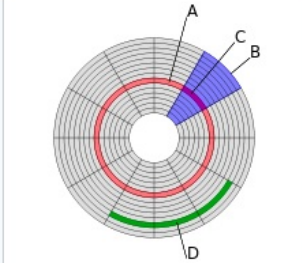
Sistemas de arquivos: Inodos
Borrado de ficheiros non implica perda de información

NOTA: Para verificar o que acontece na práctica crear unha máquina virtual en VirtualBox que arranque cunha ISO Live Debian 32bits, escritorio XFCE, 512MB de RAM e disco duro dinámico de 8GB. Imos supor que esta máquina virtual posúe o nome **Debian32-Recovery** e o disco duro posúe o nome **Debian32-Recovery.vdi**. Verificar que a primeira opción de arranque sexa o CD Virtual.

Por cada ficheiro ou directorio no sistema, existe un **inodo**, unha estrutura de datos, que garda a información do ficheiro. É similar aos rexistros do MFT en NTFS.



Estructura de disco que muestra:
(A) una pista (roja),
(B) un sector geométrico (azul),
(C) un **sector** de una pista (magenta),
(D) y un grupo de sectores o clúster (verde).

Wikipedia

Sector = **Bloque**

Sector lóxico != **Sector físico**

Comandos de interese sobre sistemas de ficheiros ext2/ext3/ext4

- **debugfs** #O comando debugfs permite depurar sistemas de ficheiros ext2/ext3/ext4
- **stat** #O comando stat permite amosar información sobre ficheiros ou sistemas de ficheiros.
- **dumpe2fs** #O comando dumpe2fs permite listar información sobre sistemas de ficheiros ext2/ext3/ext4.
- **tune2fs** #O comando tune2fs permite axustar os parámetros do sistema de ficheiros sobre sistemas de ficheiros ext2/ext3/ext4.

Práctica Borrado de ficheiros non implica perda de información

1. Arrancar a máquina virtual creada en modo Inicio normal

   `VBoxManage startvm Debian32-Recovery`

2. Na contorna gráfica (shell xfce) abrir un terminal e executar:
   $ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   $ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

Crear e formatear particións

parted --script /dev/sda mklabel msdos #Crear a etiqueta de disco (táboa de particións) ao dispositivo /dev/sda sen ter que acceder ao prompt de parted

parted --script /dev/sda mkpart primary 0 50% -a cylinder #Crear unha partición primaria no disco /dev/sda cos primeiros 5GB, alineando a cilindros, sen ter que acceder ao prompt de parted

parted --script /dev/sda mkpart primary 50% 70% -a cylinder #Crear unha partición primaria no disco /dev/sda de 2GB a continuación da partición de 5GB, alineando a cilindros, sen ter que acceder ao prompt de parted

parted --script /dev/sda print #Amosa a táboa de particións do disco /dev/sda

```
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sda: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start        End        Size       Type      File system  Flags
 1           32.3kB    4294MB  4294MB  primary  ext4
 2           4294MB  6013MB  1719MB  primary  ext3
```

mkfs.ext4 -F -L 'PARTICION1' /dev/sda1 #Formatear en ext4 coa etiqueta PARTICION1 a partición primaria /dev/sda1

```
mke2fs 1.43.4 (31-Jan-2017)
/dev/sda1 contains a ext4 file system labelled 'PARTICION1'
        last mounted on /mnt/recuperacion on Mon Oct 29 17:58:50 2018
Creating filesystem with 1048233 4k blocks and 262144 inodes
Filesystem UUID: 459fb916-7189-4b3f-83de-fd81b56973f8
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

mkfs.ext3 -F -L 'PARTICION2' /dev/sda2 #Formatear en ext3 coa etiqueta PARTICION2 a partición primaria /dev/sda2

```
mke2fs 1.43.4 (31-Jan-2017)
/dev/sda2 contains a ext3 file system labelled 'PARTICION2'
        created on Mon Oct 29 17:58:29 2018
Creating filesystem with 419698 4k blocks and 105040 inodes
Filesystem UUID: d5c70817-fa3c-4734-8825-fa78463558cd
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

