超全！Linux 誤刪文件恢復命令及方法

網絡安全編程與黑客程序員 前天

作者：漠效

https://blog.csdn.net/GX_1_11_real/article/details/84571303

前言

無論在哪個系統中，刪除文件都是必須謹慎的操作。

因為如果不小心刪除了重要文件，就會導致個人或公司出現重大的損失。

類似於windows系統誤刪了文件，可以使用一些軟件進行恢復操作。Linux也是有幾款軟件可以做到誤刪恢復的。

注意事項：雖然有軟件可以對誤刪的數據進行恢復，但是完全恢復數據的概率並不是百分百的。

因此，使用rm命令刪除文件的時候，一定要小心；重要的數據一定要有備份；並且恢復刪除的數據前，刪除文件的目錄內不能往進存放新東西，否則覆蓋掉的信息無法找回。

下面介紹的就是對Linux中誤刪文件的恢復操作。

1、lsof

原理：

這個命令實際上並不能直接用來恢復文件，不過它可以列出被各種進程打開的文件信息。

配合其他命令，從/proc目錄下的信息中恢復“文件已刪除，但進程仍保持打開該文件的狀態”的文件。

/proc目錄是掛載的是在內存中所映射的一塊區域，當我們對這些文件進行讀取和寫入時，實際上是在從內存中獲取相關信息。

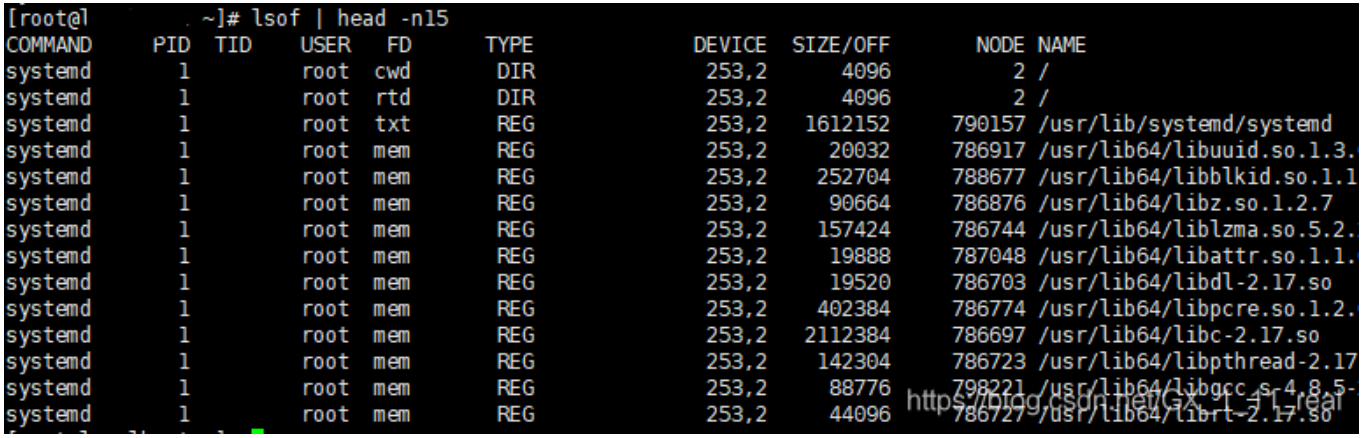
因此，當我們對文件進行讀取或寫入時(即有進程正使用文件時)，哪怕硬盤中的該文件已刪除，還可以從內存中的信息恢復文件。

注意：
必須以root用戶的權限運行，因為lsof需要訪問核心內存和各種文件。

只能恢復“文件已刪除，但進程仍保持打開該文件的狀態”的文件。

如果誤刪了目錄，目錄中的其他文件未被進程打開，沒有進行使用的文件將無法使用此方法恢復。

lsof輸出信息的意義：



COMMAND	进程的PID(进程标识符)
USER	进程所有者
FD	用来识别该文件(文件描述符)
DEVICE	指定磁盘的名称
SIZE	文件的大小
NODE	索引节点(文件在磁盘上的标识)
NAME	打开文件的确切名称

