Выполнил: Серебряков Алексей 431

# Планы проведения практического занятия по теме «Архитектура и криминалистически значимые элементы файловых систем Ext2fs, Ext3fs»

***Вопросы занятия:***

1. Создание файловой системы и основные операции с файлами

2. Изучение состояния и динамики файловой системы.

3. Изучение возможности восстановления информации в файловых системах extXfs

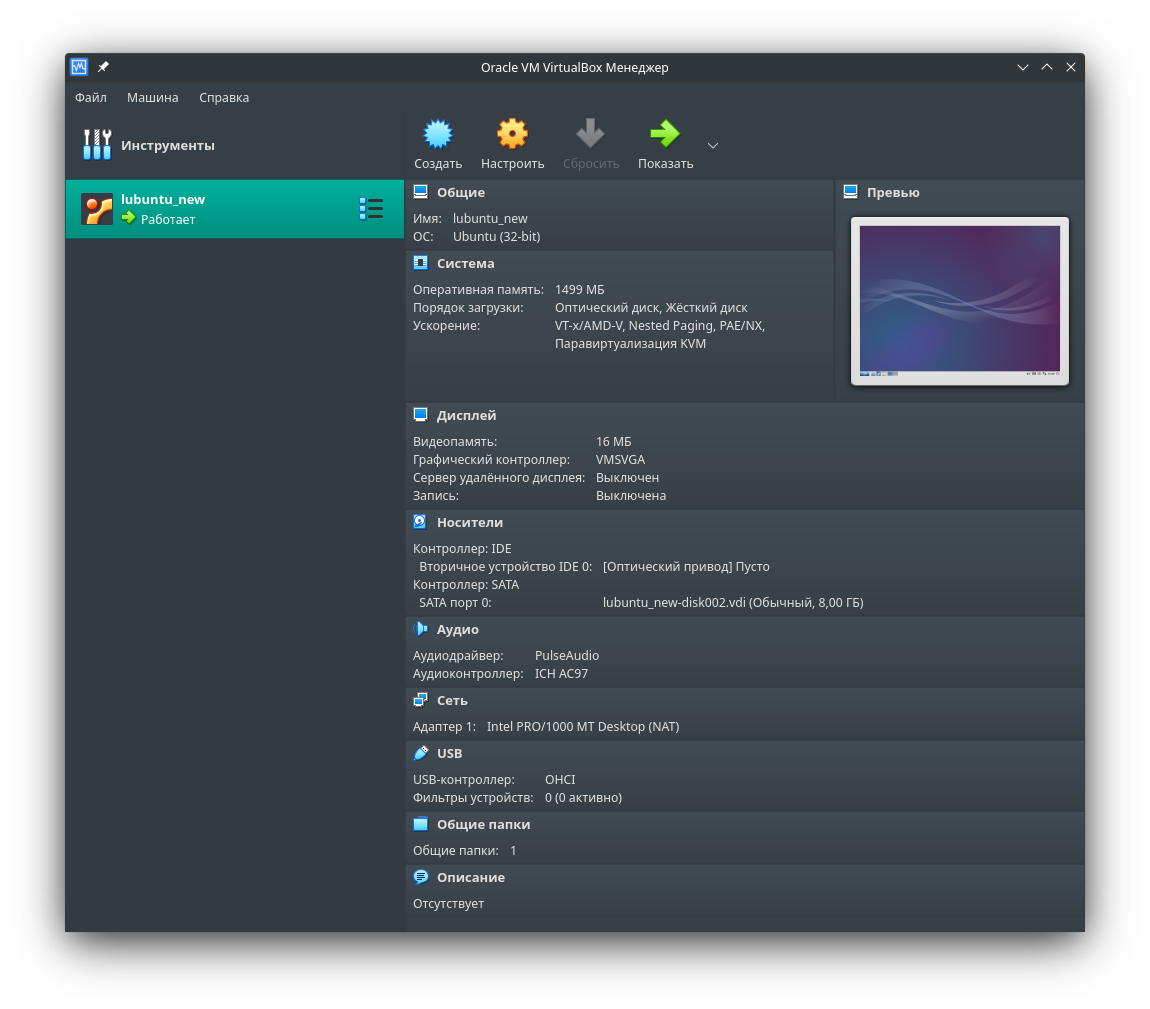
**Используемые материалы и средства** (инструментальные средства)**:**

1. Компьютерный класс.
2. Virtual Box.
3. Linux
4. Редактор диска lde.

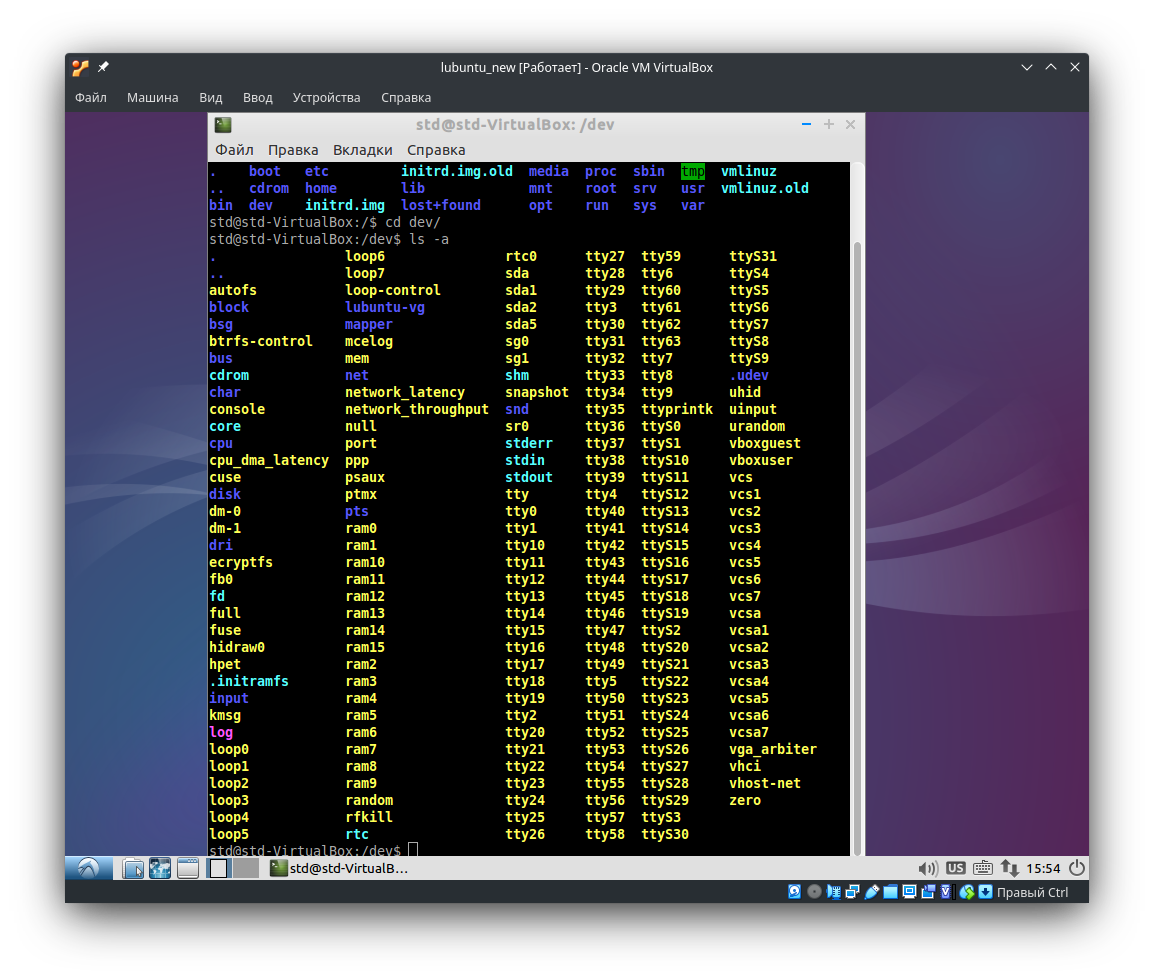
Содержание занятия.

