**[Лабораторная работа №5. Восстановление данных.](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html)**

* + [**Основные теоретические сведения**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#id1)
    - [**Восстановление данных TestDisk**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#testdisk)
    - [**Восстановление данных PhotoRec**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#photorec)
    - [**Восстановление данных Extundelete**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#extundelete)
    - [**Восстановление данных Foremost.**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#foremost)
  + [**Задания к лабораторной работе**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#id2)
  + [**Вопросы к лабораторной работе**](https://xn--80aqobguv5e.xn--p1ai/%D0%BE%D0%B8%D0%B1/lr5.html#id3)

**Лабораторная работа №5. Восстановление данных.**

**Основные теоретические сведения**

**Цель:** Получение теоритических и практических навыков программного восстановления данных.

**Восстановление данных TestDisk**

**TestDisk** — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (например, потеря MBR).

* Установка **<sudo apt-get install testdisk>**.
* Запускаем TestDisk **<sudo testdisk>**.
* Появляется окошко приветствия TestDisk, нам предлагается вести лог работы (для выполнения данной работы лог не требуется).
* Выбираем нужный диск и нажимаем **Enter**.
* Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем **Enter**.
* Выбираем **Analise**.
* Выбираем **QuickSearch**.
* Нам выводят таблицу разделов. Выбираем раздел и нажимаем **P**, чтобы вывести список файлов.
* Выбираем файлы для восстановления и нажимаем **C**.
* Выбираем папку, куда будут сохранены файлы и нажимаем **C**.

**Восстановление данных PhotoRec**

**PhotoRec** - это утилита, входящая в состав пакета TestDisk. Предназначена для восстановления испорченных файлов с карт памяти цифровых фотоаппаратов (CompactFlash, Secure Digital, SmartMedia, Memory Stick, Microdrive, MMC), USB flash-дисков, жестких дисков и CD/DVD. Восстанавливает файлы большинства распространенных графических форматов, включая JPEG, аудио-файлы, включая MP3, файлы документов в форматах Microsoft Office, PDF и HTML, а также архивы, включая ZIP. Может работать с файловыми системами ext2, ext3, ext4 FAT, NTFS и HFS+, причем способна восстановить графические файлы даже в том случае, когда файловая система повреждена или отформатирована.

* Установка **<sudo apt-get install testdisk>**.
* Запускаем PhotoRec **<sudo photorec>**.
* Выбираем нужный диск и нажимаем **Enter**.
* В нижнем меню можно выбрать **File Opt**, чтобы выбрать типы файлов для восстановления (по умолчанию выбраны все).
* Чтобы начать восстановление нажмите **Enter**, выбрав **Search**.
* У нас выбрана система ext4, поэтому выбираем первый вариант [ ext2/ext3 ].
* Если выбрать пункт **FREE**, то поиск будет произведен в пустом пространстве и в этом случае будут восстановлены только удаленные файлы, а если выбрать **WHOLE**, то поиск будет произведен на всем диске.
* Теперь нужно указать директорию, куда будем сохранять нужные нам файлы. Выбираем нужную папку и нажимаем **С**.
* Выбираем файлы для восстановления и нажимаем **C**.

**Восстановление данных Extundelete**

**Extundelete** – утилита, позволяющая восстанавливать файлы, которые были удалены с разделов ext3/ext4.

* Установка: **<sudo apt-get install extundelete>**.
* Как только вы поняли, что удалили нужные файлы, необходимо отмонтировать раздел: **<umount /dev/<partition> >**
* Зайдите в каталог, в который будут восстанавливаться удаленные данные. Он должен быть расположен на разделе отличном от того, на котором хранились восстанавливаемые данные: **cd /<путь\_к\_каталогу\_куда\_восстанавливать\_данные>**
* Запустите **extundelete**, указав раздел, с которого будет происходить восстановление и файл, который необходимо восстановить: **sudo extundelete /dev/<partition> –restore-file /<путь к файлу>/<имя\_файла>**
* Можно так же восстанавливать содержимое каталогов: **sudo extundelete /dev/<partition> –restore-directory /<путь\_к\_директории>**

**Восстановление данных Foremost.**

**Foremost** - консольная программа, позволяющая искать файлы на дисках или их образах по hex-данным, характерным заголовкам и окончаниям. Программа проверяет файлы на предмет совпадения заранее определённых hex-кодов (сигнатур), соответствующих наиболее распространённым форматам файлов. После чего экстрагирует их из диска/образа и складывает в каталог, вместе с подробным отчётом о том, чего, сколько и откуда было восстановлено. Типы файлов, которые foremost может сразу восстановить: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp. Есть возможность добавлять свои форматы (в конфигурационном файле /etc/foremost.conf), о которых программа не знает.

* Установка: **<sudo apt-get install foremost>**
* Пример использования для восстановления изображений с диска **/dev/sdb** в каталог **~/out\_dir**: **<sudo foremost -t jpg,gif,png,bmp -i /dev/sdb -o ~/out\_dir>**

**Задания к лабораторной работе**

* Добавьте в виртуальную машину виртуальный жесткий диск.
* Запустите виртуальную машину с Linux.
* Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами.
* Отформатируйте созданные разделы в файловую систему ext4.
* Установите TestDisk.
* Удалите MBR (или таблицу разделов) с помощью команды DD.
* Восстановите MBR (или таблицу разделов) с помощью TestDisk.
* Смонтируйте восстановленные разделы и создайте там произвольные файлы.
* Удалите созданные файлы.
* С помощью TestDisk восстановите данные.
* Создайте произвольный каталог и запишите туда данные каталога /var/log/ .
* Удалите данные с созданного каталога.
* С помощью PhotoRec восстановите данные.
* Создайте произвольный каталог и запишите туда данные каталога /etc/ .
* С помощью Extundelete или Foremost восстановите данные.

**Вопросы к лабораторной работе**

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?
2. Какие файловые системы поддерживает PhotoRec?
3. Какие форматы поддерживает PhotoRec?
4. Как Foremost восстанавливает файлы?
5. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?
6. Все ли данные скопированные с каталога /var/log/ восстановились?
7. Все ли данные скопированные с каталога /etc/ восстановились?

**Составьте отчет о выполнении лабораторной работы.**

**Включите в него копии экрана и ответы на вопросы лабораторной работы.**