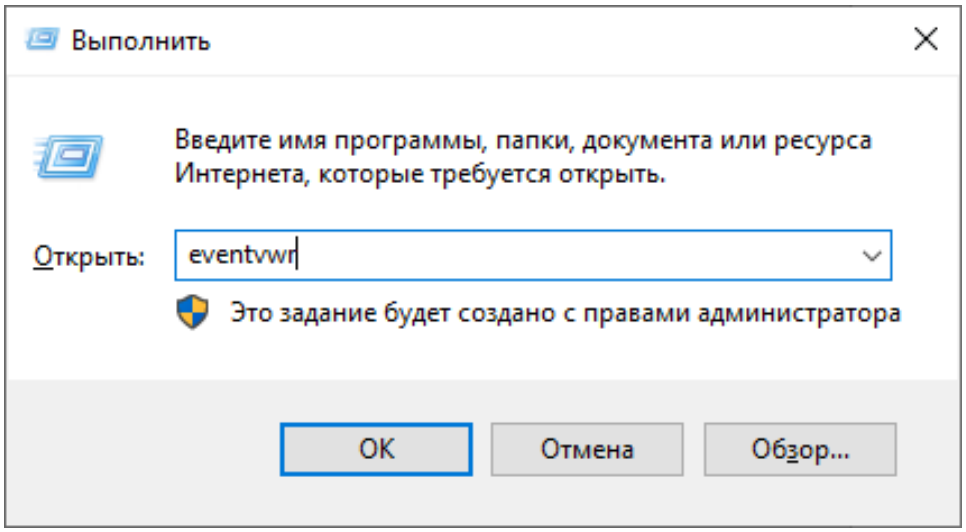
1.3 Сделать экспорт всех сведений каждой ветви реестра в текстовый файл.



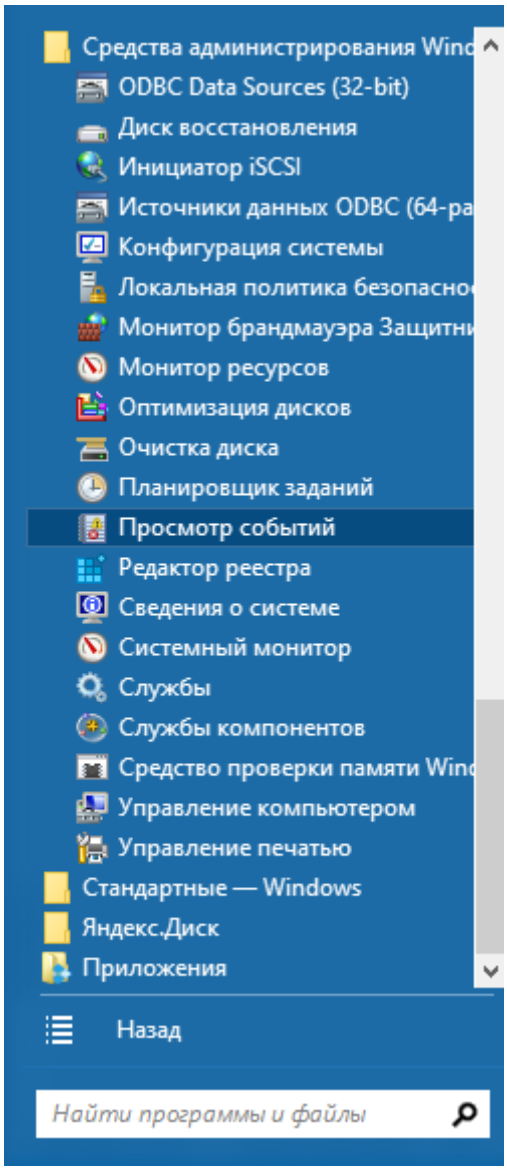
1.4 Сохранить полученные три текстовых файла с присвоением соответствующих имен USB.txt, USBPRINT.txt, USBSTOR.txt.

1.5. Запустить журнал событий исследуемого ПК несколькими способами.

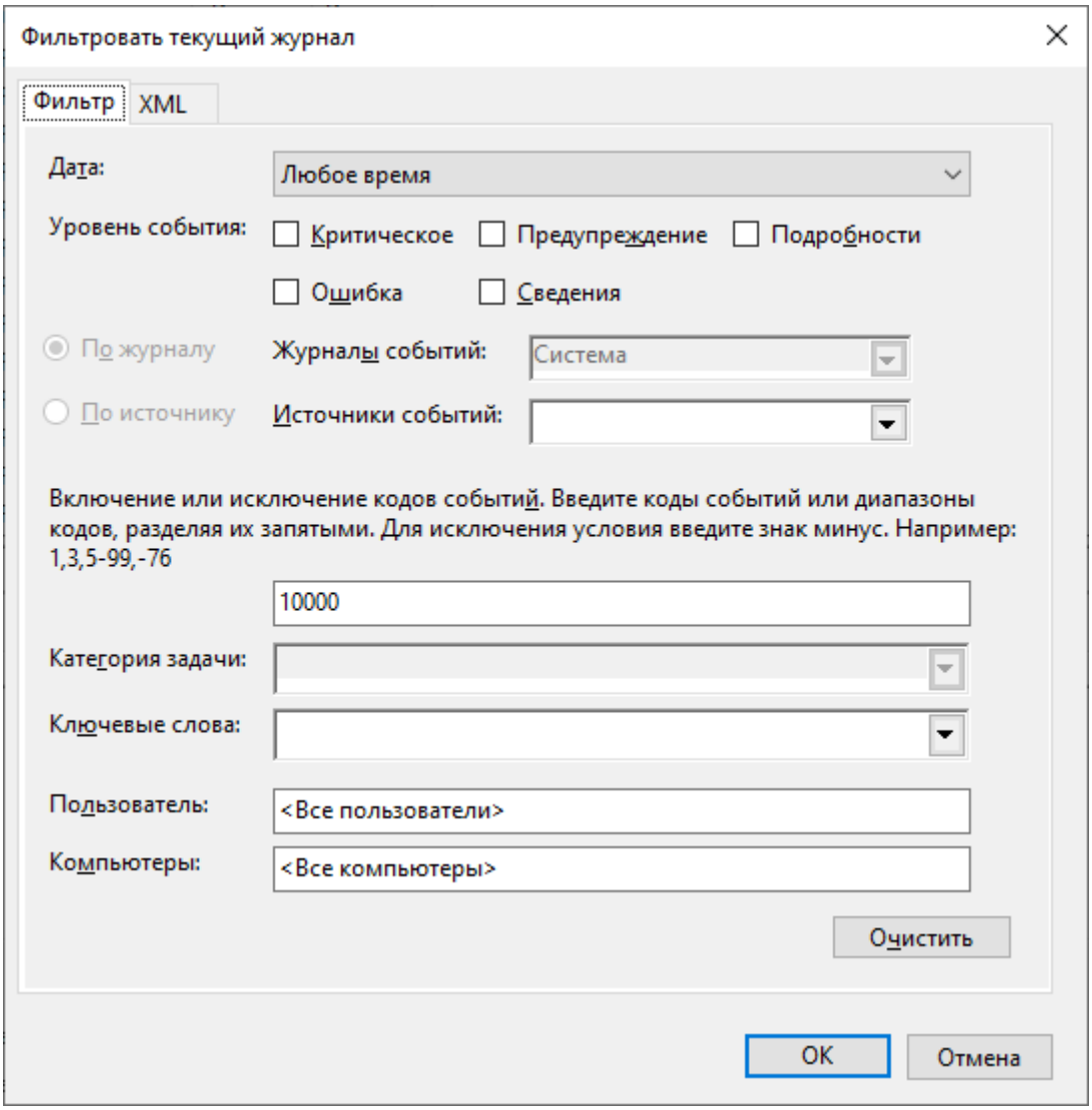
1.5.1 Выполнить команду Пуск\Выполнить\eventvwr



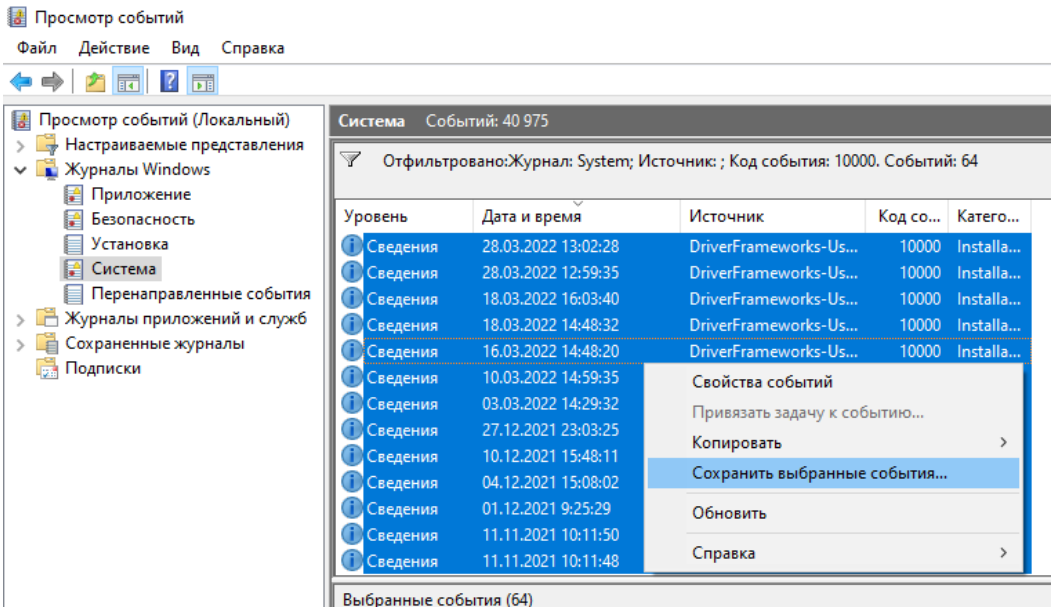
1.5.2 Выполнить команду «Пуск\Все программы\ Средства администрирования Windows\Просмотр событий»



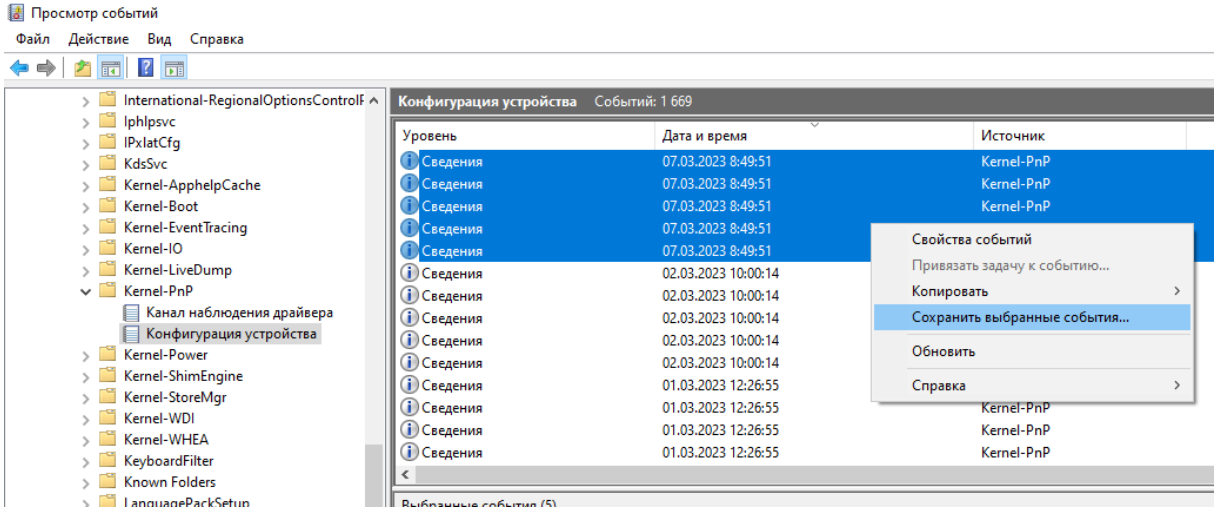
1.6. Обнаружить журнал Windows «Система».
1.7. Установить фильтр текущего журнала 10000.



1.8 Сохранить выбранные события в текстовый файл «СобытияUSB.txt».



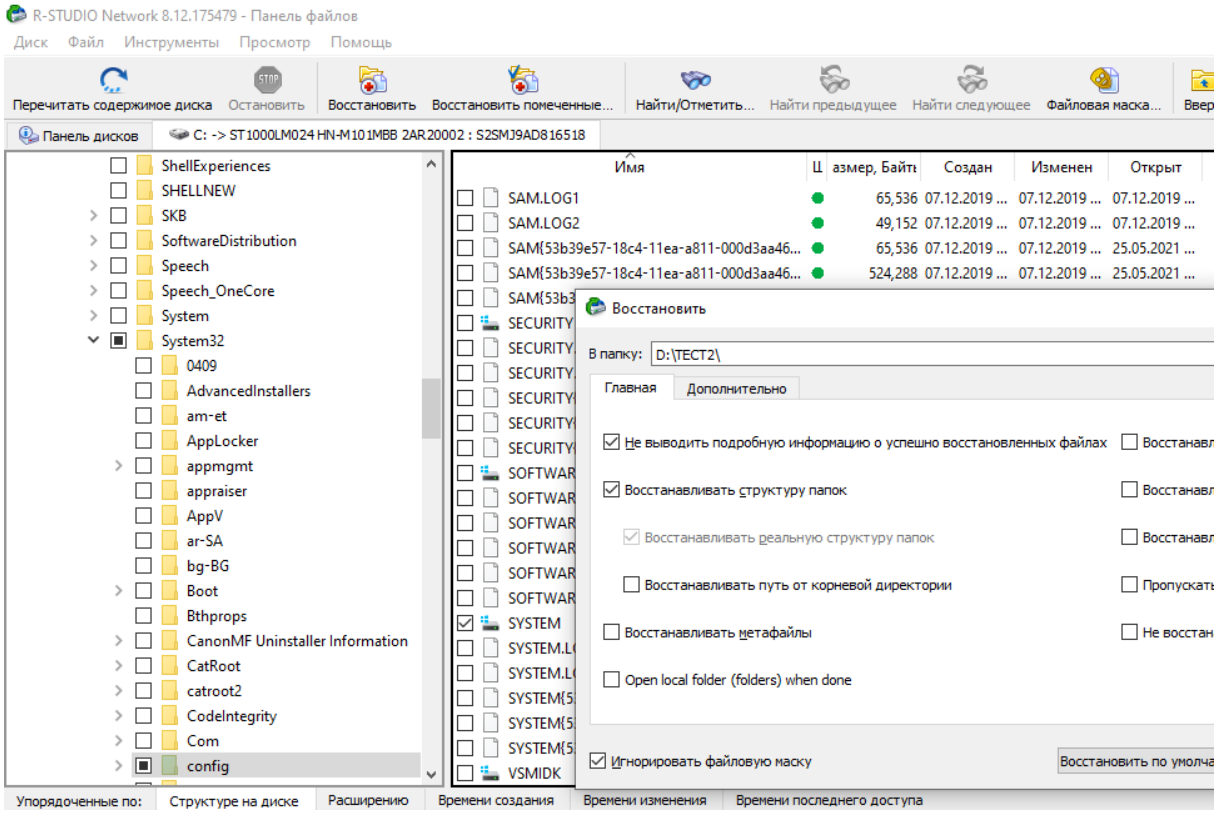
1.9. Обнаружить журнал «Журналы приложений и служб\Microsoft\Windows\Kernel-PnP\Конфигурация устройства».
1.10. Сохранить выбранные события в текстовый файл «События_Kernel-PnP.txt»



2. Исследование неактивной системы.

При исследовании неактивной системы (ситуация, когда исследуемый накопитель с операционной системой подключен к лабораторному ПК, и в момент проведения исследования запущена лабораторная ОС) после введения команд или выбора пунктов меню, указанных в разделе №1 данной лабораторной работы, будут обнаружены сведения лабораторной системы. Для обнаружения сведений на исследуемом накопителе с незапущенной операционной системой необходимо выполнить следующие действия.

2.1. Обнаружить файлы реестра в каталоге исследуемого накопителя \Windows\System32\config.
2.2. С помощью программы AccessData FTK Imager или R-Studio экспортировать файл SYSTEM во временный каталог.



2.3. С помощью программы Windows Registry Recovery открыть экспортированный файл SYSTEM.
2.4. Выполнить пункты 1.2–1.4 с помощью программы Windows Registry Recovery.
2.5. Обнаружить файлы журналов событий в каталоге исследуемого накопителя \Windows\System32\winevt\Logs\.
2.6. С помощью программы AccessData FTK Imager или R-Studio экспортировать файлы журналов событий во временный каталог.
2.7. Открыть экспортированные файлы с помощью стандартного средства «Просмотр событий» лабораторного ПК.
2.8. Выполнить пункты 1.6–1.10 с помощью стандартного средства «Просмотр событий» по отношению к экспортированным файлам журналов событий.
3. Сравнить полученные в пунктах 1 и 2 сведения. Сделать соответствующие выводы.

4. Дополнительное задание повышенной сложности.
4.1. Самостоятельно обнаружить на исследуемом накопителе в каталоге Windows\inf файлы setupapi.dev.log и usb.inf.
4.2. Экспортировать их во временный каталог.
4.3. Сравнить содержимое файлов setupapi.dev.log и usb.inf с полученными в пунктах 1 и 2 результатами и сделать дополнительный вывод.

Контрольные вопросы

1. Какие разделы реестра просматриваются для определения данных о подключенных USB устройствах?
2. Назначение ветки реестра USB.
3. Назначение ветки реестра USBPRINT.
4. Назначение ветки реестра USBSTOR.
5. В каком каталоге находятся файлы реестра?
6. В каком каталоге находятся файлы журналов событий?
7. Какая криминалистически значимая информация может содержаться в реестре?
8. Какая криминалистически значимая информация может содержаться в журналах событий?
9. С помощью каких программных продуктов возможно получение информации из файлов реестра?
10. Какой код события в журнале имеют сведения об установке драйверов USB устройств?
11. С помощью какого программного обеспечения можно экспортировать файлы реестра и файлы журналов событий?
12. Опишите алгоритм получения информации из файлов реестра при активной и неактивной системе.
13. Кроме реестра, где еще можно обнаружить сведения о подключенных USB устройствах?

ЛАБОРАТОРНАЯ РАБОТА № 5

ОПРЕДЕЛЕНИЕ СВЕДЕНИЙ О ДАТЕ ПОСЛЕДНЕЙ РАБОТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ НА АКТИВНОЙ И НЕАКТИВНОЙ СИСТЕМЕ

Цель работы: Получение практических навыков обнаружения данных о дате последней работы ОС.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

«Просмотр событий» – один из множества стандартных инструментов Windows, предоставляющий возможность просмотра всех событий, происходящих в среде операционной системы. В числе таковых всевозможные неполадки, ошибки, сбои и сообщения, связанные как непосредственно с ОС и ее компонентами, так и сторонними приложениями.

Существует несколько вариантов открытия журнала событий на компьютере с Windows 10, но в целом все они сводятся к ручному запуску исполняемого файла или его самостоятельному поиску в среде операционной системы. Расскажем подробнее о каждом из них.

Как понятно из названия, «Панель» предназначена для того, чтобы управлять операционной системой и входящими в ее состав компонентами, а также быстрого вызова и настройки стандартных инструментов и средств. Неудивительно, что с помощью этого раздела ОС можно вызвать в том числе и журнал событий.

Любым удобным способом откройте «Панель управления». Например, нажмите на клавиатуре Win+R, введите в строку открывшегося окна выполнить команду control без кавычек, нажмите ОК или Enter для запуска.

Найдите раздел «Администрирование» и перейдите в него, кликнув левой кнопкой мышки (ЛКМ) по соответствующему наименованию. Если потребуется, предварительно измените режим просмотра «Панели» на «Мелкие значки».

Отыщите в открывшейся директории приложение с наименованием «Просмотр событий» и запустите его двойным нажатием ЛКМ.

Журнал событий Windows будет открыт, а значит, вы сможете перейти к изучению его содержимого и использованию полученной информации для устранения потенциальных проблем в работе операционной системы либо же банальному изучению того, что происходит в ее среде.

И без того простой и быстрый в своем выполнении вариант запуска «Просмотра событий», который нами был описан выше, при желании можно немного сократить и ускорить.

Вызовите окно «Выполнить», нажав на клавиатуре клавиши Win+R.
Введите команду «eventvwr.msc» без кавычек и нажмите Enter или ОК.
Журнал событий будет открыт незамедлительно.
Функцию поиска, которая в десятой версии Windows работает особенно хорошо, можно использовать для вызова различных системных компонентов и не только их. Так, для решения нашей сегодняшней задачи необходимо выполнить следующее:

Нажмите по значку поиска на панели задач ЛКМ или воспользуйтесь клавишами Win+S.

Начните вводить в поисковую строку запрос «Просмотр событий» и, когда увидите в перечне результатов соответствующее приложение, кликните по нему ЛКМ для запуска.

Это откроет журнал событий Windows.

Аудит события входа пользователей в Windows

При расследовании различных инцидентов администратору необходимо получить информацию кто и когда заходил на определенный компьютер Windows. Историю входов пользователя в доменной сети можно получить из журналов контроллеров домена. Но иногда проще получить информацию непосредсвенно из логов компьютера. Рассмотрим, как получить и проанализировать историю входа пользователей на компьютер/сервер Windows. Такая статистика поможет вам ответить на вопрос: «Как в Windows проверить кто и когда использовал этот компьютер?»
После того как вы включили политики аудита входа, при каждом входе пользователя в Windows в журнале Event Viewer будет появляться запись о входе. Посмотрим, как она выглядит.

Откройте оснастку Event Viewer (eventvwr.msc);

Разверните секцию Windows Logs и выберите журнал Security;

Щелкните по нему правой клавишей и выберите пункт Filter Current Log;

В поле укажите ID события 4624 и нажмите OK;

В окне события останутся только события входа пользователей, системных служб с описанием

В описании события указано имя и домен пользователя, вошедшего в систему

Ниже перечислены другие полезные EventID:

Event ID	Описание
4624	A successful account logon event
4625	An account failed to log on
4648	A logon was attempted using explicit credentials
4634	An account was logged off
4647	User initiated logoff

Если полистать журнал событий, можно заметить, что в нем присутствуют не только события входа пользователей на компьютер. Здесь также будут события сетевого доступа к этому компьютеру (при открытии по сети общих файлов или печати на сетевых принтерах), запуске различных служб и заданий планировщика и т.д. Т.е. очень много лишних событий, которые не относятся ко входу локального пользователя. Чтобы выбрать только события интерактивного входа пользователя на консоль компьютера, нужно дополнительно сделать выборку по значению параметра Logon Type. В таблице ниже перечислены коды Logon Type.

При удаленном подключении к рабочему столу компьютера по RDP, в журнале событий появится записи с Logon Type 10 или 3.

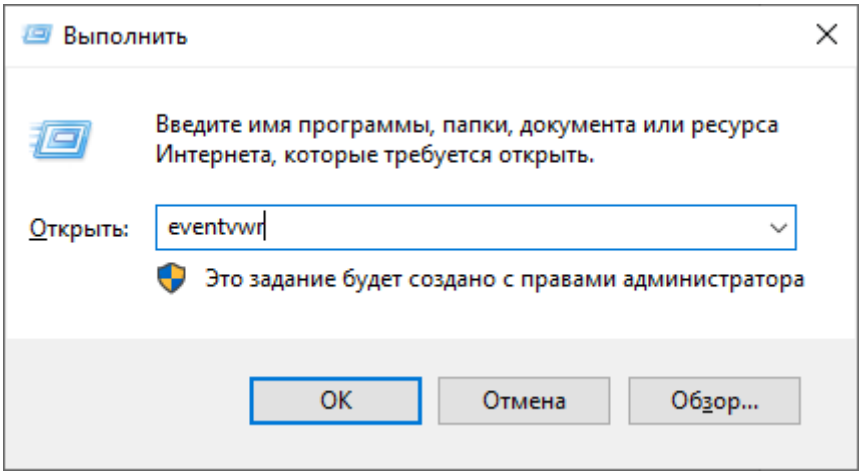
В соответствии с этой таблицей событие локального входа пользователя на компьютер должно содержать Logon Type: 2.

Этот код событий появляется при автоматическом входе в Windows. Для фильтрации события входа по содержать Logon Type лучше использовать PowerShell.

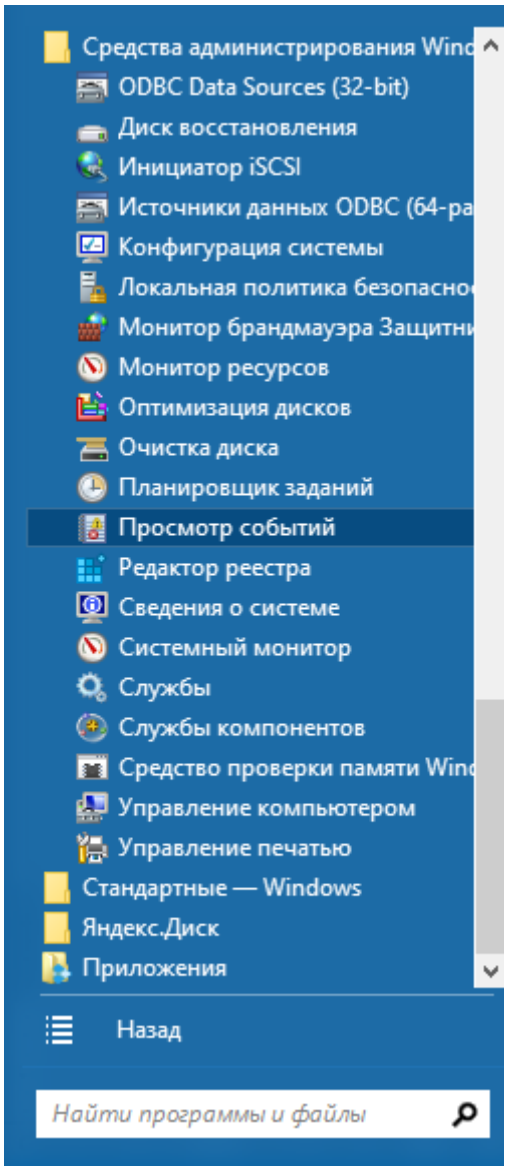
Код Logon Type	Описание
0	System
2	Interactive
3	Network
4	Batch
5	Service
6	Proxy
7	Unlock
8	NetworkCleartext
9	NewCredentials
10	RemoteInteractive
11	CachedInteractive
12	CachedRemoteInteractive
13	CachedUnlock

Порядок выполнения работы

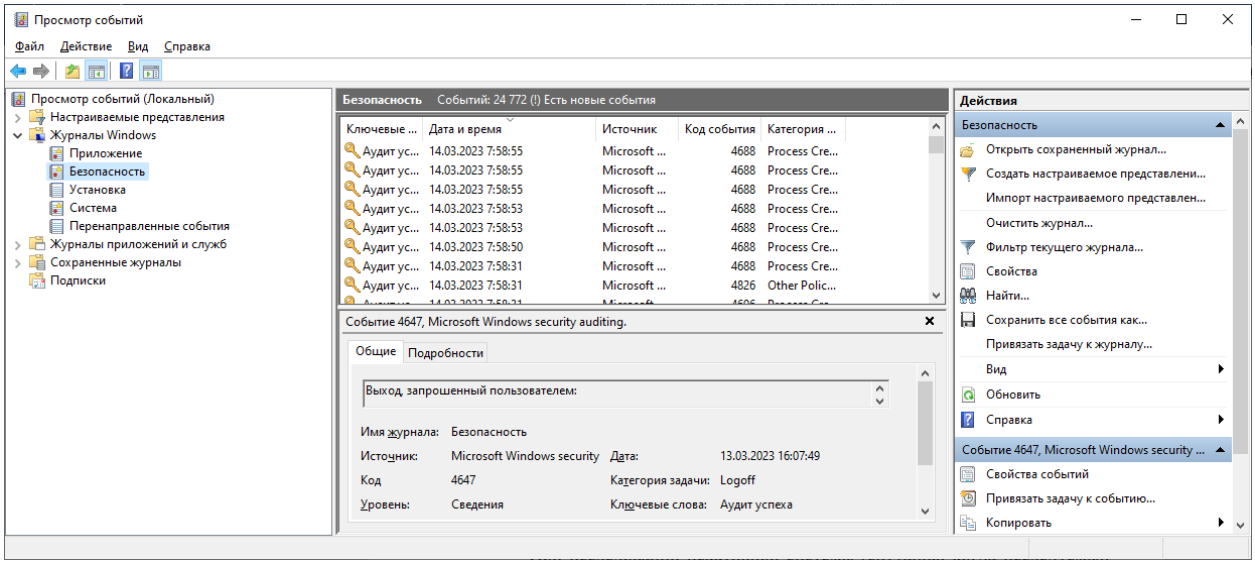
1. Исследование активной системы.
1.1. Запустить журнал событий исследуемого ПК несколькими способами.
1.1.1 Выполнить команду «Пуск\Выполнить\eventvwr



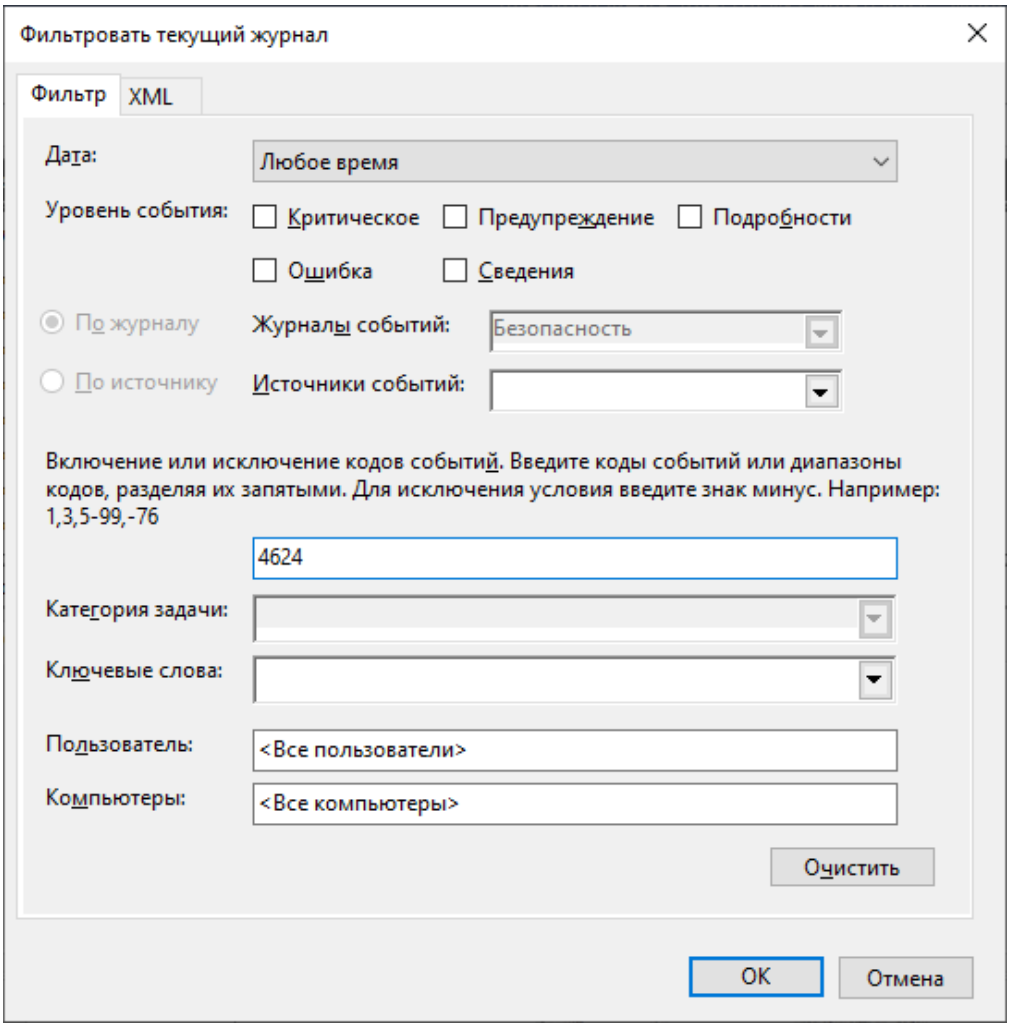
1.1.2 Выполнить команду «Пуск\Все программы\ Средства администрирования Windows\Просмотр событий»



1.2. Обнаружить журнал Windows «Безопасность».



1.3. Установить фильтр текущего журнала 4624. Определить тип события.

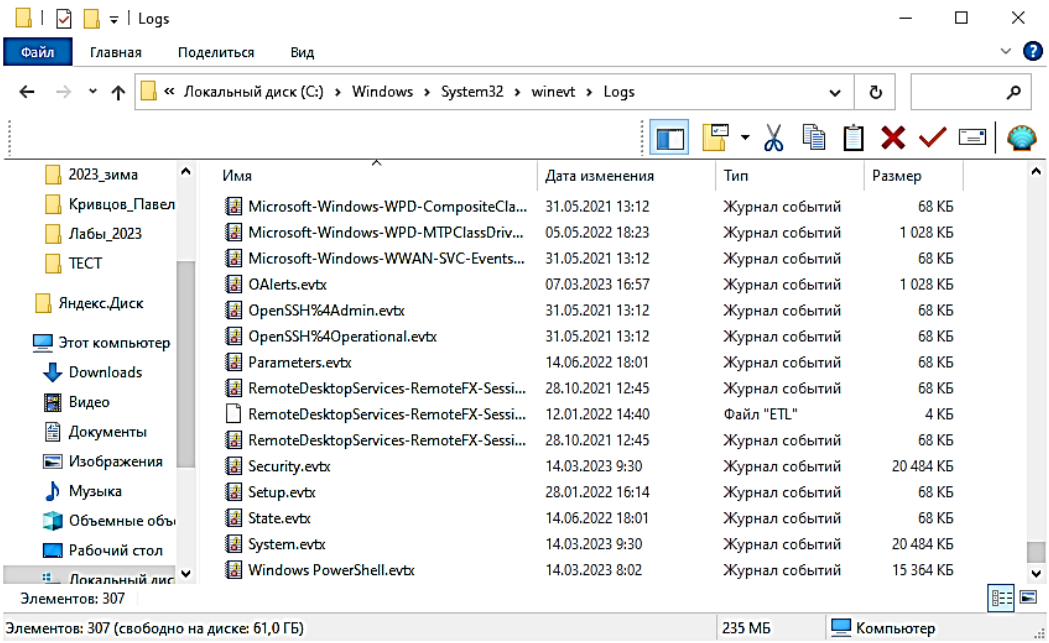


1.4. Сохранить выбранные события в текстовый файл «СобытияUSB.txt».
1.5 Провести поиск «код Logon Type» – «3». Проверить осуществлялся ли сетевой вход в систему.

2. Исследование неактивной системы

При исследовании неактивной системы (ситуация, когда исследуемый накопитель с операционной системой подключен к лабораторному ПК, и в момент проведения исследования запущена лабораторная ОС) после введения команд или выбора пунктов меню, указанных в разделе № 1 данной лабораторной работы, будут обнаружены сведения лабораторной системы. Для обнаружения сведений на исследуемом накопителе с незапущенной операционной системой необходимо выполнить следующие действия.

2.1. Обнаружить файлы журналов событий в каталоге исследуемого накопителя \Windows\System32\winevt\Logs\.



2.2. С помощью программы AccessData FTK Imager или R-Studio экспортировать файлы журналов событий во временный каталог.
2.3. Открыть экспортированные файлы с помощью стандартного средства «Просмотр событий» лабораторного ПК.
2.4. Выполнить пункты 1.3-1.5 с помощью стандартного средства «Просмотр событий» по отношению к экспортированным файлам журналов событий.
3. Сравнить полученные в пунктах 1 и 2 сведения. Сделать соответствующие выводы.

Контрольные вопросы

1. В каком каталоге находятся файлы журналов событий?
2. Какая криминалистически значимая информация может содержаться в реестре?
3. Какая криминалистически значимая информация может содержаться в журналах событий?
4. С помощью каких программных продуктов возможно получение информации из журналов событий?
5. Какой код события в журнале имеют сведения о входе в систему?
6. С помощью какого программного обеспечения можно экспортировать файлы журналов событий?
7. Опишите алгоритм получения информации из файлов журналов событий при активной и неактивной системе.
8. Какой код Logon Type имеет событие сетевого входа в систему?
9. Какие EventID могут помочь при анализе работы ОС по журналам событий?
10. Какой код события в журнале имеют сведения о выходе из системы?

ЛАБОРАТОРНАЯ РАБОТА № 6

ПОЛУЧЕНИЕ СВЕДЕНИЙ ОБ ОПЕРАЦИОННОЙ СИСТЕМЕ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

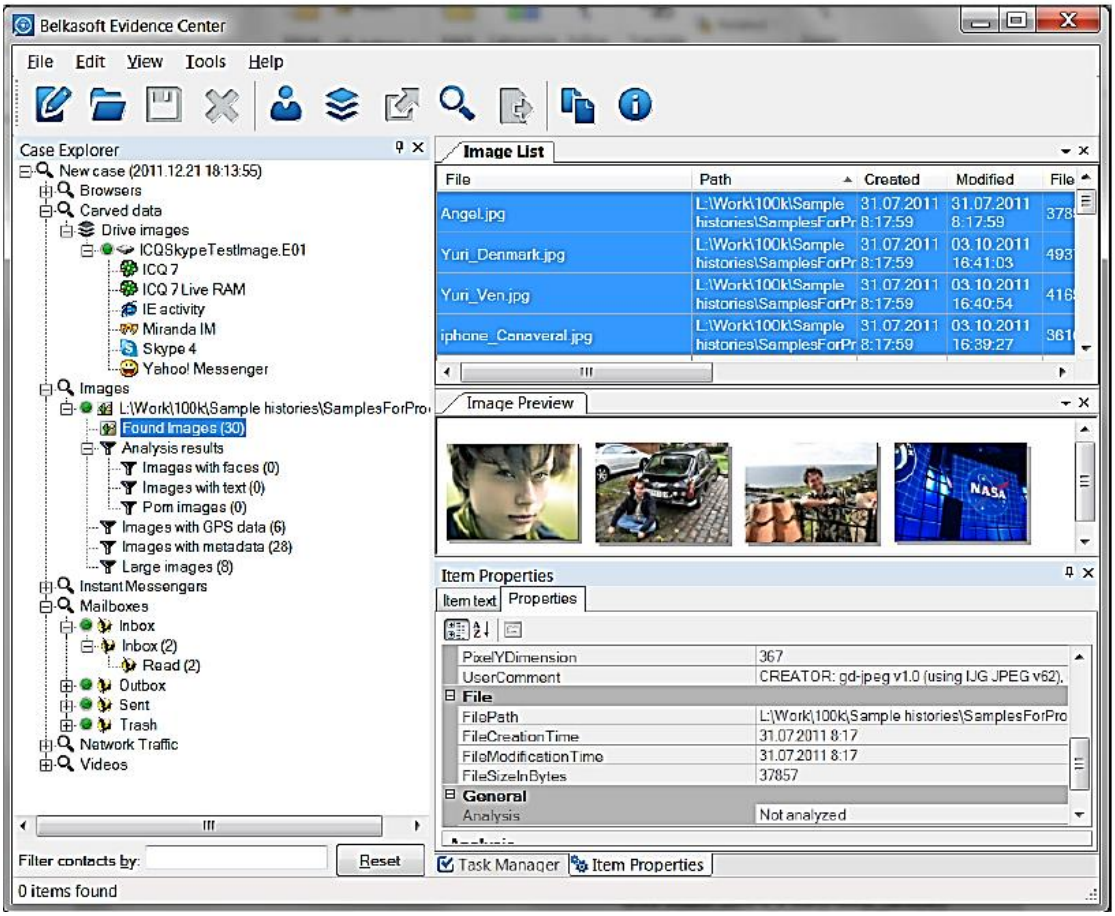


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»

- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

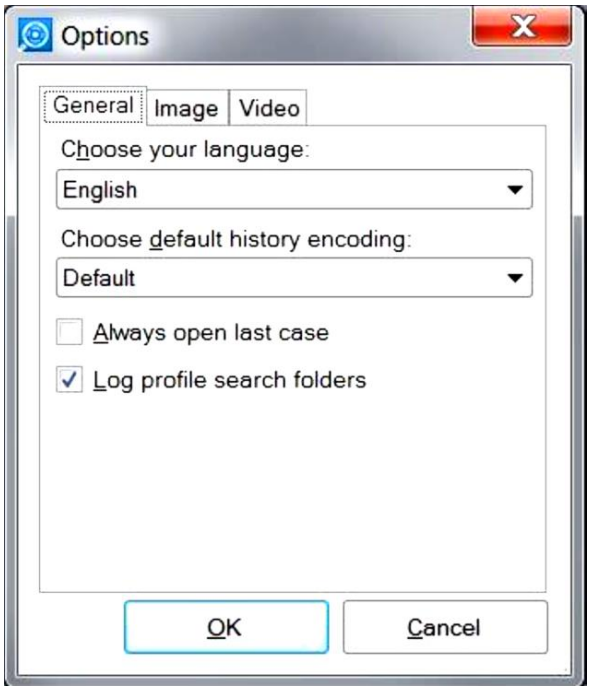


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

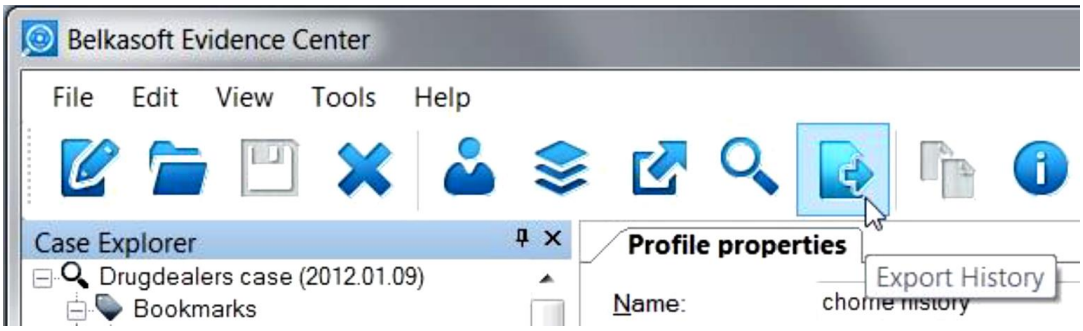


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

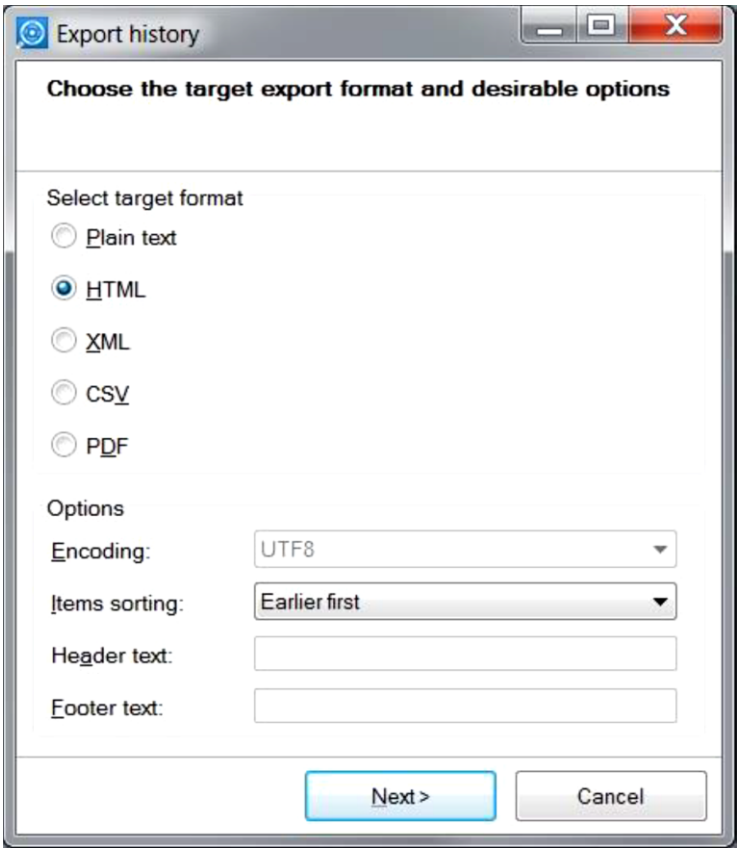


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

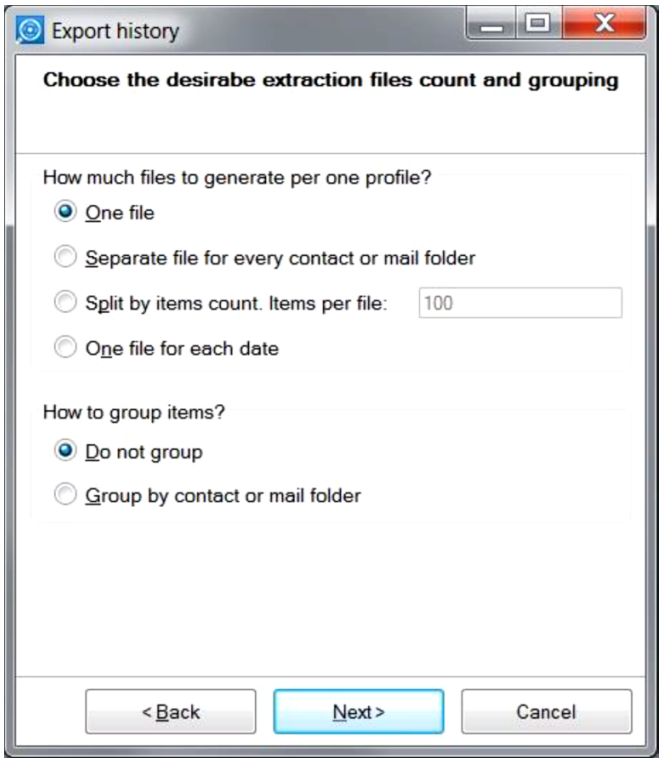


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.

- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

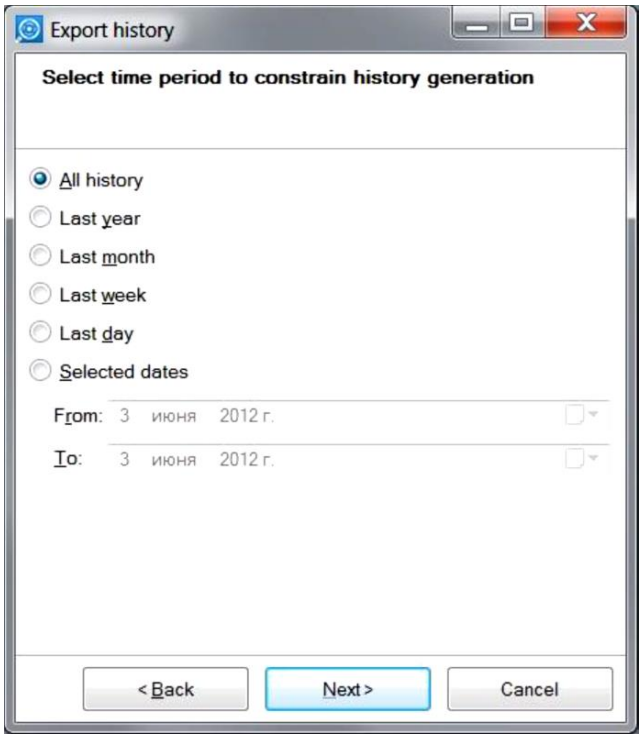


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

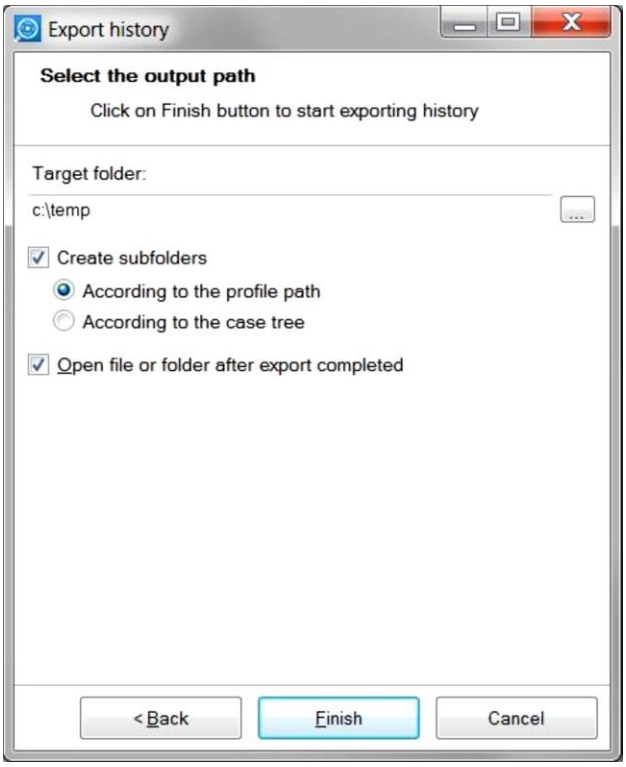


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

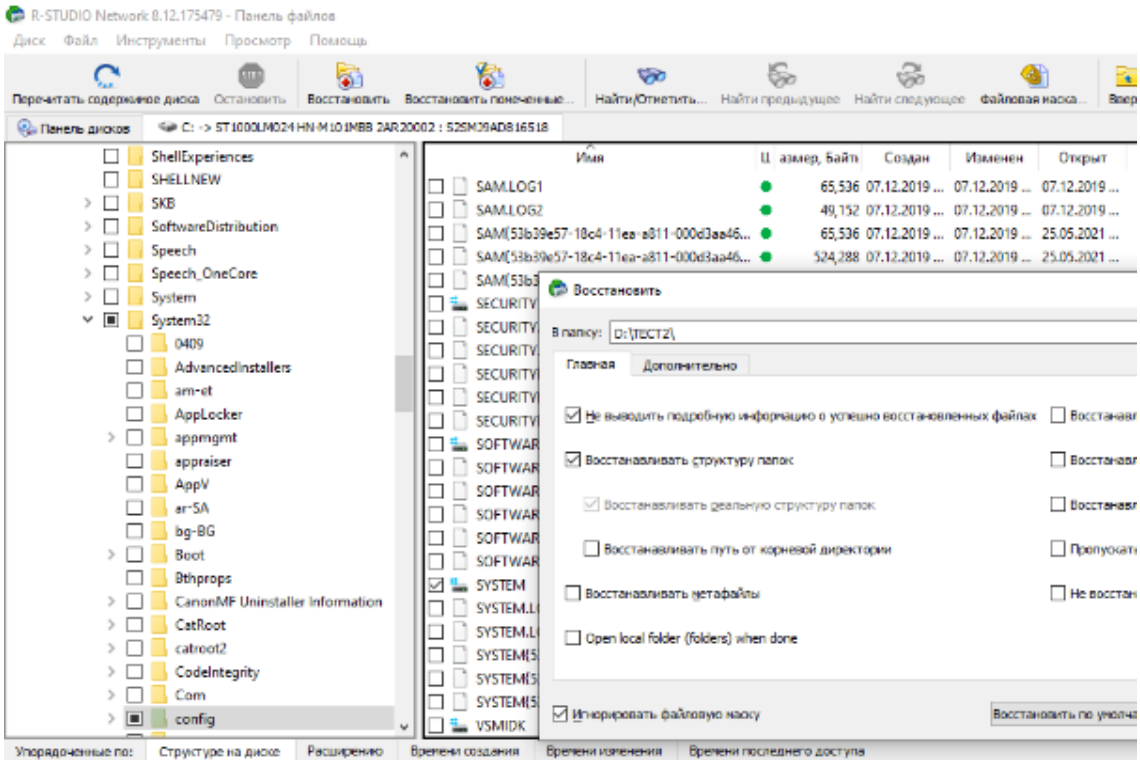
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I shan't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffed a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, perhaps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go. Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go. Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wisht you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424683493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424683493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424683493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424683493 (Aunt Polly)	Tom, I hoped you loved me that much,
IN	09.07.2009 14:49:53	424683493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you,
IN	09.07.2009 14:50:21	424683493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

1. Обнаружить файлы реестра в каталоге исследуемого накопителя \Windows\System32\config.
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталог config во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center проанализировать временный каталог.

3.1 Для этого запустить ПО Belkasoft Evidence Center.

3.2 Создать новое дело и сохранить его в заранее созданный каталог на диске D.

3.3 Добавить источник данных существующий, папка и выбрать временный каталог с файлами config.

3.4 В качестве артефактов выбрать «Системные файлы».

4. Обнаружить сведения об ОС. Название, дата и время установки, Product ID, учетные записи.

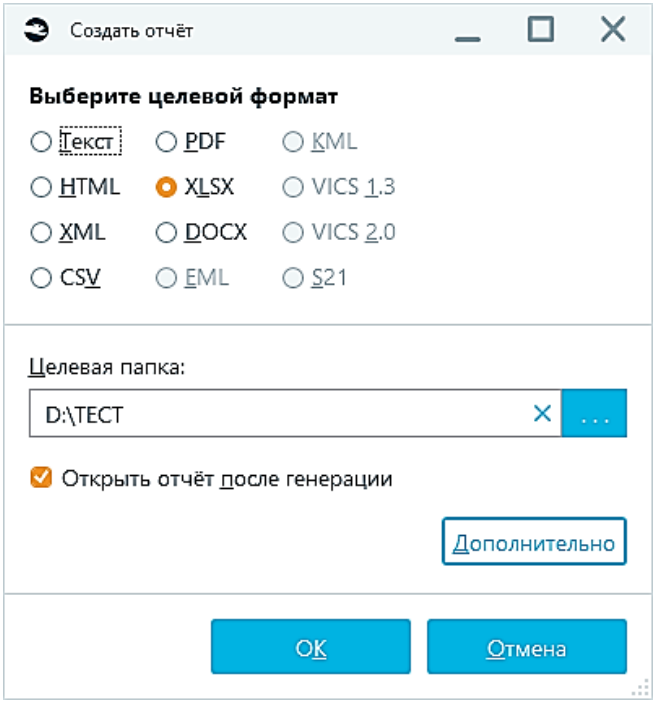
...ения	RID	Имя пользователя	
	000001F4	Администратор	02000
	000001F5	Гость	02000
	000001F7	DefaultAccount	02000
	000001F8	WDAGUtilityAccount	02000
	000003E8	Prof	02000
	000003E9	User	02000

Имя значения	Тип значения	Значение
RegisteredOwner	REG_SZ	User Windows
RegisteredOwner	REG_SZ	User Windows
ProductName	REG_SZ	Windows 10 Enterprise
ProductName	REG_SZ	Windows 10 Enterprise
ProductId	REG_SZ	00328-90000-00000-AAOEM
LastLoggedOnUser	REG_SZ	.\Prof
LastLoggedOnSAMUser	REG_SZ	.\Prof
InstallDate	REG_DWORD	
InstallDate	REG_DWORD	

Текст элемента | Hex | Реестр

2021.03.30 14:37:26

5. Создать отчет по обнаруженным сведениям в формате XLSX.



6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера, доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 7

ПОЛУЧЕНИЕ СВЕДЕНИЙ О СЕТЕВЫХ СОЕДИНЕНИЯХ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

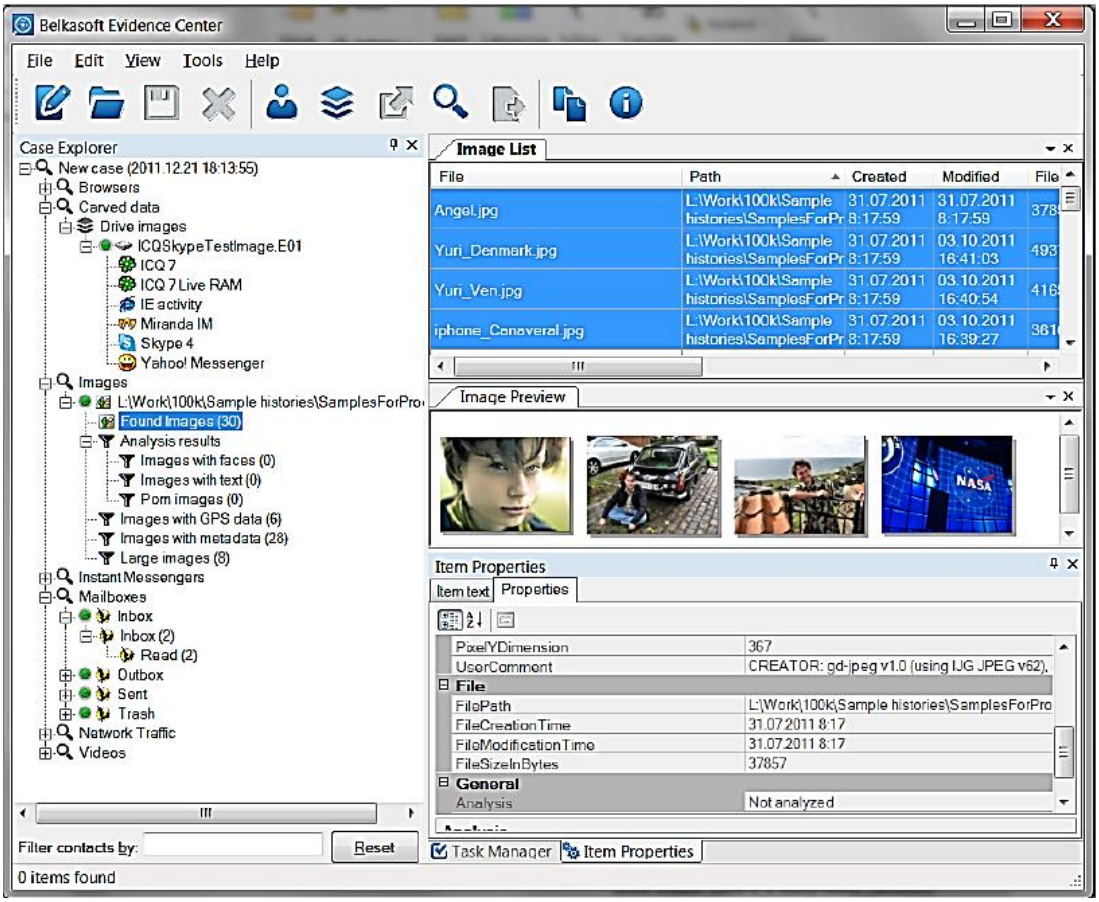


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»
- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)

- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

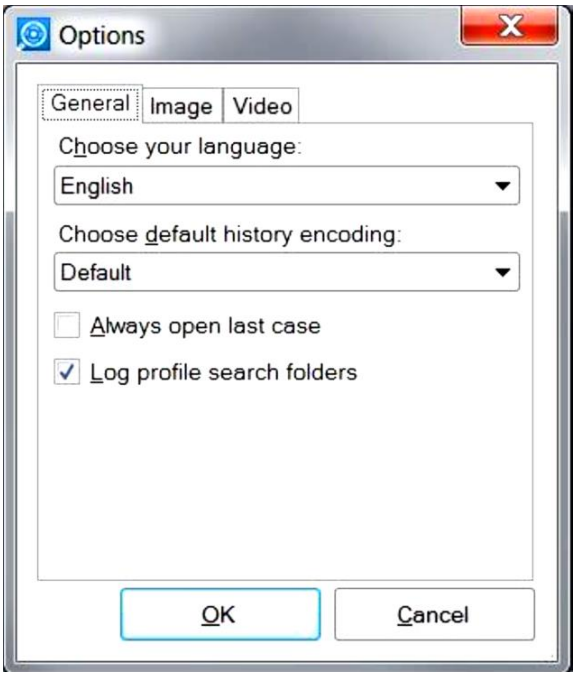


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

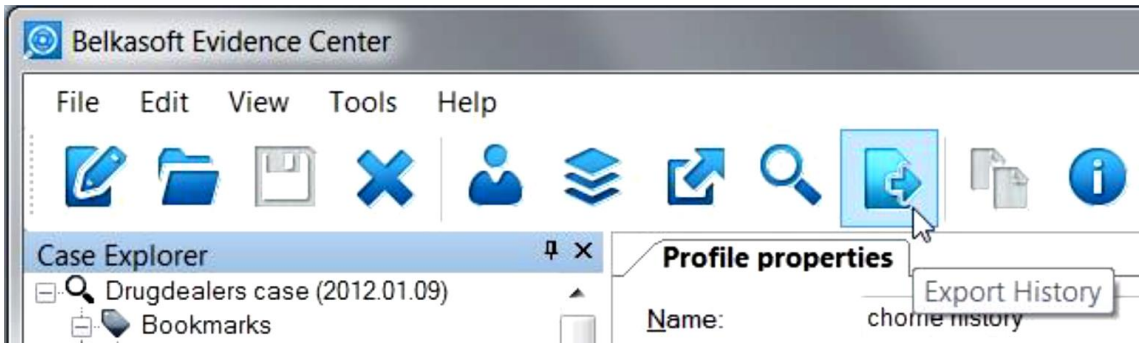


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

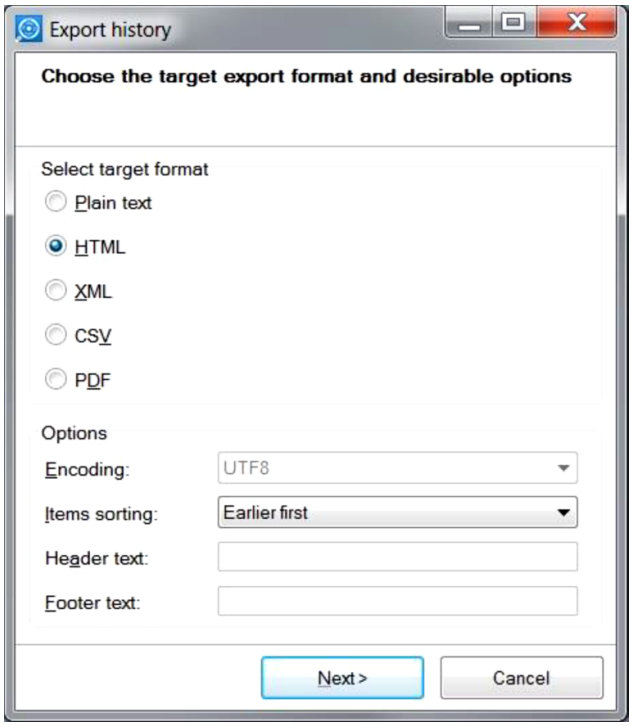


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

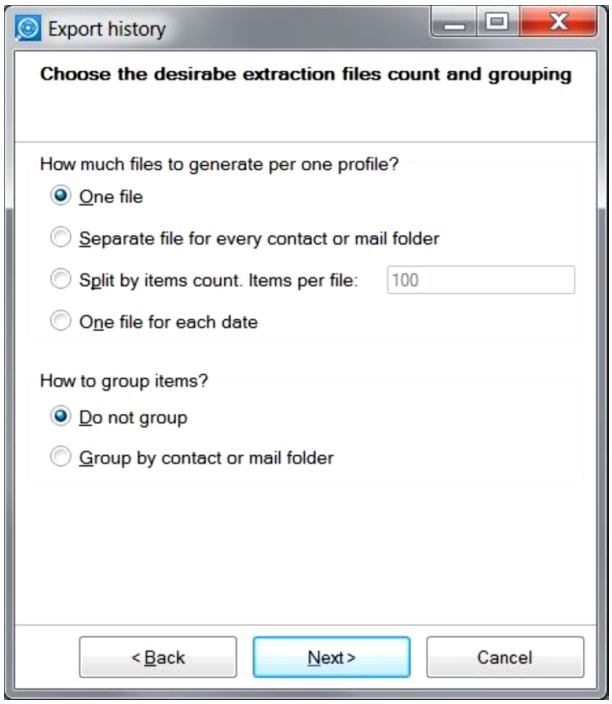


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.
- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

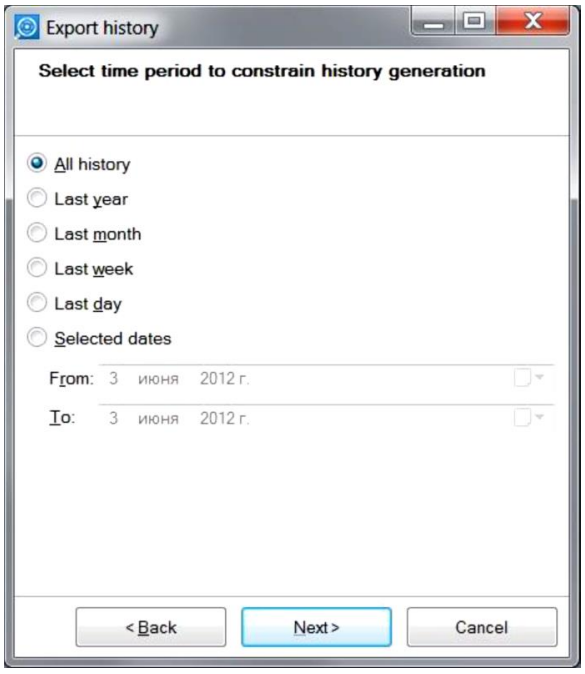


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

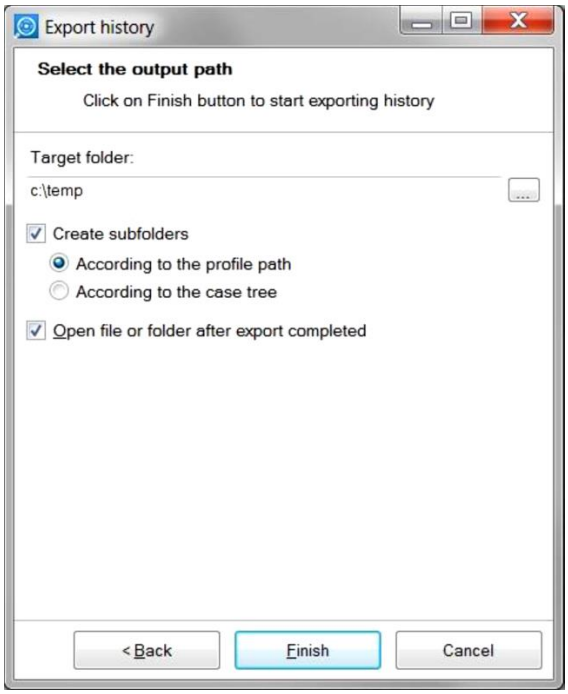


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

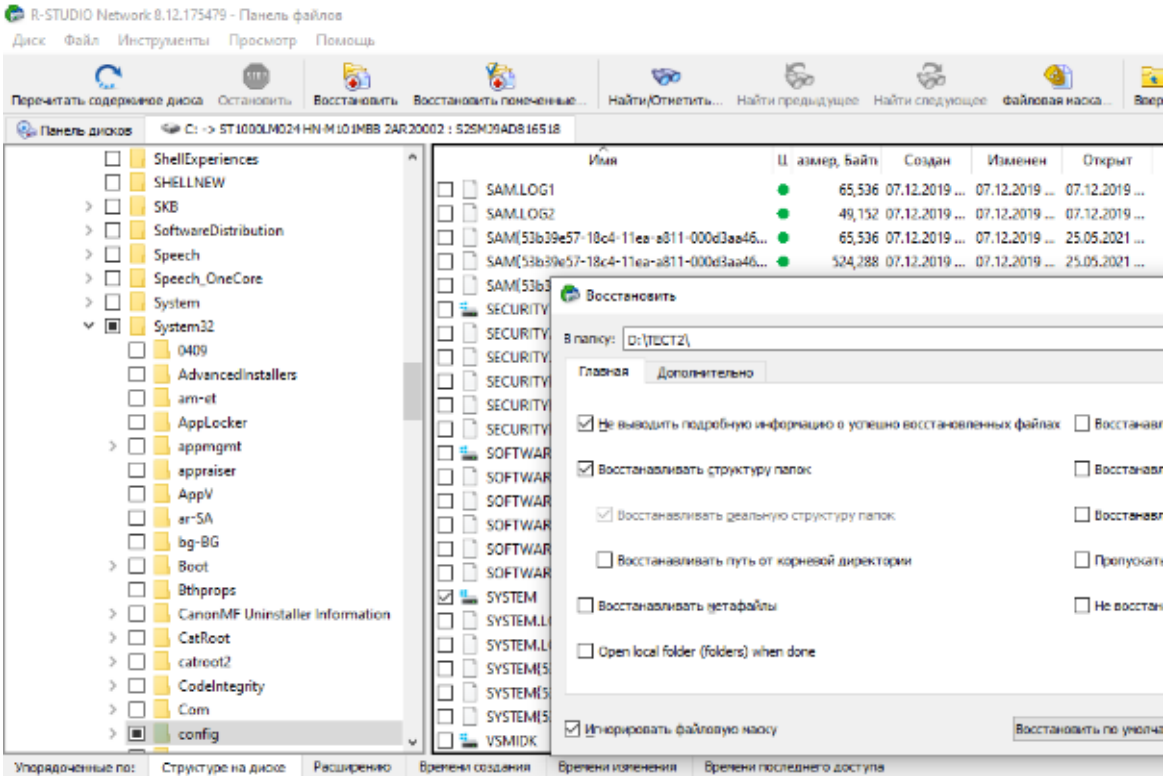
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I sha'n't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffed a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, per'aps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go. Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go, Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wisht you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424583493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering 'most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424583493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424583493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424583493 (Aunt Polly)	Tom, I hoped you loved me that much,
IN	09.07.2009 14:49:53	424583493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you,
IN	09.07.2009 14:50:21	424583493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

1. Обнаружить файлы реестра в каталоге исследуемого накопителя \Windows\System32\config.
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталог config во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center проанализировать временный каталог.

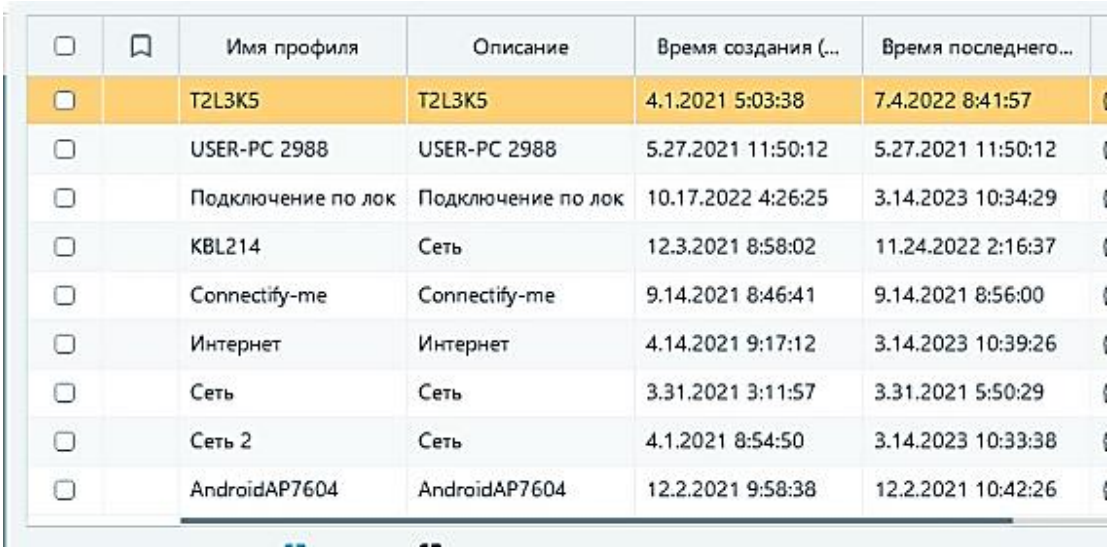
3.1. Для этого запустить ПО Belkasoft Evidence Center.

3.2. Создать новое дело и сохранить его в заранее созданный каталог на диске D.

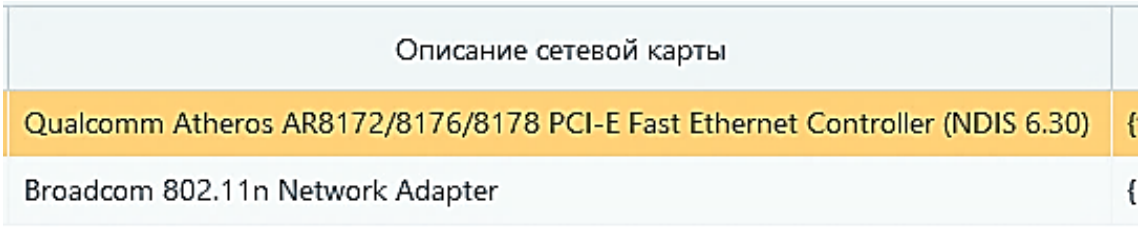
3.3. Добавить источник данных существующий, папка и выбрать временный каталог с файлами config.

3.4. В качестве артефактов выбрать «Системные файлы».

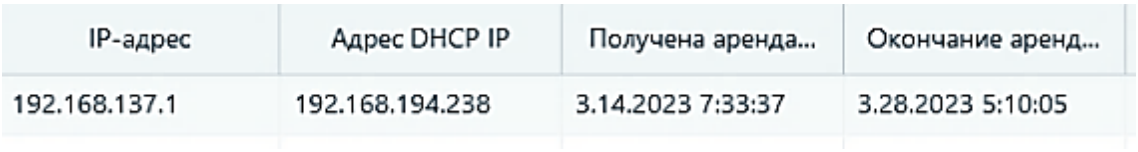
4. Обнаружить сведения о сетевых соединениях. Название сетей, дата и время подключения, сведения об IP-адресах, сведения о сетевых картах.



Имя профиля	Описание	Время создания (...	Время последнего...
T2L3K5	T2L3K5	4.1.2021 5:03:38	7.4.2022 8:41:57
USER-PC 2988	USER-PC 2988	5.27.2021 11:50:12	5.27.2021 11:50:12
Подключение по лок	Подключение по лок	10.17.2022 4:26:25	3.14.2023 10:34:29
KBL214	Сеть	12.3.2021 8:58:02	11.24.2022 2:16:37
Connectify-me	Connectify-me	9.14.2021 8:46:41	9.14.2021 8:56:00
Интернет	Интернет	4.14.2021 9:17:12	3.14.2023 10:39:26
Сеть	Сеть	3.31.2021 3:11:57	3.31.2021 5:50:29
Сеть 2	Сеть	4.1.2021 8:54:50	3.14.2023 10:33:38
AndroidAP7604	AndroidAP7604	12.2.2021 9:58:38	12.2.2021 10:42:26

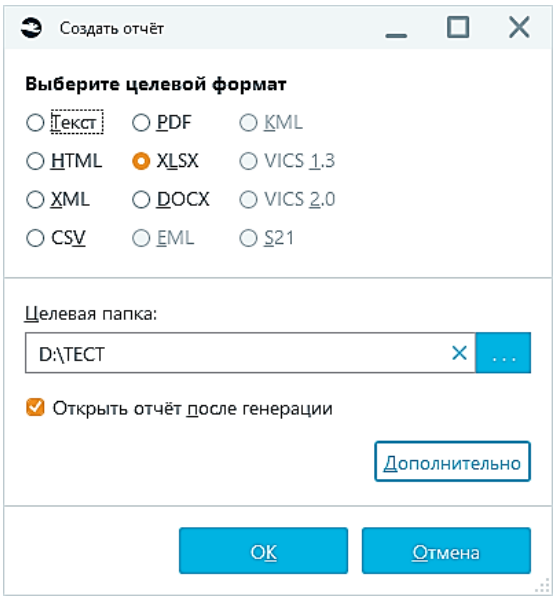


Описание сетевой карты
Qualcomm Atheros AR8172/8176/8178 PCI-E Fast Ethernet Controller (NDIS 6.30)
Broadcom 802.11n Network Adapter



IP-адрес	Адрес DHCP IP	Получена аренда...	Окончание аренд...
192.168.137.1	192.168.194.238	3.14.2023 7:33:37	3.28.2023 5:10:05

5. Создать отчет по обнаруженным сведениям в формате XLSX.



6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера, доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 8

ПОЛУЧЕНИЕ СВЕДЕНИЙ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНЫХ ПРОДУКТОВ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

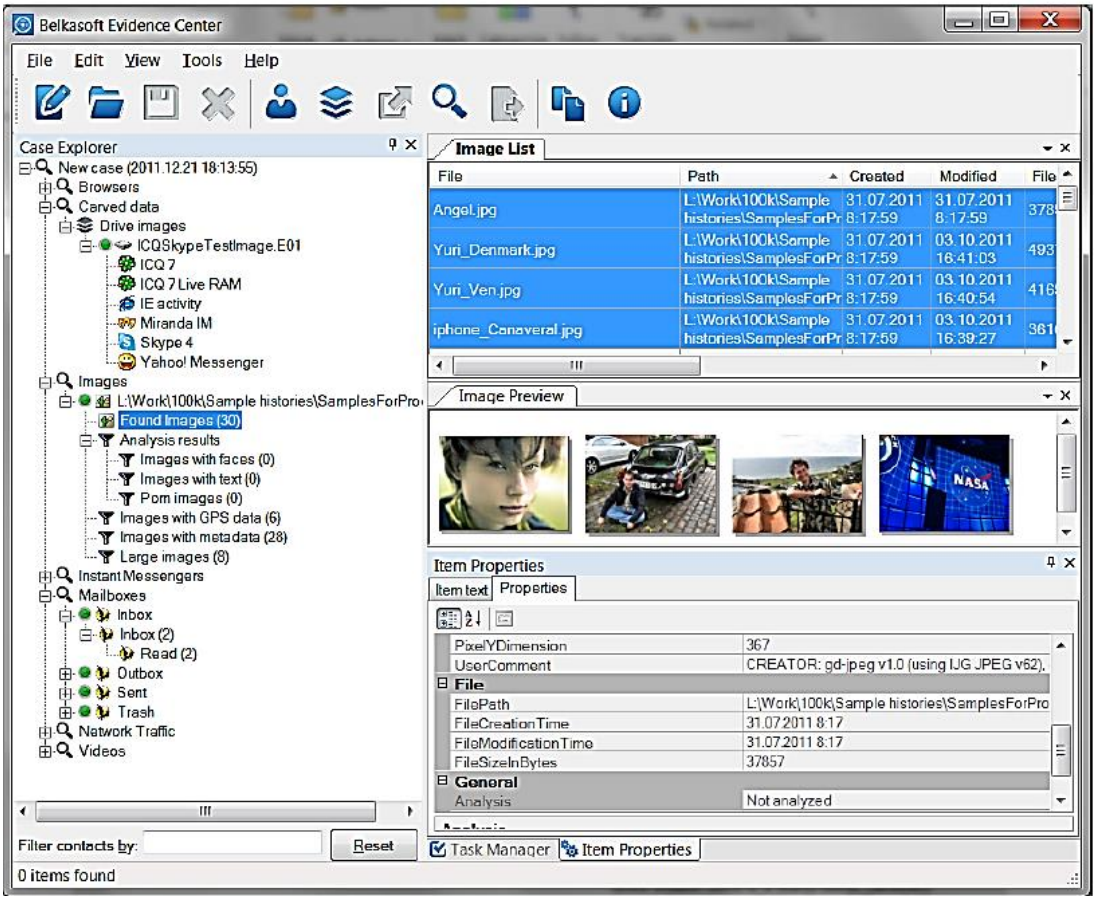


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»
- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)

- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

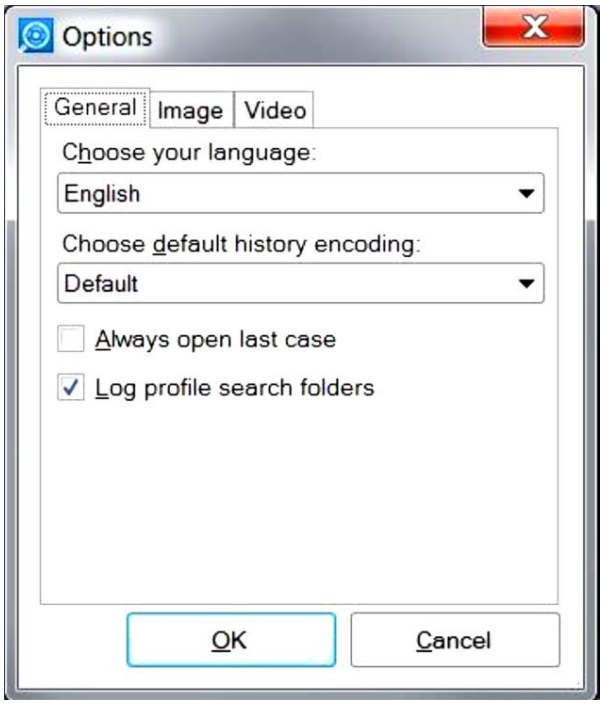


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

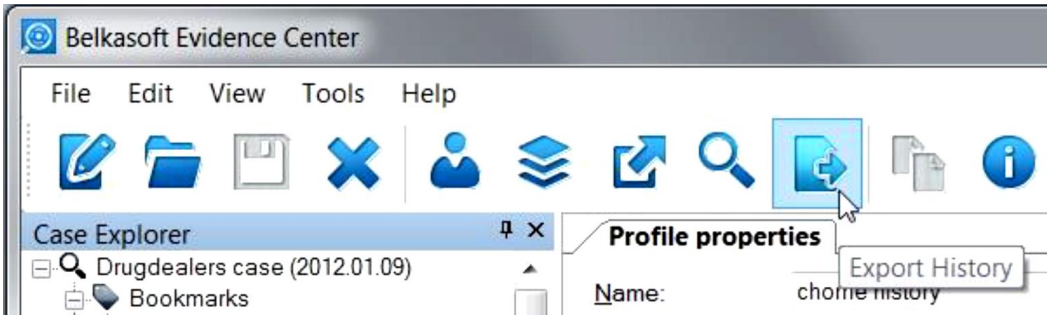


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

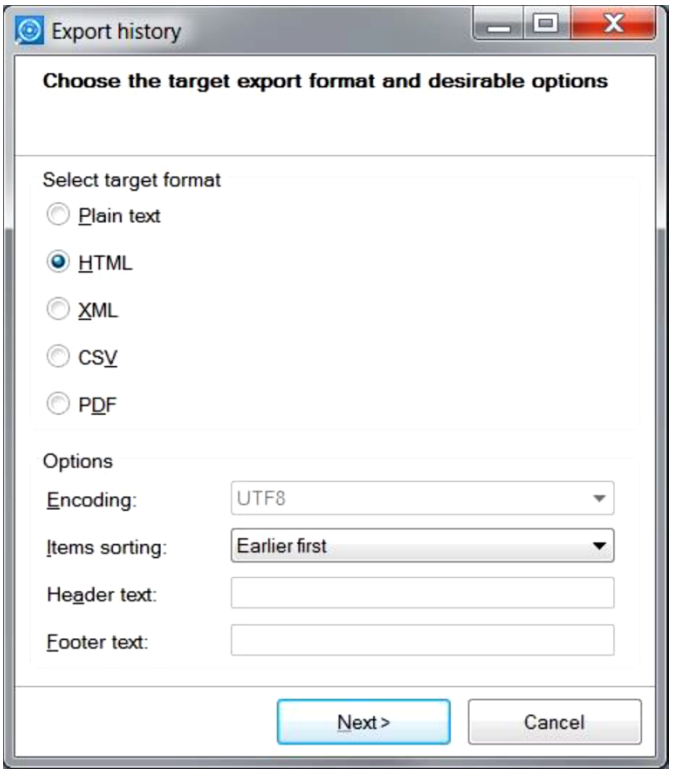


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

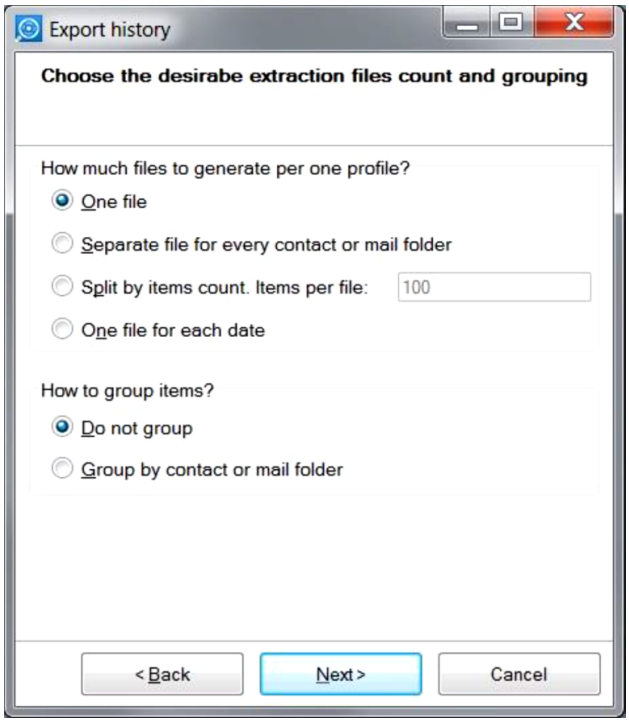


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.
- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

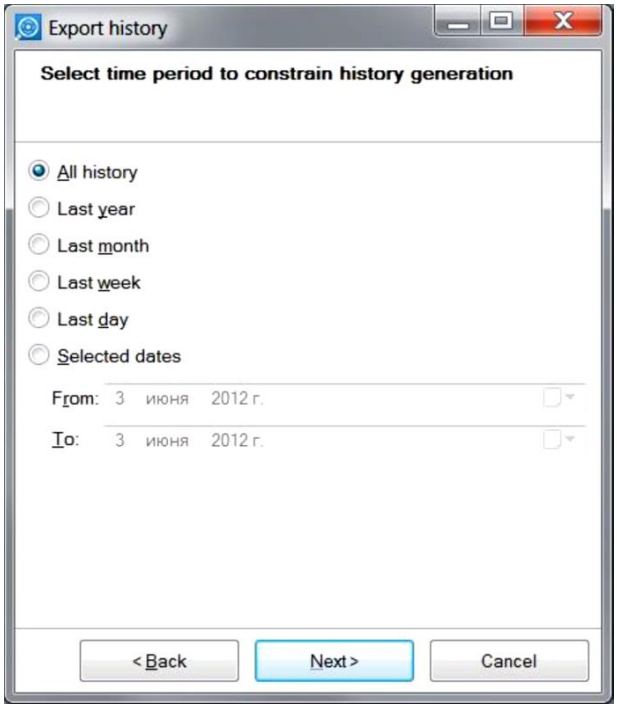


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

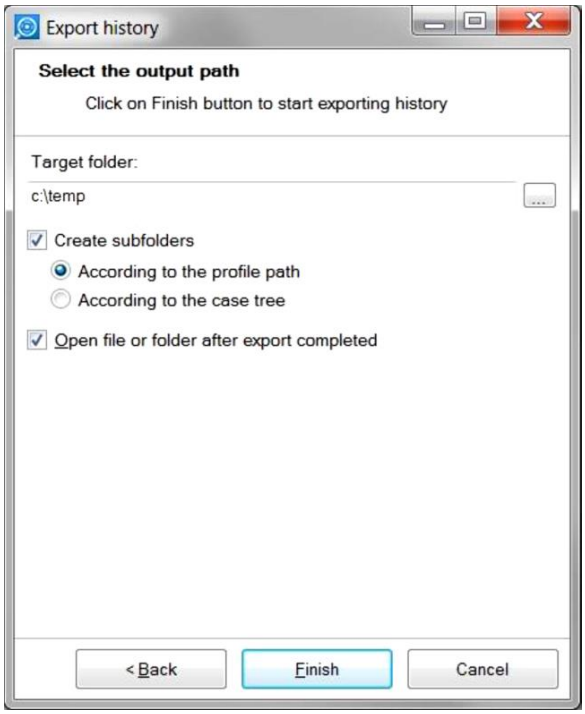


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

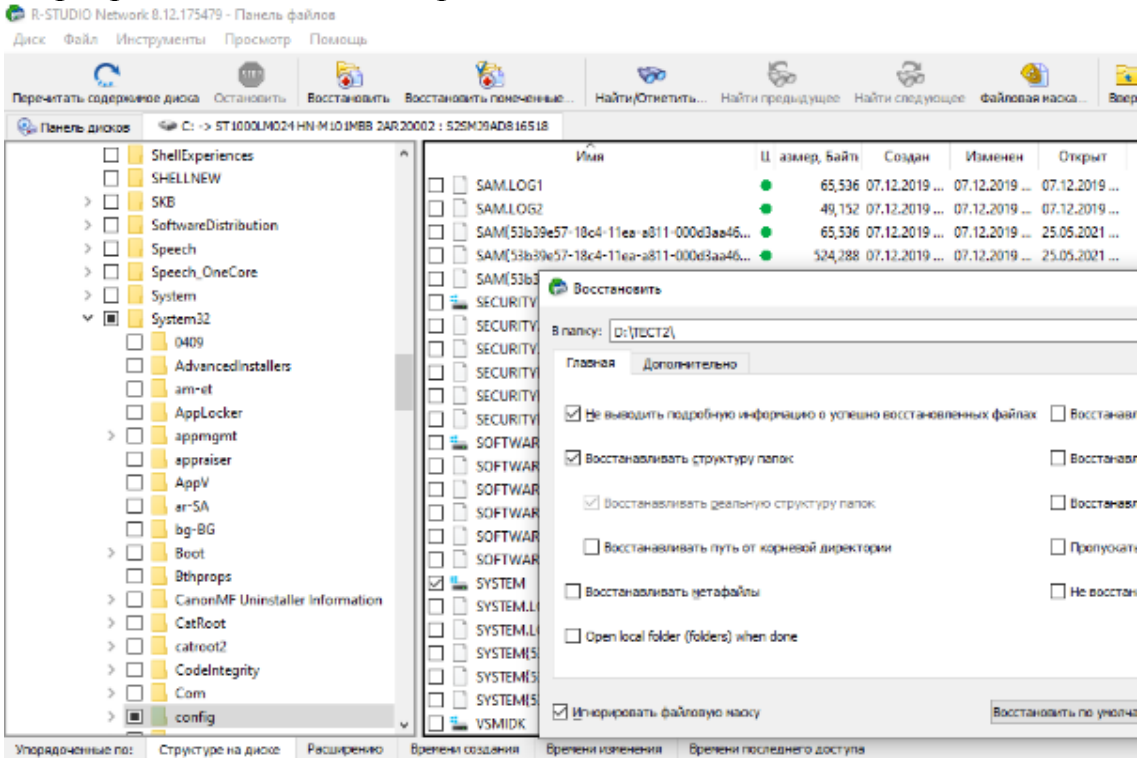
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I sha'n't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffed a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, per'aps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go. Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go, Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wisht you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424583493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424583493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424583493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424583493 (Aunt Polly)	Tom, I hoped you loved me that much.
IN	09.07.2009 14:49:53	424583493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you.
IN	09.07.2009 14:50:21	424583493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

1. Обнаружить служебные и системные каталоги на исследуемом накопителе:
\Windows\System32\config;
\Windows\Prefetch;
\Users\Professional\AppData\Roaming\Microsoft.
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталоги во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center проанализировать временный каталог.