***Вопрос 1.* Создание файловой системы и основные операции с файлами**

1. Загрузить ОС представленной виртуальной машины (используйте пару логин: std, пароль:123456)



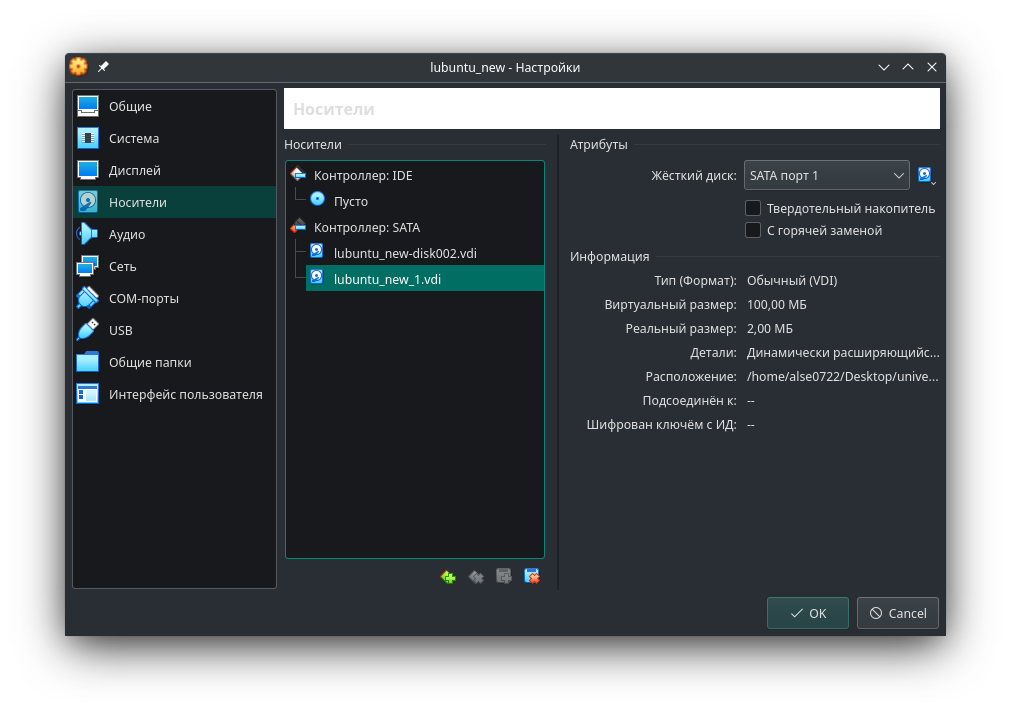
1. Выписать все файлы-устройства из каталога dev, отвечающие за устройства внешней памяти на жестких магнитных дисках (/dev/sda\*, /dev/sdb\*…)



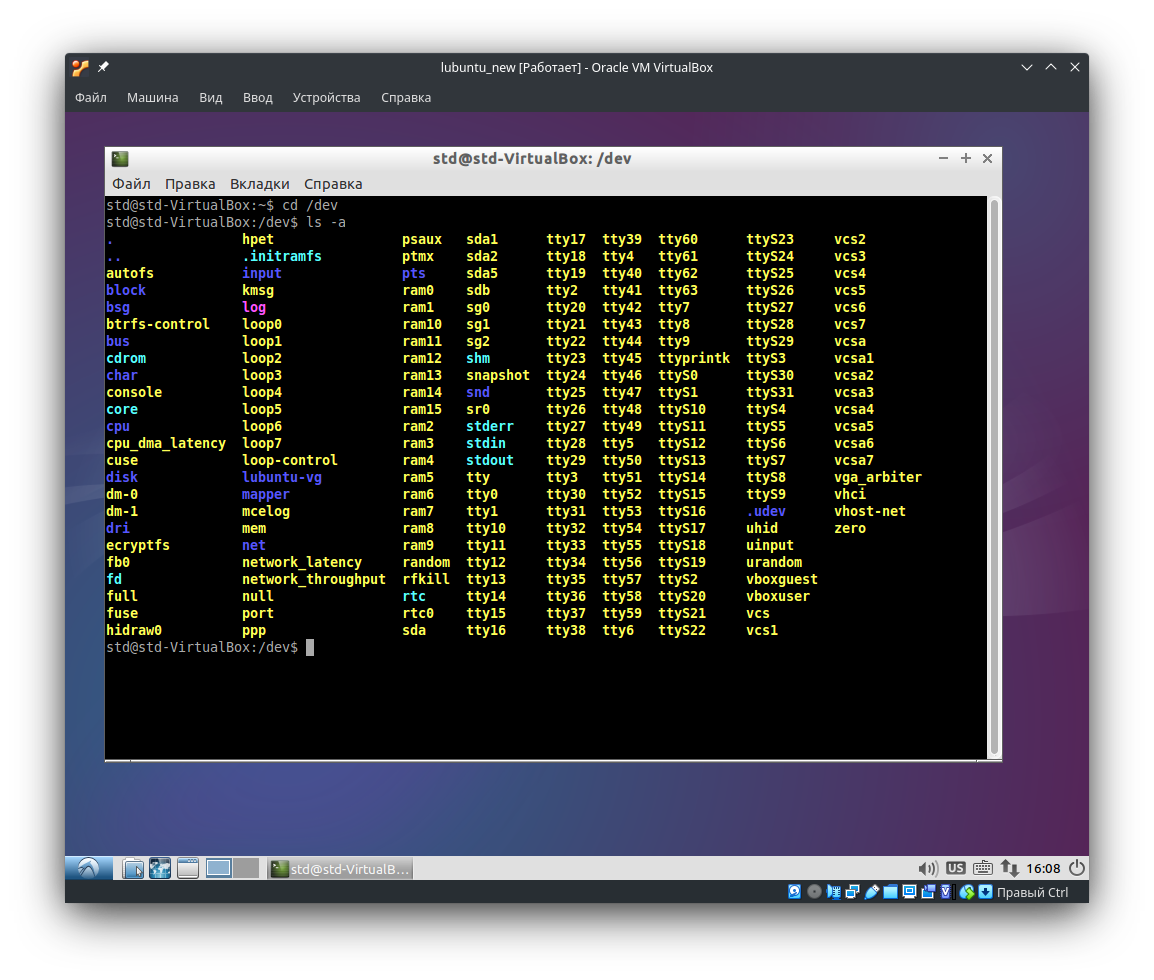
1. Завершить сеанс работы с ОС Linux в виртуальной машине