最常用参数:

-c	显示某进程现在打开的文件
-p	显示哪些文件被某pid进程打开
-g	显示归属某gid的进程情况
-d	显示目录下被进程开启的文件
-d	显示使用fd为4的进程
-i:80	显示打开80端口的进

恢復文件操作

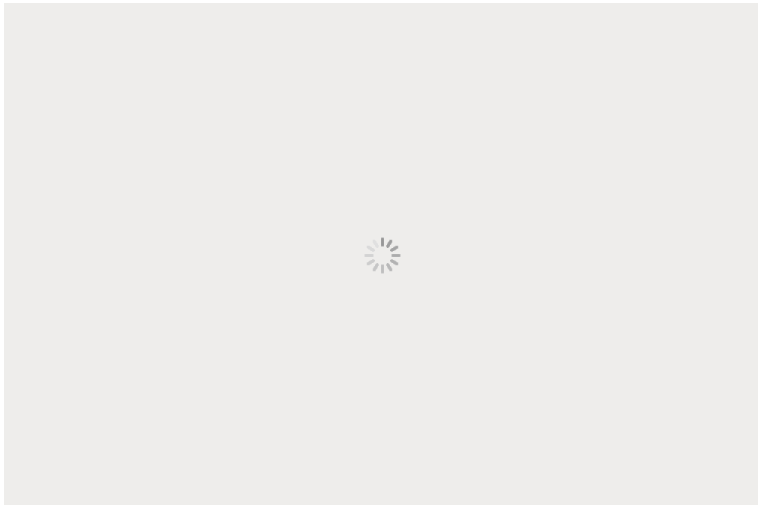
環境：
在/mnt下有一些文件，其中一個文件train.less正在被查看，然後另一個終端將其刪除

【1】lsof查看

查看正在使用刪除文件的進程號

```
lsof /mnt
```

```
[root@          mnt]# lsof /mnt/
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
bash    30694 root  cwd    DIR 253,17        0 1313234 /mnt/ferris/static (deleted)
bash    30701 root  cwd    DIR 253,17     4096       2 /mnt
less    31284 root  cwd    DIR 253,17        0 1313234 /mnt/ferris/static (deleted)
less    31284 root    4r   REG 253,17      358 1313235 /mnt/ferris/static/train.less (deleted)
lsof    31297 root  cwd    DIR 253,17     4096       2 /mnt
lsof    31298 root  cwd    DIR 253,17     4096       2 /mnt
```

