Программное восстановление файлов на Linux, Android и Windows

Владимир

Восстановление файлов нужно не только «**Криминалистам**», но и обыкновенным «**Пользователям**». Электронные носители «**Информации**» распространены повсеместно и каждый сталкивается с проблемой «**Повреждения**» или случайного «**Удаления**» файлов. Вернуть «**Информацию**» можно «**Аппаратным**» или «**Программным**» путем. Методика восстановления «**Аппаратным**» способом имеет особенности для каждого оборудования и требует специальных приборов. «**Программный**» же способ доступен каждому.

В результате восстановления «**Данных**» любым способом, далеко не всегда удается их успешно прочитать. Чаще всего получается восстановить только поврежденную «**Структуру**» файла, но не «**Данные**». Учитывая, что вся «**Информация**» имеет свой стандарт «**Кодировки**» и «**Структуры**», все равно, есть шанс восстановить части файла вручную. Для этого необходимо знать файл какого типа поврежден, изучить «**Структуру**» его «**Заголовка**» и заменить ее на корректную. Но это работает не всегда. Для «**Шифрованных**» или «**Сжатых**» файлов удастся восстановить только независимые блоки «**Данных**».

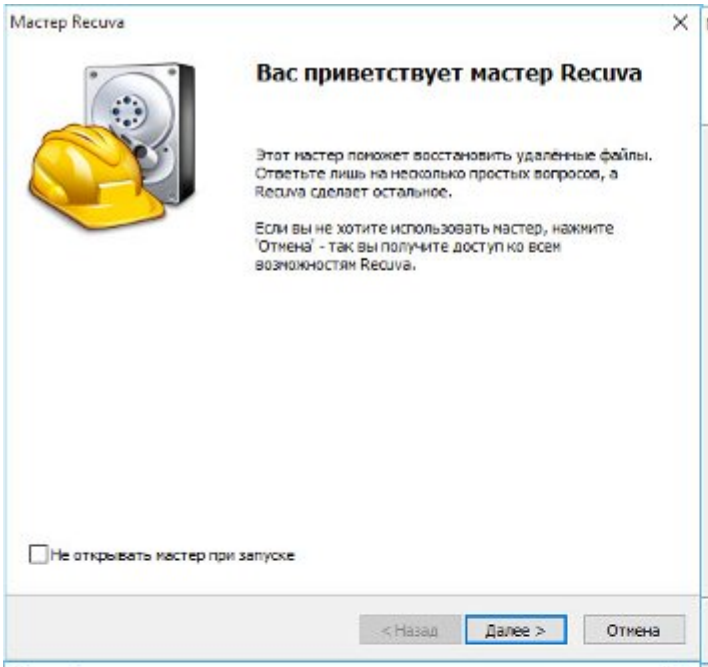
Файлы имеют «**Заголовок**» или "шапку", поэтому необходимо найти корректный «**Заголовок**» файла. Его можно скопировать из рабочего однотипного файла. Он должен быть большего размера, чем исходный. Изучив «**Заголовок**», необходимо определить его длину и положение, чтобы произвести корректное копирование. После этого можно запустить файл, желательно, использовать программы, которые способы читать «**Поврежденные**» и «**Недокаченные**» файлы. Если видно или слышится некорректное изображение или звучание, «**Данные**» после заголовка нужно смещать по одному «**Биту**» до тех пор, пока не будут слышны или видны неповрежденные участки данных.

