

TCTUTILS INSTALLATION & USE

Taken From the TCTUTILS Documentation (Brian Carrier)

Introduction

TCTUTILS use functions and structures from The Coroners Toolkit (TCT) and provides further functionality. The biggest new addition is the utility 'fls' that processes a directory inode. It allows deleted file names to be displayed and allows the file structure of a drive image to be examined. These tools can be combined with the Autopsy Forensic Browser for a graphical interface to images.

Installation

1. Put the files in any directory, i.e. /usr/local/tctutils.
2. Edit the TCT_DIR entry in the src/Makefile to point to the TCT installation (default: usr/local/tct)
3. Type make. This will place the executable files in the bin directory.
4. If you want to also use the Autopsy Forensic Browser, it will be easiest to maintain if symlinks are created from /usr/local/tctutils 1to /usr/local/tctutils-X and similarly from tct to tct-X.

Program Descriptions

bcat

Desc: Display the contents of a disk block to stdout

Input: image

block number

of bytes to read (must be a multiple of DEV_BSIZE, 512 usually)

Opt: -a Displays in all ASCII

-f fstype (currently only swap is supported. Otherwise uses the default for the system.

-h Displays in hexdump like fashion

-s Display block stats about the image

-w Print in HTML format (with tables)

Uses: This can be used to show the contents of a block that has been identified by running grep on an image. Or it can be used to test other programs that try and parse the contents of the block. If swap is selected as the fstype, then it opens the image as a normal file. In this case, the supplied "block number" is used as a "page number" where pages are 4096 bytes each.

fls

Desc: List the file and directory entries in a directory inode. By default it will print all entries in the directory (including deleted file names) and will not print "." or "..". Deleted files are denoted by a '*'.

TCTUTILS INSTALLATION & USE

Taken From the TCTUTILS Documentation (Brian Carrier)

Input: image
inode number of directory

Opt: -a Display "." and ".."
-d Display deleted entries only
-D Display directory entries only
-f Display file (all non-directory) entries only
-l Long format. display all associated inode data
-m Display in mactimes like fashion. Requires a string argument to denote mounting point is for the image.
-p Display the full path for each entry. By default it denotes directory depth on recursive printouts with a '+' sign.
-r Recursively display directories. Will not follow deleted directories, because it can't.
-u Display undeleted entries only
-z Time zone difference in hours. This is only useful when the -l option is used

Uses: This tool has many interesting uses. First, it will show you the deleted file names. Depending on the OS, the inode number may still be available and the inode can be viewed using `istat` or `icat`. The `-m` option allows files that were deleted with still valid inodes to be used in a `mactimes` time line. By using the `mac_merge` perl script, the two outputs can be parsed together to form a useful time line. Combine this with `ils` and `ils2mac` to determine some of the names of deleted inodes. The time zone difference allows an analysis to be performed in a different time zone, while viewing the time that would be seen if you were on-site. This makes it easier to correlate times given from `fls` with times in log entries.

find_file

Desc: Given an image and an inode number, determine which file has allocated it. This program searches recursively through directory inodes until it finds a file with the inode number. This means that deleted files will also be printed if the entry has not been overwritten. It is similar to doing a recursive `fls` and grepping out the inode number. Deleted files are prepended by a '*'. This is very similar to the UNIX `ncheck(1)` utility, except that it uses TCT code and displays deleted file names.

Input: image
inode

Opt: -a find all occurrences (default is just the first one)
-d display only deleted entries
-u display only undeleted entries

TCTUTILS INSTALLATION & USE

Taken From the TCTUTILS Documentation (Brian Carrier)

Uses: This can be used to find out which file has allocated a block that contains interesting data. When used in conjunction with `find_block`, the file that is using a block can be determined.

find_inode

Desc: Given an image and a block number, determine which inode has allocated it. This program searches all the inodes to determine which one has it its block lists. If it isn't, but it is within the range as a possible fragment, it will be returned.

Input: image
block

Uses: This can be used to determine which file has allocated a block that contains interesting data. The inode number can be fed into `find_inode` to determine which file is using the inode.

istat

Desc: Given an image and an inode, display information about the inode. This is a more glorious version of `'ils -a'` using TCT.

Input: image
inode

Opt: `-v` verbose
`-z` time zone difference in hours. Allows the times displayed to be in the compromised system time, not in local time.

Uses: This allows verbose data about an inode to be easily displayed. Prints all blocks and mac times.

mac_merge

Desc: Merge the output from `'fls -m'` with TCT mactimes output to create one big time line. The output is sent to stdout.

Input: output from mactimes
output from `'fls -m'`