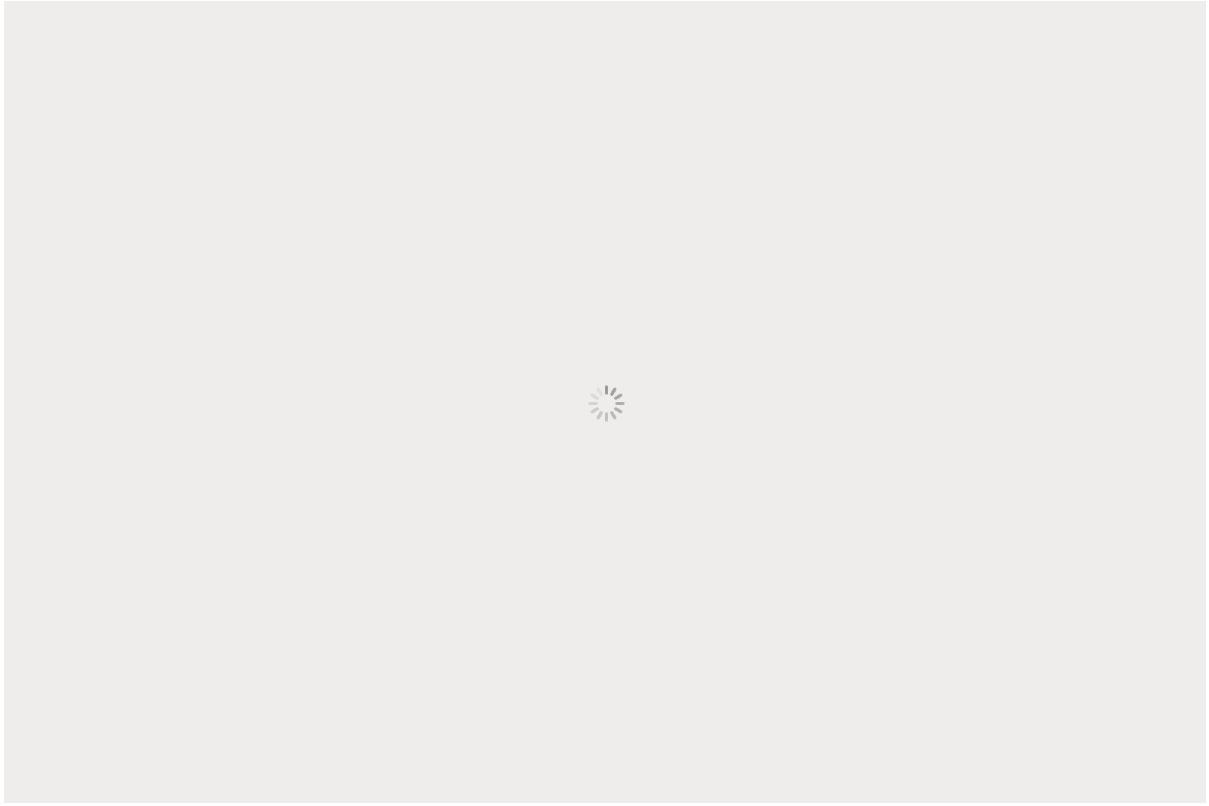


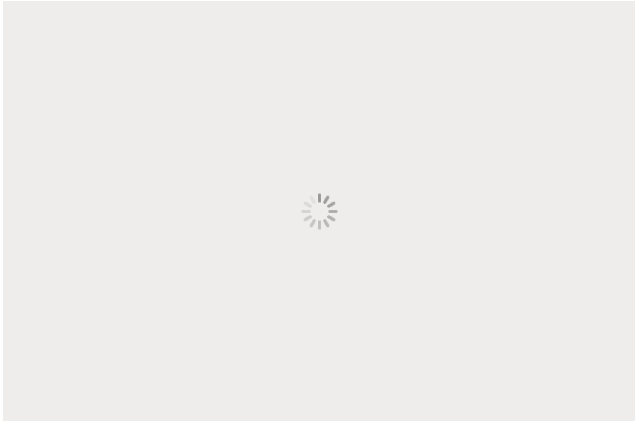
【2】恢復

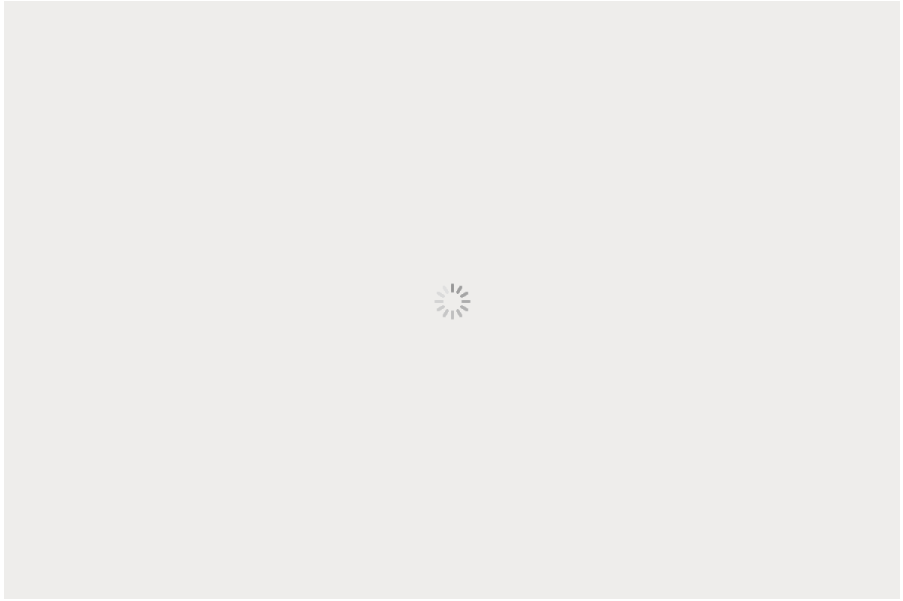
切換到/proc下，刪除文件對應的進程的pid下的文件描述符中的目錄中；將對應的內容重定向或cp到其他文件中