Montar particións e crear ficheiros e directorios

mkdir /mnt/recuperacion #Crear o directorio /mnt/recuperacion

mount /dev/sda1 /mnt/recuperacion #Montar (facer uso) a partición primaria /dev/sda1 en /mnt/recuperacion

cd /mnt/recuperacion #Acceder ao directorio /mnt/recuperacion

mkdir proverbios #Crear o directorio /mnt/recuperacion/proverbios:

cd proverbios #Acceder ao directorio /mnt/recuperacion/proverbios:

echo 'Aprender sen pensar é inútil. Pensar sen aprender, perigoso. Confucio' > Confucio1.txt #Crear o ficheiro /mnt/recuperacion/proverbios/Confucio1.txt co contido 1 frase.

echo 'Eu non procuro coñecer as preguntas; procuro coñecer as respostas. Confucio' > Confucio2.txt #Crear o ficheiro /mnt/recuperacion/proverbios/Confucio2.txt co contido 1 frase.

echo 'Estudia o pasado se queres pronosticar o futuro. Confucio' > Confucio3.txt #Crear o ficheiro /mnt/recuperacion/proverbios/Confucio3.txt co contido 1 frase.

ls -lia #Listar de forma extendida e amosar os inodos dos ficheiros e directorios contidos en /mnt/recuperacion/proverbios

```
total 20
131073 drwxr-xr-x 2 root root 4096 Nov 1 00:25 .
2 drwxr-xr-x 4 root root 4096 Nov 1 00:24 ..
131074 -rw-r--r-- 1 root root 72 Nov 1 00:24 Confucio1.txt
131075 -rw-r--r-- 1 root root 69 Nov 1 00:25 Confucio2.txt
131076 -rw-r--r-- 1 root root 58 Nov 1 00:25 Confucio3.txt
```

cat Confucio1.txt Confucio2.txt Confucio3.txt #Ver os contidos dos ficheiros Confucio1.txt Confucio2.txt Confucio3.txt

```
Aprender sen pensar é inútil. Pensar sen aprender, perigoso. Confucio
Eu non procuro coñecer as preguntas; procuro coñecer as respostas. Confucio
Estudia o pasado se queres pronosticar o futuro. Confucio
```

Desmontar para poder intentar recuperar a información

cd #Acceder ao directorio casa do usuario (/home/user)

umount /mnt/recuperacion #Desmontar (deixar de facer uso) a partición primaria /dev/sda1 que estaba montada en /mnt/recuperacion

Revisar os bloques que referencian a información.

debugfs /dev/sda1 #Executar o comando debugfs sobre a partición primaria /dev/sda1

```
debugfs 1.43.4 (31-Jan-2017)
debugfs: stat <131074>  #Ver información sobre o inodo 131074
Inode: 131074 Type: regular Mode: 0644 Flags: 0x80000
Generation: 204948144 Version: 0x00000000:00000001
User:0 Group:0 Project:0 Size: 72
File ACL: 0 Directory ACL: 0
Links: 1 Blockcount: 8
Fragment: Address: 0 Number: 0 Size: 0
ctime: 0x5bda47db:8ec2f228 -- Thu Nov 1 00:24:59 2018
atime: 0x5bda4810:9270b1e4 -- Thu Nov 1 00:25:52 2018
mtime: 0x5bda47db:8ec2f228 -- Thu Nov 1 00:24:59 2018
crtime: 0x5bda47db:8ec2f228 -- Thu Nov 1 00:24:59 2018
Size of extra inode fields: 32
Inode checksum: 0x53cfeeeb
EXTENTS:
(0):557056
(END)
```