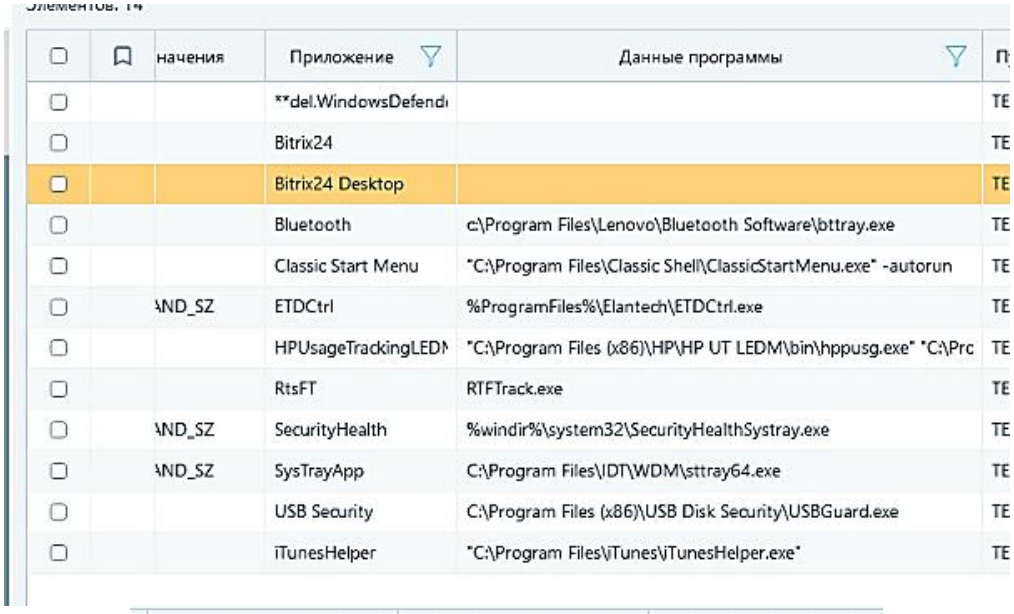
3.1 Для этого запустить ПО Belkasoft Evidence Center.

3.2 Создать новое дело и сохранить его в заранее созданный каталог на диске D.

3.3 Добавить источник данных существующий, папка и выбрать временный каталог с файлами.

3.4 В качестве артефактов выбрать «Системные файлы».

4. Обнаружить сведения об использовании программных продуктов. Название, расположение, дата и время использования, файлы, которые открывались с помощью ПО.

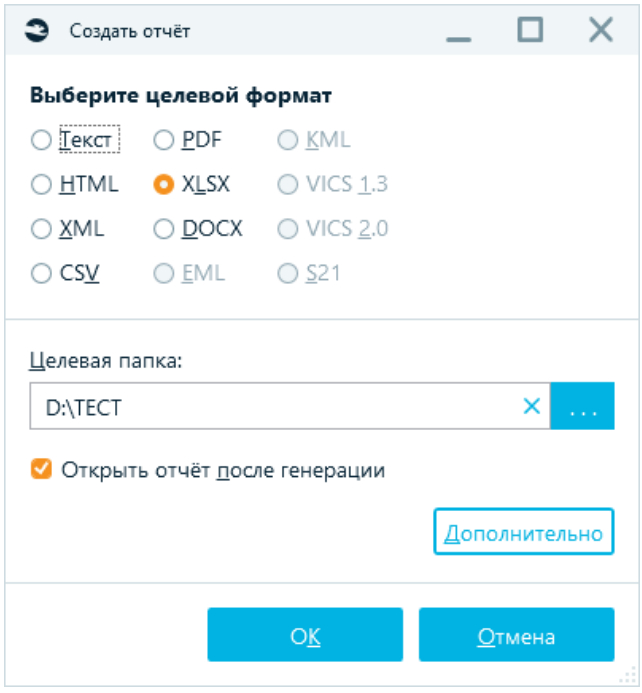


		начения	Приложение	Данные программы	
☐			**del.WindowsDefend		TE
☐			Bitrix24		TE
☐			Bitrix24 Desktop		TE
☐			Bluetooth	c:\Program Files\Lenovo\Bluetooth Software\bttray.exe	TE
☐			Classic Start Menu	"C:\Program Files\Classic Shell\ClassicStartMenu.exe" -autorun	TE
☐		ND_SZ	ETDCtrl	%ProgramFiles%\Elantech\ETDCtrl.exe	TE
☐			HPUsageTrackingLED	"C:\Program Files (x86)\HP\HP UT LEDM\bin\hppusg.exe" "C:\Prc	TE
☐			RtsFT	RTFTrack.exe	TE
☐		ND_SZ	SecurityHealth	%windir%\system32\SecurityHealthSystray.exe	TE
☐		ND_SZ	SysTrayApp	C:\Program Files\IDT\WDM\sttray64.exe	TE
☐			USB Security	C:\Program Files (x86)\USB Disk Security\USBGuard.exe	TE
☐			iTunesHelper	"C:\Program Files\iTunes\iTunesHelper.exe"	TE

Имя файла	Имя исполня...	Время пос...
WINWORD.EXE-2607I	WINWORD.EXE	3.14.2023 9:40:29
AUDIODG.EXE-BDFD3	AUDIODG.EXE	3.14.2023 9:19:19
SVCHOST.EXE-EE1C9A	SVCHOST.EXE	3.14.2023 9:13:57
WMIPRVSE.EXE-1628(	WMIPRVSE.EXE	3.14.2023 9:13:00
SPPSVC.EXE-B0F8131	SPPSVC.EXE	3.14.2023 9:12:19
EXCEL.EXE-E0855370.	EXCEL.EXE	3.14.2023 9:12:16
SEARCHFILTERHOST.E	SEARCHFILTERHOST.E	3.14.2023 9:02:27
SEARCHPROTOCOLHC	SEARCHPROTOCOLHC	3.14.2023 9:02:26
DLLHOST.EXE-39796I	DLLHOST.EXE	3.14.2023 8:55:49
SERVICE_UPDATE.EXE-	SERVICE_UPDATE.EXE	3.14.2023 8:51:02
BROWSER.EXE-5E2FA6	APPLICATIONCLIENT.I	3.14.2023 8:45:52
CEFSHARP.BROWSERS	CEFSHARP.BROWSERS	3.14.2023 8:44:01
RSTUDIO64.EXE-01F2	RSTUDIO64.EXE	3.14.2023 8:38:57

Имя файла	Создан (U...
Bandicam.lnk	10.7.2022 9:32:39
Bandicam.lnk	10.7.2022 9:32:39
Шифрование диска BitLocker (2).lnk	10.7.2022 9:32:02
Шифрование диска BitLocker (2).lnk	10.7.2022 9:32:02
План проведения лаб. работ_1.doc.	10.7.2022 8:18:16
Журнал 5 курс КБиТЭ 2022.doc.LNK	10.7.2022 7:31:40
Журнал 4 курс КБиТЭ 2022.doc.LNK	10.7.2022 6:19:16
Downloads (15).lnk	10.7.2022 6:19:15
Downloads (15).lnk	10.7.2022 6:19:15
Рецензия_КБ_ЭНКИиРУ.doc.LNK	10.5.2022 8:01:58
Рецензия_КБ_ПиАД.doc.LNK	10.5.2022 8:01:16
Рецензия КБ_ОТОСКЭ.doc.LNK	10.5.2022 7:58:43
Рецензия_КБ_Экспертиза_носителе	10.5.2022 7:24:32

5. Создать отчет по обнаруженным сведениям в формате XLSX.



6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера доступ ко входу в учетную запись ОС Windows которого ограничен паролем?
9. В каких каталогах хранятся сведения об использовании программного обеспечения?
10. Как с помощью ПО Belkasoft Evidence Center получить сведения об использовании программного обеспечения?

ЛАБОРАТОРНАЯ РАБОТА № 9

ПОЛУЧЕНИЕ СВЕДЕНИЙ О ПОДКЛЮЧЕНИИ USB-УСТРОЙСТВ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

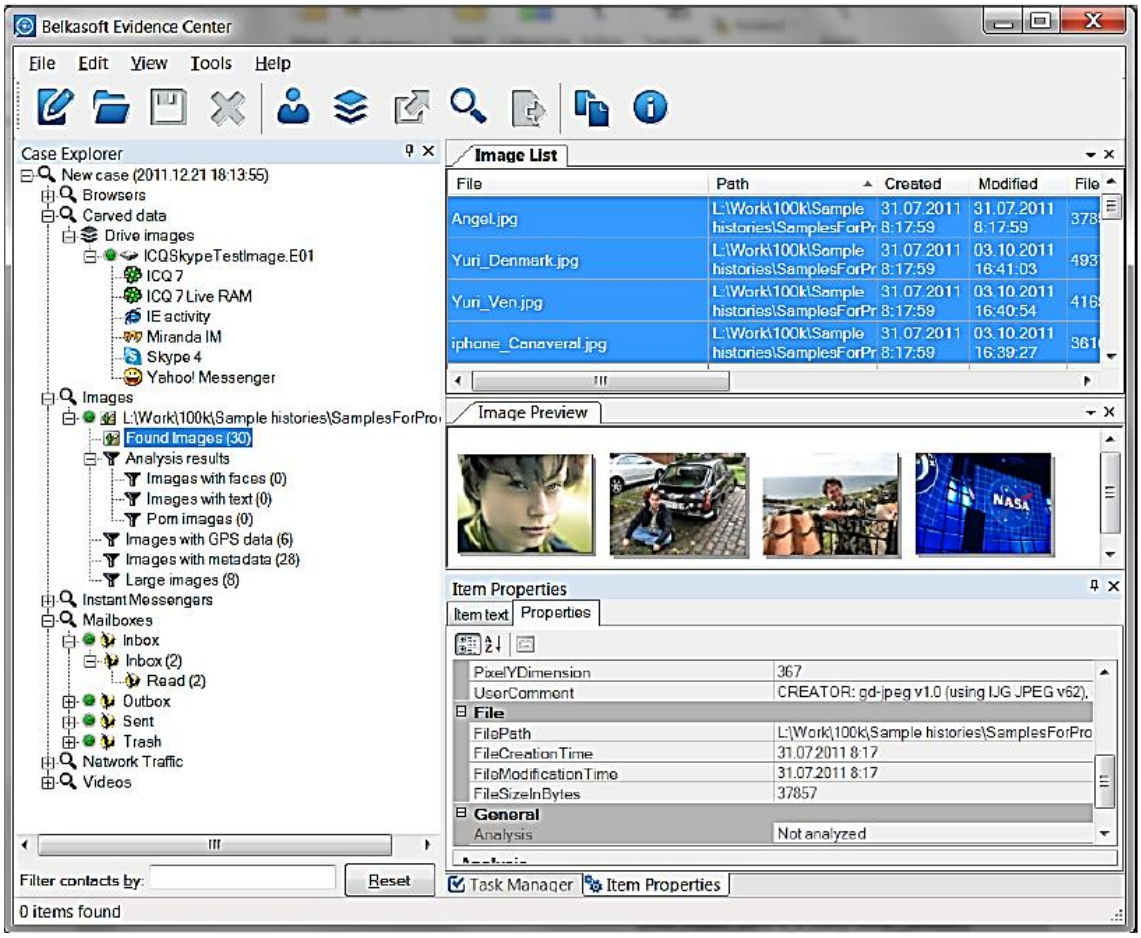


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»

- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

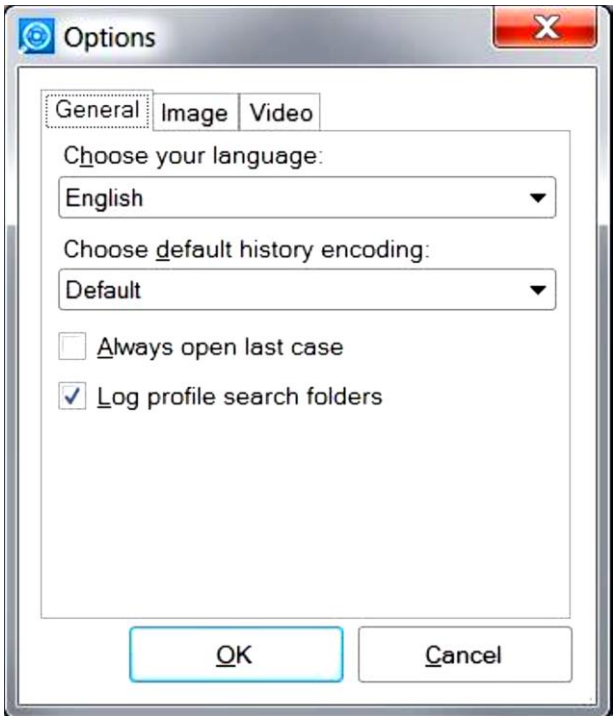


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

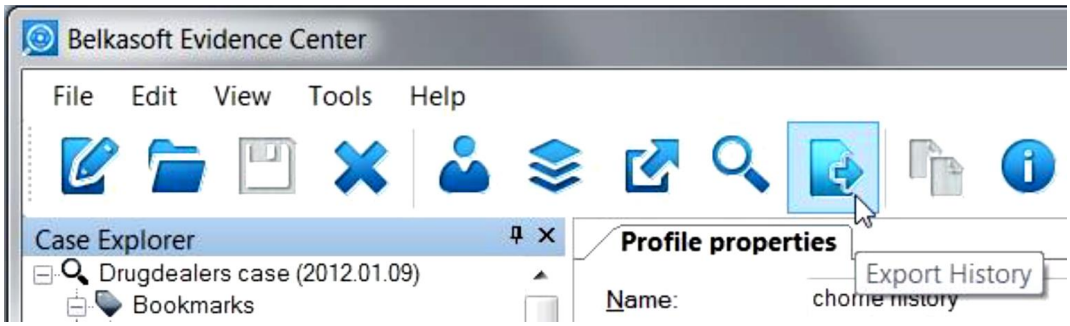


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

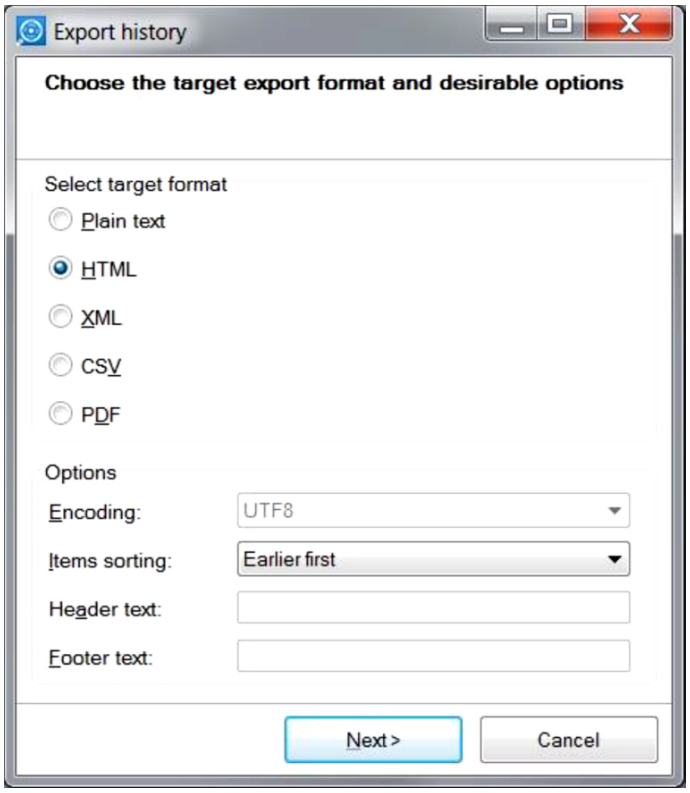


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

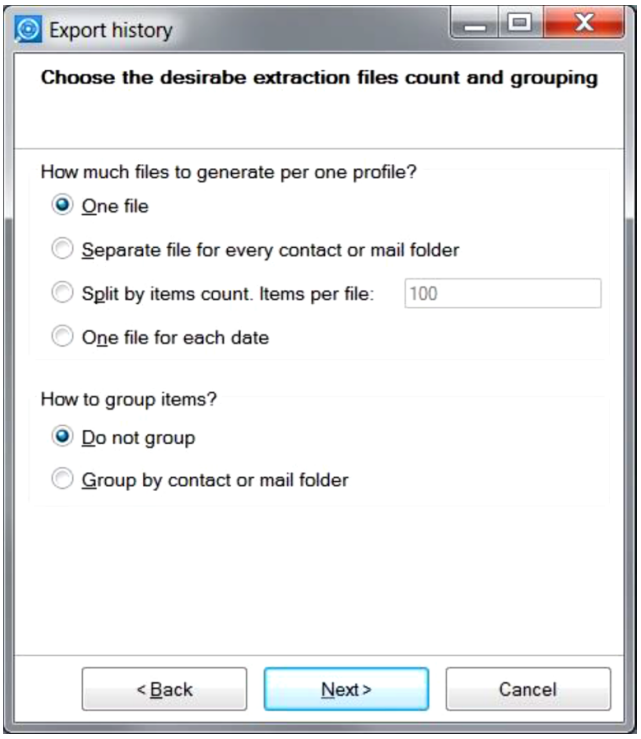


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.
- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

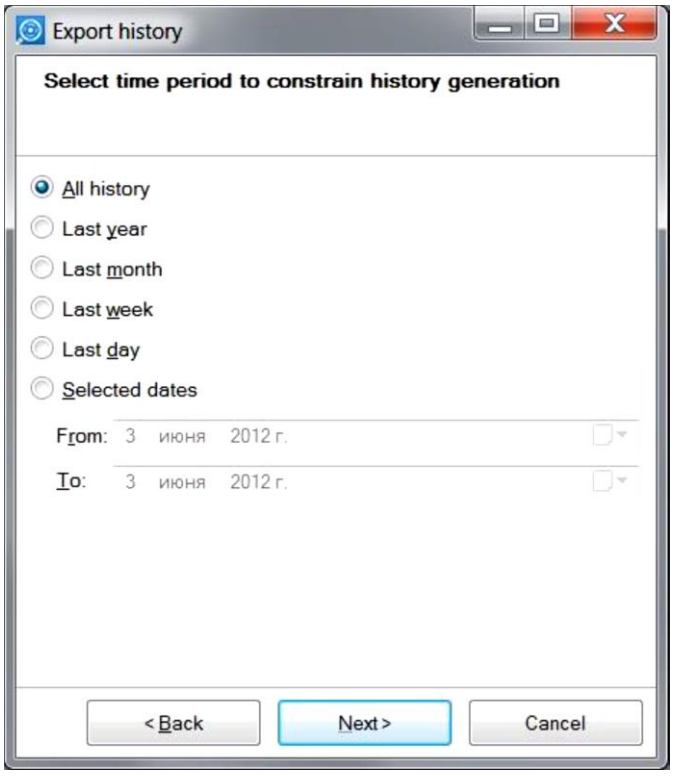


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

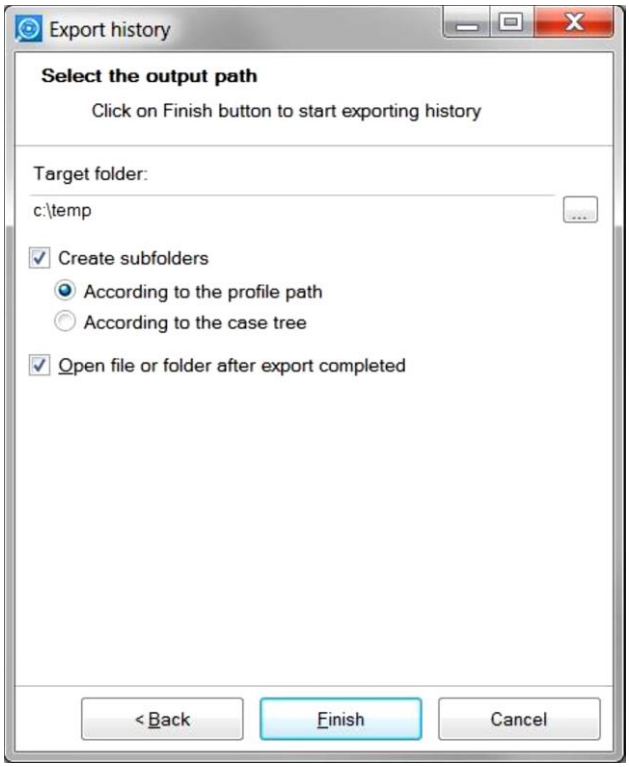


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

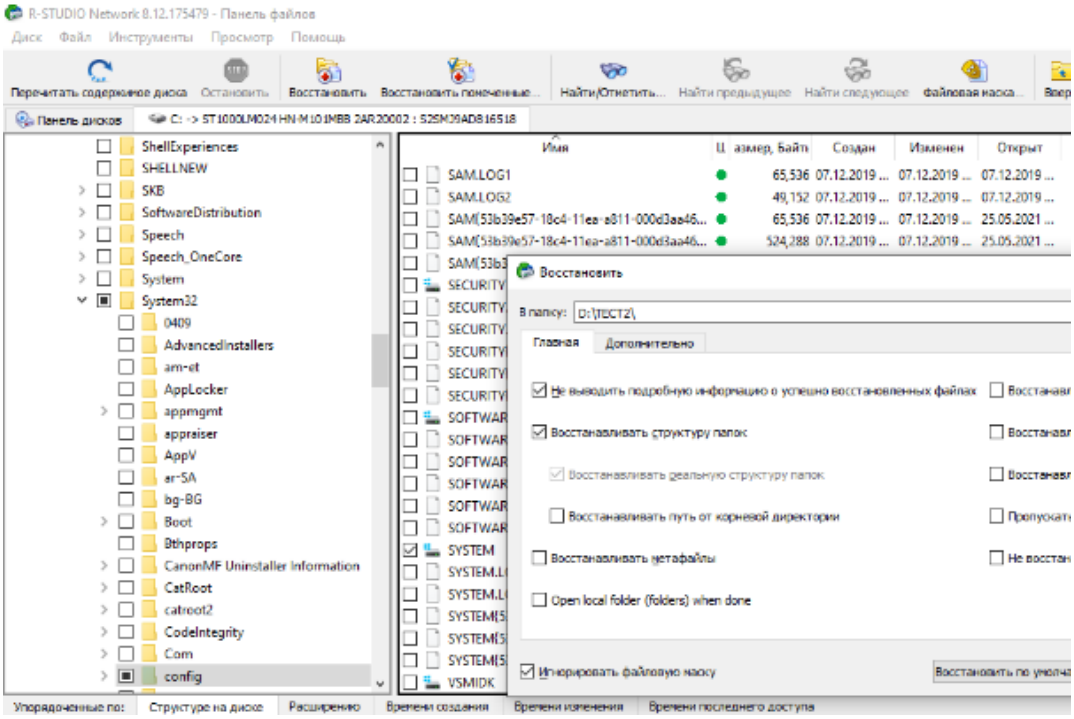
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I sha'n't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffed a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, per'aps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go. Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go, Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wisht you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424583493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering 'most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424583493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424583493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424583493 (Aunt Polly)	Tom, I hoped you loved me that much,
IN	09.07.2009 14:49:53	424583493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you,
IN	09.07.2009 14:50:21	424583493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

1. Обнаружить служебные и системные каталоги на исследуемом накопителе:
\Windows\System32\config;
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталоги во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center проанализировать временный каталог.

3.1 Для этого запустить ПО Belkasoft Evidence Center.

3.2 Создать новое дело и сохранить его в заранее созданный каталог на диске D.

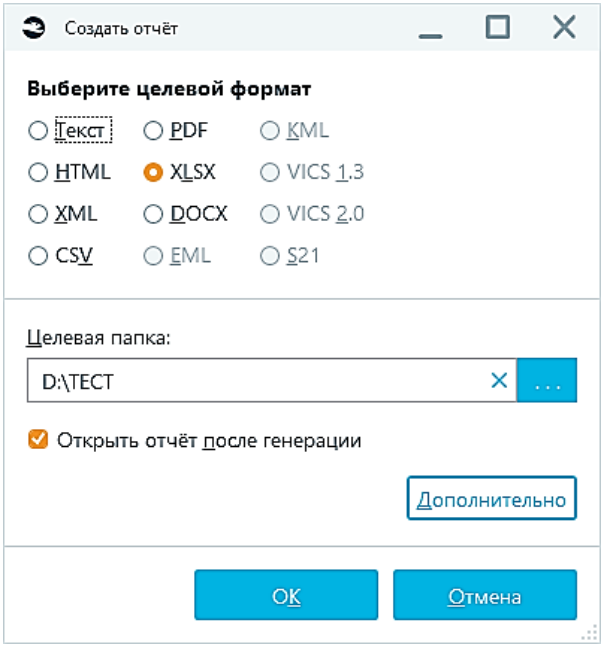
3.3 Добавить источник данных существующий, папка и выбрать временный каталог с файлами.

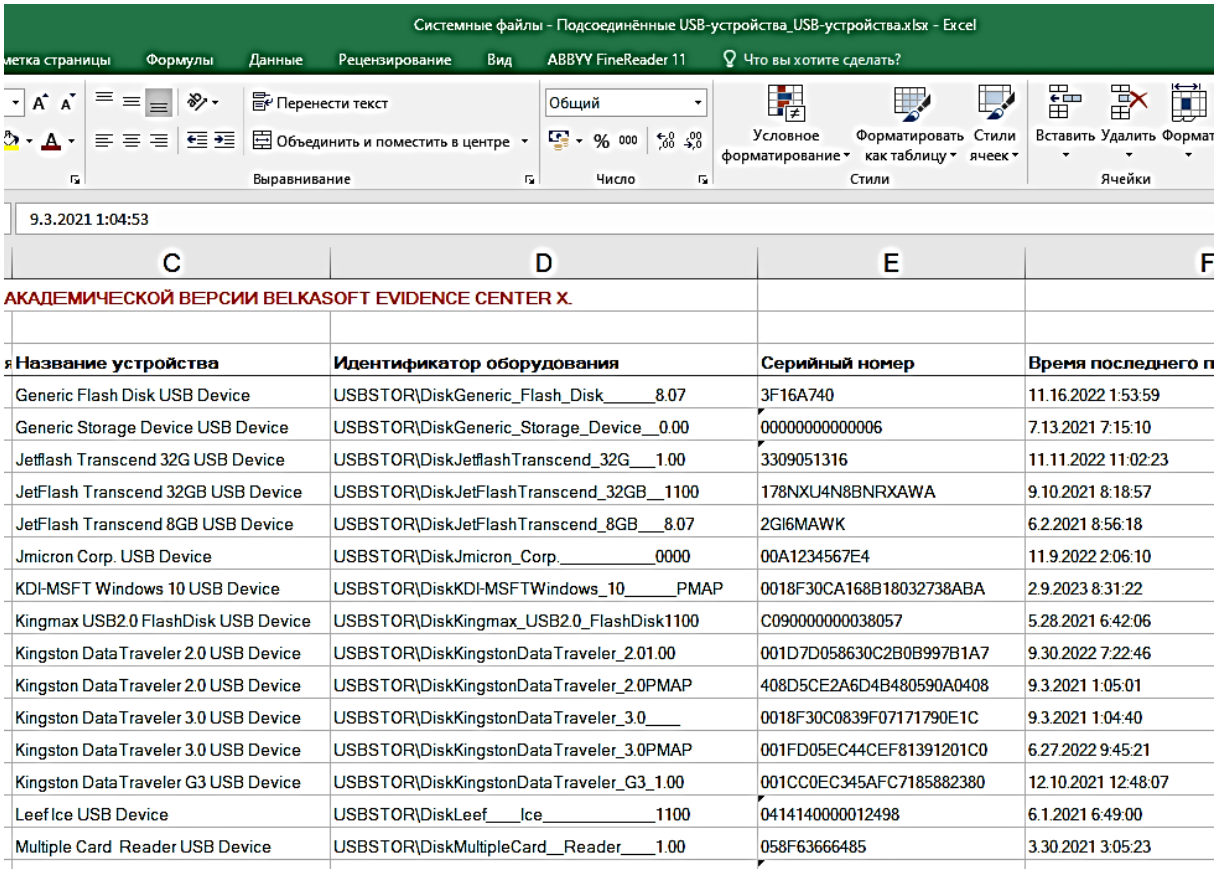
3.4 В качестве артефактов выбрать «Системные файлы».

4. Обнаружить сведения о подключении USB устройств. Название, серийный номер, дата и время подключения.

Название устройства	Серийный но...	Время последн...
Verbatim STORE N GO USB Device	19053009002068	3.1.2023 9:24:12
Verbatim STORE N GO USB Device	19053009002068	3.1.2023 9:24:12
USB Mass Storage Device	19053009002068	3.1.2023 9:24:12
USB Mass Storage Device	19053009002068	3.1.2023 9:24:12
Seagate Expansion USB Device	NA41J55J	2.25.2023 8:23:43
Seagate Expansion USB Device	NA41J55J	2.25.2023 8:23:43
USB Mass Storage Device	NA41J55J	2.25.2023 8:23:43
Seagate Expansion USB Device	NA41J55J	2.25.2023 8:23:43
USB Mass Storage Device	NA41J55J	2.25.2023 8:23:43
Seagate Expansion USB Device	NA41J55J	2.25.2023 8:23:43
USB Mass Storage Device	90000B3B87F1B032	2.15.2023 10:20:09
USB Mass Storage Device	90000B3B87F1B032	2.15.2023 10:20:09
USB Mass Storage Device	57584E32454130305	2.13.2023 7:08:22

5. Создать отчет по обнаруженным сведениям в формате XLSX.





Название устройства	Идентификатор оборудования	Серийный номер	Время последнего п
Generic Flash Disk USB Device	USBSTOR\DiskGeneric_Flash_Disk_____8.07	3F16A740	11.16.2022 1:53:59
Generic Storage Device USB Device	USBSTOR\DiskGeneric_Storage_Device__0.00	00000000000006	7.13.2021 7:15:10
Jetflash Transcend 32G USB Device	USBSTOR\DiskJetflashTranscend_32G___1.00	3309051316	11.11.2022 11:02:23
JetFlash Transcend 32GB USB Device	USBSTOR\DiskJetFlashTranscend_32GB__1100	178NXU4N8BNRXAWA	9.10.2021 8:18:57
JetFlash Transcend 8GB USB Device	USBSTOR\DiskJetFlashTranscend_8GB___8.07	2GI6MAWK	6.2.2021 8:56:18
Jmicron Corp. USB Device	USBSTOR\DiskJmicron_Corp._____0000	00A1234567E4	11.9.2022 2:06:10
KDI-MSFT Windows 10 USB Device	USBSTOR\DiskKDI-MSFTWindows_10_____PMAP	0018F30CA168B18032738ABA	2.9.2023 8:31:22
Kingmax USB2.0 FlashDisk USB Device	USBSTOR\DiskKingmax_USB2.0_FlashDisk1100	C090000000038057	5.28.2021 6:42:06
Kingston DataTraveler 2.0 USB Device	USBSTOR\DiskKingstonDataTraveler_2.01.00	001D7D058630C2B0B997B1A7	9.30.2022 7:22:46
Kingston DataTraveler 2.0 USB Device	USBSTOR\DiskKingstonDataTraveler_2.0PMAP	408D5CE2A6D4B480590A0408	9.3.2021 1:05:01
Kingston DataTraveler 3.0 USB Device	USBSTOR\DiskKingstonDataTraveler_3.0____	0018F30C0839F07171790E1C	9.3.2021 1:04:40
Kingston DataTraveler 3.0 USB Device	USBSTOR\DiskKingstonDataTraveler_3.0PMAP	001FD05EC44CEF81391201C0	6.27.2022 9:45:21
Kingston DataTraveler G3 USB Device	USBSTOR\DiskKingstonDataTraveler_G3_1.00	001CC0EC345AFC7185882380	12.10.2021 12:48:07
Leef Ice USB Device	USBSTOR\DiskLeef____Ice_____1100	0414140000012498	6.1.2021 6:49:00
Multiple Card Reader USB Device	USBSTOR\DiskMultipleCard__Reader____1.00	058F63666485	3.30.2021 3:05:23

6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера, доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 10

ПОЛУЧЕНИЕ СВЕДЕНИЙ О ДАТЕ ПОСЛЕДНЕЙ РАБОТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

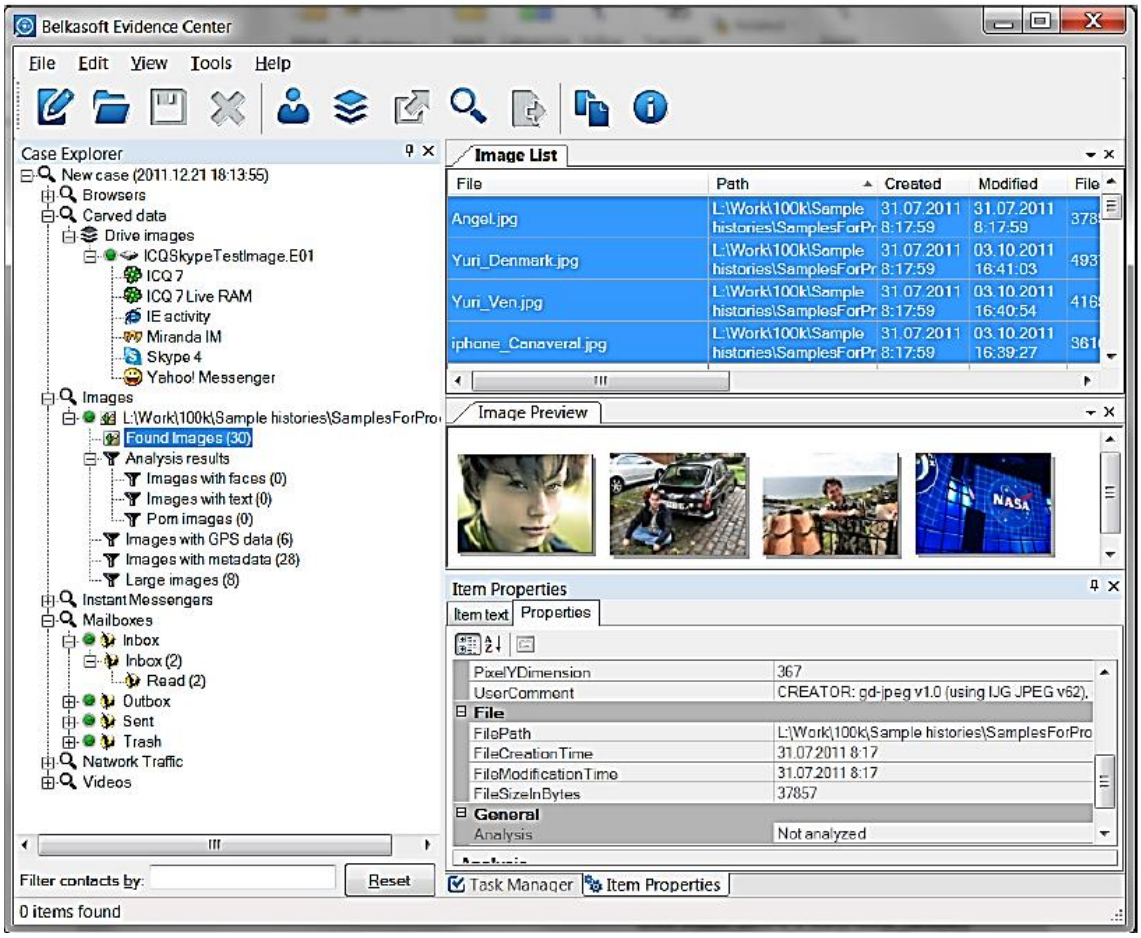


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»

- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «основные опции» содержит следующие настройки:

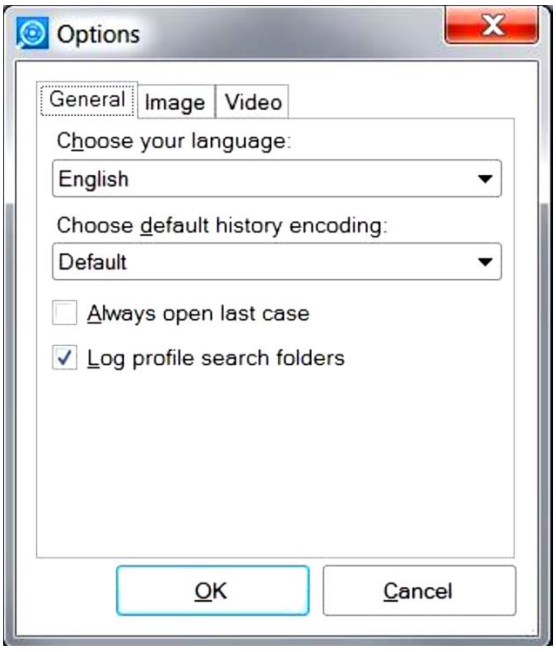


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

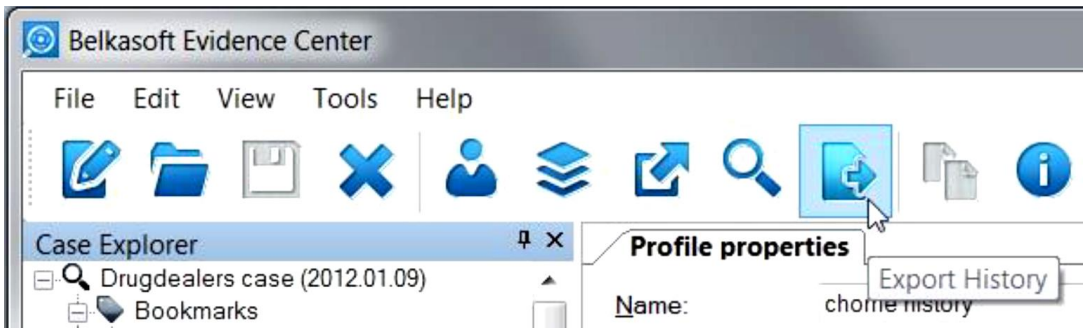


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

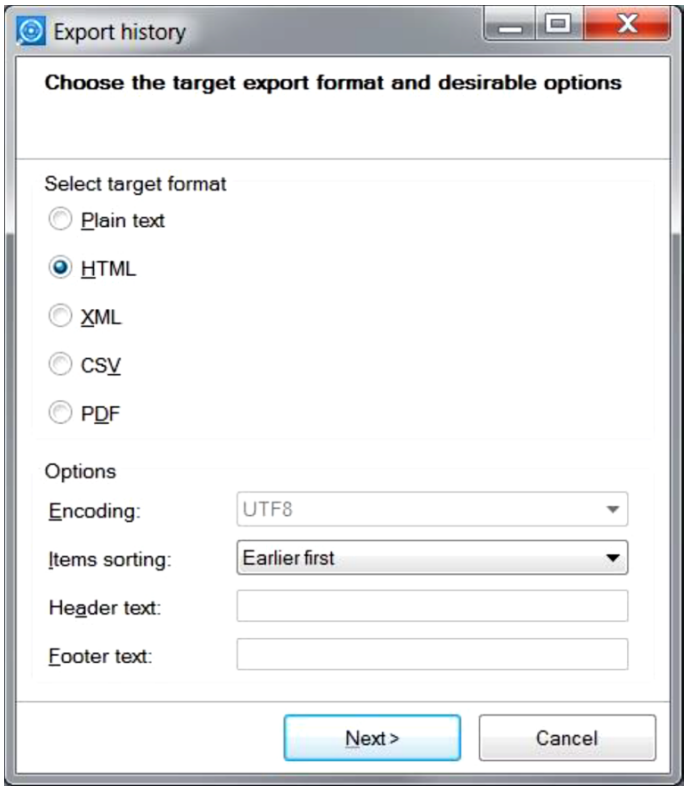


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

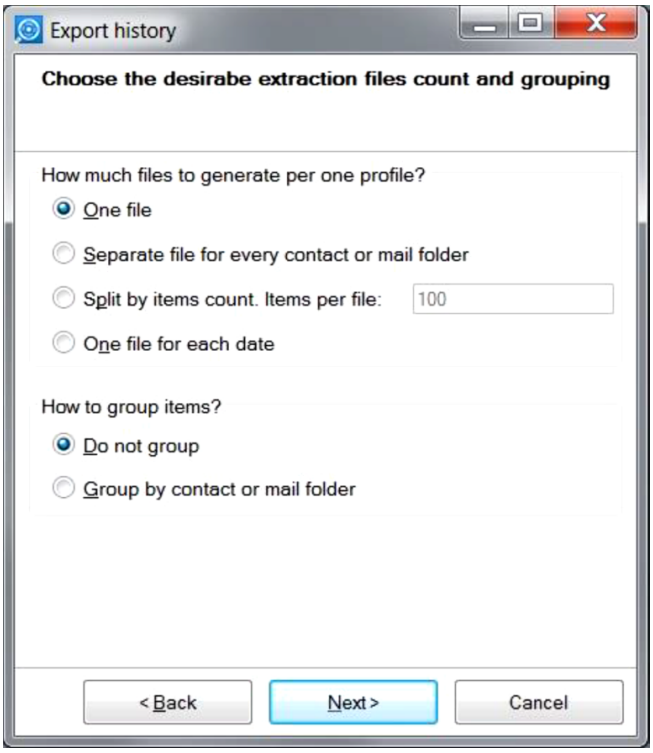


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.

- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

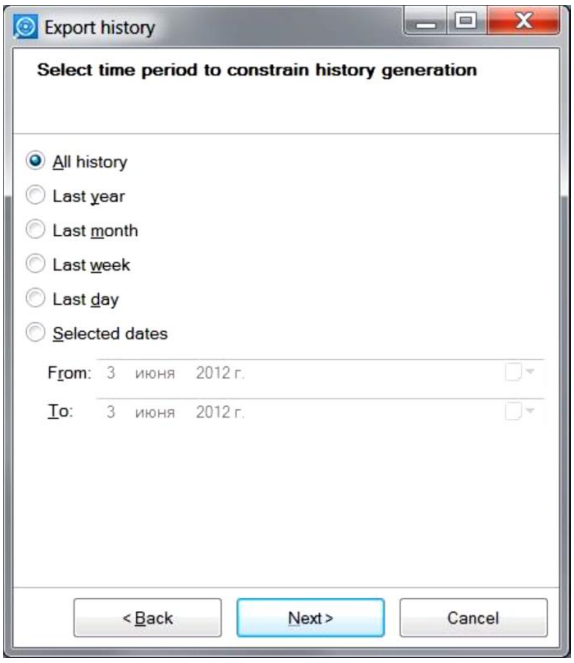


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

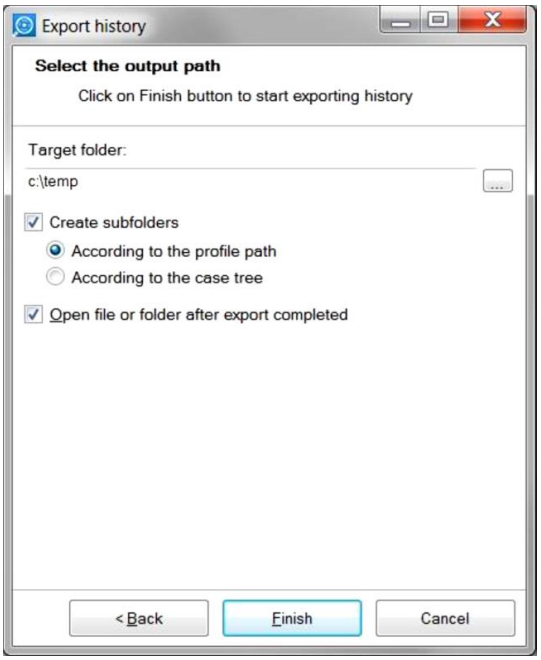


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

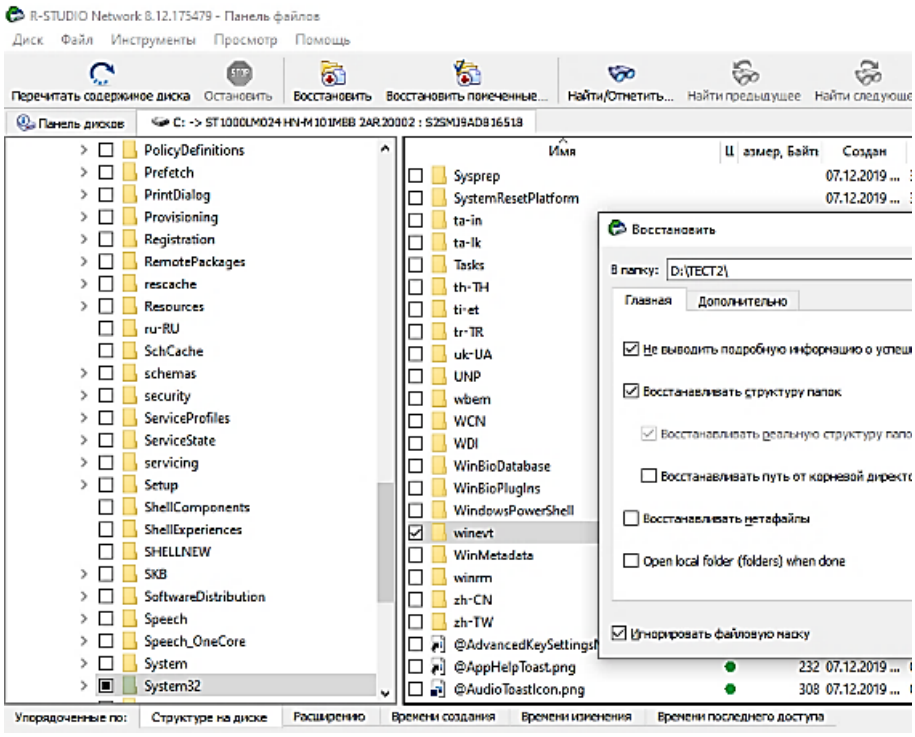
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I sha'n't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffed a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, per'aps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go, Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go, Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wish you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424583493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering 'most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424583493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424583493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424583493 (Aunt Polly)	Tom, I hoped you loved me that much,
IN	09.07.2009 14:49:53	424583493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you,
IN	09.07.2009 14:50:21	424583493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

1. Обнаружить служебные и системные каталоги на исследуемом накопителе:
\Windows\System32\winevt\;
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталоги во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center

проанализировать временный каталог.

3.1 Для этого запустить ПО Belkasoft Evidence Center.

3.2 Создать новое дело и сохранить его в заранее созданный каталог на диске D.

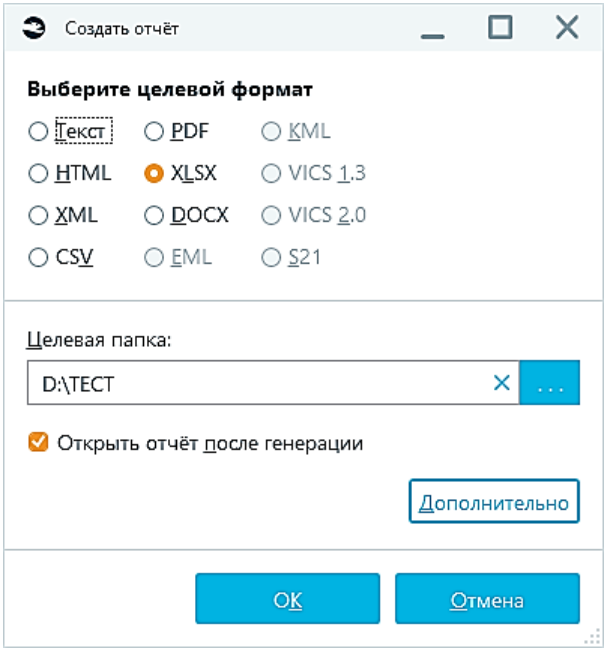
3.3 Добавить источник данных существующий, папка и выбрать временный каталог с файлами.

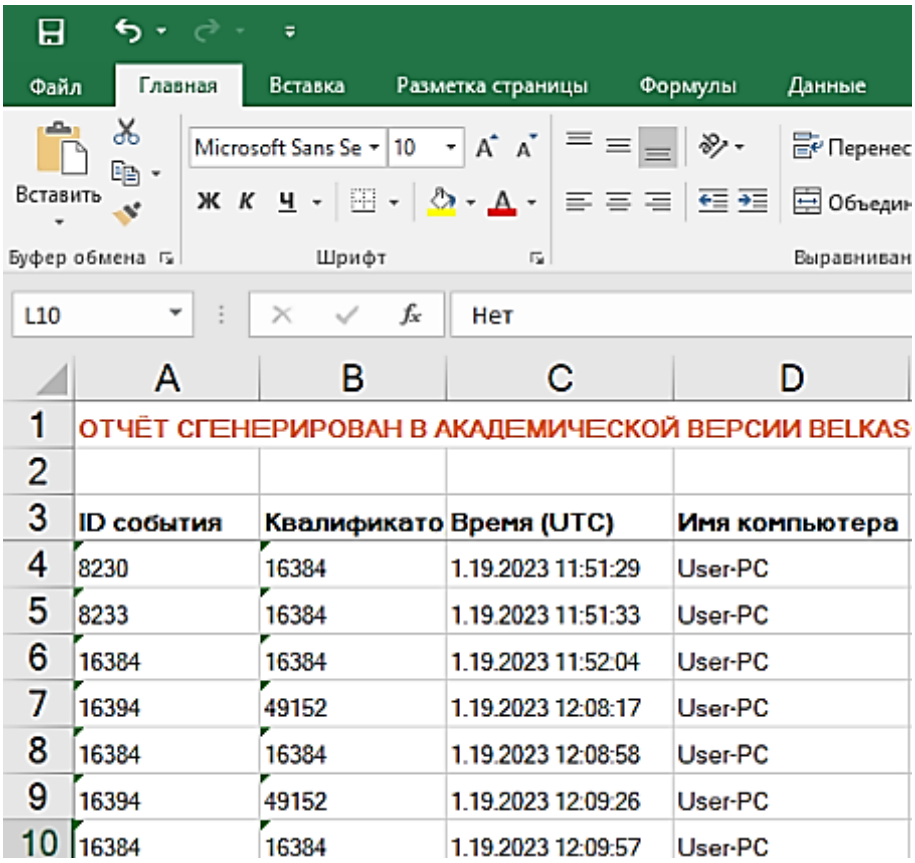
3.4 В качестве артефактов выбрать «Системные файлы».

4. Обнаружить сведения о дате последней работы ОС.

Квалификаторы со...	Время (UT...	Имя компьют...
16384	3.14.2023 10:51:21	User-PC
16384	3.14.2023 10:51:21	User-PC
49152	3.14.2023 10:51:20	User-PC
16384	3.14.2023 10:37:39	User-PC
16384	3.14.2023 10:36:58	User-PC
16384	3.14.2023 10:36:58	User-PC
16384	3.14.2023 10:36:58	User-PC
49152	3.14.2023 10:36:58	User-PC

5. Создать отчет по обнаруженным сведениям в формате XLSX.





	A	B	C	D
1	ОТЧЁТ СГЕНЕРИРОВАН В АКАДЕМИЧЕСКОЙ ВЕРСИИ BELKAS			
2				
3	**ID события**	**Квалификато**	**Время (UTC)**	**Имя компьютера**
4	8230	16384	1.19.2023 11:51:29	User-PC
5	8233	16384	1.19.2023 11:51:33	User-PC
6	16384	16384	1.19.2023 11:52:04	User-PC
7	16394	49152	1.19.2023 12:08:17	User-PC
8	16384	16384	1.19.2023 12:08:58	User-PC
9	16394	49152	1.19.2023 12:09:26	User-PC
10	16384	16384	1.19.2023 12:09:57	User-PC

6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера, доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 11

ПОЛУЧЕНИЕ СВЕДЕНИЙ О ВЫХОДЕ В СЕТЬ ИНТЕРНЕТ С ПОМОЩЬЮ ПРОГРАММ-БРАУЗЕРОВ, ИСПОЛЬЗУЯ СПЕЦИАЛИЗИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Цель работы: Получение практических навыков использования специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

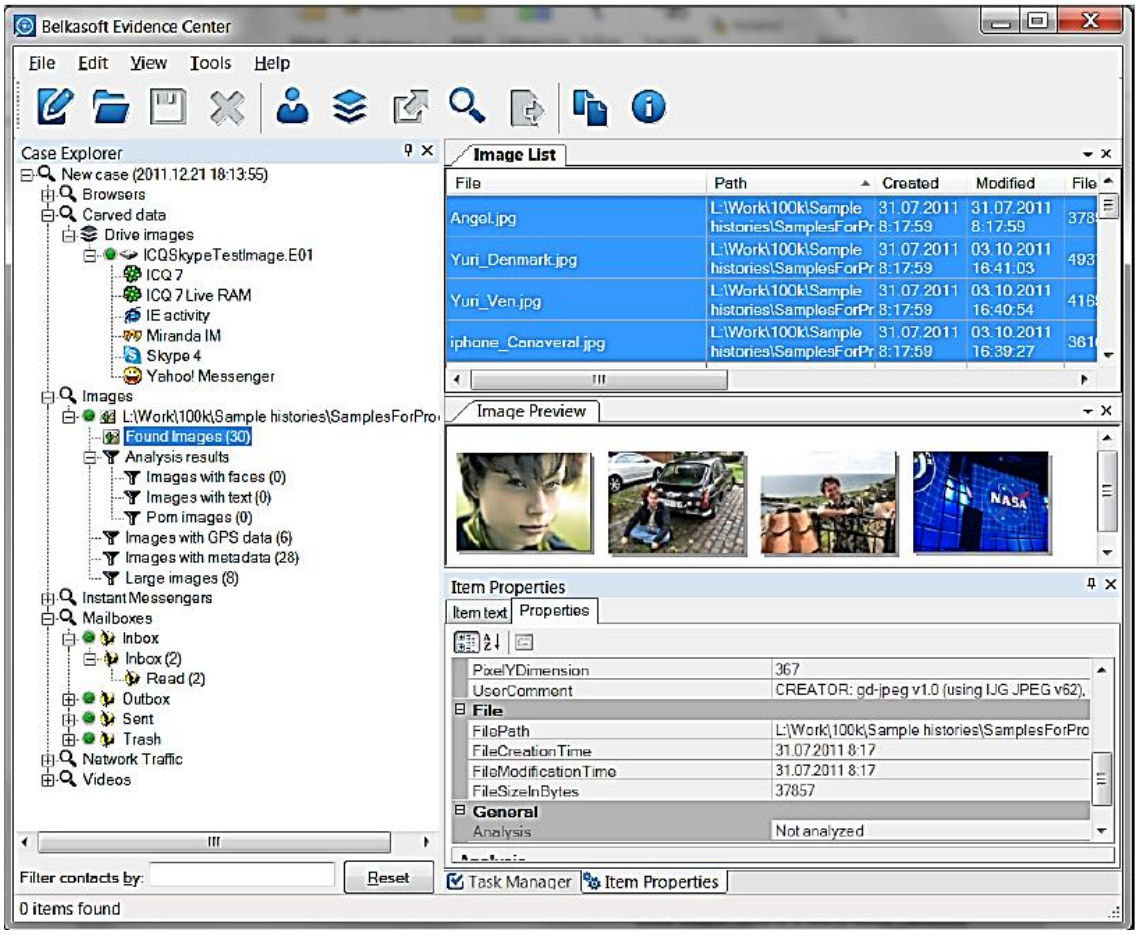


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»

- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

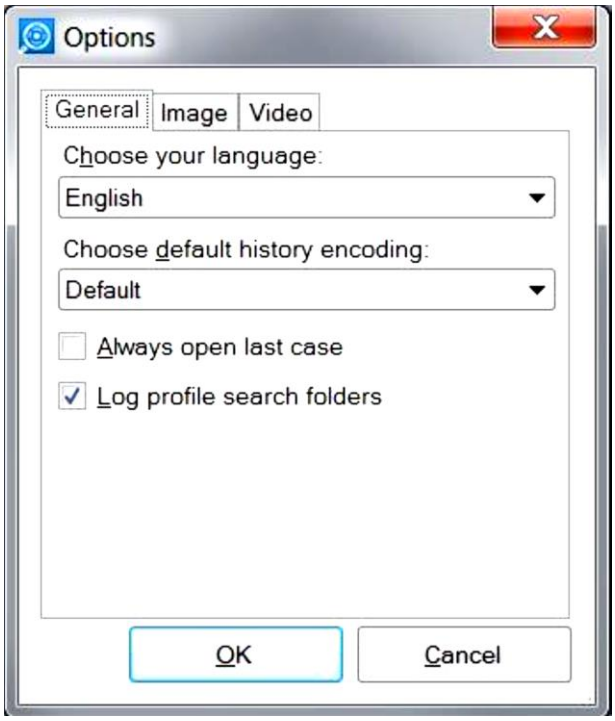


Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

Создание отчётов.

Продукт позволяет вам экспортировать историю (создавать отчёты). Эта операция доступна почти из всех частей пользовательского интерфейса. Поддержаны различные форматы отчётов, такие как HTML или PDF. Чтобы создать отчёт, вы можете выбрать одно из следующего:

- Узел дела в Обозревателе дел
- Узлы типов историй, такие как Instant Messengers, Browsers, Mailboxes, Carvers, Network Traffic, Images, Video или узел закладок Bookmarks в Обозревателе дел
- Одиночный профиль (например, профиль Skype) в Обозревателе дел
- Одиночную закладку в Обозревателе дел
- Один или несколько элементов в списке элементов, таком как Message List (список чатов), URLs (список ссылок) или Bookmark List (список элементов закладки)
- Один или несколько элементов в окне результатов поиска

После этого вы можете либо нажать кнопку Export History (создать отчёт) панели инструментов, выбрать пункт меню Export History из главного меню Edit или пункт Export History из контекстного меню Обозревателя дел. Если вы экспортируете выбранные элементы из любого списка элементов, единственный способ начать создание отчёта выбрать пункт Export History из контекстного меню списка элементов.

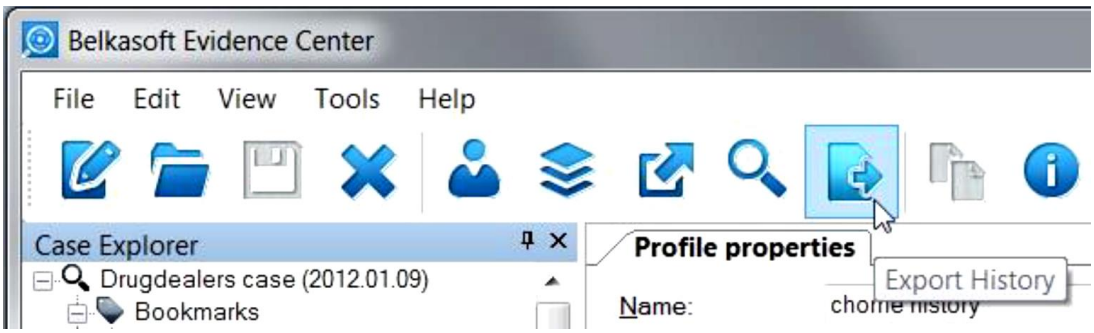


Рис. 3. Создание файлов-отчетов

После этого появится мастер Export history:

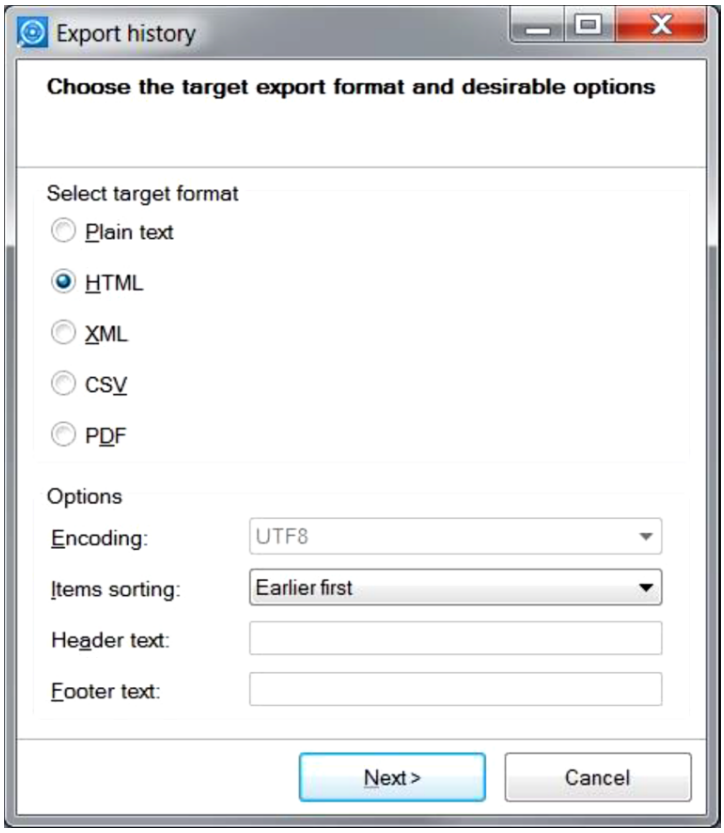


Рис. 4. Выбор формата файлов-отчетов

Первый шаг мастера позволяет вам выбрать целевой формат. В настоящее время поддержаны следующие форматы:

- Plain text (текст)
- HTML
- XML
- CSV
- PDF
- EML (только для почты)

На этой же странице мастера вы можете выбрать следующие опции:

- Encoding (кодировка). Эта опция позволит вам выбрать целевую кодировку для текста или формата CSV. Например, если вы экспортируете китайский текст, вы можете выбрать Chinese Simplified. Формат по умолчанию – UTF8.
- Item sorting (сортировка элементов). Вы можете отсортировать элементы по дате и времени в порядке возрастания или убывания.

Следующая страница мастера позволяет вам задать, сколько файлов будет сгенерировано.

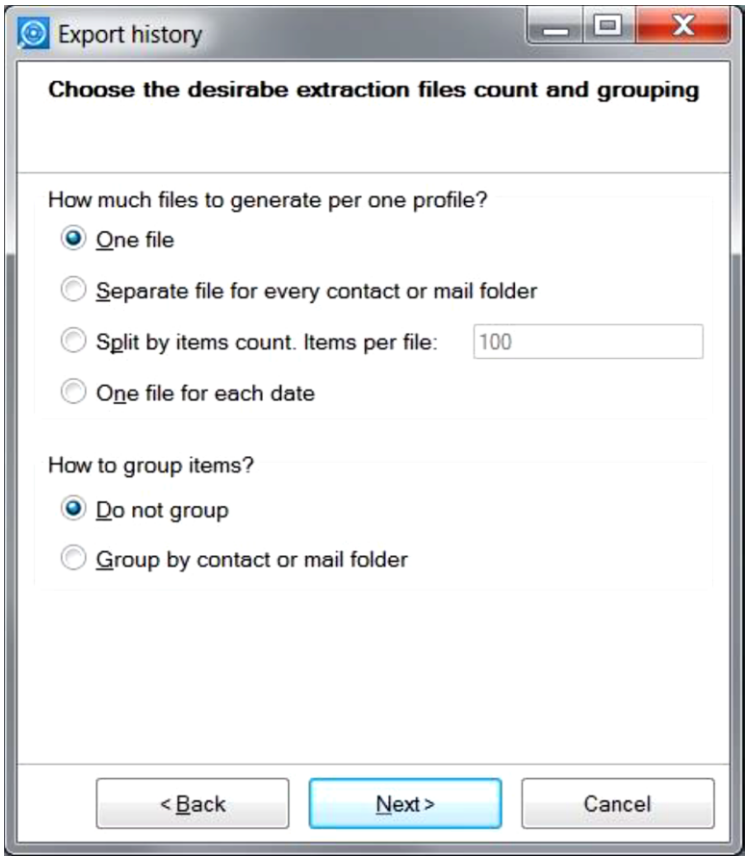


Рис. 5. Параметры создания файлов-отчетов

Доступны следующие опции:

- One file (один файл). Выбирайте эту опцию, когда размер истории, которую вы экспортируете, невелик. Иначе, если файл отчёта будет слишком велик, это может вызвать значительные задержки при его просмотре. Например, файл HTML размером 1Mb может «подвесить» ваш браузер на долгое время, а также привести к большому потреблению памяти.
- Separate file for every contact or mail folder (отдельный файл для каждого контакта или почтовой папки). Выбирайте эту опцию, когда вы экспортируете интернет-чаты или почтовую переписку. В этом случае для каждого контакта или для каждой почтовой папки будет создан отдельный файл.
- Split by items count (разбить по количеству элементов). Выбирайте эту опцию, чтобы получить файлы отчётов определённого размера. Когда у вас есть существенное количество истории, вы можете захотеть генерировать файлы предсказуемого размера, например, файлы, содержащие не более 1000 сообщений. В этом случае вы можете получить большое количество файлов, но зато они не приведут к понижению производительности просмотрщика из-за слишком большого размера.

- One file per each date (один файл на каждую дату). Выбирайте эту опцию, когда вам важно увидеть, какие события случились в ту или иную дату.

На той же странице мастера вы можете выбрать тип группировки. Доступны следующие опции:

- Do not group (не группировать). В этом случае вы увидите все события по порядку, отсортированные по времени и дате. Например, для профиля интернет-пейджера, вы увидите все чаты по порядку. Это удобно, когда вам требуется построить таймлайн всех разговоров пользователя.
- Group by contact or mail folder (группировать по контакту или почтовой папке). В этом случае элементы будут сгруппированы. Например, для интернет-пейджеров, все чаты с определённым контактом («другом») будут сгруппированы вместе, и внутри отсортированы по дате и времени. Затем будет представлена история со следующим контактом и т.д. Это удобно, когда вас интересует история с тем или иным контактом.

Учтите, что некоторые из этих опций будут проигнорированы в зависимости от формата. Например, в формате CSV невозможно произвести группировку, поэтому эта опция не будет влиять на конечный отчёт в CSV.

На следующей странице мастера вы можете выбрать период времени, которым следует ограничить отчёт:

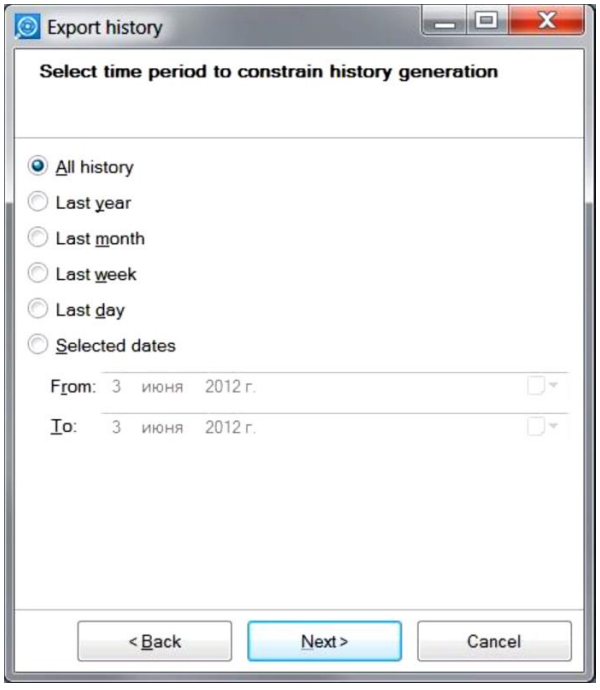


Рис. 6. Период времени, которым следует ограничить отчёт

На следующей странице мастера вы сможете указать целевую директорию для файлов отчёта:

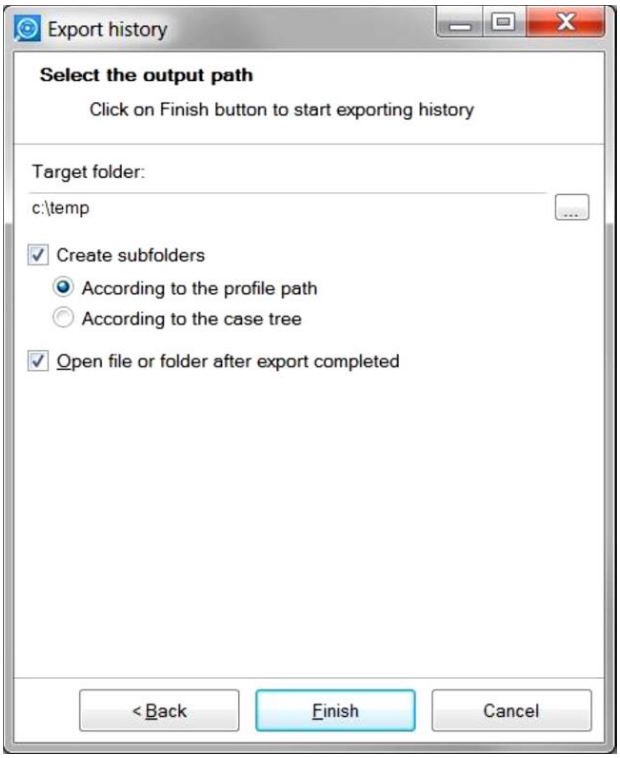


Рис. 7. Выбор директории для файлов отчёта

Обратите внимание, что продукт создаст поддиректорию внутри выбранной директории, названную по имени профиля (или закладки). Если продукт определит, что внутри уже существует подобная директория, он добавит номер к имени директории, чтобы сделать имя уникальным. Это позволит вам не беспокоиться о перетирании предыдущих результатов экспорта – этого никогда не произойдёт.

Флажок Open file or folder after export completed (открыть файл или папку, когда завершится экспорт) позволяет вам открыть результат экспорта с помощью программы по умолчанию. Например, если вы выбрали экспортировать в один файл в формате HTML, по завершению экспорта результирующий файл откроется в браузере по умолчанию.

Если вы экспортируете в несколько файлов, по окончании экспорта будет открыт Windows Explorer с целевой папкой, что даст вам возможность вручную выбрать любой из получившихся файлов для дальнейшей работы.

Мастер отчётов запоминает все ваши предпочтения, поэтому в следующий раз вы можете просто нажимать кнопку Next для генерации отчёта с теми же самыми предпочтениями. Единственное, что вам придётся менять – это источник экспорта – профиль или набор элементов истории.

Belkasoft
forensics made easier

Messenger History

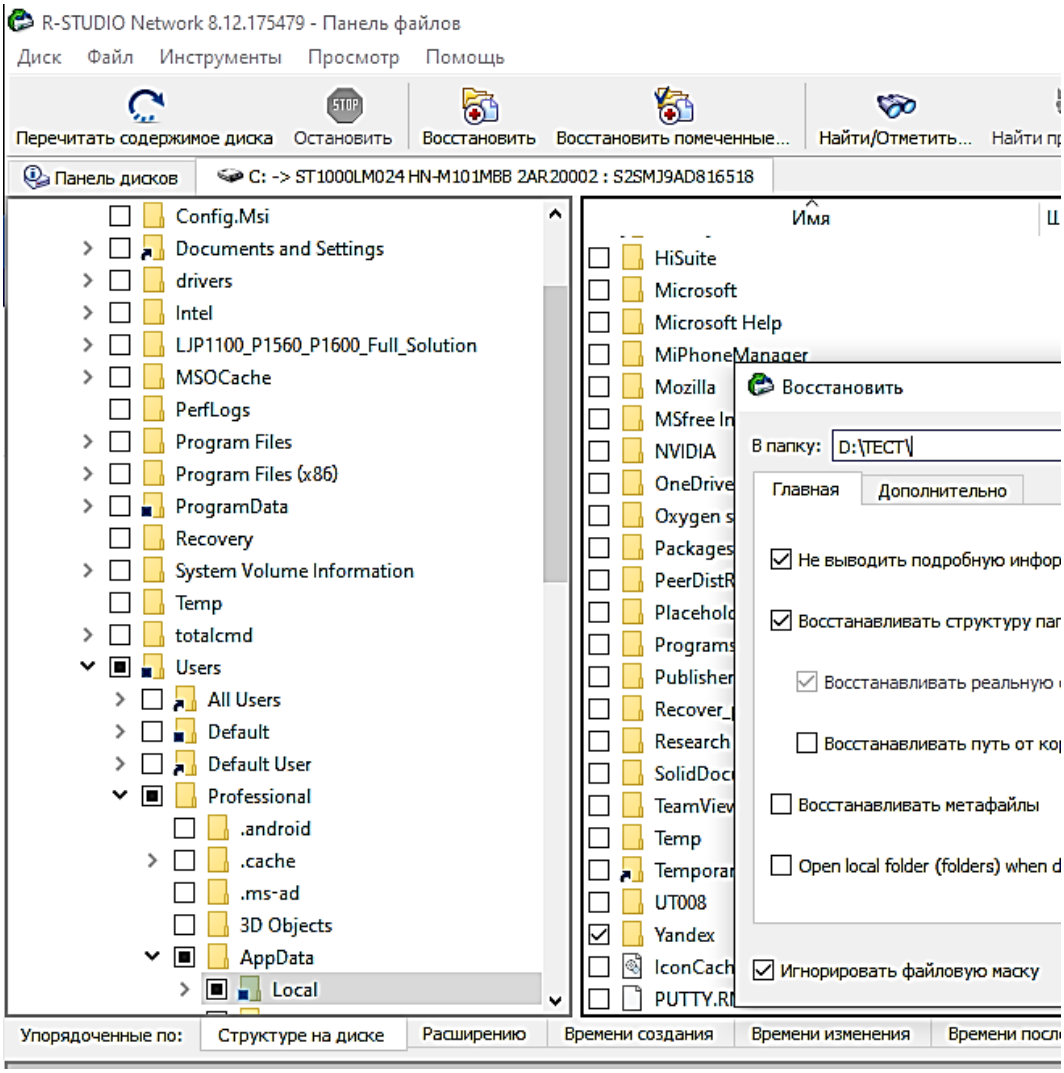
2 of 4

Direction	Time	Author	Message
OUT	09.07.2009 14:44:10	494417976	Just think of the fishing that's here.
IN	09.07.2009 14:44:21	476573648 (Joe)	I don't care for fishing. I want to go home.
OUT	09.07.2009 14:44:28	494417976	But, Joe, there ain't such another swimming-place anywhere.
IN	09.07.2009 14:44:35	476573648 (Joe)	Swimming's no good. I don't seem to care for it, somehow, when there ain't anybody to say I sha'n't go in. I mean to go home.
OUT	09.07.2009 14:44:43	494417976	Oh, shucks! Baby! You want to see your mother, I reckon.
IN	09.07.2009 14:44:51	476573648 (Joe)	Yes, I do want to see my mother -- and you would, too, if you had one. I ain't any more baby than you are." And Joe snuffled a little.
OUT	09.07.2009 14:45:07	494417976	Well, we'll let the cry-baby go home to his mother, won't we, Huck? Poor thing -- does it want to see its mother? And so it shall. You like it here, don't you, Huck? We'll stay, won't we?.
IN	09.07.2009 14:45:31	476573648 (Joe)	I'll never speak to you again as long as I live,
IN	09.07.2009 14:45:34	476573648 (Joe)	There now!
OUT	09.07.2009 14:45:41	494417976	Who cares!
OUT	09.07.2009 14:45:49	494417976	Nobody wants you to. Go 'long home and get laughed at. Oh, you're a nice pirate. Huck and me ain't cry-babies. We'll stay, won't we, Huck? Let him go if he wants to. I reckon we can get along without him, per'aps.
IN	09.07.2009 14:45:58	476573648 (Joe)	I want to go, Tom. It was getting so lonesome anyway, and now it'll be worse. Let's us go, Tom.
OUT	09.07.2009 14:47:16	494417976	I won't! You can all go, if you want to. I mean to stay.
IN	09.07.2009 14:47:22	476573648 (Joe)	Tom, I better go.
OUT	09.07.2009 14:47:30	494417976	Well, go 'long -- who's hendering you.
IN	09.07.2009 14:47:36	476573648 (Joe)	Tom, I wisht you'd come, too. Now you think it over. We'll wait for you when we get to shore.
OUT	09.07.2009 14:47:44	494417976	Well, you'll wait a blame long time, that's all.
IN	09.07.2009 14:49:05	424583493 (Aunt Polly)	Well, I don't say it wasn't a fine joke, Tom, to keep everybody suffering 'most a week so you boys had a good time, but it is a pity you could be so hard-hearted as to let me suffer so. If you could come over on a log to go to your funeral, you could have come over and give me a hint some way that you warn't dead, but only run off.
IN	09.07.2009 14:49:28	424583493 (Aunt Polly)	Yes, you could have done that, Tom.
IN	09.07.2009 14:49:31	424583493 (Aunt Polly)	and I believe you would if you had thought of it.
OUT	09.07.2009 14:49:40	494417976	I -- well, I don't know. 'Twould 'a' spoiled everything.
IN	09.07.2009 14:49:48	424583493 (Aunt Polly)	Tom, I hoped you loved me that much,
IN	09.07.2009 14:49:53	424583493 (Aunt Polly)	It would have been something if you'd cared enough to think of it, even if you didn't do it.
OUT	09.07.2009 14:50:10	494417976	Now, auntie, you know I do care for you,
IN	09.07.2009 14:50:21	424583493 (Aunt Polly)	I'd know it better if you acted more like it.