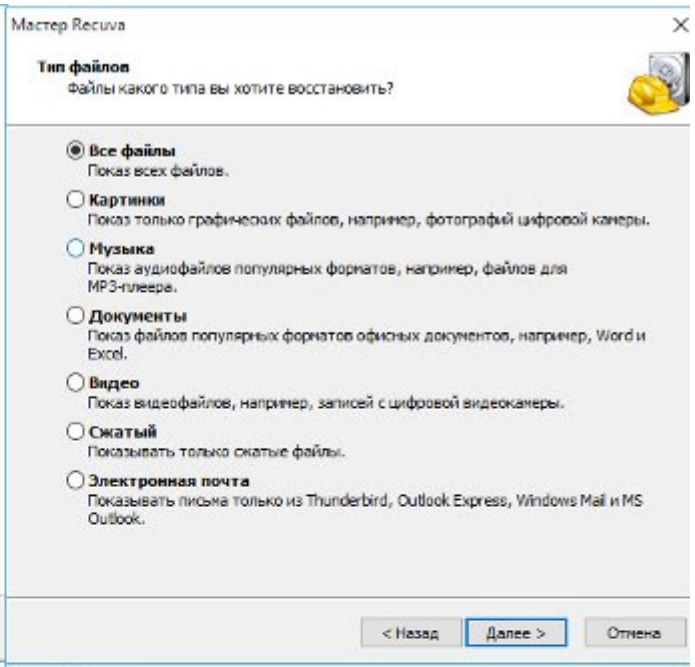
Также, стоит отметить, что возможны ситуации, когда «**Данные**» просто не были записаны на носитель «**Информации**». Поэтому важно, если это записывающий «**Съемный носитель**» или другое устройство, проверять наличие таковой «**Записи**». Это можно сделать путем сверки «**Индикации**». Но возможны сбои устройства, которые приводят к остановке «**Записи**», даже при наличии «**Индикации**». Поэтому, проверяйте присутствие последних «**Записей**» в меню устройства, например, по «**Дате**». Рекомендуется делать это при каждом повторном использовании устройства или периодично.

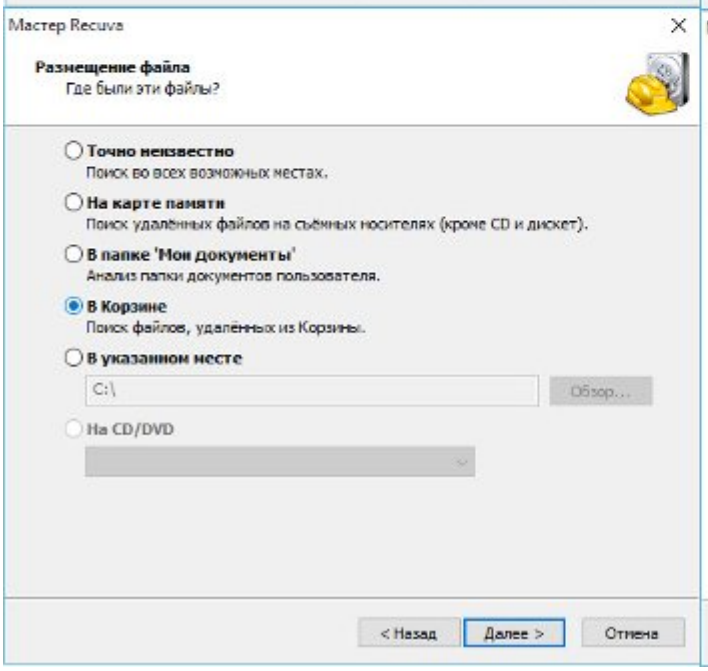
Причины, по которым это может произойти различны: «**Сбой электроники**», «**Электромагнитные помехи**», в том числе, преднамеренные и