重點關注：PID與FD

```
cd /proc/31284/fd/
 cat 4 > /mnt/ferris_train.less
```







2、extundelete

原理：

使用存儲在分區日誌中的信息，嘗試恢復已從ext3或ext4的分區中刪除的文件

優點：

相比於ext3grep只能恢復ext3文件系統的文件，其適用範圍更廣，恢復速度更快

extundelete官方地址(官方文檔)：

http://extundelete.sourceforge.net

extundelete下載地址：

http://downloads.sourceforge.net/project/extundelete/extundelete/0.2.4/extundelete

-0.2.4.tar.bz2

(最新版本的extundelete是0.2.4，於2013年1月發布)

注意：

- 在數據刪除之後，要卸載被刪除數據所在的磁盤或是分區
- 如果是系統根分區遭到誤刪除，就要進入單用戶模式,將根分區以只讀的方式掛載,盡可能避免數據被覆蓋
- 數據被覆蓋後無法找回
- 恢復仍有一定的機率失敗，平時應對重要數據作備份，小心使用rm

安裝

1、依賴安裝

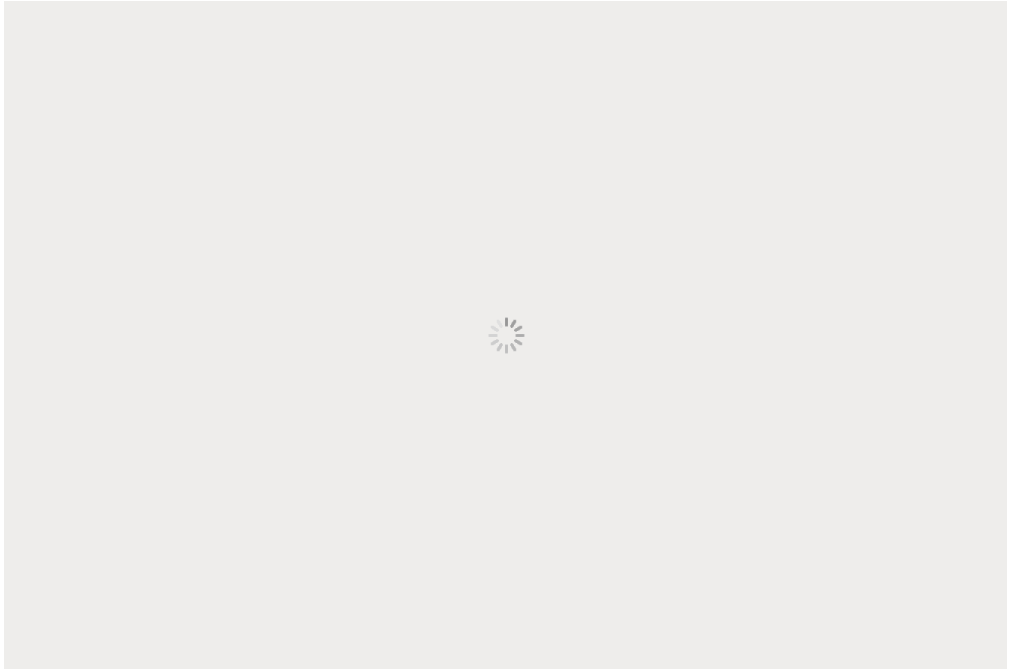
```
centos安装操作
yum install e2fsprogs-devel   e2fsprogs* gcc*

ubuntu安装操作
apt-get install build-essential  e2fslibs-dev  e2fslibs-dev
```

