NAME

ils − List inode information

SYNOPSIS

ils [-emOpvV] [-f *fstype* **] [-s** *seconds* **] [-i** *imgtype* **] [-o** *imgoffset* **] [-b dev_sector_size]** *image [images] [start-stop]*

ils [-aAlLvVzZ] [-f *fstype* **] [-s** *seconds* **] [-i** *imgtype* **] [-o** *imgof fset* **]** *image [images] [start-stop]*

DESCRIPTION

ils opens the named *image(s)* and lists inode information. By default, **ils** lists only the inodes of removed files.

Arguments:

-e List every inode in the file system.

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

-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.

-m Display the inode details in the format that the mactime program reads (replaces the ils2mac script from TCT)

-O List only inodes of removed files that are still open or executing. This option is short-hand notation for **-aL** "(see the **fine controls** section below). (this used to be −o).

-p Display orphan inodes (unallocated with no file name)

-r (default) List only inodes of removed files. This option is short-hand notation for **-LZ** (see the **fine controls** section below).

-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.

-v Turn on verbose mode, output to stderr.

-V Display Version.

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.

start-stop
Examine the specified inode number or number range.

Fine controls:

-a List only allocated inodes: these belong to files with at least one directory entry in the file system, and to removed files that are still open or executing.

-A List only unallocated inodes: these belong to files that no longer exist.

-l List only inodes with at least one hard link. These belong to files with at least one directory entry in the file system.

-L List only inodes without any hard links. These belong to files that no longer exist, and to removed files that are still open or executing.

-z List only inodes that were likely to have not been used.

-Z List only inodes that were likely to be used.

The output format is in time machine format. The output begins with a two-line header that describes the data origin, and is followed by a one-line header that lists the names of the data attributes that make up the remainder of the output:

st_ino The inode number.

st_alloc
Allocation status: ‘a’ for allocated inode, ‘f’ for free inode.

st_uid Owner user ID.

st_gid Owner group ID.

st_mtime
UNIX time (seconds) of last file modification.

st_atime
UNIX time (seconds) of last file access.

st_ctime
UNIX time (seconds) of last inode status change.

st_dtime
UNIX time (seconds) of file deletion (LINUX only).

st_mode
File type and permissions (octal).

st_nlink
Number of hard links.

st_size File size in bytes.

st_block0,st_block1
The first two entries in the direct block address list.

SEE ALSO

mactime(1)

LICENSE

HISTORY

First appeared in The Coroners Toolkit (TCT) 1.0.

AUTHOR(S)

Wietse Venema IBM T.J. Watson Research P.O. Box 704 Yorktown Heights, NY 10598, USA

This version is maintained by Brian Carrier (carrier at sleuthkit dot org)

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