Рис. 8. Отчёт в формате PDF, открытый в просмотрщике PDF по умолчанию

Порядок выполнения работы

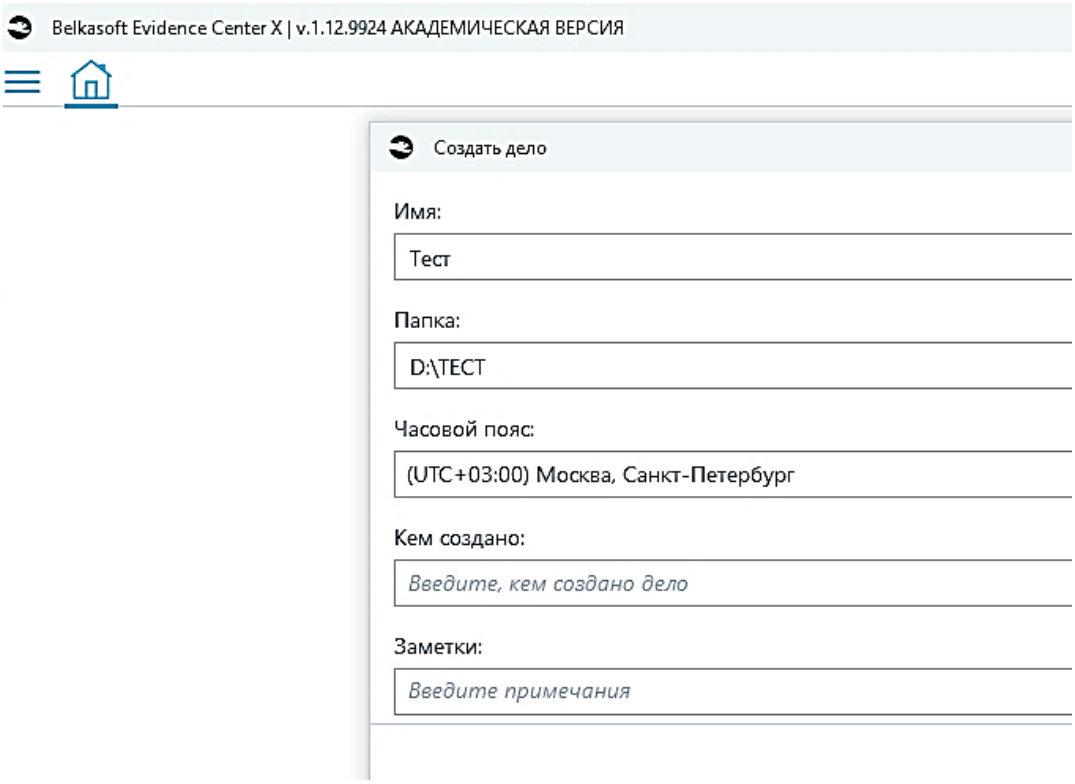
1. На исследуемом накопителе обнаружить служебные и системные каталоги, в которых располагаются сведения о работе программы-браузера: \Users\Professional\AppData\Local\Yandex\;
2. С помощью программы AccessData FTK Imager или R-Studio экспортировать каталоги во временный каталог.



3. С помощью специализированного ПО Belkasoft Evidence Center проанализировать временный каталог.

3.1 Для этого запустить ПО Belkasoft Evidence Center.

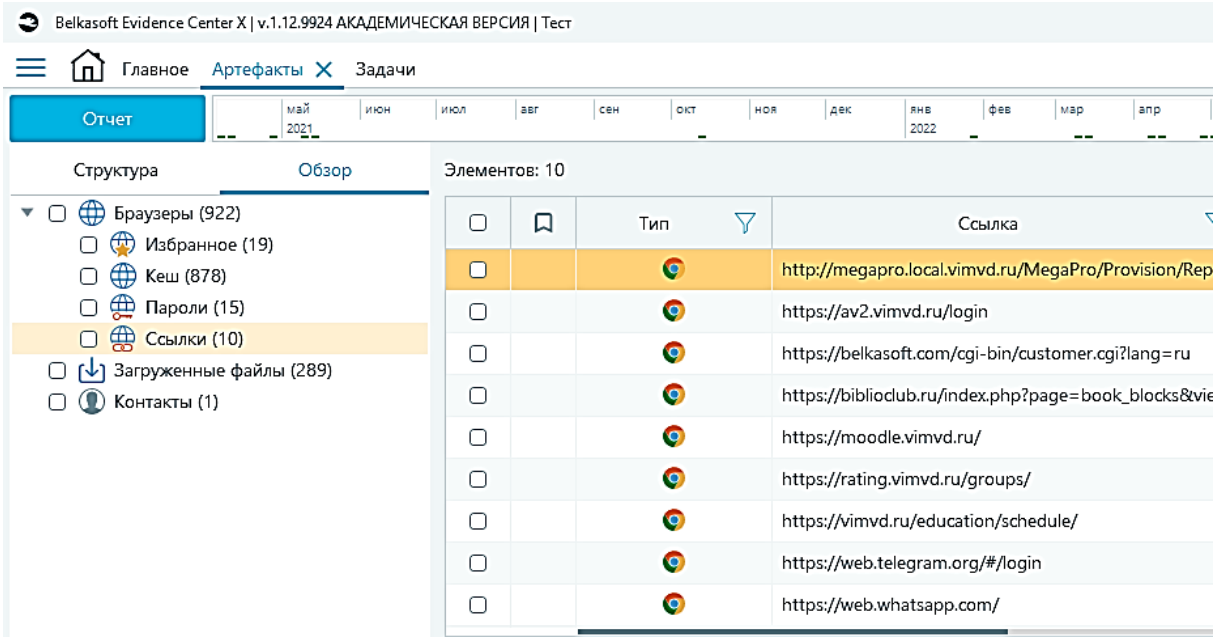
3.2 Создать новое дело и сохранить его в заранее созданный каталог на диске D.



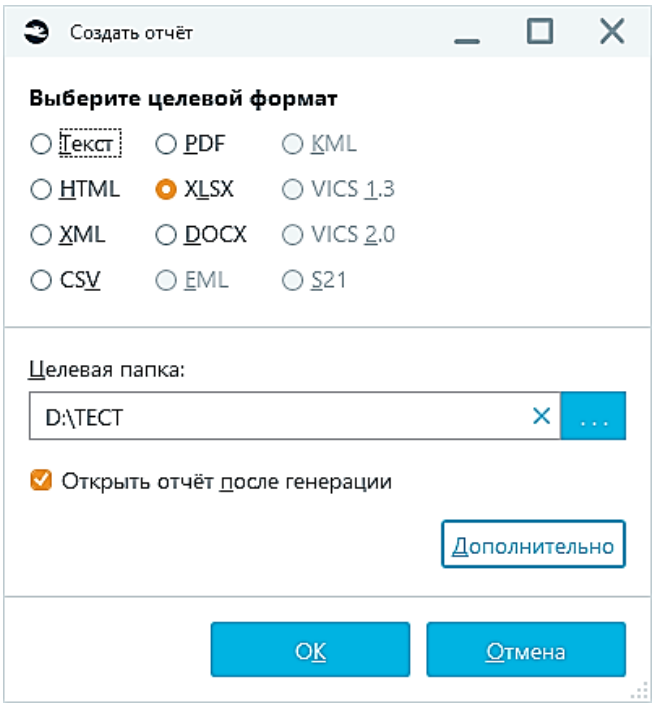
3.3 Добавить источник данных существующий, папка и выбрать временный каталог с файлами.

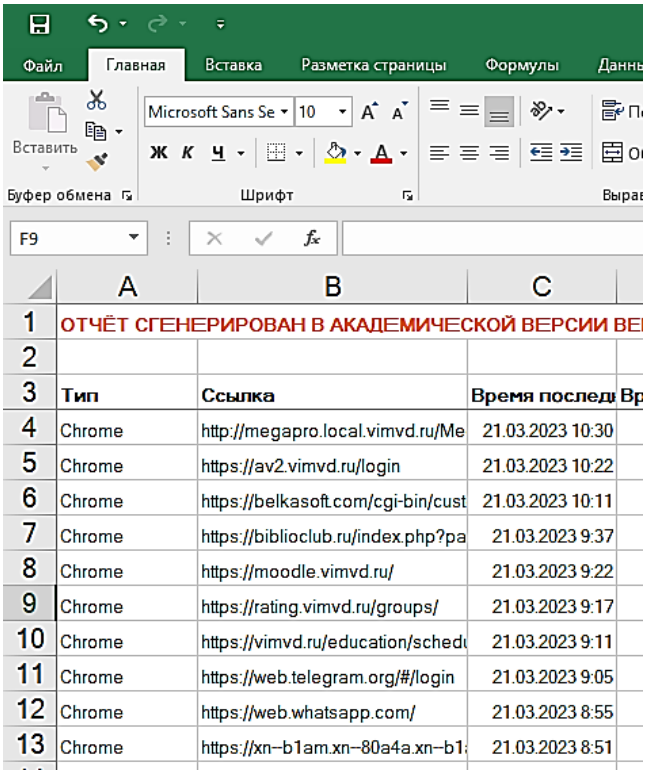
3.4 В качестве артефактов выбрать «Браузеры».

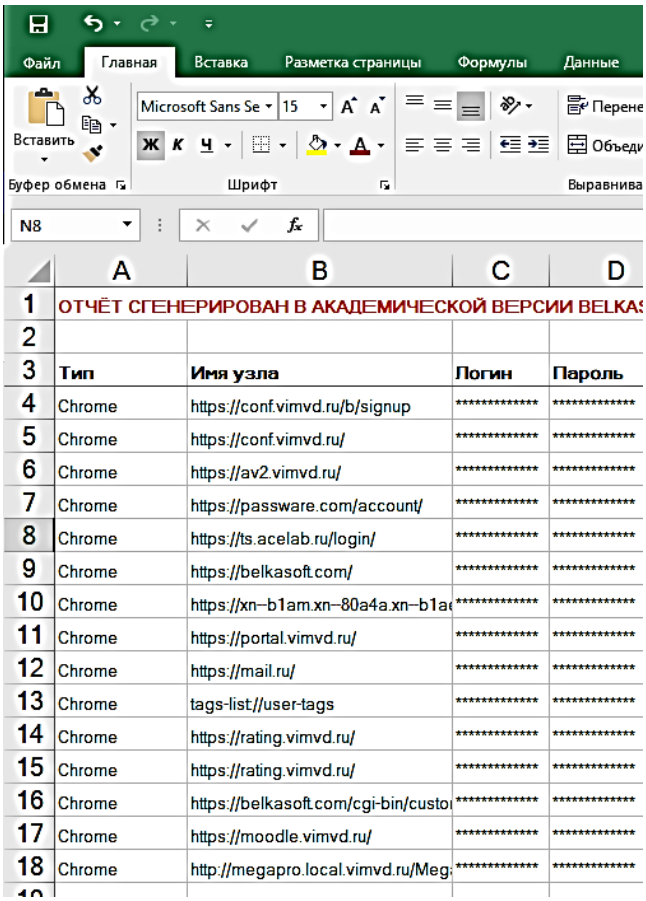
4. Обнаружить сведения о выходе в сеть интернет с помощью программы-браузера, с указанием ссылки, даты и времени посещения. Обнаружить сохраненные сведения: кеш, пароли, избранное, сведения о загруженных файлах и т.д.



5. Создать отчет по обнаруженным сведениям в формате XLSX.







	A	B	C	D
1	ОТЧЁТ СГЕНЕРИРОВАН В АКАДЕМИЧЕСКОЙ ВЕРСИИ BELKAS			
2				
3	**Тип**	**Имя узла**	**Логин**	**Пароль**
4	Chrome	https://conf.vimvd.ru/b/signup	**********	**********
5	Chrome	https://conf.vimvd.ru/	**********	**********
6	Chrome	https://av2.vimvd.ru/	**********	**********
7	Chrome	https://passware.com/account/	**********	**********
8	Chrome	https://ts.acelab.ru/login/	**********	**********
9	Chrome	https://belkasoft.com/	**********	**********
10	Chrome	https://xn--b1am.xn--80a4a.xn--b1a	**********	**********
11	Chrome	https://portal.vimvd.ru/	**********	**********
12	Chrome	https://mail.ru/	**********	**********
13	Chrome	tags-list://user-tags	**********	**********
14	Chrome	https://rating.vimvd.ru/	**********	**********
15	Chrome	https://rating.vimvd.ru/	**********	**********
16	Chrome	https://belkasoft.com/cgi-bin/custo	**********	**********
17	Chrome	https://moodle.vimvd.ru/	**********	**********
18	Chrome	http://megapro.local.vimvd.ru/Meg	**********	**********

(В приведенном примере реальные логины и пароли умышленно скрыты звездочками).
6. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Перечислите основные возможности ПО Belkasoft Evidence Center.
2. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
3. С какими источниками данных может работать ПО Belkasoft Evidence Center?
4. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
5. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
6. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
7. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
8. Где располагаются каталоги, содержащие сведения о работе программ-браузеров?
9. Какие сведения о работе программ-браузеров можно получить с помощью ПО Belkasoft Evidence Center?

ЛАБОРАТОРНАЯ РАБОТА № 12

ВОССТАНОВЛЕНИЕ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ FAT32 ФАЙЛА-ОБРАЗА

Цель работы: Получение практических навыков создания файлов-образов и восстановления информации из них.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное

меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и

содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т.д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

Как работают программы восстановления данных

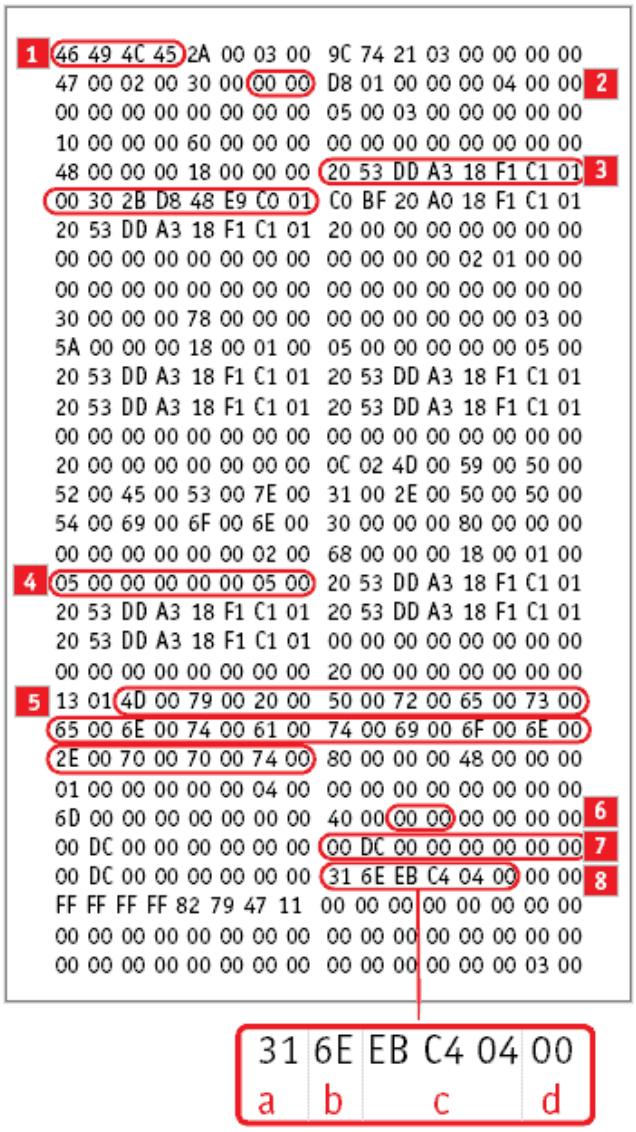
Каждый только что удаленный файл все еще находится на жестком диске, но Windows его больше не видит. Если программе восстановления данных необходимо восстановить этот файл, она просматривает загрузочный сектор раздела (Partition Boot Sector). В нем содержится вся информация о строении раздела, например размер секторов (как правило, 512 байт) и количество секторов в одном кластере.

В разделе NTFS размером более 2 Гбайт в одном кластере содержится четыре сектора. В нашем примере показан небольшой раздел размером 500 Мбайт, у которого каждому сектору соответствует один кластер.

Наряду с этой информацией программы восстановления данных сканируют главную таблицу файлов(Master File Table, MFT), которая тоже находится в Partition Boot Sector. Она представляет собой список всех файлов, находящихся в разделе, в ней содержатся все файловые атрибуты и информация о том, в каких секторах винчестера находятся сами файлы. Те из них, что по размерам менее 1500 байт, записываются прямо в MFT. Для файлов большего объема в MFT есть ссылки на адреса секторов, в которых лежат данные.

В начале MFT находятся другие записи, например, так называемая битовая карта распределения кластеров (Cluster Bitmap), показывающая все

используемые кластеры, а также файл плохих кластеров (Bad Cluster File), регистрирующий все кластеры с ошибками. Только с 17-й записи начинается собственно описание файлов. Обычно таблица MFT в Windows не видна. Но есть дисковые редакторы, например WinHex, которые показывают содержание MFT в шестнадцатеричных кодах.



Выше на рисунке вы видите MFT-запись удаленного файла в HEX-коде. Для программы восстановления данных достаточно этой информации, чтобы восстановить файл.

Значения, которые программа восстановления файлов находит в Master File Table:

1. Эти четыре байта (File Identifier) обозначают начало нового файла. Байты до следующего FileIdentifier содержат всю информацию о файле.

2. Эти два байта зарезервированы для флагов, которые дают справку о состоянии файла. Если их значение равно 0, как в нашем случае, это значит, что файл удален.

3. Из этих 16 байт программа восстановления данных узнает, когда файл был создан и в последний раз подвергался изменениям.

4. Эта ссылка на каталог, в котором находится файл (Parent Directory Record Number). С ее помощью программа-спасатель может включить файл в структуру каталогов.

5. Здесь появляется имя файла, в нашем случае My Presentation.ppt.

6. Если эти два байта имеют значение 0, то файл не сжат.

7. Эти восемь байт сообщают размер файла, в нашем случае 56 320 байт.

8. Важнейшая часть записи MFT, называющаяся Data runs, показывает, где фактически находятся данные.

Здесь указано где находятся данные.

a. Первый байт сообщает, сколько байт необходимо для адреса первого кластера (3 байта) и отображения длины файла во всех кластерах (1 байт).

b. Второй байт содержит длину файла, в нашем примере — 110 кластеров.

c. Следующие три байта означают, что файл начинается с кластера 312 555.

d. Последний байт имеет значение 0. Это означает, что файл не фрагментирован. Следовательно, нет никаких дополнительных записей Data runs.

Как программа восстанавливает данные

Теперь у программы восстановления данных есть вся информация, необходимая для успешного восстановления удаленного файла. Она обращается к кластеру 312 555, прочитывает данные в следующих 110 кластерах и сохраняет их под именем My Presentation.ppt

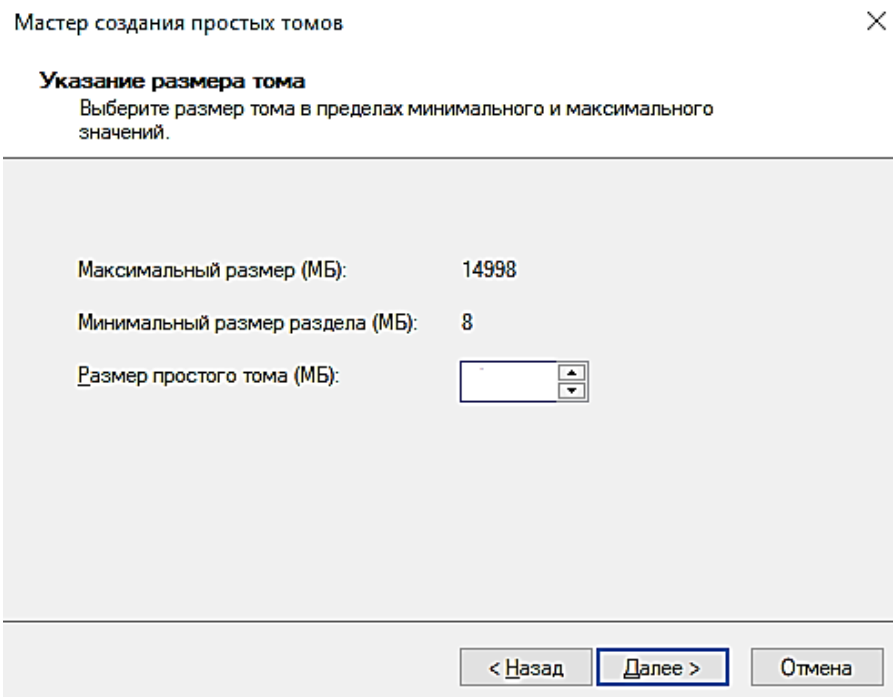
Порядок выполнения работы

1. Создать файл-образ с файловой системой FAT32.

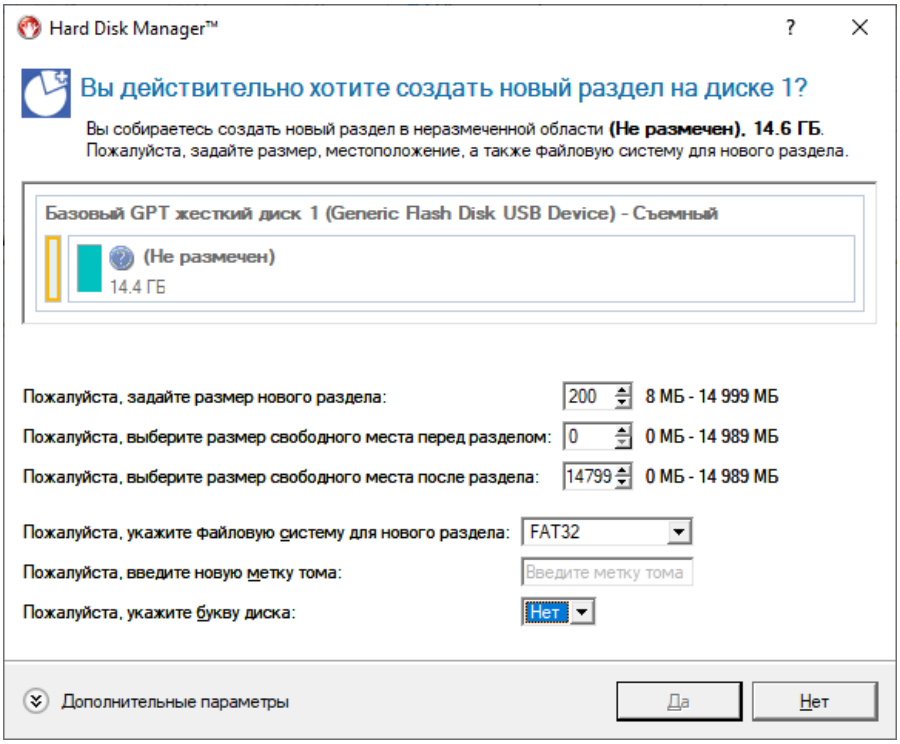
1.1. Получить у преподавателя накопитель информации.

1.2. Создать на нем раздел с файловой системой FAT32.

1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками.



1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager



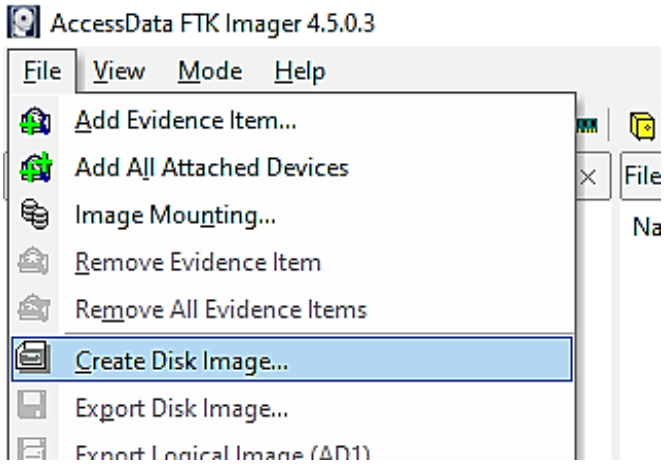
1.3. Скопировать в созданный раздел несколько произвольных графических файлов. Сделать скриншот.

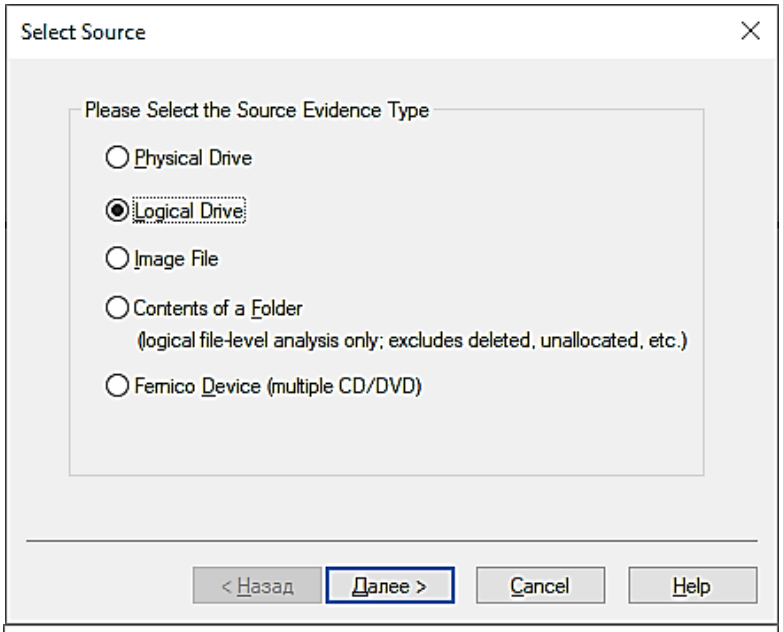
1.4. Удалить скопированные графические файлы.

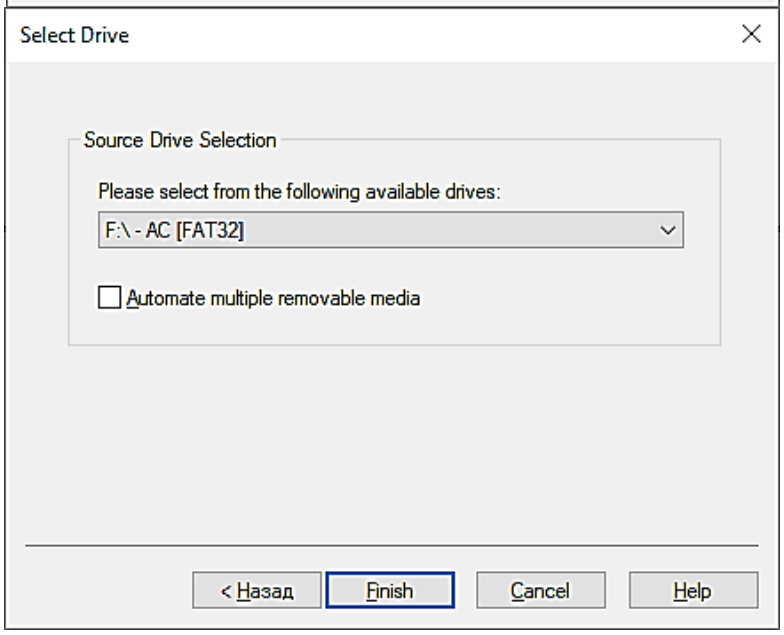
1.5. Создать файл-образ созданного раздела.

1.5.1. Для этого запустить ПО AccessData FTK Image».

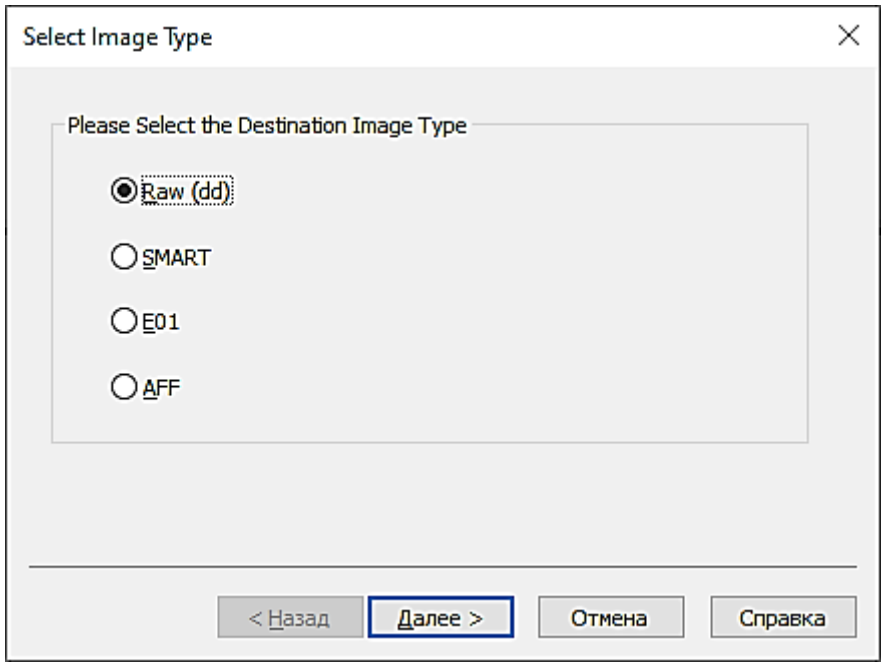
1.5.2. Выбрать пункт Create Disk Image.


AccessData FTK Imager 4.5.0.3
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)

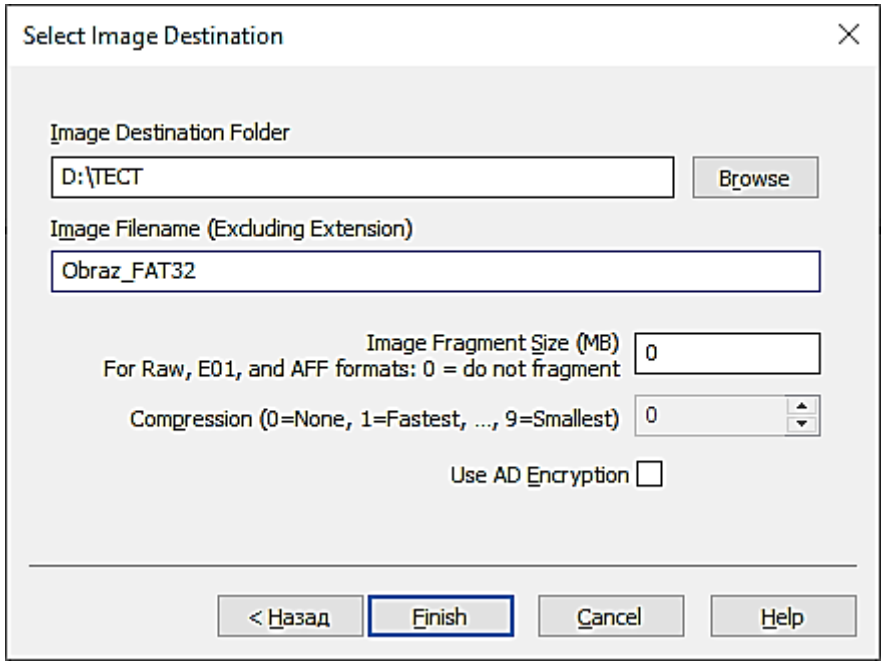

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Назад
Далее >
Cancel
Help


Select Drive
Source Drive Selection
Please select from the following available drives:
F:\ - AC [FAT32]
Automate multiple removable media
< Назад
Finish
Cancel
Help

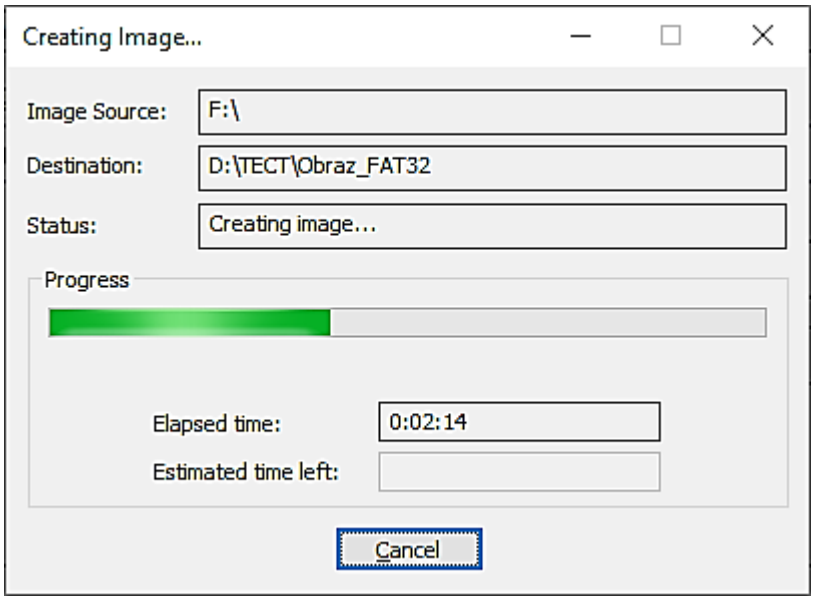
1.5.3. Выбрать формат файла образа Raw(dd).



1.5.4. Указать место сохранения файла образа диск D. Присвоить имя файлу образа. Размер фрагмента указать 0.



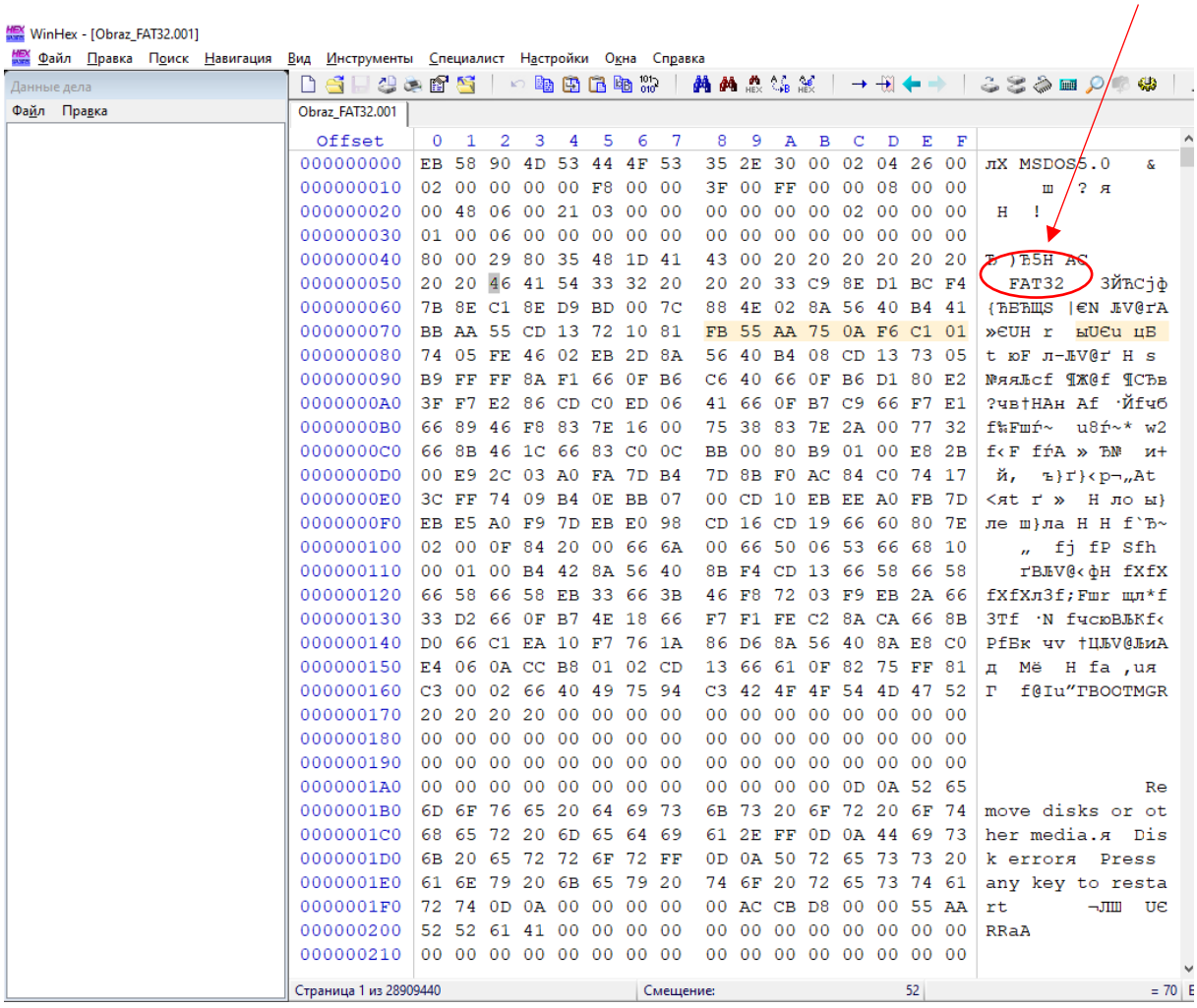
1.5.5 Если все сделали правильно, то запустится процесс создания файла-образа.



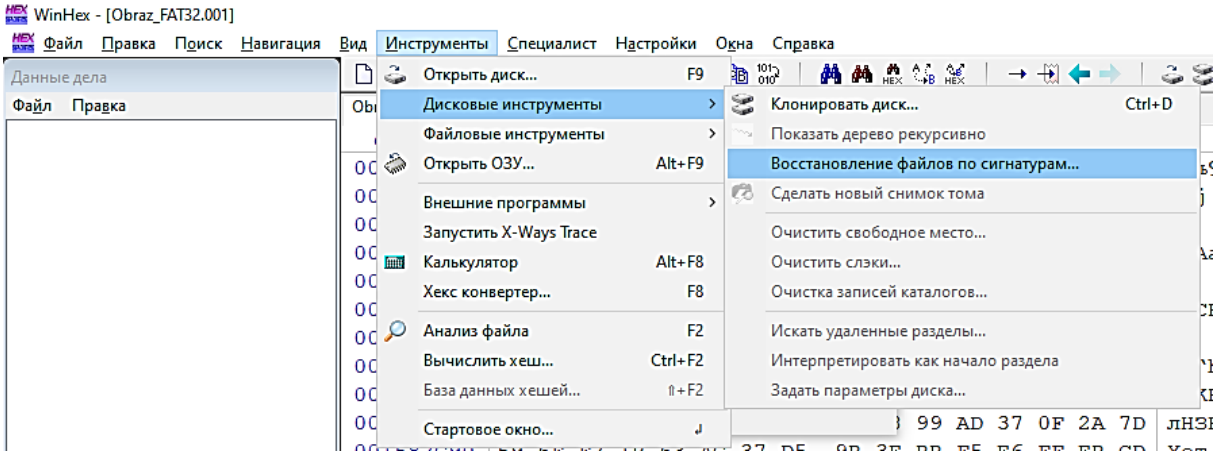
2. Восстановить удаленные графические файлы из файла-образа.

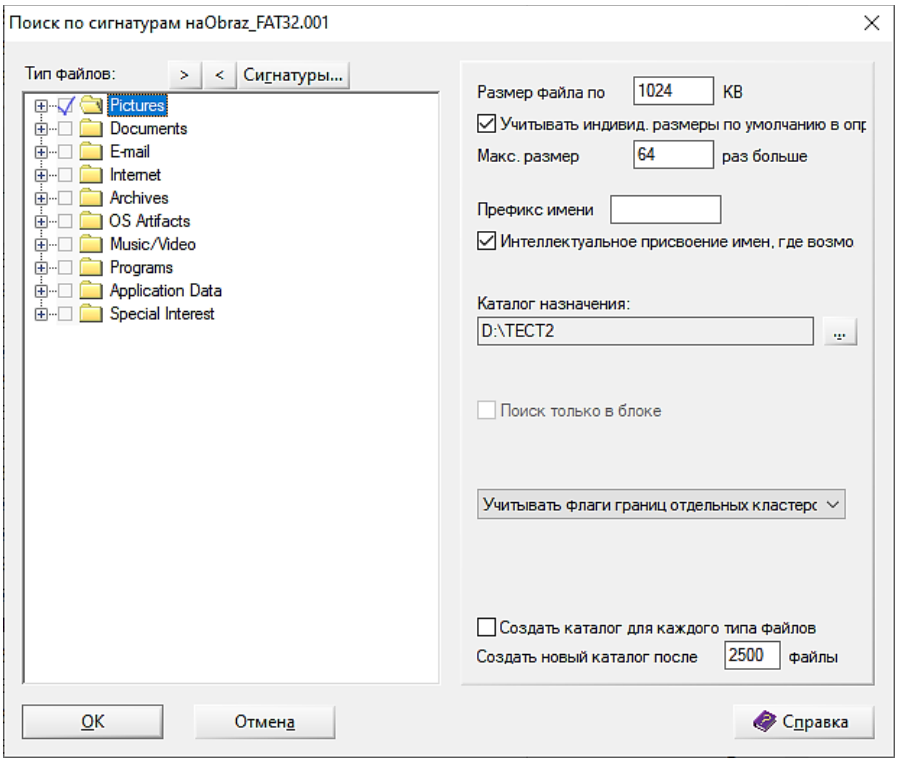
2.1. Открыть созданный файл-образ в программе WinHex.

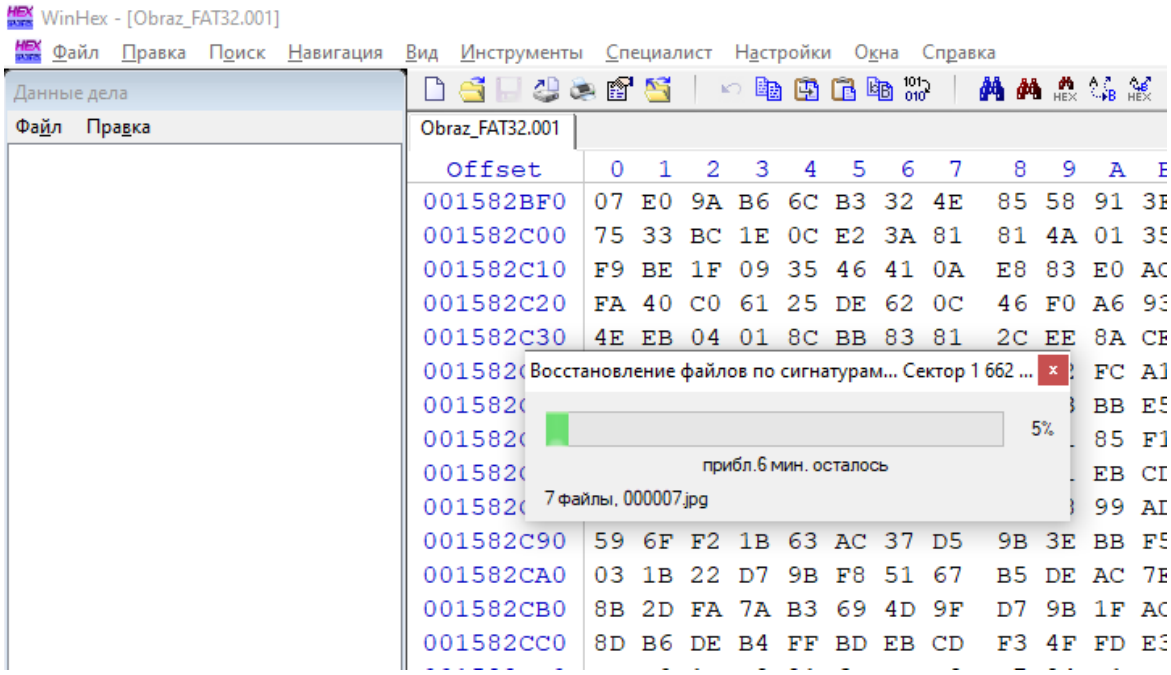
2.2. Убедиться, что файл-образ имеет файловую систему FAT32.



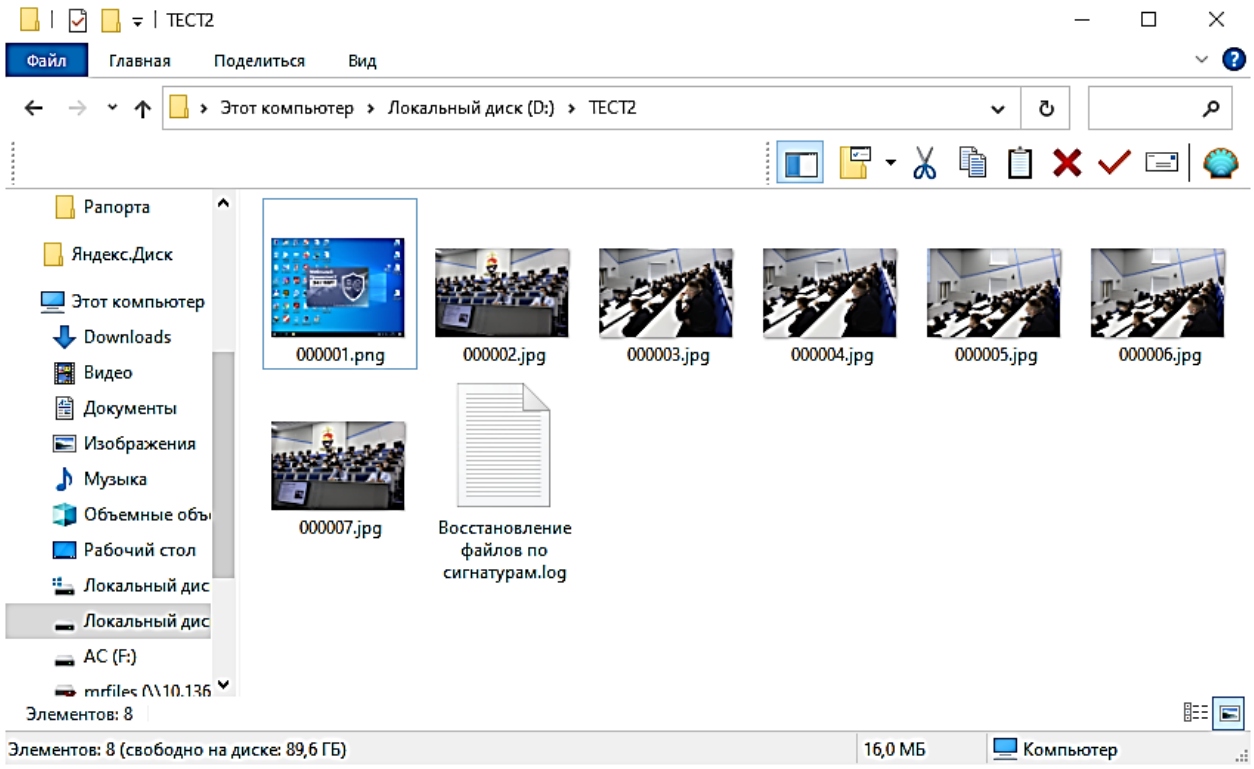
2.3. Восстановить графические файлы по сигнатурам.







3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы FAT32?
3. Какого максимального размера файлы можно помещать в файловую систему FAT32?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм создания файла-образа.
10. Какие типы файлов вы знаете?

ЛАБОРАТОРНАЯ РАБОТА № 13

ВОССТАНОВЛЕНИЕ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ NTFS ФАЙЛА-ОБРАЗА

Цель работы: Получение практических навыков создания файлов-образов и восстановления информации из них.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное

меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель

начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т. д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

Как работают программы восстановления данных

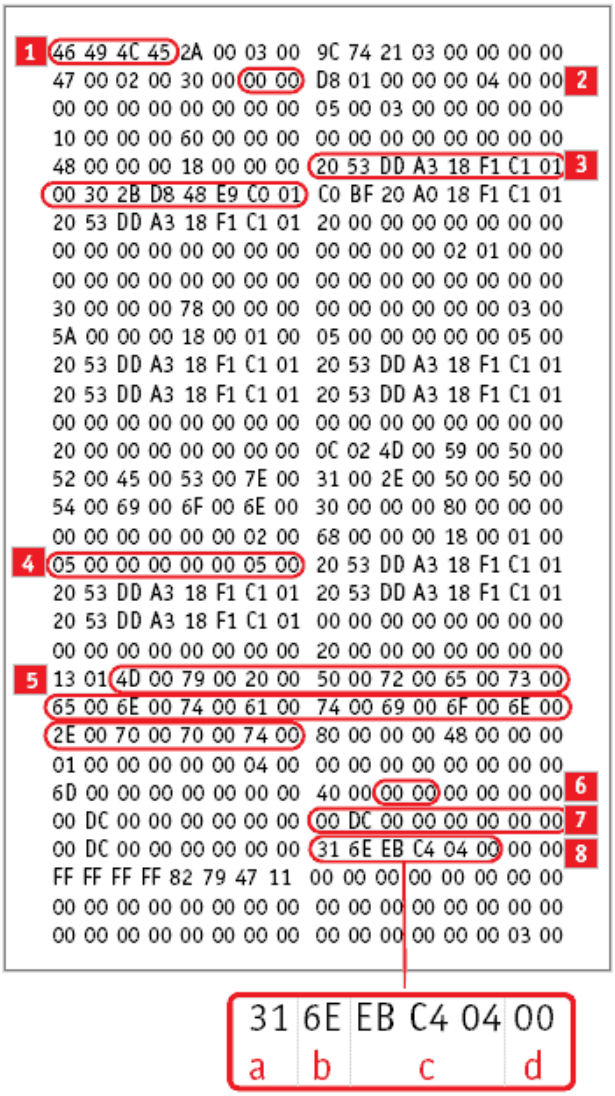
Каждый только что удаленный файл все еще находится на жестком диске, но Windows его больше не видит. Если программе восстановления данных необходимо восстановить этот файл, она просматривает загрузочный сектор раздела (Partition Boot Sector). В нем содержится вся информация о строении раздела, например размер секторов (как правило, 512 байт) и количество секторов в одном кластере.

В разделе NTFS размером более 2 Гбайт в одном кластере содержится четыре сектора. В нашем примере показан небольшой раздел размером 500 Мбайт, у которого каждому сектору соответствует один кластер.

Наряду с этой информацией программы восстановления данных сканируют главную таблицу файлов(Master File Table, MFT), которая тоже находится в Partition Boot Sector. Она представляет собой список всех файлов, находящихся в разделе, в ней содержатся все файловые атрибуты и информация о том, в каких секторах винчестера находятся сами файлы. Те из них, что по размерам менее 1500 байт, записываются прямо в MFT. Для файлов большего объема в MFT есть ссылки на адреса секторов, в которых лежат данные.

В начале MFT находятся другие записи, например так называемая битовая карта распределения кластеров (Cluster Bitmap), показывающая все

используемые кластеры, а также файл плохих кластеров (Bad Cluster File), регистрирующий все кластеры с ошибками. Только с 17-й записи начинается собственно описание файлов. Обычно таблица MFT в Windows не видна. Но есть дисковые редакторы, например WinHex, которые показывают содержание MFT в шестнадцатеричных кодах.



Выше на рисунке вы видите MFT-запись удаленного файла в HEX-коде. Для программы восстановления данных достаточно этой информации, чтобы восстановить файл.

Значения, которые программа восстановления файлов находит в Master File Table:

1. Эти четыре байта (File Identifier) обозначают начало нового файла. Байты до следующего FileIdentifier содержат всю информацию о файле.

2. Эти два байта зарезервированы для флагов, которые дают справку о состоянии файла. Если их значение равно 0, как в нашем случае, это значит, что файл удален.

3. Из этих 16 байт программа восстановления данных узнает, когда файл был создан и в последний раз подвергался изменениям.

4. Эта ссылка на каталог, в котором находится файл (Parent Directory Record Number). С ее помощью программа-спасатель может включить файл в структуру каталогов.

5. Здесь появляется имя файла, в нашем случае My Presentation.ppt.

6. Если эти два байта имеют значение 0, то файл не сжат.

7. Эти восемь байт сообщают размер файла, в нашем случае 56 320 байт.

8. Важнейшая часть записи MFT, называющаяся Data runs, показывает, где фактически находятся данные.

Здесь указано где находятся данные.

a. Первый байт сообщает, сколько байт необходимо для адреса первого кластера (3 байта) и отображения длины файла во всех кластерах (1 байт).

b. Второй байт содержит длину файла, в нашем примере — 110 кластеров.

c. Следующие три байта означают, что файл начинается с кластера 312 555.

d. Последний байт имеет значение 0. Это означает, что файл не фрагментирован. Следовательно, нет никаких дополнительных записей Data runs.

Как программа восстанавливает данные

Теперь у программы восстановления данных есть вся информация, необходимая для успешного восстановления удаленного файла. Она обращается к кластеру 312 555, прочитывает данные в следующих 110 кластерах и сохраняет их под именем My Presentation.ppt

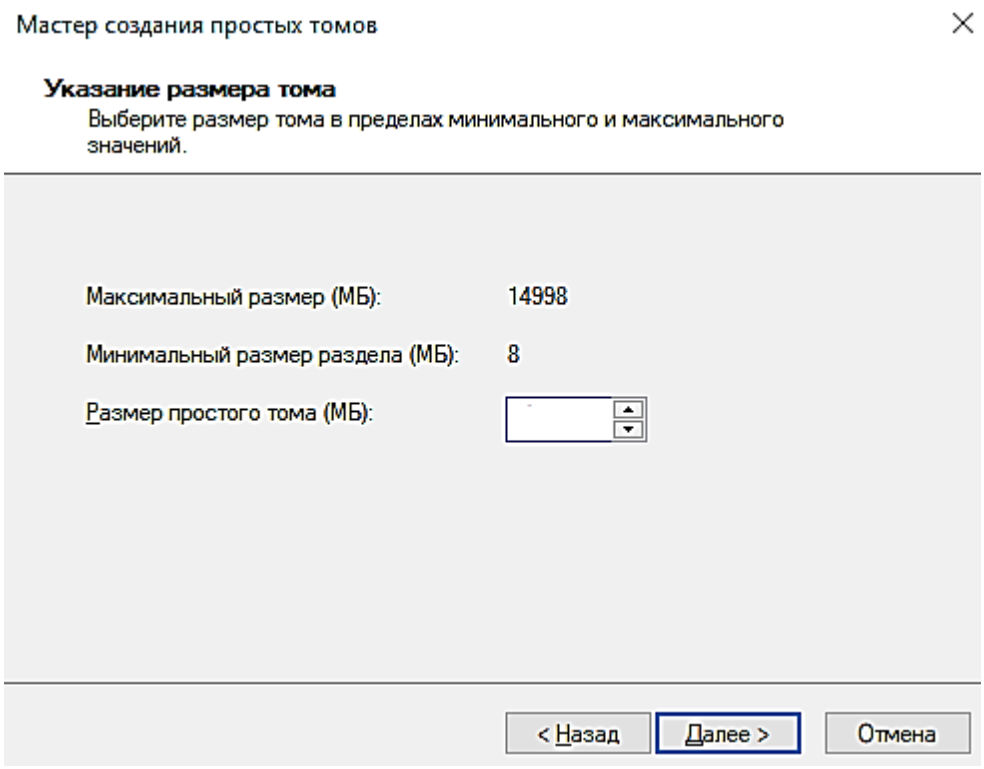
Порядок выполнения работы

1. Создать файл-образ с файловой системой NTFS.

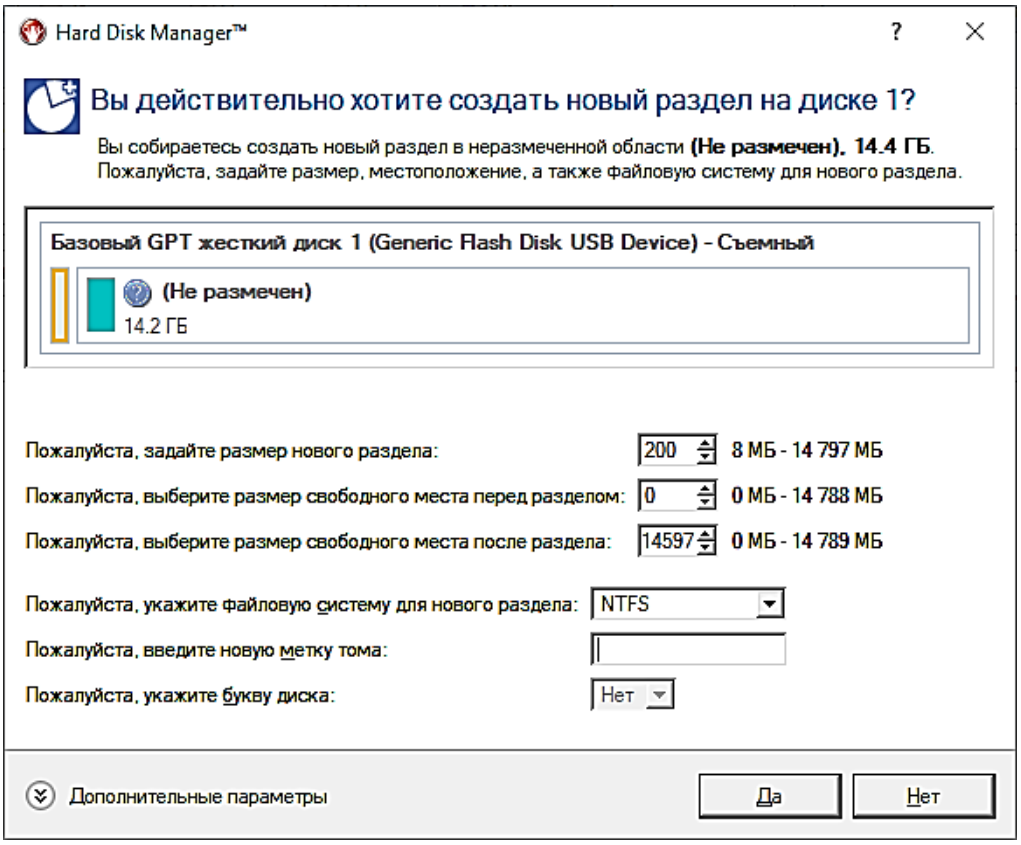
1.1. Получить у преподавателя накопитель информации.

1.2. Создать на нем раздел с файловой системой NTFS.

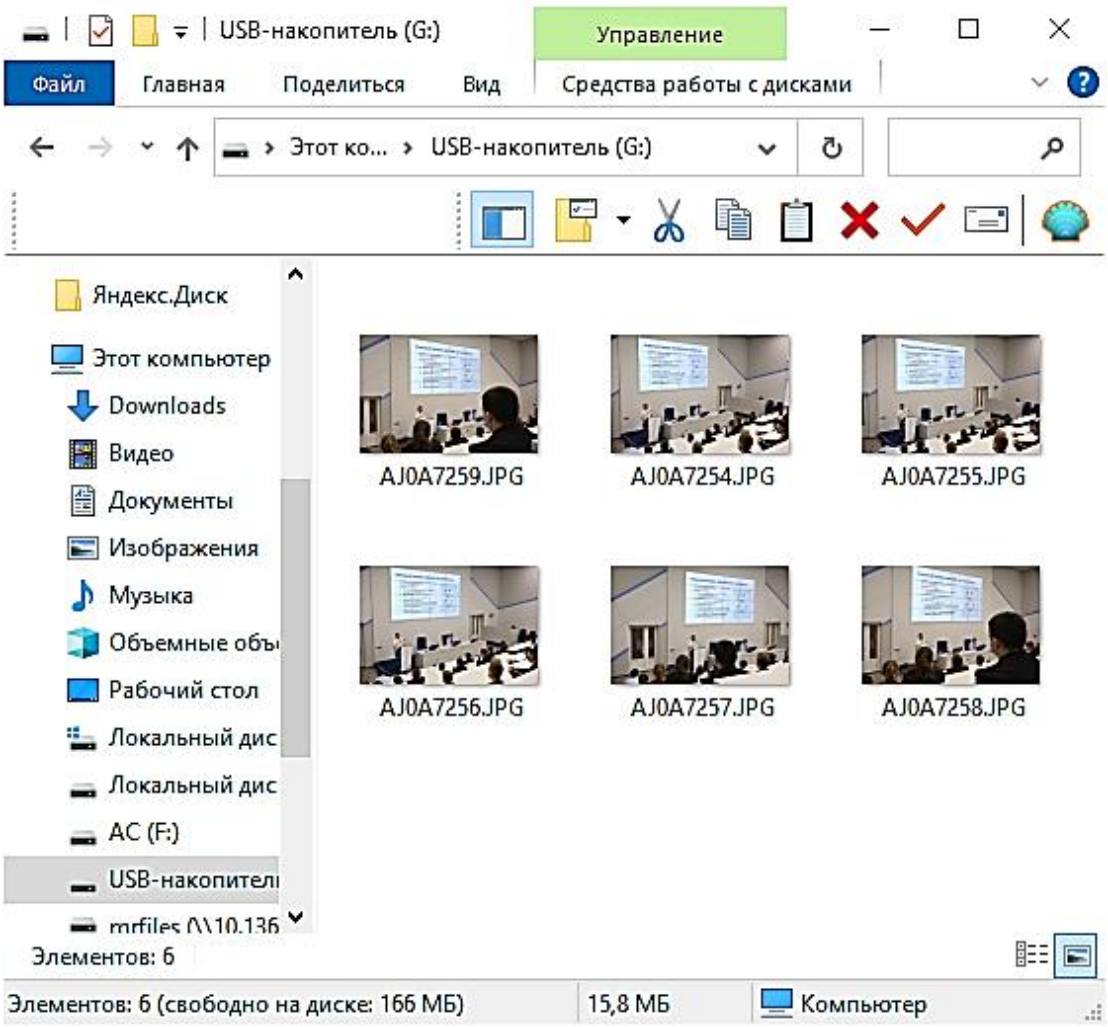
1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками.



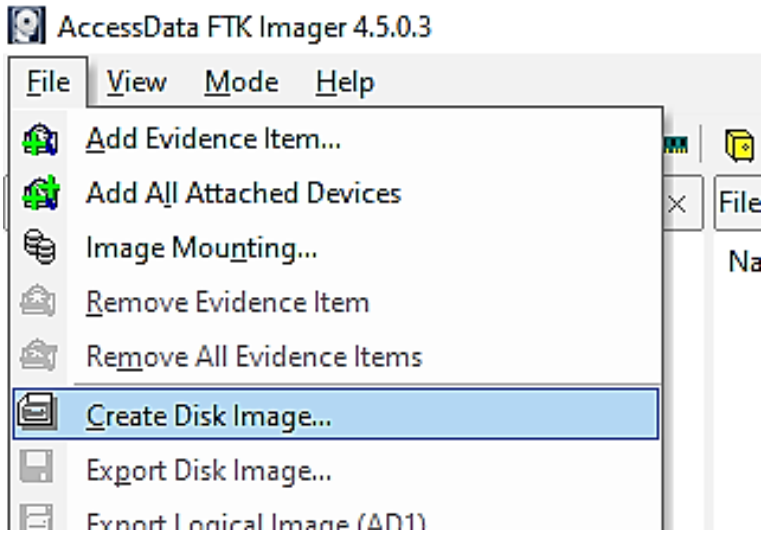
1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager.

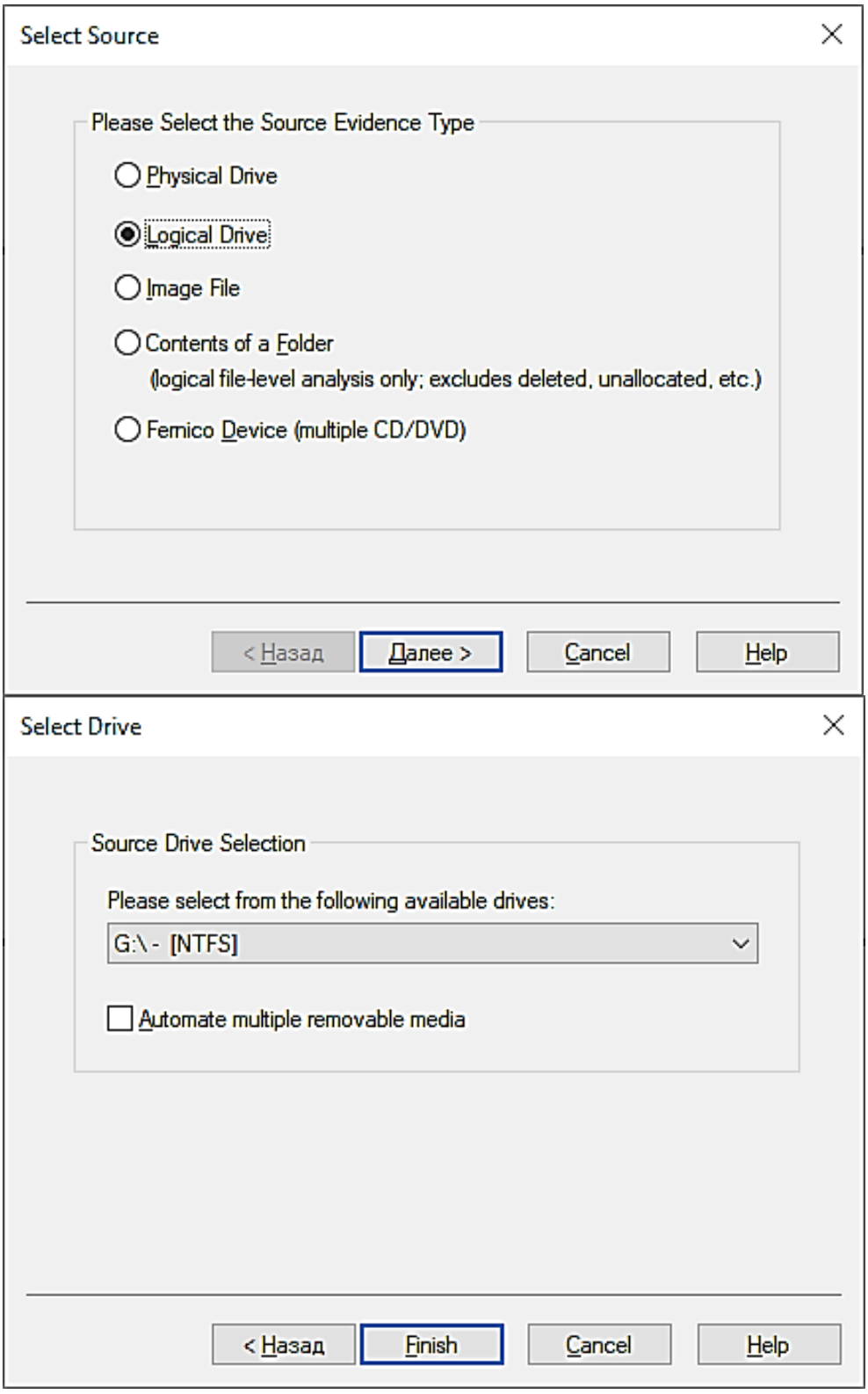


1.3. Скопировать в созданный раздел несколько произвольных графических файлов. Сделать скриншот.

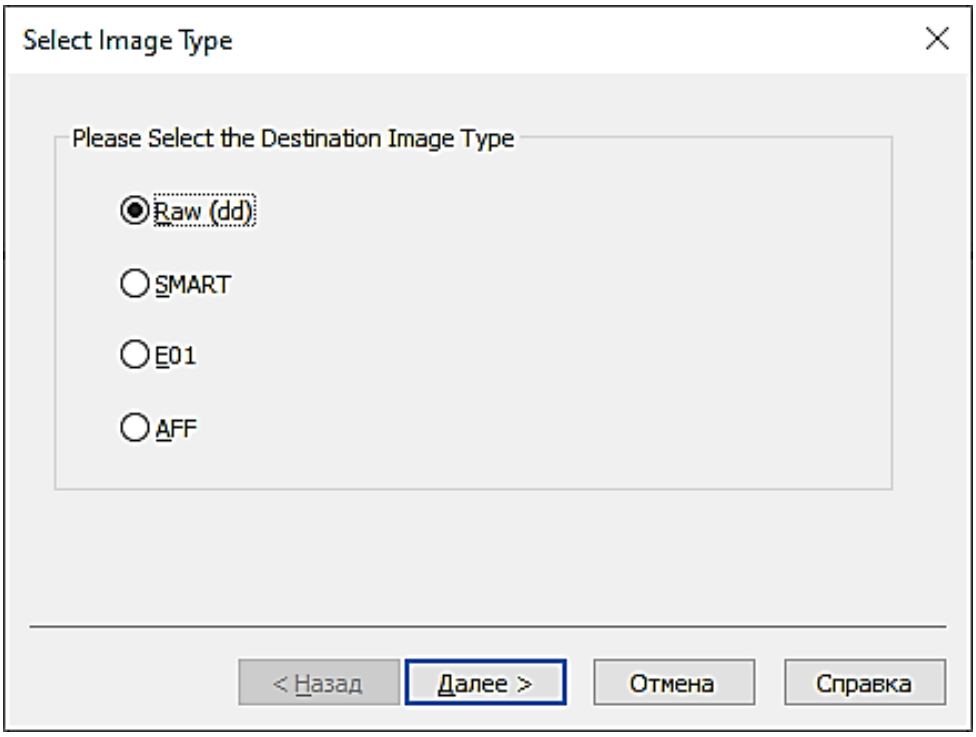


1.4. Удалить скопированные графические файлы.
1.5. Создать файл-образ созданного раздела.
1.5.1. Для этого запустить ПО AccessData FTK Imager.
1.5.2. Выбрать пункт Create Disk Image.

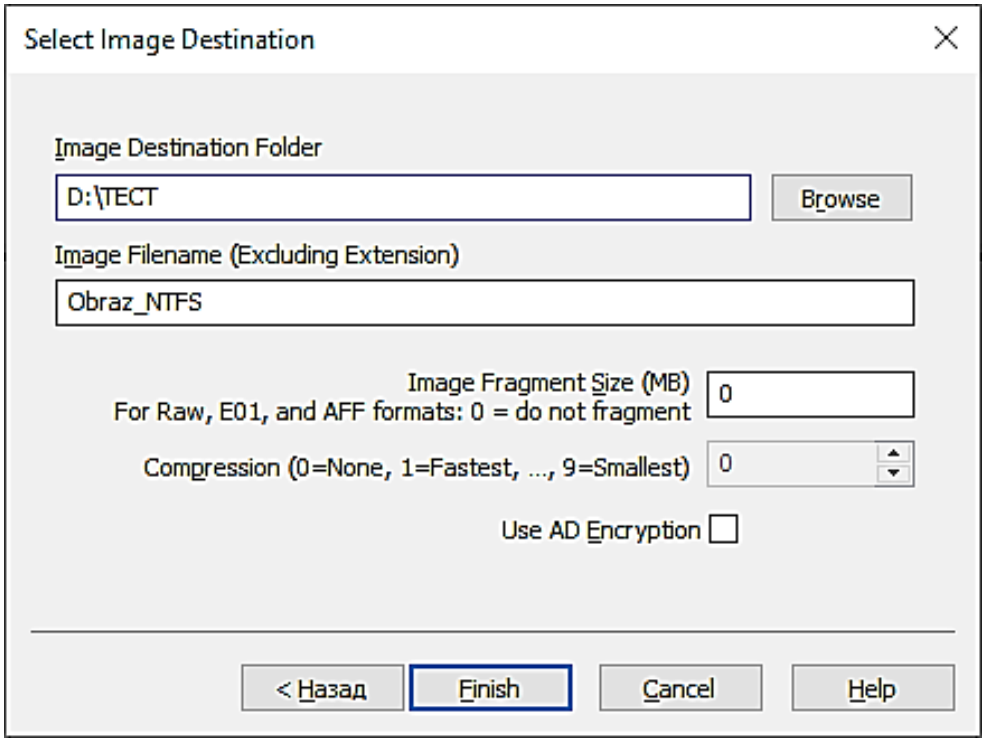




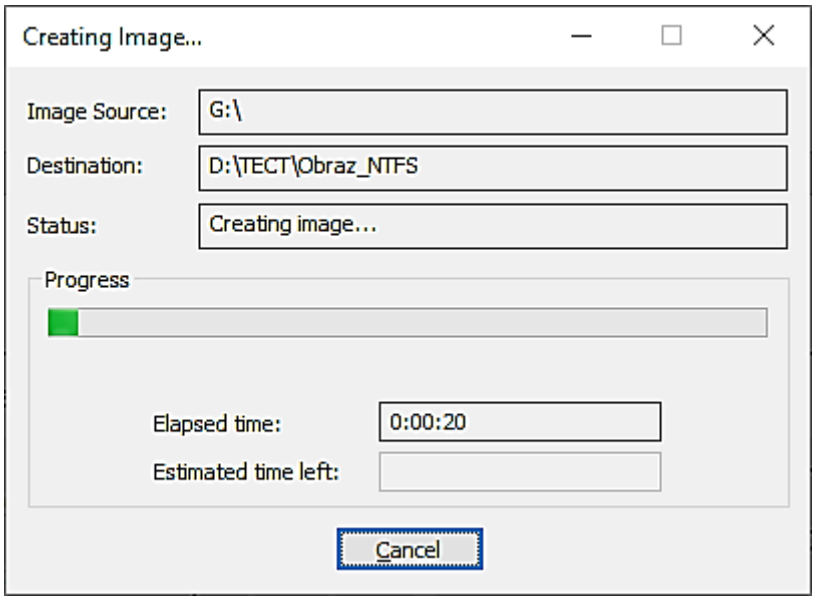
1.5.3. Выбрать формат файла образа Raw(dd).



1.5.4. Указать место сохранения файла образа диск D. Присвоить имя файлу образа. Размер фрагмента указать 0.



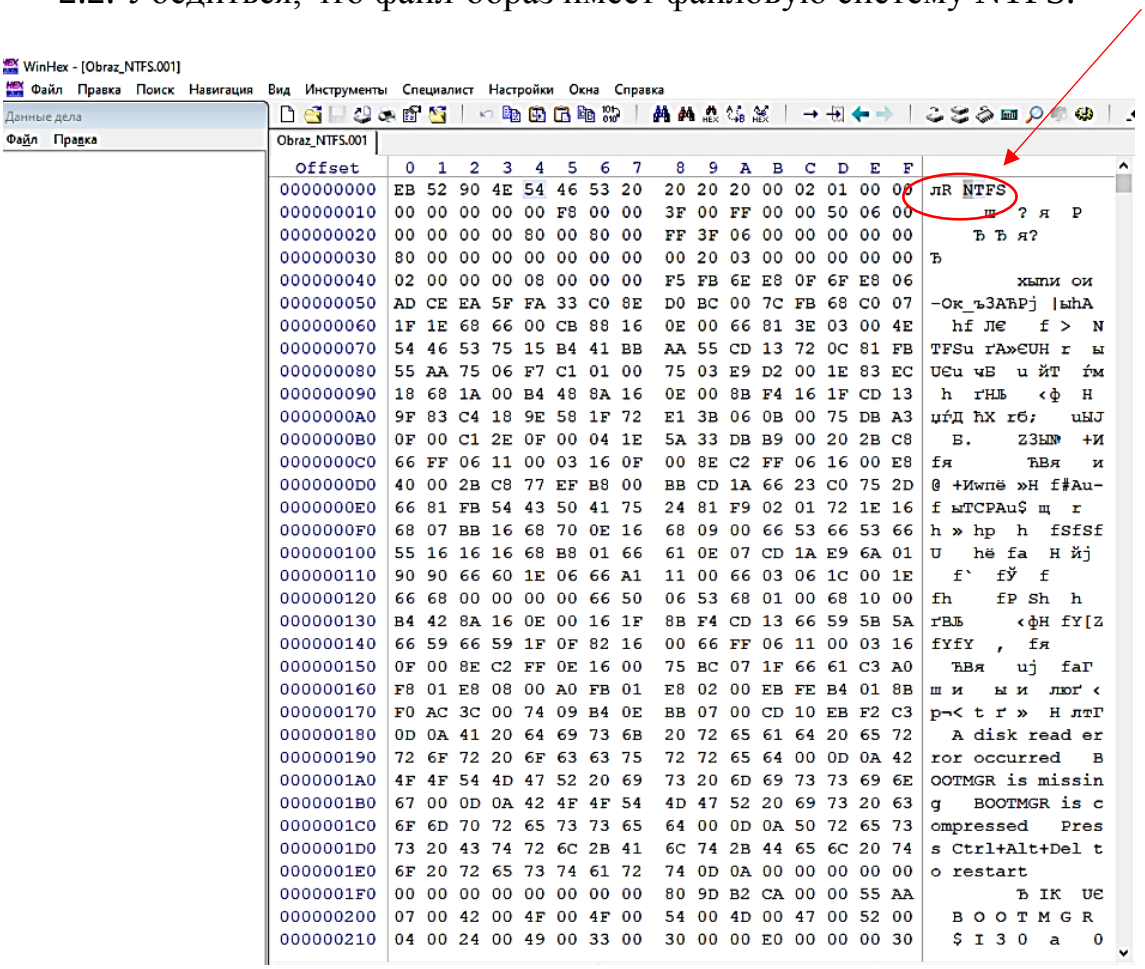
1.5.5. Если все сделали правильно, то запустится процесс создания файла-образа.



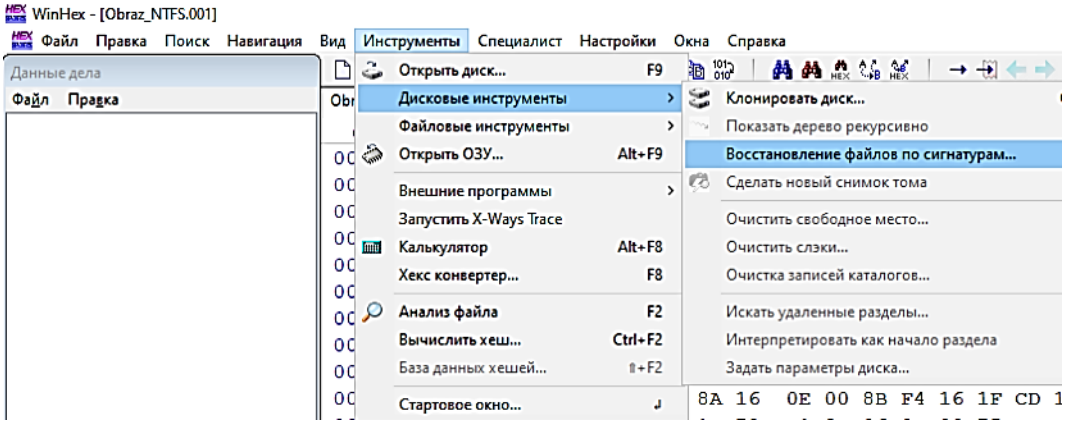
2. Восстановить удаленные графические файлы из файла-образа.

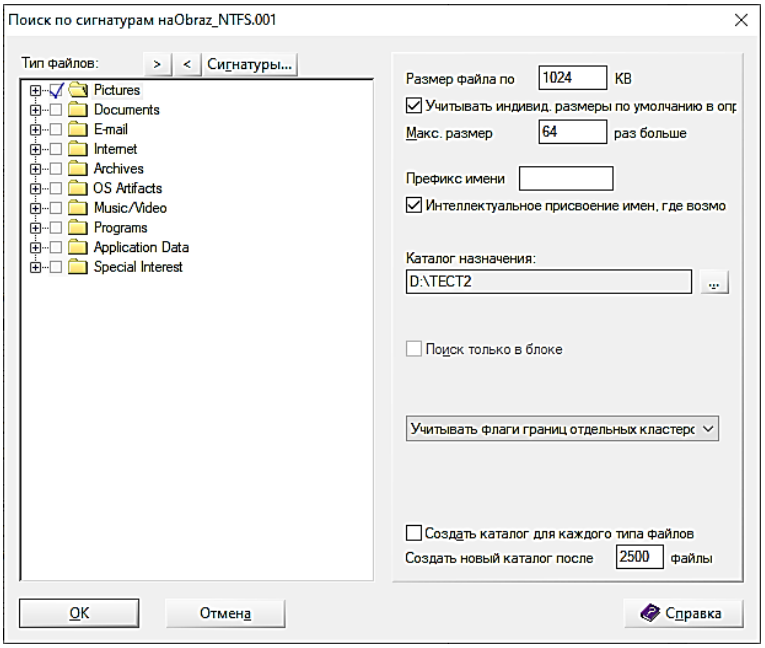
2.1. Открыть созданный файл-образ в программе WinHex.

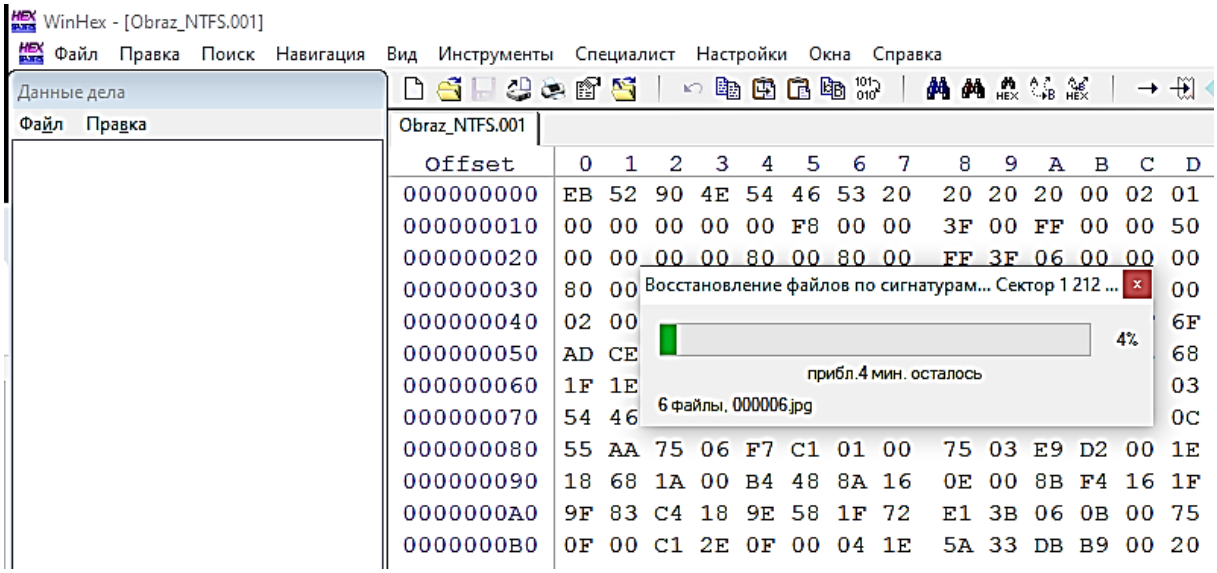
2.2. Убедиться, что файл-образ имеет файловую систему NTFS.



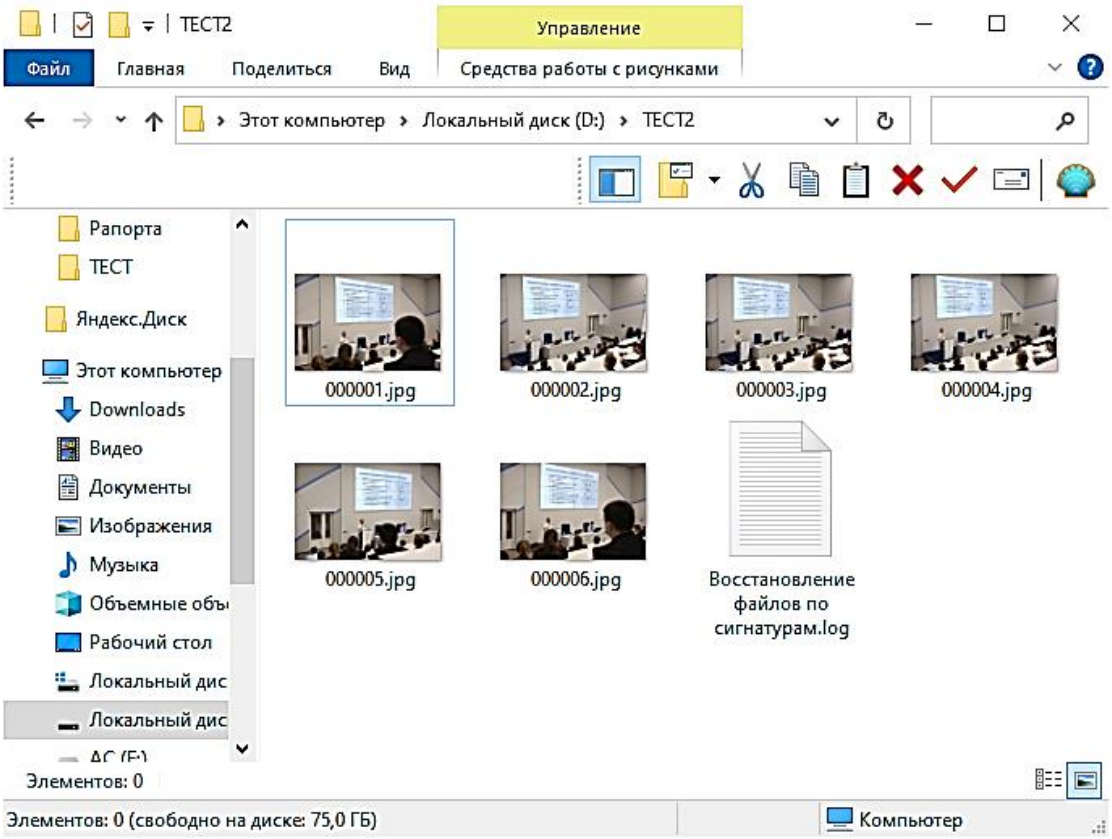
2.3. Восстановить графические файлы по сигнатурам.







3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы NTFS?
3. Какого максимального размера файлы можно помещать в файловую систему NTFS?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм создания файла-образа.
10. Какие типы файлов вы знаете?

ЛАБОРАТОРНАЯ РАБОТА № 14

ВОССТАНОВЛЕНИЕ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ FAT32 ФЛЕШ-НАКОПИТЕЛЯ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков по восстановлению информации с помощью специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации.