2、編譯安裝

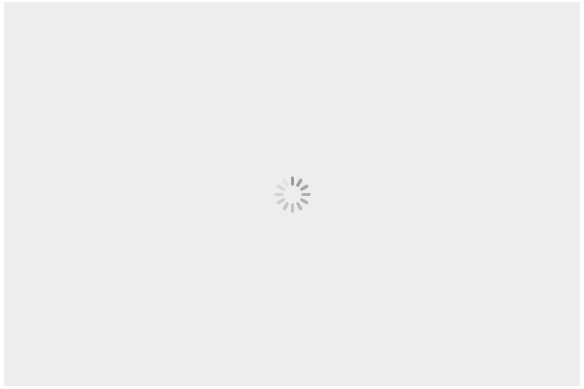
```
wget http://downloads.sourceforge.net/project/extundelete/extundelete/0.2.4
tar xf  extundelete-0.2.4.tar.bz2
cd  extundelete-0.2.4
./configure
make
```

```
6 make install
```

```
cd /root/extundelete-0.2.4/src
```



```
extundelete -v
```



執行make命令會在src目錄下生成extundelete可執行文件，可在此直接執行恢復命令。

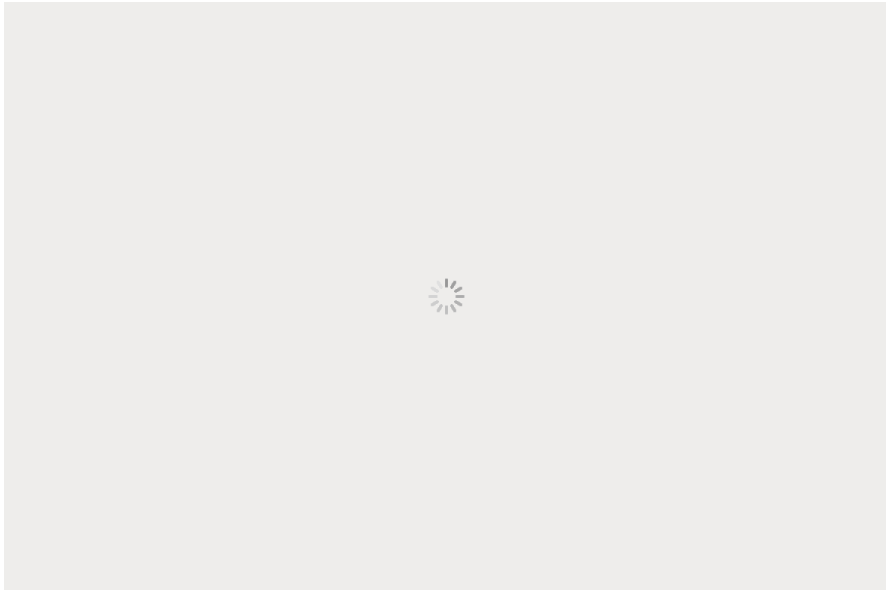
执行make install会将程序安装在/usr/local/bin/下

恢复文件操作

执行extundelete命令的当前目录必须是可写的。

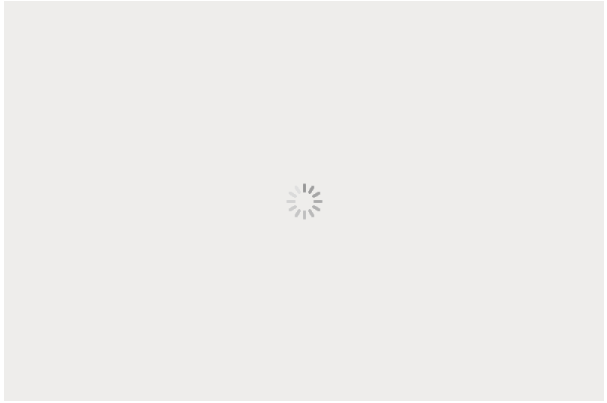
1、查看要恢复文件的分区的文件系统

```
df  -Th
```



2、对要恢复文件的分区解除挂载

```
umount /mnt
```

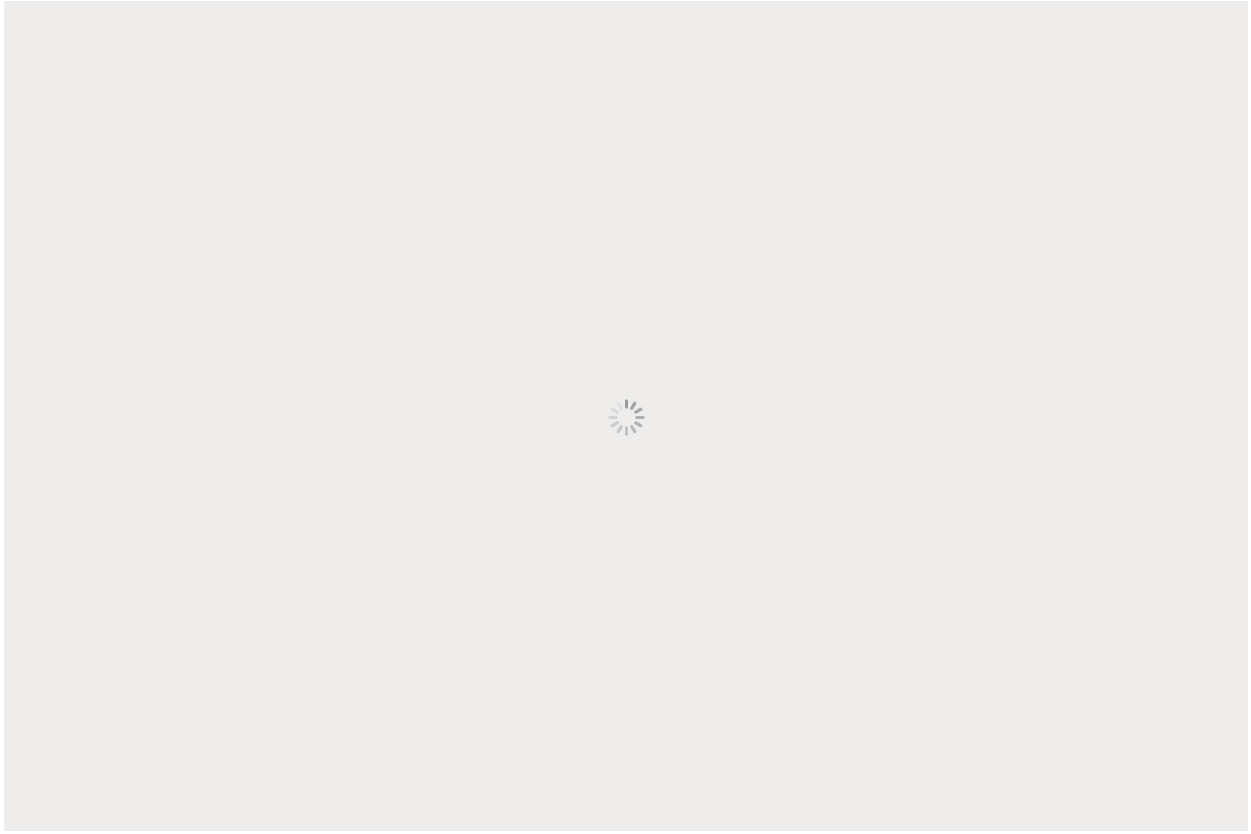


3、查看可以恢复的数据

指定误删文件的分区进行查找

最后一列标记为Deleted的文件，即为删除了的文件

```
extundelete /dev/vdb1 --inode 2 （根分区的inode值是2）
```

