NAME

ifind − Find the meta-data structure that has allocated a given disk unit or file name.

SYNOPSIS

ifind [-avVl] [-f fstype] [-d data_unit] [-n file] [-p par_inode] [-z ZONE] [-i imgtype] [-o imgoffset] [-b dev_sector_size] *image [images]*

DESCRIPTION

ifind finds the meta-data structure that has *data_unit* allocated a data unit or has a given file name. In some cases any of the structures can be unallocated and this will still find the results.

ARGUMENTS

There are several required and optional arguments. The image file names must be specified each time:

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.

You must also specify what you are looking for and include one of the following:

-d data_unit
Finds the meta data structure that has allocated a given data unit (block, cluster, etc.)

-n file Finds the meta data structure that is pointed to by the given file name.

-p par_inode
Finds the unallocated MFT entries in an NTFS image that have the given inode as the parent. Can be used with ’−l and −z’.

There are also several optional arguments:

-a Find all meta-data structures (only works when looking with a data_unit).

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

-l List the details of each file found with ’−p’, like ’fls −l’.

-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 Verbose output to stderr.

-V Display version.

-z ZONE
If ’−p −l’ were given, this will set the timezone for the correct times.

EXAMPLES

```
# ifind −f fat −d 456 fat-img.dd

# ifind −f linux-ext2 −n "/etc/" linux-img.dd

# ifind −f ntfs −p 5 −l −z EST5EDT ntfs-img.dd
```

AUTHOR

Brian Carrier <carrier at sleuthkit dot org>

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