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы

узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology

File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т.д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

Специализированное ПО Belkasoft Evidence Center

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными

стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

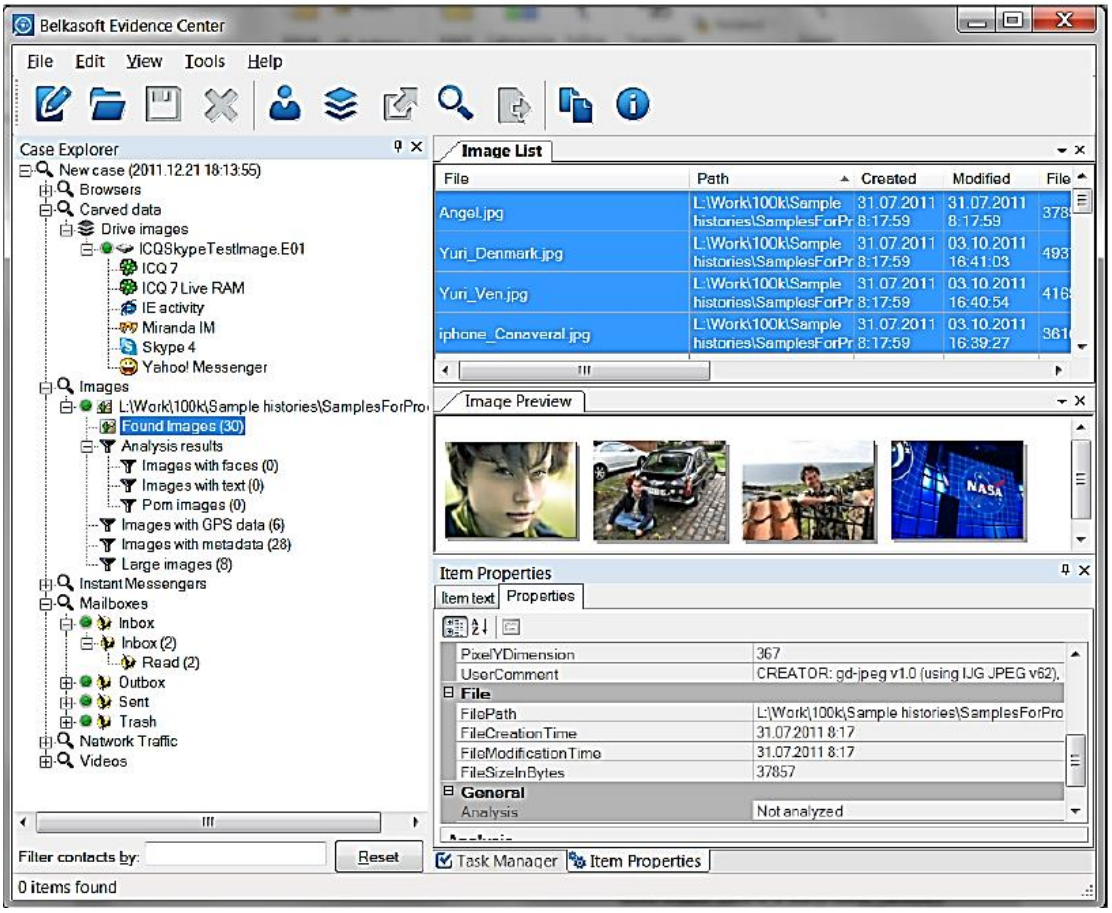


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных

- Доказательства можно разбивать по «делам»
- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

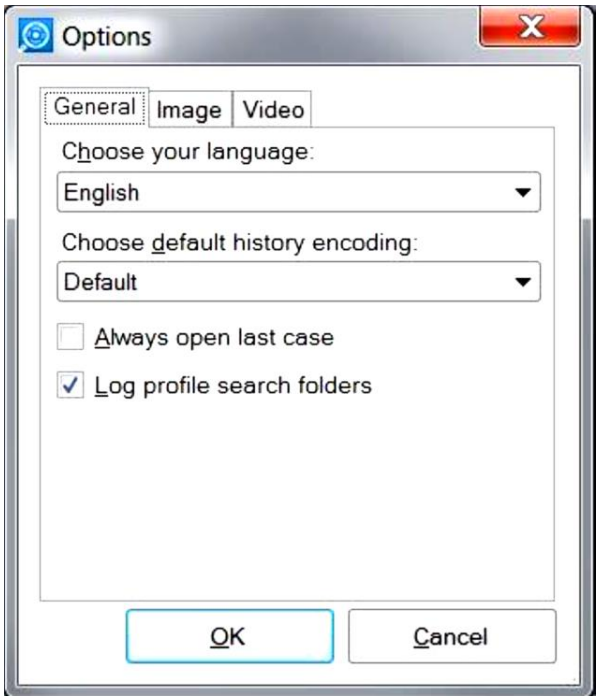


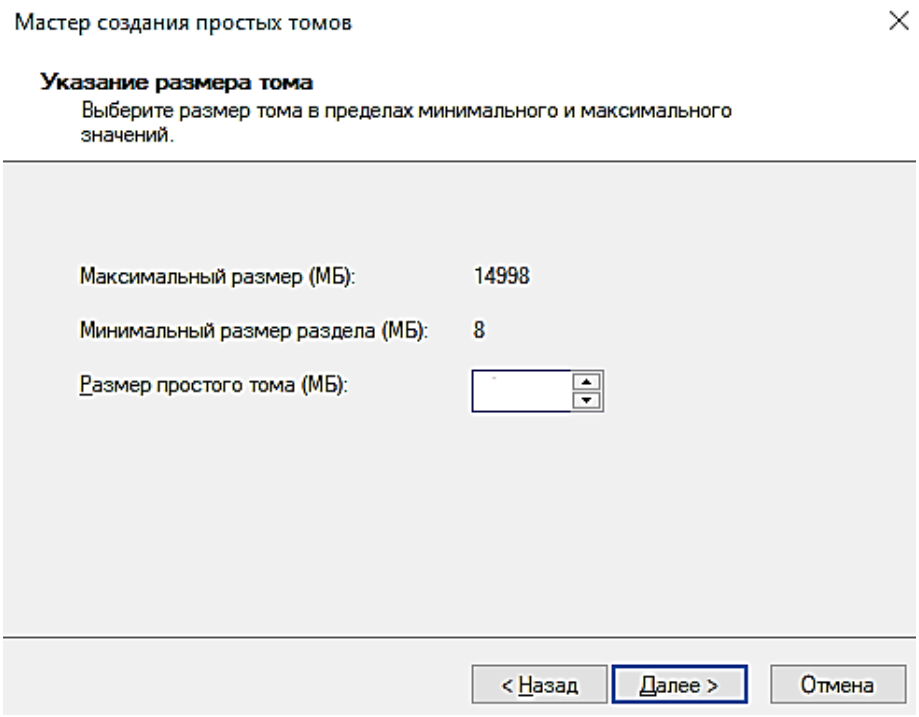
Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

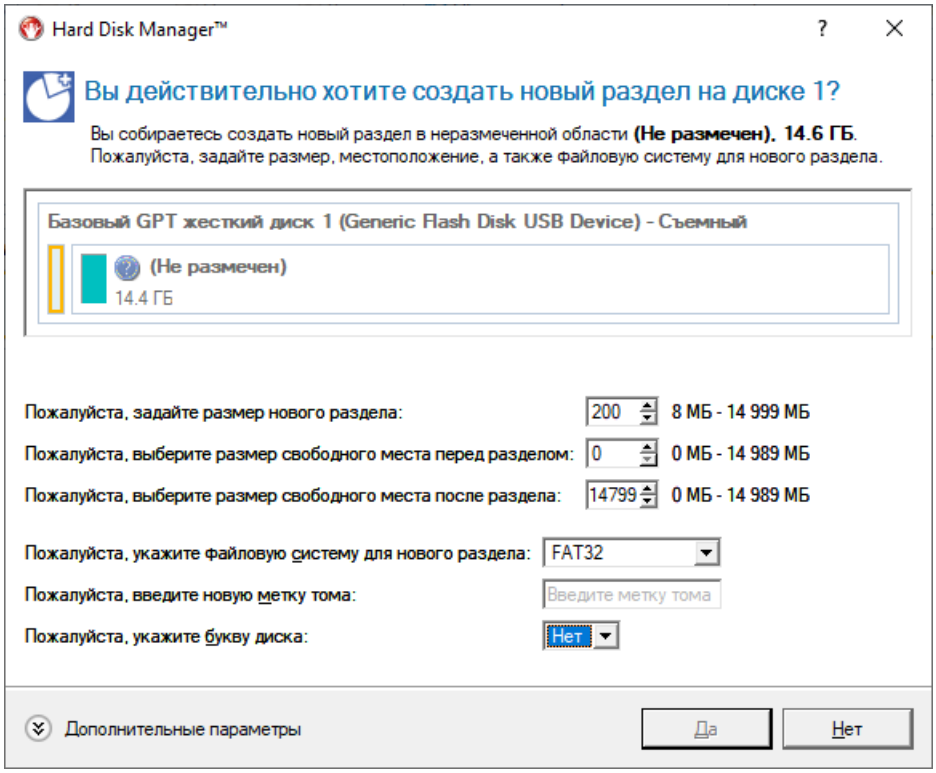
Порядок выполнения работы

1. Получить у преподавателя накопитель информации.
2. Создать на нем раздел с файловой системой FAT32 размером 200 Мб.

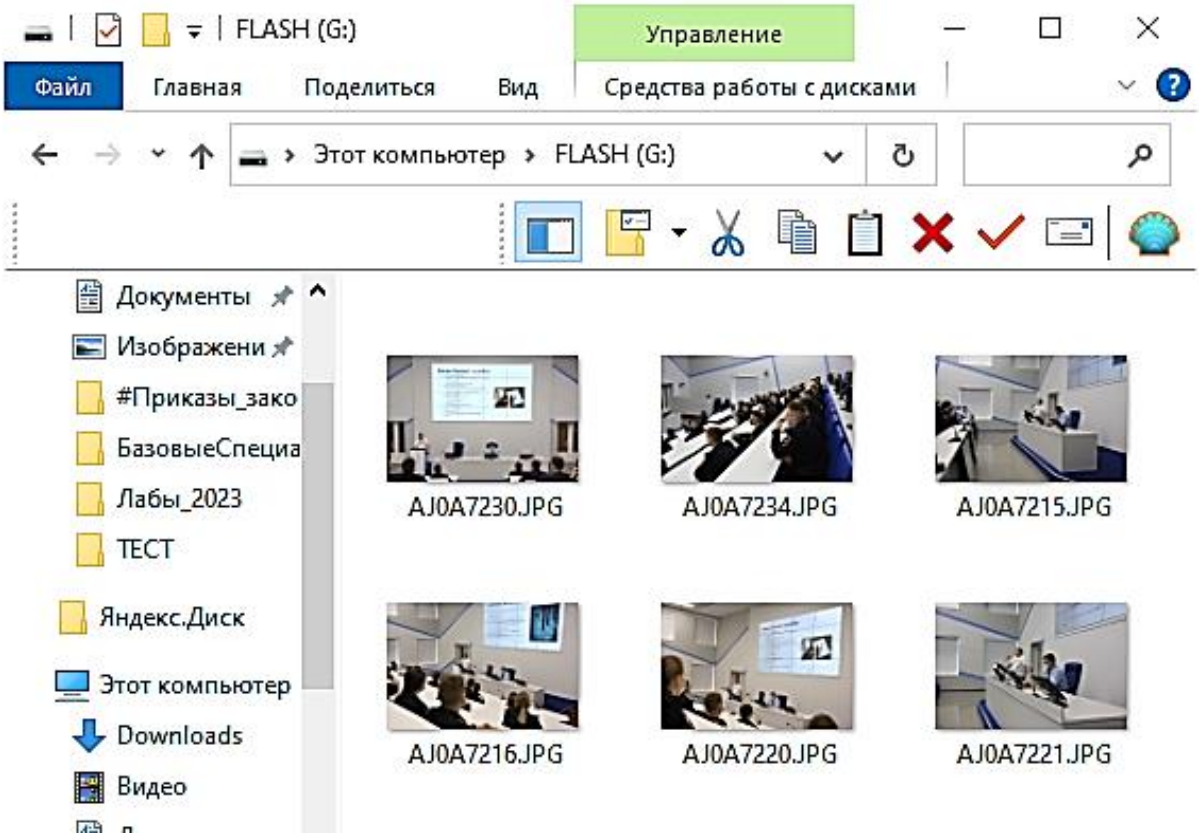
2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками.



2.2. Либо можно использовать ПО Paragon Hard Disk Manager.



3. Скопировать в созданный раздел несколько произвольных графических файлов. Сделать скриншот.



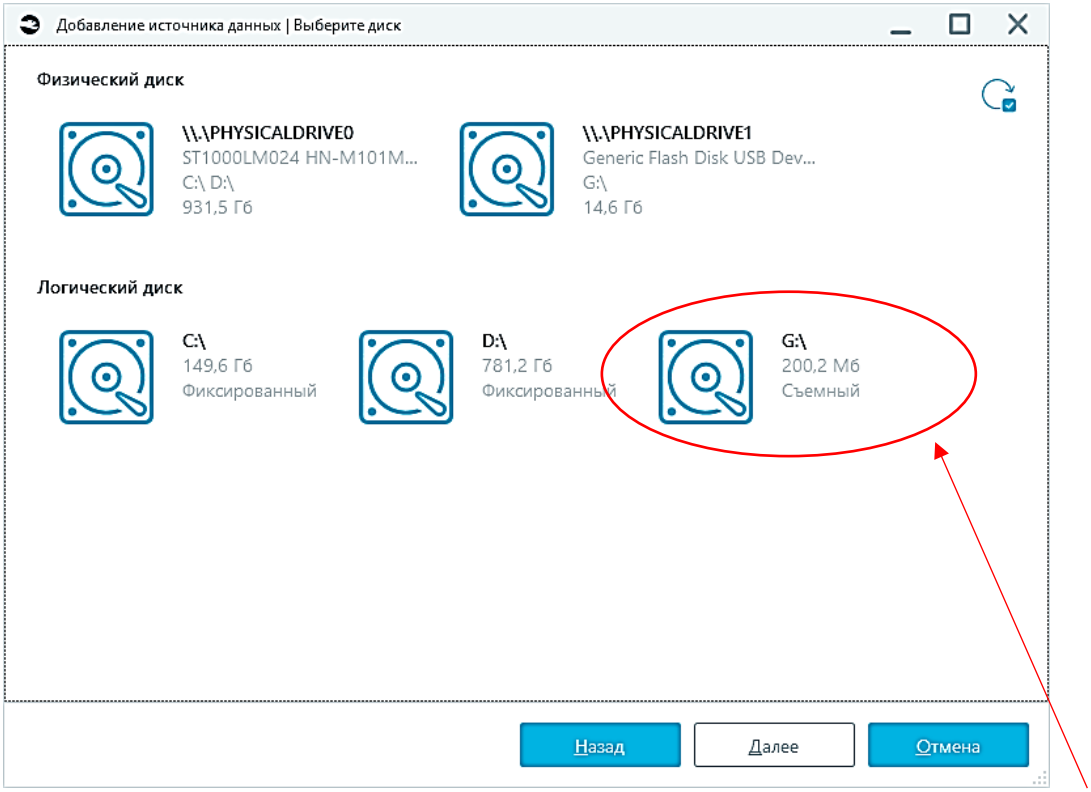
4. Удалить скопированные графические файлы.

5. Восстановить удаленные графические файлы с флеш накопителя с файловой системой FAT32 с помощью специализированного ПО Belkasoft Evidence Center.

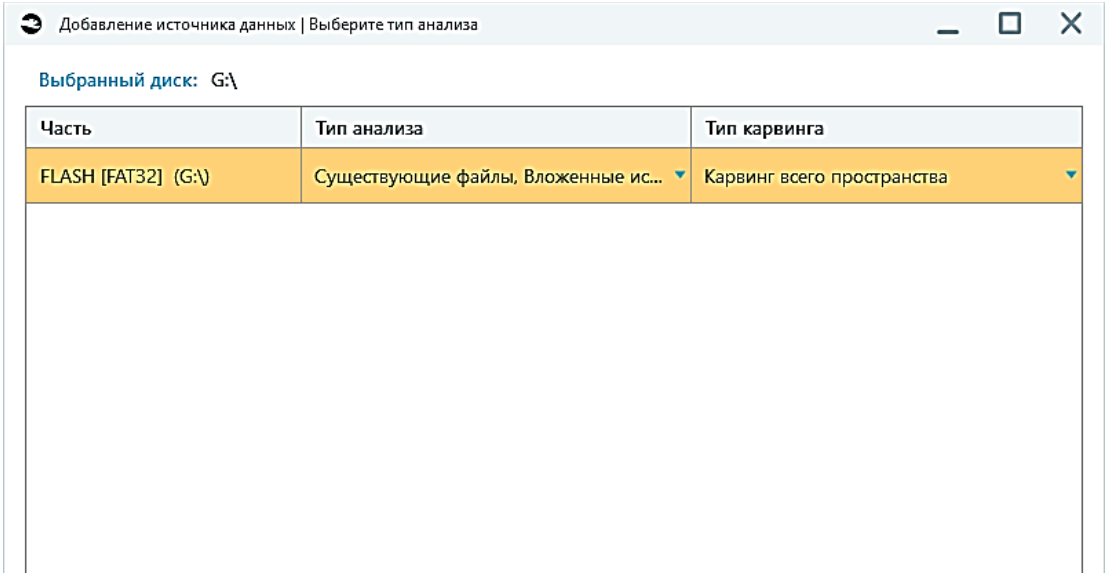
5.1. Для этого запустить ПО Belkasoft Evidence Center.

5.2. Создать новое дело и сохранить его в заранее созданный каталог на диске D.

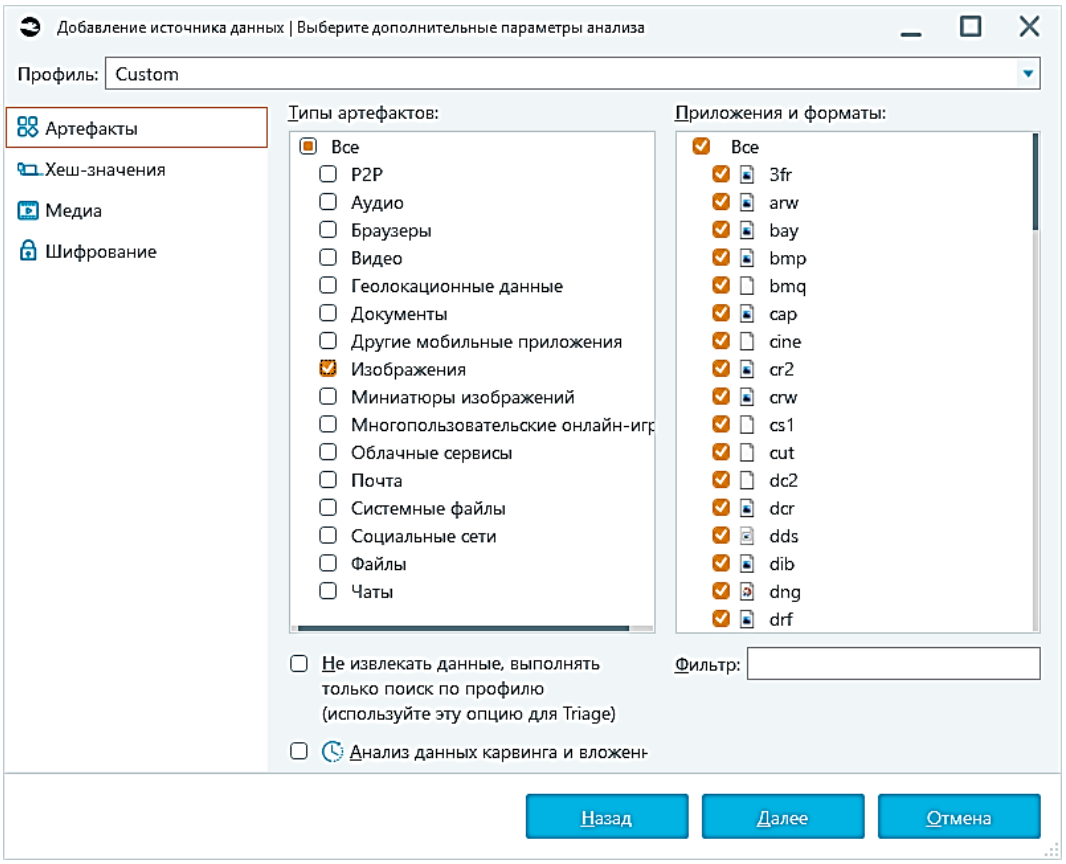
5.3. Добавить источник данных существующий, накопитель и выбрать флеш-накопитель с файловой системой FAT32. Логический диск.



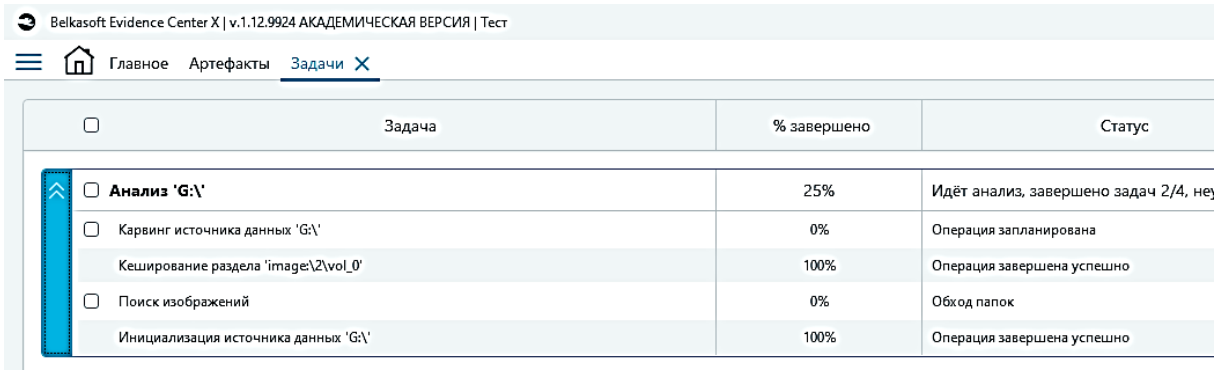
5.4. Выбрать «карвинг всего пространства» для раздела с файловой системой FAT32.



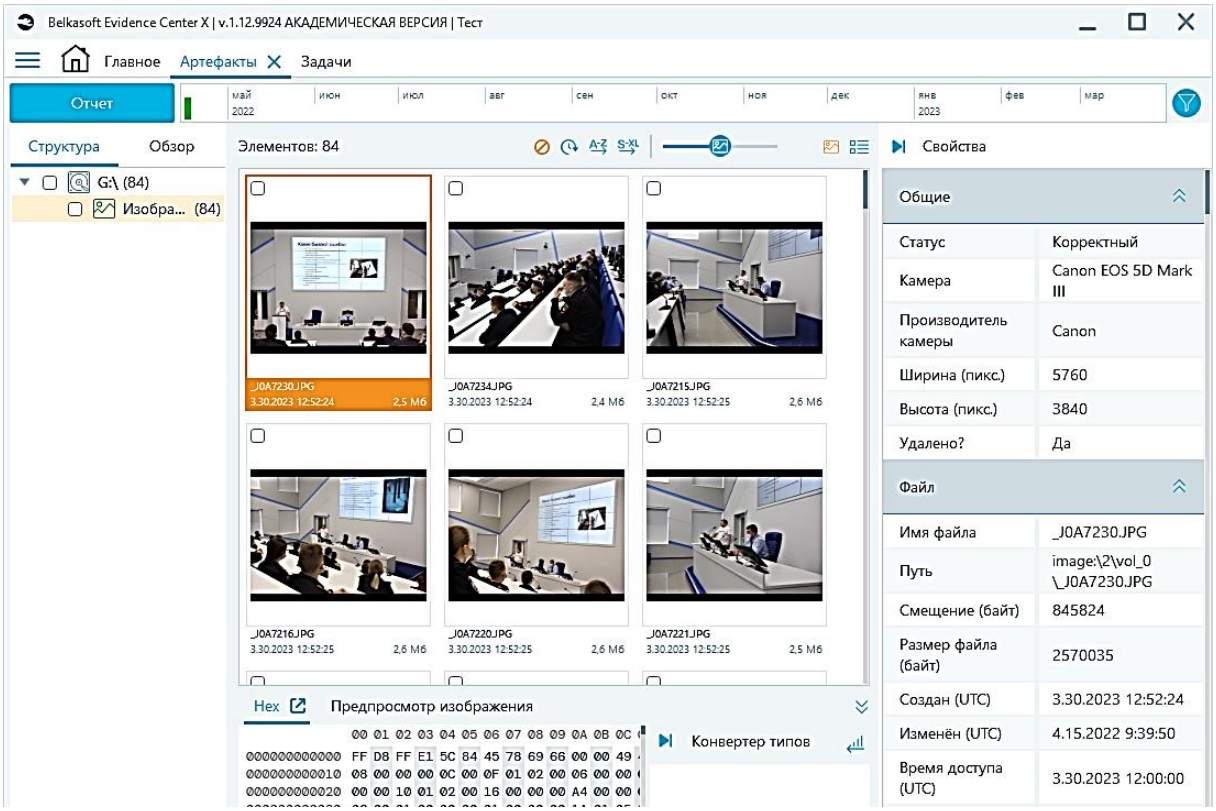
5.5. Выбрать артефакты «Изображения».



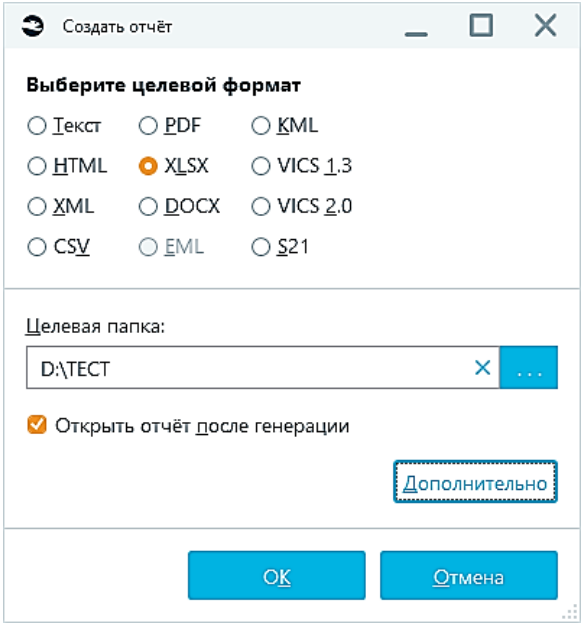
5.6. Проверить запущенную задачу.



6. Проверить восстановленные файлы. Сделать скриншот.



7. Сравнить скриншоты из пунктов 3 и 6.
8. Создать отчет по обнаруженным файлам-изображениям в формате XLSX. В отчете должны быть сведения о размере файла, дате его создания и дате последнего изменения. Для настройки нужных колонок воспользуйтесь пунктом «Дополнительно» перед созданием отчета.



9. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы FAT32?
3. Какого максимального размера файлы можно помещать в файловую систему FAT32?
4. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
5. Какие типы файлов вы знаете?
6. Перечислите основные возможности ПО Belkasoft Evidence Center.
7. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
8. С какими источниками данных может работать ПО Belkasoft Evidence Center?
9. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
10. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
11. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
12. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
13. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 15

ВОССТАНОВЛЕНИЕ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ NTFS ФЛЕШ-НАКОПИТЕЛЯ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков по восстановлению информации с помощью специализированного ПО.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации.

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы

узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology

File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т. д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

Специализированное ПО Belkasoft Evidence Center

Belkasoft Evidence Center позволяет извлекать данные, искать, хранить и делиться цифровыми доказательствами, полученными из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий.

Данными, полученными в ходе экспертизы, можно делиться с другими экспертами и прочими заинтересованными лицами при помощи бесплатного портативного инструмента Evidence Reader.

При поиске цифровых доказательств Belkasoft Evidence Center использует подходы, позволяющие быстро находить наиболее значимые артефакты, не тратя время на избыточные операции.

Мощные аналитические функции, такие как граф связей с обнаружением групп, временная шкала, анализ изображений, основанный на современных искусственных нейронных сетях, анализ видео- и аудиофайлов помогут вам быстро обнаружить необходимые улики.

Belkasoft Evidence Center автоматизирует большинство задач, благодаря чему вы получаете возможность заниматься более сложными

стратегическими задачами, которые могут быть выполнены только экспертом-криминалистом.

Продукт облегчает исследователю задачи поиска, анализа и хранения цифровых улик, найденных в чатах интернет-пейджеров, историях браузеров, почтовых ящиках, изображениях, видео, социальных сетях, программах P2P и многопользовательских онлайн-играх.

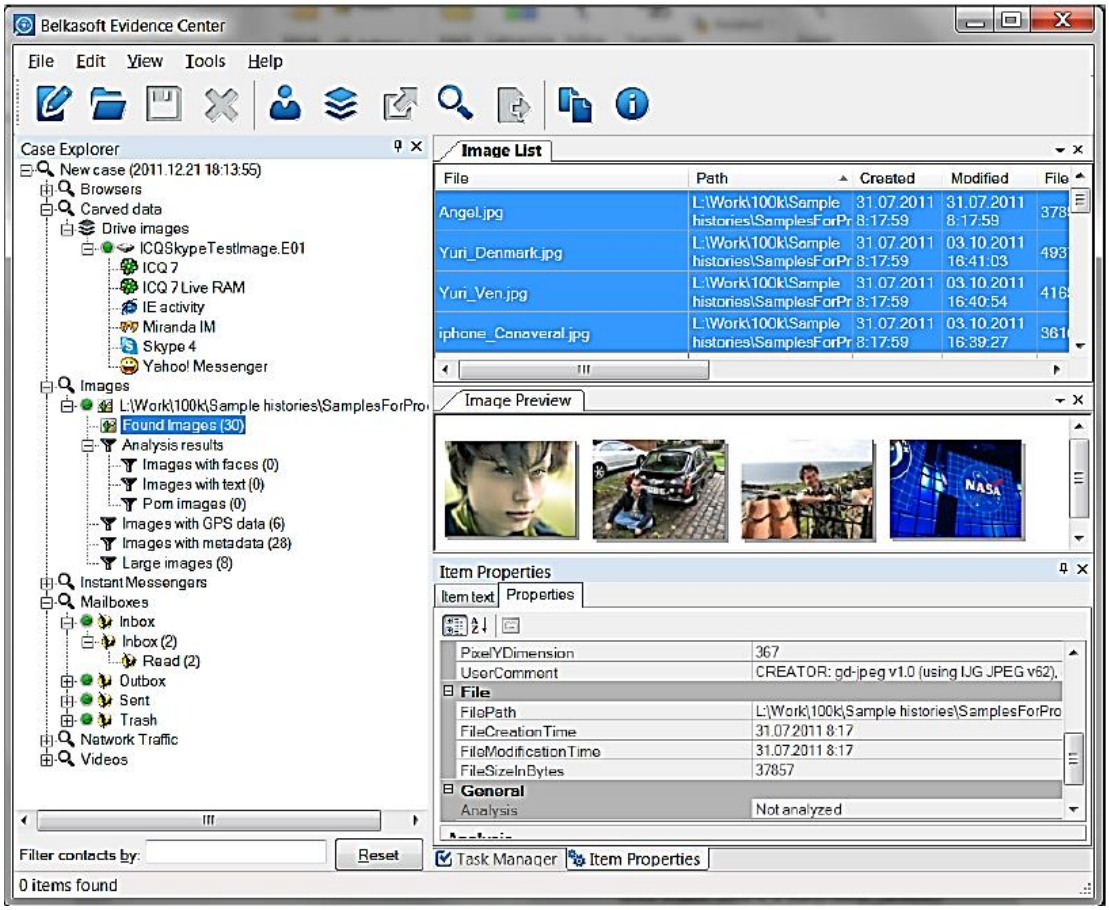


Рис. 1. Главное окно программы

- Поддержаны все основные интернет-чаты: Skype, Yahoo Messenger, ICQ и т.п.; в общей сложности более, чем 100 типов программ для Windows, Linux, Mac OS X и мобильных устройств
- Поддержаны все основные браузеры под ОС Windows
- Поддержано извлечение чатов и прочей информации, такой, как обновления статусов Twitter, отправленных в социальные сети; P2P программ и разговоров в многопользовательских онлайн-играх
- Изображения и видео-файлы анализируются на наличие порнографии, лиц и отсканированного текста
- Найденная информация сохраняется в базе данных
- Доказательства можно разбивать по «делам»

- Поддержано извлечение удалённой истории (при условии, что она не перетёрта или не удалена специальными средствами)
- Стандартные образы дисков в формате EnCase, SMART и DD могут быть подключены к «делу», включая диски ОС Windows и MacOS
- Доступен анализ дампов оперативной памяти
- Благодаря наличию быстрой СУБД Microsoft SQL Server 2008, поддержана возможность работы с большими делами (например, содержащими несколько 10-гигабайтных почтовых ящиков)
- Редакция Team Edition позволяет одновременную работу нескольких пользователей

В мире цифровой криминалистики есть набор правил, которому должно соответствовать ПО, претендующее на звание «криминалистическое». Belkasoft Evidence Center полностью соответствует этим правилам.

• ПО никогда не пытается писать на носитель, которые подвергается анализу. Благодаря этому оно может работать с устройствами защиты от записи, образами дисков и дампами оперативной памяти. Ни единого бита информации не будет изменено!

• Чтобы удостовериться, что исследуемая история не изменена в процессе анализа, ПО подсчитывает хеш-значения для каждого профиля, добавленного в дело. Вы можете сравнить исходное хеш-значение с текущим в любое время

• ПО не требует никаких паролей или прочей информации владельца того или иного профиля. Всё извлечение данных и их расшифровка производятся без требования указать подобную информацию (кроме профилей Яху, см. далее)

• ПО работает под логином аналитика на компьютере аналитика и не требует наличия на нём установленных клиентских программ, профили которых изучаются. Например, не требуется установленного Outlook, чтобы извлечь почту из почтового ящика Outlook.

Продукт позволяет установить некоторые опции, доступные в подменю Options (опции) меню Tools (инструменты) главного меню.

В зависимости от редакции продукта, которую вы имеете, окно опций может содержать одну или более вкладок, включая вкладки General (основные), Image (изображение) and Video (видео).

Закладка «Основные опции» содержит следующие настройки:

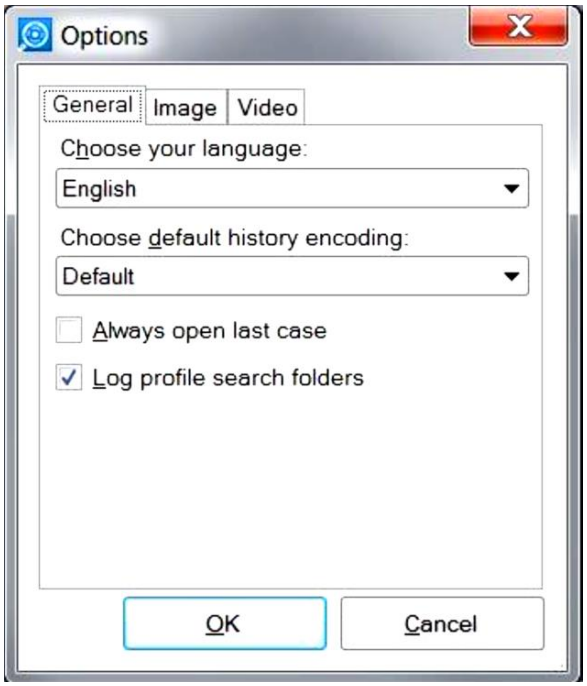


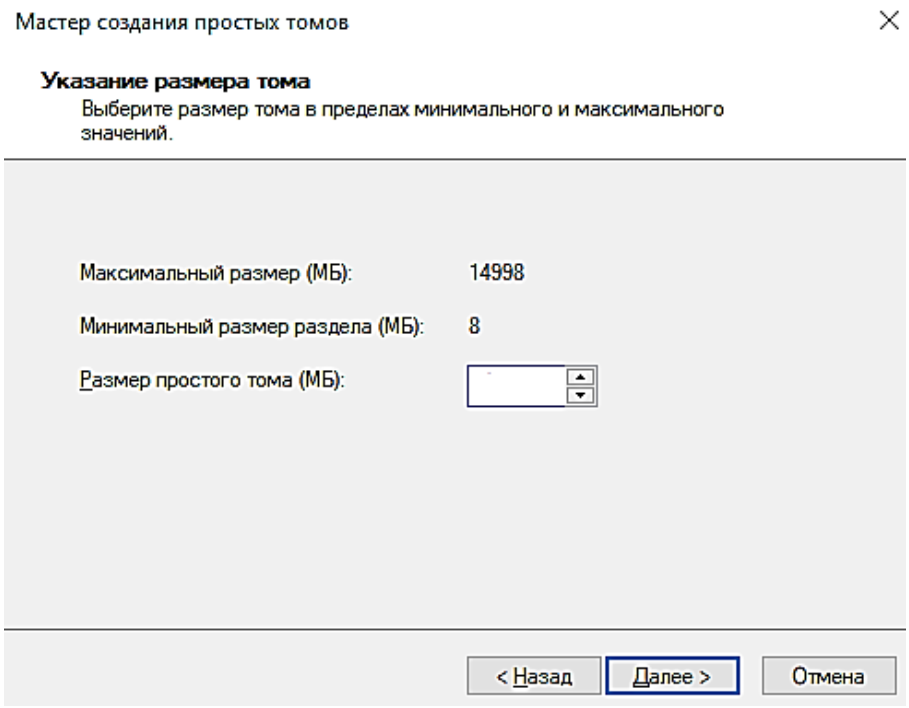
Рис. 2. Закладка «Основные опции»

- Language (язык). Английский является языком по умолчанию. Прочие варианты будут появляться по мере перевода на другие языки.
- Default encoding (кодировка по умолчанию). Если вы часто работаете с историями в некоторой кодировке, отличной от вашей системной, вы можете сэкономить время, установив нужную кодировку по умолчанию. Например, если ваша системная кодировка по умолчанию – немецкая, а вы работаете чаще всего с китайской, выберите Chinese Simplified как кодировку по умолчанию. Это позволит вам не выбирать каждый раз эту кодировку для каждого отдельного профиля.
- Always open the last case (всегда открывать последнее дело). Когда эта опция выбрана, продукт не будет спрашивать вас при старте, какое дело вы хотите открыть. Он всегда будет открывать то, с которым вы работали в последний раз.
- Log profile search folders (логгировать директории поиска профилей). Если вы подозреваете, что продукт не обошёл все существующие директории на интересующем вас устройстве, вы можете установить эту опцию. Когда она выбрана, продукт сохранит в логе задачи поиска профилей все директории, которые он сумел обойти. Этот файл вы сможете просмотреть с помощью Управления задачами по окончании поиска. Учтите, что лог-файл может стать весьма большим, потому что на диске могут быть тысячи директорий.

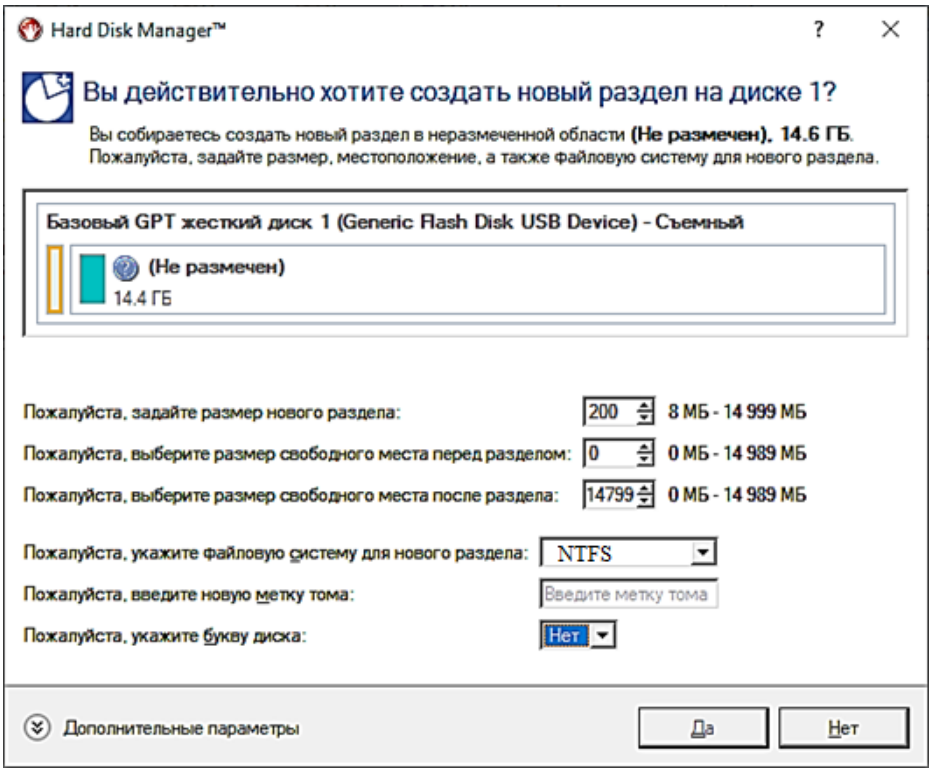
Порядок выполнения работы

1. Получить у преподавателя накопитель информации.
2. Создать на нем раздел с файловой системой NTFS размером 200 Мб.

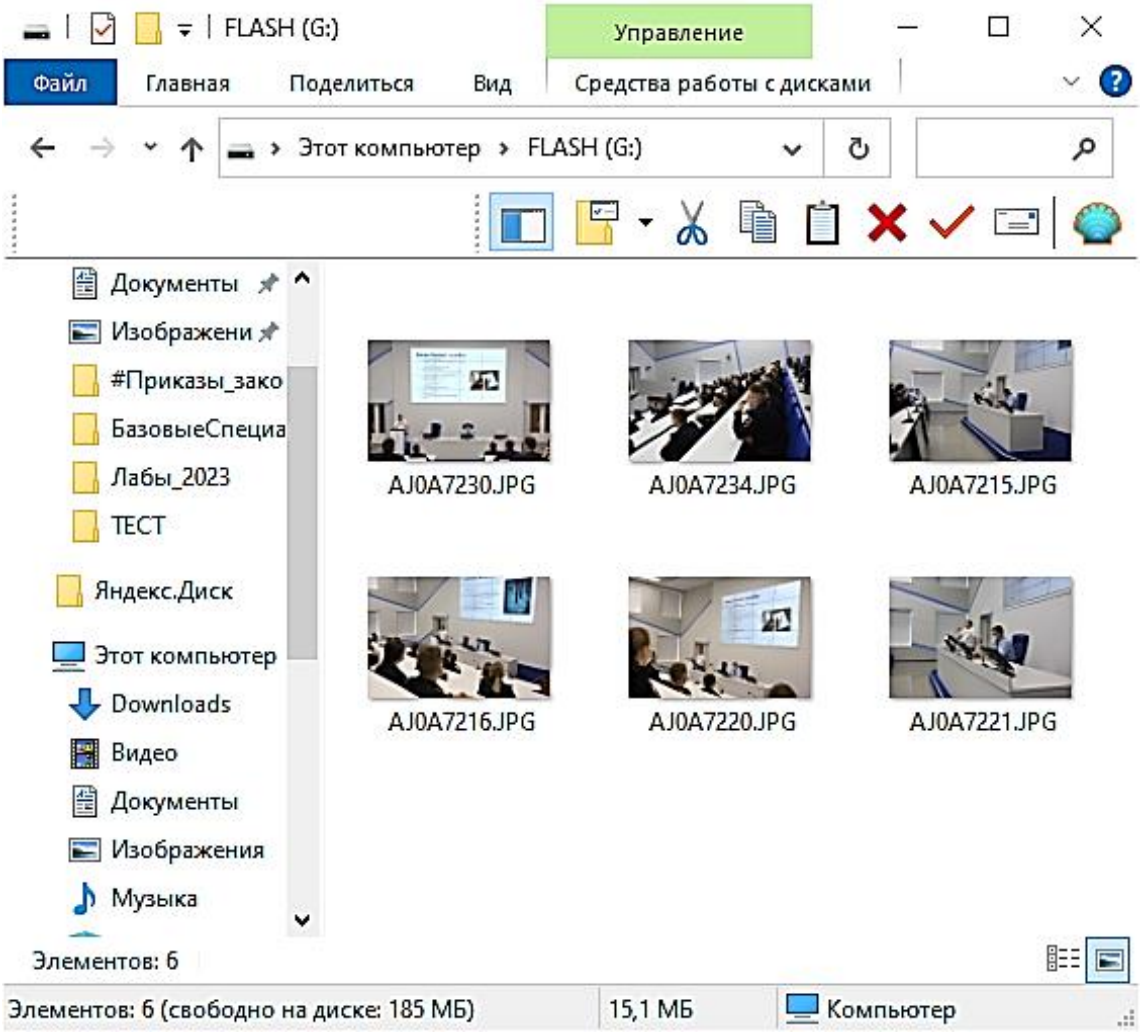
2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками.



2.2 Либо можно использовать ПО Paragon Hard Disk Manager.



3. Скопировать в созданный раздел несколько произвольных графических файлов. Сделать скриншот.



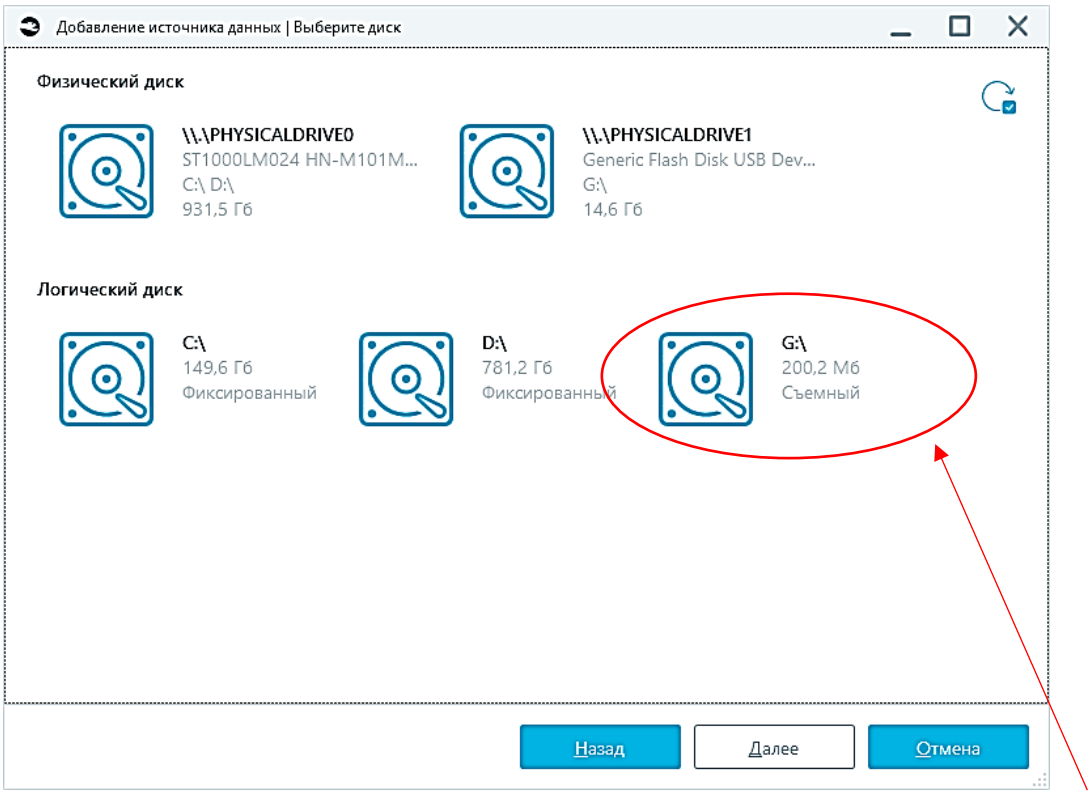
4. Удалить скопированные графические файлы.

5. Восстановить удаленные графические файлы с флеш накопителя с файловой системой NTFS с помощью специализированного ПО Belkasoft Evidence Center.

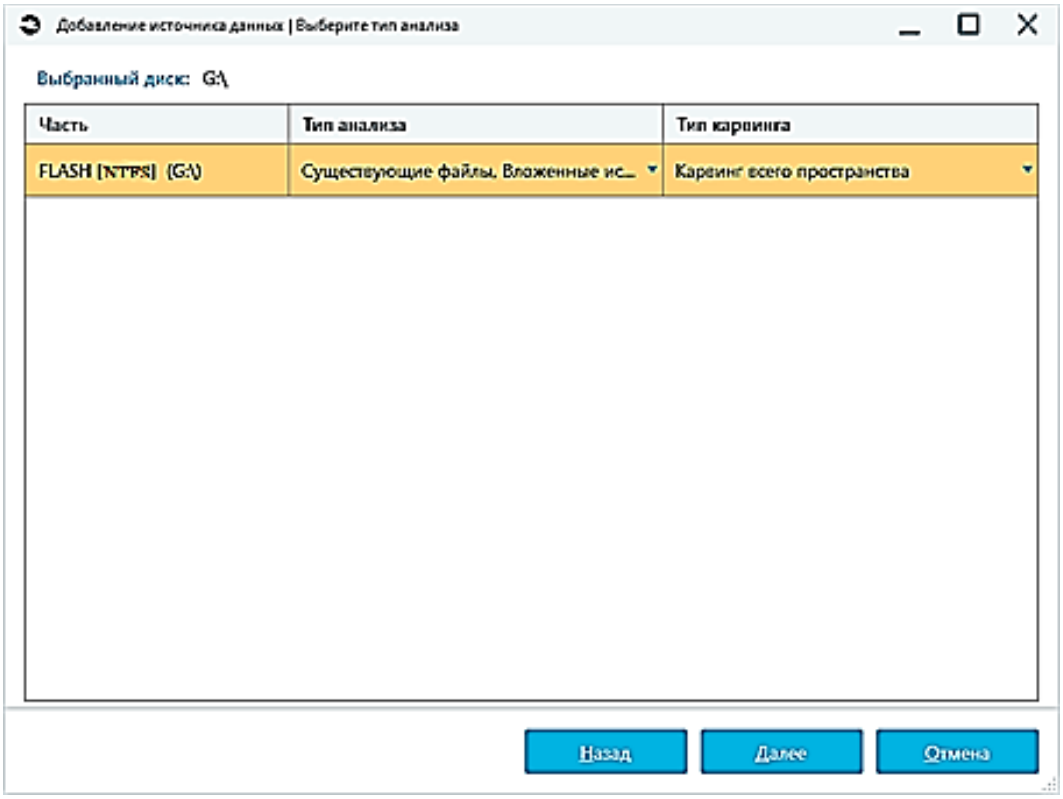
5.1. Для этого запустить ПО Belkasoft Evidence Center.

5.2. Создать новое дело и сохранить его в заранее созданный каталог на диске D.

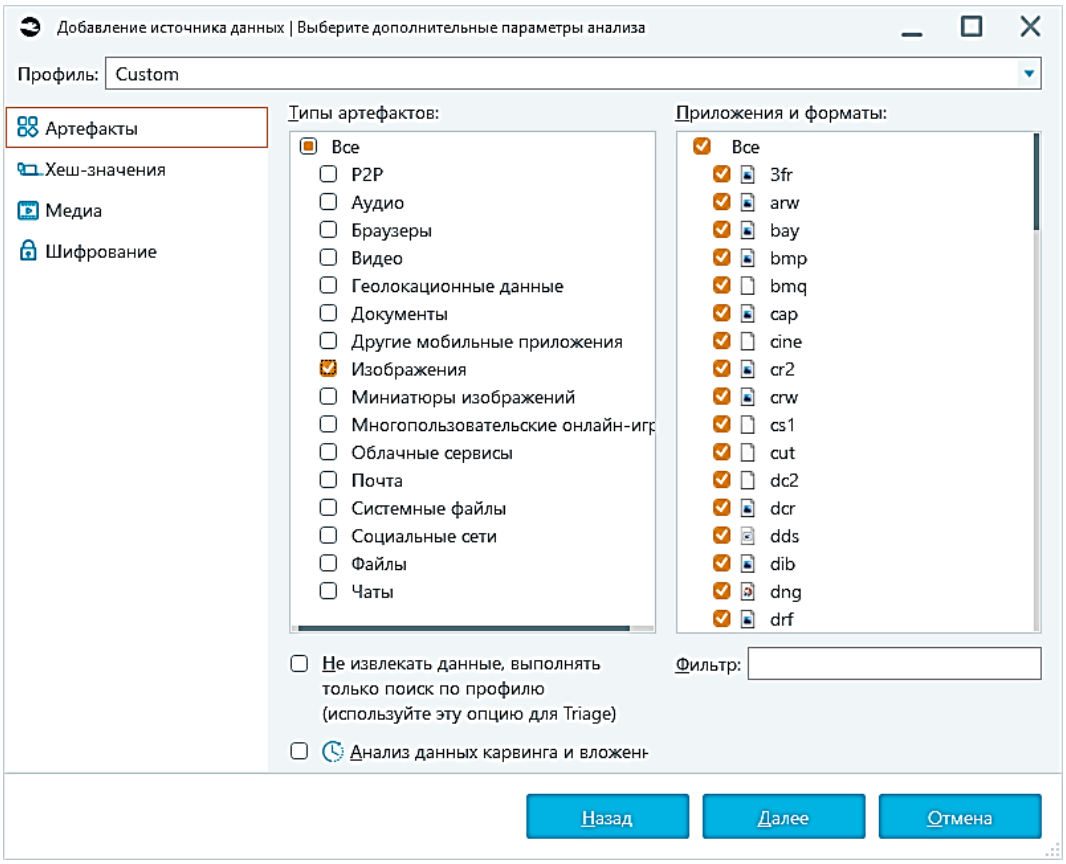
5.3. Добавить источник данных существующий, накопитель и выбрать флеш-накопитель с файловой системой NTFS. Логический диск.



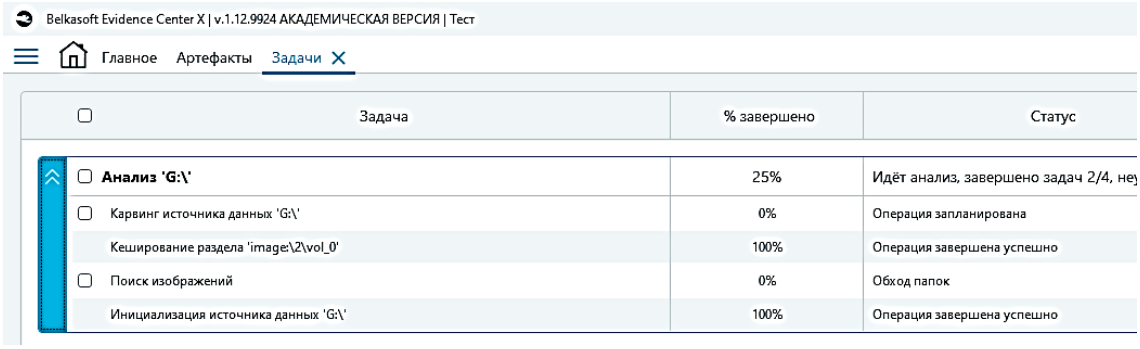
5.4. Выбрать «Карвинг всего пространства» для раздела с файловой системой NTFS.



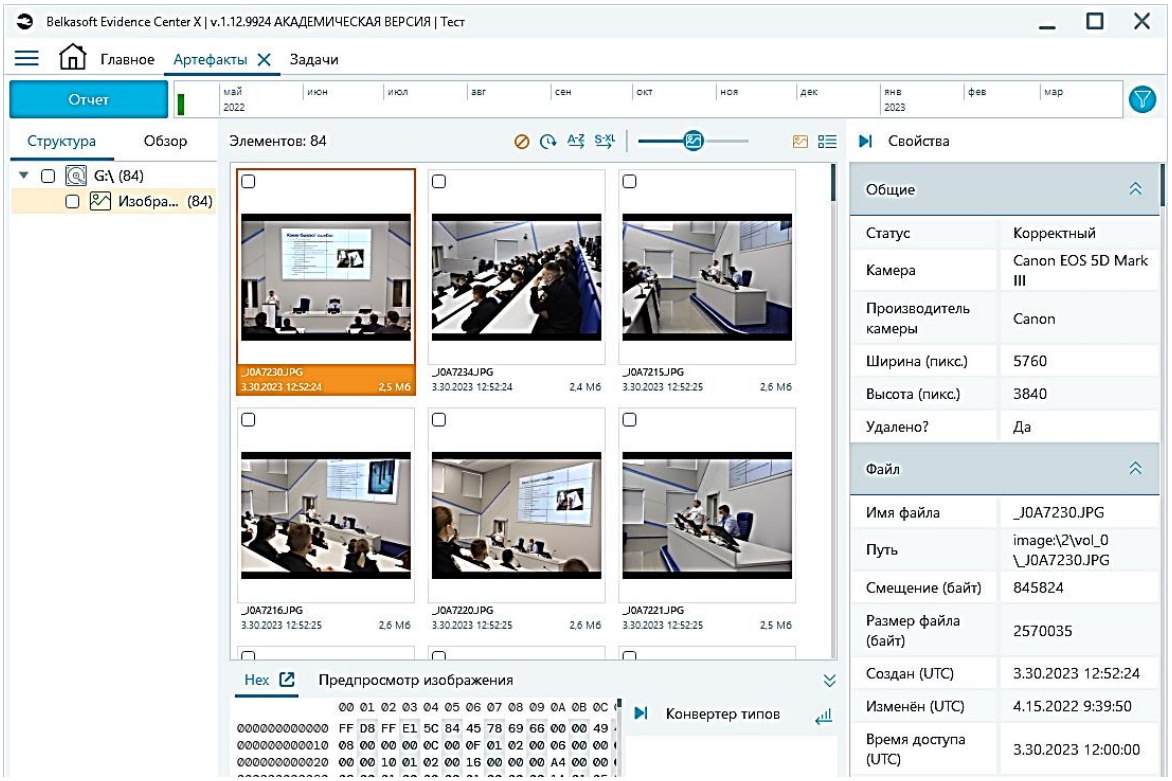
5.5. Выбрать артефакты «Изображения».



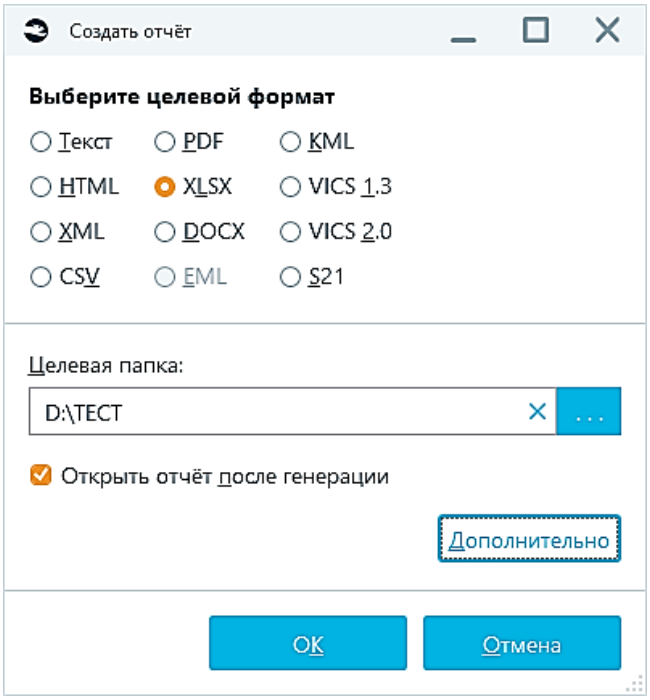
5.6. Проверить запущенную задачу.



6. Проверить восстановленные файлы. Сделать скриншот.



7. Сравнить скриншоты из пунктов 3 и 6.
8. Создать отчет по обнаруженным файлам-изображениям в формате XLSX. В отчете должны быть сведения о размере файла, дате его создания и дате последнего изменения. Для настройки нужных колонок воспользуйтесь пунктом «Дополнительно» перед созданием отчета.



9. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы NTFS?
3. Какого максимального размера файлы можно помещать в файловую систему NTFS?
4. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
5. Какие типы файлов вы знаете?
6. Перечислите основные возможности ПО Belkasoft Evidence Center.
7. Какую важную информацию из исследуемого персонального компьютера может извлекать ПО Belkasoft Evidence Center?
8. С какими источниками данных может работать ПО Belkasoft Evidence Center?
9. Поиск каких типов данных поддерживает ПО Belkasoft Evidence Center?
10. Для чего предназначена функция «Карвить» в ПО Belkasoft Evidence Center?
11. С какими объектами, кроме персонального компьютера, может работать ПО Belkasoft Evidence Center?
12. В какие форматы может выгружать отчеты ПО Belkasoft Evidence Center?
13. Как с помощью ПО Belkasoft Evidence Center произвести извлечение информации из персонального компьютера доступ ко входу в учетную запись ОС Windows которого ограничен паролем?

ЛАБОРАТОРНАЯ РАБОТА № 16

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ ДАМПА ОПЕРАТИВНОЙ ПАМЯТИ, ФАЙЛА ПОДКАЧКИ И ФАЙЛА ГИБЕРНАЦИИ

Цель работы: Получение практических навыков по восстановлению информации.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т. д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

Файлы подкачки и гибернации

В операционных системах Windows для работы используется так называемый файл подкачки pagefile.sys (скрытый и системный, обычно находится на диске C), представляющий своего рода «расширение» оперативной памяти компьютера (иначе – виртуальная память) и обеспечивающий работу программ даже в том случае, когда физической памяти RAM недостаточно. Windows 10, 8.1 или Windows 7 также пытается переместить неиспользуемые данные из оперативной памяти в файл подкачки, причем, по информации Microsoft, каждая новая версия делает это лучше.

Помимо файла подкачки pagefile.sys, который был и в предыдущих версиях ОС, в Windows 10 присутствует новый скрытый системный файл swapfile.sys так же находящийся в корне системного раздела диска и, по сути, тоже представляющий собой своеобразный файл подкачки, используемый не для обычных («Классическое приложение» в терминологии Windows 10), а для «Универсальных приложений» UWP.

Новый файл подкачки swapfile.sys потребовался в связи с тем, что для универсальных приложений изменились способы работы с памятью и, в отличие от обычных программ, которые используют файл подкачки как обычную оперативную память, файл swapfile.sys используется как файл, хранящий «полное» состояние отдельных приложений, своего рода файл гибернации конкретных приложений, из которого они могут в короткое время могут продолжать работу при обращении. Предвидя вопрос о том, как удалить swapfile.sys: его наличие зависит от того, включен ли обычный файл

подкачки (виртуальная память), т.е. удаляется он тем же способом, что и pagefile.sys, они взаимосвязаны.

Файл hiberfil.sys – это файл гибернации, используемый в Windows для хранения данных и их последующей быстрой загрузки в оперативную память при включении компьютера или ноутбука.

В последних версиях операционной системы Windows 7, 8 и Windows 10 имеются два варианта управления питанием в режиме сна – один – это спящий режим, в котором компьютер или ноутбук работает с низким потреблением электроэнергии (но при этом работает) и вы можете почти мгновенно привести к состоянию, в котором он был, перед тем, как Вы его перевели в режим сна.

Второй режим – гибернация, в котором Windows полностью записывает все содержимое оперативной памяти на жесткий диск и выключает компьютер. При последующем включении не происходит загрузка системы «с нуля», а загружается содержимое файла. Соответственно, чем больше размер оперативной памяти компьютера или ноутбука, тем больше места hiberfil.sys занимает на диске.

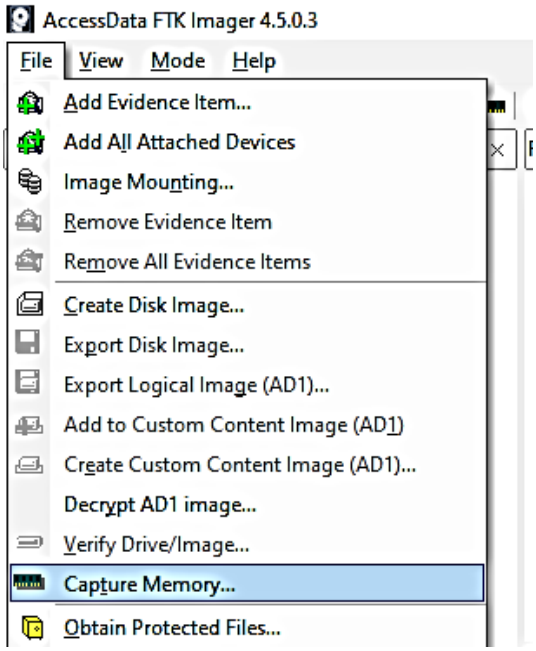
Режим гибернации использует файл hiberfil.sys, чтобы сохранять текущее состояние памяти компьютера или ноутбука, а так как это системный файл, вы не можете удалить его в Windows обычными методами, хотя возможность удаления всё равно существует.

Порядок выполнения работы

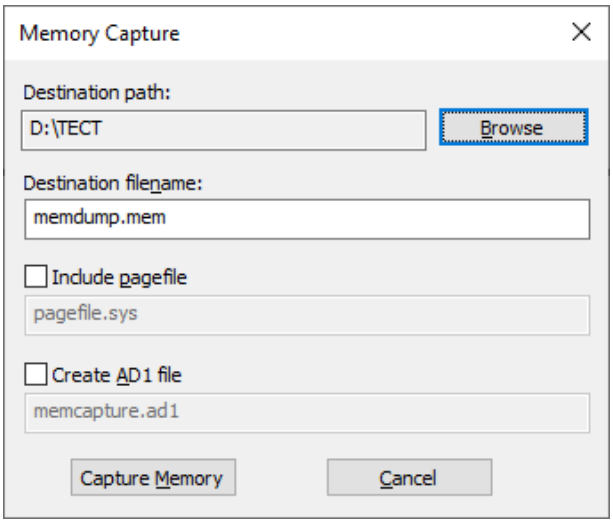
1. Сделать дамп оперативной памяти.

1.1. Для этого запустить ПО AccessData FTK Imager.

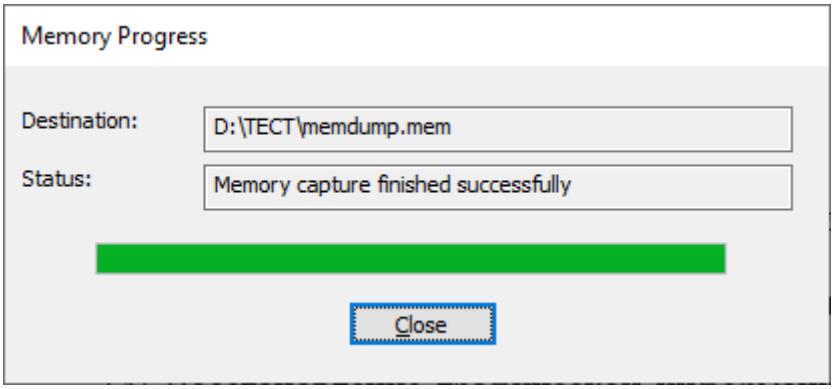
1.2. Выбрать пункт Capture Memory.



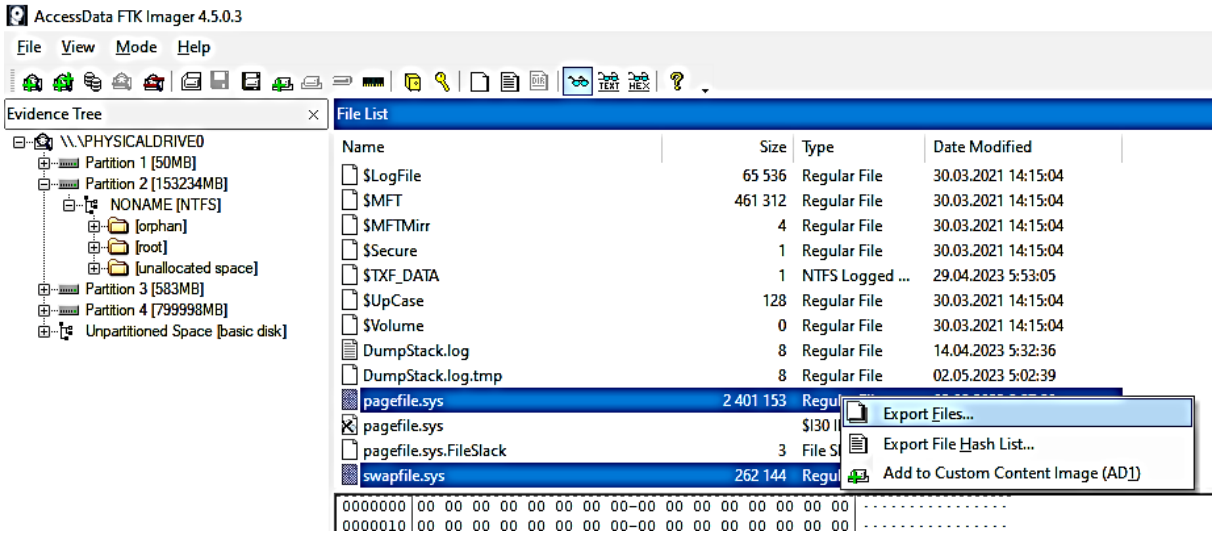
1.3. Выбрать место сохранения файла дампа оперативной памяти свой каталог на диске D.

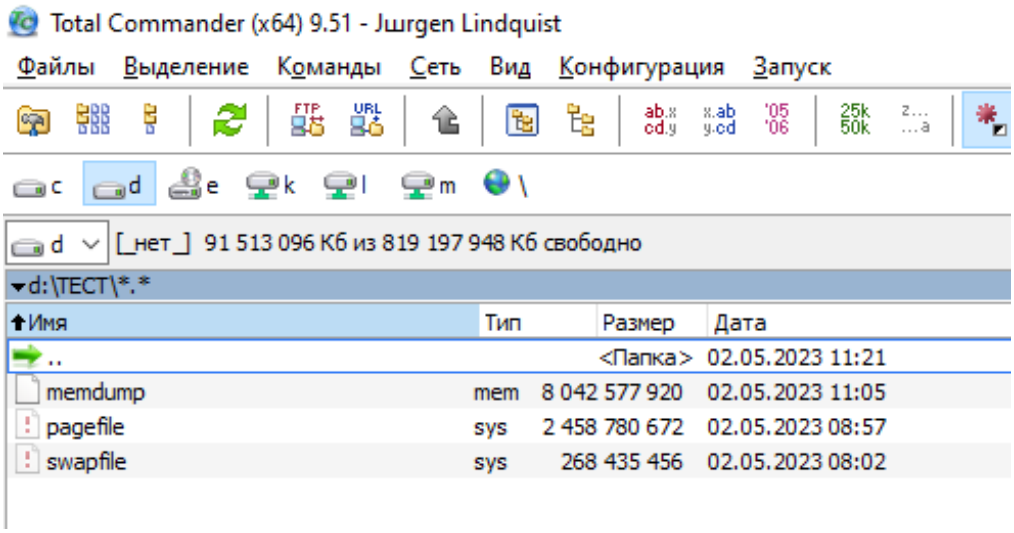


1.4. Дождаться окончания процесса создания файла дампа оперативной памяти.

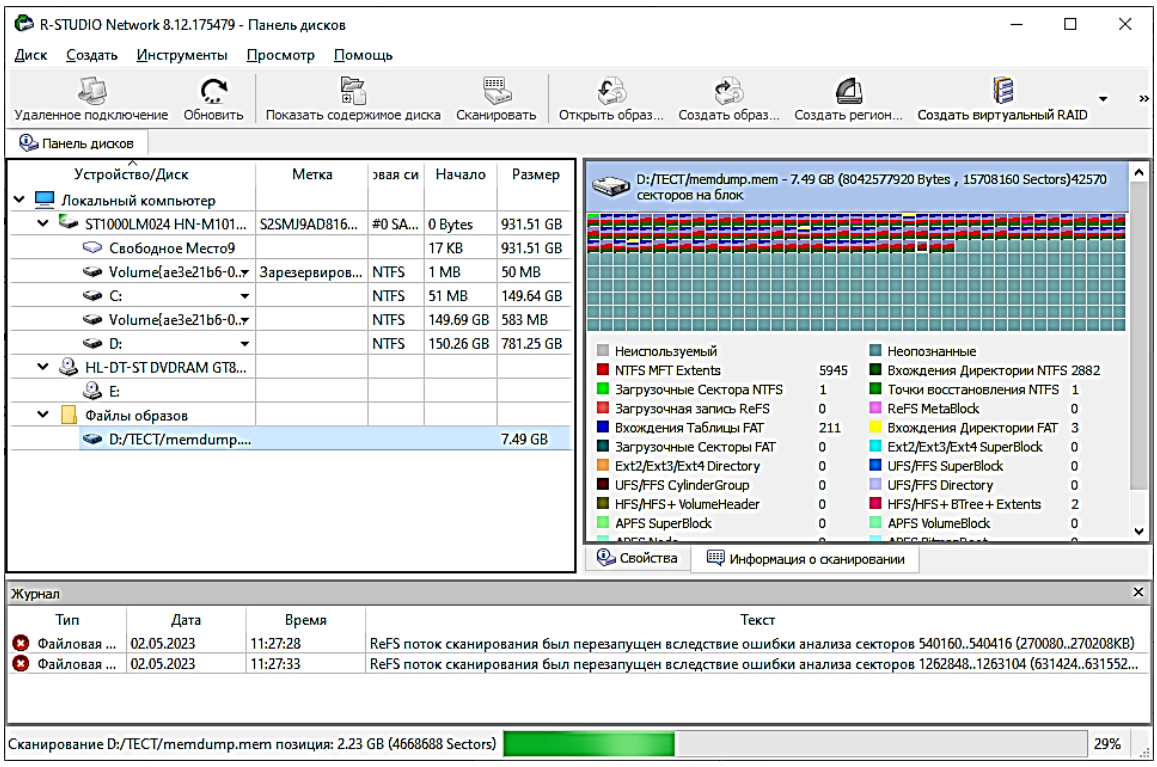


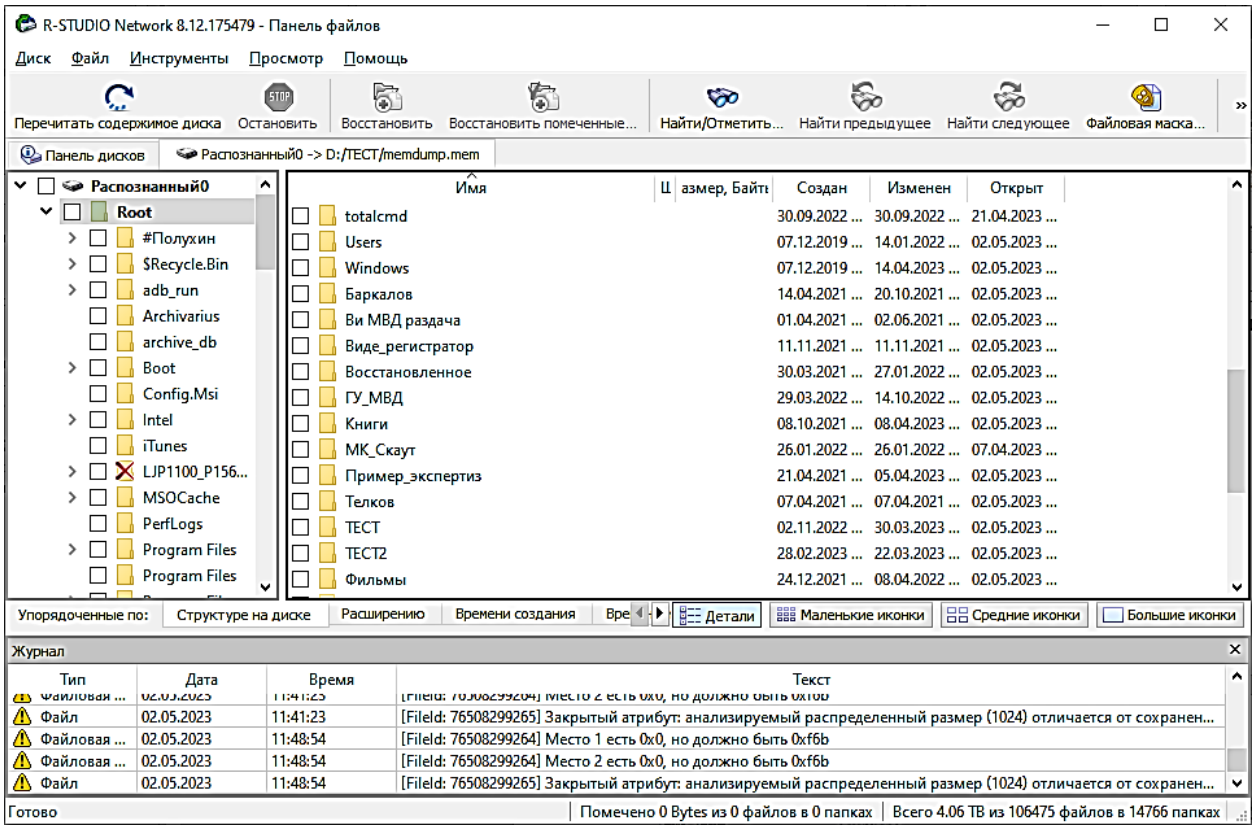
2. Сделать экспорт файлов pagefile.sys и swapfile.sys в свой каталог на диске D с помощью ПО AccessData FTK Imager или R-Studio.

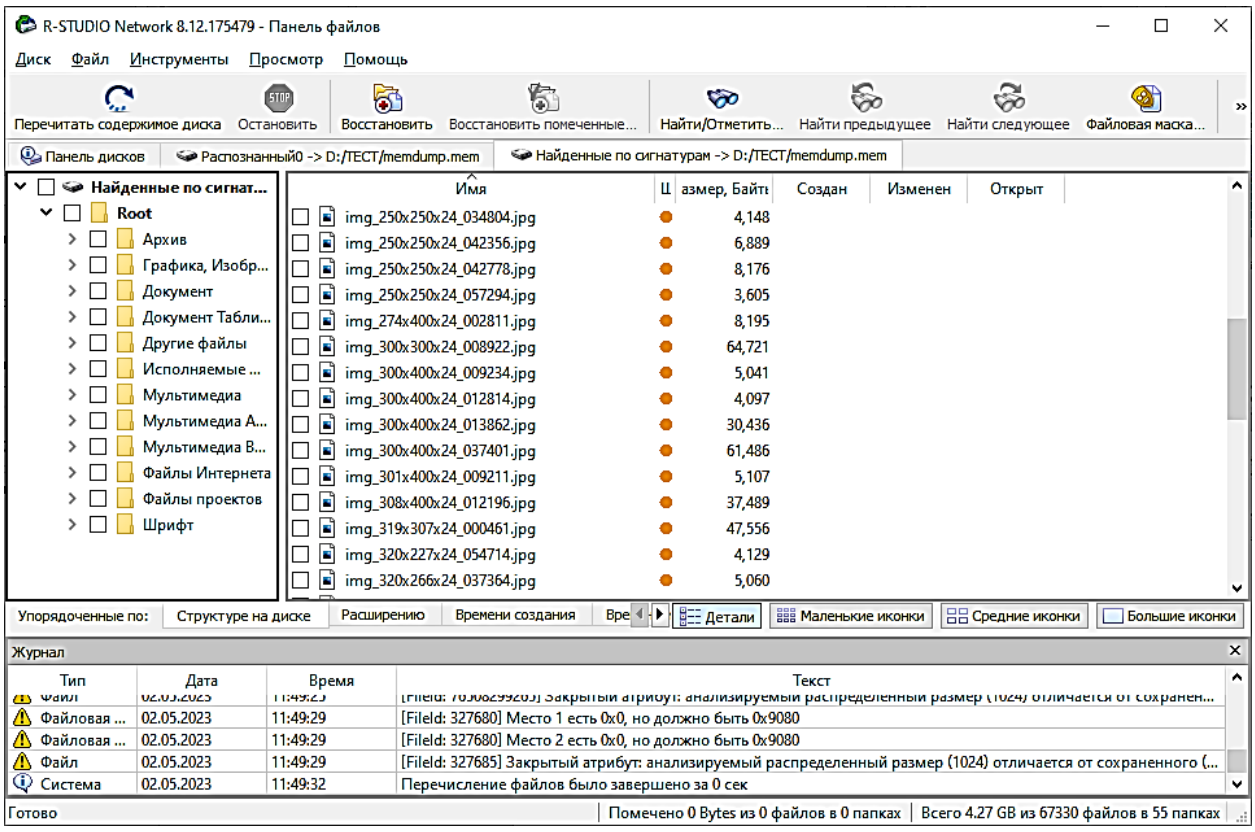




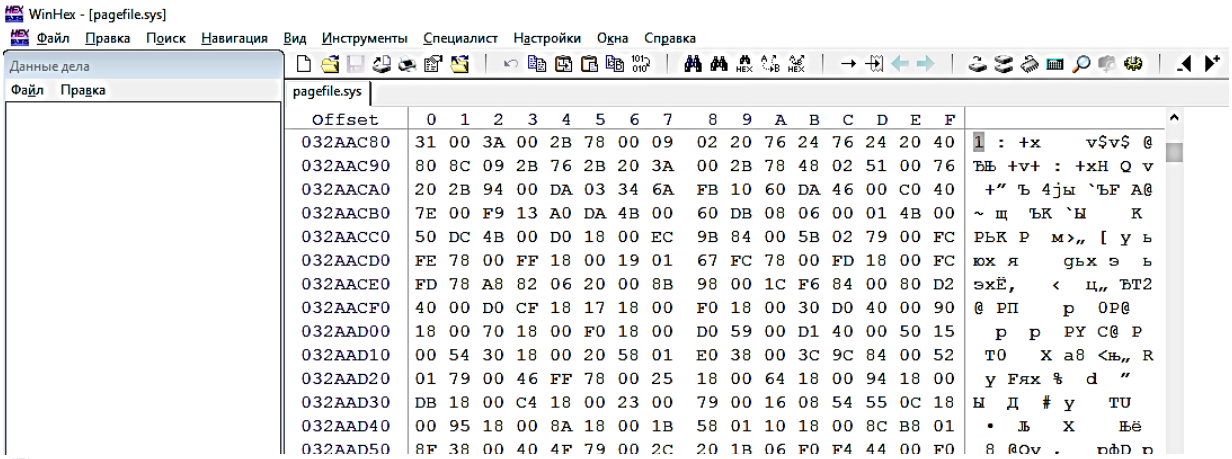
3. С помощью ПО R-Studio открыть файл memdump.mem и восстановить указанную преподавателем информацию.

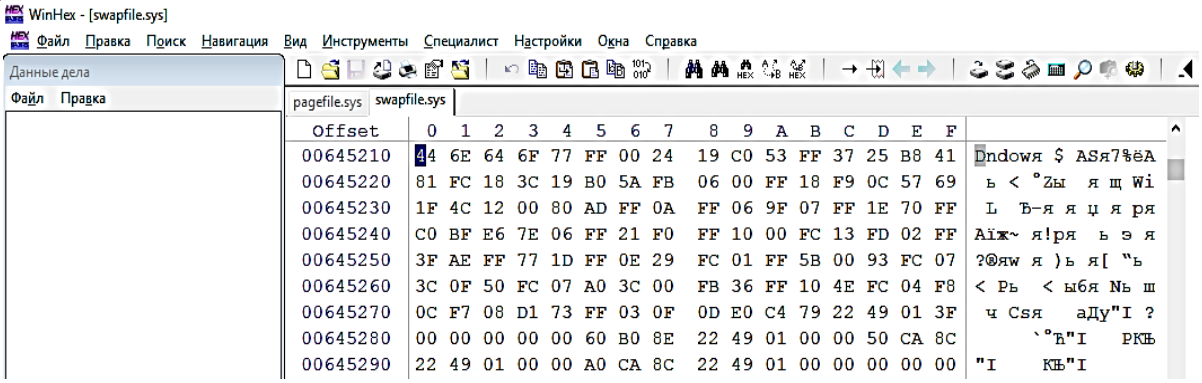


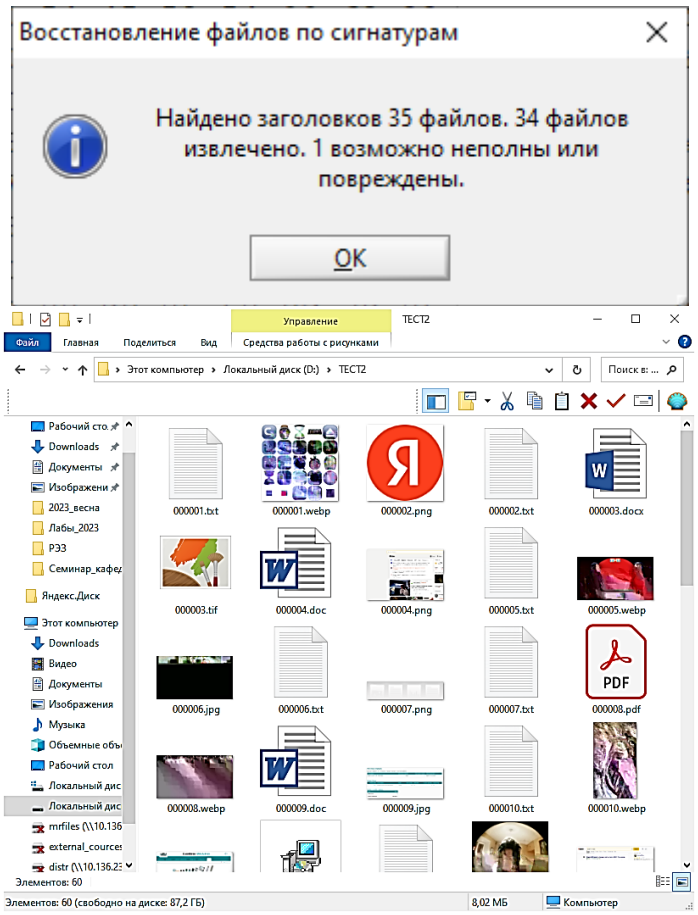




4. С помощью ПО WinHex поочередно открыть файлы pagefile.sys и swapfile.sys и восстановить указанную преподавателем информацию.







