NAME

tsk_comparedir - compare the contents of a directory with the contents of an image or local device.

SYNOPSIS

tsk_comparedir [-vV] [-n *start_inum* **] [-f** *fstype* **] [-i** *imgtype* **] [-b** *dev_sector_size* **] [-o** *sector_offset* **]** *image [images] comparison_directory*

DESCRIPTION

tsk_comparedir compares the contents of *image* to the contents of *comparison_directory.* This can be useful for detecting rootkits and when testing. Rootkits can be detected by comparing the contents of a local directory and a local raw device. The rootkits typically don't hide data when it is read directly from the raw device.

The arguments are as follows:

-o sector_offset
: Sector offset for a partition in the image or device to compare with.

-n start_inum
: Starting inum for a directory in the image to start the comparison at.

-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.

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 compare the directories in image.dd to those in directory:

```
# tsk_comparedir ./image.dd ./directory
```

AUTHOR

Brian Carrier <carrier at sleuthkit dot org>

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