**Лабораторная работа 5.**

**Восстановление данных**

**Серт Серкан Группа 8**

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

**Вопросы к лабораторной работе**

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?

* TestDisk,
* PhotoRec,
* Extundelete ,
* Foremost

1. Какие файловые системы поддерживает PhotoRec?

* DOS/Win9x
* Windows
* Linux
* FreeBSD, NetBSD, OpenBSD
* Sun Solaris
* Mac OS X

1. Какие форматы поддерживает PhotoRec?

* FAT,
* NTFS,
* EXT2/EXT3 filesystem
* HFS+

1. Как Foremost восстанавливает файлы?

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

1. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?

* Нет

1. Все ли данные скопированные с каталога /var/log/ восстановились?
2. Все ли данные скопированные с каталога /etc/ восстановились?

/var/log/ и /etc/ - это два различных каталога в файловой системе Linux, каждый из которых имеет свою специфическую цель и хранит различные типы файлов.

**/var/log/**

* **Назначение**: Каталог /var/log/ используется для хранения системных и приложений логов (журналов) в Linux. В этом каталоге находятся файлы, содержащие информацию о работе системы, событиях, ошибках, предупреждениях и действиях, произошедших на компьютере.

**Примеры файлов в /var/log/:**

* syslog: Основной системный журнал, содержащий информацию о работе ядра и системных служб.
* auth.log: Журнал аутентификации, где регистрируются события аутентификации пользователей.
* kern.log: Журнал ядра, содержащий сообщения ядра операционной системы.

**/etc/**

* Назначение: Каталог /etc/ содержит конфигурационные файлы (настройки) для различных программ и служб на компьютере. Эти файлы определяют параметры работы программ, настройки сети, правила безопасности и другие параметры системы.

**Примеры файлов в /etc/:**

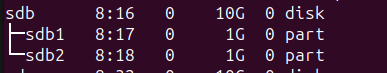
* passwd: Файл, содержащий информацию о пользователях системы.
* group: Файл, содержащий информацию о группах пользователей.
* hosts: Файл, определяющий соответствия между IP-адресами и именами хостов.
* network/: Папка с конфигурационными файлами сети.

**Задания к лабораторной работе**

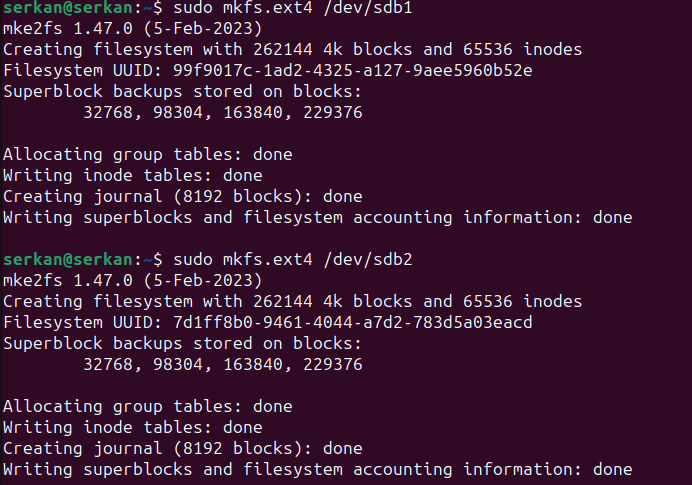
Добавьте в виртуальную машину виртуальный жесткий диск.

Запустите виртуальную машину с Linux.

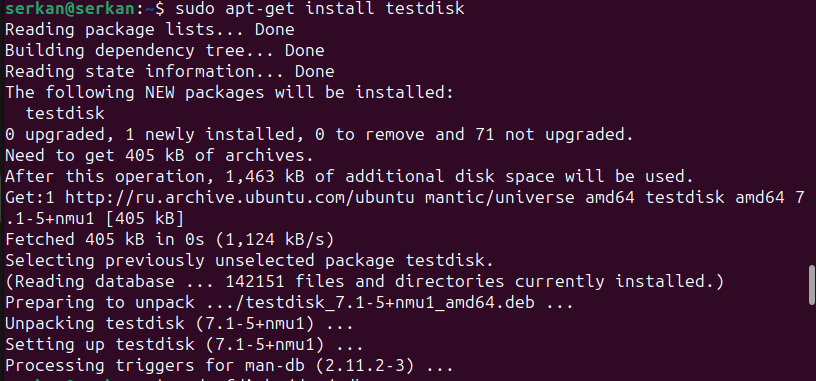
Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами



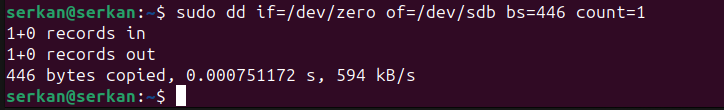
Отформатируйте созданные разделы в файловую систему ext4.

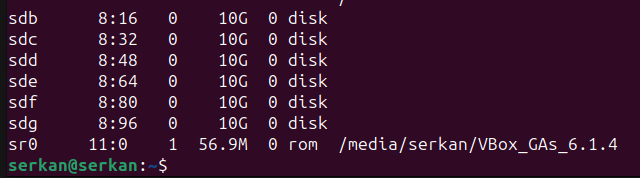


Установите TestDisk

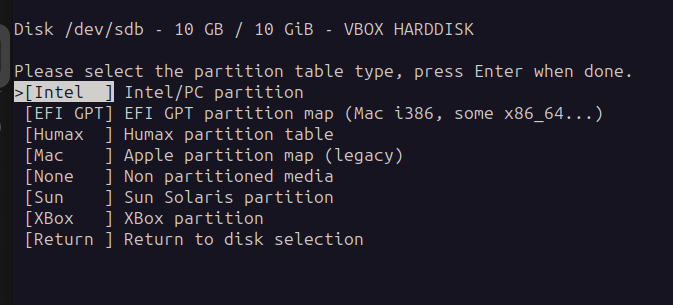


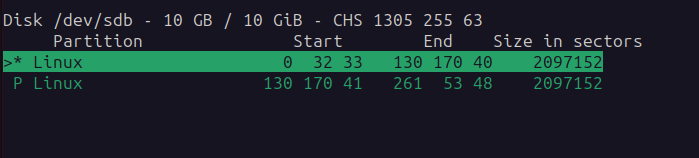
Удалите MBR (или таблицу разделов) с помощью команды DD.





Восстановите MBR (или таблицу разделов) с помощью TestDisk.

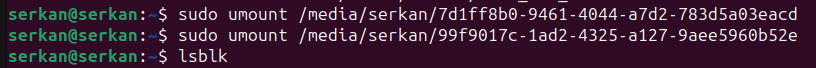




Смонтируйте восстановленные разделы и создайте там произвольные файлы

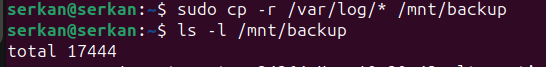


Удалите созданные файлы

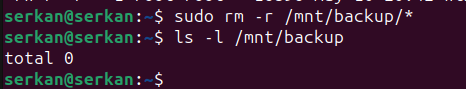


Создайте произвольный каталог и запишите туда данные каталога /var/log/ .

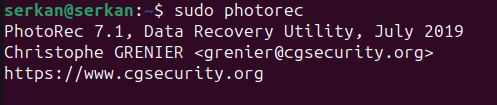


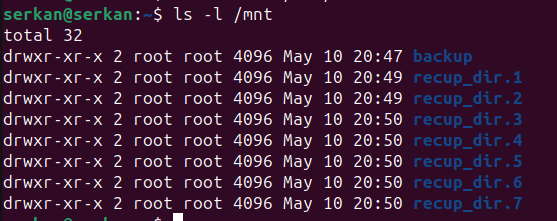


Удалите данные с созданного каталога

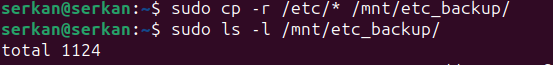


С помощью PhotoRec восстановите данные.





Создайте произвольный каталог и запишите туда данные каталога /etc/ .



С помощью Extundelete или Foremost восстановите данные