5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Где располагаются файлы pagefile.sys и swapfile.sys?
3. Какая информация может храниться в дампе оперативной памияти?
4. С помощью какого ПО можно получить дамп оперативной памяти?
5. Какие типы файлов вы знаете?
6. С помощью какого ПО можно восстановить информацию из дампа оперативной памяти?
7. С помощью какого ПО можно восстановить и проанализировать информацию из файлов подкачки и гибернации?
8. Какое расширение имеют файлы подкачки и гибернации?
9. Для чего операционной системе нужны файлы подкачки и гибернации?

ЛАБОРАТОРНАЯ РАБОТА № 17

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ FAT32 ФЛЕШ-НАКОПИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков восстановления информации из файловой системы FAT32.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы

узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology

File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т.д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

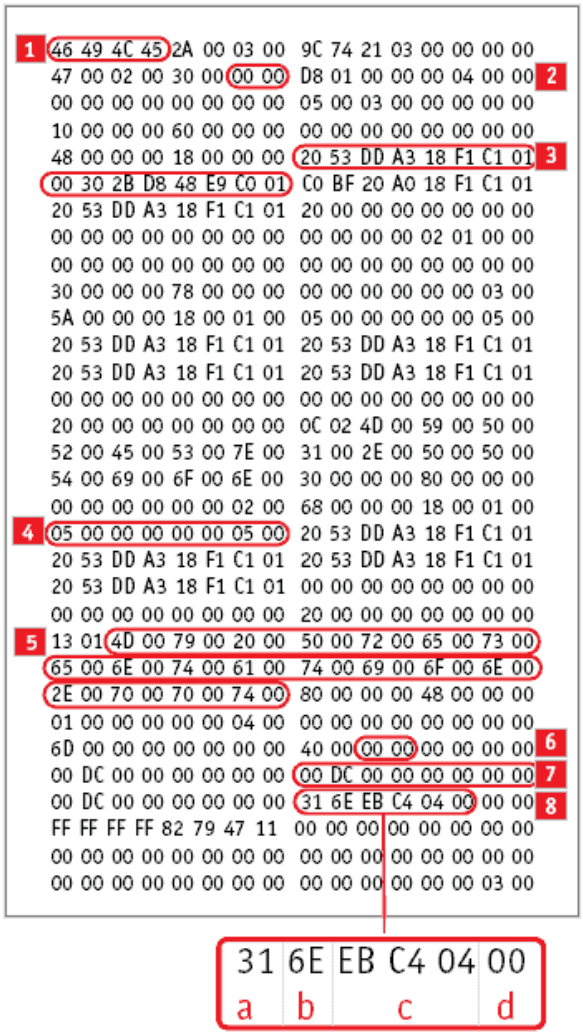
Как работают программы восстановления данных

Каждый только что удаленный файл все еще находится на жестком диске, но Windows его больше не видит. Если программе восстановления данных необходимо восстановить этот файл, она просматривает загрузочный сектор раздела (Partition Boot Sector). В нем содержится вся информация о строении раздела, например размер секторов (как правило, 512 байт) и количество секторов в одном кластере.

В разделе NTFS размером более 2 Гбайт в одном кластере содержится четыре сектора. В нашем примере показан небольшой раздел размером 500 Мбайт, у которого каждому сектору соответствует один кластер.

Наряду с этой информацией программы восстановления данных сканируют главную таблицу файлов(Master File Table, MFT), которая тоже находится в Partition Boot Sector. Она представляет собой список всех файлов, находящихся в разделе, в ней содержатся все файловые атрибуты и информация о том, в каких секторах винчестера находятся сами файлы. Те из них, что по размерам менее 1500 байт, записываются прямо в MFT. Для файлов большего объема в MFT есть ссылки на адреса секторов, в которых лежат данные.

В начале MFT находятся другие записи, например так называемая битовая карта распределения кластеров (Cluster Bitmap), показывающая все используемые кластеры, а также файл плохих кластеров(Bad Cluster File), регистрирующий все кластеры с ошибками. Только с 17-й записи начинается собственно описание файлов. Обычно таблица MFT в Windows не видна. Но есть дисковые редакторы, например WinHex, которые показывают содержание MFT в шестнадцатеричных кодах.



Выше на рисунке вы видите MFT-запись удаленного файла в HEX-коде. Для программы восстановления данных достаточно этой информации, чтобы восстановить файл.

Значения, которые программа восстановления файлов находит в Master File Table:

1. Эти четыре байта (File Identifier) обозначают начало нового файла. Байты до следующего FileIdentifier содержат всю информацию о файле.

2. Эти два байта зарезервированы для флагов, которые дают справку о состоянии файла. Если их значение равно 0, как в нашем случае, это значит, что файл удален.

3. Из этих 16 байт программа восстановления данных узнает, когда файл был создан и в последний раз подвергался изменениям.

4. Эта ссылка на каталог, в котором находится файл (Parent Directory Record Number). С ее помощью программа-спасатель может включить файл в структуру каталогов.

5. Здесь появляется имя файла, в нашем случае My Presentation.ppt.

6. Если эти два байта имеют значение 0, то файл не сжат.

7. Эти восемь байт сообщают размер файла, в нашем случае 56 320 байт.

8. Важнейшая часть записи MFT, называющаяся Data runs, показывает, где фактически находятся данные.

Здесь указано где находятся данные.

a. Первый байт сообщает, сколько байт необходимо для адреса первого кластера (3 байта) и отображения длины файла во всех кластерах (1 байт).

b. Второй байт содержит длину файла, в нашем примере — 110 кластеров.

c. Следующие три байта означают, что файл начинается с кластера 312 555.

d. Последний байт имеет значение 0. Это означает, что файл не фрагмен--тирован. Следовательно, нет никаких дополнительных записей Data runs.

Как программа восстанавливает данные.

Теперь у программы восстановления данных есть вся информация, необходимая для успешного восстановления удаленного файла. Она обращается к кластеру 312 555, прочитывает данные в следующих 110 кластерах и сохраняет их под именем My Presentation.ppt

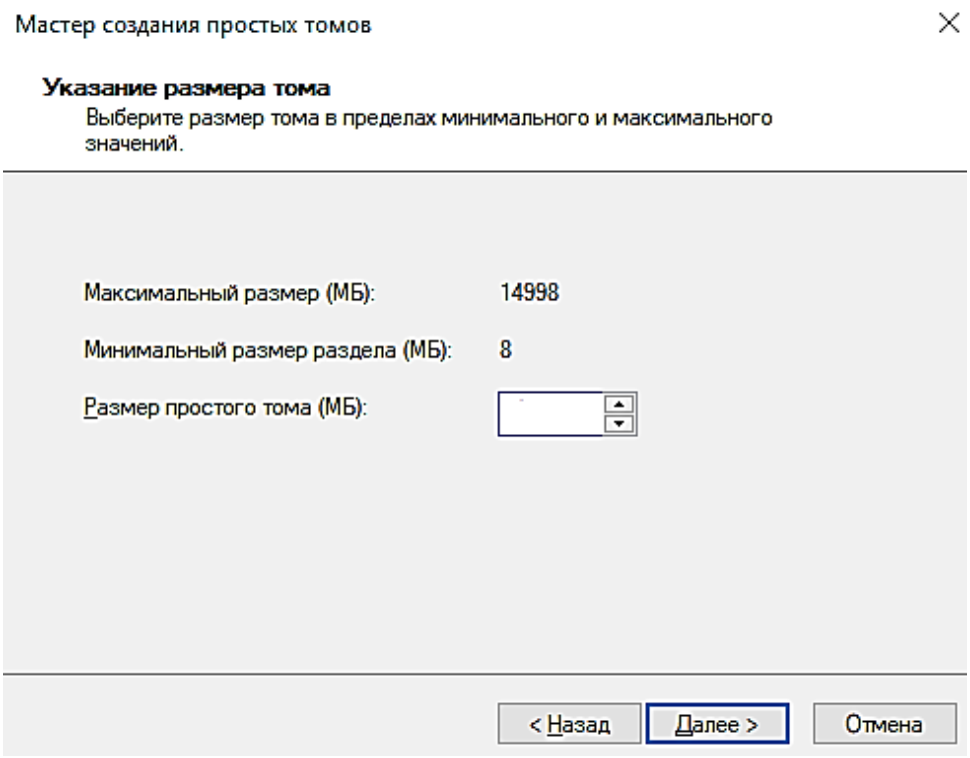
Порядок выполнения работы

1. Подготовить флеш-накопитель с файловой системой FAT32.

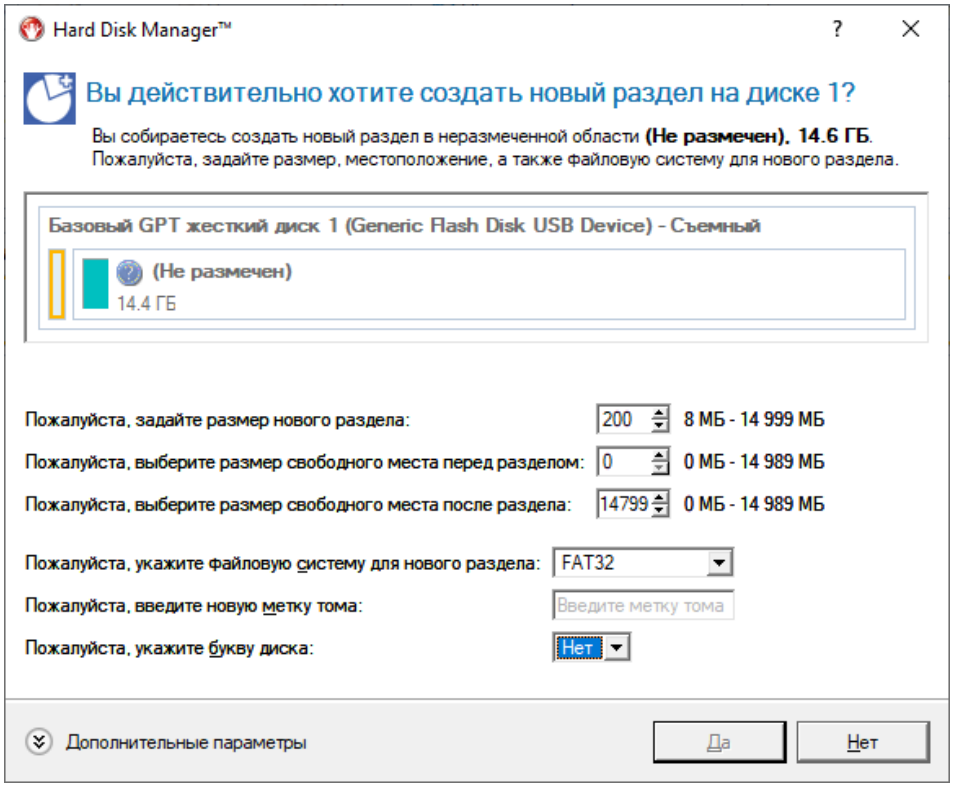
1.1. Получить у преподавателя накопитель информации.

1.2. Создать на нем раздел с файловой системой FAT32.

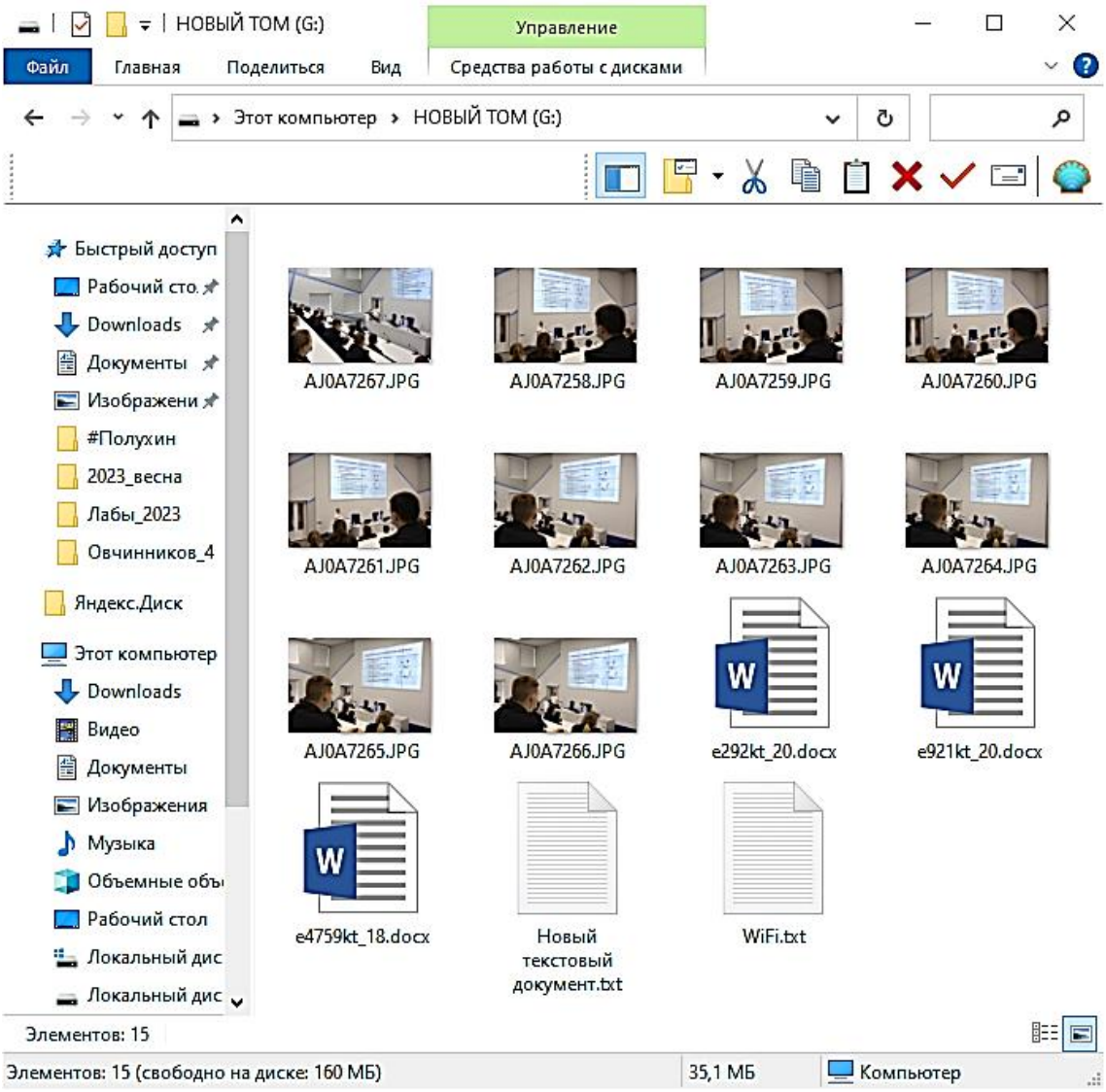
1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками. Создать том размером 200 МБ.



1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager.



1.3. Скопировать в созданный раздел несколько произвольных графических и текстовых файлов. Сделать скриншот.



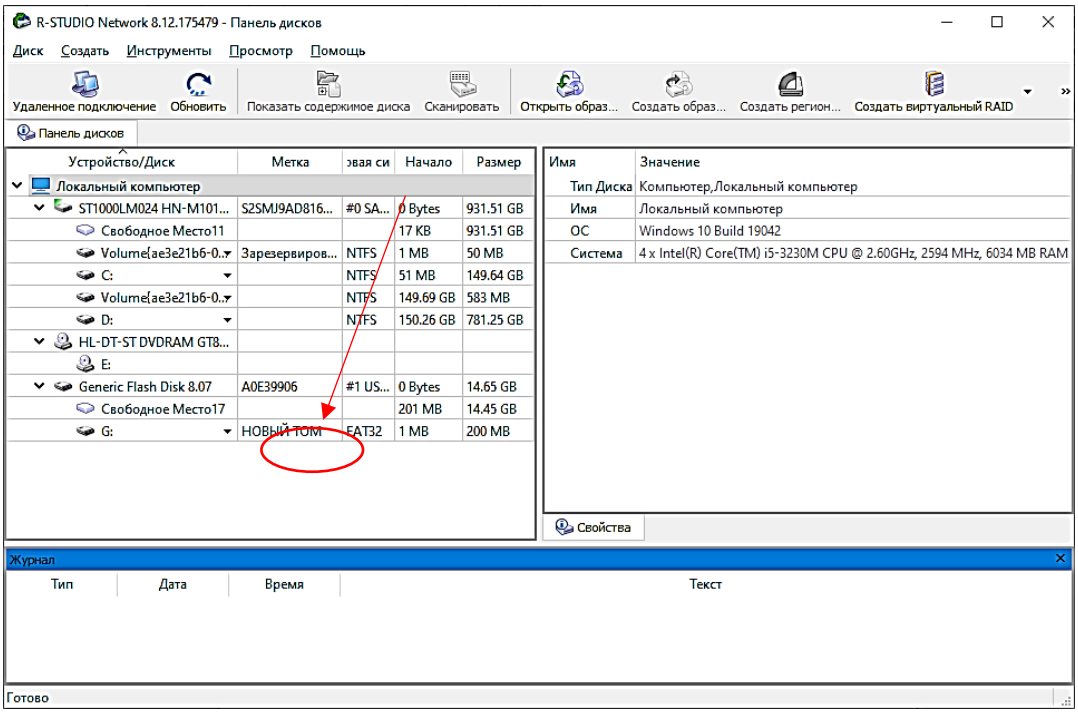
1.4. Удалить скопированные файлы.

2. Восстановить удаленные файлы с флеш-накопителя.

2.1. Запустить программу R-Studio.

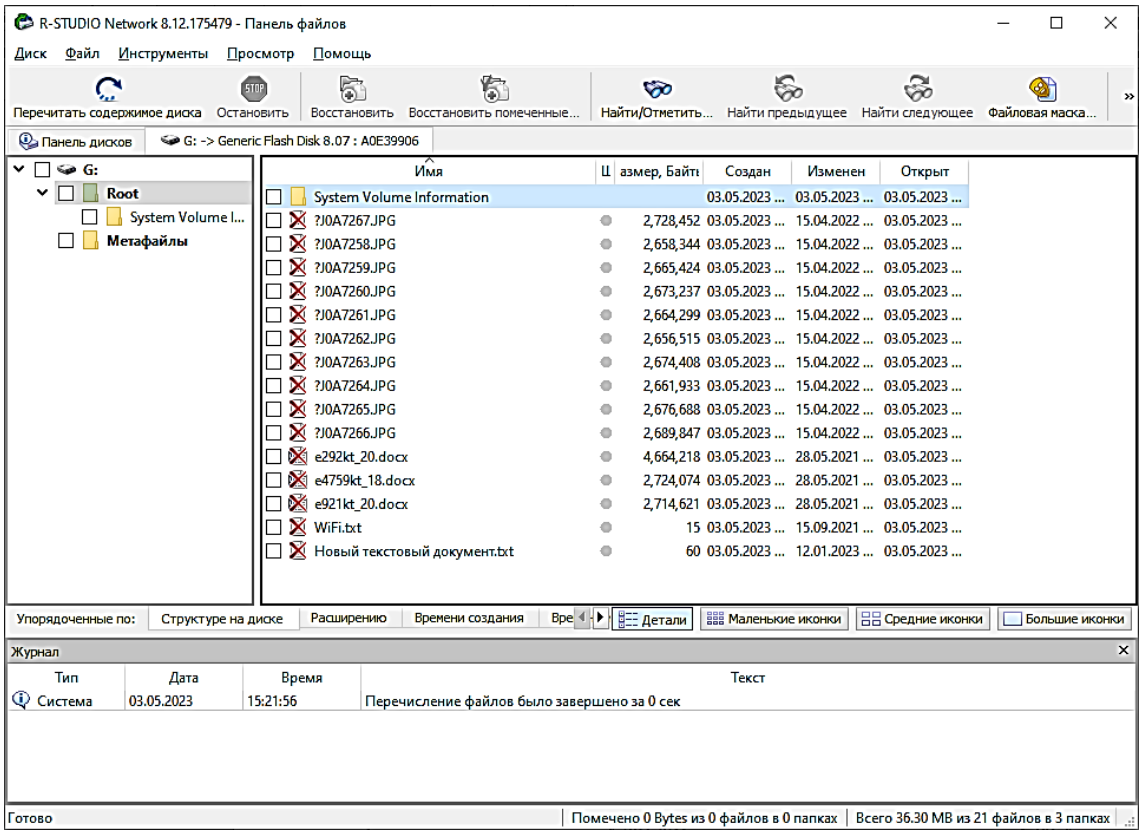
2.2. Обнаружить в программе исследуемый флеш-накопитель.

2.3. Проверить файловую систему FAT32.

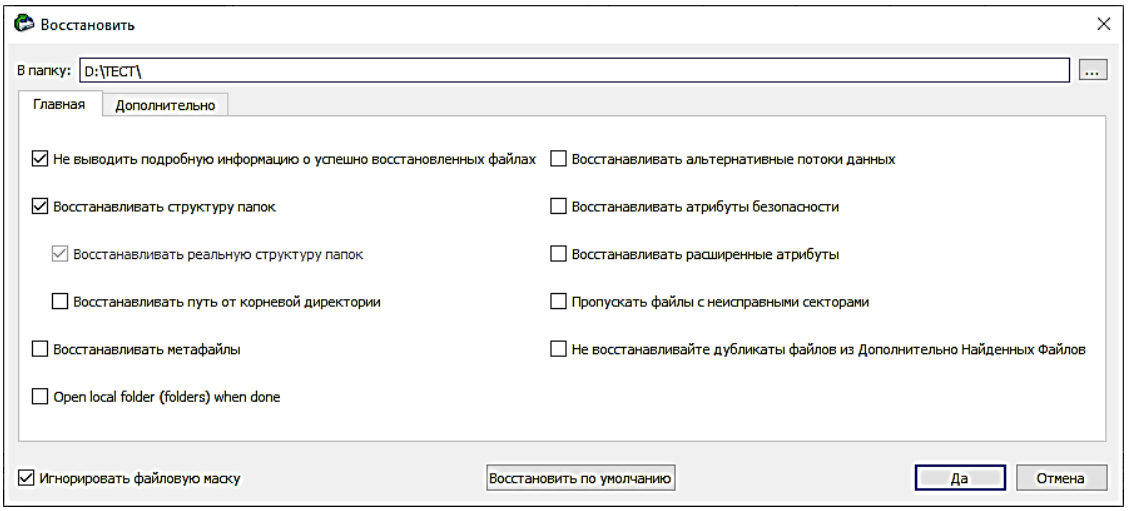


2.4. Запустить быстрое сканирование. Для этого дважды кликнуть ЛКМ на выбранный флеш-накопитель в программе R-Studio.

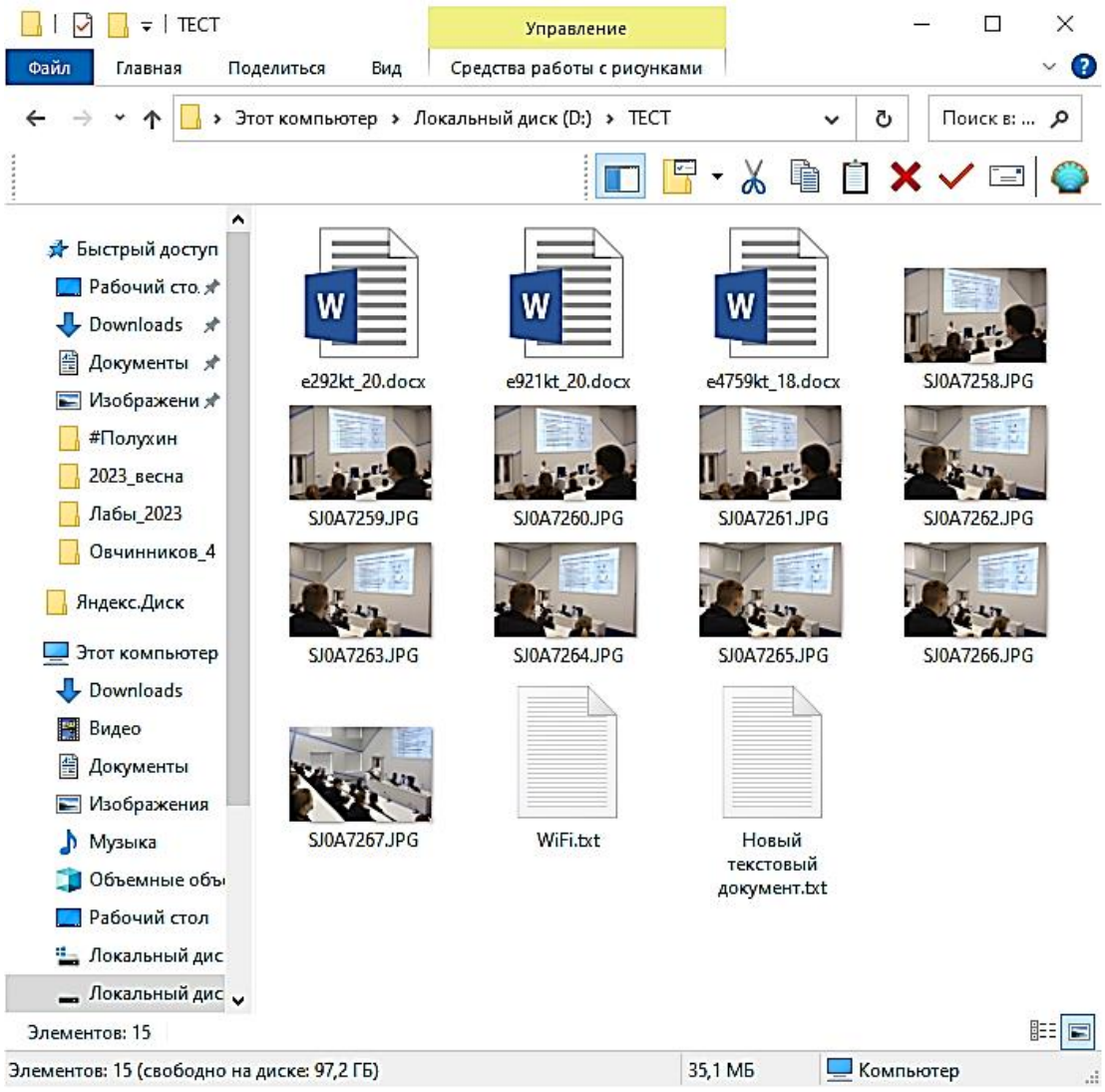
2.5. Обнаружить удаленные файлы. Они будут помечены красным крестиком.



2.6. Отметить галочкой удаленные файлы и восстановить их в каталог на диске D.



3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы FAT32?
3. Какого максимального размера файлы можно помещать в файловую систему FAT32?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм восстановления файлов с помощью программы R-Studio.
10. Какие типы файлов вы знаете?
11. Как обнаружить удаленные файлы с помощью программы R-Studio?

ЛАБОРАТОРНАЯ РАБОТА № 18

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ NTFS ФЛЕШ-НАКОПИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков восстановления информации из файловой системы NTFS.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное программное обеспечение.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

Восстановление удаленной информации

Операционные системы становятся все более совершенными, а соответственно, и сложными. Усложняются и структуры разделов, на которые разбиты диски. Это приводит и к усложнению способов восстановления информации. Мы рассмотрим разные программы, которые могут пригодиться, чтобы восстановить случайно удаленные файлы.

В большинстве случаев файлы, удаленные с жесткого диска, находятся на нем, пока поверх них не будет записана другая информация, поэтому если вы спохватились, вспомнив, что удалили что-нибудь важное, во-первых, ничего не записывайте на диск. Чем дольше вы работаете с диском после удаления файла, тем меньше шансов что-либо восстановить. Файлы, которые удаляются не в корзину (с помощью Shift+Delete), не вытираются с диска. Система просто вытирает первую букву в имени файла и игнорирует его пока на его место не будет что-то записано.

Утилиты для восстановления информации в таких самых простых случаях есть почти в любом наборе системных утилит. Следует обратить внимание еще и на то, поддерживает ли выбранная вами программа файловую систему, с которой работает ваша операционная система. Чтобы

узнать, какая файловая система используется на вашем жестком диске, зайдите в «Мой компьютер» и откройте правой кнопкой мыши контекстное меню нужного диска, выбрав «Свойства», посмотрите на параметр «Файловая система».

При форматировании жесткого диска создается специальная таблица расположения файлов (FileAllocation Table – FAT в FAT32 или Master File Table – MFT в NTFS). В случае ее повреждения или полного уничтожения система никак не сможет найти информацию на диске.

Программы восстановления могут воссоздать таблицы FAT или MFT из их архивных копий. Если же копии тоже повреждены, хорошая утилита все же может попытаться восстановить потерянные данные.

Если в вашем распоряжении только те средства, которые входят в Windows, то стертый файл, удаленный из мусорной корзины Recycle Bin, кажется пропавшим навсегда. На самом деле это не так.

С помощью специальных аппаратных и программных средств можно восстановить практически любой файл, даже если поверх него записаны другие данные, диск переформатирован, загрузочный сектор засорен, а контроллер диска перестал функционировать. Это очень удобно, когда вы хотите восстановить чрезвычайно важный файл, но никуда не годится, если нежелательно, чтобы ваши личные данные прочитали посторонние. Правильное решение зависит от того, сколько времени и денег вы готовы потратить.

Чтобы понять, как восстанавливаются удаленные данные, надо сначала выяснить, как они сохраняются. Накопитель на жестком магнитном диске (НЖМД) состоит из пакета дисковых пластин. Сохраняемые на пластинах данные располагаются по концентрическим окружностям, называемым дорожками. Для доступа к различным частям жесткого диска головки чтения-записи перемещаются по поверхности пластин. Так как к данным возможен непосредственный доступ повсюду на жестком диске, то файлы или их фрагменты могут храниться на его поверхности в любом месте. Помещать их в последовательном порядке совсем не обязательно.

Данные на жестких дисках хранятся группами (кластерами). Размеры кластеров варьируются в зависимости от операционной системы и размеров логического тома. Если размер кластера жесткого диска составляет 4 Кбайт, то даже 1-Кбайт файл будет занимать 4 Кбайт. Большие файлы могут занимать сотни или тысячи кластеров, разбросанных по всему диску. Все эти отдельные порции данных отслеживаются и управляются входящей в состав операционной системы файловой системой.

В настоящее время существует три вида файловых систем, используемых ОС Microsoft Windows. Первая – таблица размещения файлов FAT (File Allocation Table) – была введена в системе DOS. Вместе с Windows 95 появилась система FAT32, а выпуск ОС Windows NT 4.0 сопровождался появлением файловой системы новой технологии NTFS (New Technology

File System). Все три системы построены по одному и тому же принципу. Имеется каталог, где перечислены файлы на диске и содержится указатель начального кластера, который фиксирует начало файла. Запись в FAT о начальном кластере содержит указатель следующего кластера и т.д., пока не будет достигнут маркер конца файла.

Когда вы с помощью обычной операции Windows удаляете файл, он на самом деле не стирается. Если вы удаляете его в системе каталогов Windows Explorer, то он оказывается в корзине. Но даже если вы очищаете корзину или действуете в обход ее, файл попросту игнорируется. Первая буква имени файла изменяется на специальный символ, а кластеры, где содержатся эти данные, помечаются как свободные, но данные все еще там. Когда вы в следующий раз сохраняете какой-нибудь файл, эти кластеры могут использоваться для хранения новых данных, которые записываются поверх старых. Однако до этого момента прежние данные остаются совершенно невредимыми. Вы можете их восстановить с помощью утилиты, которая действует в обход ОС и непосредственно считывает записанное на жестком диске.

Если вы хотите восстановить случайно удаленный чрезвычайно важный файл, нужно постараться ничего не записать поверх него. Немедленно прекратите работу на своем компьютере и ничего не записывайте на диск. Не надо даже инсталлировать программу восстановления, так как все записываемое на жесткий диск может попасть в кластеры файла, который вы хотите восстановить. Если программа восстановления еще не инсталлирована, запустите ее с гибкого диска.

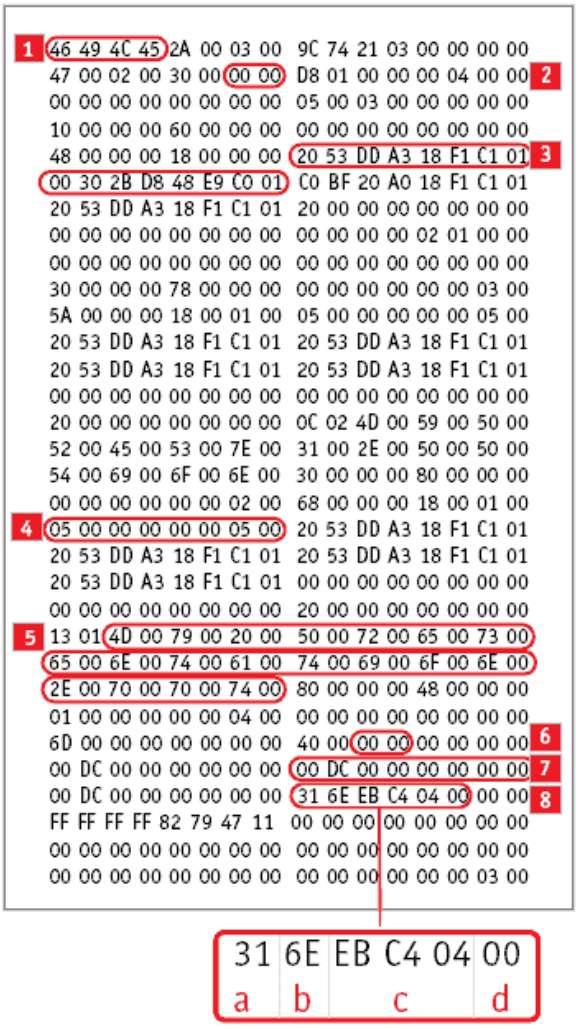
Как работают программы восстановления данных

Каждый только что удаленный файл все еще находится на жестком диске, но Windows его больше не видит. Если программе восстановления данных необходимо восстановить этот файл, она просматривает загрузочный сектор раздела (Partition Boot Sector). В нем содержится вся информация о строении раздела, например размер секторов (как правило, 512 байт) и количество секторов в одном кластере.

В разделе NTFS размером более 2 Гбайт в одном кластере содержится четыре сектора. В нашем примере показан небольшой раздел размером 500 Мбайт, у которого каждому сектору соответствует один кластер.

Наряду с этой информацией программы восстановления данных сканируют главную таблицу файлов (Master File Table, MFT), которая тоже находится в Partition Boot Sector. Она представляет собой список всех файлов, находящихся в разделе, в ней содержатся все файловые атрибуты и информация о том, в каких секторах винчестера находятся сами файлы. Те из них, что по размерам менее 1500 байт, записываются прямо в MFT. Для файлов большего объема в MFT есть ссылки на адреса секторов, в которых лежат данные.

В начале MFT находятся другие записи, например так называемая битовая карта распределения кластеров (Cluster Bitmap), показывающая все используемые кластеры, а также файл плохих кластеров(Bad Cluster File), регистрирующий все кластеры с ошибками. Только с 17-й записи начинается собственно описание файлов. Обычно таблица MFT в Windows не видна. Но есть дисковые редакторы, например WinHex, которые показывают содержание MFT в шестнадцатеричных кодах.



Выше на рисунке вы видите MFT-запись удаленного файла в HEX-коде. Для программы восстановления данных достаточно этой информации, чтобы восстановить файл.

Значения, которые программа восстановления файлов находит в Master File Table:

1. Эти четыре байта (File Identifier) обозначают начало нового файла. Байты до следующего FileIdentifier содержат всю информацию о файле.

2. Эти два байта зарезервированы для флагов, которые дают справку о состоянии файла. Если их значение равно 0, как в нашем случае, это значит, что файл удален.

3. Из этих 16 байт программа восстановления данных узнает, когда файл был создан и в последний раз подвергался изменениям.

4. Эта ссылка на каталог, в котором находится файл (Parent Directory Record Number). С ее помощью программа-спасатель может включить файл в структуру каталогов.

5. Здесь появляется имя файла, в нашем случае My Presentation.ppt.

6. Если эти два байта имеют значение 0, то файл не сжат.

7. Эти восемь байт сообщают размер файла, в нашем случае 56 320 байт.

8. Важнейшая часть записи MFT, называющаяся Data runs, показывает, где фактически находятся данные.

Здесь указано где находятся данные.

a. Первый байт сообщает, сколько байт необходимо для адреса первого кластера (3 байта) и отображения длины файла во всех кластерах (1 байт).

b. Второй байт содержит длину файла, в нашем примере — 110 кластеров.

c. Следующие три байта означают, что файл начинается с кластера 312 555.

d. Последний байт имеет значение 0. Это означает, что файл не фрагментирован. Следовательно, нет никаких дополнительных записей Data runs.

Как программа восстанавливает данные.

Теперь у программы восстановления данных есть вся информация, необходимая для успешного восстановления удаленного файла. Она обращается к кластеру 312 555, прочитывает данные в следующих 110 кластерах и сохраняет их под именем My Presentation.ppt

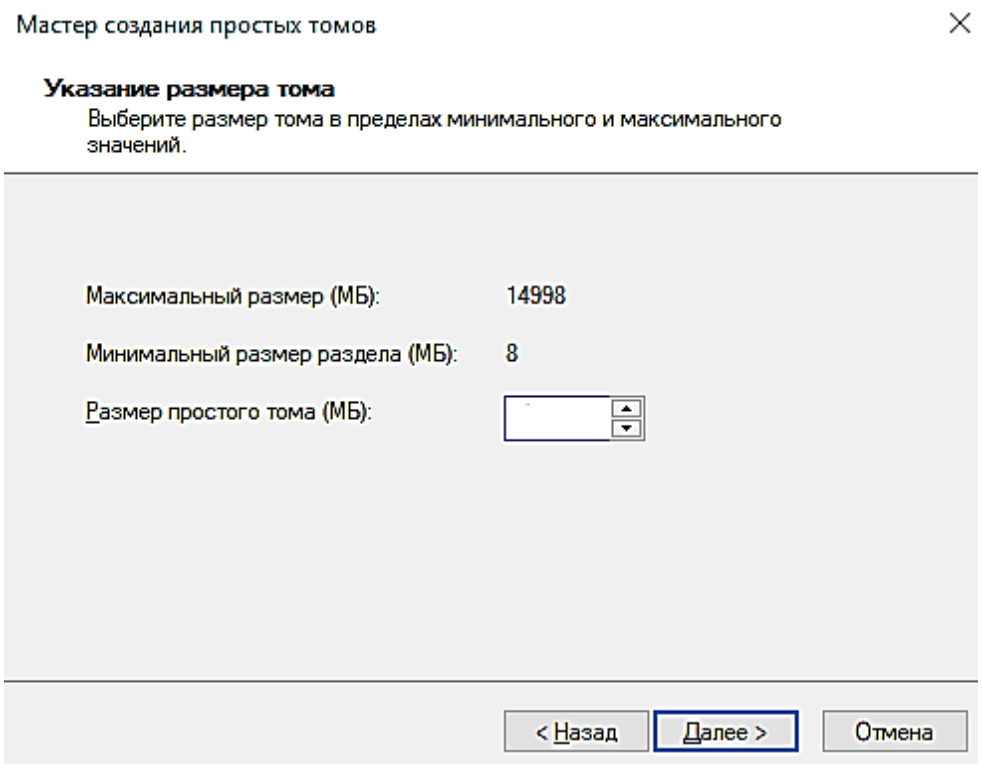
Порядок выполнения работы

1. Подготовить флеш-накопитель с файловой системой NTFS.

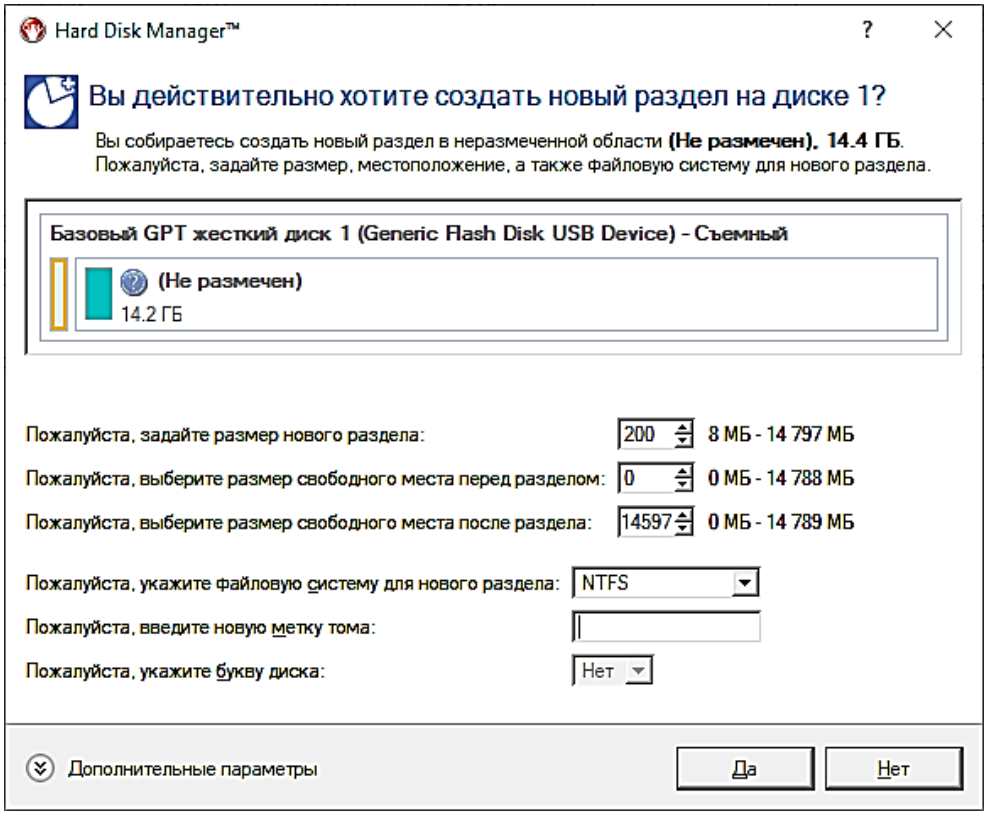
1.1. Получить у преподавателя накопитель информации.

1.2. Создать на нем раздел с файловой системой NTFS.

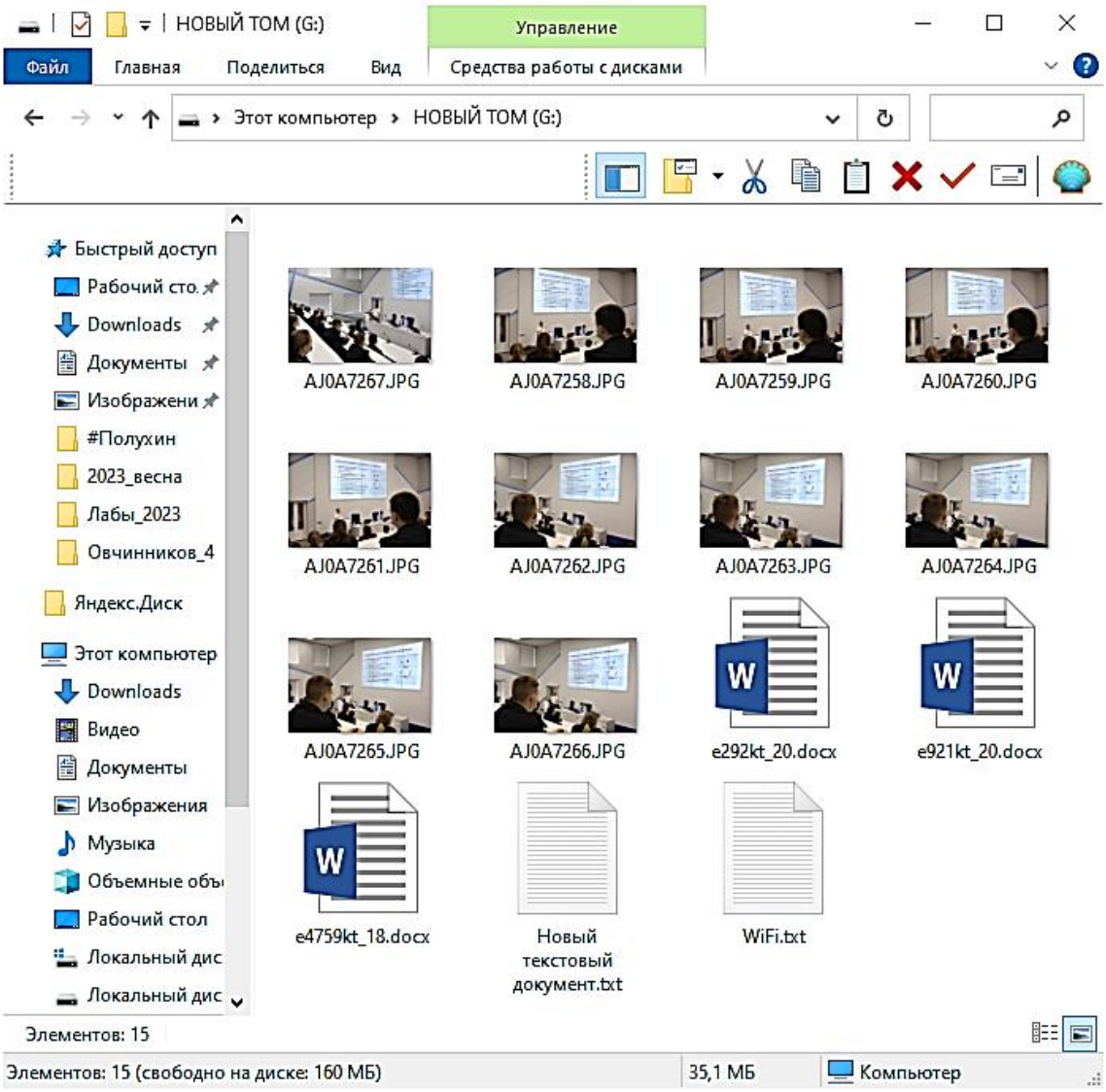
1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками. Создать том размером 200 МБ.



1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager.



1.3. Скопировать в созданный раздел несколько произвольных графических и текстовых файлов. Сделать скриншот.



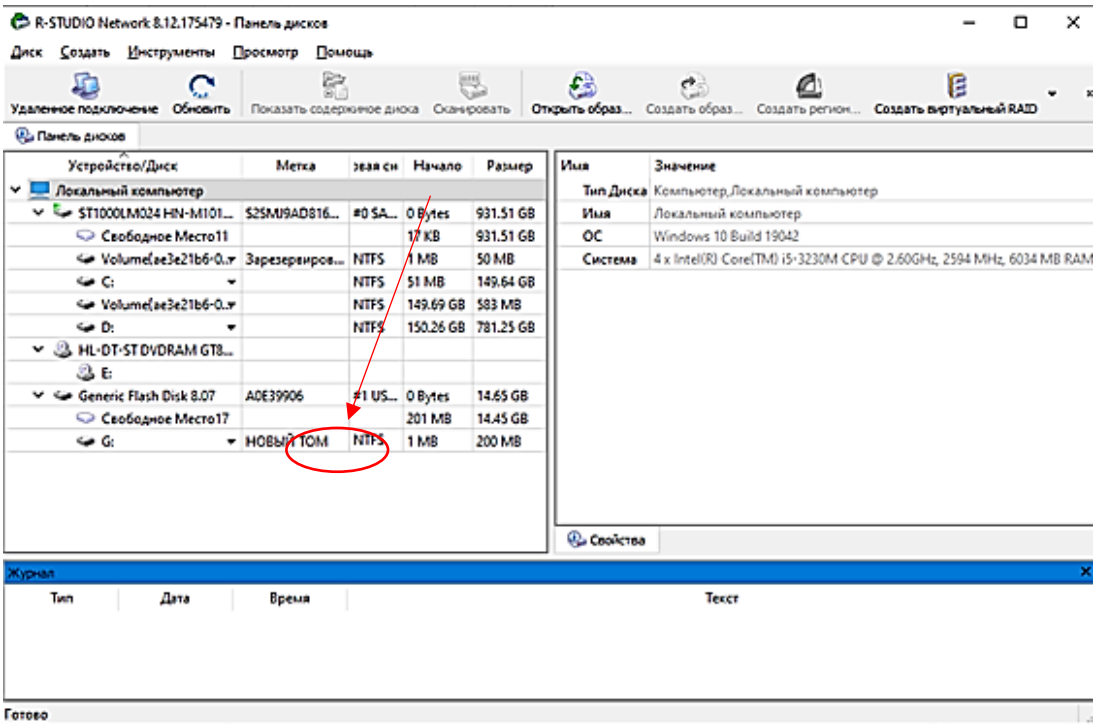
1.4. Удалить скопированные файлы.

2. Восстановить удаленные файлы с флеш-накопителя.

2.1. Запустить программу R-Studio.

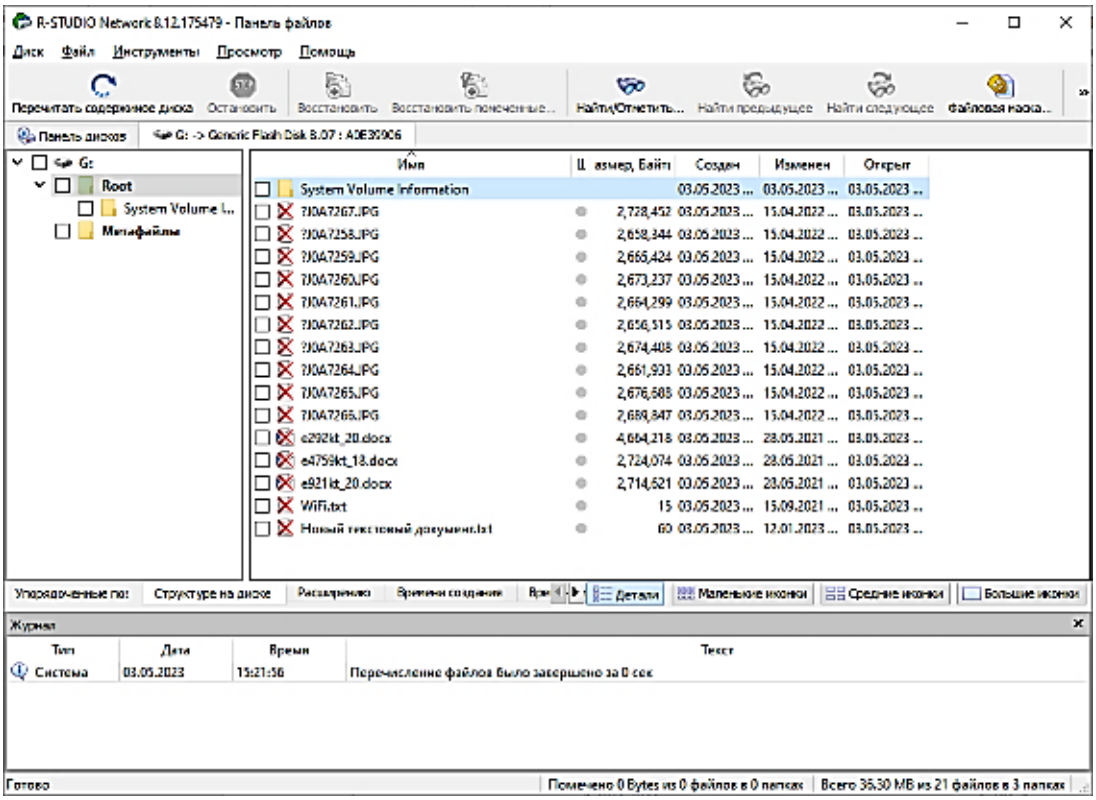
2.2. Обнаружить в программе исследуемый флеш-накопитель.

2.3. Проверить файловую систему NTFS.

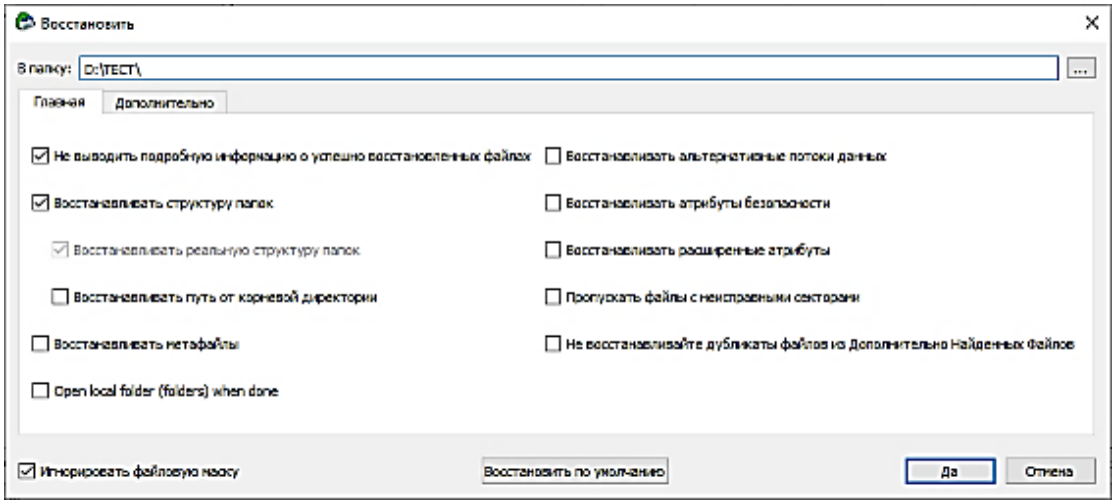


2.4. Запустить быстрое сканирование. Для этого дважды кликнуть ЛКМ на выбранный флеш-накопитель в программе R-Studio.

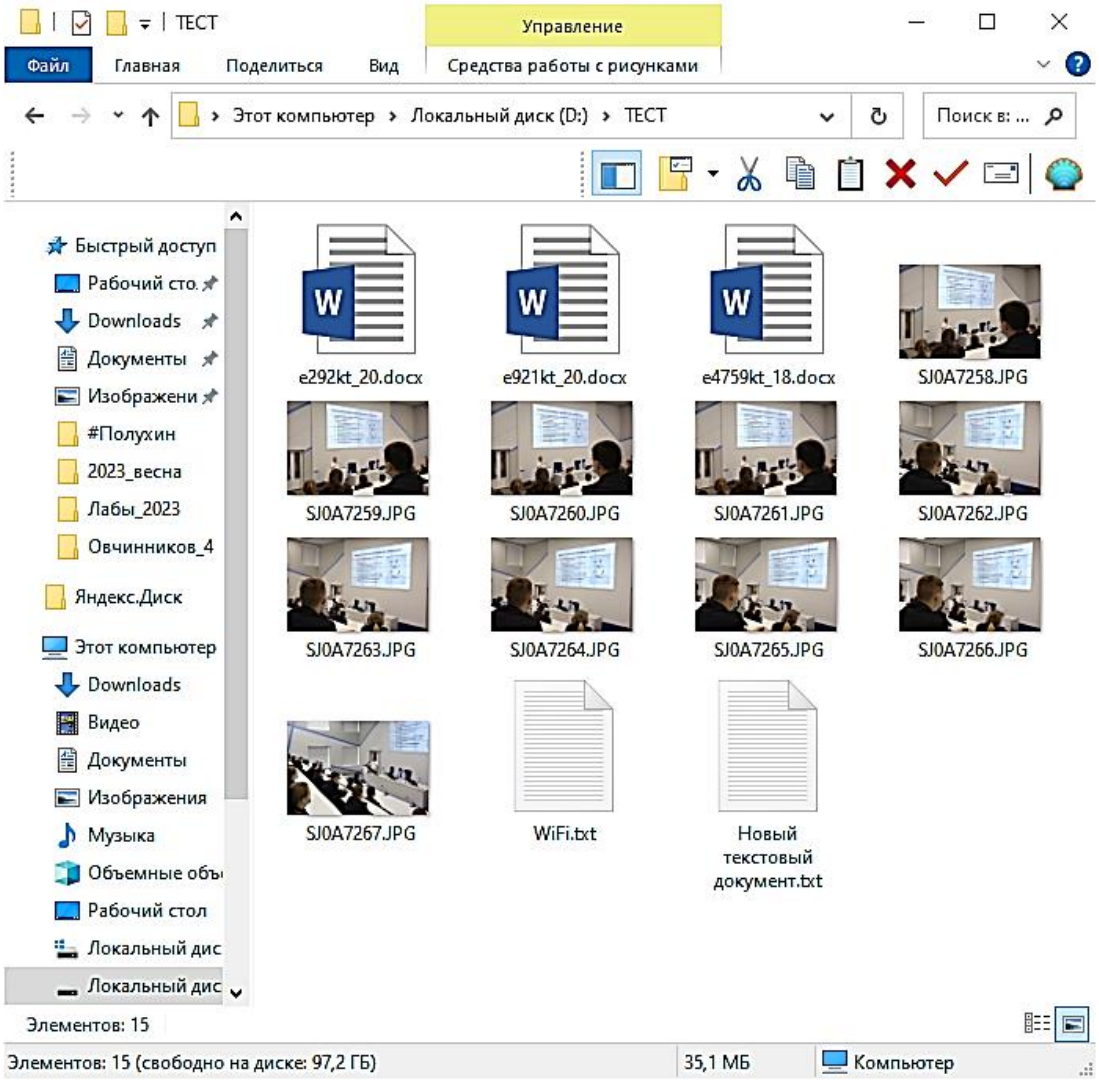
2.5. Обнаружить удаленные файлы. Они будут помечены красным крестиком.



2.6. Отметить галочкой удаленные файлы и восстановить их в каталог на диске D.



3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы NTFS?
3. Какого максимального размера файлы можно помещать в файловую систему NTFS?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм восстановления файлов с помощью программы R-Studio.
10. Какие типы файлов вы знаете?
11. Как обнаружить удаленные файлы с помощью программы R-Studio?

ЛАБОРАТОРНАЯ РАБОТА № 19

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ FAT32 С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПАК PC-3000

Цель работы: Получение практических навыков работы с ПАК PC-3000.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное оборудование.

Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

PC-3000 Portable – это портативный программно-аппаратный комплекс, предназначенный для диагностики, ремонта и восстановления пользовательских данных с накопителей HDD/SSD1, имеющих физические неисправности носителей и логические повреждения файловых систем. К физическим неисправностям HDD относятся: повреждения платы электроники, магнитных дисков, головок чтения-записи, предусилителя, микропрограммы, служебной информации. К физическим неисправностям SDD относятся: повреждения платы электроники, контроллера, деградация ячеек массива NAND-Flash памяти, повреждение микропрограммы, служебной информации и др. К логическим неисправностям относятся: повреждения дисковых структур, структур файловых систем и комбинации этих проблем. Дополнительно, PC-3000 Portable позволяет создавать имидж-копии данных с накопителей HDD, SSD, USB-Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны.

Диагностируемые HDD/SSD/Flash накопители, подлежащие восстановлению данных, подключаются непосредственно к контроллеру PC 3000 Portable – к ег.о портам SOURCE – USB и Port0. К портам TARGET – Port1

и Port2 подключаются HDD/SSD накопители для создания имидж-копии данных. В некоторых режимах работы порты Port1 и Port2 также могут использоваться для подключения диагностируемых/восстанавливаемых накопителей, увеличивая тем самым общее число одновременно восстанавливаемых HDD/SSD до трех.

Порты SOURCE – USB и Port 0 допускают блокировку от записи, для ее включения необходимо воспользоваться переключаетелем Write Protection. При включенной блокировке должен гореть жетлый светодиод.

Контроллер PC-3000 Portable подключается к внешнему источнику питания -19В, и в случае работы через управляющий компьютер подключается к нему через интерфейс USB 3.0.

В существующей реализации контроллер PC-3000 Portable допускает подключение накопителей HDD/SSD с интерфейсом SATA-III (совместим с SATA-I/II, SSD M.2 NVMe PCIe) и накопителей с USB интерфесом, соответствующих классификации Mass Storage Device – внешние HDD/ SSD USB 2.0/3.0 и USB-Flash накопители. Подключение накопителей с интерфейсом PATA (IDE) возможно через специальный адаптер PATA, который поставляется опционально.

Комплекс поддерживает работу с моделями накопителей от 40 [б до 6 Тб. За это время плотность записи информации увеличилась в сотни раз, и такой разрыв не мог не отразиться на различии архитектурных решений накопителей, различиях в подходах, методиках и сложностях восстановления информации. В результате многие методики восстановления данных, хорошо работающие на HDD емкостью 40-100 [б, оказываются неприменимы для HDD - 1-6 Тб. В данном комплексе собраны наиболее универсальные методы, работающие для всех поколений HDD. При этом для работы с PC-3000 Portable не потребуется

глубокое знание принципов работы накопителей, следует только придерживаться методик, описанных в документации к комплексу.

Операционная система Windows, работая с поврежденным носителем информации, применяет доступные ей программные средства восстановления данных. Часто это лишь ухудшает ситуацию с повреждениями данных на неисправных накопителях. При использовании комплекса PC-3000 Portable доступ ОС к неисправному HDD исключается. Но при необходимости можно использовать программный драйвер монтирования дисков, который позволяет «смонтировать» диагностируемый накопитель, подключенный к портам PC-3000 Portable как дисковое устройство ОС.

Для целого ряда накопителей HDD/SSD имеется возможность использовать технологический режим, т.е., режим, который используется на заводе-изготовителе в процессе производства. Это дает расширенные возможности для получения доступа к данным пользователя и их копирования.

Комплекс PC-3000 Portable может работать в трех режимах: автономном, упрощенном и полнофункциональном. В автономном режиме используется встроенное ПО PC-3000 Portable, в нем доступны функции диагностики и создания посекторной копии данных с накопителей подключенных к портам USB и Port 0. Иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. При использовании управляющего компьютера доступны режимы упрощенный и полнофункциональный. Упрощенный режим содержит необходимый набор автоматических функций для диагностики, извлечения данных и создания иммидж-копий с накопителей подключенных к портам USB и Port 0. Как и в автономном режиме, иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. В упрощенном режиме возможно создание «Дела» и получение всех отчетов о работе с накопителем, что будет полезно специалистам области Форензик. Полнофункциональный режим содержит максимальные возможности по работе с поврежденными накопителями и является аналогом ПО комплексов PC-3000 Express и PC-3000 UDMA, отличия касаются только количества и скоростных характеристик диагностических портов контроллеров. В качестве управляющего компьютера может быть использован настольный ПК или Ноутбук. Подключение контроллера PC-3000 Portable к компьютеру осуществляется через интерфейс USB 3.0, что позволяет использовать данный комплекс, как мобильную станцию для восстановления данных и проводить работы непосредственно у заказчика.

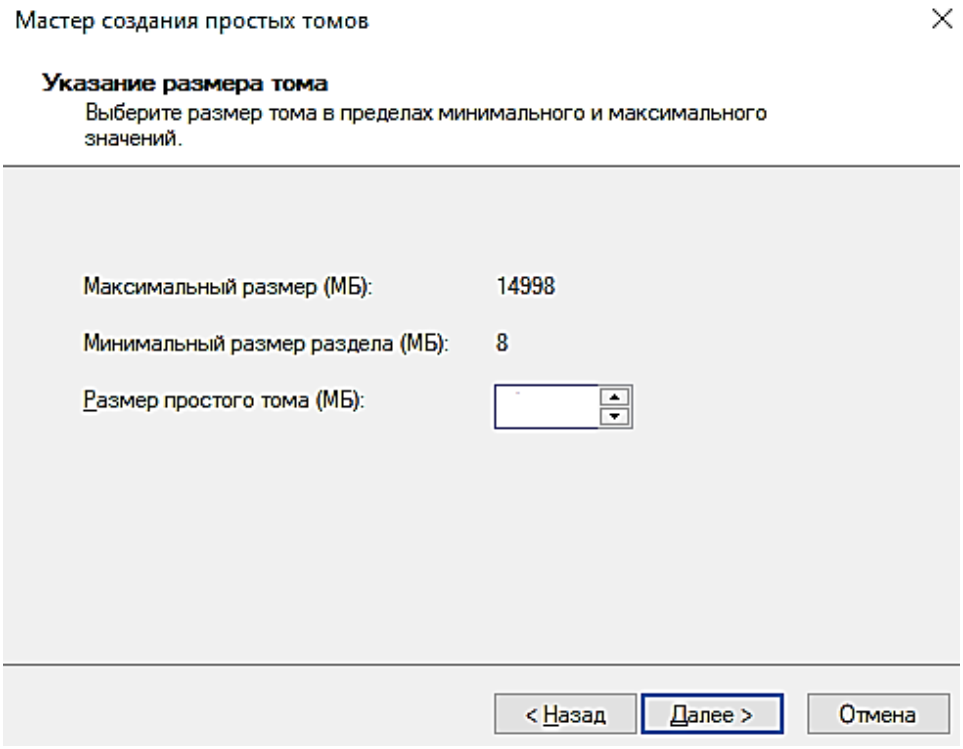
Порядок выполнения работы

1. Подготовить флеш-накопитель с файловой системой FAT32.

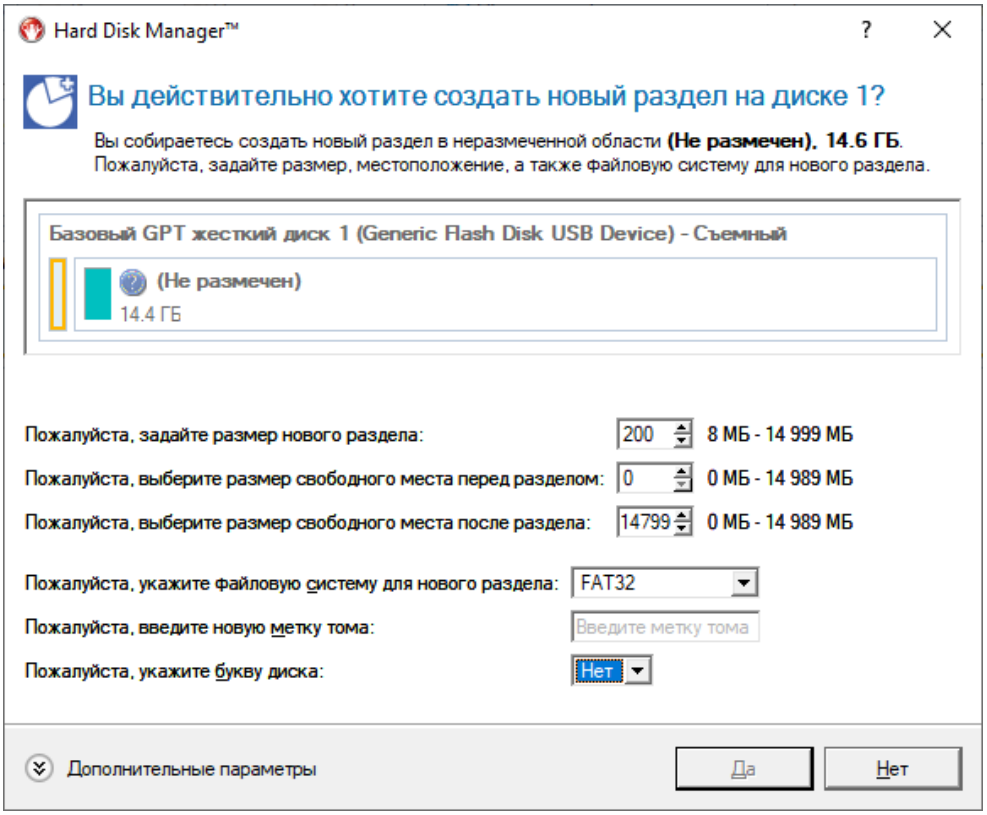
1.1. Получить у преподавателя накопитель информации.

1.2. Создать на нем раздел с файловой системой FAT32.

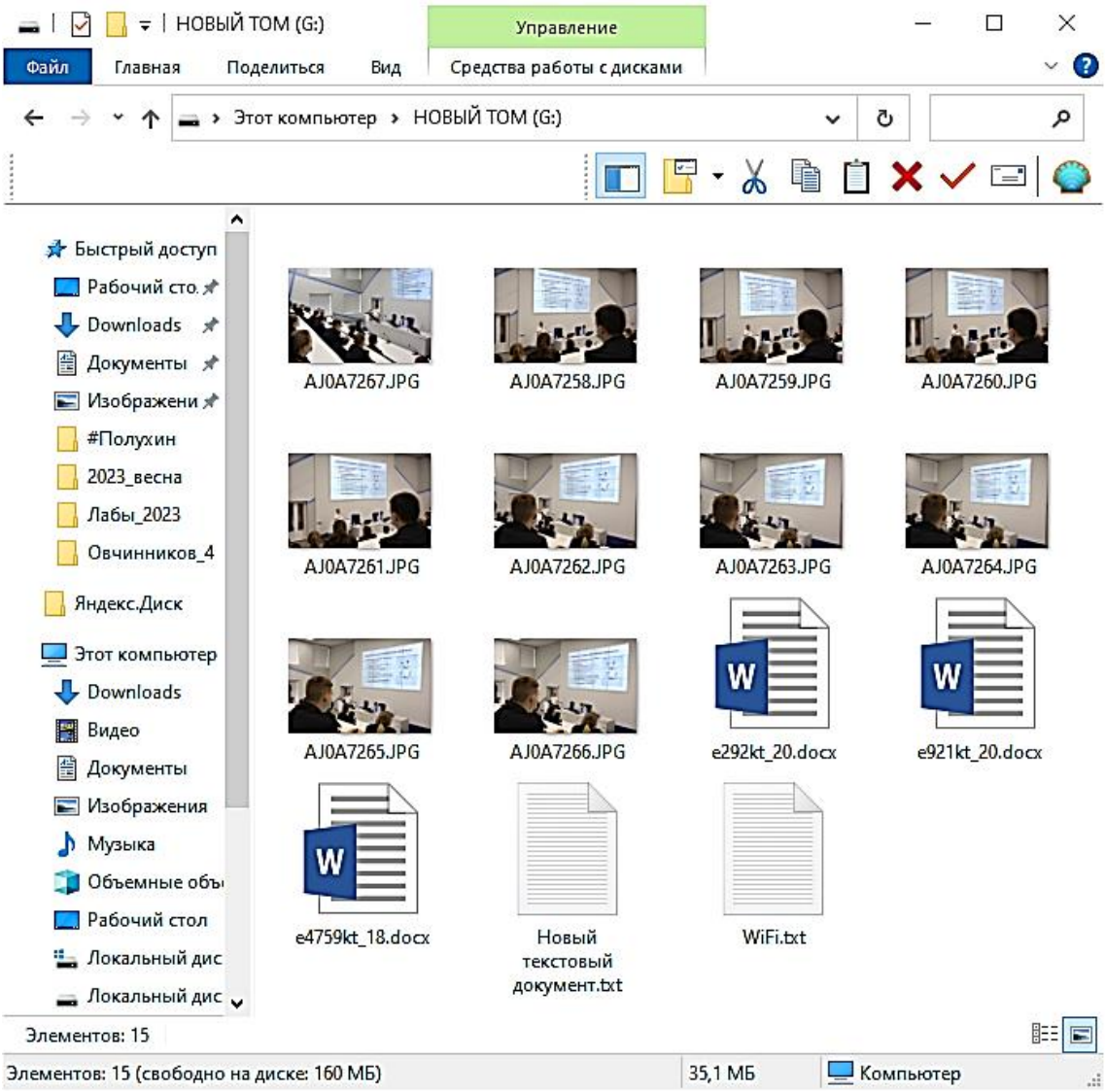
1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками. Создать том размером 200 МБ.



1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager.



1.3. Скопировать в созданный раздел несколько произвольных графических и текстовых файлов. Сделать скриншот.



1.4. Удалить скопированные файлы.

2. Восстановить удаленные файлы с флеш-накопителя.

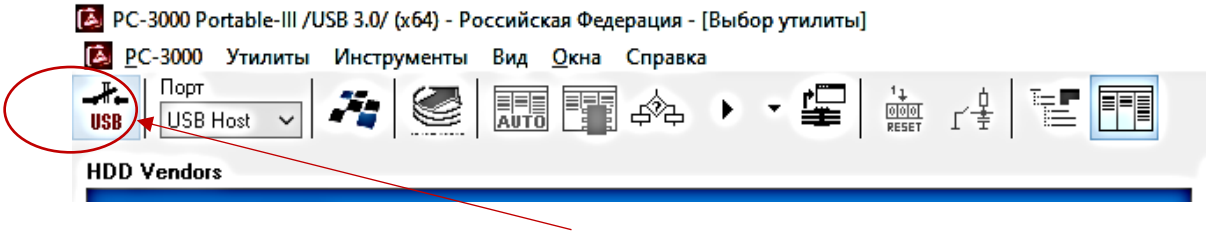
2.1. Подключить ПАК «PC-3000» к лабораторному компьютеру.

2.2. Продемонстрировать правильно подключенный ПАК «PC-3000» преподавателю ПЕРЕД ВКЛЮЧЕНИЕМ!!!

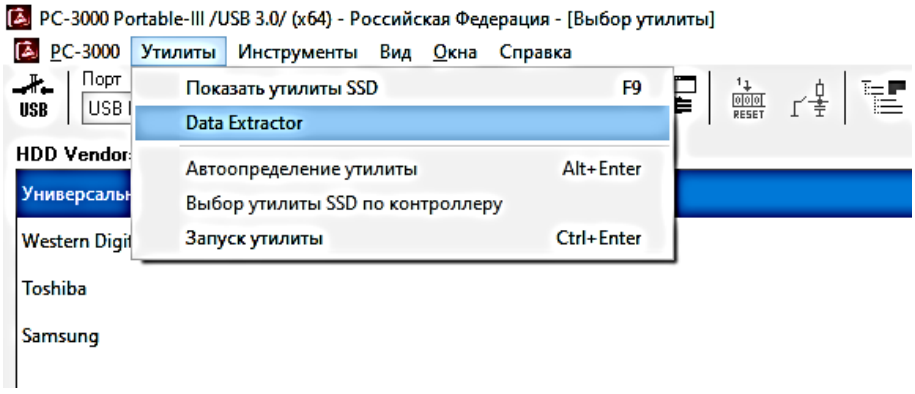
2.3. Запустить программу «PC-3000 Portable-III». Отметить галочкой порт USB.

2.4. Подключить исследуемый флеш-накопитель к ПАК «PC-3000» через интерфейсный разъем USB.

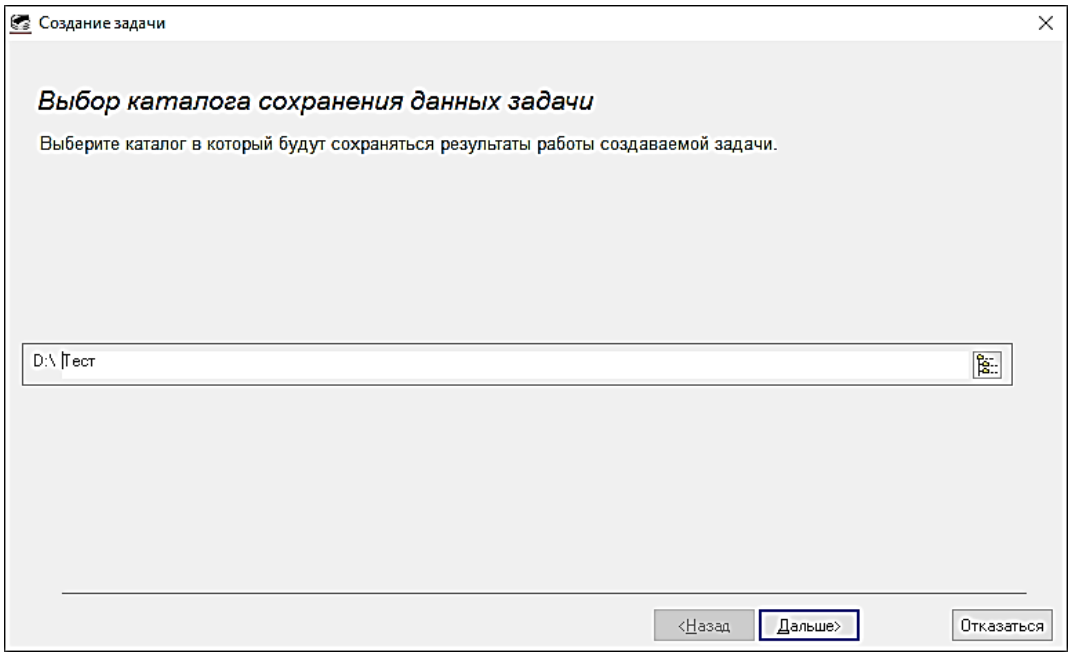
2.5. Включить питание разъема USB.



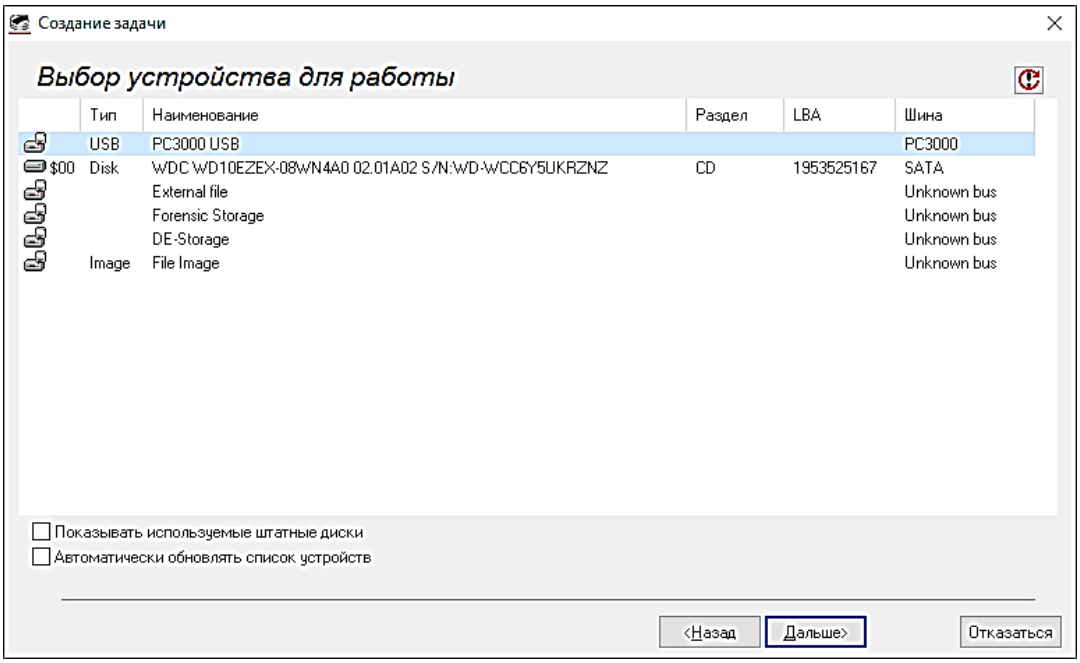
2.6. Запустить утилиту Data Extractor



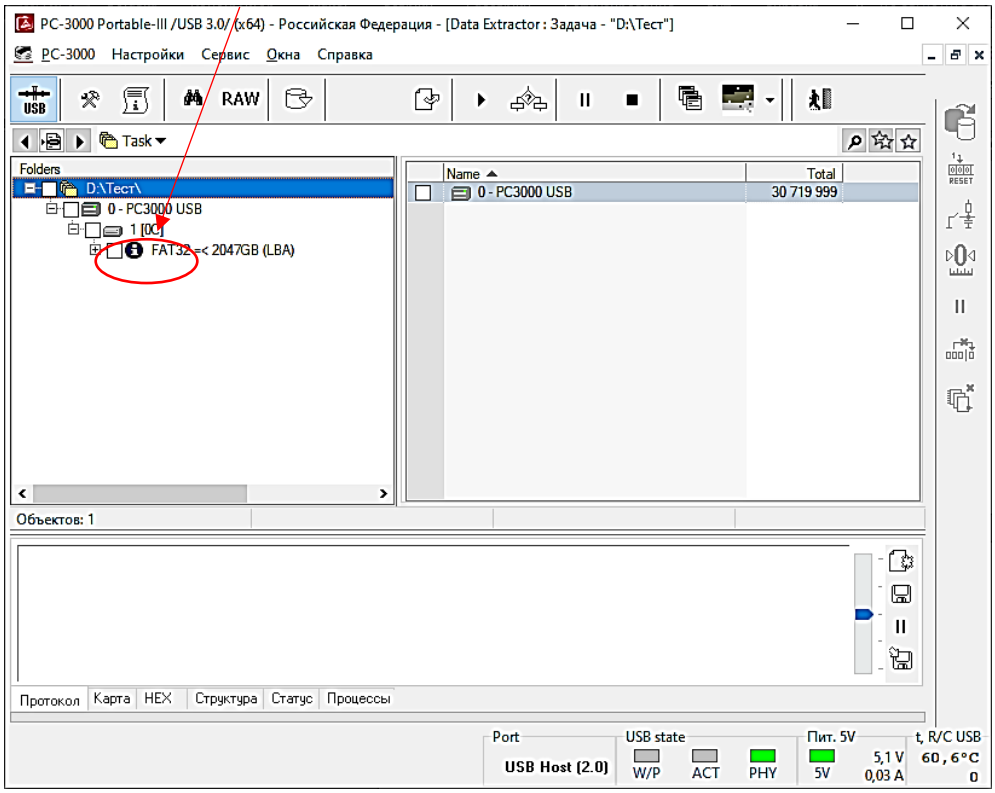
2.6. Создать новую задачу. Каталог сохранения данных задачи выбрать на диске D.



2.7. В качестве устройства для работы необходимо выбрать PC3000 USB.

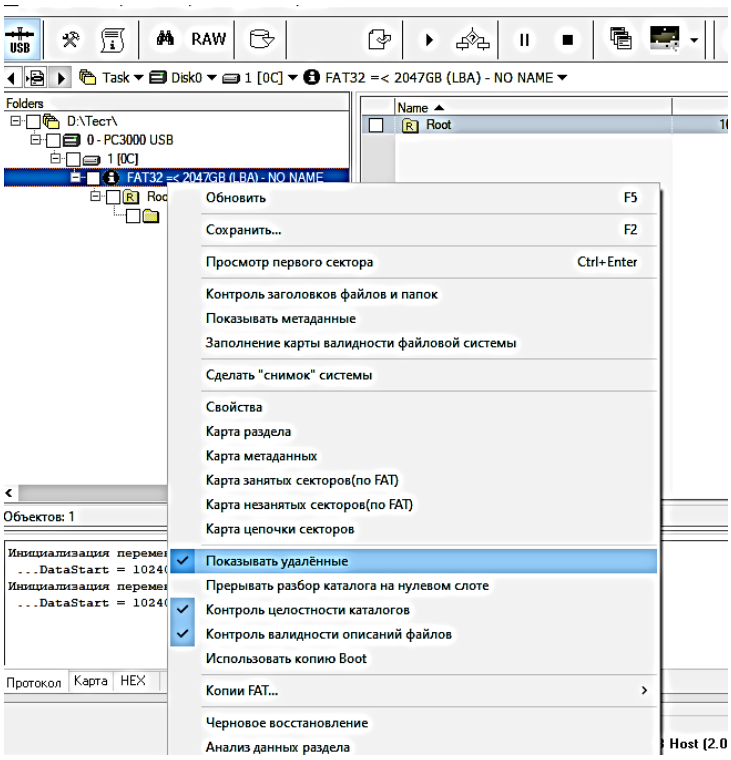


2.8. Остальные параметры оставить по умолчанию.
2.9. Если все было сделано правильно, то появится окно работы с флеш-накопителем.