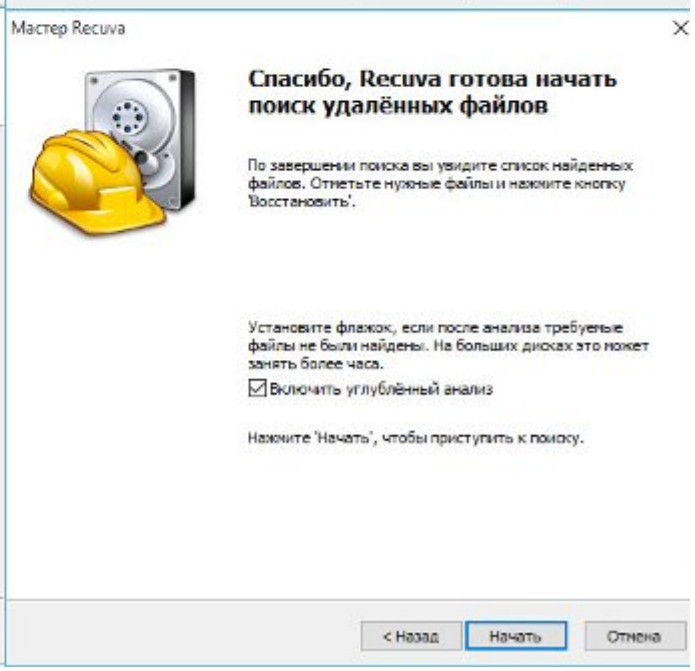
выводящие из строя оборудование, «**Старое оборудование**» ,«**Дистанционное использование закладки**» в устройстве для отключения записи на носитель (такое есть в большом количестве устройств, к сожалению) и др. Размещать устройства лучше в изолированном от внешнего мира помещении и обязательно вести «**Журналирование**». Если возможно организовать безопасный канал, то логи «**Журнала**» стоит передавать по нему постоянно.

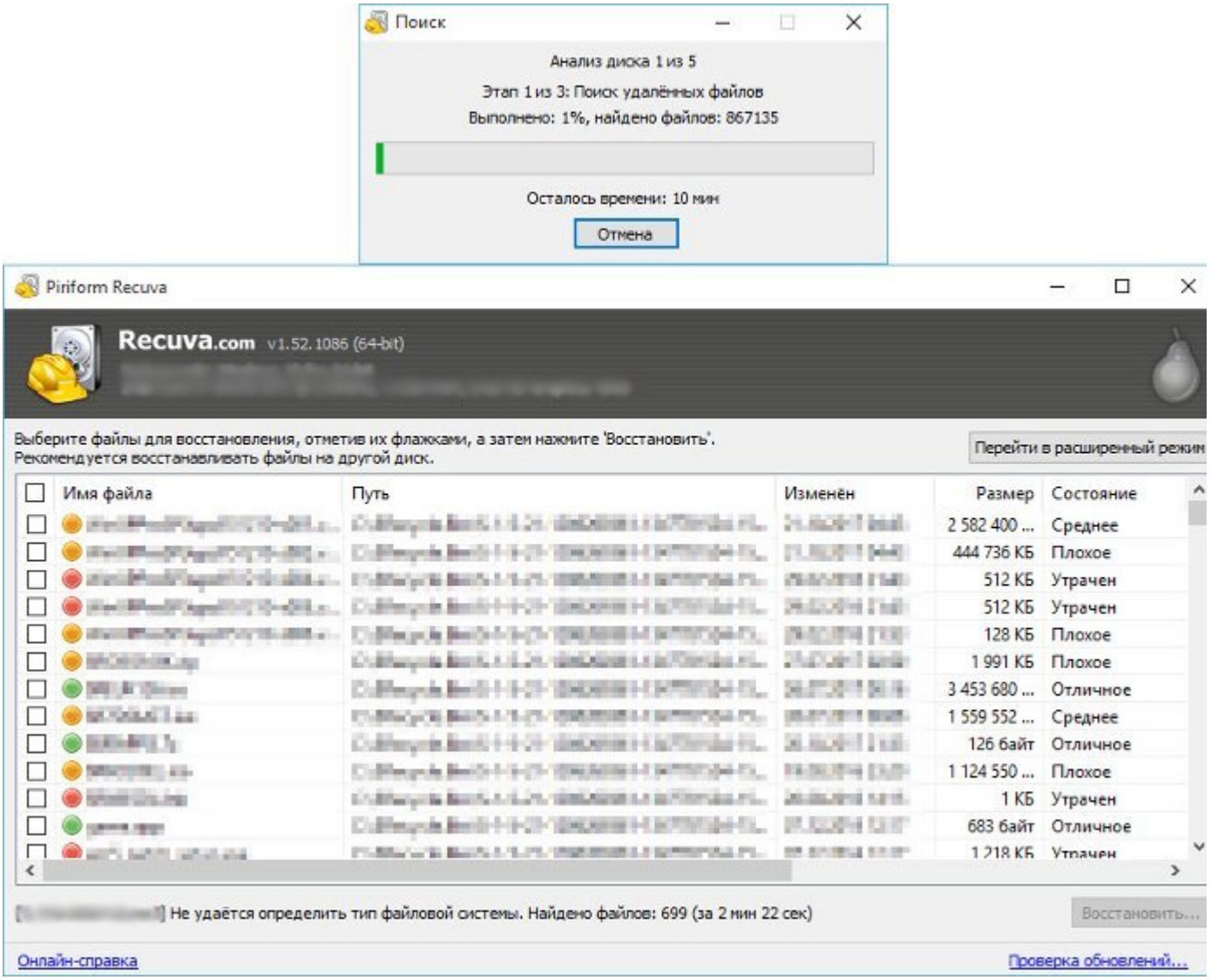
Приступим непосредственно к работе с программами восстановления файлов. «**Recuva**» при запуске открывает «**Мастер восстановления**», благодаря которому легко сконфигурировать настройки процедуры восстановления. Использование программы очень просто. Но стоит отметить один ньюанс: по умолчанию «**Recuva**» восстанавливает только удаленные файлы. Для того, чтобы включить режим «**Поиск не удаленных файлов (восстановление с поврежденного носителя)**», нужно после поиска по «**Мастеру восстановления**», в окне, где отображены результаты поиска, нажать «**Перейти в расширенный режим**».


