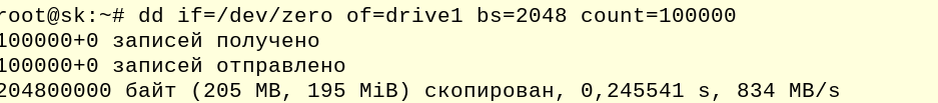
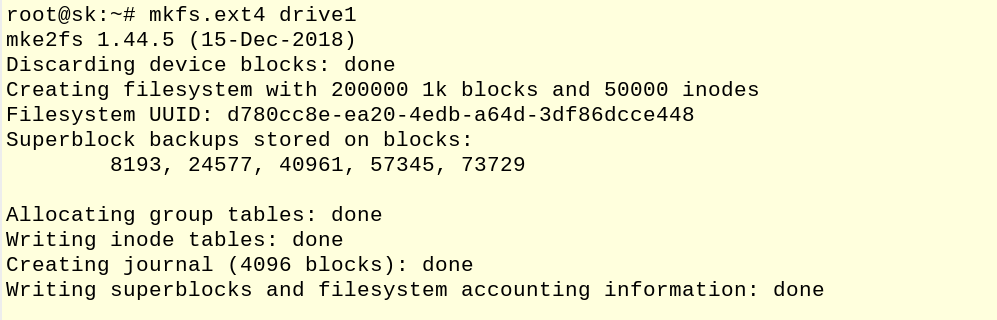
**Работаем с файлом как с диском (изучаем журнал ext4 и восстанавливаем файлы)**

Создаем файл. Он должен быть достаточно большим, чтобы мы могли создать журнал

dd if=/dev/zero of=drive1 bs=2048 count=100000



Создаем файловую систему ext4



Важно, что журнал был создан

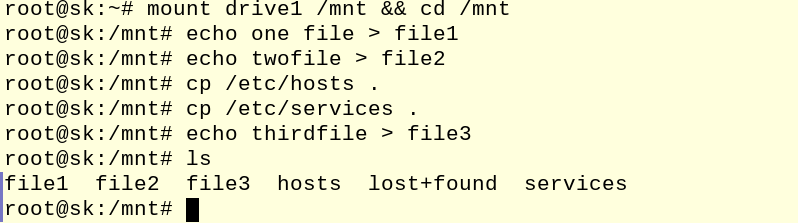
Монтируем наш диск

mount drive1 /mnt

Переходим в /mnt

cd /mnt

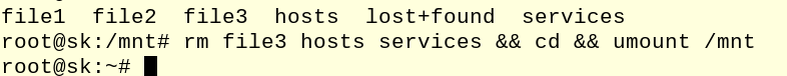
Создаем и копируем сюда файлы



Некоторые файлы удалим и отмонтируем /mnt

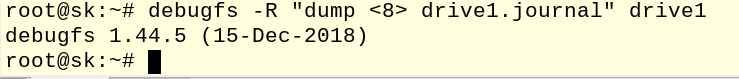
Сделаем это одной командой

rm file3 hosts services && cd && umount /mnt



Создадим копию журнала

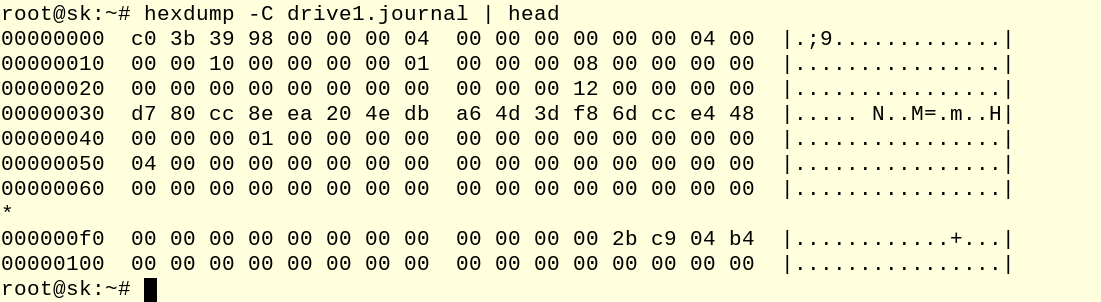
debugfs -R "dump <8> drive1.journal" drive1



Кстати, 8 в угловых скобках - это номер айнода журнала.

