NAME

mactime − Create an ASCII time line of file activity

SYNOPSIS

mactime [-b *body* **] [-g** *group file* **] [-p** *password file* **] [-i** *(day|hour) index file* **] [-dhmVy] [-z** *TIME_ZONE* **] [DATE_RANGE]**

DESCRIPTION

mactime creates an ASCII time line of file activity based on the body file specified by ’−b’ or from STDIN. The time line is written to STDOUT. The body file must be in the time machine format that is created by ’ils −m’, ’fls −m’, or the mac-robber tool.

ARGUMENTS

-b body Specify the location of a body file. This file must be generated by a tool such as ’fls −m’ or ’ils −m’. The ’mac-robber’ and ’grave-robber’ tools can also be used to generate the file.

-g group file
: Specify the location of the group file. mactime will display the group name instead of the GID if this is given.

-p password file
: Specify the location of the passwd file. mactime will display the user name instead of the UID of this is given.

-i day|hour index file
: Specify the location of an index file to write to. The first argument specifies the granularity, either an hourly summary or daily. If the '−d' flag is given, then the summary will be separated by a ’,’ to import into a spread sheet.

-d Display timeline and index files in comma delimited format. This is used to import the data into a spread sheet for presentations or graphs.

-h Display header info about the session including time range, input source, and passwd or group files.

-V Display version to STDOUT.

-m The month is given as a number instead of name (does not work with −y).

-y The date is displayed in ISO8601 format.

-z TIME_ZONE
: The timezone from where the data was collected. The name of this argument is system dependent (examples include EST5EDT, GMT+1). Does not work with −y.

-z list List valid timezones.

DATE_RANGE
: The range of dates to make the time line for. The standard format is yyyy-mm-dd for a starting date and no ending date. For an ending date, use yyyy-mm-dd..yyyy-mm-dd. Date can contain time, use format yyyy-mm-ddThh:mm:ss for starting and/or ending date.

LICENSE

The changes from mactime in TCT and mac-daddy are distributed under the Common Public License, found in the *cpl1.0.txt* file in the The Sleuth Kit licenses directory.

HISTORY

A version of **mactime** first appeared in **The Coroner’s Toolkit (TCT) (Dan Farmer)** and later **mac-daddy (Rob Lee)**.

AUTHOR

Brian Carrier <carrier at sleuthkit dot org>

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