

File Activity Timelines

Sleuth Kit Reference Document

www.sleuthkit.org

Brian Carrier

Last Updated: June 2003

Introduction

Creating a timeline of file activity will give an investigator clues regarding where to probe further. This document will describe how to generate one using The Sleuth Kit. The timelines in The Sleuth Kit allow one to quickly get a high-level look at system activity, such as when files were compiled and when archives were opened.

Background

Many files and directories have times associated with them. The quantity and description of which depend on the file system type. FFS file systems have a Modified, Accessed, and Changed time associated with them. EXT2FS file systems have a Modified, Accessed, Changed, and Deleted time. FAT stores the Written, Accessed, and Created time, although by spec the Created and Access times are optional and the Access time is only accurate to the day.

Timeline Creation

The creation of a file activity timeline in The Sleuth Kit has three phases.

1. Gather file data. Using the 'fls' tool, the data associated with allocated and some unallocated files can be gathered. To do this requires the '-m' argument with the '-r' flag to gather all files. This needs to be done for each partition image.

```
# fls -f openbsd -m / -r images/root.dd > data/body
# fls -f openbsd -m /var/ -r images/var.dd >> data/body
# fls -f openbsd -m /usr/ -r images/usr.dd >> data/body
```

NOTE: Some systems delete the link between deleted file names and meta data, such as Solaris, so only information about allocated files will be useful.

NOTE: This replaces the actions of 'grave-robber -m' in TCT. The 'mac-robber' tool (on the www.sleuthkit.org web site) can also be used to gather allocated file data on a mounted file system. 'mac-robber' is useful for file systems where tools do not exist (such as AIX jfs).

2. Gather unallocated meta data. Using the 'ils' tool, the data associated with unallocated meta data can be gathered. When files are deleted, the times associated with the file are updated. Although many times we may not be able to link the original name to the meta data, it will still give some clue with respect to when activity occurred. This uses the '-m' flag of 'ils'.

```
# ils -f openbsd -m images/root.dd >> data/body
# ils -f openbsd -m images/root.dd >> data/body
# ils -f openbsd -m images/var.dd >> data/body
# ils -f openbsd -m images/usr.dd >> data/body
```

NOTE: Because of the way that FAT stores time, the timezone is needed while executing 'ils'. If you will be giving 'mactime' a timezone to use then set the TZ environment variable:

```
# set TZ=EST5EDT
```

3. Format the data nicely. The 'body' file now needs to be run through the 'mactime' program to sort it and make it organized.

```
# mactime -b data/body 3/01/2002 > t1.03.01.2002
```

The above command generates a timeline of file activity from the previously created data/body file for all activity starting in March. If the /etc/passwd or /etc/group files are known, they can be specified using the '-p' and '-g' flags. Otherwise the numerical values will be displayed. The '-z' flag can be used to specify the time zone.

```
# mactime -b data/body -p data/passwd -g data/group 3/01/2002 >
t1.03.01.2002
```

The output format has changed slightly since the 'mactime' in TCT. The inode value is now displayed in a separate column. Previously it was not displayed.

Some example outputs of mactime will now be shown. The next two entries are for a deleted socket in an EXT2FS image:

```

Wed Mar 20 2002 16:56:12 0 ..c s/srwxrwxr-x 500 500 127 /tmp/
socket1 (deleted)
                                0 ..c      srwxrwxr-x 500 500 127 <linux.
dd-dead-127>

```

The first is the 'fls' entry and the second is the corresponding entry from 'ils'. While it may seem redundant to show both, many times 'fls' will not show the deleted file name because the entry has been reallocated. Therefore, just the 'ils' dead entry will appear and the investigator will not know the original path location.

The first 0 is the file size. The "..c" string means that this entry is for the "Change" value. The dots are replaced with 'm' or 'a' for other entry types (deleted entries are not created for EXT2FS). The next string is the file system mode. The entries from 'fls' will have the directory entry type first, followed by a slash and the mode from the inode entry. 'ils' entries will only have the inode mode. The next two are the UID and GID (or names if the group and passwd file are specified), followed by the inode. The final entry is the file name (or for unallocated inodes).

The next two are for file that is deleted, but the inode that the directory entry points to is deleted.

```

Fri Aug 23 2002 16:56:12 11 .a. l/-rw-r--r-- 0 0 34689 /tmp/
file1 (deleted-realloc)
                                11 .a. -/-rw-r--r-- 0 0 34689 /etc/
sysconfig/desktop

```

This can be seen because they are both entries for the deleted file (tmp/file1) and the allocated file (desktop), which have the same inode (34689). It can also be seen because the deleted entry has different values for the file type (l and -).

If you are going to include the resulting timeline in a document, then it may be better to supply the '-d' argument to output in comma delimited format. The resulting timeline can then be imported into a spreadsheet and included as a table.

The '-i' option to 'mactime' creates an index summary file, including how many hits were found per day or hour. Using '-d' with '-i' allows one to easily import data into a spreadsheet that can be graphed to spot suspicious behavior.

```

# mactime -b data/body -d -i hour data/tl-hour-sum.txt > data/
timeline.txt

```

Time Skew

The time skew of the system can also be taken into consideration. Using the '-s' argument to 'fls' and 'ils', the intermediate body file can have the adjusted times so that the system is consistent with other servers.

The argument reflects the skew in seconds. If the original system was 100 seconds slower than NTP or some other 'main' server, then the argument would be '-s -100'. If it were 145 seconds fast, then it would be '-s 145'.

Autopsy

The Autopsy Forensic Browser is a graphical interface to The Sleuth Kit and it can automate the process of creating and viewing a time line.

<http://www.sleuthkit.org/autopsy>

Copyright © 2002-2003 by Brian Carrier. All Rights Reserved