NAME

tsk_gettimes - Collect MAC times from a disk image into a body file.

SYNOPSIS

tsk_gettimes [-vV] [-f *fstype* **] [-i** *imgtype* **] [-b** *dev_sector_size* **] [-z** *zone* **] [-s** *seconds* **]** *image [images]*

DESCRIPTION

tsk_gettimes examines each of the file systems in a disk image and returns the data about them in the MACtime body format (the same as running ’fls −m’ on each file system). The output of this can be used as input to mactime to make a timeline of file activity. The data is printed to STDOUT, which can then be redirected to a file.

The arguments are as follows:

-v verbose output to stderr

-V Print version

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

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

-b dev_sector_size
The size (in bytes) of the device sectors. If not given, autodetection methods are used.

-o sector_offset
Sector offset for a volume to recover (recovers only that volume) If not given, will attempt to recover all volumes in image and save them to different folders.

-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.

-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.

EXAMPLES

To collect data about image image.dd:

```
# tsk_gettimes ./image.dd > body.txt
```

AUTHOR

Brian Carrier <carrier at sleuthkit dot org>

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