Сделано.

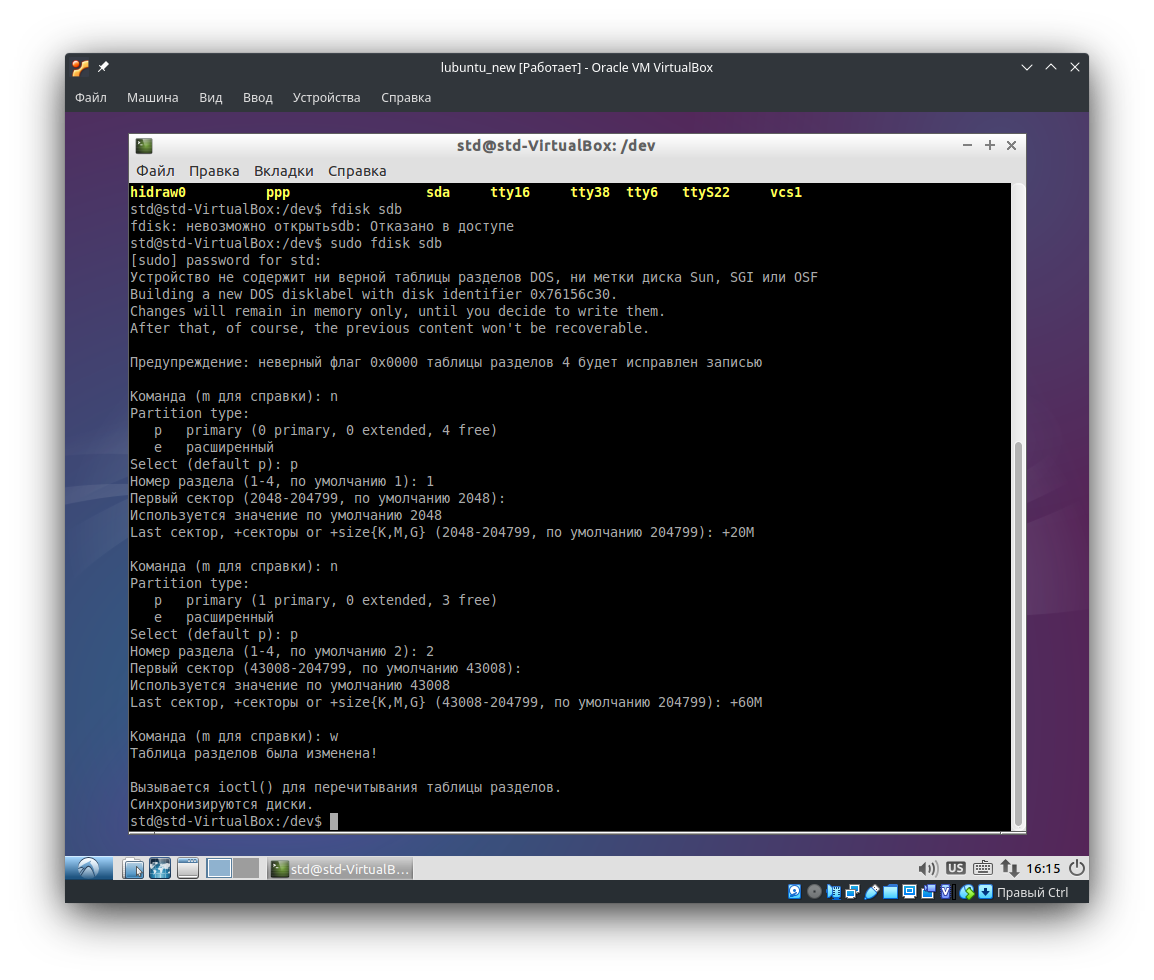
1. Добавить в конфигурацию виртуальный НЖМД размеров 100 Mb



1. Загрузить ОС виртуальной машины и найти изменения в перечне файлов-устройств, отвечающих за устройства внешней памяти на жестких магнитных дисках (/dev/sda\*, dev/sdb\*)