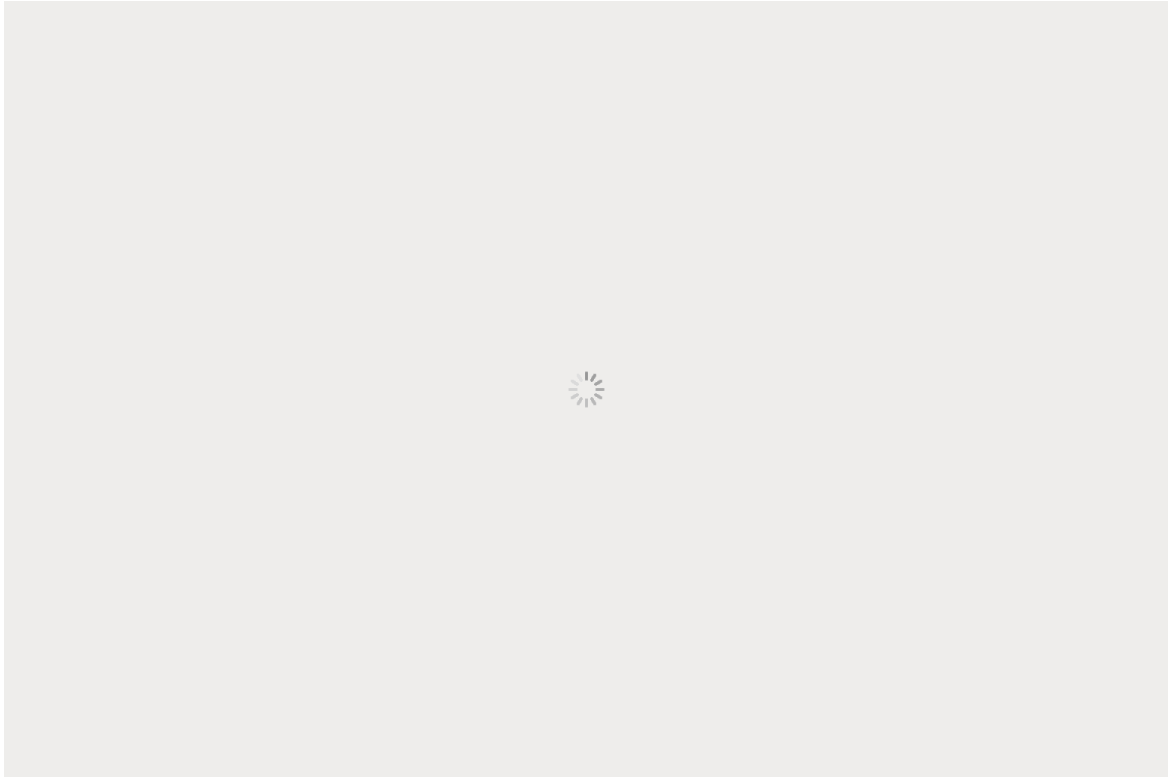


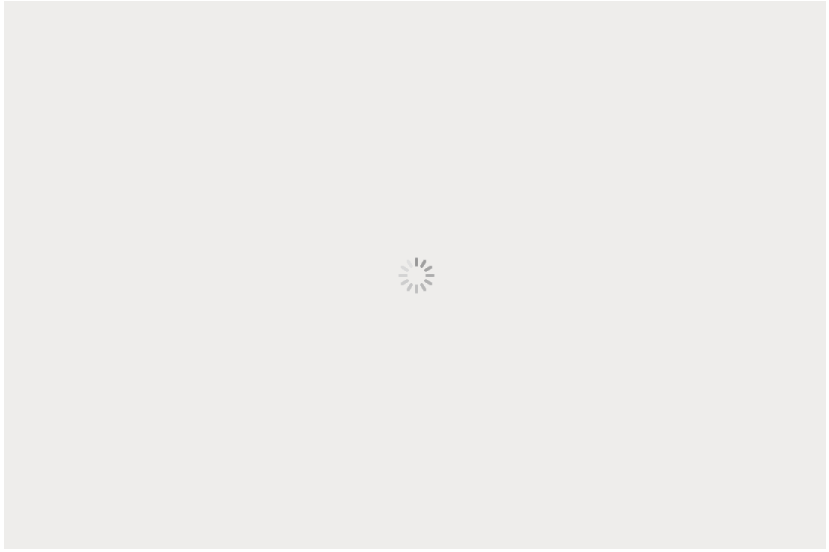
4、恢复单个目录

指定要恢复的目录名

如果是空目录，则不会恢复

```
extundelete /dev/vdb1 --restore-directory  ferris
```





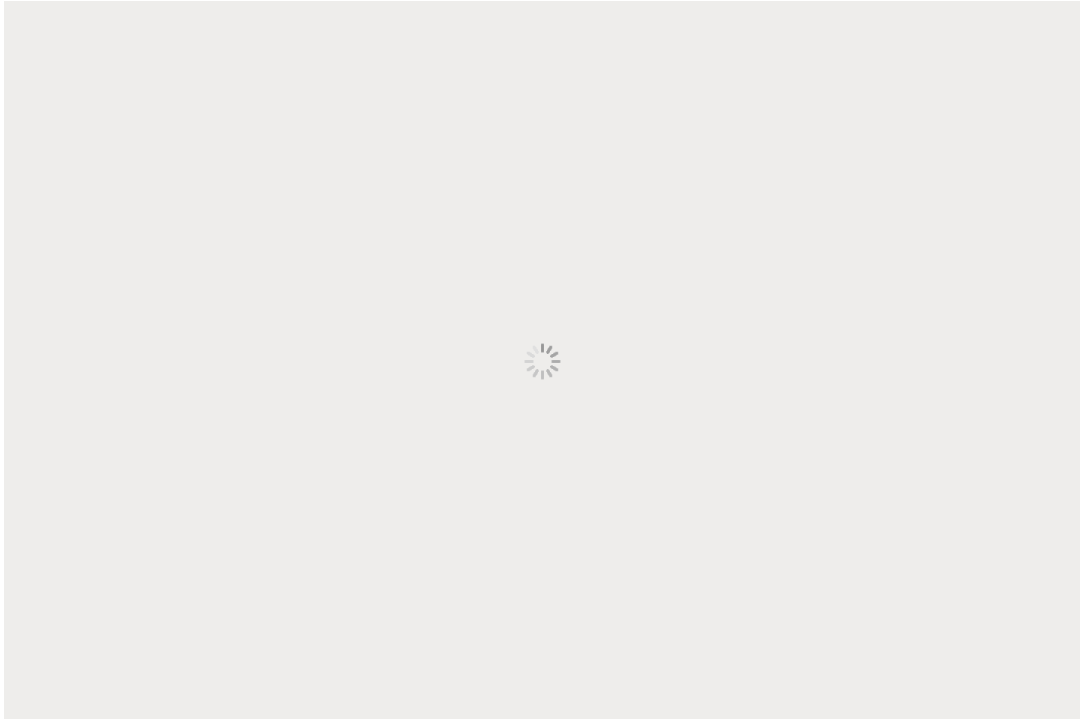
当执行恢复文件的命令后，会在执行命令的当前的目录下生成RECOVERED_FILES目录，恢复的文件都会放入此目录中。如未生成目录，即为失败。

5、恢复单个文件

指定要恢复的文件名

如果几k大小的小文件，有很大几率恢复失败

```
extundelete /dev/vdb1 --restore-file openssh-7.7p1.tar.gz
```



6、恢复全部删除的文件

无需指定文件名或目录名，恢复全部删除的数据

```
extundelete /dev/vdb1 --restore-all
```

喜欢此内容的人还喜欢

windows下远程不落地上线的方式

雷神众测

Linux系统安全-SELinux入门

谢公子学安全

组策略限制3389登录的绕过方式

潇湘信安