Vemos que logo de EXTENTS aparece/n o/s bloque/s onde está gardada a información. Premer a tecla **q** para voltar á consola debugfs

```
debugfs: cat <131074> #Ver o contido do ficheiro que corresponde co inodo 131074.
Aprender sen pensar é inútil. Pensar sen aprender, perigoso. Confucio
debugfs: blocks <131074> #Ver o/s bloque/s que apunta/n ao contido do ficheiro que corresponde co inodo 131074
557056
```

debugfs: q #Premer de novo a tecla q para saír da consola debugfs

Eliminar ficheiros

mount /dev/sda1 /mnt/recuperacion #Montar (facer uso) a partición primaria /dev/sda1 en /mnt/recuperacion

cd /mnt/recuperacion/proverbios #Acceder ao directorio /mnt/recuperacion/proverbios

rm Confucio1.txt #Borrar o ficheiro /mnt/recuperacion/proverbios/Confucio1.txt

Desmontar para revisar o que pasou coa información

cd #Acceder ao directorio casa do usuario (/home/user)

umount /mnt/recuperacion #Desmontar (deixar de facer uso) a partición primaria /dev/sda1 que estaba montada en /mnt/recuperacion

Revisar os bloques que referencian a información.

debugfs /dev/sda1 #Executar o comando debugfs sobre a partición primaria /dev/sda1

```
debugfs 1.43.4 (31-Jan-2017)
debugfs: stat <131074>  #Ver información sobre o inodo 131074
Inode: 131074 Type: regular Mode: 0644 Flags: 0x80000
Generation: 204948144 Version: 0x00000000:00000001
User:0 Group:0 Project:0 Size: 0
File ACL: 0 Directory ACL: 0
Links: 0 Blockcount: 0
Fragment: Address: 0 Number: 0 Size: 0
ctime: 0x5bda4b93:21e4db74 -- Thu Nov 1 00:40:51 2018
atime: 0x5bda4810:9270b1e4 -- Thu Nov 1 00:25:52 2018
mtime: 0x5bda4b93:21e4db74 -- Thu Nov 1 00:40:51 2018
crtime: 0x5bda47db:8ec2f228 -- Thu Nov 1 00:24:59 2018
dtime: 0x5bda4b93:(21e4db74) -- Thu Nov 1 00:40:51 2018
Size of extra inode fields: 32
Inode checksum: 0xcd1b5c5b
EXTENTS
(END)
```

Vemos que logo de EXTENTS non aparece ningún bloque onde está gardada a información, é dicir, ao borrar o arquivo perdeuse a referencia dos bloques correspondnetes ao contido pero a información segue existindo a non ser que fose sobreescrita. Premer a tecla **q** para voltar á consola debugfs

```
debugfs: cat <131074> #Ver o contido do ficheiro que corresponde co inodo 131074.
```

Neste caso non vemos contido xa que o ficheiro foi eliminado.

```
debugfs: blocks <131074> #Ver o/s bloque/s que apunta/n ao contido do ficheiro que corresponde co inodo 131074
```

Neste caso non vemos referencia ningún bloque xa que o ficheiro foi eliminado perdendo así a referencia ao/s bloque/s. Como anteriormente vimos o/s bloque/s referenciados **(557056)** ao contido do ficheiro Confucio1.txt imos revisar se podemos ver o contido dese bloque. E no caso de poder ver o contido como non sobreescribimos o/s bloque/s deberiamos ver o texto do ficheiro Confucio1.txt

```
debugfs: block_dump 557056
0000 4170 7265 6e64 6572 2073 656e 2070 656e Aprender sen pen
0020 7361 7220 c3a9 2069 6ec3 ba74 696c 2e20 sar .. in..til.
0040 5065 6e73 6172 2073 656e 2061 7072 656e Pensar sen apren
0060 6465 722c 2070 6572 6967 6f73 6f2e 2043 der, perigoso. C
0100 6f6e 6675 6369 6f0a 0000 0000 0000 0000 onfucio.........
0120 0000 0000 0000 0000 0000 0000 0000 0000 ................
*
```

Acabamos de ver que o bloque non está referenciado a ningún ficheiro pero segue preservando o contido do ficheiro Confucio1.txt porque non foi reescrito por ningún outro arquivo que o referencie.