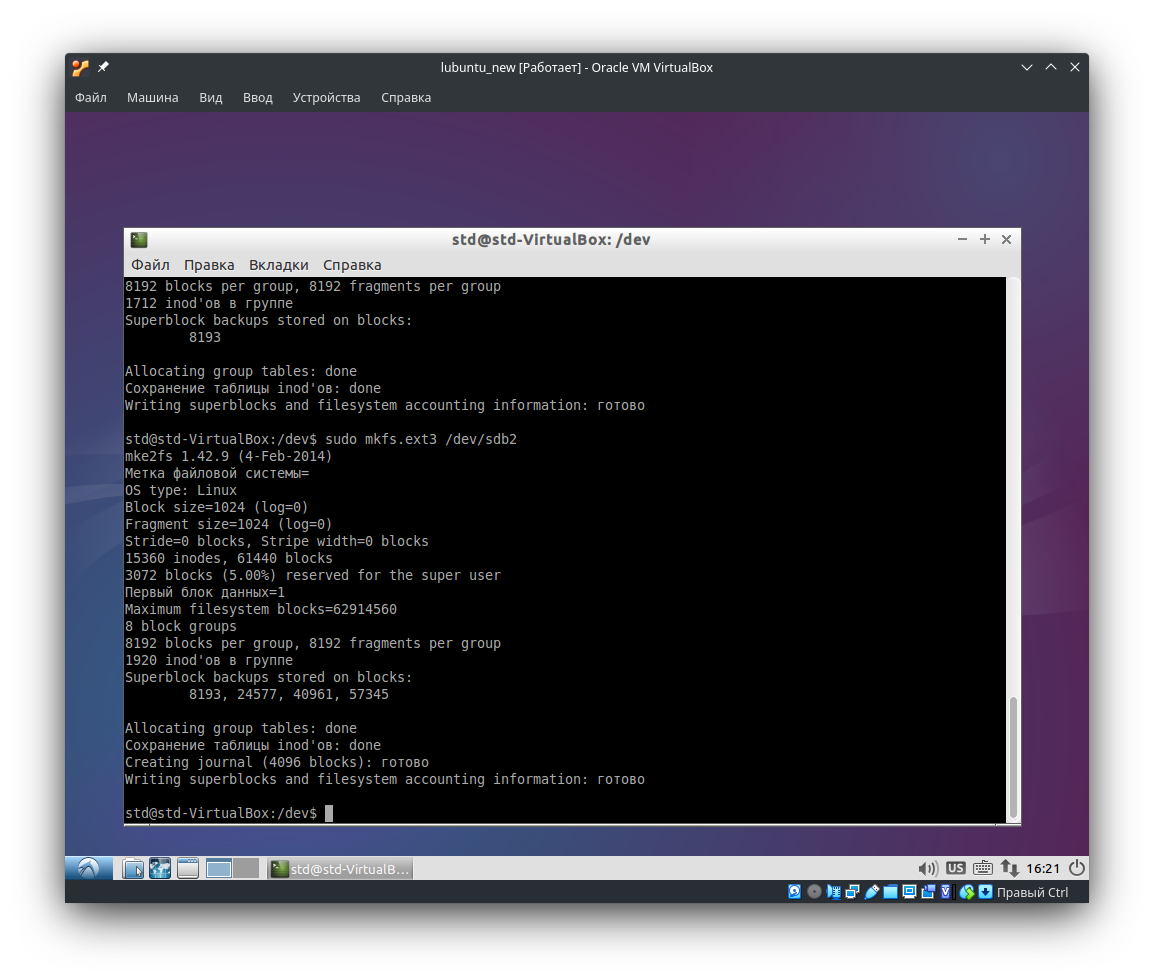
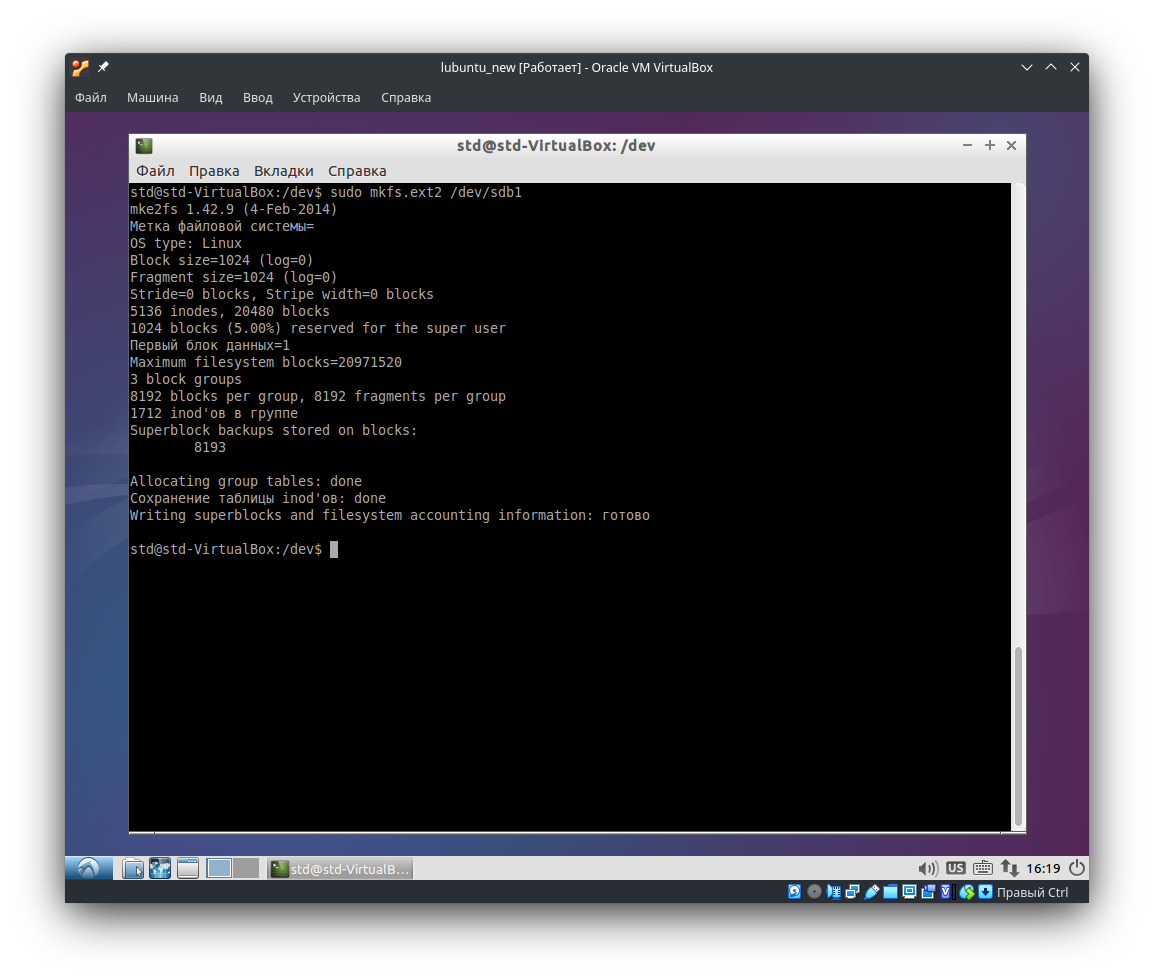


1. На обнаруженном новом устройстве создать два раздела: первый объемом 60 Mb в формате ext2fs, второй – объемом 20 Mb в формате ext3fs.



Для совершения операций установите права доступа суперпользователя sudo su и введите пароль текущего пользователя.

Далее используйте программу fdisk имя\_устройства и команды mkfs.ext2 имя\_раздела и mkfs.ext3 имя\_раздела соответственно.