Проверим, что журнал не пустой

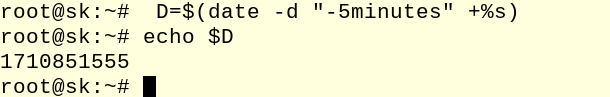
hexdump -C drive1.journal | head



Если ничего не вывелось значит, маленький файл создали, нужно вернуться в начало и задать больший count в dd.

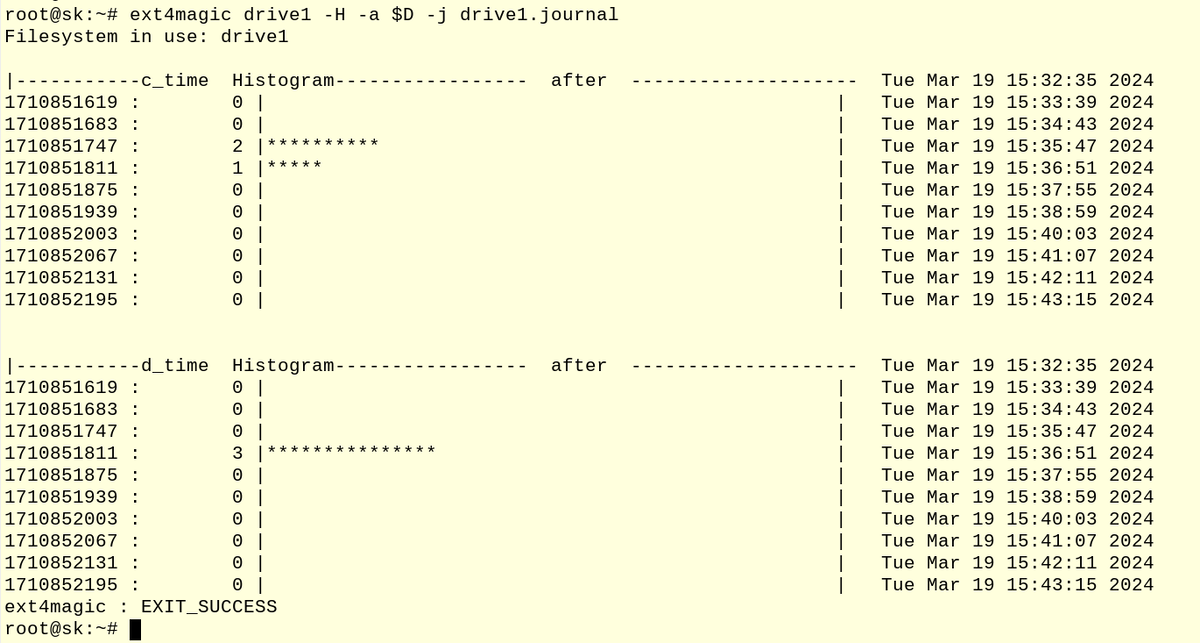
Получим дату на 5 минут раньше чем есть сейчас и сохраним ее в переменную D

D=$(date -d "-5minutes" +%s)

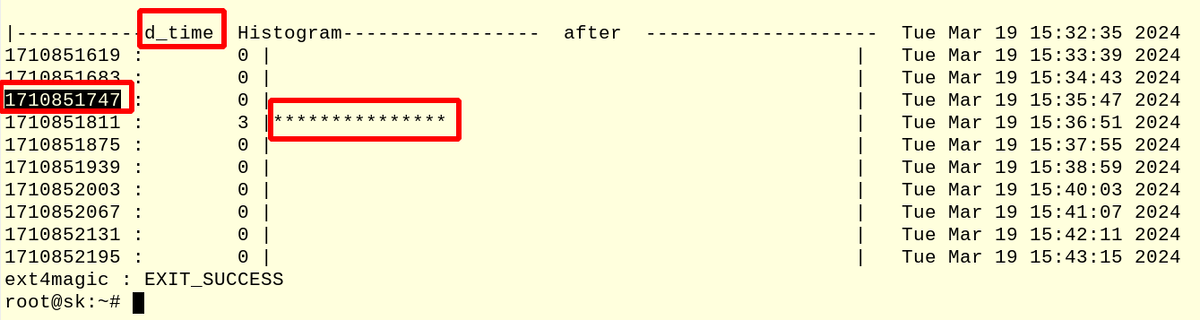


Посмотрим события, причем используя копию журнала (не забываем это, раз и далее будем работать с копией)