Мастер Recuva
Вас приветствует мастер Recuva
Этот мастер поможет восстановить удаленные файлы. Ответьте лишь на несколько простых вопросов, а Recuva сделает остальное.
Если вы не хотите использовать мастер, нажмите 'Отмена' - так вы получите доступ ко всем возможностям Recuva.
Не открывать мастер при запуске
< Назад
Далее >
Отмена

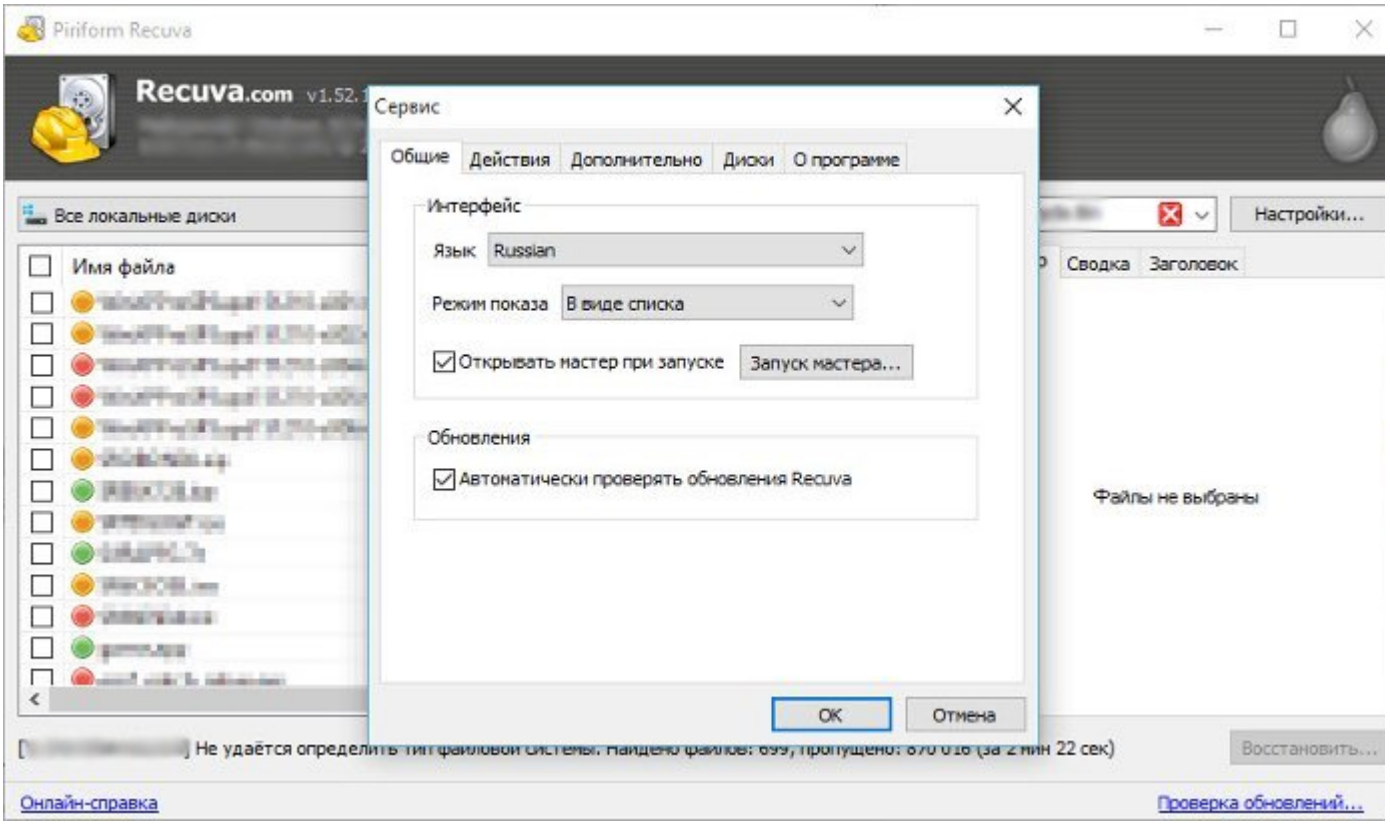

Мастер Recuva
Тип файлов
Файлы какого типа вы хотите восстановить?
Все файлы
Показ всех файлов.
Картинки
Показ только графических файлов, например, фотографий цифровой камеры.
Музыка
Показ аудиофайлов популярных форматов, например, файлов для MP3-плеера.
Документы
Показ файлов популярных форматов офисных документов, например, Word и Excel.
Видео
Показ видеофайлов, например, записей с цифровой видеокамеры.
Сжатый
Показывать только сжатые файлы.
Электронная почта
Показывать письма только из Thunderbird, Outlook Express, Windows Mail и MS Outlook.
< Назад
Далее >
Отмена