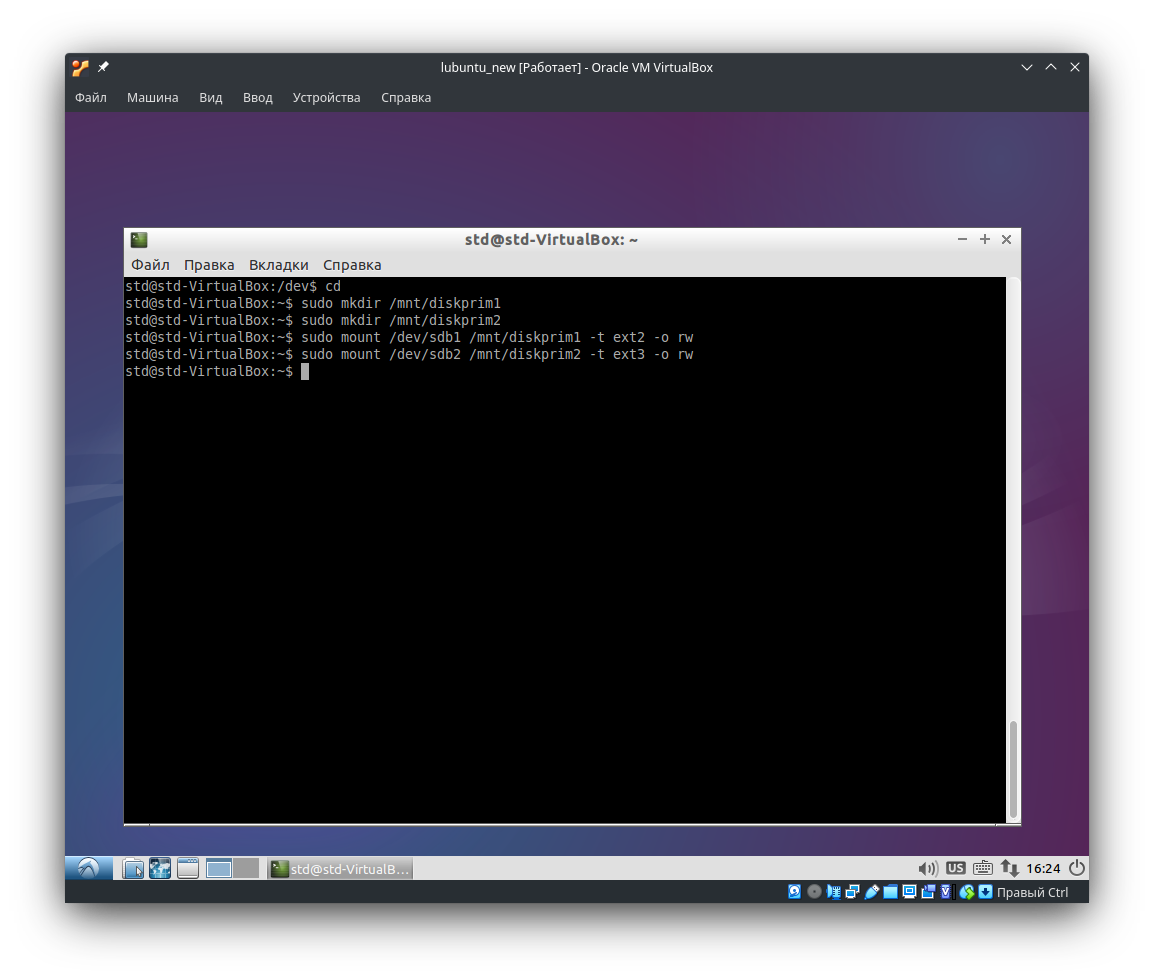


В каталоге MNT создать каталоги с именами diskprim1 и diskprim2 cмонтировать на них созданные разделы.

Для этого используйте команды:

mount имя\_устройства /mnt/diskprim1 –t ext2 –o rw

mount имя\_устройства /mnt/diskprim2 –t ext3 –o rw

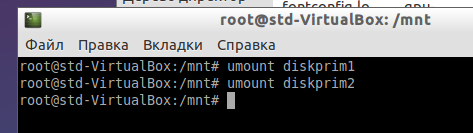


1. Скопировать в каждый раздел по несколько (10-20) файлов разного размера, например из каталога /var/log.

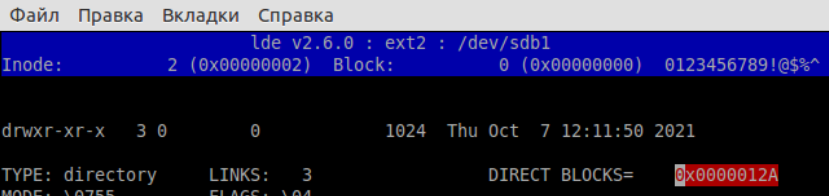


***Вопрос 2.* Изучение состояния и динамики файловой системы**

1. Отмонтируйте разделы на каталогах diskprim1 и diskprim2.

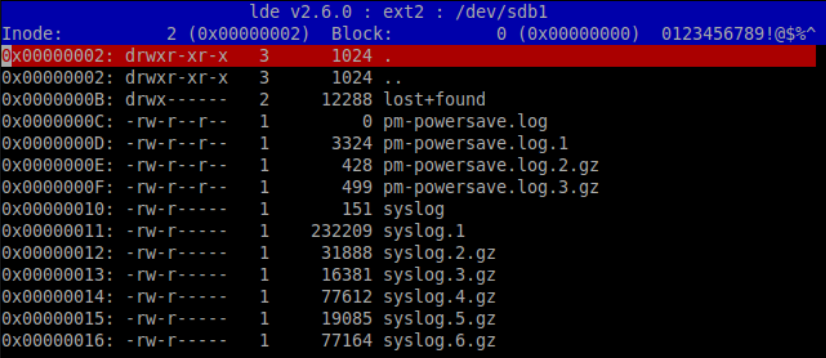


1. Используя редактор lde откройте просмотр первого раздела дополнительного диска. найдите inode корневого каталога. Ответить на вопросы: какой номер этого inode? - 2

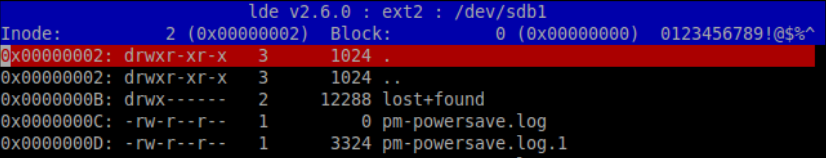


Inode number - 0x00000002

1. Установите просмотр этого файла как каталога и выберите любой файл. Просмотрите его inode. Выберу pm-powersave.log.1. Его inode – 13 (0x0000000D).



1. Определить какое имя имеет файл, зарегистрированный с inode 12. Это pm-powersave.log (0x0000000C)



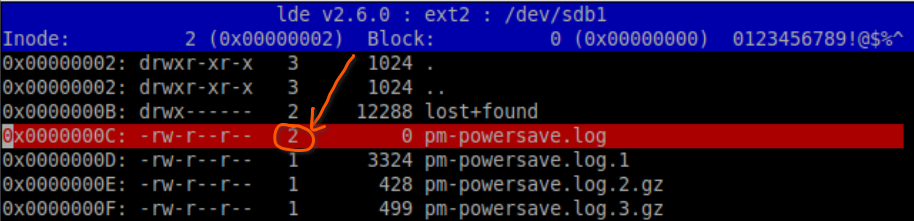
Также просматривая этот inode в режиме дампа (<SHIFT-B>), найдите имя интересующего файла, и, отсчитывая от его первой буквы влево 8 позиций, убедитесь, что там прописан номер inode этого файла.