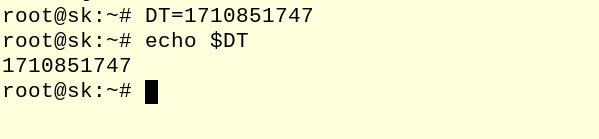
ext4magic drive1 -H -a $D -j drive1.journal



Берем метку, предшествующую событию из секции d\_time

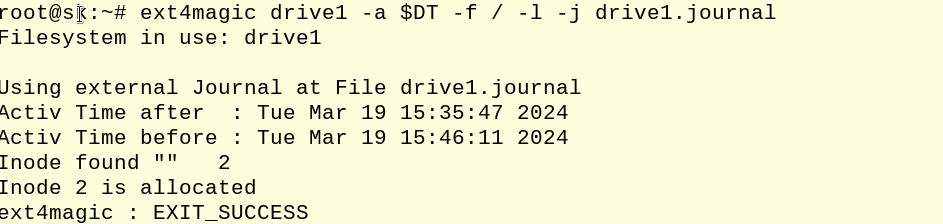


Присвоим ее переменной DT



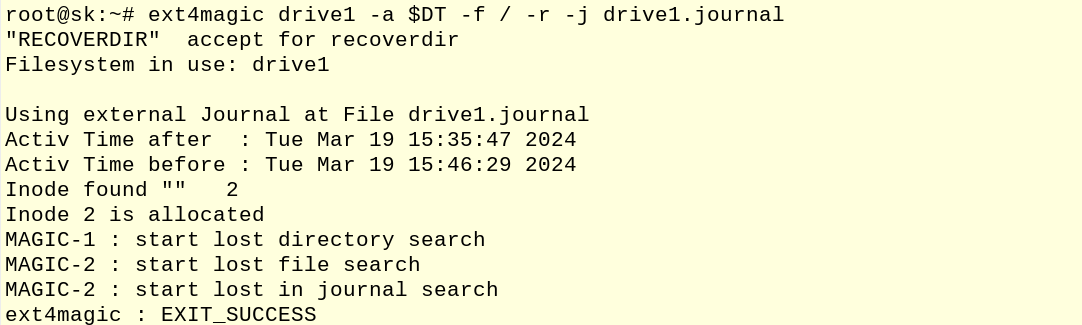
Смотрим, есть ли что восстановить

ext4magic drive1 -a $DT -f / -l -j drive1.journal

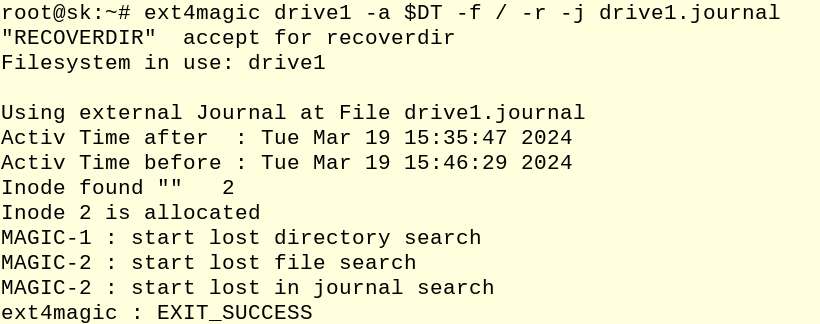


Нечего. Но мы все равно попытаемся, вдруг сохранились без имени?

ext4magic drive1 -a $DT -f / -r -j drive1.journal



Пытаемся восстановить



Гипотеза подтвердилась - ни одного файла не найдено.