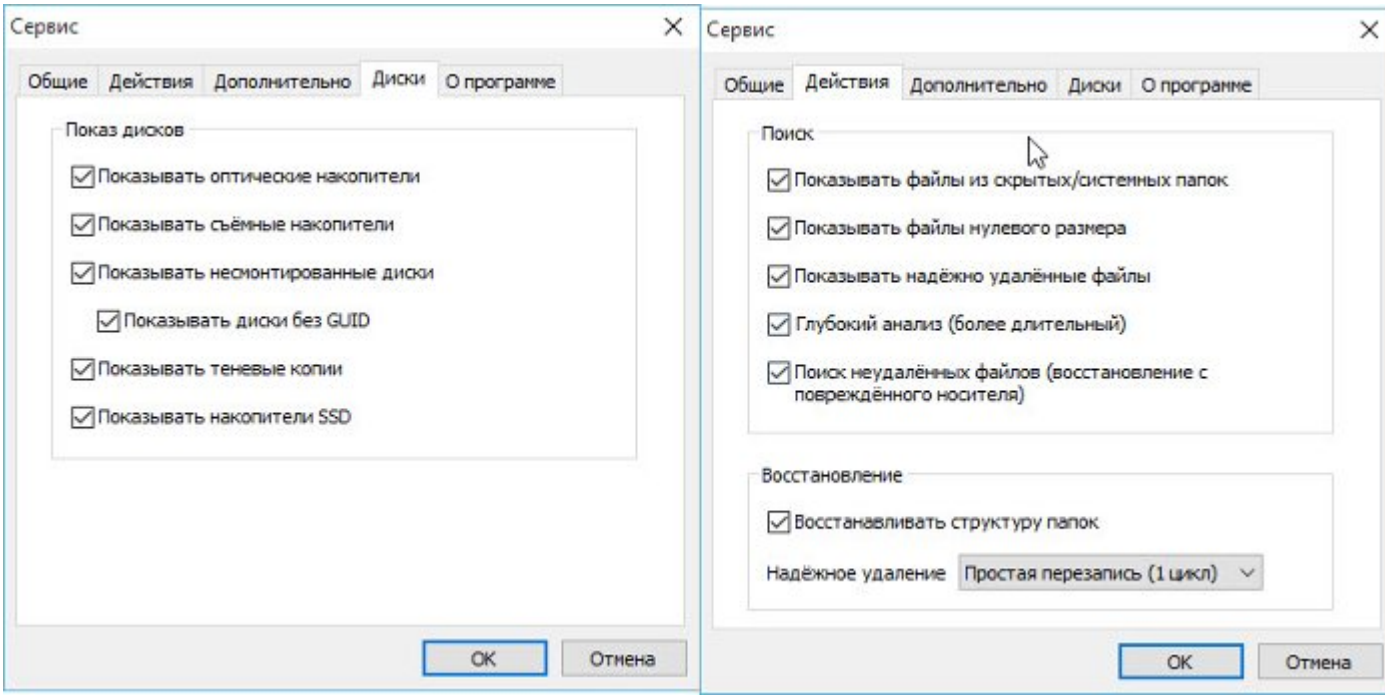

Мастер Recuva
Размещение файла
Где были эти файлы?
Точно неизвестно
Поиск во всех возможных местах.
На карте памяти
Поиск удалённых файлов на съёмных носителях (кроме CD и дискет).
В папке 'Мои документы'
Анализ папки документов пользователя.
В Корзине
Поиск файлов, удалённых из Корзины.
В указанном месте
C:\
Обзор...
На CD/DVD
< Назад
Далее >
Отмена


Мастер Recuva
Спасибо, Recuva готова начать поиск удалённых файлов
По завершении поиска вы увидите список найденных файлов. Отметьте нужные файлы и нажмите кнопку 'Восстановить'.
Установите флажок, если после анализа требуемые файлы не были найдены. На больших дисках это может занять более часа.
Включить углублённый анализ
Нажмите 'Начать', чтобы приступить к поиску.
< Назад
Начать
Отмена