1. Выйти из lde и создать жесткую ссылку используя в качестве исходного имени имя установленного файла. Используйте для этого команду ln



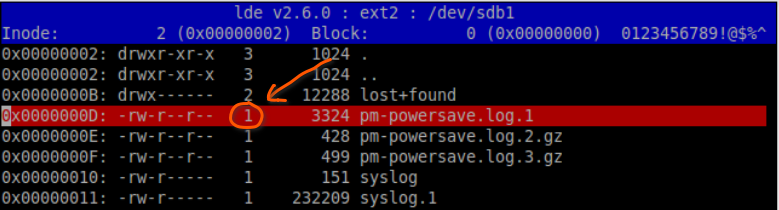
1. Используя редактор lde просмотреть inode 12. Обратить внимание на количество жестких ссылок на это файл.



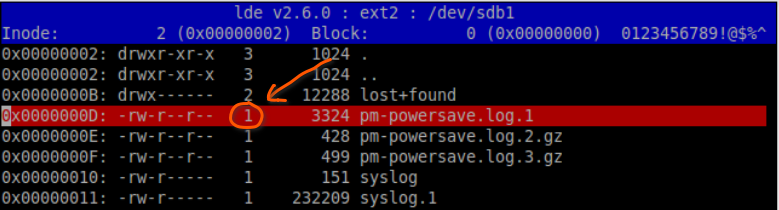
1. Выйти из lde и удалить одно из имен исследуемого файла.



1. Используя редактор lde просмотреть inode 12. Обратить внимание на количество жестких ссылок на это файл.



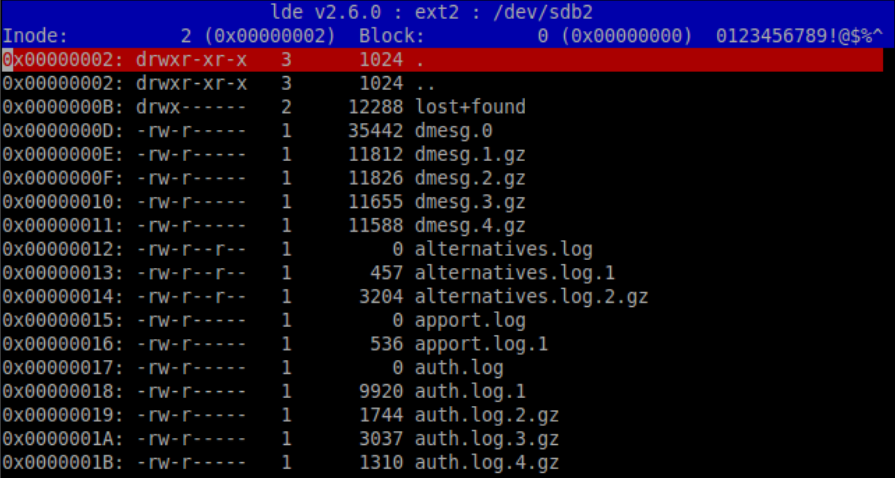
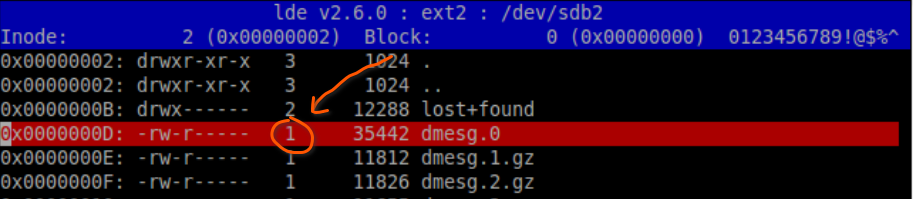
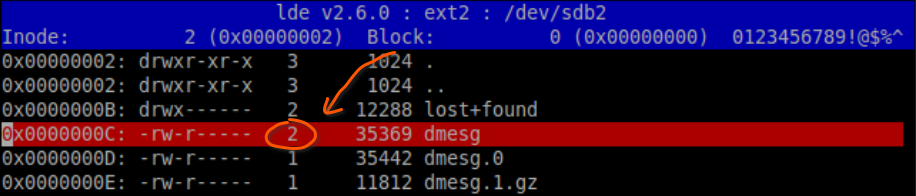
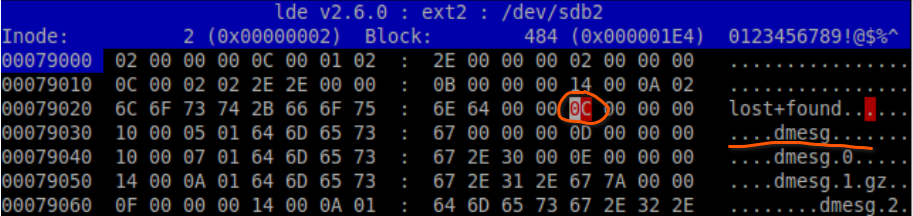
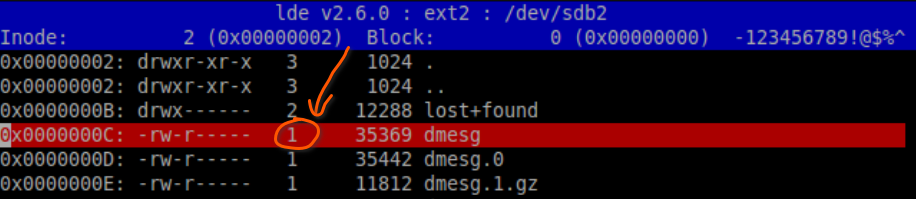
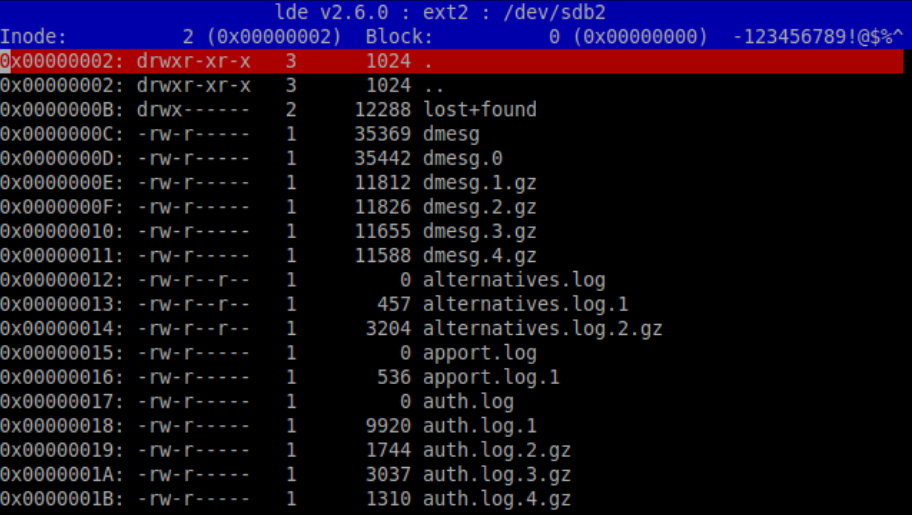
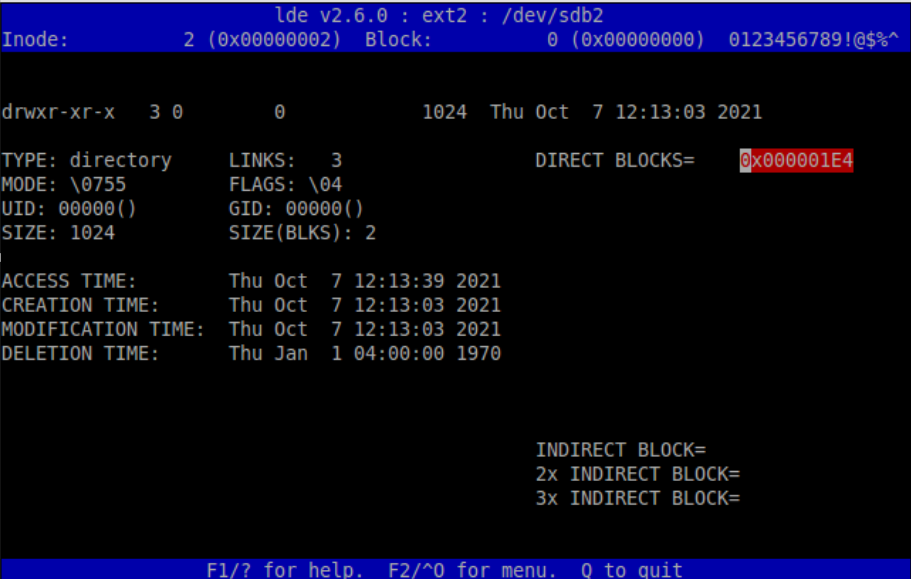
1. Выйти из lde и удалить оставшееся имя исследуемого файла.