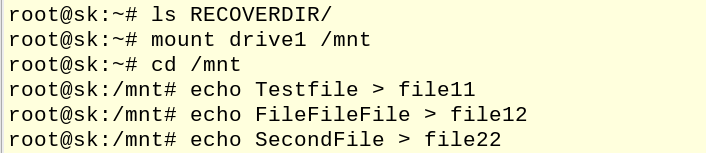
Но все равно смотрим, что есть в RECOVERDIR



Пусто.

Снова монтируем drive1 в mnt и переходим в него

mount drive1 /mnt cd /mnt Создаем новые файлы



Копируем файлы из /etc

cp /etc/\* .

Мы не указали -r, потому подкаталоги не копируются.

Смотрим, что вышло с помощью ls

Удалим файлы начинающиеся на a

rm a\*

Немного подумаем и удалим также начинающиеся на e,g,h,m,n,o

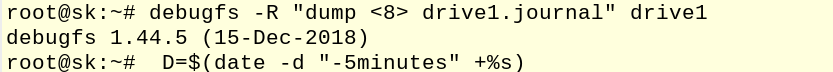
rm e\* g\* h\* m\* n\* o\*

А дальше аналогично

Снова создаем копию журнала и выясняем метку времени на 5 минут раньше чем сейчас

debugfs -R "dump <8> drive1.journal" drive1

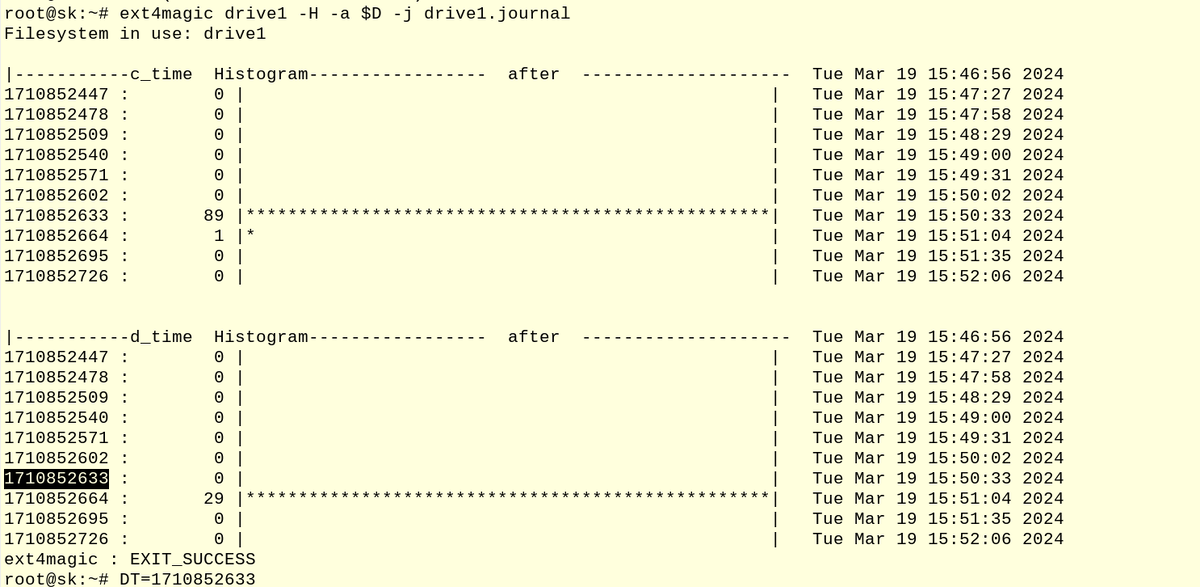
D=$(date -d "-5minutes" +%s)