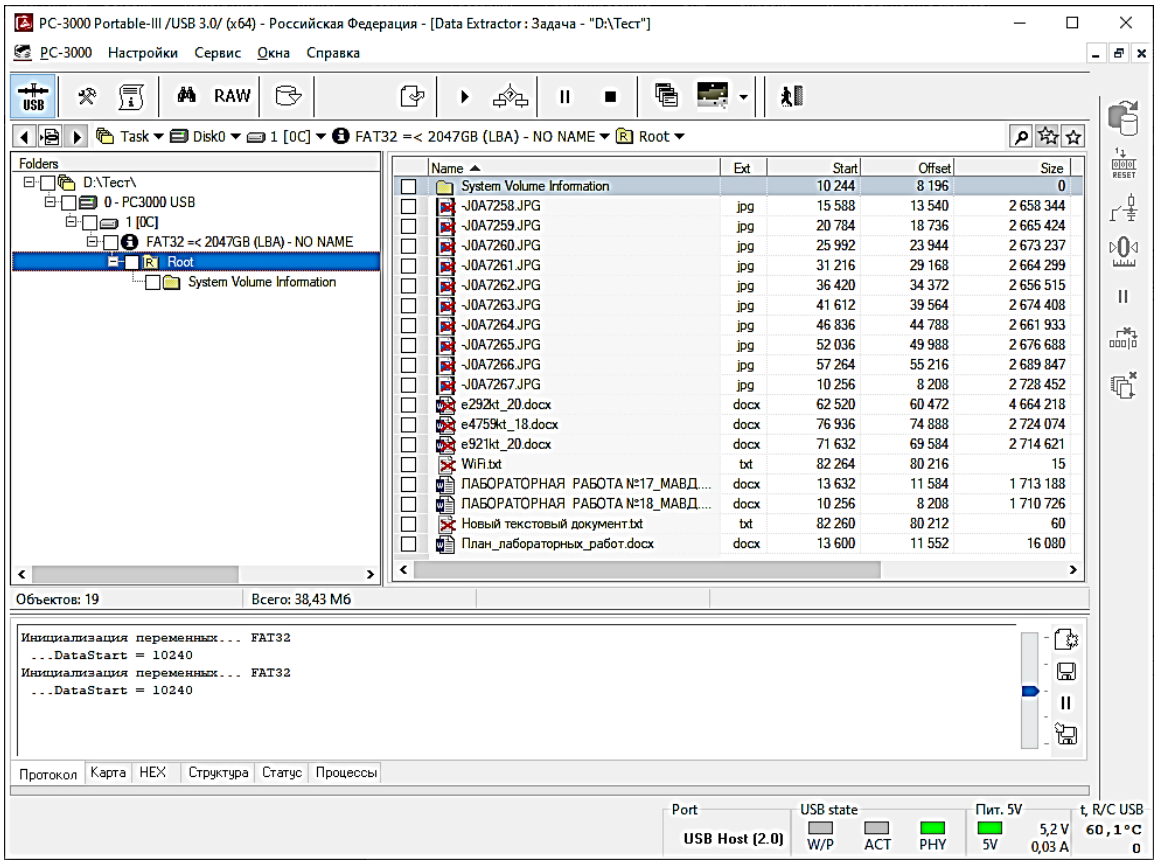


2.10. Проверить файловую систему FAT32.

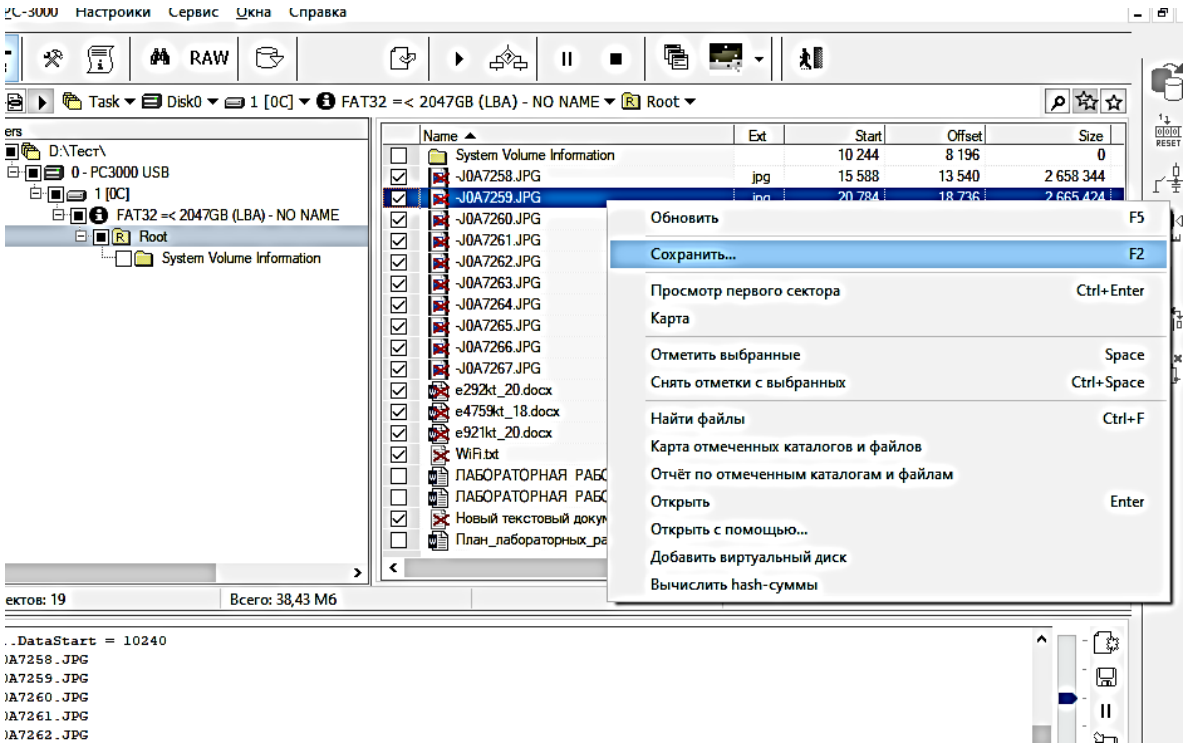
2.11. Запустить быстрое сканирование удаленных файлов. Для этого нажать на файловую систему ПКМ и выбрать пункт «Показывать удаленные».

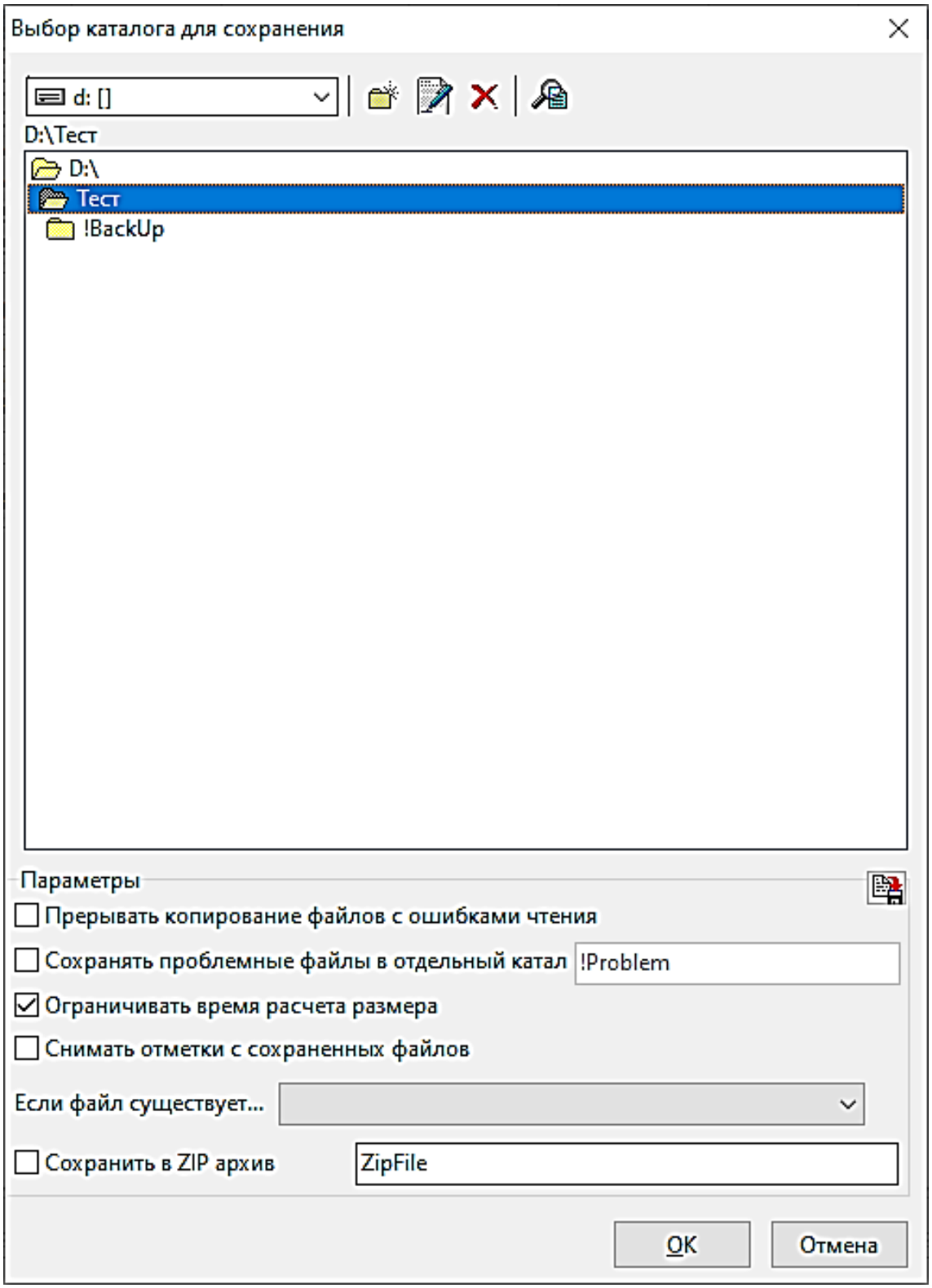


2.12. Обнаружить удаленные файлы. Они будут помечены красным крестиком.

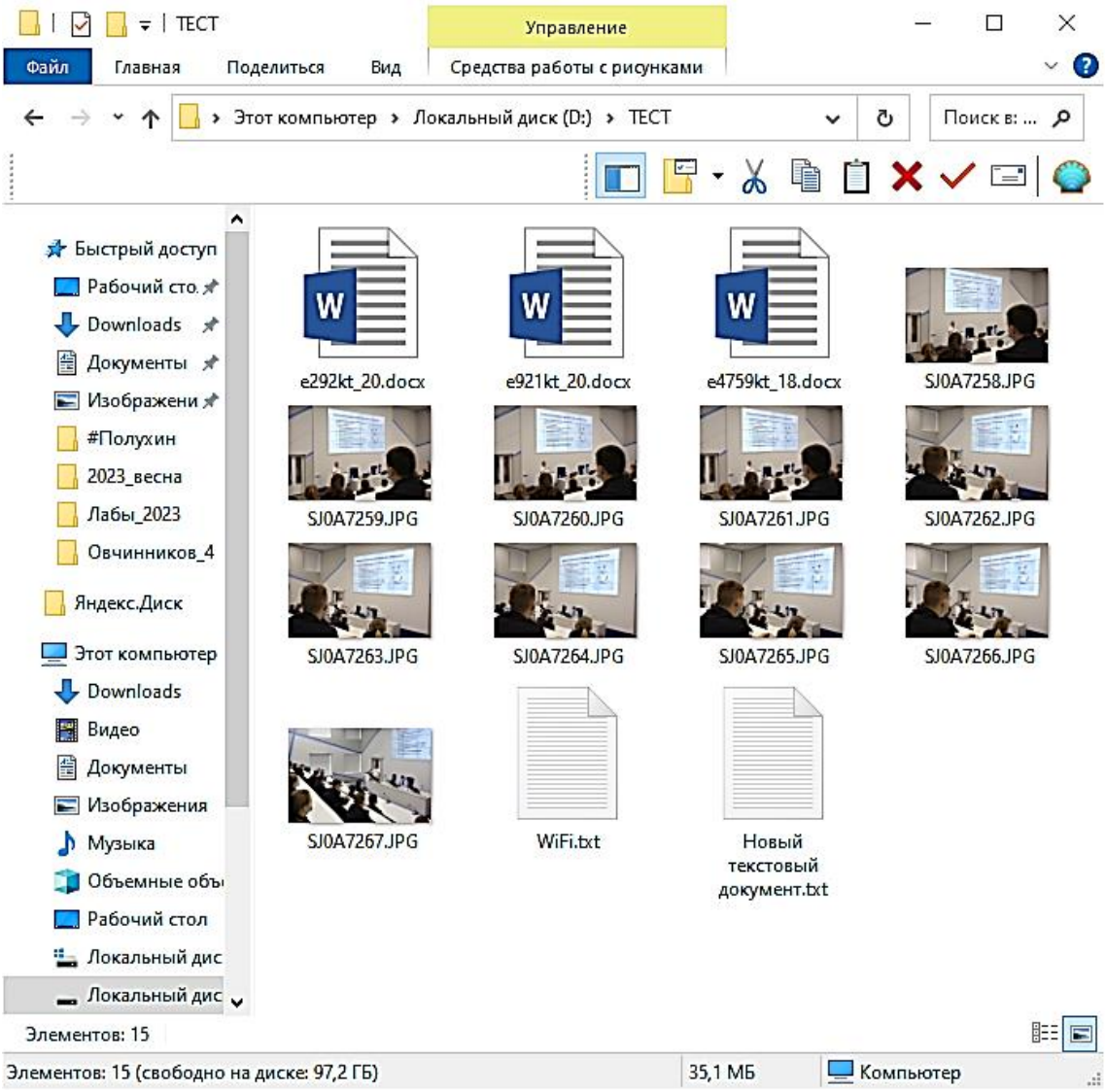


2.13. Отметить галочкой удаленные файлы и восстановить их в каталог на диске D.





3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы FAT32?
3. Какого максимального размера файлы можно помещать в файловую систему FAT32?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм восстановления файлов с помощью ПАК «PC-3000».
10. Какие типы файлов вы знаете?
11. Как обнаружить удаленные файлы с помощью ПАК «PC-3000»?
12. Для чего предназначен ПАК «PC-3000»?
13. Через какой интерфейс ПАК «PC-3000» подключается к лабораторному компьютеру?
14. Какие интерфейсные разъемы для подключения исследуемых объектов имеет ПАК «PC-3000»?
15. Как заблокировать запись на исследуемом объекте, подключенном через ПАК «PC-3000»?

ЛАБОРАТОРНАЯ РАБОТА № 20

ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ ФАЙЛОВОЙ СИСТЕМЫ NTFS С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПАК PC-3000

Цель работы: Получение практических навыков работы с ПАК PC-3000.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное оборудование.

Подготовка к выполнению работы

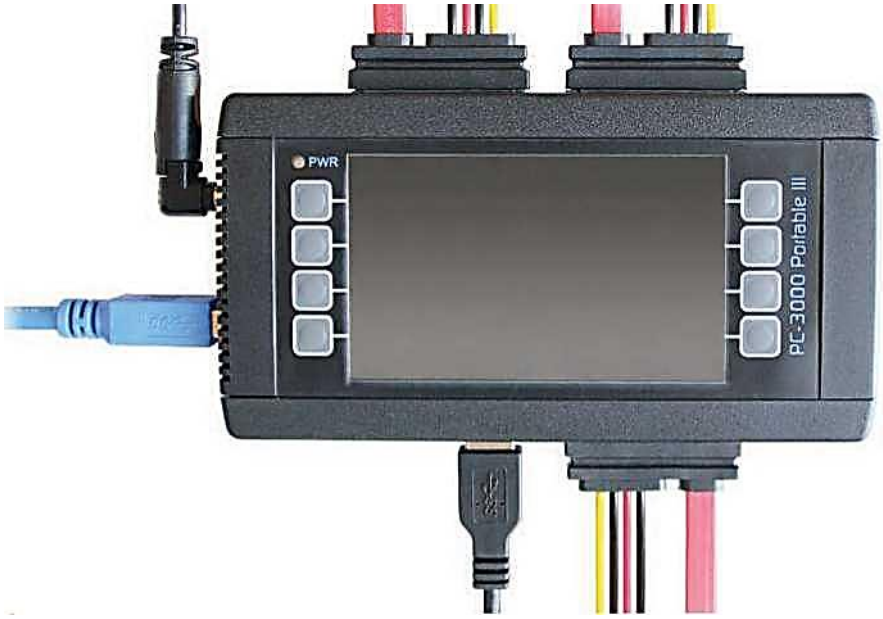
1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

PC-3000 Portable – это портативный программно-аппаратный комплекс, предназначенный для диагностики, ремонта и восстановления пользовательских данных с накопителей HDD/SSD1, имеющих физические неисправности носителей и логические повреждения файловых систем. К физическим неисправностям HDD относятся: повреждения платы электроники, магнитных дисков, головок чтения-записи, предусилителя, микропрограммы, служебной информации. К физическим неисправностям SDD относятся: повреждения платы электроники, контроллера, деградация ячеек массива NAND-Flash памяти, повреждение микропрограммы, служебной информации и др. К логическим неисправностям относятся: повреждения дисковых структур, структур файловых систем и комбинации этих проблем. Дополнительно, PC-3000 Portable позволяет создавать имидж-копии данных с накопителей HDD, SSD, USB-Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны.

Диагностируемые HDD/SSD/Flash накопители, подлежащие восстановлению данных, подключаются непосредственно к контроллеру PC 3000 Portable – к его портам SOURCE – USB и Port0. К портам TARGET – Port1 и Port2 подключаются HDD/SSD накопители для создания имидж-копии

данных. В некоторых режимах работы порты Port1 и Port2 также могут использоваться для подключения диагностируемых/восстанавливаемых накопителей, увеличивая тем самым общее число одновременно восстанавливаемых HDD/SSD до трех.



Порты SOURCE - USB и Port 0 допускают блокировку от записи, для ее включения необходимо воспользоваться переключателем Write Protection. При включенной блокировке должен гореть жетлый светодиод.

Контроллер PC-3000 Portable подключается к внешнему источнику питания -19В, и в случае работы через управляющий компьютер подключается к нему через интерфейс USB 3.0.

В существующей реализации контроллер PC-3000 Portable допускает подключение накопителей HDD/SSD с интерфейсом SATA-III (совместим с SATA-I/II, SSD M.2 NVMe PCIe) и накопителей с USB интерфесом, соответствующих классификации Mass Storage Device – внешние HDD/ SSD USB 2.0/3.0 и USB-Flash накопители. Подключение накопителей с интерфейсом PATA (IDE) возможно через специальный адаптер PATA, который поставляется опционально.

Комплекс поддерживает работу с моделями накопителей от 40 [б до 6 Тб. За это время плотность записи информации увеличилась в сотни раз, и такой разрыв не мог не отразиться на различии архитектурных решений накопителей, различиях в подходах, методиках и сложностях восстановления информации. В результате многие методики восстановления данных, хорошо работающие на HDD емкостью 40-100 [б, оказываются неприменимы для HDD - 1-6 Тб. В данном комплексе собраны наиболее универсальные методы, работающие для всех поколений HDD. При этом для работы с PC-3000 Portable не потребуется глубокое знание принципов работы накопителей, следует только придерживаться методик, описанных в документации к комплексу.

Операционная система Windows, работая с поврежденным носителем информации, применяет доступные ей программные средства восстановления данных. Часто это лишь ухудшает ситуацию с повреждениями данных на неисправных накопителях. При использовании комплекса PC-3000 Portable доступ ОС к неисправному HDD исключается. Но при необходимости можно использовать программный драйвер монтирования дисков, который позволяет «смонтировать» диагностируемый накопитель, подключенный к портам PC-3000 Portable как дисковое устройство ОС.

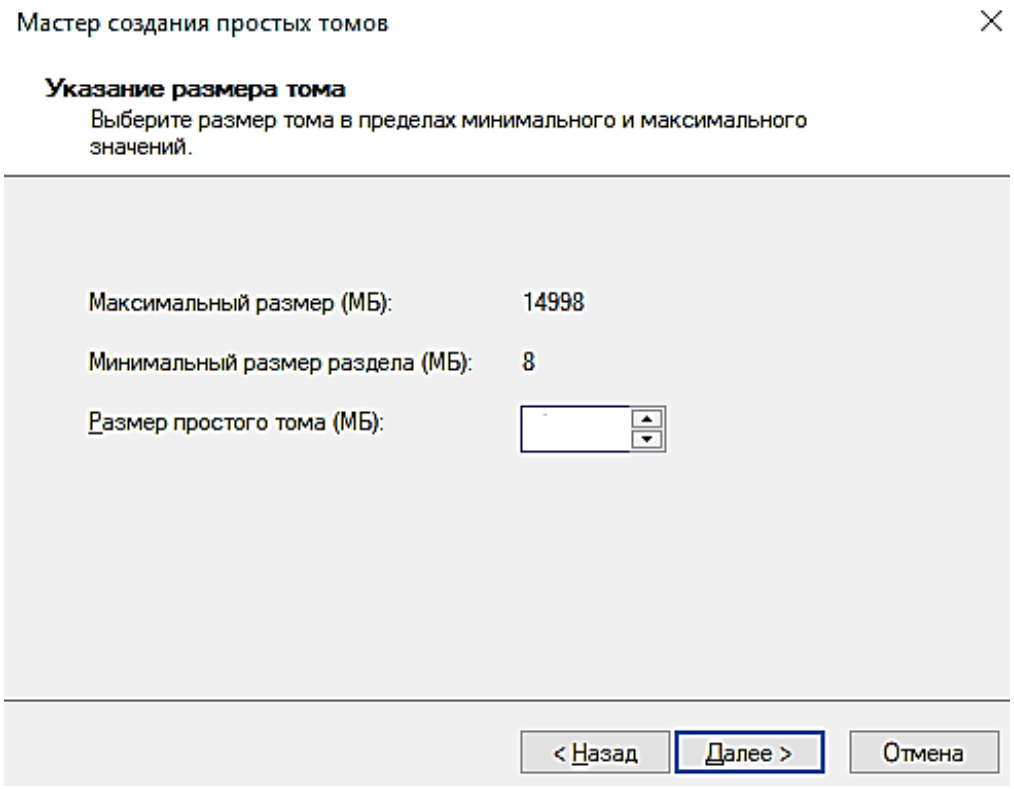
Для целого ряда накопителей HDD/SSD имеется возможность использовать технологический режим, т.е., режим, который используется на заводе-изготовителе в процессе производства. Это дает расширенные возможности для получения доступа к данным пользователя и их копирования.

Комплекс PC-3000 Portable может работать в трех режимах: автономном, упрощенном и полнофункциональном. В автономном режиме используется встроенное ПО PC-3000 Portable, в нем доступны функции диагностики и создания посекторной копии данных с накопителей подключенных к портам USB и Port 0. Иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. При использовании управляющего компьютера доступны режимы упрощенный и полнофункциональный. Упрощенный режим содержит необходимый набор автоматических функций для диагностики, извлечения данных и создания иммидж-копий с накопителей подключенных к портам USB и Port 0. Как и в автономном режиме, иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. В упрощенном режиме возможно создание «Дела» и получение всех отчетов о работе с накопителем, что будет полезно специалистам области Форензик. Полнофункциональный режим содержит максимальные возможности по работе с поврежденными накопителями и является аналогом ПО комплексов PC-3000 Express и PC-3000 UDMA, отличия касаются только количества и скоростных характеристик диагностических портов контроллеров. В качестве управляющего компьютера может быть использован настольный ПК или Ноутбук. Подключение контроллера PC-3000 Portable к компьютеру осуществляется через интерфейс USB 3.0, что позволяет использовать данный комплекс, как мобильную станцию для восстановления данных и проводить работы непосредственно у заказчика.

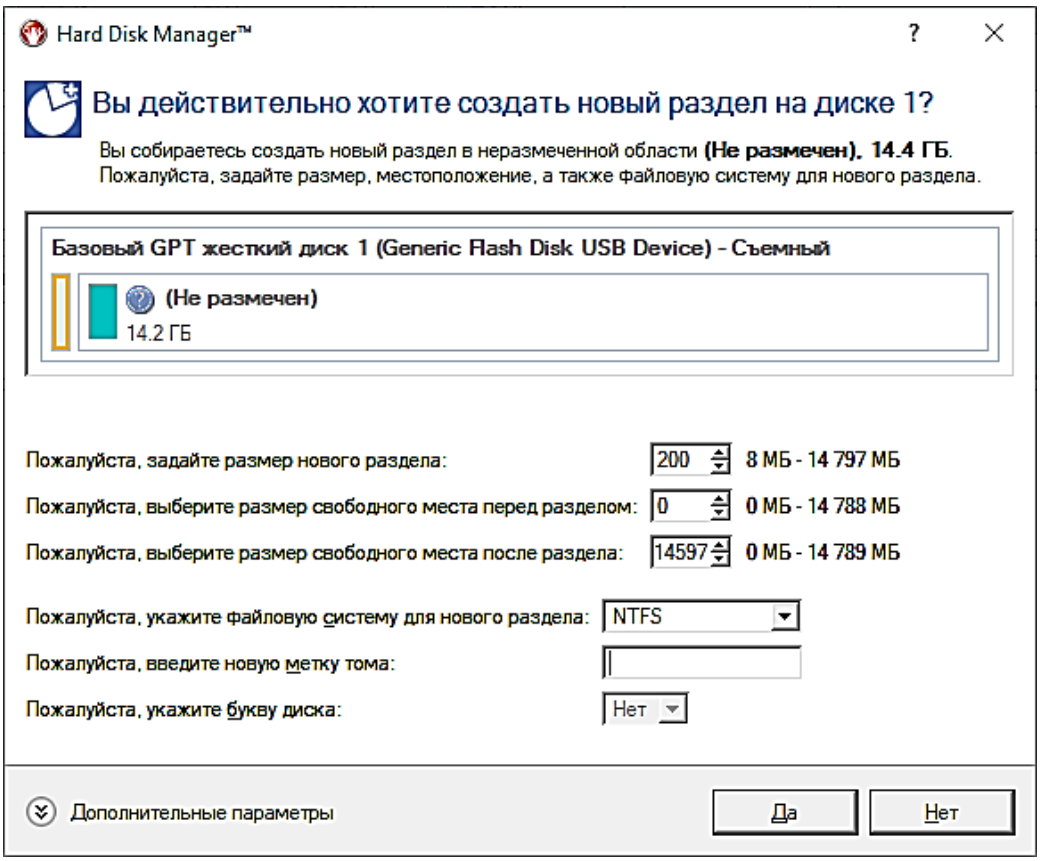
Порядок выполнения работы

1. Подготовить флеш-накопитель с файловой системой NTFS.
    1.1. Получить у преподавателя накопитель информации.
    1.2. Создать на нем раздел с файловой системой NTFS.

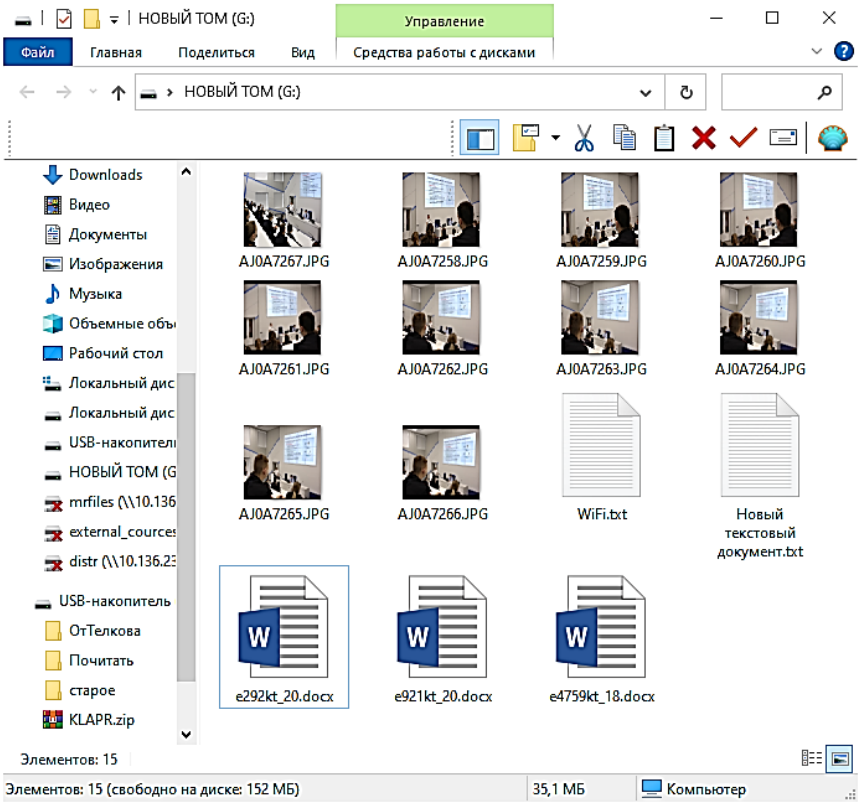
1.2.1. Для этого нажать ПКМ на компьютер и выбрать пункт «Управление»\Управление дисками. Создать том размером 200 МБ.



1.2.2. Либо можно использовать ПО Paragon Hard Disk Manager.



1.3. Скопировать в созданный раздел несколько произвольных графических и текстовых файлов. Сделать скриншот.



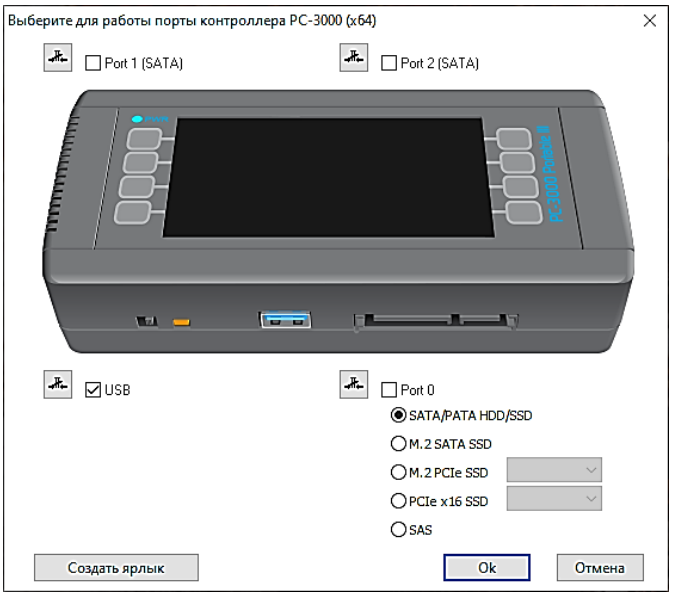
1.4. Удалить скопированные файлы.

2. Восстановить удаленные файлы с флеш-накопителя.

2.1. Подключить ПАК «PC-3000» к лабораторному компьютеру.

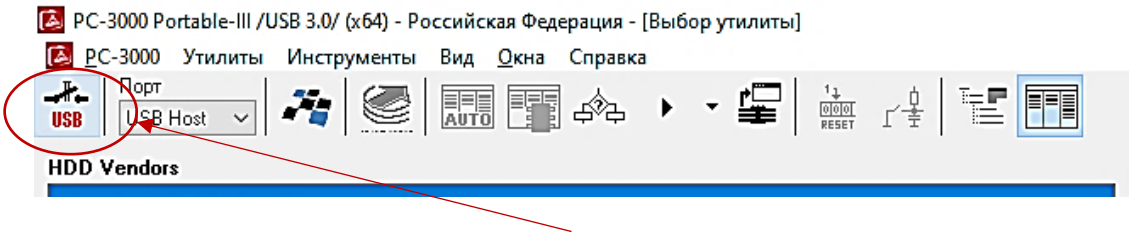
2.2. Продемонстрировать правильно подключенный ПАК «PC-3000» преподавателю ПЕРЕД ВКЛЮЧЕНИЕМ!!!

2.3. Запустить программу «PC-3000 Portable-III». Отметить галочкой порт USB.

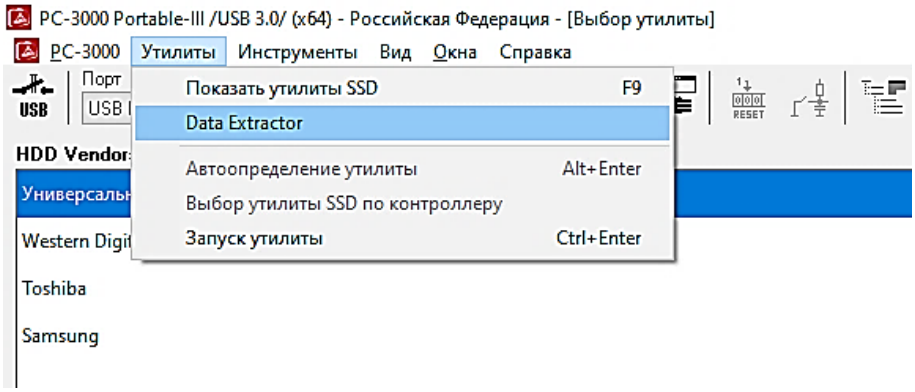


2.4. Подключить исследуемый флеш-накопитель к ПАК «PC-3000» через интерфейсный разъем USB.

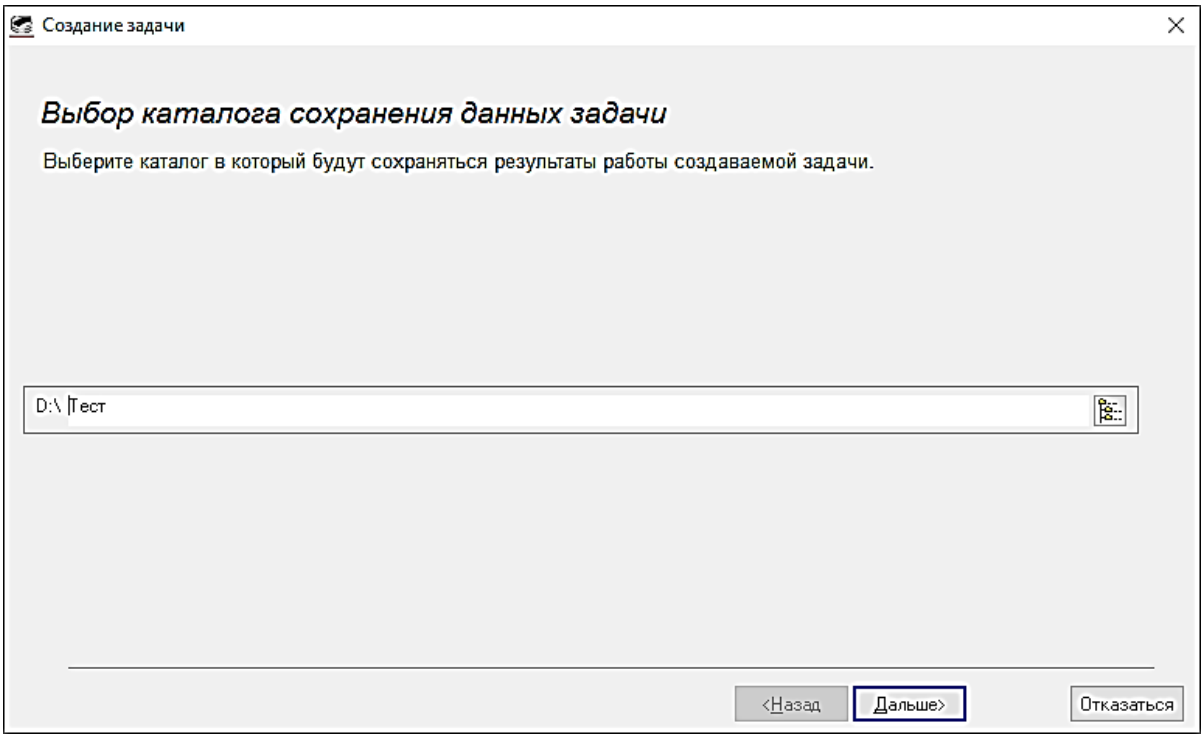
2.5. Включить питание разъема USB.



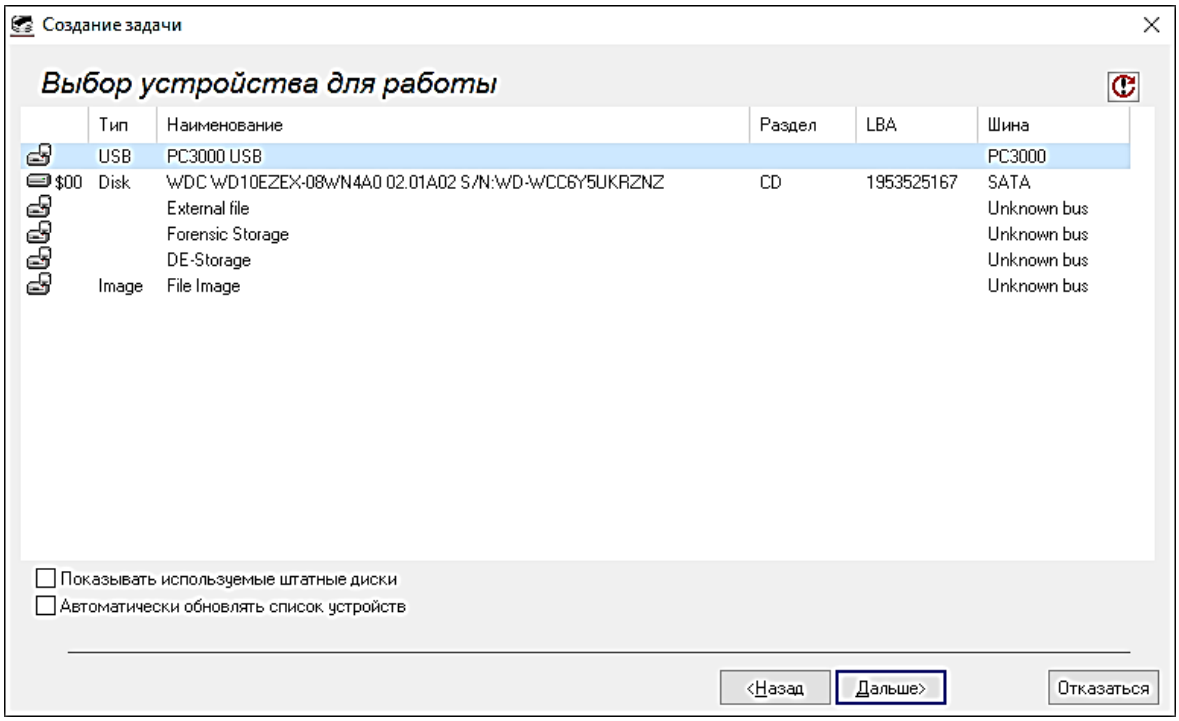
2.6. Запустить утилитуData Extractor.



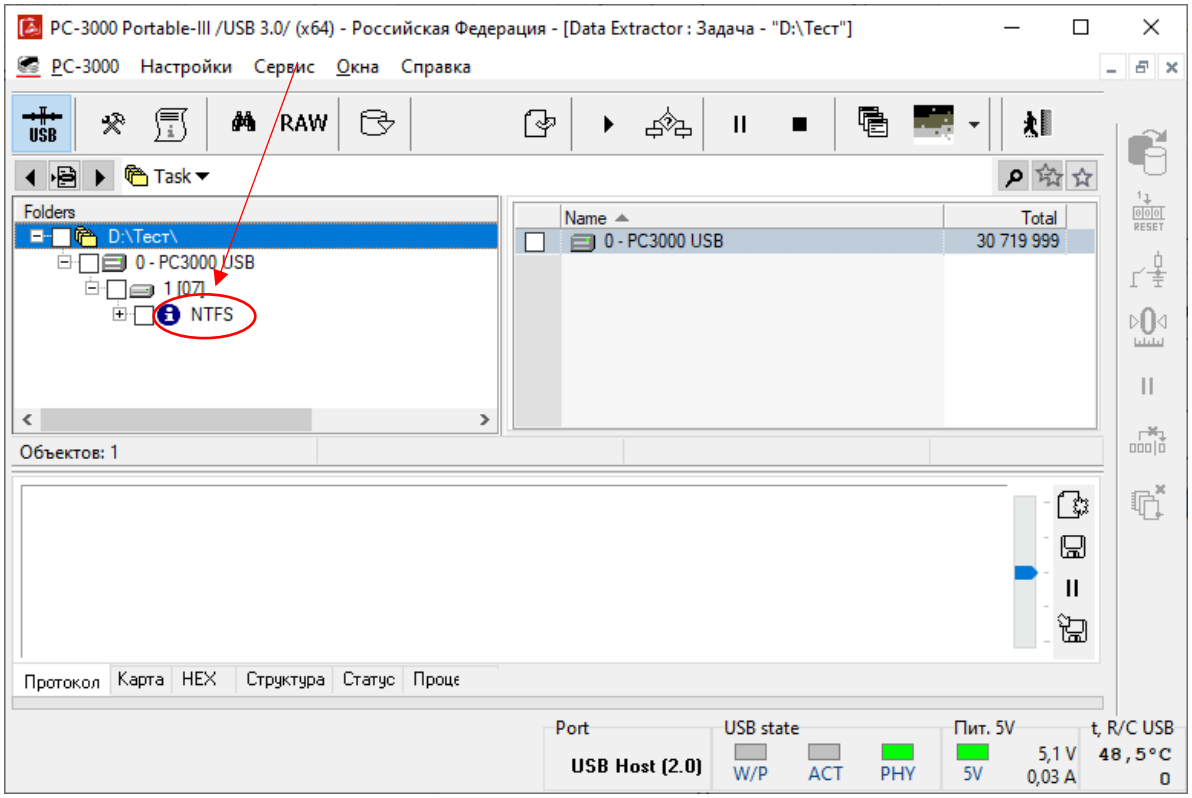
2.6. Создать новую задачу. Каталог сохранения данных задачи выбрать на диске D.



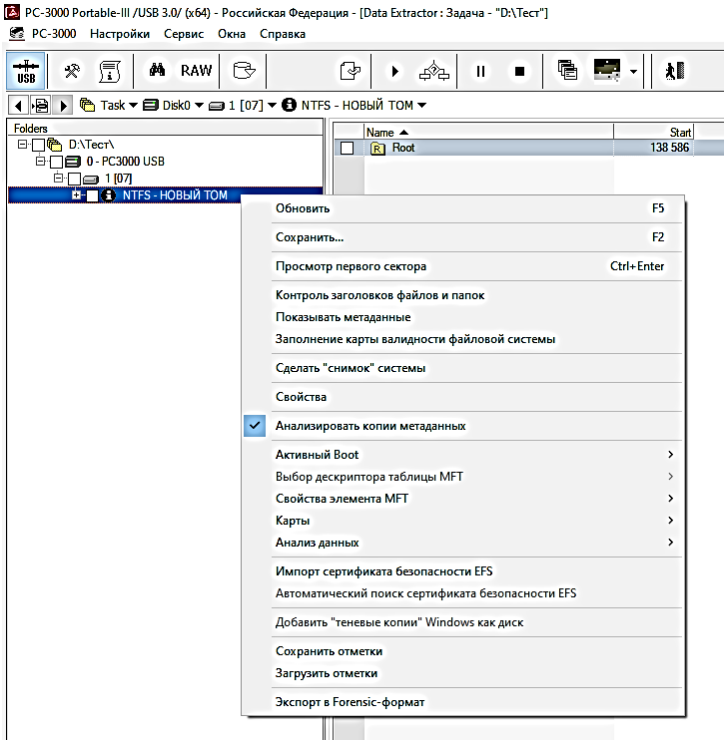
2.7. В качестве устройства для работы необходимо выбрать PC3000 USB.



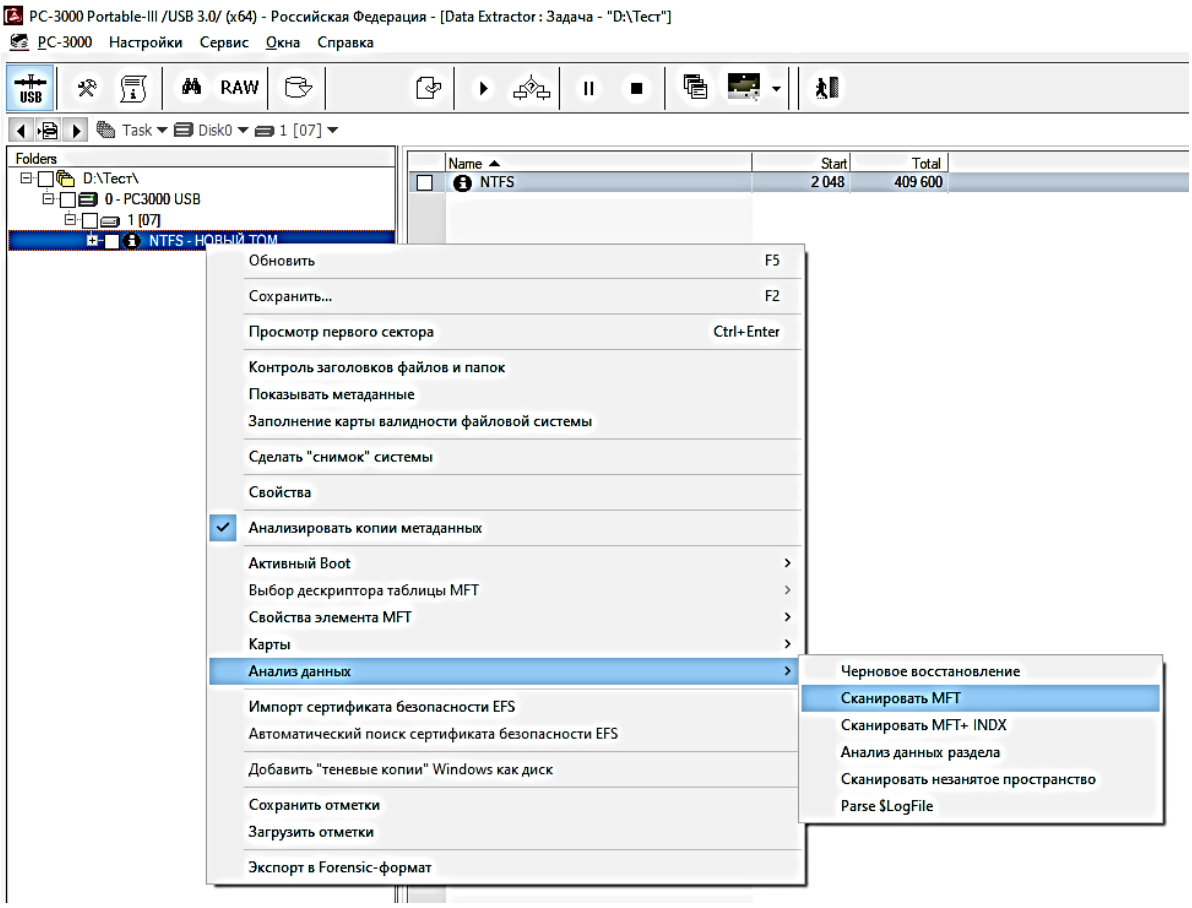
2.8. Остальные параметры оставить по умолчанию.
2.9. Если все было сделано правильно, то появится окно работы с флеш-накопителем.



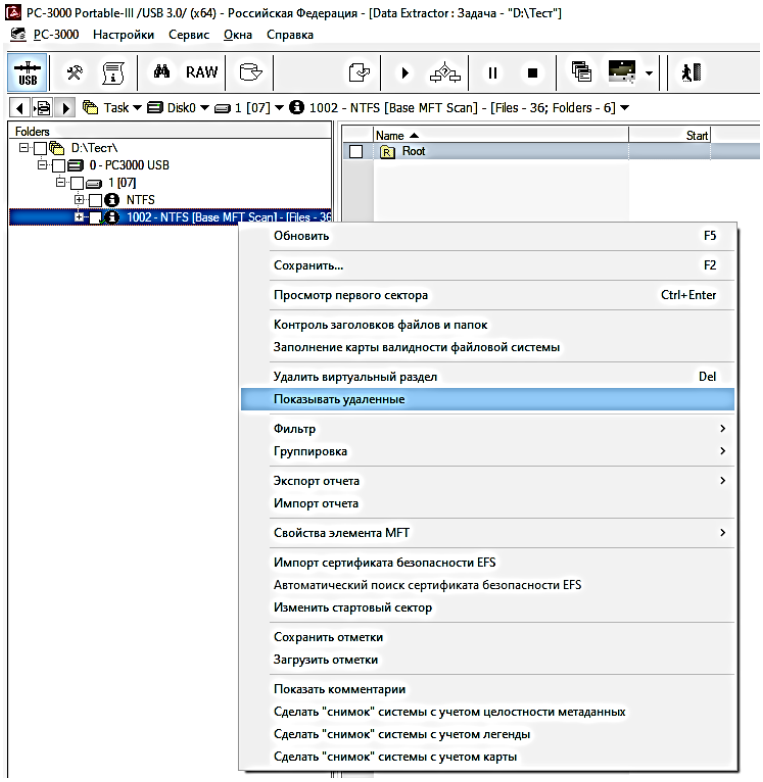
2.10. Проверить файловую систему NTFS.
2.11. Запустить быстрое сканирование удаленных файлов. Для этого нажать на файловую систему ПКМ и выбрать пункт «Показывать удаленные».



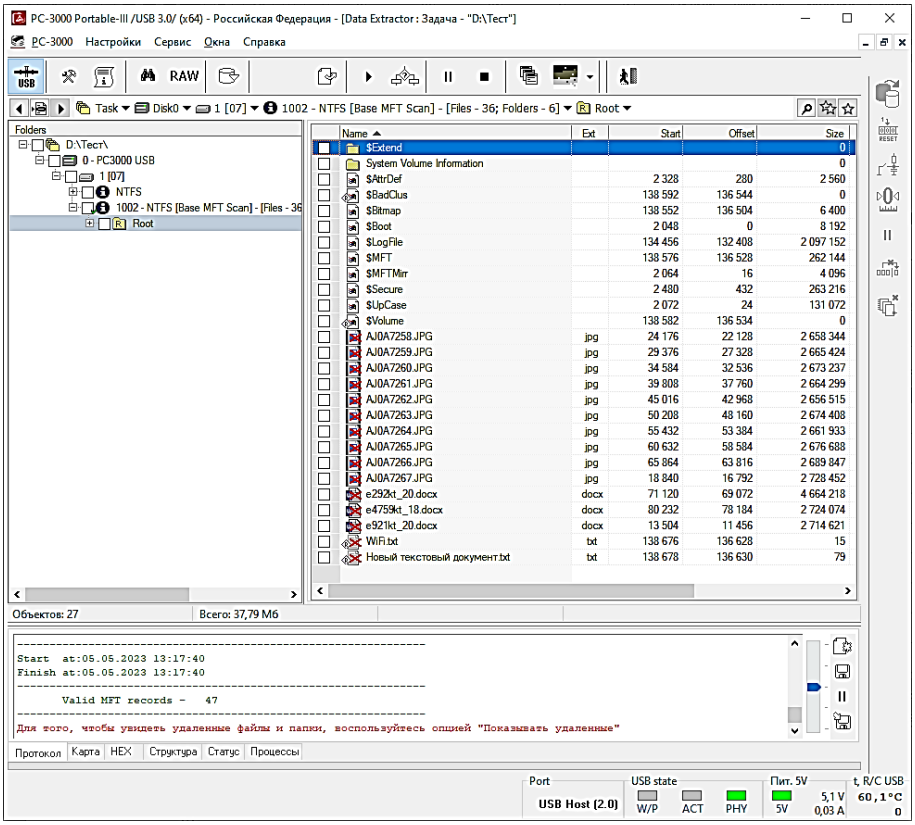
2.11.1. Если такого пункта меню нет, то необходимо сначала провести анализ данных и просканировать MFT.



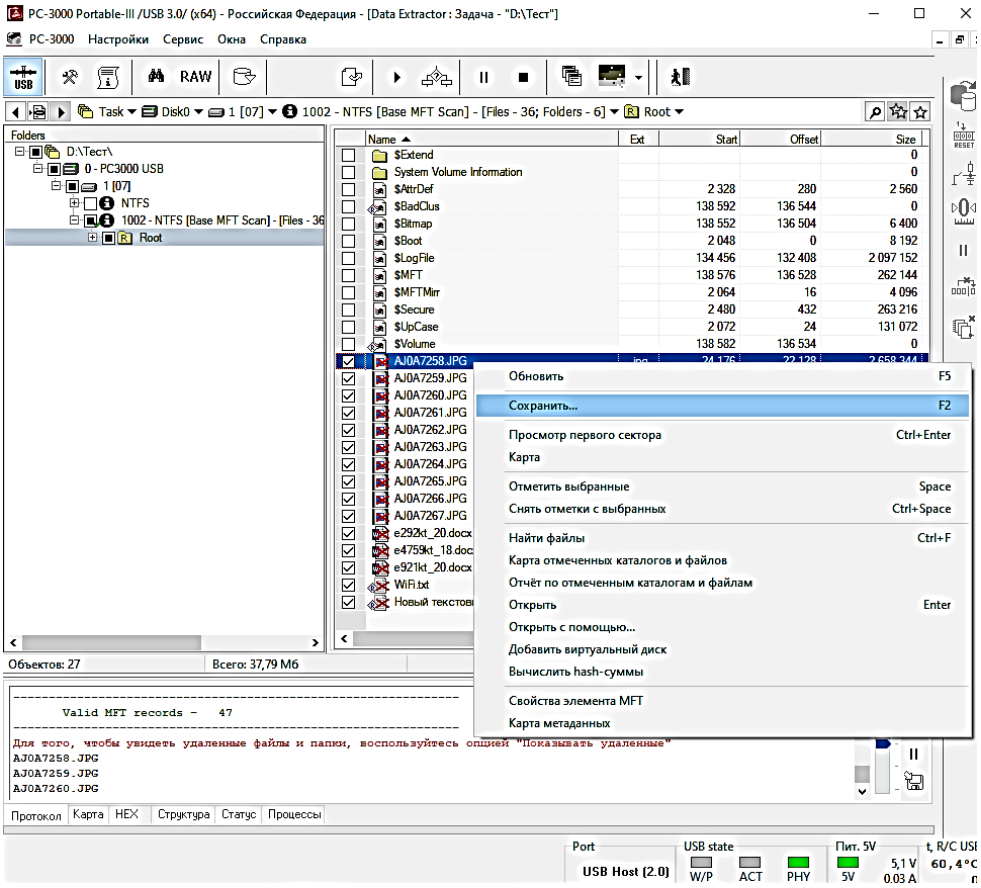
2.11.2. Затем нажать на файловую систему нового виртуального раздела ПКМ и выбрать пункт «Показывать удаленные».

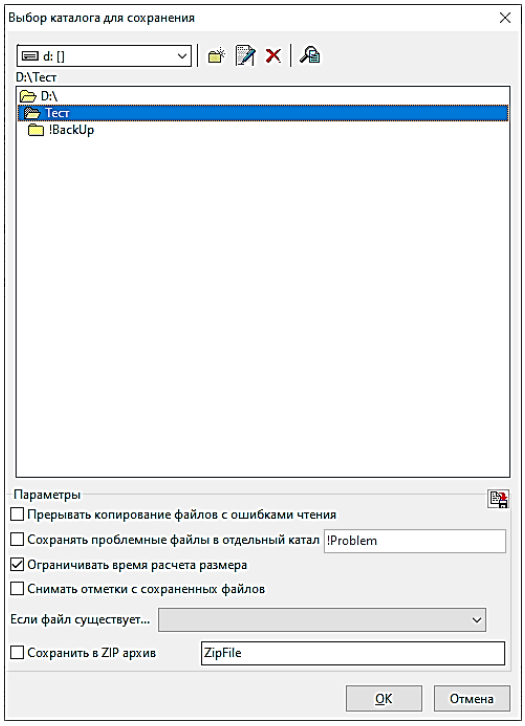


2.12. Обнаружить удаленные файлы. Они будут помечены красным крестиком.

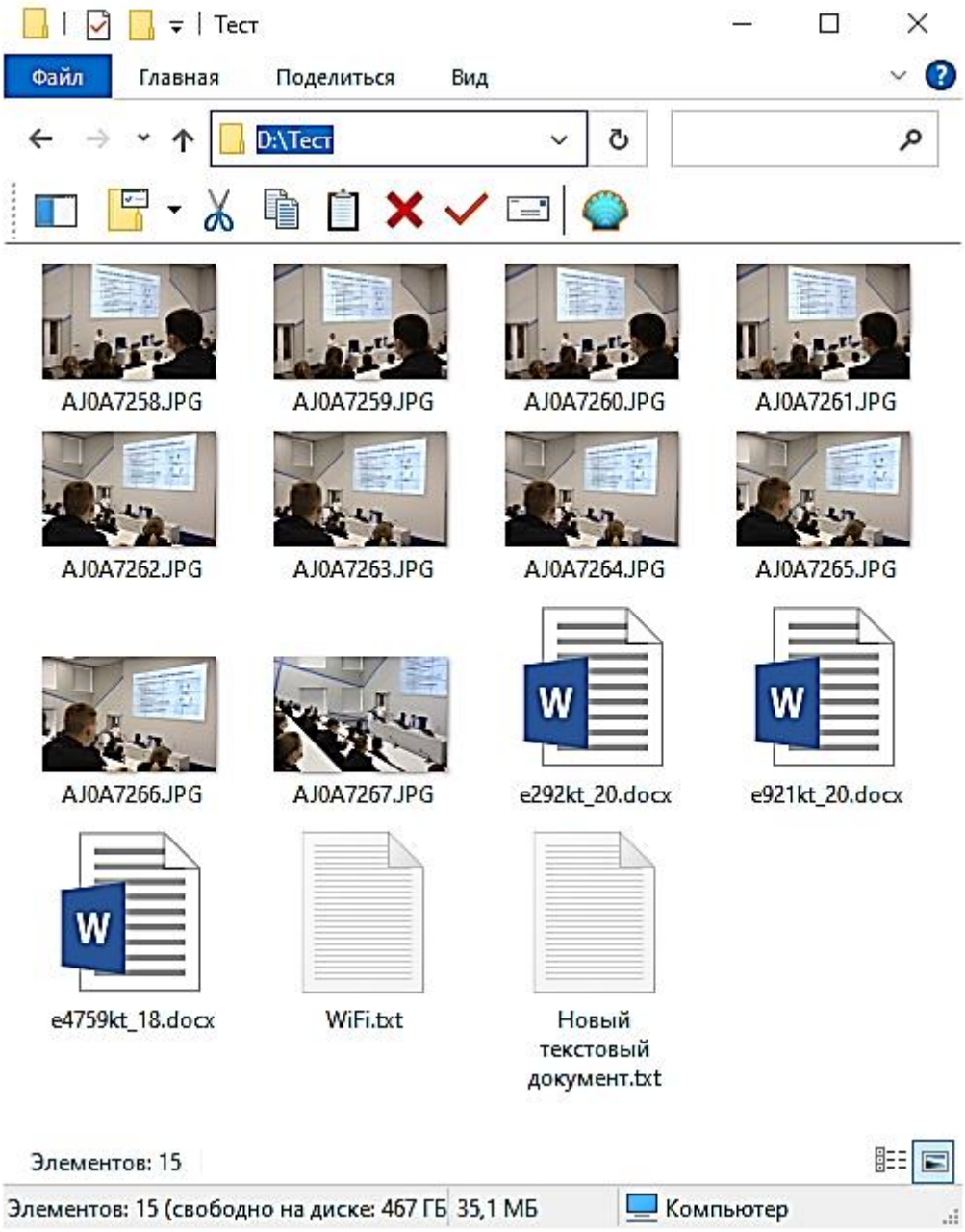


2.13. Отметить галочкой удаленные файлы и восстановить их в каталог на диске D.





3. Проверить восстановленные файлы. Сделать скриншот.



4. Сравнить скриншоты из пунктов 1.3 и 3.
5. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Какие особенности файловой системы NTFS?
3. Какого максимального размера файлы можно помещать в файловую систему NTFS?
4. Что такое MFT?
5. Какая информация хранится в MFT?
6. Как MFT может помочь в восстановлении информации?
7. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
8. Какое программное обеспечение позволяет создавать файлы-образы?
9. Опишите алгоритм восстановления файлов с помощью ПАК «PC-3000».
10. Какие типы файлов вы знаете?
11. Как обнаружить удаленные файлы с помощью ПАК «PC-3000»?
12. Для чего предназначен ПАК «PC-3000»?
13. Через какой интерфейс ПАК «PC-3000» подключается к лабораторному компьютеру?
14. Какие интерфейсные разъемы для подключения исследуемых объектов имеет ПАК «PC-3000»?
15. Как заблокировать запись на исследуемом объекте, подключенном через ПАК «PC-3000»?

ЛАБОРАТОРНАЯ РАБОТА № 21

ВОССТАНОВЛЕНИЕ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ИЗ НЕИЗВЕСТНОЙ ФАЙЛОВОЙ СИСТЕМЫ ФЛЕШ-НАКОПИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ КОМБИНИРОВАННОГО СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков работы с ПАК PC-3000 и ПО R-Studio.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное оборудование.

Подготовка к выполнению работы

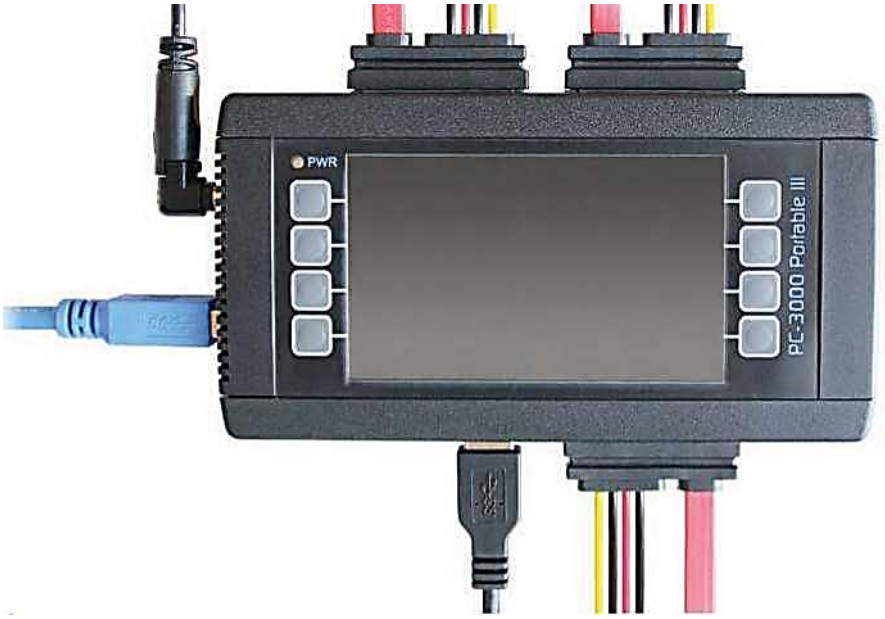
1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

PC-3000 Portable – это портативный программно-аппаратный комплекс, предназначенный для диагностики, ремонта и восстановления пользовательских данных с накопителей HDD/SSD1, имеющих физические неисправности носителей и логические повреждения файловых систем. К физическим неисправностям HDD относятся: повреждения платы электроники, магнитных дисков, головок чтения-записи, предусилителя, микропрограммы, служебной информации. К физическим неисправностям SDD относятся: повреждения платы электроники, контроллера, деградация ячеек массива NAND-Flash памяти, повреждение микропрограммы, служебной информации и др. К логическим неисправностям относятся: повреждения дисковых структур, структур файловых систем и комбинации этих проблем. Дополнительно, PC-3000 Portable позволяет создавать имидж-копии данных с накопителей HDD, SSD, USB-Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны.

Диагностируемые HDD/SSD/Flash накопители, подлежащие восстановлению данных, подключаются непосредственно к контроллеру PC

3000 Portable – к его портам SOURCE - USB и Port0. К портам TARGET - Port1 и Port2 подключаются HDD/SSD накопители для создания имидж-копии данных. В некоторых режимах работы порты Port1 и Port2 также могут использоваться для подключения диагностируемых/восстанавливаемых накопителей, увеличивая тем самым общее число одновременно восстанавливаемых HDD/SSD до трех.



Порты SOURCE - USB и Port 0 допускают блокировку от записи, для ее включения необходимо воспользоваться переключаетелем Write Protection. При включенной блокировке должен гореть жетлый светодиод.

Контроллер PC-3000 Portable подключается к внешнему источнику питания -19В, и в случае работы через управляющий компьютер подключается к нему через интерфейс USB 3.0.

В существующей реализации контроллер PC-3000 Portable допускает подключение накопителей HDD/SSD с интерфейсом SATA-III (совместим с SATA-I/II, SSD M.2 NVMe PCIe) и накопителей с USB интерфесом, соответствующих классификации Mass Storage Device – внешние HDD/ SSD USB 2.0/3.0 и USB-Flash накопители. Подключение накопителей с интерфейсом PATA (IDE) возможно через специальный адаптер PATA, который поставляется опционально.

Комплекс поддерживает работу с моделями накопителей от 40 [б до 6 Тб. За это время плотность записи информации увеличилась в сотни раз, и такой разрыв не мог не отразиться на различии архитектурных решений накопителей, различиях в подходах, методиках и сложностях восстановления информации. В результате многие методики восстановления данных, хорошо работающие на HDD емкостью 40-100 [б, оказываются неприменимы для HDD - 1-6 Тб. В данном комплексе собраны наиболее универсальные методы, работающие для всех поколений HDD. При этом для работы с PC-3000 Portable не потребуется глубокое знание

принципов работы накопителей, следует только придерживаться методик, описанных в документации к комплексу.

Операционная система Windows, работая с поврежденным носителем информации, применяет доступные ей программные средства восстановления данных. Часто это лишь ухудшает ситуацию с повреждениями данных на неисправных накопителях. При использовании комплекса PC-3000 Portable доступ ОС к неисправному HDD исключается. Но при необходимости можно использовать программный драйвер монтирования дисков, который позволяет «смонтировать» диагностируемый накопитель, подключенный к портам PC-3000 Portable как дисковое устройство ОС.

Для целого ряда накопителей HDD/SSD имеется возможность использовать технологический режим, т.е., режим, который используется на заводе-изготовителе в процессе производства. Это дает расширенные возможности для получения доступа к данным пользователя и их копирования.

Комплекс PC-3000 Portable может работать в трех режимах: автономном, упрощенном и полнофункциональном. В автономном режиме используется встроенное ПО PC-3000 Portable, в нем доступны функции диагностики и создания посекторной копии данных с накопителей подключенных к портам USB и Port 0. Иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. При использовании управляющего компьютера доступны режимы упрощенный и полнофункциональный. Упрощенный режим содержит необходимый набор автоматических функций для диагностики, извлечения данных и создания иммидж-копий с накопителей подключенных к портам USB и Port 0. Как и в автономном режиме, иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. В упрощенном режиме возможно создание «Дела» и получение всех отчетов о работе с накопителем, что будет полезно специалистам области Форензик. Полнофункциональный режим содержит максимальные возможности по работе с поврежденными накопителями и является аналогом ПО комплексов PC-3000 Express и PC-3000 UDMA, отличия касаются только количества и скоростных характеристик диагностических портов контроллеров. В качестве управляющего компьютера может быть использован настольный ПК или Ноутбук. Подключение контроллера PC-3000 Portable к компьютеру осуществляется через интерфейс USB 3.0, что позволяет использовать данный комплекс, как мобильную станцию для восстановления данных и проводить работы непосредственно у заказчика.

R-Studio это семейство утилит для восстановления файлов. Программа функционирует как на локальных, так и на удаленных компьютерах по сети, даже если разделы дисков были форматированы, повреждены или удалены. Уникальная технология сканирования

IntelligentScan и удобный в установке параметров интерфейс программы дают пользователю абсолютный контроль над процессом восстановления данных.

Для восстановления удаленных файлов с логического диска (найденного раздела):

Дважды щелкните левой кнопкой мыши по логическому диску на панели Диски R-Studio, чтобы перечитать файлы диска.

При попытке перечитать файлы жесткого диска или другого объекта без определенной файловой системы появится сообщение «Дважды щелкните левой кнопкой мыши по логическому диску...». Выберите логический диск объекта или отсканируйте объект.

> Панели R-Studio изменятся и будет показана структура папок/файлов диска.

R-Studio анализирует данные объекта и отображает все файлы, информация о которых была найдена. Если же файлы не найдены, то это означает, что информация о них была удалена. Для более подробной информации о восстановлении таких файлов смотри раздел Восстановление Данных. Дополнительные Операции.

Обратите внимание, что R-Studio показывает только те файлы/папки, которые соответствуют заданной маске файлов.

На панели Журнал будет показано, сколько файлов и папок имеются в данном объекте и их размер. В фильтре журнала вы можете задать, какие типы событий будут отображаться в панели журнала.

Обратите внимание: Метафайлы – это внутренние системные файлы (данные файловой системы), невидимые пользователем, которые R-Studio показывает, как файлы. Такие файлы не содержат данные пользователя и используются только при восстановлении файловой системы диска.

При появлении сообщения Too many files... вы можете временно прекратить вывод файлов и просмотреть найденные файлы. Затем вы можете продолжить вывод файлов. Вы также можете продолжить вывод файлов без просмотра. R-Studio сохранит информацию о внутренней структуре файла.

Для полного анализа структуры данных объекта его необходимо отсканировать. Любой объект на панели Устройство/Диск может быть отсканирован. Кроме того, вы можете отсканировать часть объекта, создав регион. В разделе Регионы рассматривается, как создавать и работать с регионами. Сканирование также значительно повышает оценки шансов успешного восстановления файлов.

Вы можете выбрать область и другие параметры сканирования. Результаты сканирования могут быть сохранены в файл, который затем может быть открыт.

При необходимости можно сохранить результаты сканирования на удаленном компьютере.

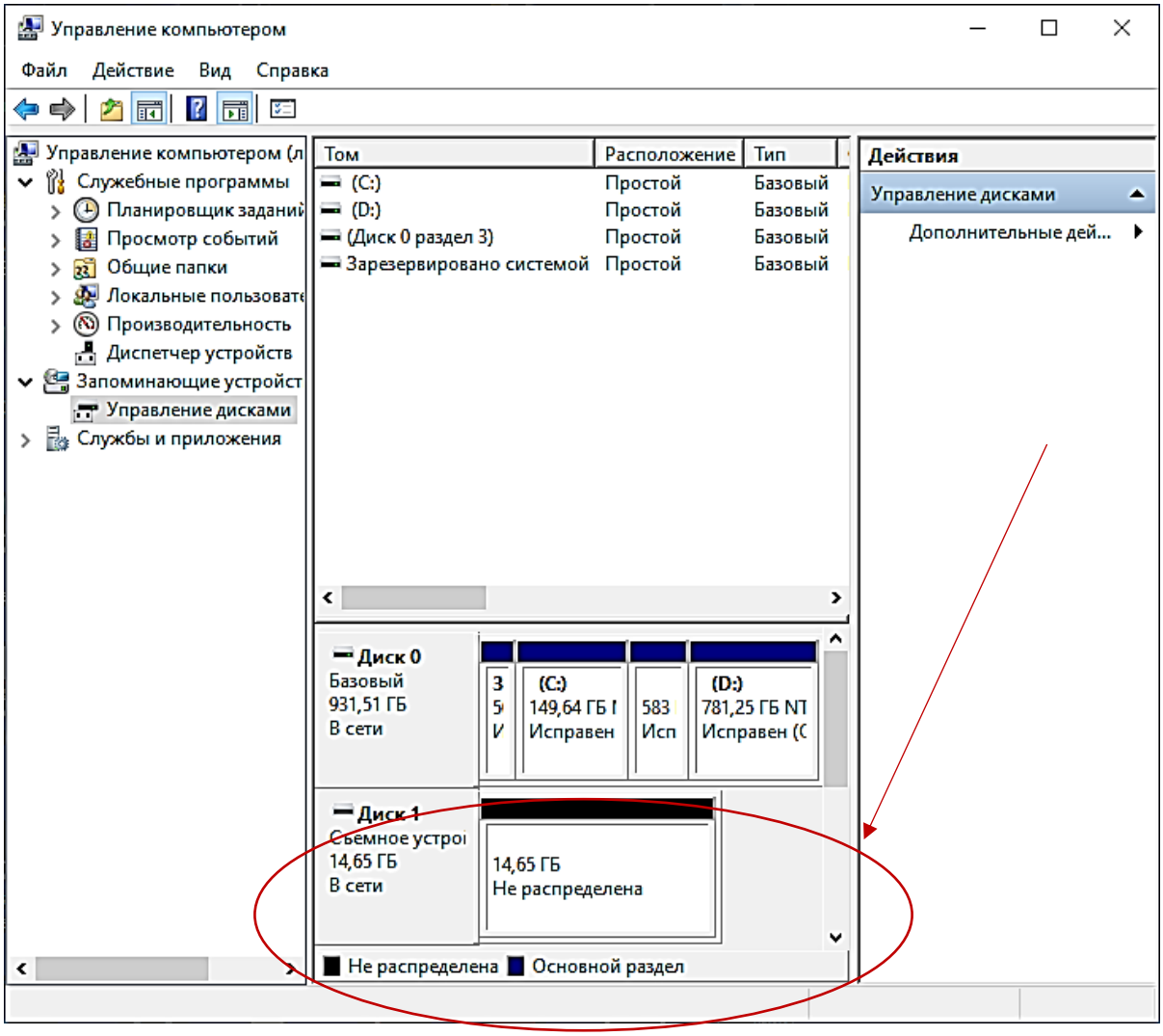
Внимание: Сканирования больших областей может занять очень много времени!

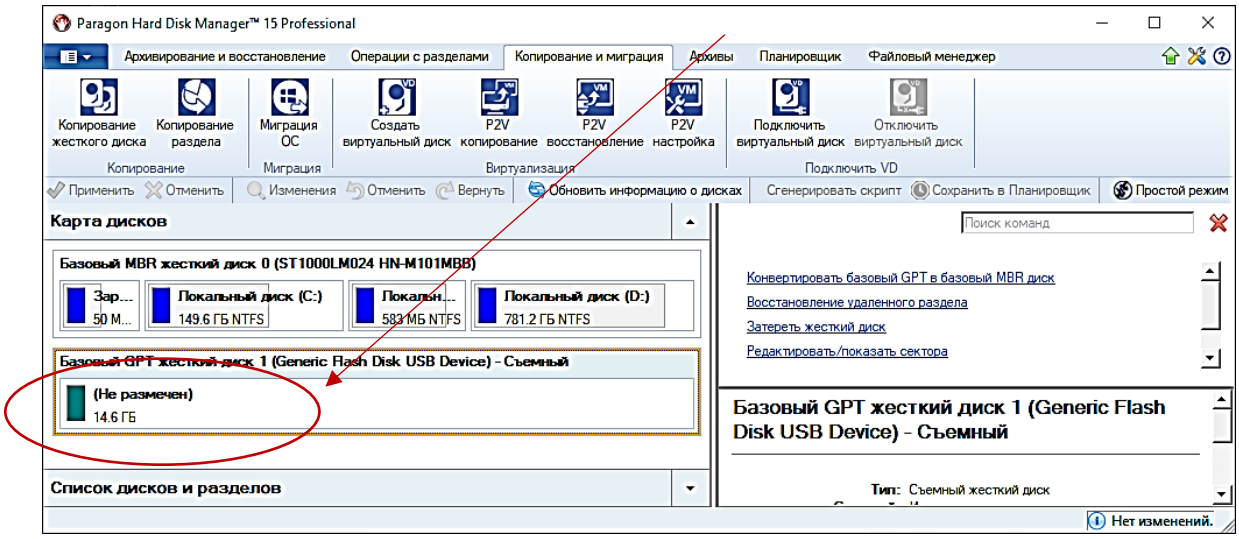
НИКОГДА НЕ ПЫТАЙТЕСЬ СОХРАНИТЬ ОТСКАНИРОВАННОЕ НА СКАНИРУЕМЫЙ ОБЪЕКТ!!!

Это может стать причиной полной утраты данных.

Порядок выполнения работы

1. Получить у преподавателя накопитель информации с неизвестной файловой системой.
2. Убедиться, что на накопителе отсутствует файловая система. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.





2.1. В случае, если на накопителе имеется файловая система – удалить ее. Оставить диск неразмеченным.

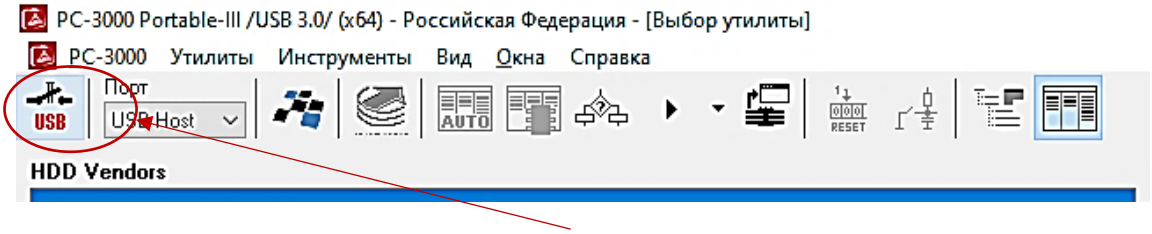
3. Подключить ПАК «PC-3000» к лабораторному компьютеру.

3.1. Продемонстрировать правильно подключенный ПАК «PC-3000» преподавателю ПЕРЕД ВКЛЮЧЕНИЕМ!!!

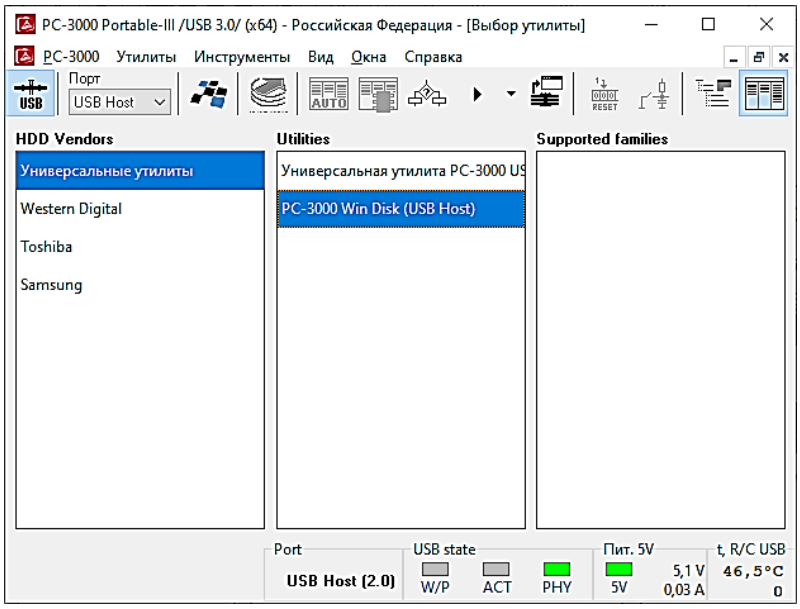
4. Запустить программу «PC-3000 Portable-III». Отметить галочкой порт USB.

5. Подключить исследуемый флеш-накопитель к ПАК «PC-3000» через интерфейсный разъем USB в режиме монтирования.

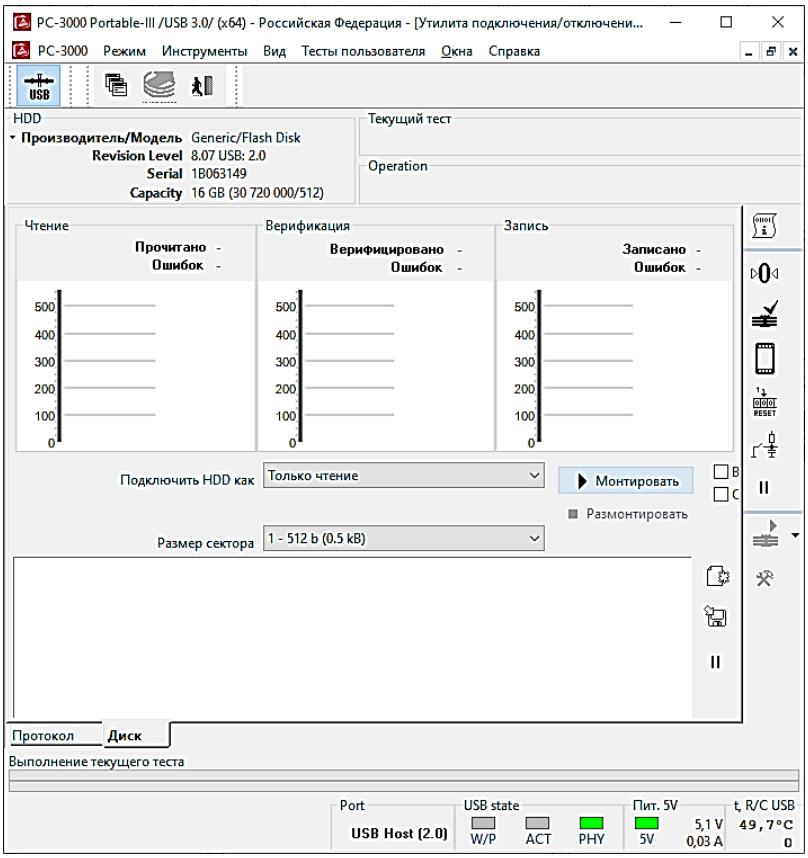
6. Включить питание разъема USB.



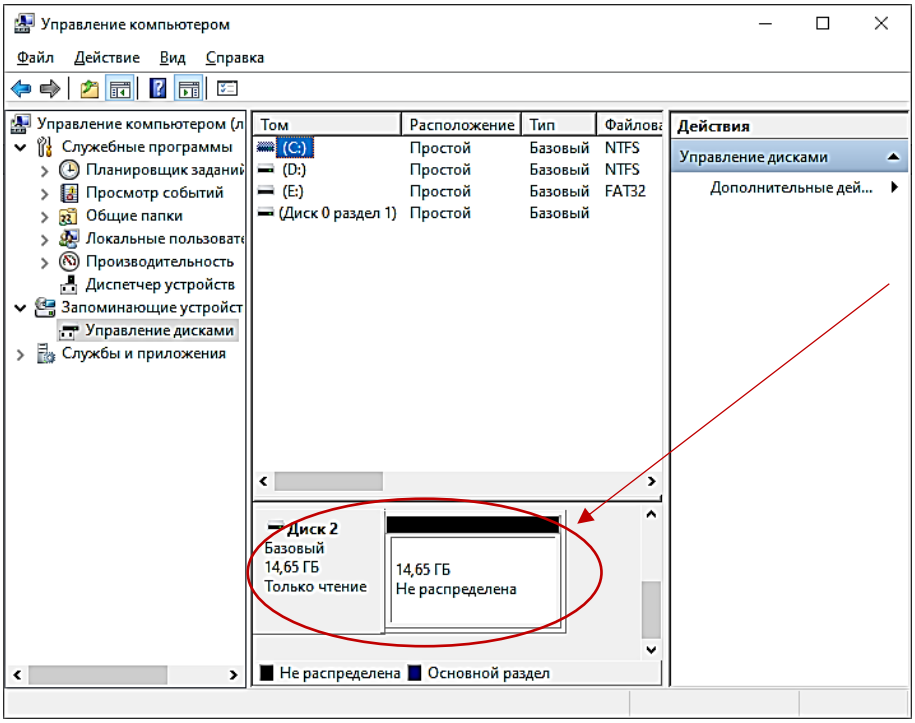
7. Запустить утилиту «PC-3000 Win Disk».

