NAME

fiwalk - print the filesystem statistics and exit

SYNOPSIS

fiwalk [*options*] *iso-name*

DESCRIPTION

fiwalk is a program that processes a disk image using the SleuthKit library and outputs its results in Digital Forensics XML, the Attribute Relationship File Format (ARFF) format used by the Weka Datamining Toolkit, or an easy-to-read textual format.

This application uses SleuthKit to generate a report of all of the files and orphaned inodes found in a disk image. It can optionally compute the MD5 of any objects, save those objects into a directory, or both.

OPTIONS

-c config.txt

> read config.txt for metadata extraction tools

-C nn   only process nn files, then do a clean exit

Include/exclude parameters; may be repeated:

-n pattern

> only match files for which the filename matches the pattern. Example: **-n** .jpeg **-n** .jpg will find all JPEG files. Case is ignored. Will not match orphan files.

Ways to make this program run faster:

-I   ignore NTFS system files

-g   just report the file objects - don't get the data

-O   only walk allocated files

-b   do not report byte runs if data not accessed

-z   do not calculate MD5 or SHA1 values

-Gnn   Only process the contents of files smaller than nn gigabytes (default 2). Use **-G0** to remove space restrictions.

Ways to make this program run slower:

-M   Report MD5 for each file (default on)

-1   Report SHA1 for each file (default on)

-f   Report the output of the 'file' command for each

Output *options*: **-m** = Output in SleuthKit 'Body file' format

-A<file>

> ARFF output to <file>

-X<file>

> XML output to a <file> (full DTD)

-X0   Write output to filename.xml

-Z   zap (erase) the output file

-x   XML output to stdout (no DTD)

-T<file>

> Walkfile output to <file>

-a <audit.txt>

> Read the scalpel audit.txt file

Misc:

        -d   debug this program

        -v   Enable SleuthKit verbose flag

AUTHOR

The Sleuth Kit was written by Brian Carrier <carrier@sleuthkit.org>.

This manual page was written by Joao Eriberto Mota Filho <eriberto@debian.org> for the Debian project (but may be used by others).