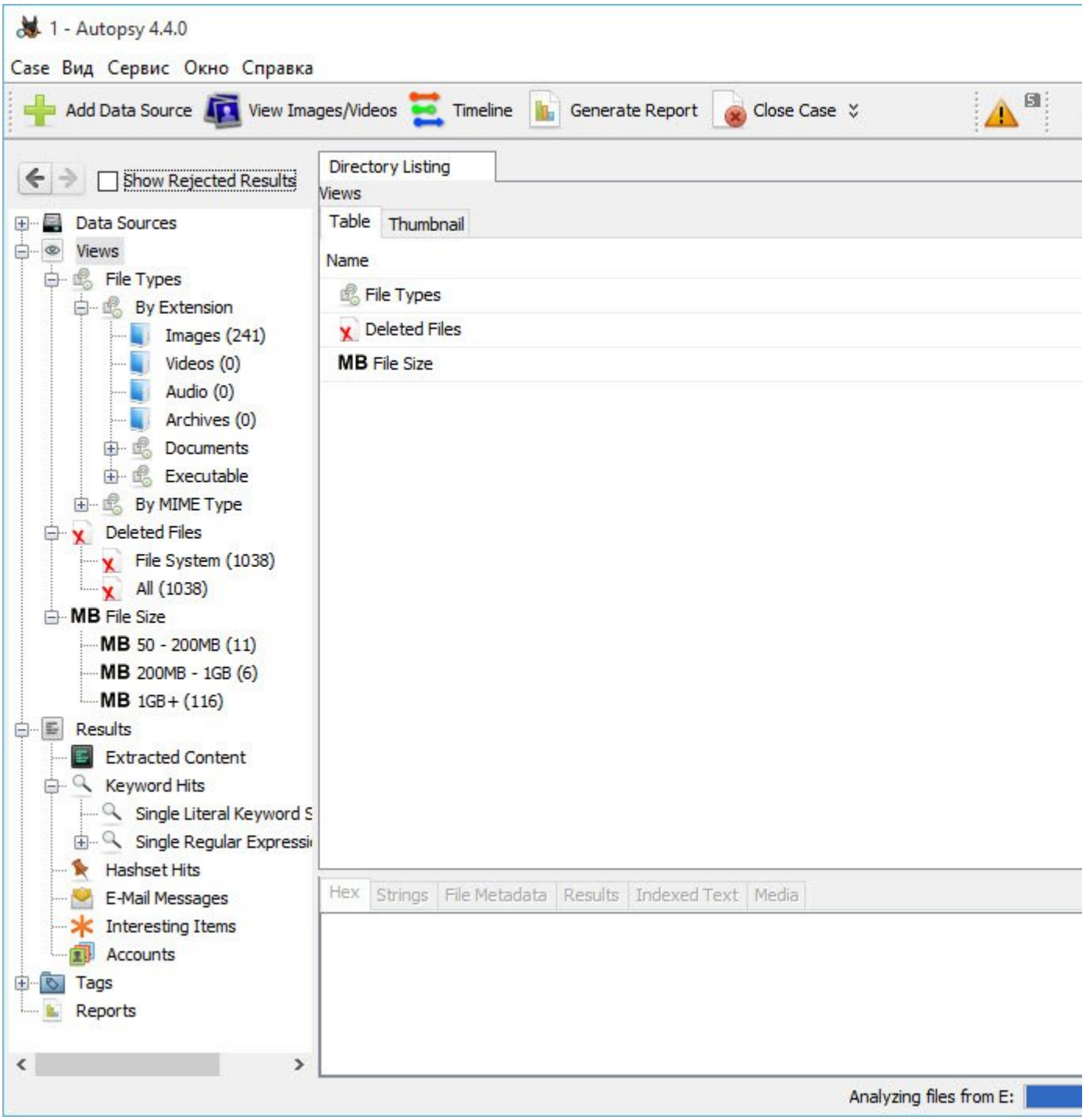
После перехода в расширенных режим, появится кнопка «**Настройки**», по ее нажатию откроется «**Сервис**». В данном окне необходимо проверить, чтобы были установлены все галки во вкладке «**Диски**» и «**Действия**». Затем провести повторный поиск из окна результатов, нажав кнопку «**Анализ**».
Программа «**Recuva**» способна восстанавливать «**Системные диски**» и «**Съемные носители**».





Существует более профессиональная программа анализа различных носителей «**Информации**» и «**Побитовых копий**» «**Жестких дисков**» и «**ОЗУ**». У программы «**Autopsy**» есть версии, как для «**Windows**» так и для «**Linux**». Но рекомендуется использовать версию для «**Windows**», потому что она имеет более удобный способ представления «**Информации**» для анализа конечному «**Пользователю**». Кроме восстановление и анализа удаленных файлов, программа способна «**Классифицировать**» огромное количество типов файлов, выделить из них «**Важные**» и «**Подозрительные**» файлы с аномальными характеристиками. Кроме этого, программа способна упорядочить все файлы в «**Timeline**», другими словами, показать историю работы на компьютере с «**Информацией**» и все

проделанные операции.



Для того, чтобы иметь возможность создания «**Побитовых копий**» рекомендуется иметь переходник с «**Системных разъемов**» дисков на универсальный «**USB**», например, «[USB 3.0 to HardDisk]». Для создания «**Побитовых копий ОЗУ**» или машин, которые нельзя выключать, вносить изменения, рекомендуется использовать «[Caine Linux]».


USB3.0 TO IDE/SATA
USB3.0 TO IDE/SATA


caine's Home
Keyboard changer
BlockOn/Off
Mixed scripts
win
Caja (root)
Network
Disk Image Mounter
Systemback (installer)
Firefox Web Browser
XAll 1.5
Guymager
INFO
QUANTUM
CAINE
Computer Aided INvestigative Environment
en
Tue 24 Oct, 20:51
31 B/s
31 B/s