Opción1 (dd): Recuperar a información do ficheiro borrado

Imos revisar o tamaño de bloque da partición /dev/sda1

dumpe2fs -h /dev/sda1 | grep -i 'block size' #Listar o tamaño de bloque en bytes mediante o comando dumpe2fs. O comando dumpe2fs permite listar información sobre sistemas de ficheiros ext2/ext3/ext4. A opción -h permite ver o tamaño do bloque, é dicir, do contido de información que ofrece o superbloque permite ver o tamaño do bloque. O comando grep -i permite polo patrón de búsqueda, neste caso 'block size', ignorando a diferenza entre maiúsculas e minúsculas.

```
Block size:               4096
```

tune2fs -l /dev/sda1 | grep -i 'block size' #Listar o tamaño de bloque en bytes mediante o comando tune2fs. O comando tune2fs permite axustar os parámetros do sistema de ficheiros sobre sistemas de ficheiros ext2/ext3/ext4. A opción -l permite ver os contidos do superbloque do sistema de ficheiros, é dicir, o contido de información sobre o sistema de ficheiros que ofrece o superbloque. O comando grep -i permite polo patrón de búsqueda, neste caso 'block size', ignorando a diferenza entre maiúsculas e minúsculas.

```
Block size:               4096
```

stat -fc %s . #Listar o tamaño de bloque mediante o comando stat. O comando stat permite amosar información sobre ficheiros ou sistemas de ficheiros. A opción -f permite amosar información sobre o sistema de ficheiros e non sobre ficheiros. A opción -c permite formatear a saída a ensinar. O argumento %s amosa o tamaño total en bytes

```
4096
```

echo revisar > revisar.txt #Xerar o ficheiro revisar.txt co contido revisar.

du -h revisar.txt #Listar o tamaño de bloque mediante o comando du. O comando du permite estimar o uso do espazo de ficheiros. A opción -h engade á saída unha letra indicativa do tamaño.

```
4.0K        revisar.txt
```

Todos os comandos anteriores amosan que o tamaño do bloque en disco é de: **4096B** ou **4.0kB**

dd if=/dev/sda1 of=recovery-data.txt bs=4096 count=1 skip=557056 #Recuperación do bloque 557056 mediante o comando dd. Recuperamos da partición /dev/sda1 no ficheiro recovery-data.txt o ficheiro eliminado Confucio1.txt. Para iso ao comando dd pasámolle como argumentos o valor do bloque (bs=4096), a cantidade de bloques a recuperar (count=1) e dende que bloque comezar a recuperar (skip=557056).

```
1+0 records in
1+0 records out
4096 bytes (4.1 kB, 4.0 KiB) copied, 0.00274002 s, 1.5 MB/s
```

cat recovery-data.txt #Ver o contido do ficheiro recovery-data.txt

```
Aprender sen pensar é inútil. Pensar sen aprender, perigoso. Confucio
```

O contido do ficheiro foi recuperado

Opción2 (extundelete): Recuperar a información do ficheiro borrado

apt-get update #Actualizar o repositorio de debian

apt-cache search extundelete #Buscar paquetes que fagan referencia a extundelete

apt-get -y install extundelete #Instalar o paquete extundelete

man extundelete #Ver as páxinas do manual do comando extundelete

ls #Listar ficheiros/directorios da ruta actual (/root)

```
recovery-data.txt  revisar.txt
```

extundelete --restore-all /dev/sda1 #Recuperar todos os ficheiros borrados da partición /dev/sda1

```
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 32 groups loaded.
Loading journal descriptors ... 27 descriptors loaded.
Searching for recoverable inodes in directory / ...
1 recoverable inodes found.
Looking through the directory structure for deleted files ...
1 recoverable inodes still lost.
```

ls #Listar ficheiros/directorios da ruta actual (/root)

```
RECOVERED_FILES  recovery-data.txt  revisar.txt
```

cd RECOVERED_FILES #Acceder ao directorio RECOVERED_FILES

ls #Listar o contido da ruta actual (/root/RECOVERED_FILES)

```
file.131074
```

cat file.131074 #Ver o contido do ficheiro file.131074

```
Aprender sen pensar é inútil. Pensar sen aprender, perigoso. Confucio
```

O contido do ficheiro foi recuperado

Ricardo Feijoo Costa