1. Используя редактор lde найти inode удаленного файла. Как изменились временные характеристики этого файла?

Creation Time совпадает с Deletion Time

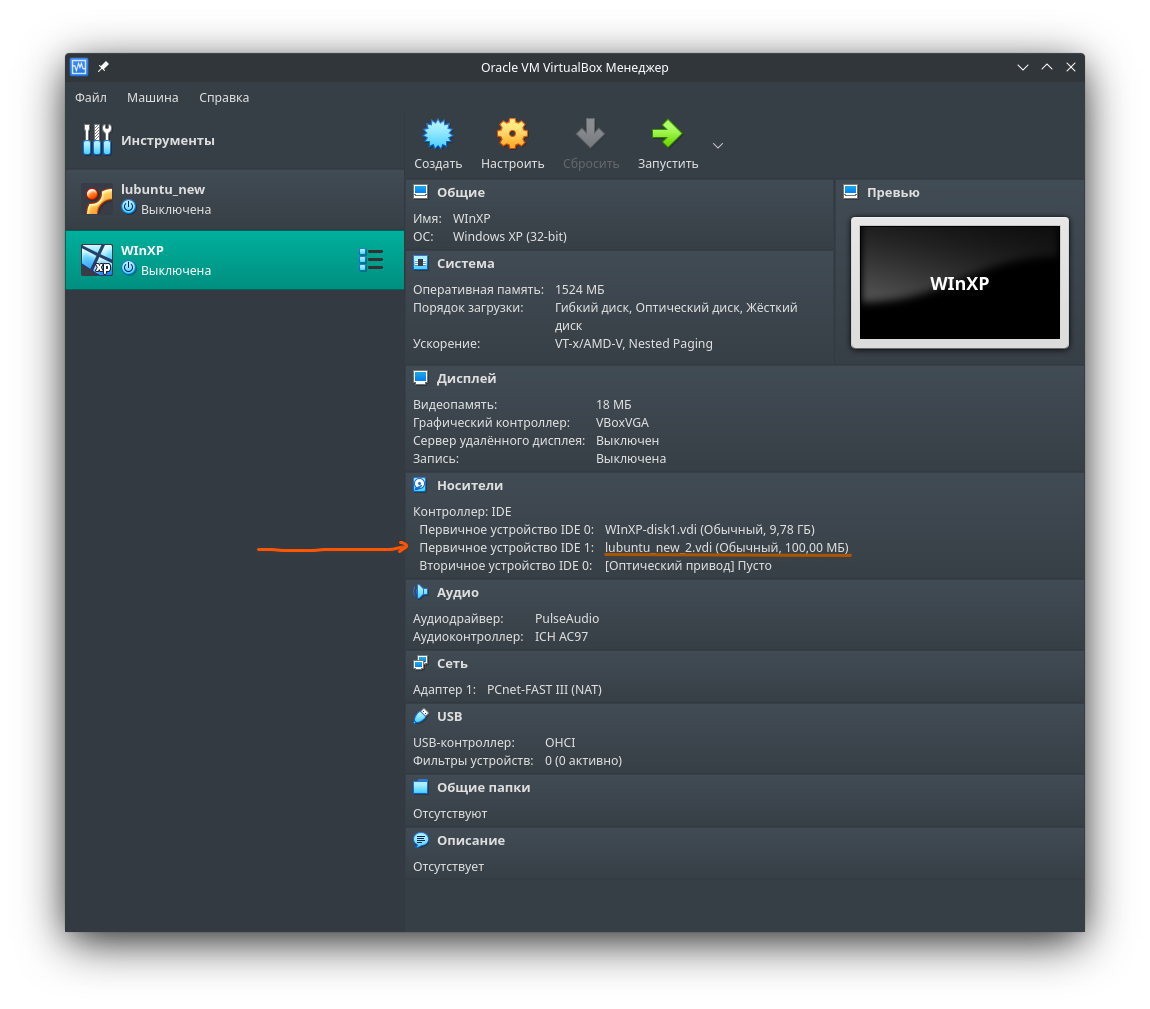
1. Проделайте то же самое с первым файлом второго раздела (ext3fs). Какова разница в представлении данных об удаленном файле?