Смотрим события

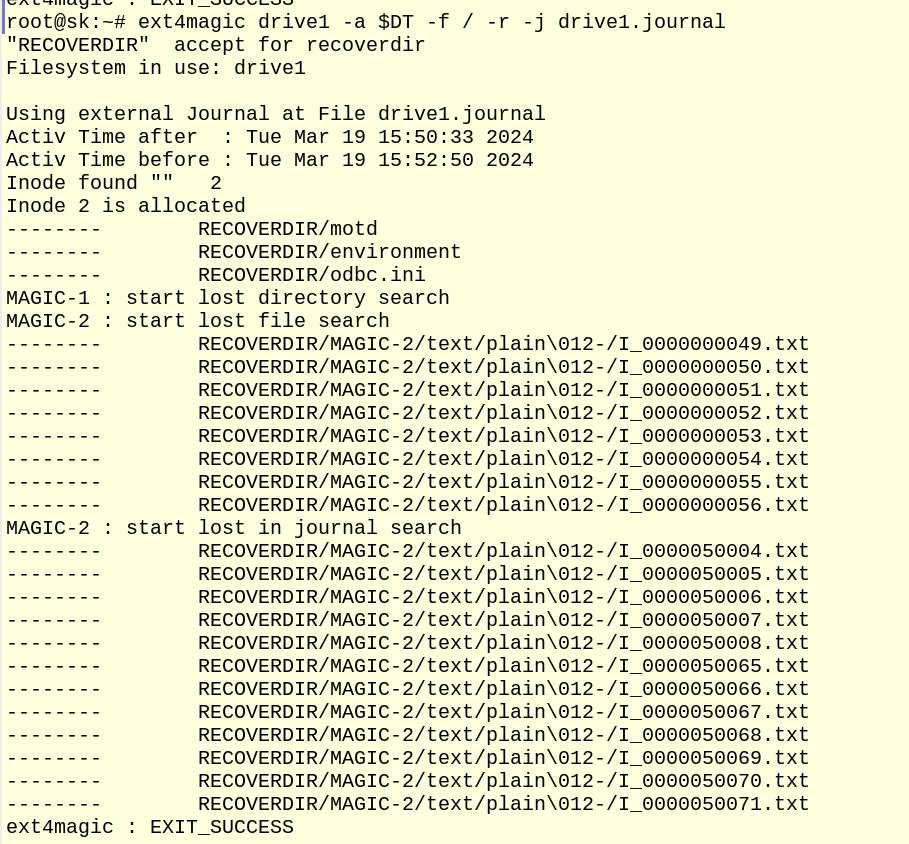
ext4magic drive1 -H -a $D -j drive1.journal

и сохраняем метку времени.



Проверяем что можно восстановить

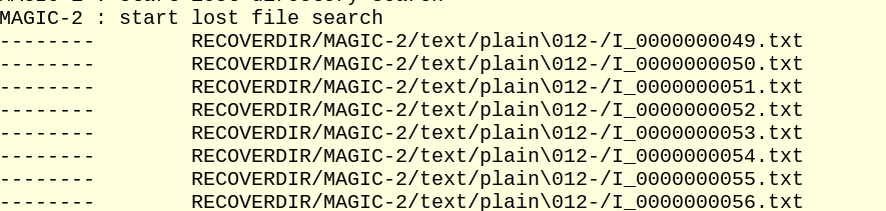
ext4magic drive1 -a $DT -f / -l -j drive1.journal



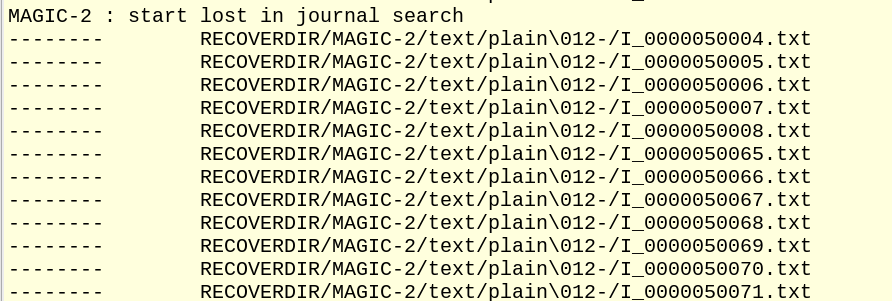
Опа! Вот в этот раз совсем не плохо.

Три файла сохранились с именами, с ними проблемы нет.

Несколько файлов были найдены без сохранения имен, причем без помощи журнала, а поиском по inode. Их имена содержат номера инодов, в которых они были найдены.



