

[TOOL] The Sleuth Kit – UNIX–based File System and Media Management Forensic Analysis Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0126.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/28/03

To: list@securiteam.com

Date: 28 Oct 2003 18:36:49 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

The Sleuth Kit – UNIX–based File System and Media Management Forensic Analysis Tool

DETAILS

The Sleuth Kit (previously known as TASK) is a collection of UNIX–based command line file system and media management forensic analysis tools. The file system tools allow you to examine NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems of a suspect computer in a non–intrusive fashion. The tools have a layer–based design and can extract data from the internal file system structures. Because the tools do not rely on the operating system to process the file systems, deleted and hidden content is shown.

The media management tools allow you to examine the layout of disks and other media. The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, and Sun slices (Volume Table of Contents). With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools.

When performing a complete analysis of a system, we all know that command line tools can become tedious. The Autopsy Forensic Browser is a graphical interface to the tools in The Sleuth Kit, which allows you to more easily conduct an investigation. Autopsy provides case management, image

Securiteam: [TOOL] The Sleuth Kit – UNIX–based File System and Media Management Forensic Analysis Tool

integrity, keyword searching, and other automated operations.

The Sleuth Kit and Autopsy are both open source and free to download.

Their combined features include:

- * View Allocated and Deleted Files and Directories
- * Access to low–level file system structures
- * Timeline of file activity
- * File category sorting and extension checking
- * Keyword searches including grep regular expressions
- * Graphic image identification and thumbnail creation
- * Hash database lookups including the NIST NSRL and Hash Keeper
- * Investigator notes
- * Report generation

Sleuth Kit Features:

- * Analyzes file system images generated by the 'dd' command, which is found on all UNIX systems and is available for Windows systems. This is a raw format and not proprietary.
- * Supports the NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems even when the host operating system does not or has a different endian ordering.
- * Displays both allocated and deleted file names
- * Displays the details file system structures
- * Displays the details and contents of all attributes for NTFS files. This includes all Alternate Data Streams and even the contents of the standard attributes such as \$STANDARD_INFORMATION.
- * Creates timelines of file activity and can import logs and other time–based events. The timelines can be imported into a spread sheet to create graphs and reports. (Sleuth Kit Informer #5)
- * Time–based tools take a timezone and time skew as arguments so that you can view times as they existed on the original host.
- * Contains a hash lookup tool that creates an index of hash database files and performs quick lookups using a binary search algorithm. The tool supports the NIST NSRL, Hash Keeper, and custom databases that have been created with the 'md5sum' tool. (Sleuth Kit Informer #6, Sleuth Kit Informer #7)

Securiteam: [TOOL] The Sleuth Kit – UNIX–based File System and Media Management Forensic Analysis Tool

* Files can be organized based on their file type. For example, all graphic images and/or executables can be easily identified and examined. While they are being sorted, hash databases can be consulted to ignore known files (such as system files that are trusted) and to alert when known bad files are found (such as known rootkits or inappropriate photographs). The extensions of files are also verified to identify files that are being hidden. Pages of thumbnails can be made of graphic images for quick analysis. (Sleuth Kit Informer #3, #4, #5)

* Tools can be run on a live UNIX system during Incident Response. These tools will show files that have been "hidden" by rootkits and will not modify the A–Time of files that are viewed.

* Partitions of different platforms and endian orderings can be extracted and analyzed using the media management tools.

* Open source software allows you to customize the tools for your environment and validate the code. See Open Source Digital Forensics Tools: The Legal Argument.

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://www.sleuthkit.org/sleuthkit/desc.php>>

<http://www.sleuthkit.org/sleuthkit/desc.php>.

The information has been provided by Brian Carrier.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list–unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list–subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.