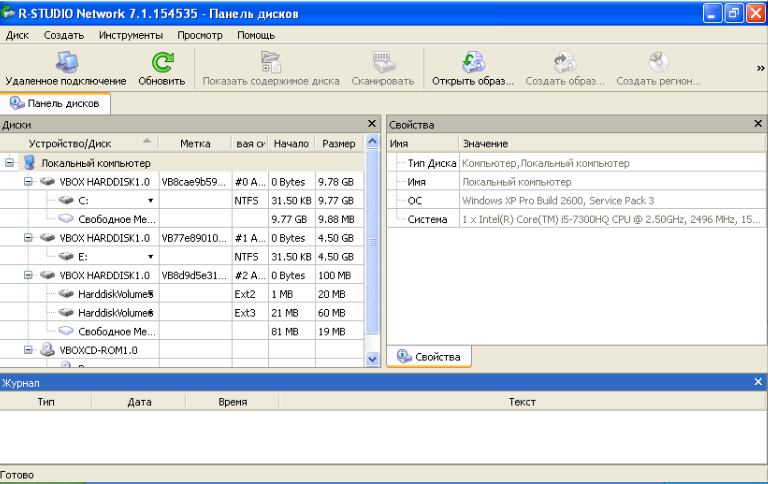
Проверка показала что в ext3 после удаления совпадают Creation Time, Modification Time, Deletion Time.

***Вопрос 3.* Изучение возможности восстановления информации в файловых системах extXfs.**

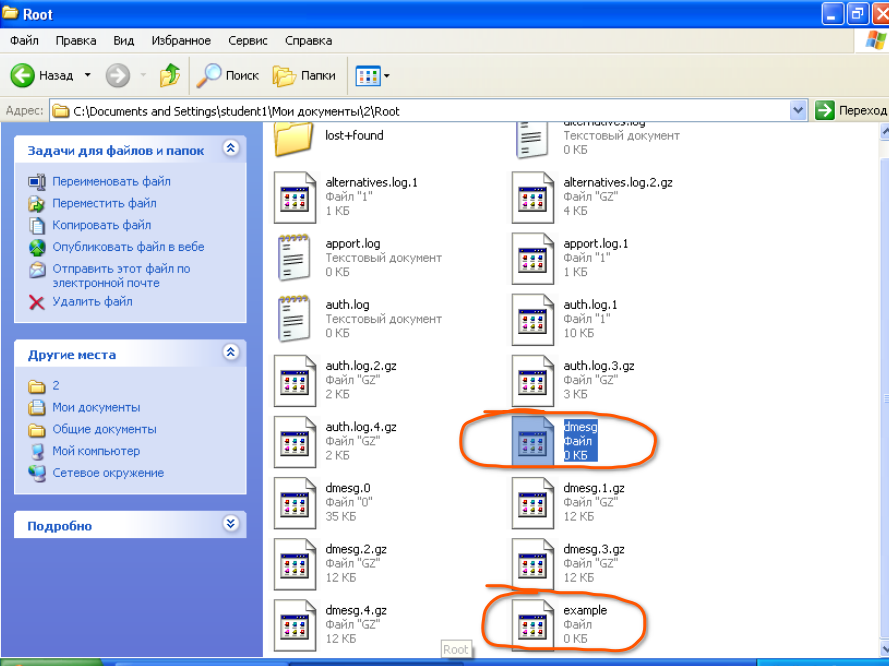
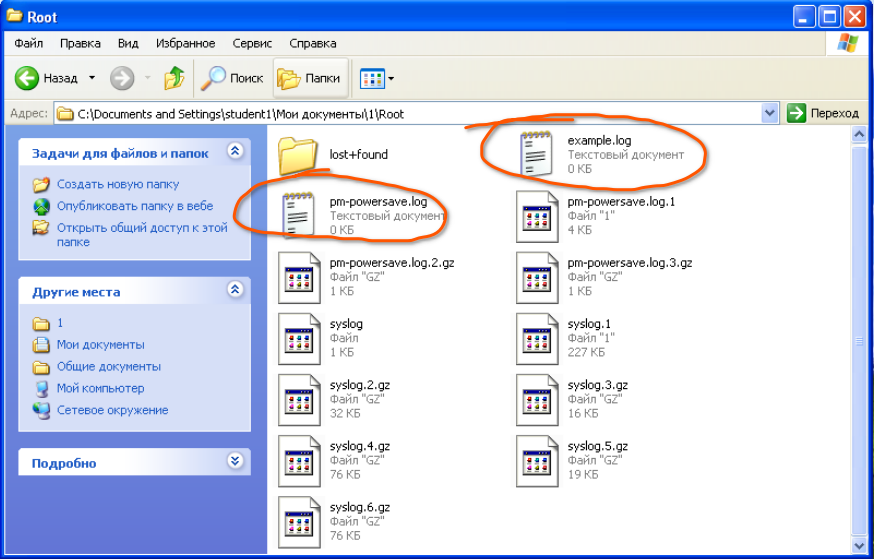
1. Завершить сеанс работы с ОС Linux в виртуальной машине
2. Подключить созданный вами виртуальный диск к виртуальной машине с Windows XP.



1. Установите программу R-Studio.



1. Попытайтесь, используя программу R-Studio восстановить данные с этот их разделов. Каков результат?

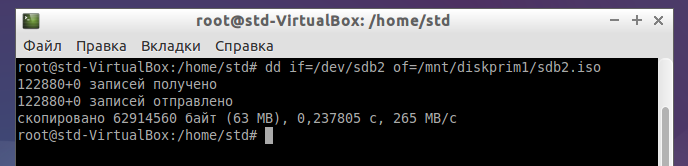


Рабочие файлы и их жесткие ссылки, которые использовались до этого и были удалены, хоть и отображаются как существующие файлы, но они не были восстановлены (их размер равен нулю).

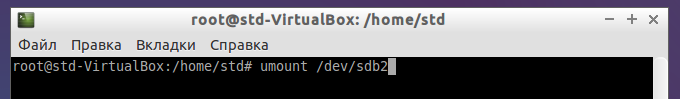
***Вопрос 4.* Клонирование файловых систем средствами Linux**

Задача: сохранить клон /dev/sdb2 на /dev/sdb1

1. Загрузите виртуальную машину с Linux.
2. Выполните команду: dd if=/dev/sdb2 of=/mnt/diskprim1/sdb2.iso



1. Размонтируйте устройство /dev/sdb2

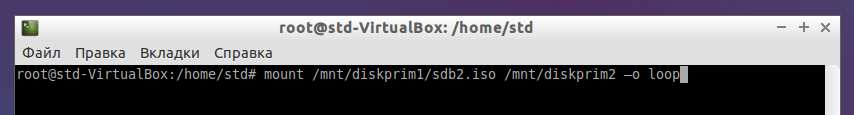


1. Проверьте смонтированные системы. Какие изменения вы заметили?

Не может быть использована /mnt/diskprim2

1. Выполните команду:

mount /mnt/diskprim1/sdb2.iso /mnt/diskprim2 –o loop



1. Проверьте смонтированные системы. Какие изменения вы заметили?



Новая точка монтирования, снова может быть использована /mnt/diskprim2