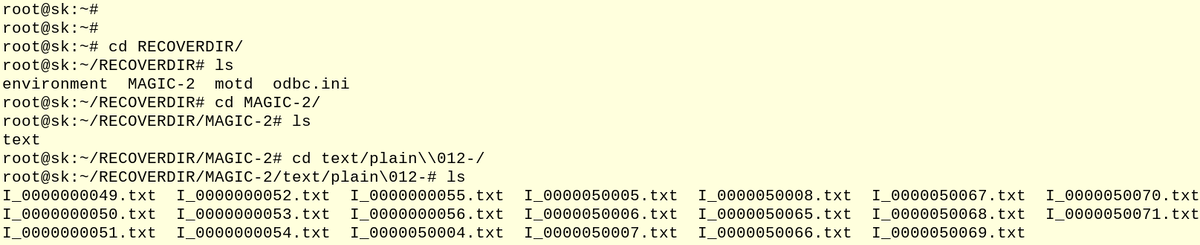
И еще несколько файлов были найдены благодаря журналу



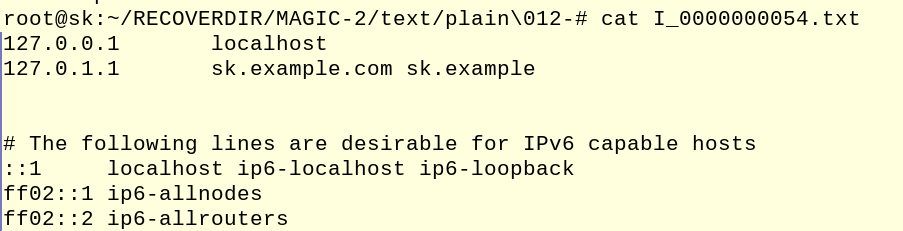
Нет смысла делать

cat RECOVERDIR/file1

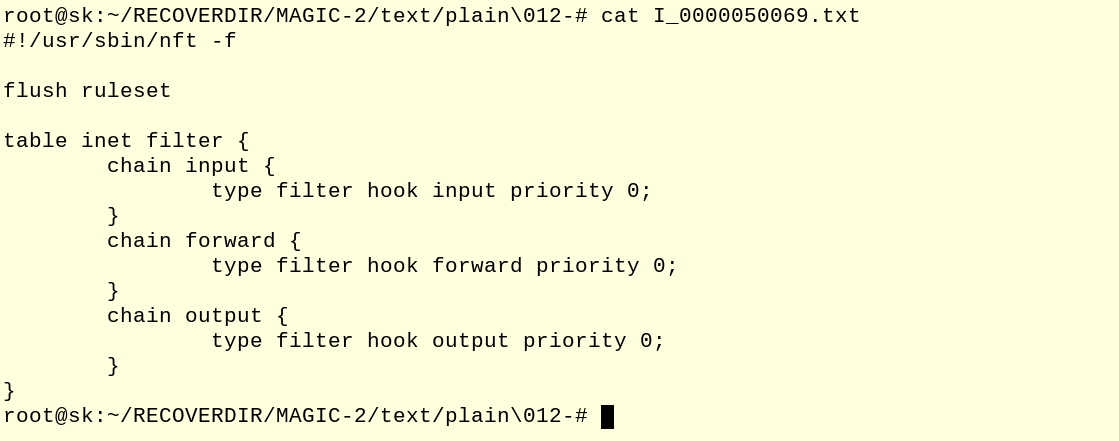
если его нет в этом списке. С другой стороны имеет смысл поисследовать RECOVERDIR



Файлы найденные, благодаря тому, что иноды не были повторно заняты



Пример файла, найденного в журнале



Среди прочего вывод - если вы не видите имя в выдаче ext4magic это не значит, что файл не восстановился.

Но то что он восстановился, тоже не значит.

Файловая система ext4 не предназначена для восстановления файлов. Возможность восстановить через журнал или айноды - побочный эффект, скорее удобный для того, чтобы понять как файловая система работает.

Делайте бэкапы!

Подписывайтесь на мой канал в дзен <https://dzen.ru/olinux> и будете в курсе новых моих статей по компьютерным сетям и ОС GNU/Linux.

Всегда с вами, Сергей Кручинин преподаватель GNU/Linux и компьютерных сетей