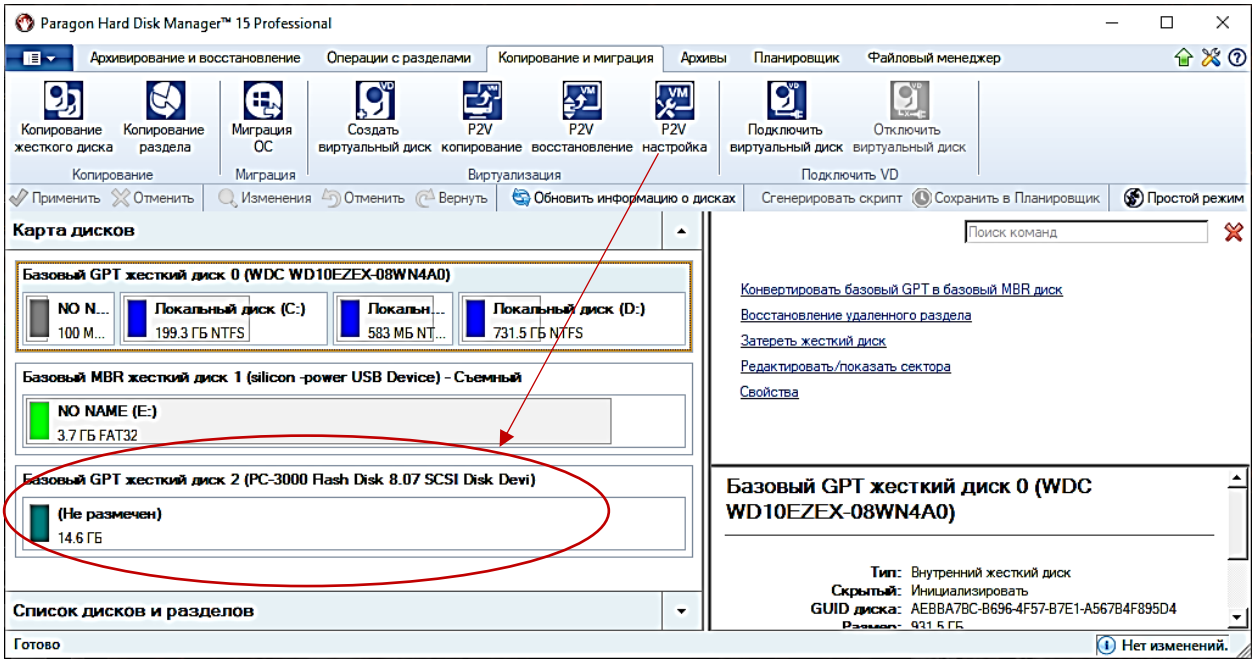


8. Монтировать исследуемый накопитель в режиме «Только чтение».



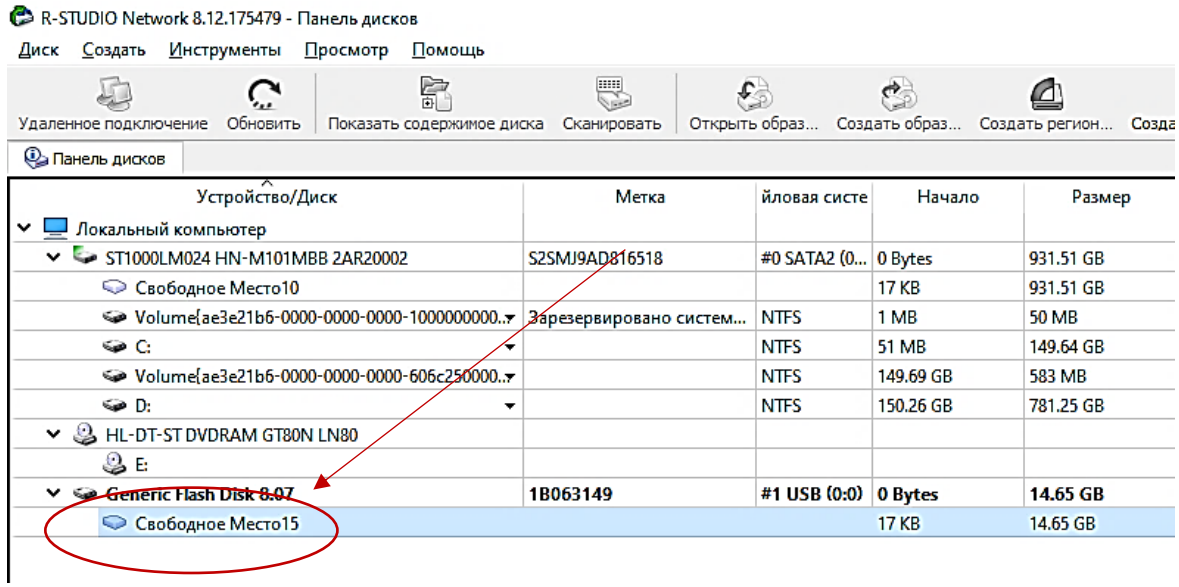
8. Убедиться, что исследуемый накопитель монтирован к ОС лабораторного компьютера. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.





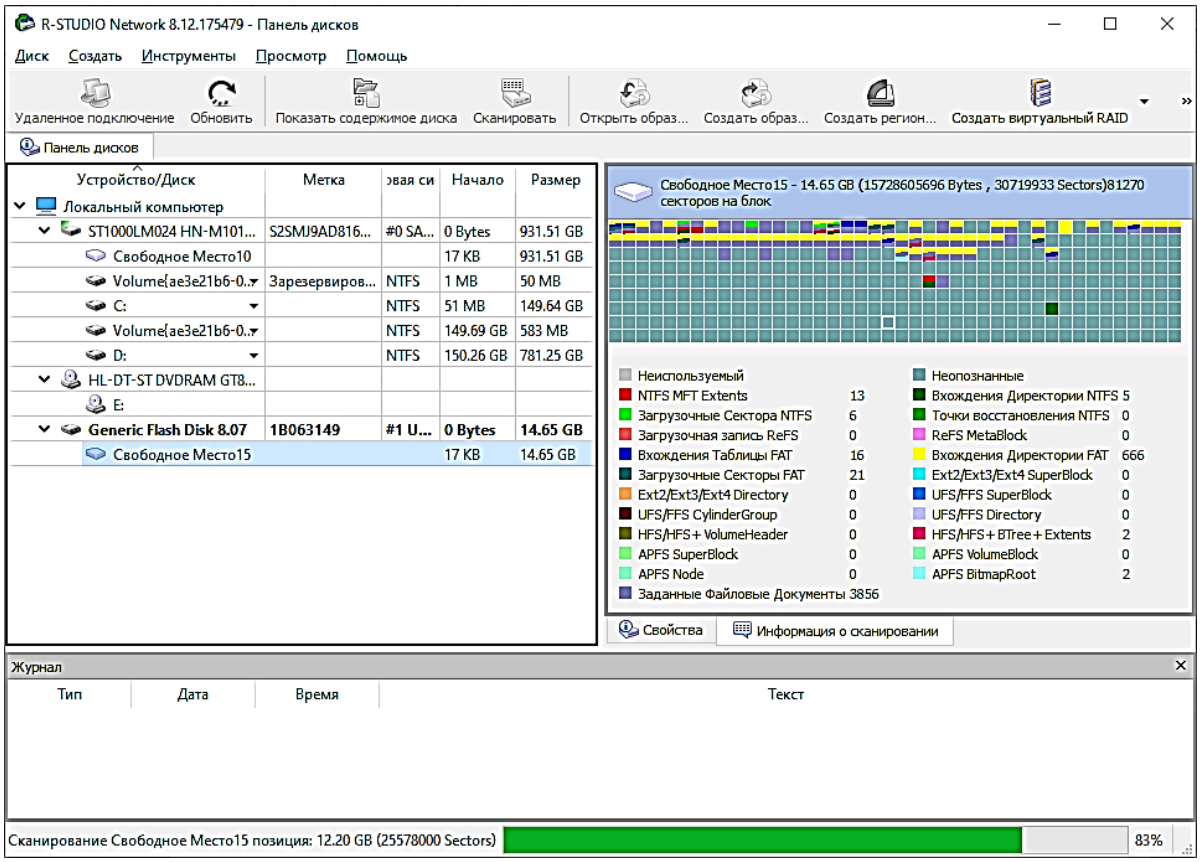
9. Запустить ПО R-Studio.

9.1. Обнаружить в программе исследуемый флеш-накопитель с отсутствующей файловой системой.

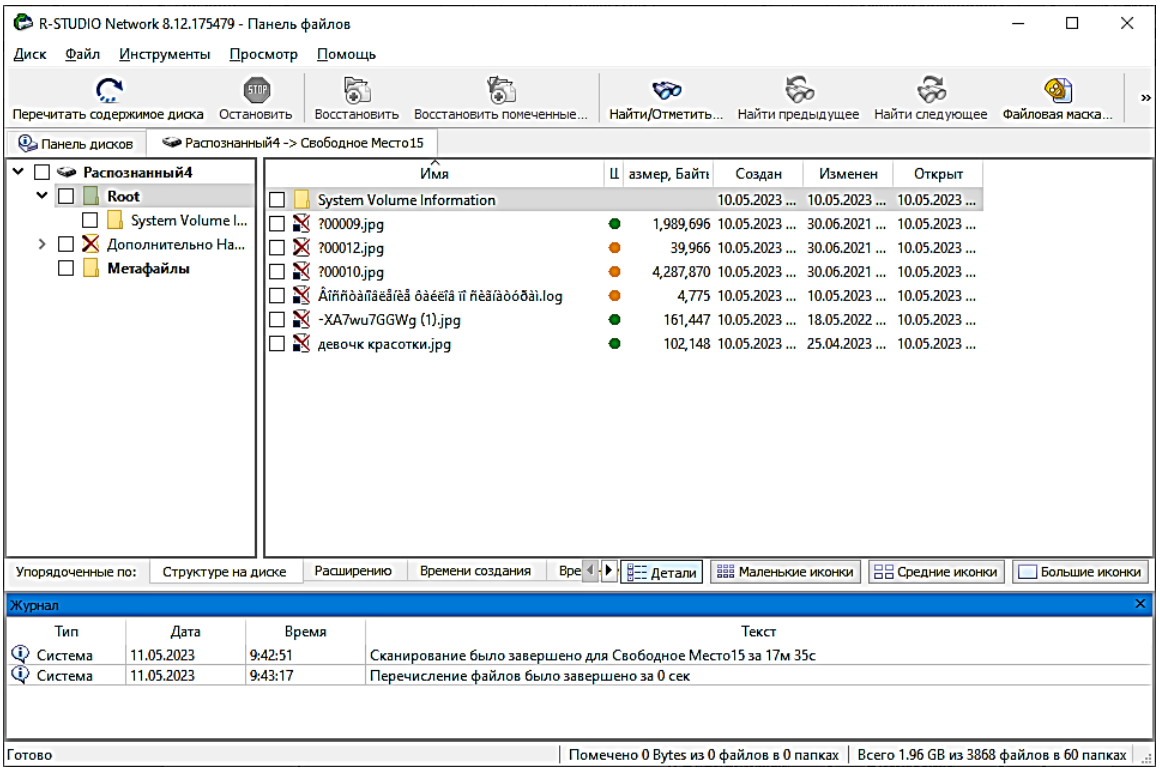


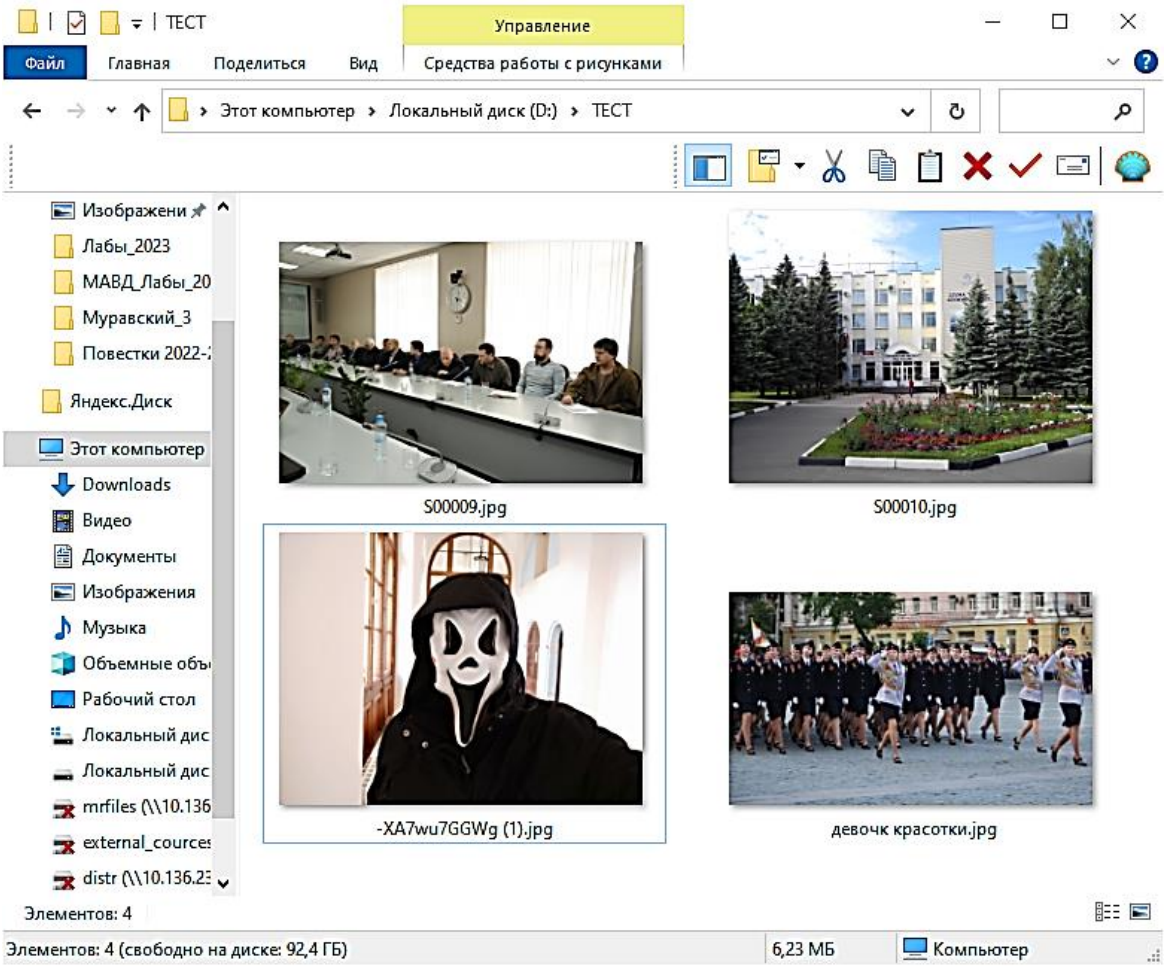
10. Запустить сканирование. Для этого кликнуть ПКМ на выбранный флеш-накопитель в программе R-Studio и выбрать пункт «Сканировать».

10.1. Запуститься процесс сканирования.



11. Проанализировать результат сканирования. Восстановить графические файлы. Сделать скриншот.





12. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Опишите алгоритм восстановления графических файлов с помощью ПО R-Studio.
3. Что такое черновое восстановление (восстановление по сигнатурам)?
4. Как обнаружить удаленные графические файлы с помощью ПО R-Studio?
5. Для чего предназначено ПО R-Studio?
6. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
7. Опишите алгоритм подключения USB-накопителя с помощью ПАК «PC-3000» в режиме монтирования.
8. Какие типы файлов вы знаете?
9. Как обнаружить удаленные графические файлы с помощью ПАК «PC-3000»?
10. Для чего предназначен ПАК «PC-3000»?
11. Через какой интерфейс ПАК «PC-3000» подключается к лабораторному компьютеру?
12. Какие интерфейсные разъемы для подключения исследуемых объектов имеет ПАК «PC-3000»?
13. Как заблокировать запись на исследуемом объекте, подключенном через ПАК «PC-3000» в режиме монтирования?

ЛАБОРАТОРНАЯ РАБОТА № 22

ВОССТАНОВЛЕНИЕ ТЕКСТОВОЙ ИНФОРМАЦИИ ИЗ НЕИЗВЕСТНОЙ ФАЙЛОВОЙ СИСТЕМЫ ФЛЕШ-НАКОПИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ КОМБИНИРОВАННОГО СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков работы с ПАК PC-3000 и ПО R-Studio.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное оборудование.

Подготовка к выполнению работы

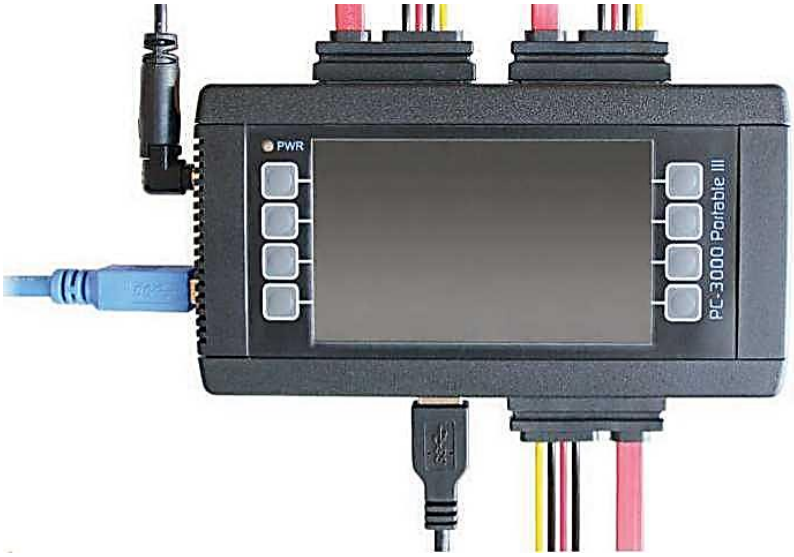
1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

PC-3000 Portable – это портативный программно-аппаратный комплекс, предназначенный для диагностики, ремонта и восстановления пользовательских данных с накопителей HDD/SSD1, имеющих физические неисправности носителей и логические повреждения файловых систем. К физическим неисправностям HDD относятся: повреждения платы электроники, магнитных дисков, головок чтения-записи, предусилителя, микропрограммы, служебной информации. К физическим неисправностям SDD относятся: повреждения платы электроники, контроллера, деградация ячеек массива NAND-Flash памяти, повреждение микропрограммы, служебной информации и др. К логическим неисправностям относятся: повреждения дисковых структур, структур файловых систем и комбинации этих проблем. Дополнительно, PC-3000 Portable позволяет создавать имидж-копии данных с накопителей HDD, SSD, USB-Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны.

Диагностируемые HDD/SSD/Flash накопители, подлежащие восстановлению данных, подключаются непосредственно к контроллеру PC

3000 Portable – к его портам SOURCE - USB и Port0. К портам TARGET - Port1 и Port2 подключаются HDD/SSD накопители для создания имидж-копии данных. В некоторых режимах работы порты Port1 и Port2 также могут использоваться для подключения диагностируемых/восстанавливаемых накопителей, увеличивая тем самым общее число одновременно восстанавливаемых HDD/SSD до трех.



Порты SOURCE - USB и Port 0 допускают блокировку от записи, для ее включения необходимо воспользоваться переключателем Write Protection. При включенной блокировке должен гореть жетлый светодиод.

Контроллер PC-3000 Portable подключается к внешнему источнику питания -19В, и в случае работы через управляющий компьютер подключается к нему через интерфейс USB 3.0.

В существующей реализации контроллер PC-3000 Portable допускает подключение накопителей HDD/SSD с интерфейсом SATA-III (совместим с SATA-I/II, SSD M.2 NVMe PCIe) и накопителей с USB интерфесом, соответствующих классификации Mass Storage Device – внешние HDD/ SSD USB 2.0/3.0 и USB-Flash накопители. Подключение накопителей с интерфейсом PATA (IDE) возможно через специальный адаптер PATA, который поставляется опционально.

Комплекс поддерживает работу с моделями накопителей от 40 [б до 6 Тб. За это время плотность записи информации увеличилась в сотни раз, и такой разрыв не мог не отразиться на различии архитектурных решений накопителей, различиях в подходах, методиках и сложностях восстановления информации. В результате многие методики восстановления данных, хорошо работающие на HDD емкостью 40-100 [б, оказываются неприменимы для HDD - 1-6 Тб. В данном комплексе собраны наиболее универсальные методы, работающие для всех поколений HDD. При этом для работы с PC-3000 Portable не потребуется глубокое знание

принципов работы накопителей, следует только придерживаться методик, описанных в документации к комплексу.

Операционная система Windows, работая с поврежденным носителем информации, применяет доступные ей программные средства восстановления данных. Часто это лишь ухудшает ситуацию с повреждениями данных на неисправных накопителях. При использовании комплекса PC-3000 Portable доступ ОС к неисправному HDD исключается. Но при необходимости можно использовать программный драйвер монтирования дисков, который позволяет «смонтировать» диагностируемый накопитель, подключенный к портам PC-3000 Portable как дисковое устройство ОС.

Для целого ряда накопителей HDD/SSD имеется возможность использовать технологический режим, т.е., режим, который используется на заводе-изготовителе в процессе производства. Это дает расширенные возможности для получения доступа к данным пользователя и их копирования.

Комплекс PC-3000 Portable может работать в трех режимах: автономном, упрощенном и полнофункциональном. В автономном режиме используется встроенное ПО PC-3000 Portable, в нем доступны функции диагностики и создания посекторной копии данных с накопителей подключенных к портам USB и Port 0. Иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. При использовании управляющего компьютера доступны режимы упрощенный и полнофункциональный. Упрощенный режим содержит необходимый набор автоматических функций для диагностики, извлечения данных и создания иммидж-копий с накопителей подключенных к портам USB и Port 0. Как и в автономном режиме, иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. В упрощенном режиме возможно создание «Дела» и получение всех отчетов о работе с накопителем, что будет полезно специалистам области Форензик. Полнофункциональный режим содержит максимальные возможности по работе с поврежденными накопителями и является аналогом ПО комплексов PC-3000 Express и PC-3000 UDMA, отличия касаются только количества и скоростных характеристик диагностических портов контроллеров. В качестве управляющего компьютера может быть использован настольный ПК или Ноутбук. Подключение контроллера PC-3000 Portable к компьютеру осуществляется через интерфейс USB 3.0, что позволяет использовать данный комплекс, как мобильную станцию для восстановления данных и проводить работы непосредственно у заказчика.

R-Studio это семейство утилит для восстановления файлов. Программа функционирует как на локальных, так и на удаленных компьютерах по сети, даже если разделы дисков были форматированы, повреждены или удалены. Уникальная технология сканирования

IntelligentScan и удобный в установке параметров интерфейс программы дают пользователю абсолютный контроль над процессом восстановления данных.

Для восстановления удаленных файлов с логического диска (найденного раздела):

Дважды щелкните левой кнопкой мыши по логическому диску на панели Диски R-Studio, чтобы перечитать файлы диска.

При попытке перечитать файлы жесткого диска или другого объекта без определенной файловой системы появится сообщение «Дважды щелкните левой кнопкой мыши по логическому диску...». Выберите логический диск объекта или отсканируйте объект.

> Панели R-Studio изменятся и будет показана структура папок/файлов диска

R-Studio анализирует данные объекта и отображает все файлы, информация о которых была найдена. Если же файлы не найдены, то это означает, что информация о них была удалена. Для более подробной информации о восстановлении таких файлов смотри раздел Восстановление Данных. Дополнительные Операции.

Обратите внимание, что R-Studio показывает только те файлы/папки, которые соответствуют заданной маске файлов.

На панели Журнал будет показано, сколько файлов и папок имеются в данном объекте и их размер. В фильтре журнала вы можете задать, какие типы событий будут отображаться в панели журнала.

Обратите внимание: Метафайлы – это внутренние системные файлы (данные файловой системы), невидимые пользователем, которые R-Studio показывает, как файлы. Такие файлы не содержат данные пользователя и используются только при восстановлении файловой системы диска.

При появлении сообщения Too many files... вы можете временно прекратить вывод файлов и просмотреть найденные файлы. Затем вы можете продолжить вывод файлов. Вы также можете продолжить вывод файлов без просмотра. R-Studio сохранит информацию о внутренней структуре файла.

Для полного анализа структуры данных объекта его необходимо отсканировать. Любой объект на панели Устройство/Диск может быть отсканирован. Кроме того, вы можете отсканировать часть объекта, создав регион. В разделе Регионы рассматривается, как создавать и работать с регионами. Сканирование также значительно повышает оценки шансов успешного восстановления файлов.

Вы можете выбрать область и другие параметры сканирования. Результаты сканирования могут быть сохранены в файл, который затем может быть открыт.

При необходимости можно сохранить результаты сканирования на удаленном компьютере.

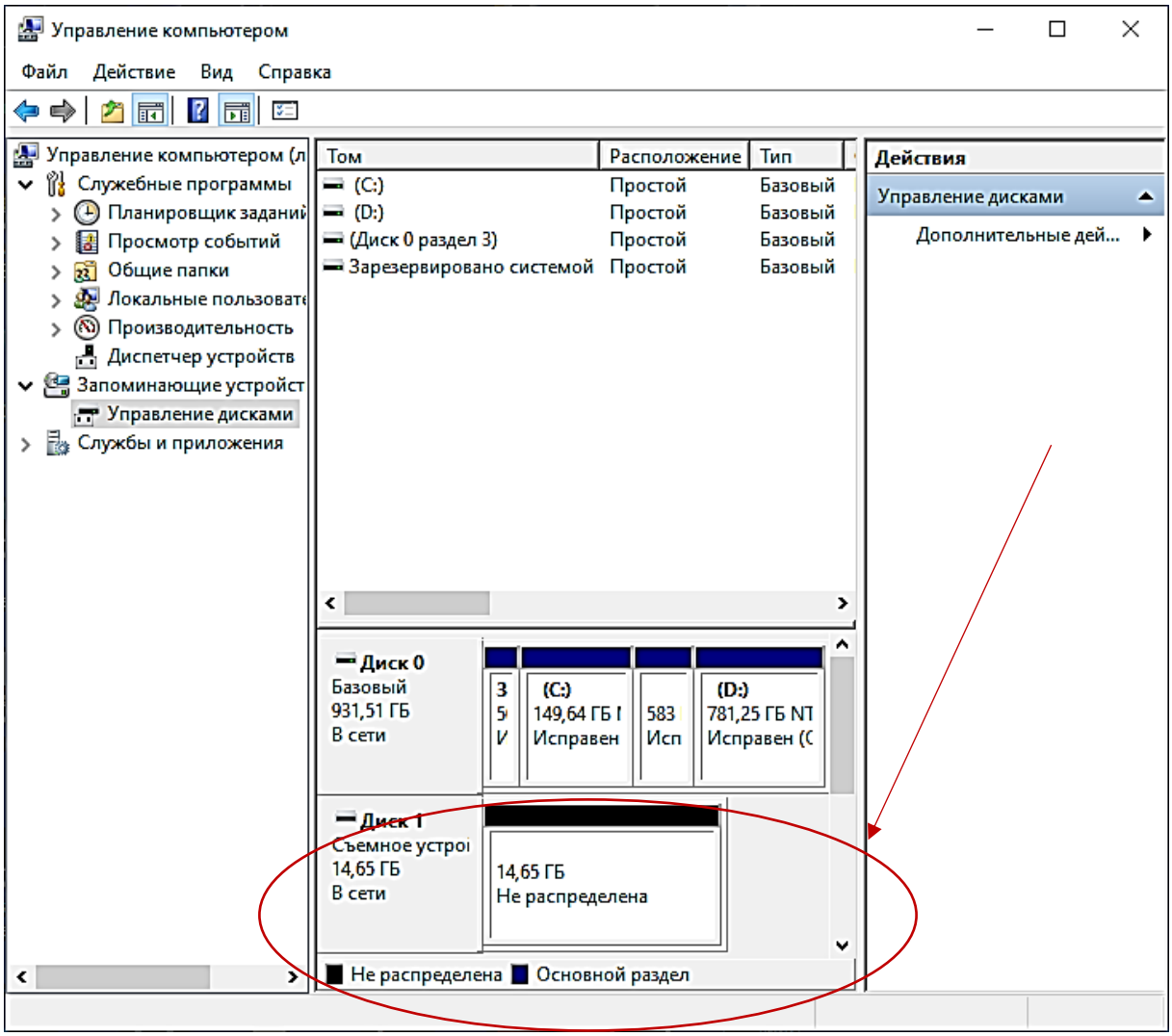
Внимание: Сканирования больших областей может занять очень много времени!

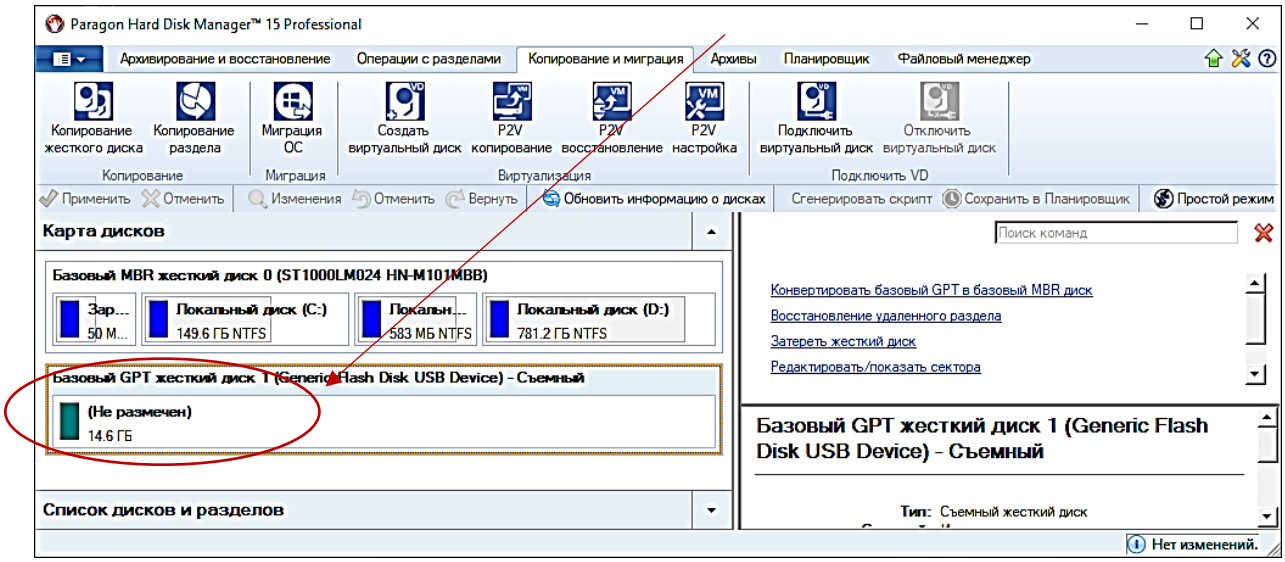
НИКОГДА НЕ ПЫТАЙТЕСЬ СОХРАНИТЬ ОТСКАНИРОВАННОЕ НА СКАНИРУЕМЫЙ ОБЪЕКТ!!!

Это может стать причиной полной утраты данных.

Порядок выполнения работы

1. Получить у преподавателя накопитель информации с неизвестной файловой системой.
2. Убедиться, что на накопителе отсутствует файловая система. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.



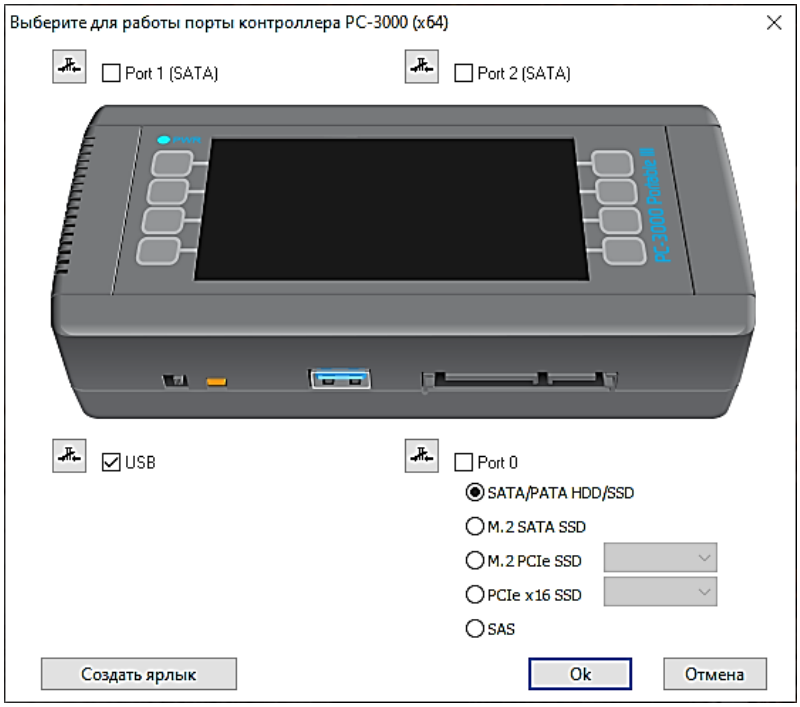


2.1. В случае, если на накопителе имеется файловая система – удалить ее. Оставить диск неразмеченным.

3. Подключить ПАК «PC-3000» к лабораторному компьютеру.

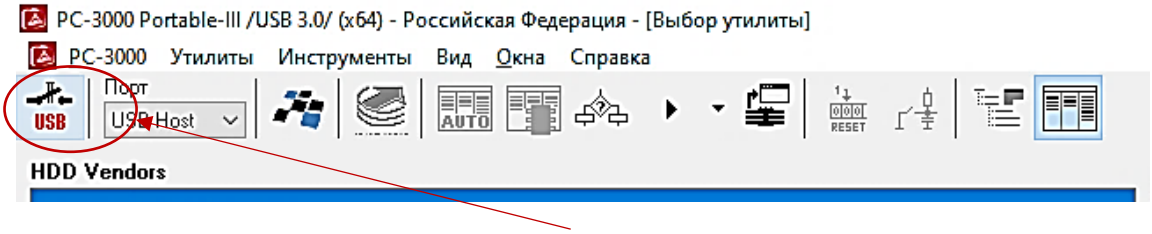
3.1. Продемонстрировать правильно подключенный ПАК «PC-3000» преподавателю ПЕРЕД ВКЛЮЧЕНИЕМ!!!

4. Запустить программу «PC-3000 Portable-III». Отметить галочкой порт USB.

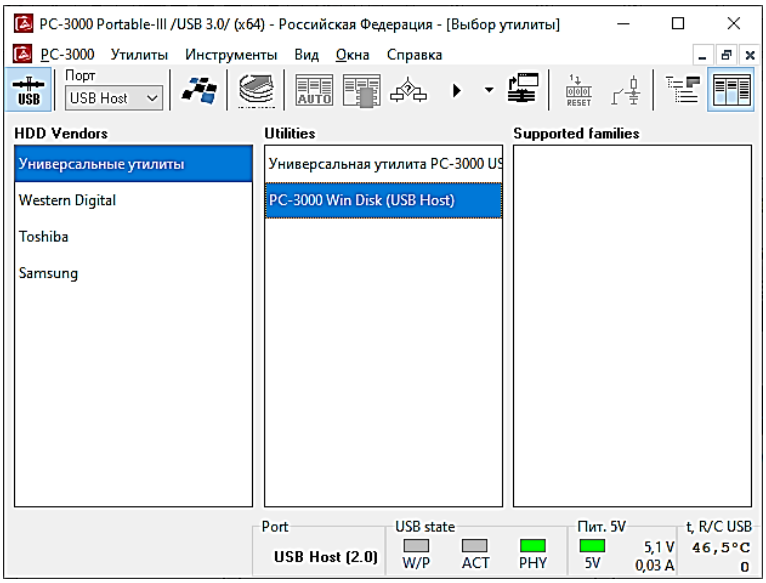


5. Подключить исследуемый флеш-накопитель к ПАК «PC-3000» через интерфейсный разъем USB в режиме монтирования.

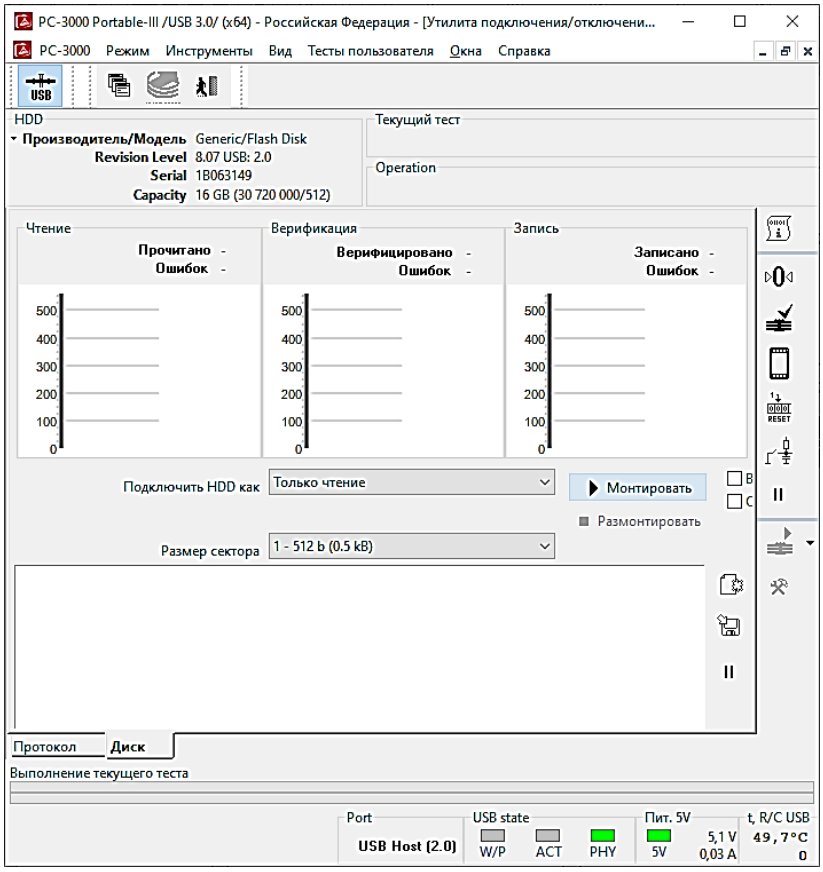
6. Включить питание разъема USB.



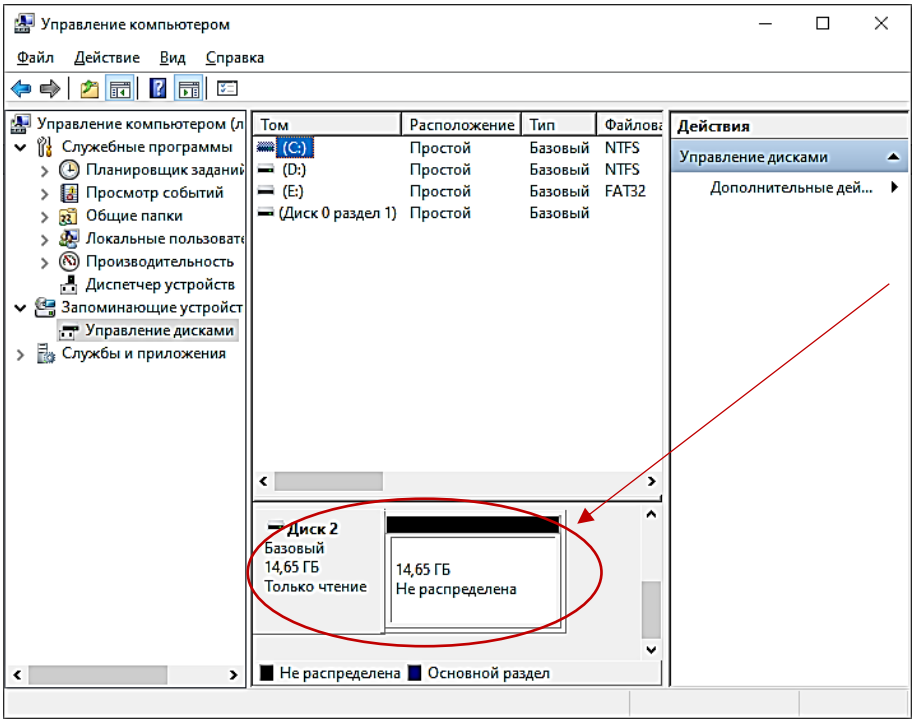
7. Запустить утилиту «PC-3000 Win Disk».

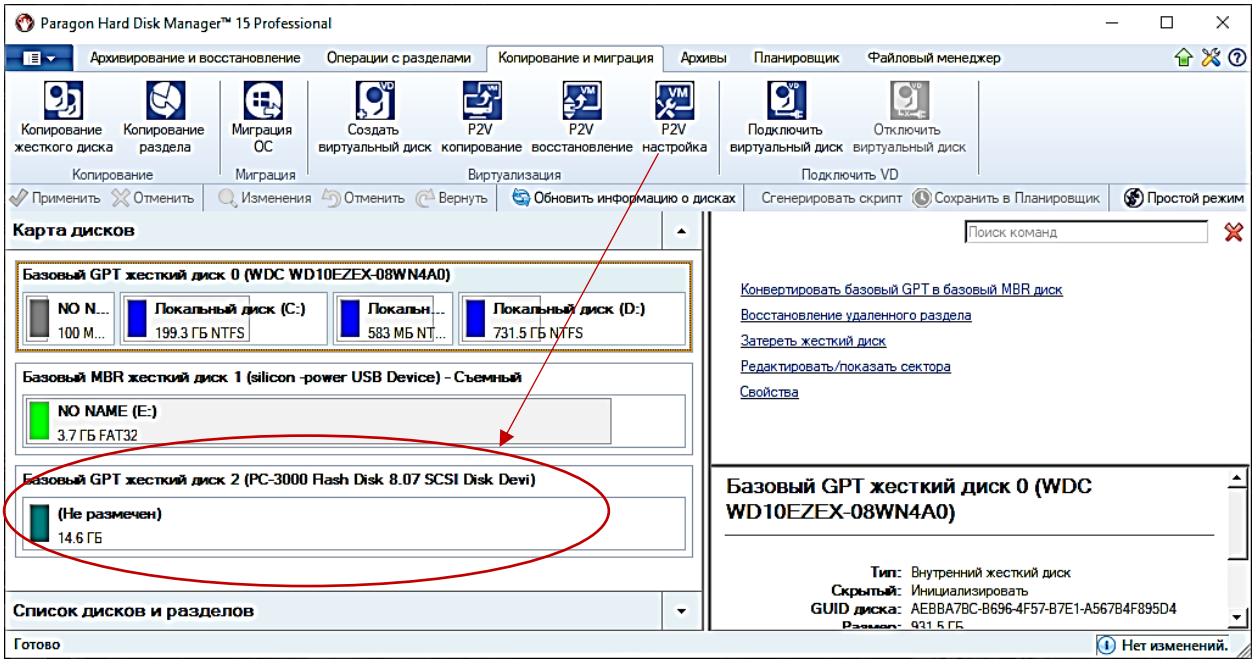


8. Монтировать исследуемый накопитель в режиме «Только чтение».



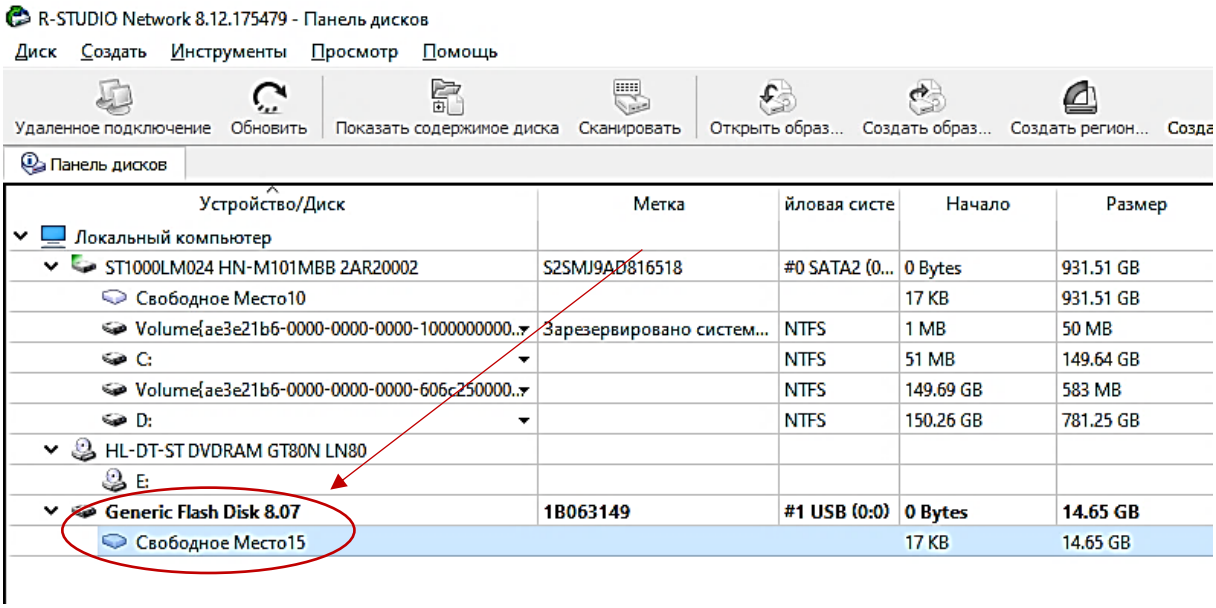
9. Убедиться, что исследуемый накопитель монтирован к ОС лабораторного компьютера. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.





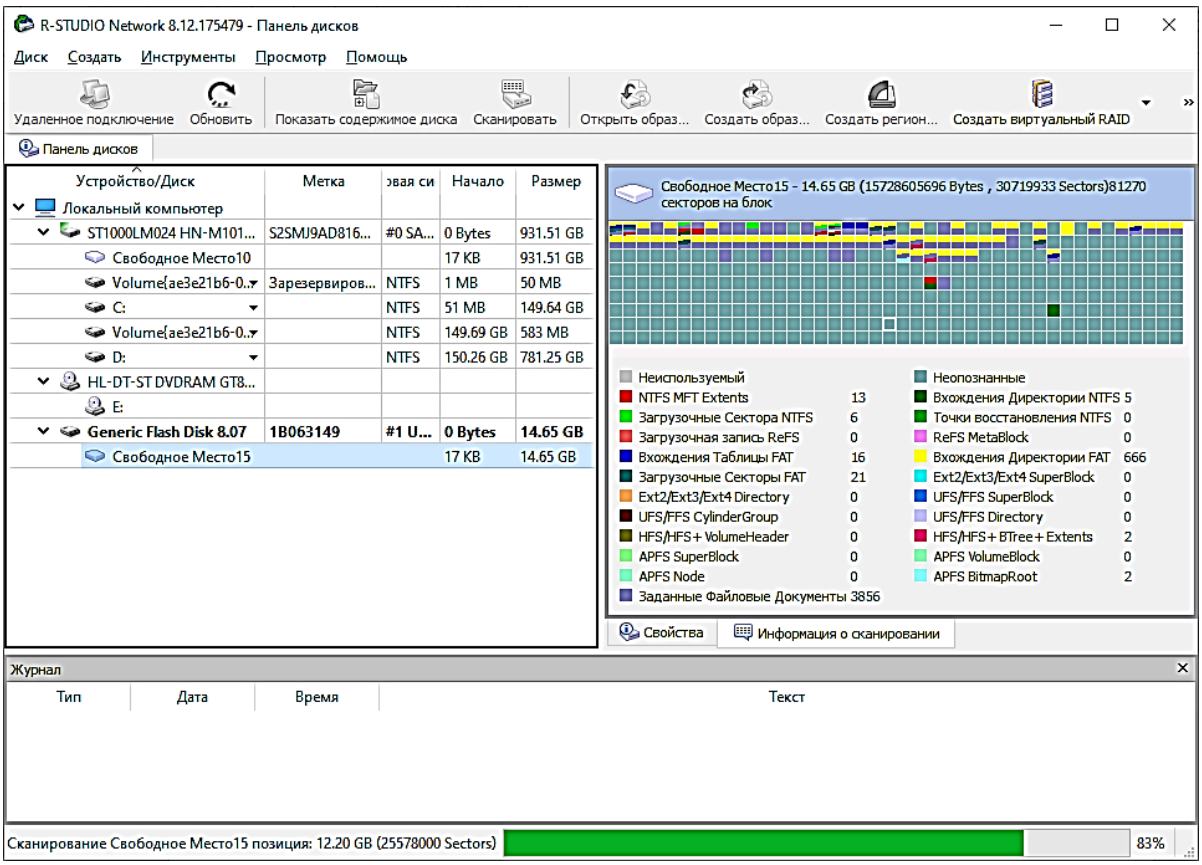
10. Запустить ПО R-Studio.

10.1. Обнаружить в программе исследуемый флеш-накопитель с отсутствующей файловой системой.

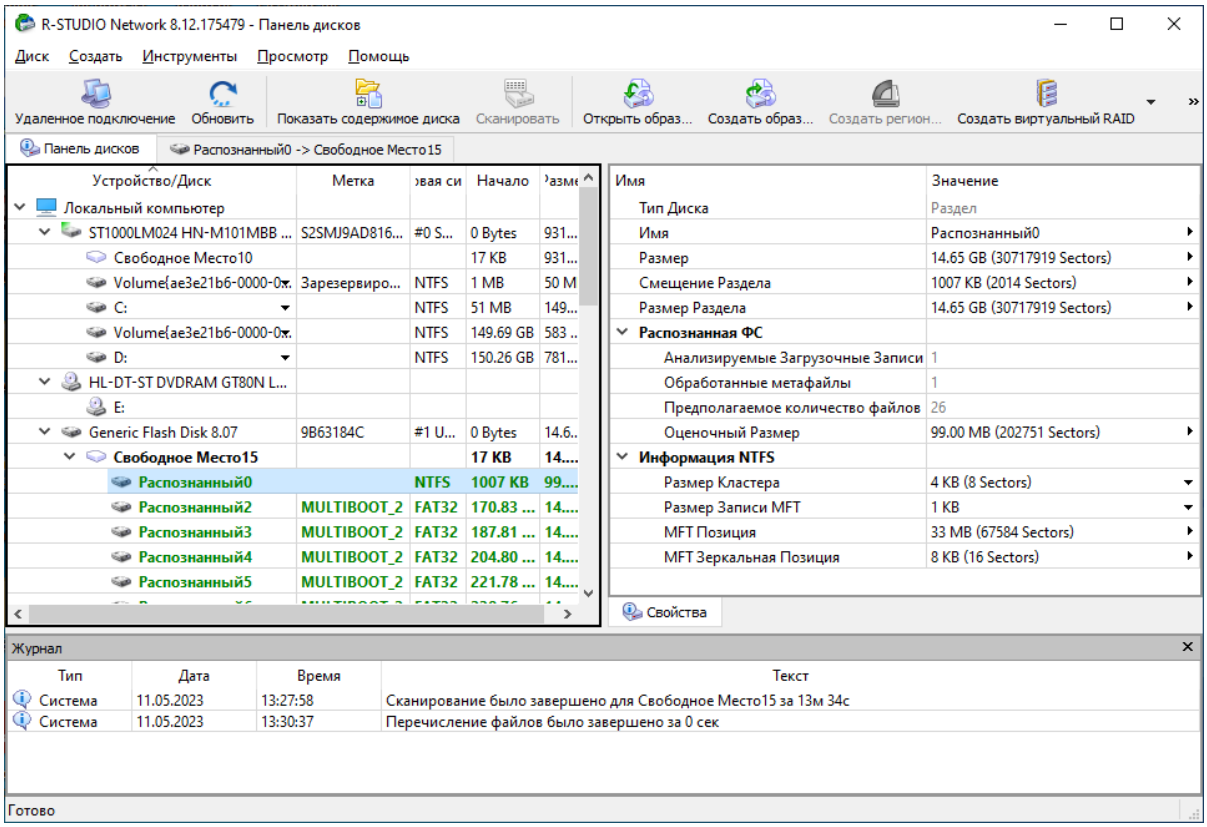


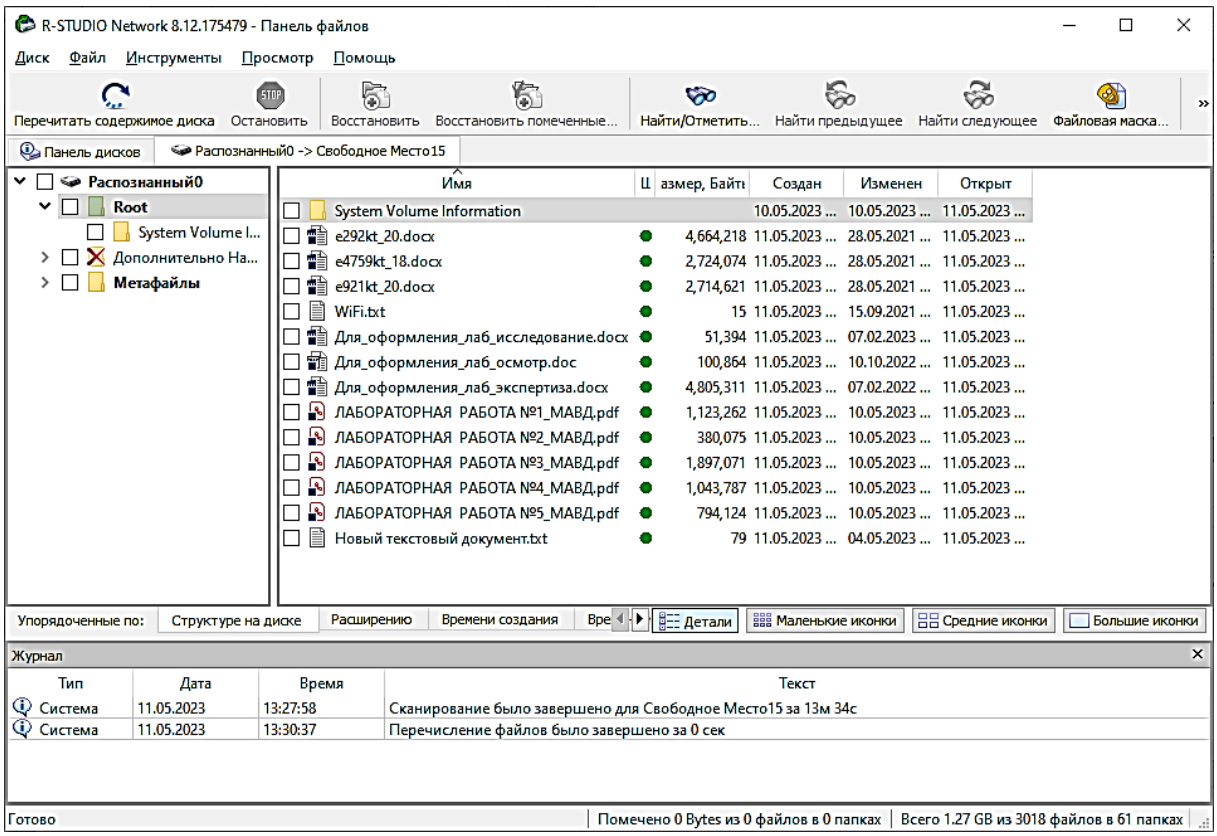
11. Запустить сканирование. Для этого кликнуть ПКМ на выбранный флеш-накопитель в программе R-Studio и выбрать пункт «Сканировать».

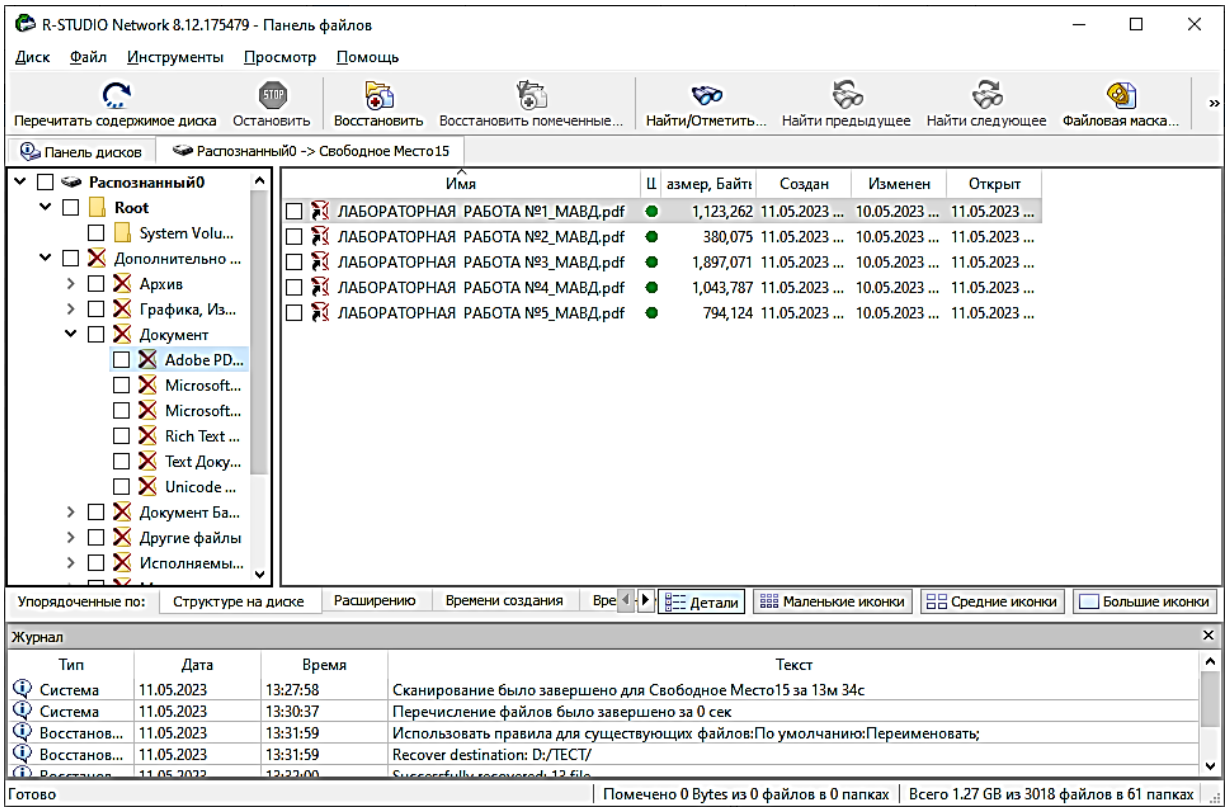
11.1. Запуститься процесс сканирования.

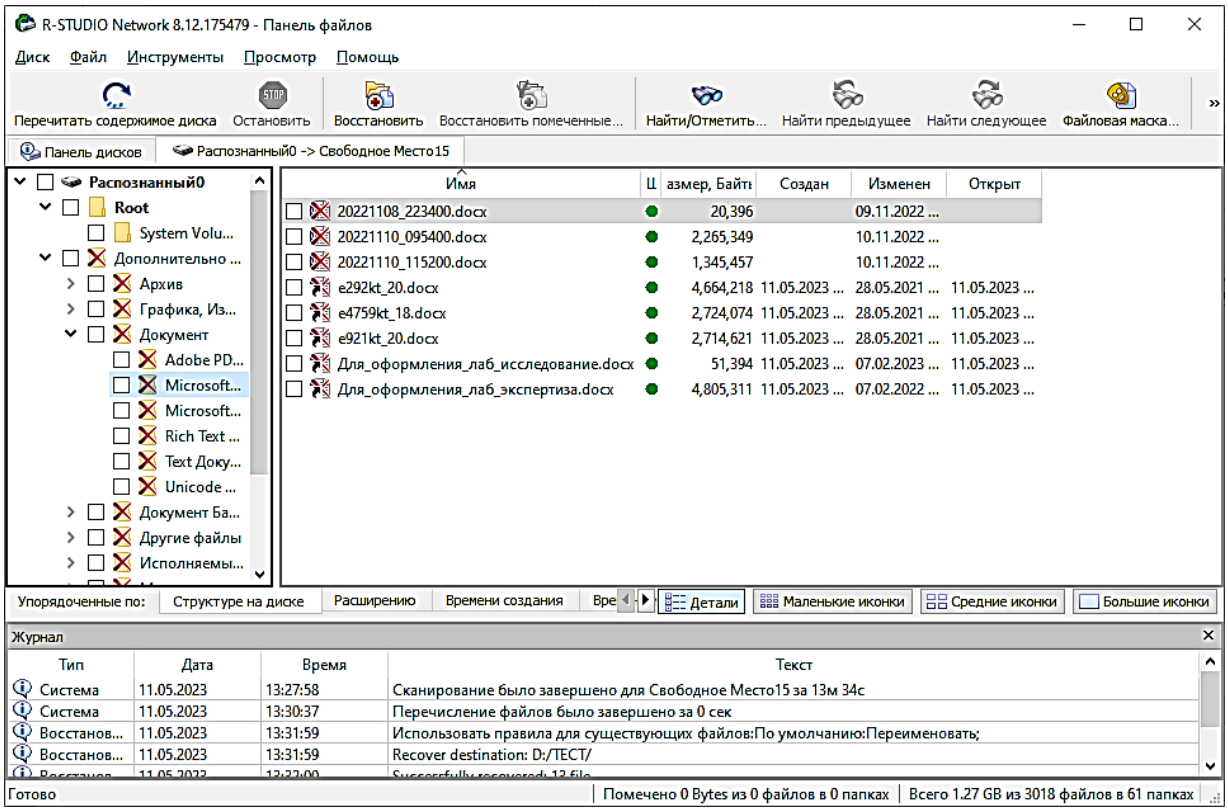


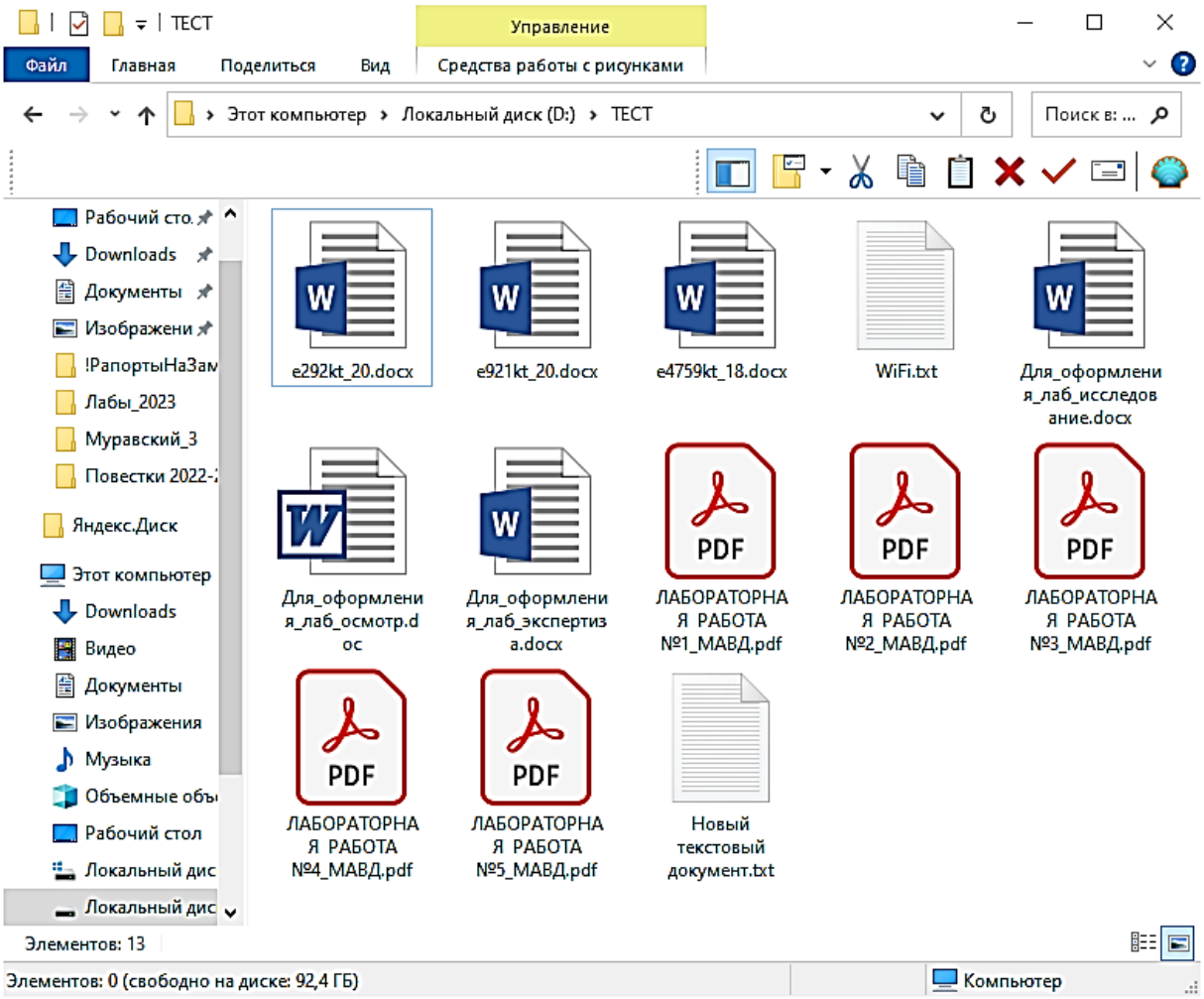
12. Проанализировать результат сканирования. Восстановить графические файлы. Сделать скриншот.


R-STUDIO Network 8.12.175479 - Панель дисков
Диск Создать Инструменты Просмотр Помощь
Удаленное подключение Обновить Показать содержимое диска Сканировать Открыть образ... Создать образ... Создать регион... Создать виртуальный RAID
Панель дисков
Распознанный0 -> Свободное Место15
Устройство/Диск Метка Начало
Локальный компьютер
ST1000LM024 HN-M101MBB ... S2SMJ9AD816... #0 S... 0 Bytes
Свободное Место10 17 KB
Volume{ae3e21b6-0000-0... Зарезервиро... NTFS 1 MB
C: NTFS 51 MB
Volume{ae3e21b6-0000-0... NTFS 149.69 GB
D: NTFS 150.26 GB
HL-DT-ST DVDRAM GT80N L...
E:
Generic Flash Disk 8.07 9B63184C #1 U... 0 Bytes
Свободное Место15 17 KB
Распознанный0 NTFS 1007 KB
Распознанный2 MULTIBOOT_2 FAT32 170.83 ...
Распознанный3 MULTIBOOT_2 FAT32 187.81 ...
Распознанный4 MULTIBOOT_2 FAT32 204.80 ...
Распознанный5 MULTIBOOT_2 FAT32 221.78 ...
Имя Значение
Тип Диска Раздел
Имя Распознанный0
Размер 14.65 GB (30717919 Sectors)
Смещение Раздела 1007 KB (2014 Sectors)
Размер Раздела 14.65 GB (30717919 Sectors)
Распознанная ФС
Анализируемые Загрузочные Записи 1
Обработанные метафайлы 1
Предполагаемое количество файлов 26
Оценочный Размер 99.00 MB (202751 Sectors)
Информация NTFS
Размер Кластера 4 KB (8 Sectors)
Размер Записи MFT 1 KB
MFT Позиция 33 MB (67584 Sectors)
MFT Зеркальная Позиция 8 KB (16 Sectors)
Свойства
Журнал
Тип Дата Время Текст
Система 11.05.2023 13:27:58 Сканирование было завершено для Свободное Место15 за 13м 34с
Система 11.05.2023 13:30:37 Перечисление файлов было завершено за 0 сек
Готово


R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска Остановить Восстановить Восстановить помеченные... Найти/Отметить... Найти предыдущее Найти следующее Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volume I...
Дополнительно На...
Метафайлы
Имя Размер, Байт Создан Изменен Открыт
System Volume Information 10.05.2023 ... 10.05.2023 ... 11.05.2023 ...
e292kt_20.docx 4,664,218 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
e4759kt_18.docx 2,724,074 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
e921kt_20.docx 2,714,621 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
WiFi.txt 15 11.05.2023 ... 15.09.2021 ... 11.05.2023 ...
Для_оформления_лаб_исследование.docx 51,394 11.05.2023 ... 07.02.2023 ... 11.05.2023 ...
Для_оформления_лаб_осмотр.doc 100,864 11.05.2023 ... 10.10.2022 ... 11.05.2023 ...
Для_оформления_лаб_экспертиза.docx 4,805,311 11.05.2023 ... 07.02.2022 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №1_МАВД.pdf 1,123,262 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №2_МАВД.pdf 380,075 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №3_МАВД.pdf 1,897,071 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №4_МАВД.pdf 1,043,787 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №5_МАВД.pdf 794,124 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
Новый текстовый документ.txt 79 11.05.2023 ... 04.05.2023 ... 11.05.2023 ...
Упорядоченные по: Структуре на диске Расширению Времени создания Детали Маленькие иконки Средние иконки Большие иконки
Журнал
Тип Дата Время Текст
Система 11.05.2023 13:27:58 Сканирование было завершено для Свободное Место15 за 13м 34с
Система 11.05.2023 13:30:37 Перечисление файлов было завершено за 0 сек
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 1.27 GB из 3018 файлов в 61 папках


R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска
Остановить
Восстановить
Восстановить помеченные...
Найти/Отметить...
Найти предыдущее
Найти следующее
Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volu...
Дополнительно ...
Архив
Графика, Из...
Документ
Adobe PD...
Microsoft...
Microsoft...
Rich Text ...
Text Доку...
Unicode ...
Документ Ба...
Другие файлы
Исполняемы...
Имя
Ц
азмер, Байт
Создан
Изменен
Открыт
ЛАБОРАТОРНАЯ РАБОТА №1_МАВД.pdf 1,123,262 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №2_МАВД.pdf 380,075 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №3_МАВД.pdf 1,897,071 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №4_МАВД.pdf 1,043,787 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
ЛАБОРАТОРНАЯ РАБОТА №5_МАВД.pdf 794,124 11.05.2023 ... 10.05.2023 ... 11.05.2023 ...
Упорядоченные по:
Структуре на диске
Расширению
Времени создания
Вре
Детали
Маленькие иконки
Средние иконки
Большие иконки
Журнал
Тип Дата Время Текст
Система 11.05.2023 13:27:58 Сканирование было завершено для Свободное Место15 за 13м 34с
Система 11.05.2023 13:30:37 Перечисление файлов было завершено за 0 сек
Восстанов... 11.05.2023 13:31:59 Использовать правила для существующих файлов:По умолчанию:Переименовать;
Восстанов... 11.05.2023 13:31:59 Recover destination: D:/ТЕСТ/
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 1.27 GB из 3018 файлов в 61 папках


R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска
Остановить
Восстановить
Восстановить помеченные...
Найти/Отметить...
Найти предыдущее
Найти следующее
Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volu...
Дополнительно ...
Архив
Графика, Из...
Документ
Adobe PD...
Microsoft...
Microsoft...
Rich Text ...
Text Доку...
Unicode ...
Документ Ба...
Другие файлы
Исполняемы...
Имя
Ц
азмер, Байт
Создан
Изменен
Открыт
20221108_223400.docx 20,396 09.11.2022 ...
20221110_095400.docx 2,265,349 10.11.2022 ...
20221110_115200.docx 1,345,457 10.11.2022 ...
e292kt_20.docx 4,664,218 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
e4759kt_18.docx 2,724,074 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
e921kt_20.docx 2,714,621 11.05.2023 ... 28.05.2021 ... 11.05.2023 ...
Для_оформления_лаб_исследование.docx 51,394 11.05.2023 ... 07.02.2023 ... 11.05.2023 ...
Для_оформления_лаб_экспертиза.docx 4,805,311 11.05.2023 ... 07.02.2022 ... 11.05.2023 ...
Упорядоченные по:
Структуре на диске
Расширению
Времени создания
Вре
Детали
Маленькие иконки
Средние иконки
Большие иконки
Журнал
Тип Дата Время Текст
Система 11.05.2023 13:27:58 Сканирование было завершено для Свободное Место15 за 13м 34с
Система 11.05.2023 13:30:37 Перечисление файлов было завершено за 0 сек
Восстанов... 11.05.2023 13:31:59 Использовать правила для существующих файлов:По умолчанию:Переименовать;
Восстанов... 11.05.2023 13:31:59 Recover destination: D:/ТЕСТ/
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 1.27 GB из 3018 файлов в 61 папках



13. Сделать вывод о проделанной работе.

Контрольные вопросы

1. Какие файловые системы вы знаете?
2. Опишите алгоритм восстановления текстовых файлов с помощью ПО R-Studio.
3. Что такое черновое восстановление (восстановление по сигнатурам)?
4. Как обнаружить удаленные текстовые файлы с помощью ПО R-Studio?
5. Для чего предназначено ПО R-Studio?
6. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
7. Опишите алгоритм подключения USB-накопителя с помощью ПАК «PC-3000» в режиме монтирования.
8. Какие типы файлов вы знаете?
9. Как обнаружить удаленные текстовые файлы с помощью ПАК «PC-3000»?
10. Для чего предназначен ПАК «PC-3000»?
11. Через какой интерфейс ПАК «PC-3000» подключается к лабораторному компьютеру?
12. Какие интерфейсные разъемы для подключения исследуемых объектов имеет ПАК «PC-3000»?
13. Как заблокировать запись на исследуемом объекте, подключенном через ПАК «PC-3000» в режиме монтирования?

ЛАБОРАТОРНАЯ РАБОТА № 23

ВОССТАНОВЛЕНИЕ И АНАЛИЗ УДАЛЕННЫХ ФАЙЛОВ РЕЕСТРА И ЖУРНАЛОВ СОБЫТИЙ ИЗ НЕИЗВЕСТНОЙ ФАЙЛОВОЙ СИСТЕМЫ ФЛЕШ-НАКОПИТЕЛЯ С ИСПОЛЬЗОВАНИЕМ КОМБИНИРОВАННОГО СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель работы: Получение практических навыков работы со специализированными программными и аппаратными комплексами.

Используемые приборы и оборудование

1. Персональный компьютер.
2. Операционная система.
3. Специальное оборудование.

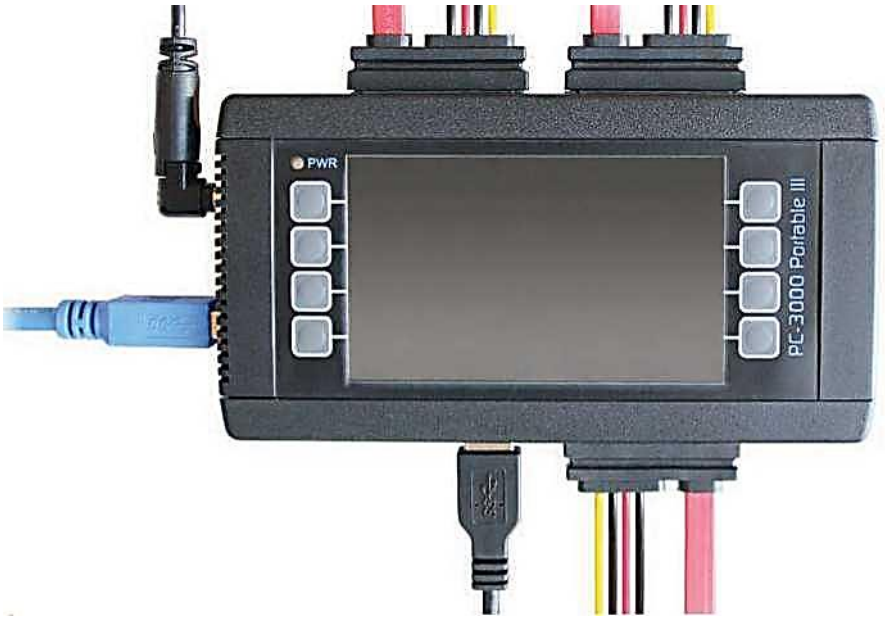
Подготовка к выполнению работы

1. Ознакомиться с описанием лабораторной работы, используемых приборов и программ.
2. Изучить теоретический материал по теме лабораторной работы.
3. Подготовить рабочий отчет, который должен содержать: название и цель лабораторной работы, основные теоретические положения, ход выполнения работы и выводы.

Основные теоретические сведения

PC-3000 Portable – это портативный программно-аппаратный комплекс, предназначенный для диагностики, ремонта и восстановления пользовательских данных с накопителей HDD/SSD1, имеющих физические неисправности носителей и логические повреждения файловых систем. К физическим неисправностям HDD относятся: повреждения платы электроники, магнитных дисков, головок чтения-записи, предусилителя, микропрограммы, служебной информации. К физическим неисправностям SDD относятся: повреждения платы электроники, контроллера, деградация ячеек массива NAND-Flash памяти, повреждение микропрограммы, служебной информации и др. К логическим неисправностям относятся: повреждения дисковых структур, структур файловых систем и комбинации этих проблем. Дополнительно, PC-3000 Portable позволяет создавать имидж-копии данных с накопителей HDD, SSD, USB-Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны.

Диагностируемые HDD/SSD/Flash накопители, подлежащие восстановлению данных, подключаются непосредственно к контроллеру PC 3000 Portable – к его портам SOURCE - USB и Port0. К портам TARGET - Port1 и Port2 подключаются HDD/SSD накопители для создания имидж-копии данных. В некоторых режимах работы порты Port1 и Port2 также могут использоваться для подключения диагностируемых/восстанавливаемых накопителей, увеличивая тем самым общее число одновременно восстанавливаемых HDD/SSD до трех.



Порты SOURCE - USB и Port 0 допускают блокировку от записи, для ее включения необходимо воспользоваться переключаетелем Write Protection. При включенной блокировке должен гореть жетлый светодиод.

Контроллер PC-3000 Portable подключается к внешнему источнику питания -19В, и в случае работы через управляющий компьютер подключается к нему через интерфейс USB 3.0.

В существующей реализации контроллер PC-3000 Portable допускает подключение накопителей HDD/SSD с интерфейсом SATA-III (совместим с SATA-I/II, SSD M.2 NVMe PCIe) и накопителей с USB интерфесом, соответствующих классификации Mass Storage Device – внешние HDD/ SSD USB 2.0/3.0 и USB-Flash накопители. Подключение накопителей с интерфейсом PATA (IDE) возможно через специальный адаптер PATA, который поставляется опционально.

Комплекс поддерживает работу с моделями накопителей от 40 [б до 6 Тб. За это время плотность записи информации увеличилась в сотни раз, и такой разрыв не мог не отразиться на различии архитектурных решений накопителей, различиях в подходах, методиках и сложностях восстановления информации. В результате многие методики восстановления данных, хорошо работающие на HDD емкостью 40-100 [б, оказываются неприменимы для HDD - 1-6 Тб. В данном комплексе собраны

наиболее универсальные методы, работающие для всех поколений HDD. При этом для работы с PC-3000 Portable не потребуется глубокое знание принципов работы накопителей, следует только придерживаться методик, описанных в документации к комплексу.

Операционная система Windows, работая с поврежденным носителем информации, применяет доступные ей программные средства восстановления данных. Часто это лишь ухудшает ситуацию с повреждениями данных на неисправных накопителях. При использовании комплекса PC-3000 Portable доступ ОС к неисправному HDD исключается. Но при необходимости можно использовать программный драйвер монтирования дисков, который позволяет «смонтировать» диагностируемый накопитель, подключенный к портам PC-3000 Portable как дисковое устройство ОС.

Для целого ряда накопителей HDD/SSD имеется возможность использовать технологический режим, т.е., режим, который используется на заводе-изготовителе в процессе производства. Это дает расширенные возможности для получения доступа к данным пользователя и их копирования.

Комплекс PC-3000 Portable может работать в трех режимах: автономном, упрощенном и полнофункциональном. В автономном режиме используется встроенное ПО PC-3000 Portable, в нем доступны функции диагностики и создания посекторной копии данных с накопителей подключенных к портам USB и Port 0. Иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. При использовании управляющего компьютера доступны режимы упрощенный и полнофункциональный. Упрощенный режим содержит необходимый набор автоматических функций для диагностики, извлечения данных и создания иммидж-копий с накопителей подключенных к портам USB и Port 0. Как и в автономном режиме, иммидж-копия данных создается на исправные накопители SATA подключенные к портам Port 1 и (или) Port 2. В упрощенном режиме возможно создание «Дела» и получение всех отчетов о работе с накопителем, что будет полезно специалистам области Форензик. Полнофункциональный режим содержит максимальные возможности по работе с поврежденными накопителями и является аналогом ПО комплексов PC-3000 Express и PC-3000 UDMA, отличия касаются только количества и скоростных характеристик диагностических портов контроллеров. В качестве управляющего компьютера может быть использован настольный ПК или Ноутбук. Подключение контроллера PC-3000 Portable к компьютеру осуществляется через интерфейс USB 3.0, что позволяет использовать данный комплекс, как мобильную станцию для восстановления данных и проводить работы непосредственно у заказчика.

R-Studio это семейство утилит для восстановления файлов. Программа функционирует как на локальных, так и на удаленных

компьютерах по сети, даже если разделы дисков были форматированы, повреждены или удалены. Уникальная технология сканирования IntelligentScan и удобный в установке параметров интерфейс программы дают пользователю абсолютный контроль над процессом восстановления данных.

Для восстановления удаленных файлов с логического диска (найденного раздела):

Дважды щелкните левой кнопкой мыши по логическому диску на панели Диски R-Studio, чтобы перечитать файлы диска.

При попытке перечитать файлы жесткого диска или другого объекта без определенной файловой системы появится сообщение «Дважды щелкните левой кнопкой мыши по логическому диску...». Выберите логический диск объекта или отсканируйте объект.

> Панели R-Studio изменятся и будет показана структура папок/файлов диска.

R-Studio анализирует данные объекта и отображает все файлы, информация о которых была найдена. Если же файлы не найдены, то это означает, что информация о них была удалена. Для более подробной информации о восстановлении таких файлов смотри раздел Восстановление Данных. Дополнительные Операции.

Обратите внимание, что R-Studio показывает только те файлы/папки, которые соответствуют заданной маске файлов.

На панели Журнал будет показано, сколько файлов и папок имеются в данном объекте и их размер. В фильтре журнала вы можете задать, какие типы событий будут отображаться в панели журнала.

Обратите внимание: Метафайлы – это внутренние системные файлы (данные файловой системы), невидимые пользователем, которые R-Studio показывает, как файлы. Такие файлы не содержат данные пользователя и используются только при восстановлении файловой системы диска.

При появлении сообщения Too many files... вы можете временно прекратить вывод файлов и просмотреть найденные файлы. Затем вы можете продолжить вывод файлов. Вы также можете продолжить вывод файлов без просмотра. R-Studio сохранит информацию о внутренней структуре файла.

Для полного анализа структуры данных объекта его необходимо отсканировать. Любой объект на панели Устройство/Диск может быть отсканирован. Кроме того, вы можете отсканировать часть объекта, создав регион. В разделе Регионы рассматривается, как создавать и работать с регионами. Сканирование также значительно повышает оценки шансов успешного восстановления файлов.

Вы можете выбрать область и другие параметры сканирования. Результаты сканирования могут быть сохранены в файл, который затем может быть открыт.

При необходимости можно сохранить результаты сканирования на удаленном компьютере.

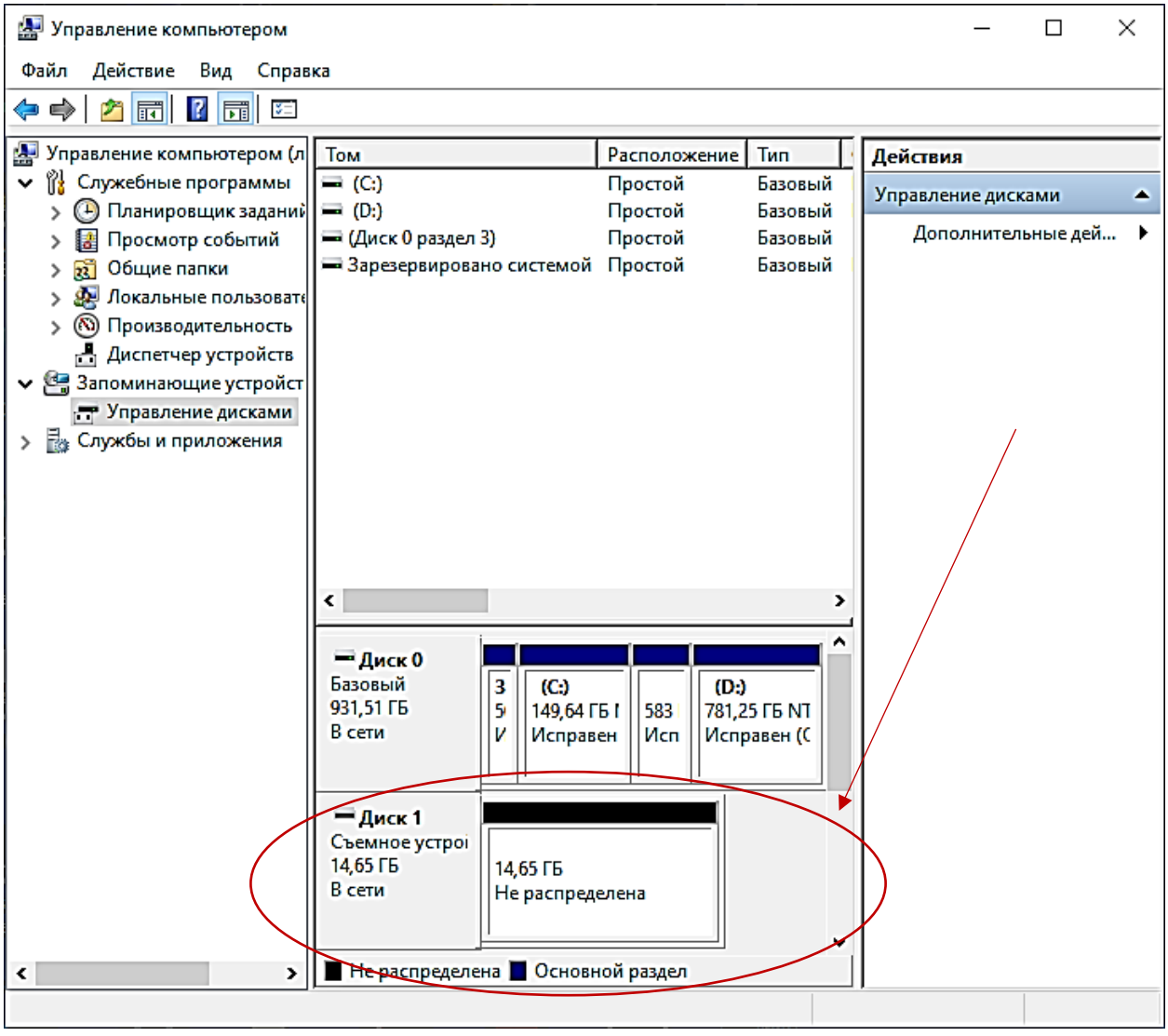
Внимание: Сканирования больших областей может занять очень много времени!

