NAME

fls − List file and directory names in a disk image.

SYNOPSIS

fls [-adDFlpruvV] [-m *mnt* **] [-z** *zone* **] [-f** *fstype* **] [-s** *seconds* **] [-i** *imgtype* **] [-o** *imgoffset* **] [-b dev_sector_size]** *image [images]* **[** *inode* **]**

DESCRIPTION

fls lists the files and directory names in the *image* and can display file names of recently deleted files for the directory using the given *inode.* If the inode argument is not given, the inode value for the root directory is used. For example, on an NTFS file system it would be 5 and on a Ext3 file system it would be 2.

The arguments are as follows:

-a Display the "." and ".." directory entries (by default it does not)

-d Display deleted entries only

-D Display directory entries only

-f fstype
The type of file system. Use '−f list' to list the supported file system types. If not given, autodetection methods are used.

-F Display file (all non-directory) entries only.

-l Display file details in long format. The following contents are displayed:

file_type inode file_name mod_time acc_time chg_time cre_time size uid gid

-m mnt Display files in time machine format so that a timeline can be created with mactime(1). The string given as *mnt* will be prepended to the file names as the mounting point (for example /usr).

-p Display the full path for each entry. By default it denotes the directory depth on recursive runs with a '+' sign.

-r Recursively display directories. This will not follow deleted directories, because it can't.

-s seconds
The time skew of the original system in seconds. For example, if the original system was 100 seconds slow, this value would be −100. This is only used if −l or −m are given.

-i imgtype
Identify the type of image file, such as raw. Use '−i list' to list the supported types. If not given, autodetection methods are used.

-o imgoffset
The sector offset where the file system starts in the image.

-b dev_sector_size
The size, in bytes, of the underlying device sectors. If not given, the value in the image format is used (if it exists) or 512-bytes is assumed.

-u Display undeleted entries only

-v Verbose output to stderr.

-V Display version.

-z zone The ASCII string of the time zone of the original system. For example, EST or GMT. These strings must be defined by your operating system and may vary.

image [images]
The disk or partition image to read, whose format is given with '−i'. Multiple image file names can be given if the image is split into multiple segments. If only one image file is given, and its name is the first in a sequence (e.g., as indicated by ending in '.001'), subsequent image segments

will be included automatically.

Once the inode has been determined, the file can be recovered using **icat(1)** from The Coroners Toolkit. The amount of information recovered from deleted file entries varies depending on the system. For example, on Linux, a recently deleted file can be easily recovered, while in Solaris not even the inode can be determined. If you just want to find what file name belongs to an inode, it is easier to use **ffind(1).**

EXAMPLES

To get a list of all files and directories in an image use:

```
# fls −r image 2
```

or just (if no inode is specified, the root directory inode is used):

```
# fls −r image
```

To get the full path of deleted files in a given directory:

```
# fls −d −p image 29
```

To get the mactime output do:

```
# fls −m /usr/local image 2
```

If you have a disk image and the file system starts in sector 63, use:

```
# fls −o 63 disk-img.dd
```

If you have a disk image that is split use:

```
# fls −i "split" −o 63 disk-1.dd disk-2.dd disk-3.dd
```

SEE ALSO

ffind(1), **icat**(1)

AUTHOR

Brian Carrier <carrier at sleuthkit dot org>

Send documentation updates to <doc-updates at sleuthkit dot org>