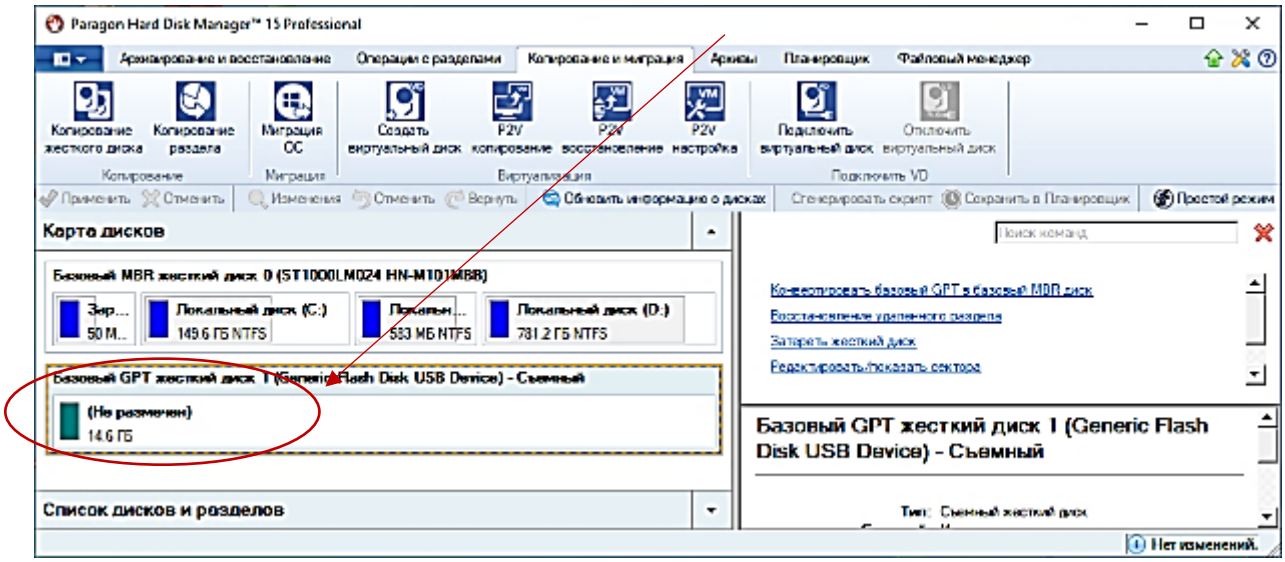
НИКОГДА НЕ ПЫТАЙТЕСЬ СОХРАНИТЬ ОТСКАНИРОВАННОЕ НА СКАНИРУЕМЫЙ ОБЪЕКТ!!!

Это может стать причиной полной утраты данных.

Порядок выполнения работы

1. Получить у преподавателя накопитель информации с неизвестной файловой системой.
2. Убедиться, что на накопителе отсутствует файловая система. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.





2.1. В случае, если на накопителе имеется файловая система – удалить ее. Оставить диск неразмеченным.

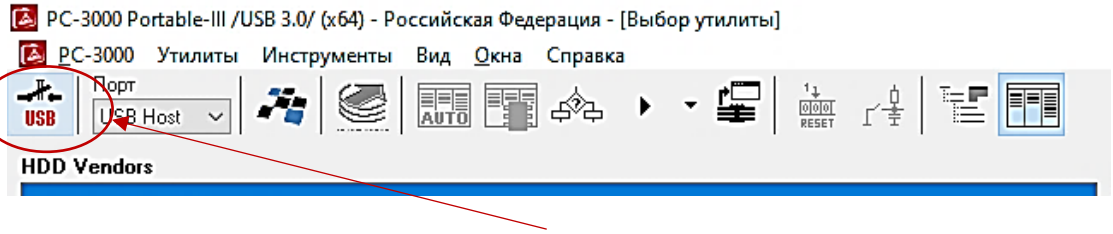
3. Подключить ПАК «PC-3000» к лабораторному компьютеру.

3.1. Продемонстрировать правильно подключенный ПАК «PC-3000» преподавателю ПЕРЕД ВКЛЮЧЕНИЕМ!!!

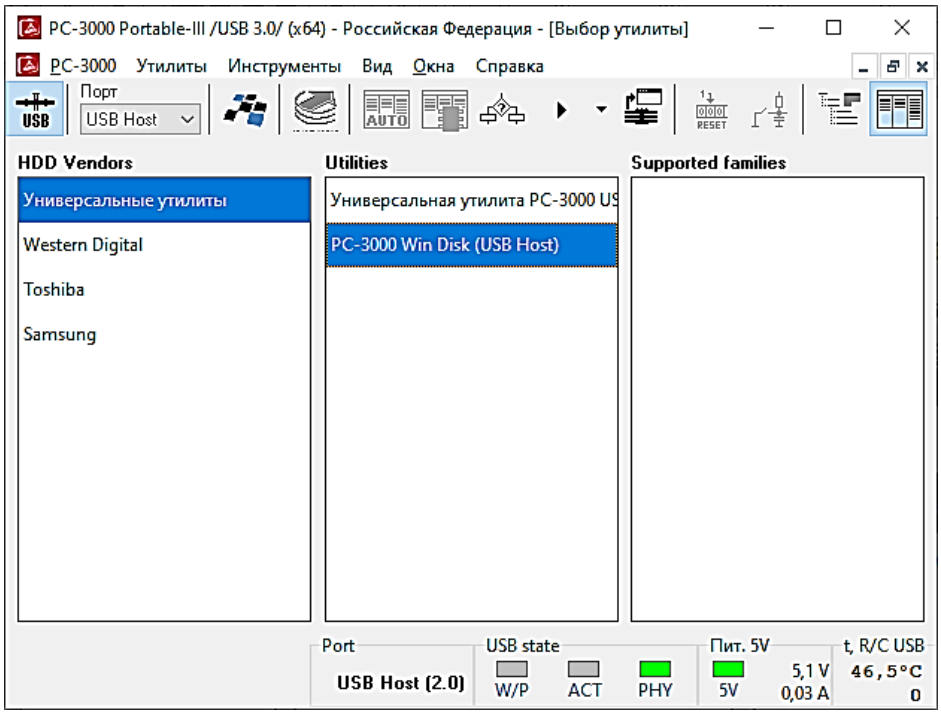
4. Запустить программу «PC-3000 Portable-III». Отметить галочкой порт USB.

5. Подключить исследуемый флеш-накопитель к ПАК «PC-3000» через интерфейсный разъем USB в режиме монтирования.

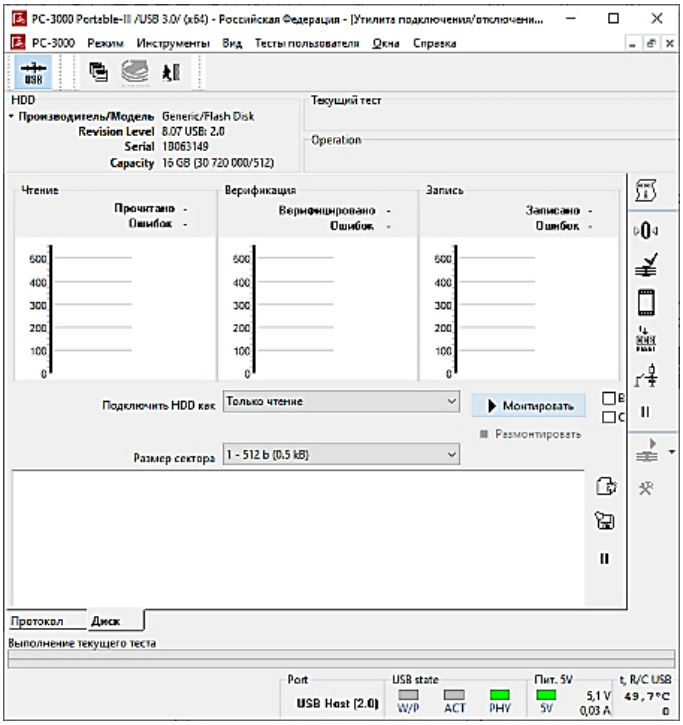
6. Включить питание разъема USB.



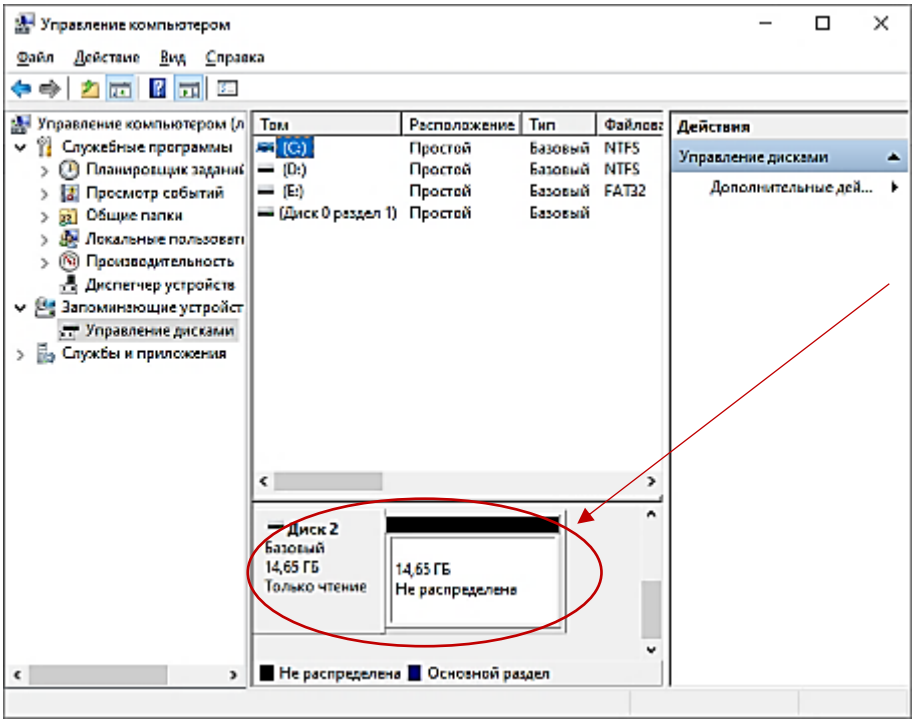
7. Запустить утилиту «PC-3000 Win Disk».

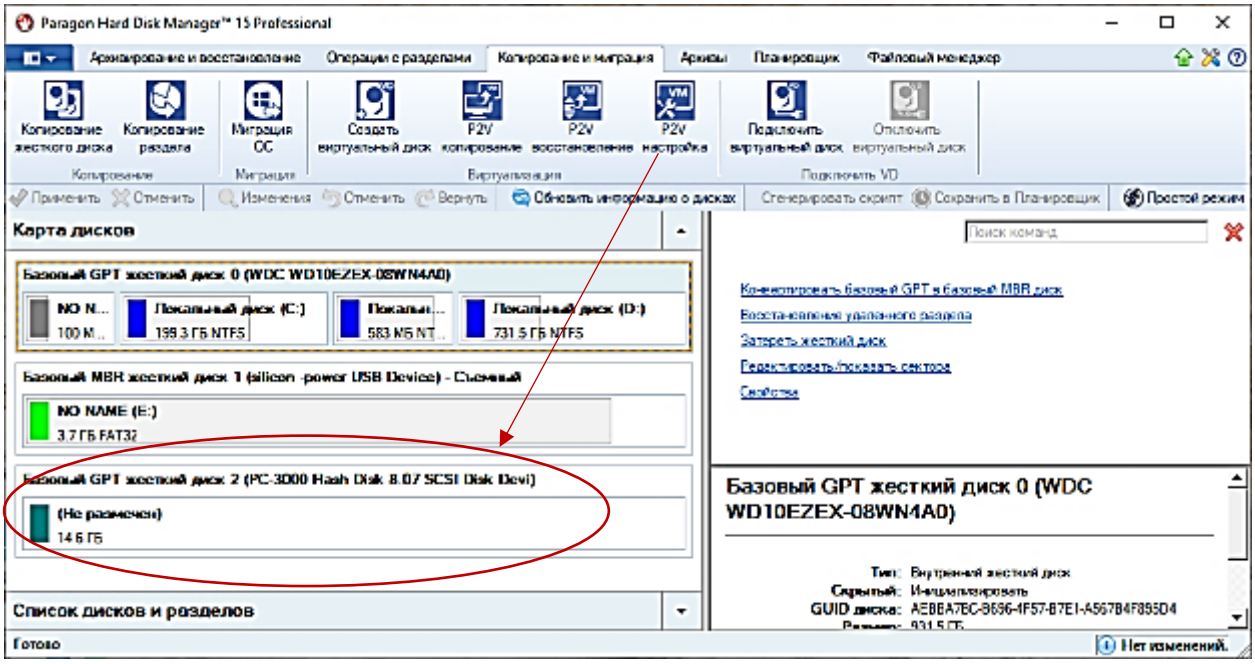


8. Монтировать исследуемый накопитель в режиме «Только чтение».



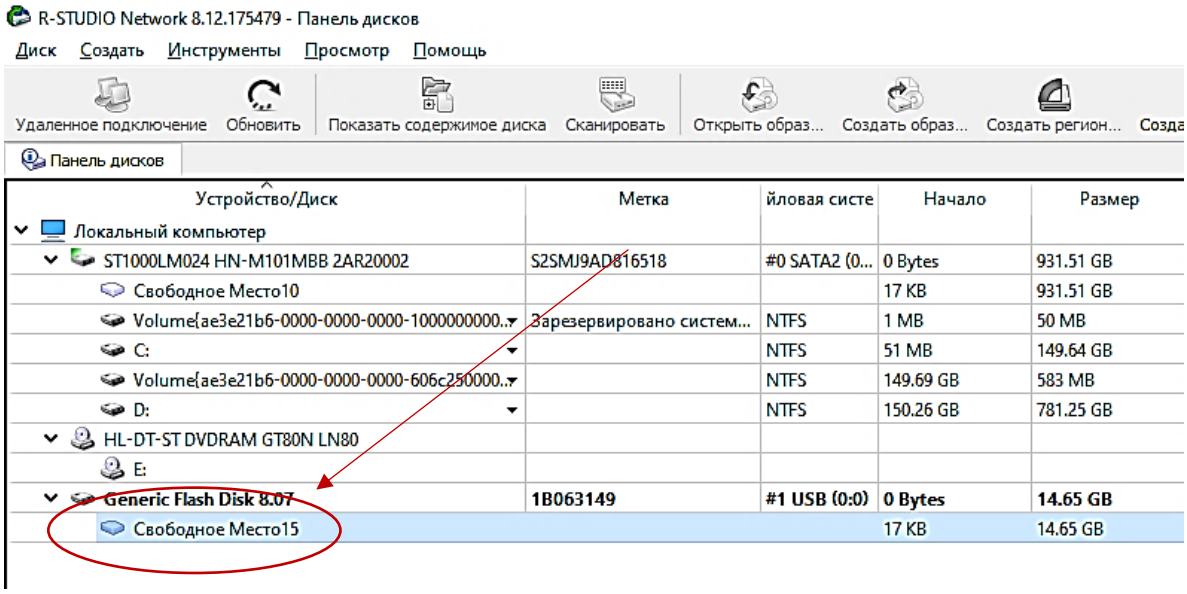
9. Убедиться, что исследуемый накопитель монтирован к ОС лабораторного компьютера. Стандартными средствами либо с помощью ПО Paragon Hard Disk Manager.





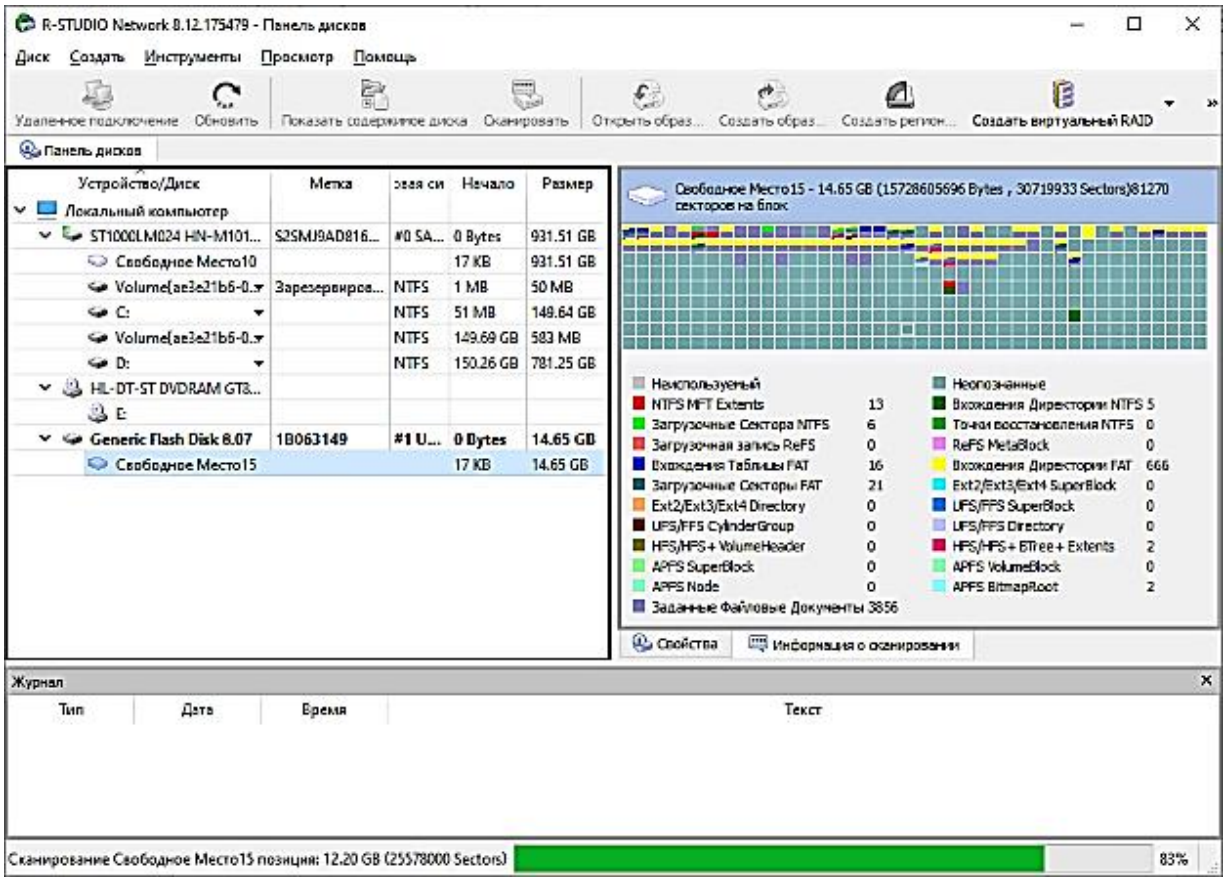
10. Запустить ПО R-Studio.

10.1. Обнаружить в программе исследуемый флеш-накопитель с отсутствующей файловой системой.

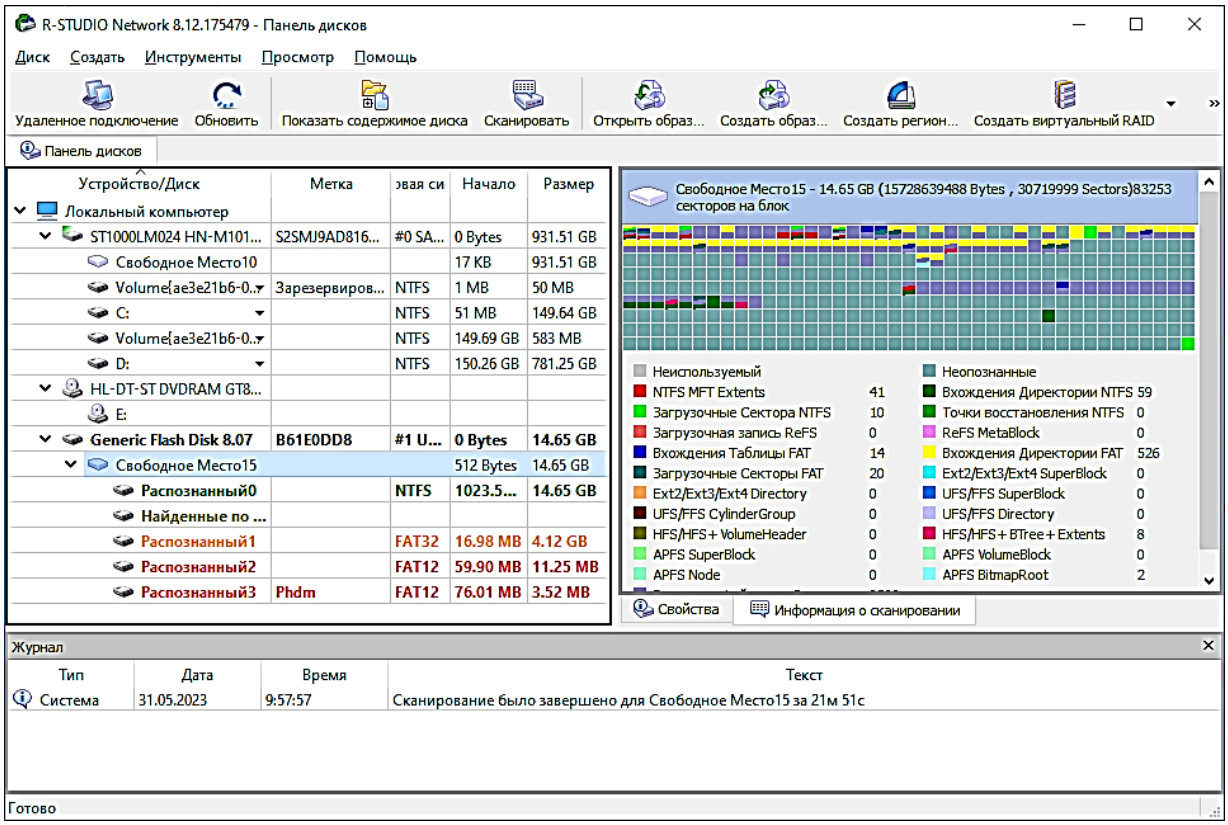


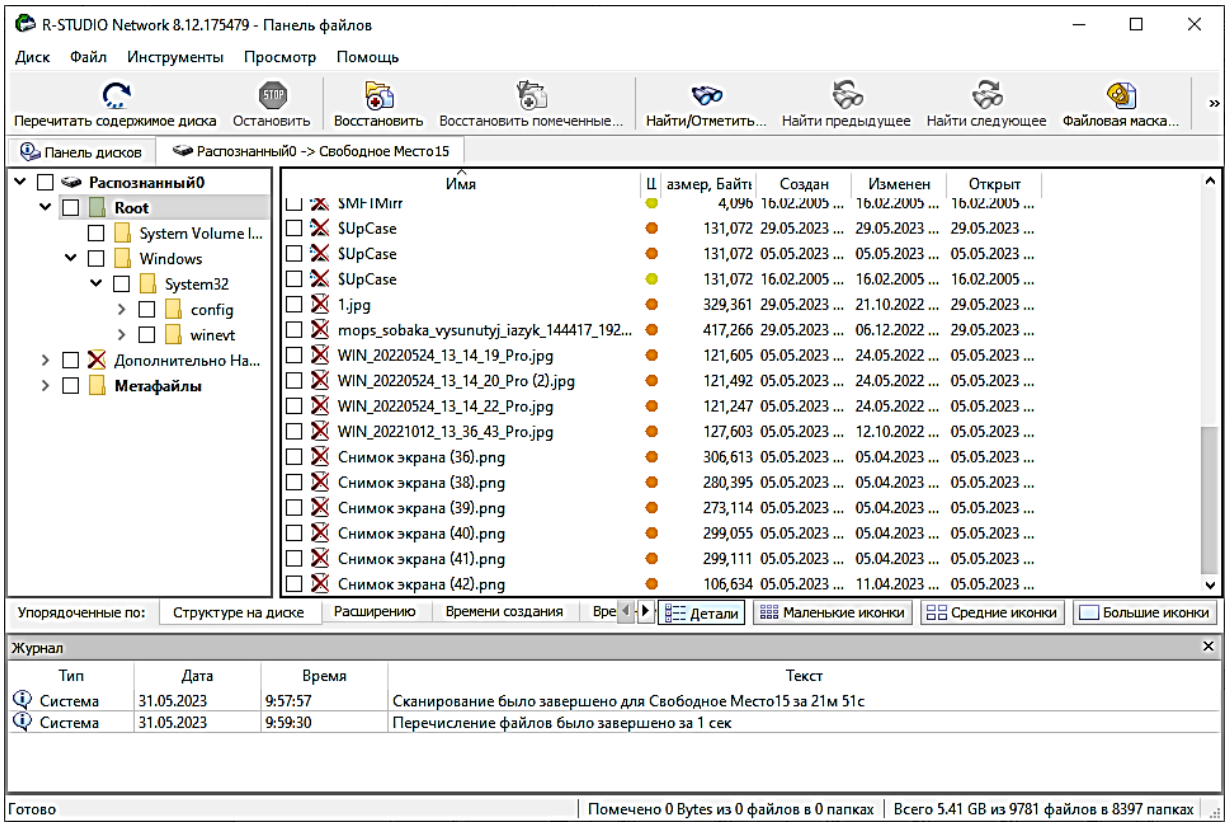
11. Запустить сканирование. Для этого кликнуть ПКМ на выбранный флеш-накопитель в программе R-Studio и выбрать пункт «Сканировать».

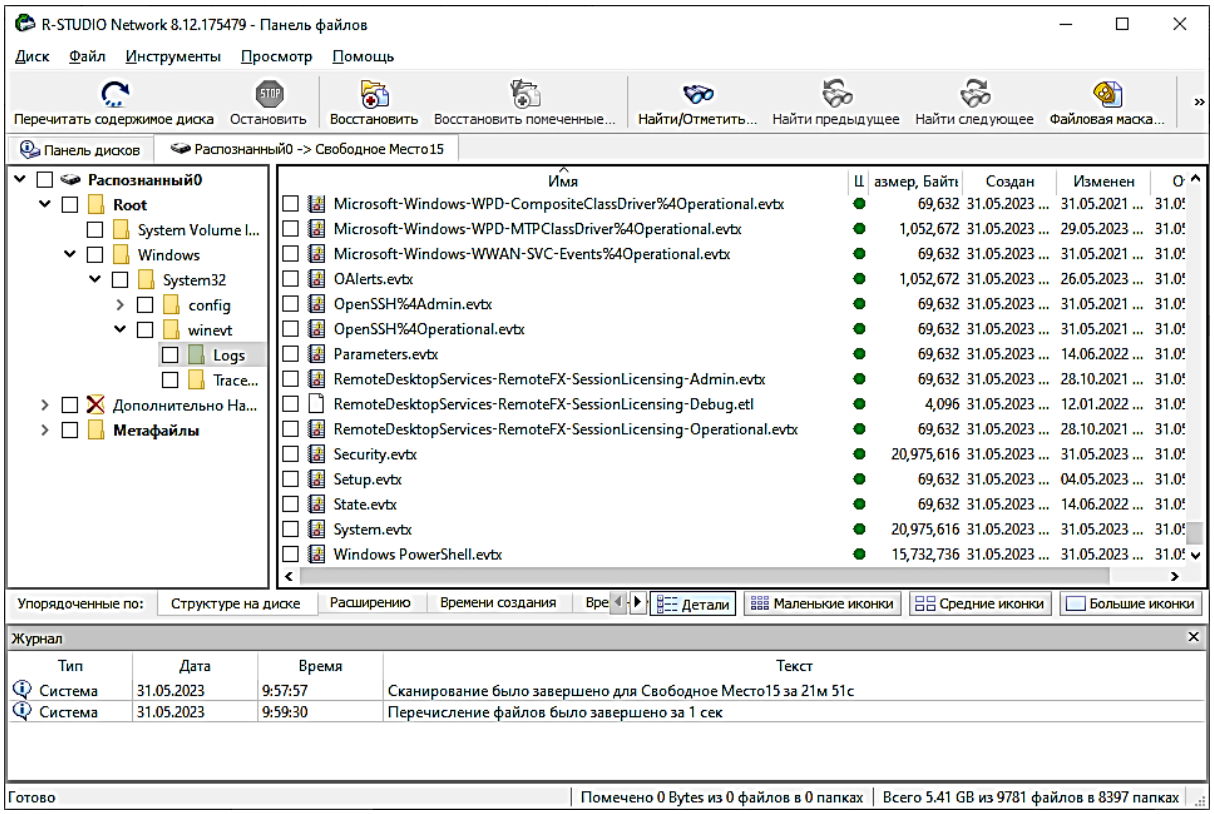
11.1. Запуститься процесс сканирования.

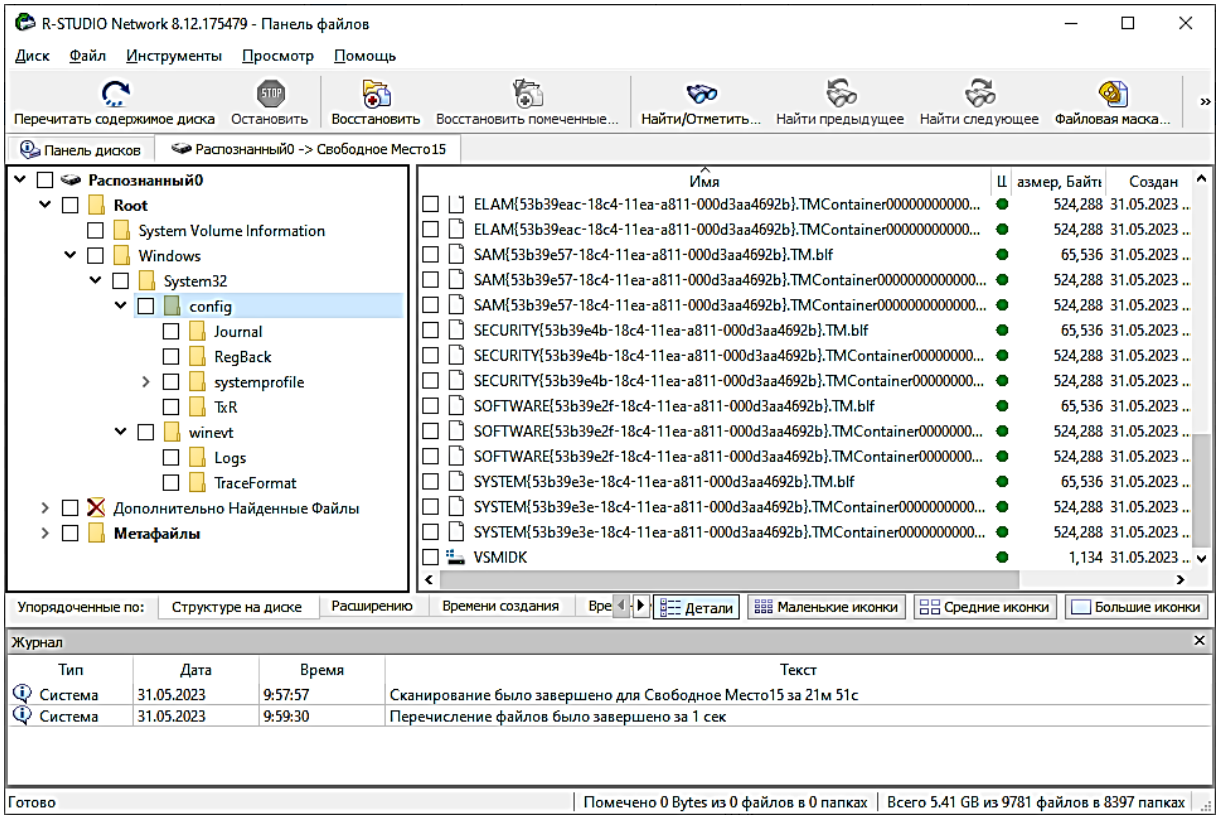


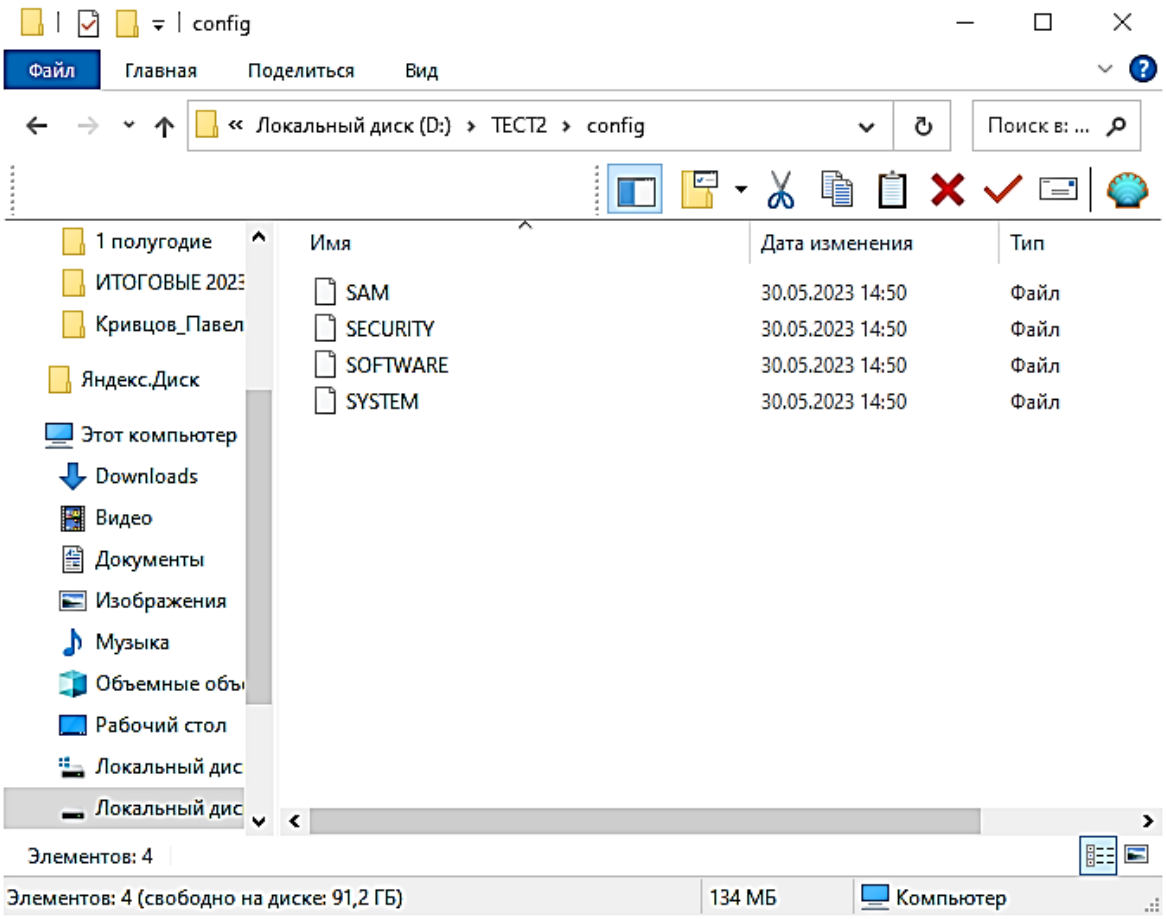
12. Проанализировать результат сканирования. Восстановить файлы реестра и журналов событий.

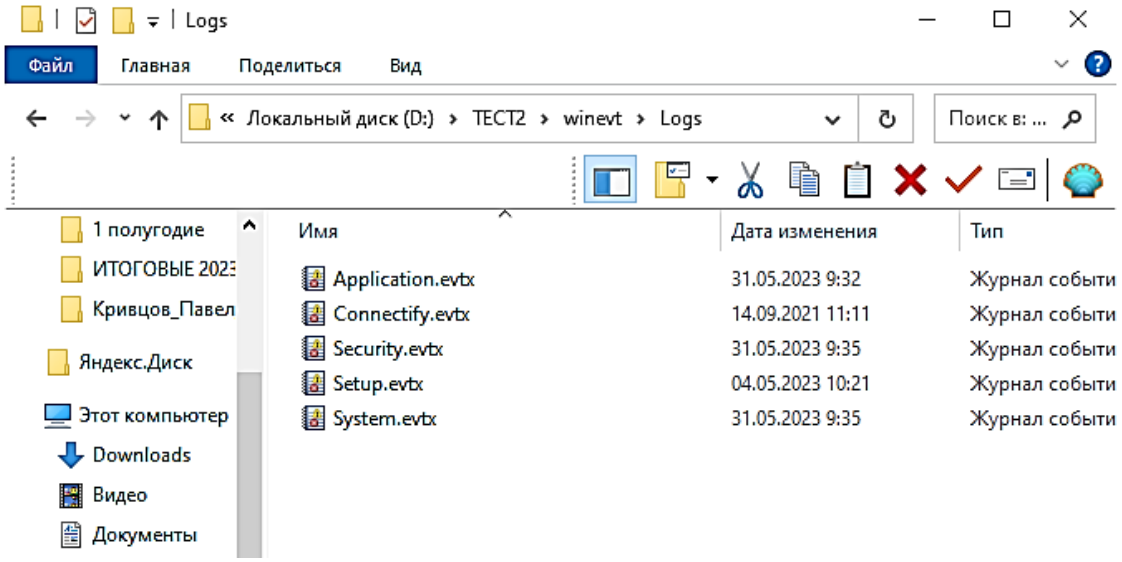

R-STUDIO Network 8.12.175479 - Панель дисков
Диск Создать Инструменты Просмотр Помощь
Удаленное подключение Обновить Показать содержимое диска Сканировать Открыть образ... Создать образ... Создать регион... Создать виртуальный RAID
Панель дисков
Устройство/Диск Метка Начало Размер
Локальный компьютер
ST1000LM024 HN-M101... S2SMJ9AD816... #0 SA... 0 Bytes 931.51 GB
Свободное Место10 17 KB 931.51 GB
Volume{ae3e21b6-0... Зарезервиров... NTFS 1 MB 50 MB
C: NTFS 51 MB 149.64 GB
Volume{ae3e21b6-0... NTFS 149.69 GB 583 MB
D: NTFS 150.26 GB 781.25 GB
HL-DT-ST DVDRAM GT8...
E:
Generic Flash Disk 8.07 B61E0DD8 #1 U... 0 Bytes 14.65 GB
Свободное Место15 512 Bytes 14.65 GB
Распознанный0 NTFS 1023.5... 14.65 GB
Найденные по ...
Распознанный1 FAT32 16.98 MB 4.12 GB
Распознанный2 FAT12 59.90 MB 11.25 MB
Распознанный3 Phdm FAT12 76.01 MB 3.52 MB
Свободное Место15 - 14.65 GB (15728639488 Bytes , 30719999 Sectors)83253 секторов на блок
Неиспользуемый
NTFS MFT Extents 41
Загрузочные Сектора NTFS 10
Загрузочная запись ReFS 0
Вхождения Таблицы FAT 14
Загрузочные Секторы FAT 20
Ext2/Ext3/Ext4 Directory 0
UFS/FFS CylinderGroup 0
HFS/HFS+ VolumeHeader 0
APFS SuperBlock 0
APFS Node 0
Неопознанные
Вхождения Директории NTFS 59
Точки восстановления NTFS 0
ReFS MetaBlock 0
Вхождения Директории FAT 526
Ext2/Ext3/Ext4 SuperBlock 0
UFS/FFS SuperBlock 0
UFS/FFS Directory 0
HFS/HFS+ BTree+ Extents 8
APFS VolumeBlock 0
APFS BitmapRoot 2
Свойства
Информация о сканировании
Журнал
Тип Дата Время Текст
Система 31.05.2023 9:57:57 Сканирование было завершено для Свободное Место15 за 21м 51с
Готово


R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска Остановить Восстановить Восстановить помеченные... Найти/Отметить... Найти предыдущее Найти следующее Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volume I...
Windows
System32
config
winevt
Дополнительно На...
Метафайлы
Имя Размер, Байт Создан Изменен Открыт
$UpCase 131,072 29.05.2023 ... 29.05.2023 ... 29.05.2023 ...
$UpCase 131,072 05.05.2023 ... 05.05.2023 ... 05.05.2023 ...
$UpCase 131,072 16.02.2005 ... 16.02.2005 ... 16.02.2005 ...
1.jpg 329,361 29.05.2023 ... 21.10.2022 ... 29.05.2023 ...
mops_sobaka_vysunutyj_iazyk_144417_192... 417,266 29.05.2023 ... 06.12.2022 ... 29.05.2023 ...
WIN_20220524_13_14_19_Pro.jpg 121,605 05.05.2023 ... 24.05.2022 ... 05.05.2023 ...
WIN_20220524_13_14_20_Pro (2).jpg 121,492 05.05.2023 ... 24.05.2022 ... 05.05.2023 ...
WIN_20220524_13_14_22_Pro.jpg 121,247 05.05.2023 ... 24.05.2022 ... 05.05.2023 ...
WIN_20221012_13_36_43_Pro.jpg 127,603 05.05.2023 ... 12.10.2022 ... 05.05.2023 ...
Снимок экрана (36).png 306,613 05.05.2023 ... 05.04.2023 ... 05.05.2023 ...
Снимок экрана (38).png 280,395 05.05.2023 ... 05.04.2023 ... 05.05.2023 ...
Снимок экрана (39).png 273,114 05.05.2023 ... 05.04.2023 ... 05.05.2023 ...
Снимок экрана (40).png 299,055 05.05.2023 ... 05.04.2023 ... 05.05.2023 ...
Снимок экрана (41).png 299,111 05.05.2023 ... 05.04.2023 ... 05.05.2023 ...
Снимок экрана (42).png 106,634 05.05.2023 ... 11.04.2023 ... 05.05.2023 ...
Упорядоченные по: Структуре на диске Расширению Времени создания Детали Маленькие иконки Средние иконки Большие иконки
Журнал
Тип Дата Время Текст
Система 31.05.2023 9:57:57 Сканирование было завершено для Свободное Место15 за 21м 51с
Система 31.05.2023 9:59:30 Перечисление файлов было завершено за 1 сек
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 5.41 GB из 9781 файлов в 8397 папках

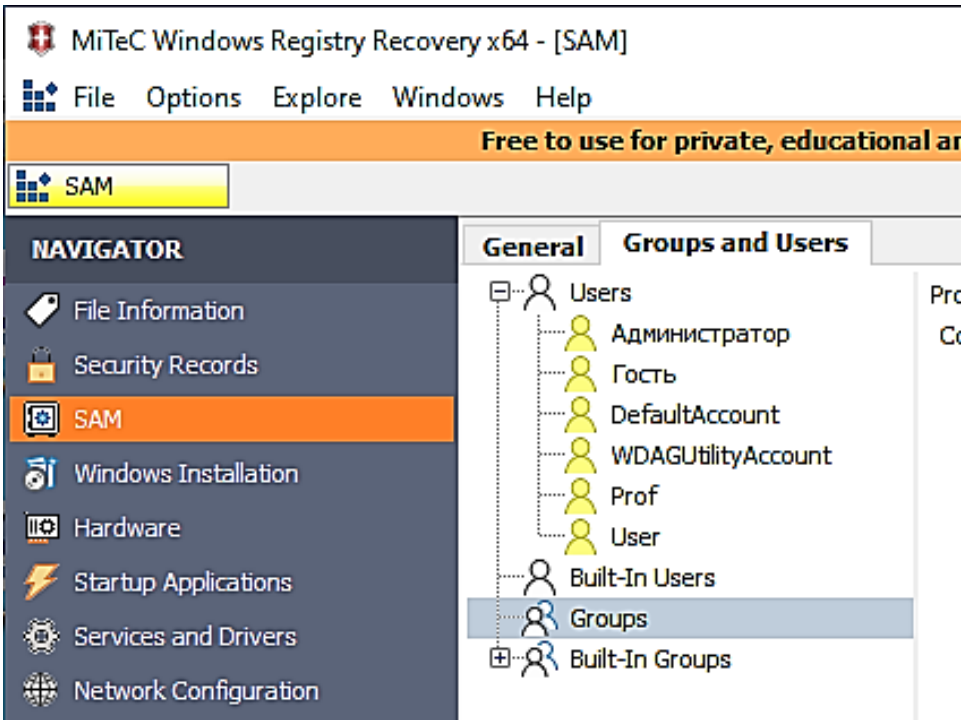

R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска
Остановить
Восстановить
Восстановить помеченные...
Найти/Отметить...
Найти предыдущее
Найти следующее
Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volume I...
Windows
System32
config
winevt
Logs
Trace...
Дополнительно На...
Метафайлы
Имя
Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx 69,632 31.05.2023 ... 31.05.2021 ...
Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx 1,052,672 31.05.2023 ... 29.05.2023 ...
Microsoft-Windows-WWAN-SVC-Events%4Operational.evtx 69,632 31.05.2023 ... 31.05.2021 ...
OAlerts.evtx 1,052,672 31.05.2023 ... 26.05.2023 ...
OpenSSH%4Admin.evtx 69,632 31.05.2023 ... 31.05.2021 ...
OpenSSH%4Operational.evtx 69,632 31.05.2023 ... 31.05.2021 ...
Parameters.evtx 69,632 31.05.2023 ... 14.06.2022 ...
RemoteDesktopServices-RemoteFX-SessionLicensing-Admin.evtx 69,632 31.05.2023 ... 28.10.2021 ...
RemoteDesktopServices-RemoteFX-SessionLicensing-Debug.etl 4,096 31.05.2023 ... 12.01.2022 ...
RemoteDesktopServices-RemoteFX-SessionLicensing-Operational.evtx 69,632 31.05.2023 ... 28.10.2021 ...
Security.evtx 20,975,616 31.05.2023 ... 31.05.2023 ...
Setup.evtx 69,632 31.05.2023 ... 04.05.2023 ...
State.evtx 69,632 31.05.2023 ... 14.06.2022 ...
System.evtx 20,975,616 31.05.2023 ... 31.05.2023 ...
Windows PowerShell.evtx 15,732,736 31.05.2023 ... 31.05.2023 ...
Упорядоченные по: Структуре на диске Расширению Времени создания
Детали
Маленькие иконки
Средние иконки
Большие иконки
Журнал
Тип Дата Время Текст
Система 31.05.2023 9:57:57 Сканирование было завершено для Свободное Место15 за 21м 51с
Система 31.05.2023 9:59:30 Перечисление файлов было завершено за 1 сек
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 5.41 GB из 9781 файлов в 8397 папках


R-STUDIO Network 8.12.175479 - Панель файлов
Диск Файл Инструменты Просмотр Помощь
Перечитать содержимое диска
Остановить
Восстановить
Восстановить помеченные...
Найти/Отметить...
Найти предыдущее
Найти следующее
Файловая маска...
Панель дисков
Распознанный0 -> Свободное Место15
Распознанный0
Root
System Volume Information
Windows
System32
config
Journal
RegBack
systemprofile
TxR
winevt
Logs
TraceFormat
Дополнительно Найденные Файлы
Метафайлы
Имя
ELAM{53b39eac-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000000... 524,288 31.05.2023 ..
ELAM{53b39eac-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000000... 524,288 31.05.2023 ..
SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TM.blf 65,536 31.05.2023 ..
SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000000000... 524,288 31.05.2023 ..
SAM{53b39e57-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000000000... 524,288 31.05.2023 ..
SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TM.blf 65,536 31.05.2023 ..
SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000... 524,288 31.05.2023 ..
SECURITY{53b39e4b-18c4-11ea-a811-000d3aa4692b}.TMContainer00000000... 524,288 31.05.2023 ..
SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TM.blf 65,536 31.05.2023 ..
SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000... 524,288 31.05.2023 ..
SOFTWARE{53b39e2f-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000... 524,288 31.05.2023 ..
SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TM.blf 65,536 31.05.2023 ..
SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000000... 524,288 31.05.2023 ..
SYSTEM{53b39e3e-18c4-11ea-a811-000d3aa4692b}.TMContainer0000000000... 524,288 31.05.2023 ..
VSMIDK 1,134 31.05.2023 ..
Упорядоченные по: Структуре на диске Расширению Времени создания
Детали
Маленькие иконки
Средние иконки
Большие иконки
Журнал
Тип Дата Время Текст
Система 31.05.2023 9:57:57 Сканирование было завершено для Свободное Место15 за 21м 51с
Система 31.05.2023 9:59:30 Перечисление файлов было завершено за 1 сек
Готово
Помечено 0 Bytes из 0 файлов в 0 папках
Всего 5.41 GB из 9781 файлов в 8397 папках

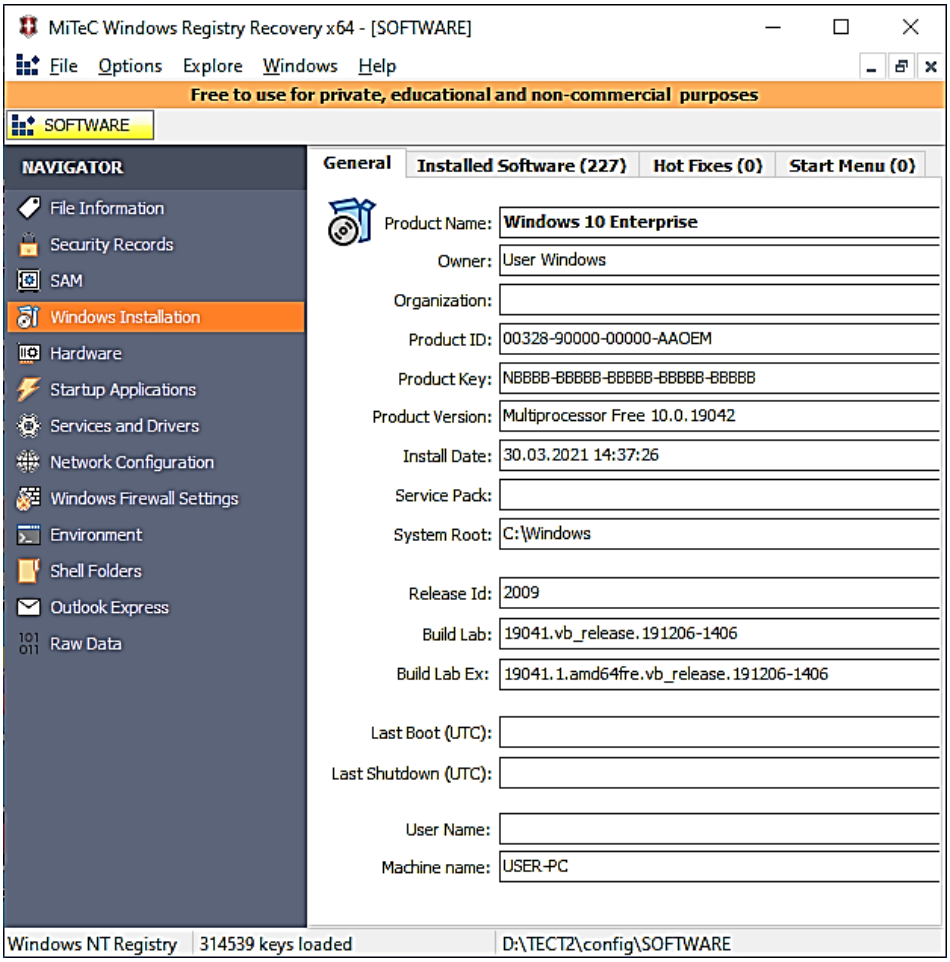




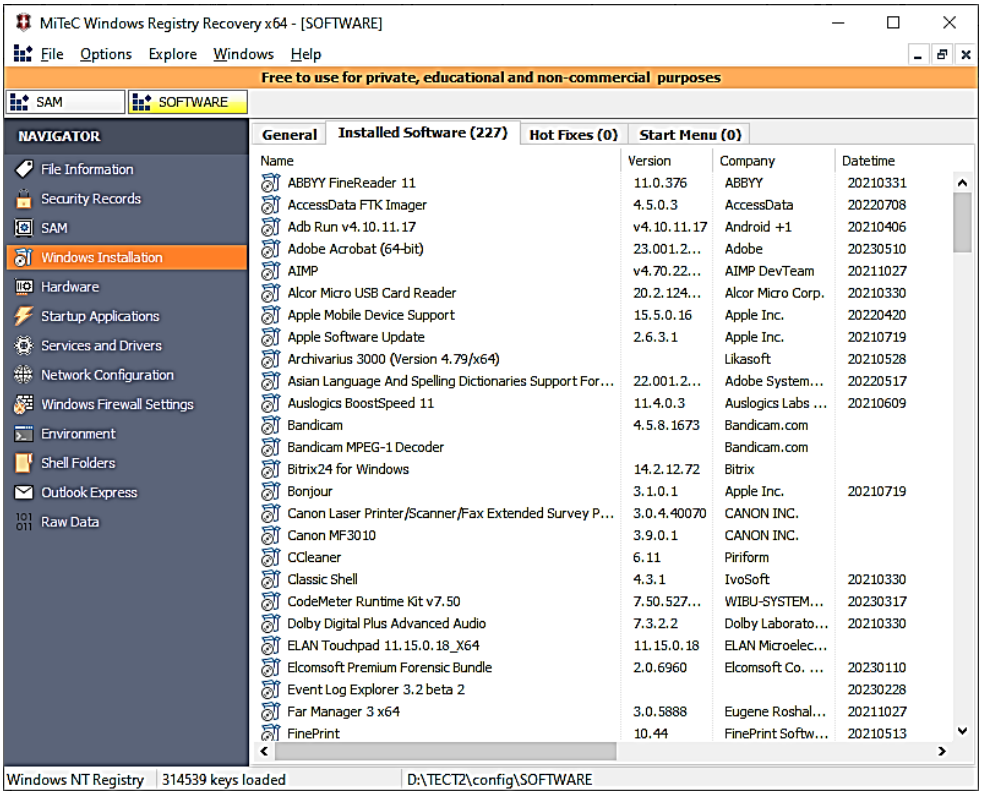
13. С помощью специализированного ПО WRR получить список пользователей ОС, используя раздел реестра SAM.



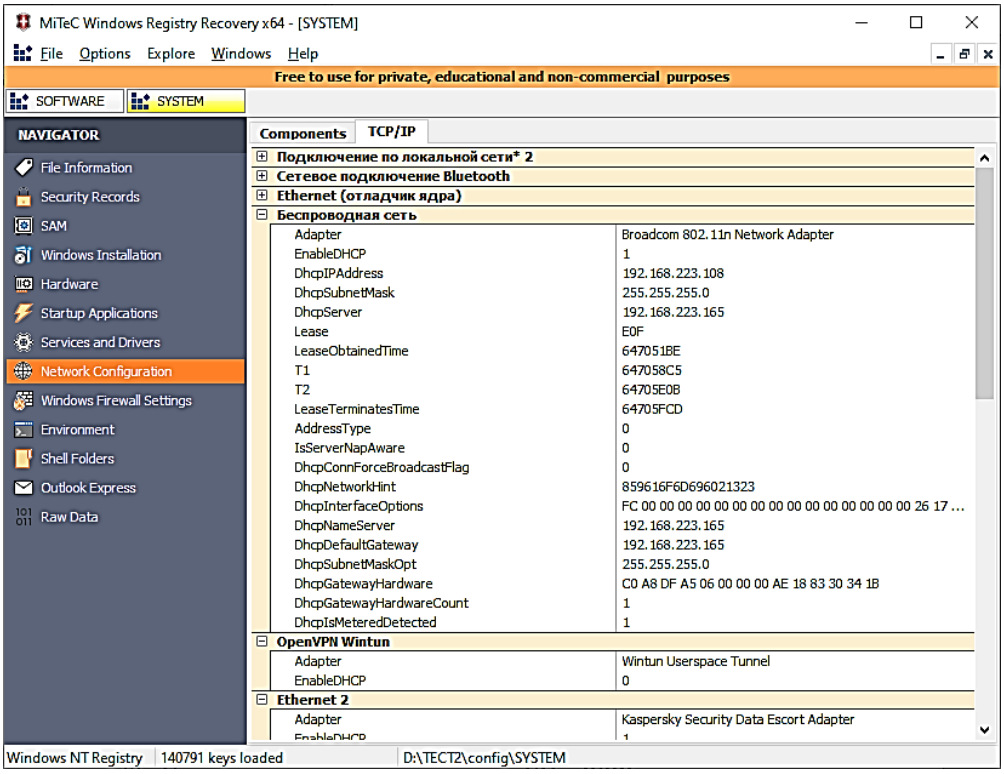
14. С помощью специализированного ПО WRR получить сведения об установленной ОС (Имя, ID, Product Key, дата установки), используя раздел реестра Software.

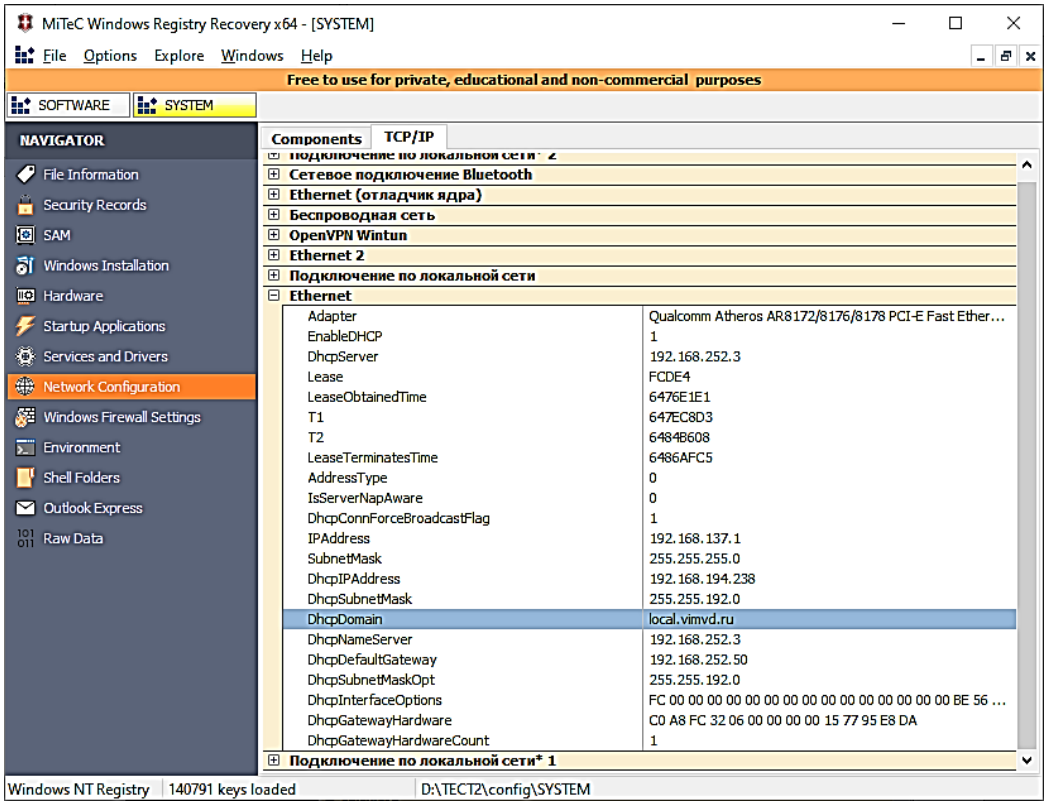


15. С помощью специализированного ПО WRR получить сведения об установленном ПО (Имя, версия, компания, дата установки), используя раздел реестра Software.

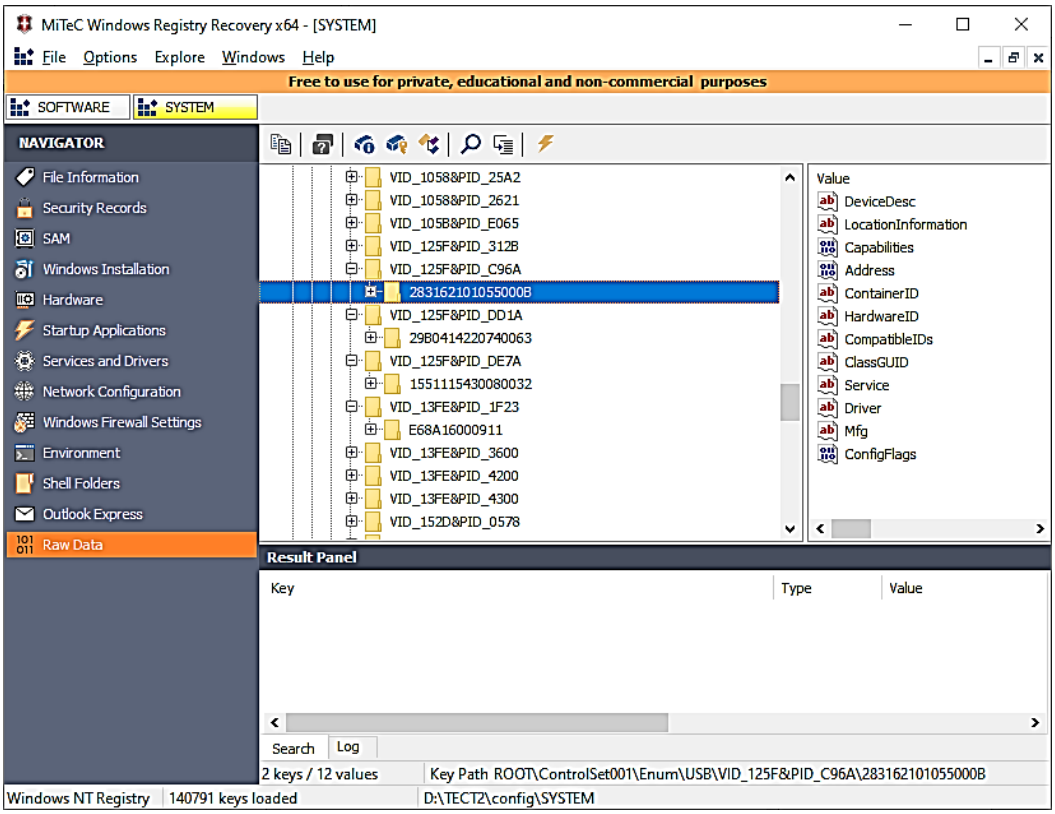


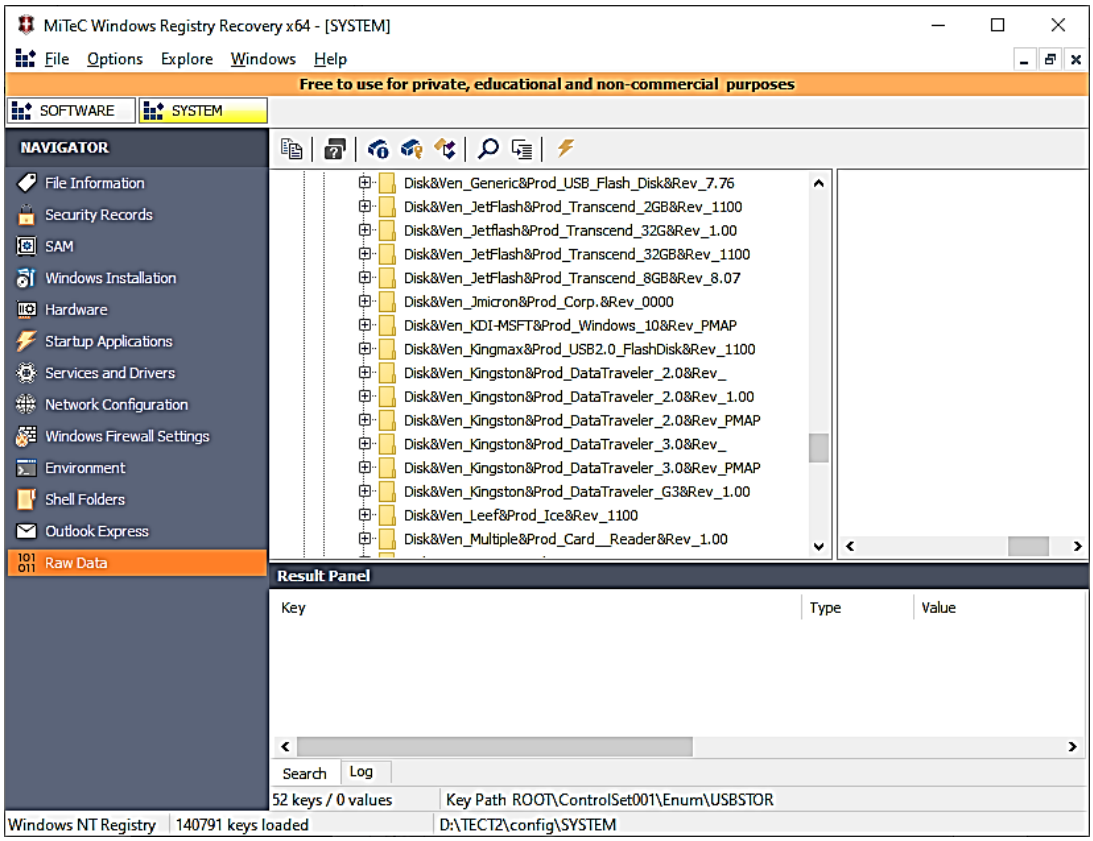
16. С помощью специализированного ПО WRR получить сведения о сетевых настройках (IP адрес, MAC адрес, DHCP адрес, DNS адрес, имя сетевого адаптера, домен), используя раздел реестра System.

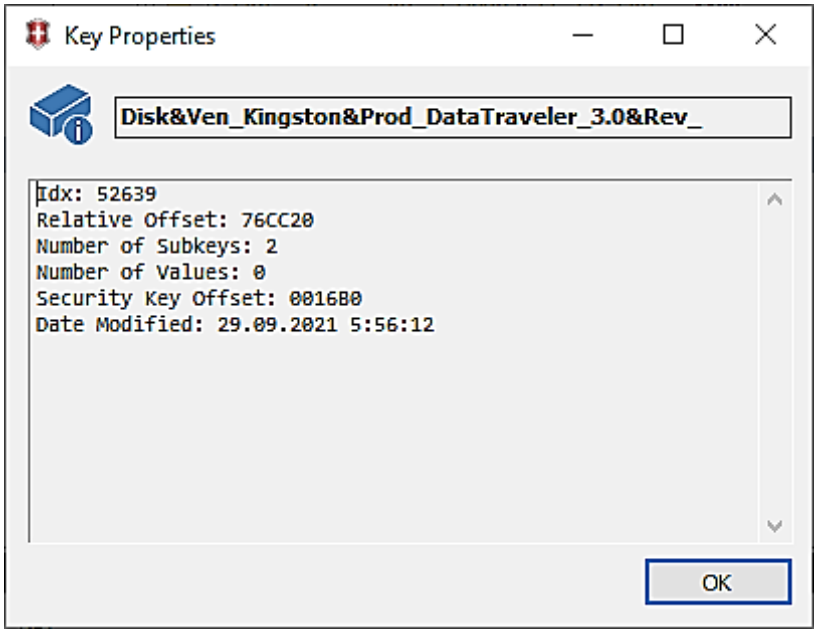


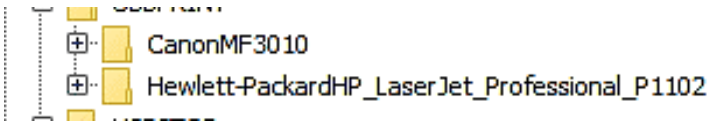


17. С помощью специализированного ПО WRR получить сведения о подключавшихся USB устройствах (серийный номер, имя, дата подключения, принтеры), используя раздел реестра System.

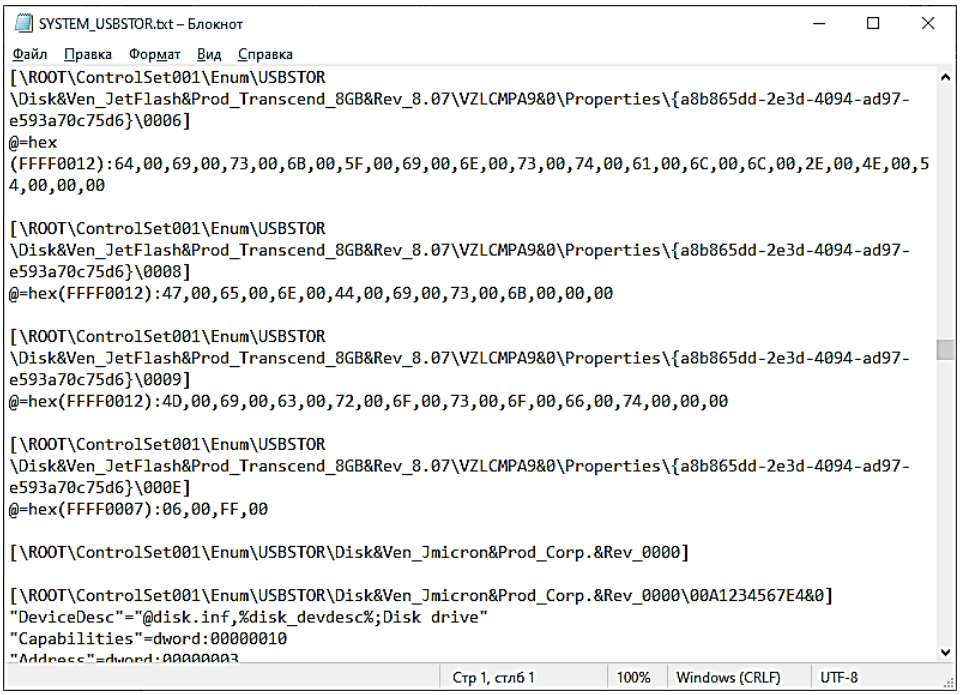




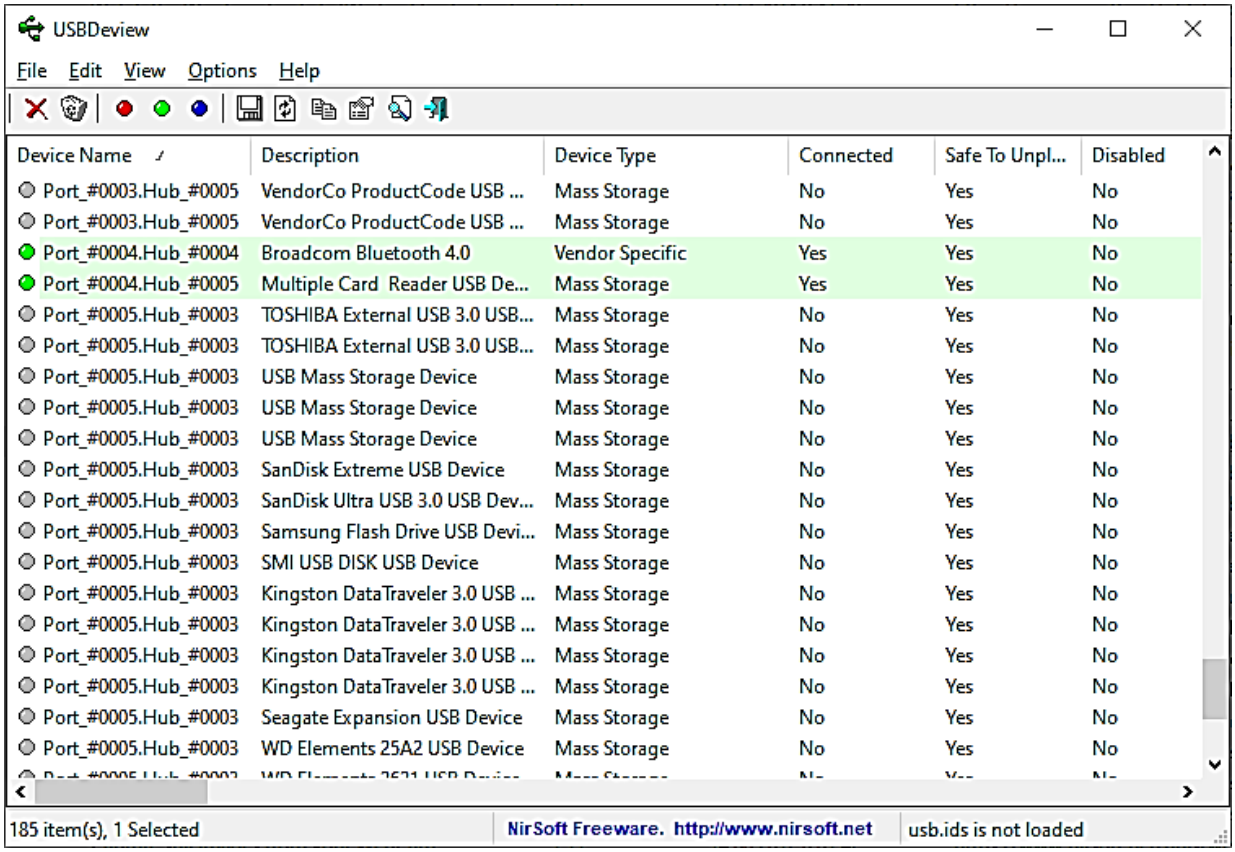




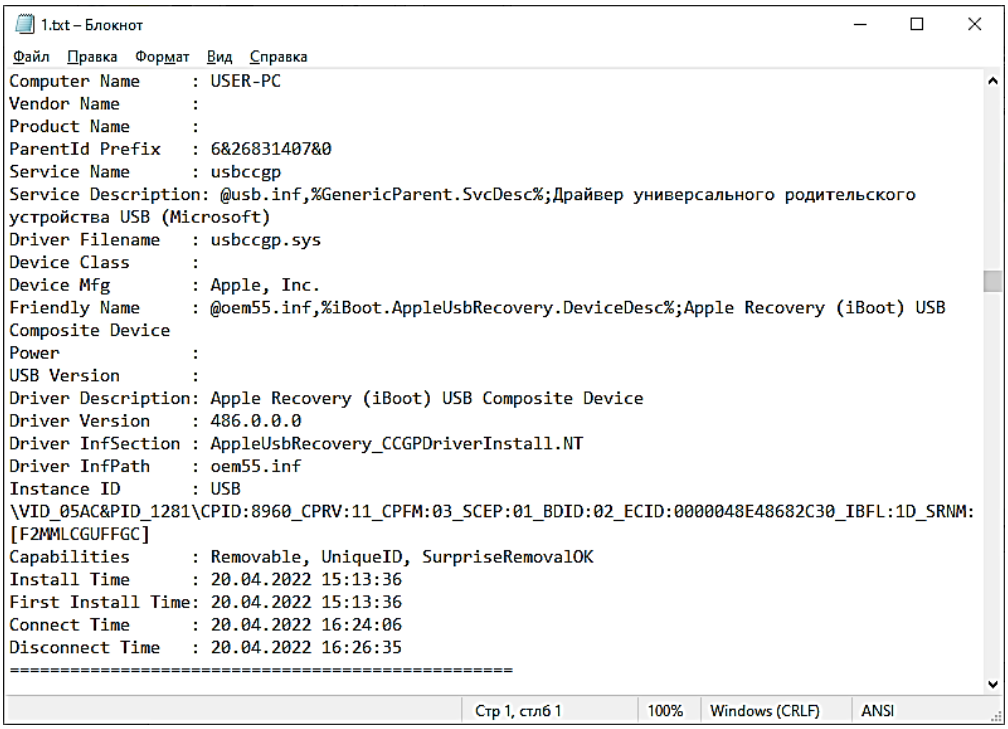
17.1. Задание повышенной трудности (самостоятельно).
Выгрузить результат в текстовый или табличный файл.



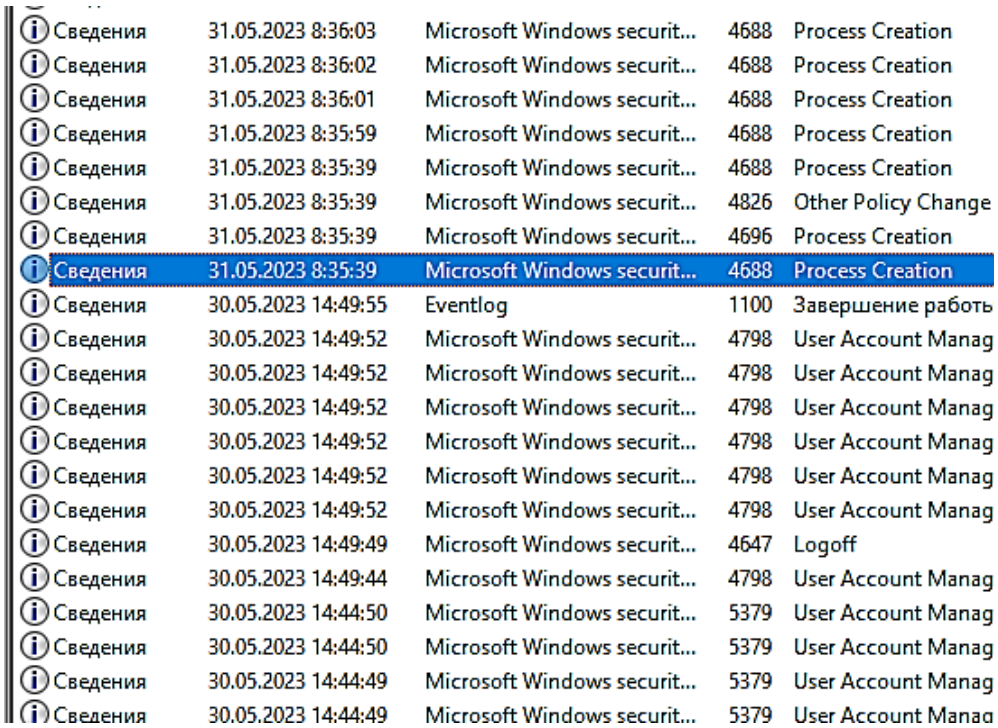
18. С помощью специализированного ПО USBDeview (пакет ПО NirLauncher) получить сведения о подключавшихся USB устройствах (серийный номер, имя, дата подключения, принтеры), используя раздел реестра System.



18.1. Задание повышенной трудности (самостоятельно).
Выгрузить результат в текстовый или табличный файл.



19. Открыть файлы журналов в стандартном приложении «Просмотр событий». Определить дату и время последнего включения ПК в соответствии с журналами работы.



Сведения	31.05.2023 8:36:03	Microsoft Windows securit...	4688	Process Creation
Сведения	31.05.2023 8:36:02	Microsoft Windows securit...	4688	Process Creation
Сведения	31.05.2023 8:36:01	Microsoft Windows securit...	4688	Process Creation
Сведения	31.05.2023 8:35:59	Microsoft Windows securit...	4688	Process Creation
Сведения	31.05.2023 8:35:39	Microsoft Windows securit...	4688	Process Creation
Сведения	31.05.2023 8:35:39	Microsoft Windows securit...	4826	Other Policy Change
Сведения	31.05.2023 8:35:39	Microsoft Windows securit...	4696	Process Creation
Сведения	31.05.2023 8:35:39	Microsoft Windows securit...	4688	Process Creation
Сведения	30.05.2023 14:49:55	Eventlog	1100	Завершение работы
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:52	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:49:49	Microsoft Windows securit...	4647	Logoff
Сведения	30.05.2023 14:49:44	Microsoft Windows securit...	4798	User Account Manag
Сведения	30.05.2023 14:44:50	Microsoft Windows securit...	5379	User Account Manag
Сведения	30.05.2023 14:44:50	Microsoft Windows securit...	5379	User Account Manag
Сведения	30.05.2023 14:44:49	Microsoft Windows securit...	5379	User Account Manag
Сведения	30.05.2023 14:44:49	Microsoft Windows securit...	5379	User Account Manag

20. Сделать вывод о проделанной работе, содержащий список обнаруженных сведения со ссылками на подтверждающие скриншоты.

Контрольные вопросы

1. Что такое черновое восстановление (восстановление по сигнатурам)?
2. Какое программное обеспечение позволяет восстанавливать удаленную информацию?
3. Опишите алгоритм подключения USB-накопителя с помощью ПАК «PC-3000» в режиме монтирования.
4. Какие интерфейсные разъемы для подключения исследуемых объектов имеет ПАК «PC-3000»?
5. Как заблокировать запись на исследуемом объекте, подключенном через ПАК «PC-3000» в режиме монтирования?
6. Какие разделы реестра просматриваются для определения данных о сетевых подключениях?
7. Какое программное обеспечение позволит получить информацию о сетевых подключениях на персональном компьютере?
8. В каком файле на персональном компьютере содержится информация о всех сетевых подключениях, в том числе о подключениях по локальной сети?
9. Какие разделы реестра просматриваются для определения данных о подключенных USB устройствах?
10. В каком каталоге находятся файлы реестра?
11. В каком каталоге находятся файлы журналов событий?
12. Какая криминалистически значимая информация может содержаться в реестре?
13. Какая криминалистически значимая информация может содержаться в журналах событий?
14. С помощью каких программных продуктов возможно получение информации из файлов реестра?
15. С помощью какого программного обеспечения можно экспортировать файлы реестра и файлы журналов событий?
16. В каком каталоге находятся файлы журналов событий?
17. Какой код события в журнале имеют сведения о входе в систему?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Баркалов Ю. М. Специальные знания, используемые при исследовании компьютерной информации : учебное пособие / Ю. М. Баркалов. – Воронеж : Воронежский институт МВД России, 2017. – 45 с.

2. Ионов В. Г. Программно-аппаратный комплекс «PC-3000» для востановления информации и ремонта накопителей на жестких магнитных дисках (НЖМД) / В. Г. Ионов // Сборник материалов XIV Всероссийской молодежной научно-инновационной школы, 2020. – С. 296–297.

3. Жуков М. М. Лабораторный практикум по дисциплине «Программно-аппаратные средства информационной безопасности» / М. М. Жуков, Ю. М. Баркалов. – Воронеж : Воронежский институт МВД РФ, 2022. – 90 с.

4. Джандарова Р. Р. Работа эксперта при исследовании HDD-дисков // Политехнический молодежный журнал. – 2018. – № 2 (19). – С. 43–47.

5. Программно-аппаратный комплекс PC-3000 Portable для начинающих. – URL: https://www.acelab.ru/dep.pc/products/PC-3000-informaciya-dlya-nachinayushchih.pdf

6. Программно-аппаратный комплекс PC-3000 Portable III. – URL: https://www.acelab.ru/dep.pc/pc-3000-portable-iii-systems.php.

7. Баркалов Ю. М. Подготовка экспертов по производству компьютерных судебных экспертиз : методические рекомендации / Ю. М. Баркалов. – Воронеж : Воронежский институт МВД России, 2013.

8. Методы анализа и восстановления данных с машинных носителей информации : практикум / М. М. Жуков, М. Ю. Баркалов, А. Ю. Телков. – Воронеж : Воронежский институт МВД РФ, 2021. – 67 с.

9. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей : учебное пособие / В. Ф. Васюков, Б. Я. Гаврилов, А. А. Кузнецов [и др.]; под общ. ред. Б. Я. Гаврилова. – Моспект : Проспект, 2017. – 160 с.

10. Баркалов Ю. М. Организационно-техническое обеспечение специальных мероприятий / Ю. М. Баркалов, О. И. Нестеровский, Д. Ю. Лиходедов. – Воронеж : Воронежский институт МВД России, 2016.

Учебное издание

Дмитрий Игоревич Полухин;
Михаил Михайлович Жуков,
кандидат технических наук, доцент

АНАЛИЗ И ВОССТАНОВЛЕНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Практикум

Редактор А. Г. Лиопа
Компьютерная верстка Д. И. Полухина

Подписано в печать 30.10.2024
Формат 60×84 1/16
Усл. печ. л. 15,69
Тираж 50 экз.
Заказ № 136

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53