Sleuth-Kit overview[2]

File System Tools

File System Layer Tools

fsstat: Shows file system details and statistics including layout, sizes, and labels.

File Name Layer Tools

ffind: Finds allocated and unallocated file names that point to a given meta data structure.

fls: Lists allocated and deleted file names in a directory.

Meta Data Layer Tools

icat: Extracts the data units of a file, which is specified by its meta data address (instead of the file name).

ifind: Finds the meta data structure that has a given file name pointing to it or the meta data structure that points to a given data unit.

ils: Lists the meta data structures and their contents in a pipe delimited format.

istat: Displays the statistics and details about a given meta data structure in an easy to read format.

Data Unit Layer Tools

blkcat: Extracts the contents of a given data unit.

blkls: Lists the details about data units and can extract the unallocated space of the file system.

blkstat: Displays the statistics about a given data unit in an easy to read format.

blkcalc: Calculates where data in the unallocated space image (from blkls) exists in the original image. This is used when evidence is found in unallocated space.

File System Journal Tools

jcat: Display the contents of a specific journal block.

jls: List the entries in the file system journal.

Volume System Tools

mmls: Displays the layout of a disk, including the unallocated spaces.

mmstat: Display details about a volume system (typically only the type).

mmcat: Extracts the contents of a specific volume to STDOUT.

Image File Tools

img_stat: tool will show the details of the image format

img_cat: This tool will show the raw contents of an image file.

Disk Tools

disk_sreset: This tool will temporarily remove a HPA if one exists. After the disk is reset, the HPA will return.

disk_stat: This tool will show if an HPA exists.

Other Tools

hfind: Uses a binary sort algorithm to lookup hashes in the NIST NSRL, Hashkeeper, and custom hash databases created by md5sum.

mactime: Takes input from the fls and ils tools to create a timeline of file activity.

sorter: Sorts files based on their file type and performs extension checking and hash database lookups.

sigfind: Searches for a binary value at a given offset. Useful for recovering lost data structures.

References

[1] CARRIER, BRIAN: The Sleuth Kit. http://www.sleuthkit.org/

[2] CARRIER, BRIAN: The Sleuth Kit Wiki, *TSK Tool Overview.* http://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview

[3] GRUNDY, BARRY J.(2008): The Law Enforcement and Forensic Examiners Introduction to Linux v3.78. *A Practioner's Guide to Linux as a Computer Forensic Platform* http://www.linuxleo.com/

[4] SANS-INSTITUTE http://www.sans.org/

The Forensic-Cheat-Sheet for Linux and TSK

Jens Vieweg

Last updated 2009/07/29

Inspired by the S.A.N.S. Institute's[4] Forensic Cheatsheet and based on the modus operandi Barry J. Grundy introduces in his Book.[3]

Retrieving disk information

```
# fdisk -l /dev/sdb
```
Partition start, end and type

```
# sfdisk -l -uS image.dd
```
or `/dev/sda1`

Partition start and end in Sectors

Imaging

dd

Make an image Inputfile, Outpufile, Blocksize

```
# dd if=/dev/sda1 of=/evidence/image.dd bs=4096
```

dc3dd

```
# dc3dd if=/dev/sdb1 of=/evidence/image1.dc3dd
progress=on hashwindow=32M hash=md5
log=/evidence/image1.dc3dd.log
```

Calculates md5-hash for 32MB packages, writes hashes and errors to log

mounting

```
# mount -t ntfs -o ro,noexec,loop image.dd
/mnt/analysis
```

Mount an NTFS-Image on loopbackdevice

NetCat

Suspect machine:

```
# dd if=/dev/sda ¦nc 192.168.55.20 4747
```

Analysis machine:

```
# nc -l -p 4747 ¦dd of=/evidence/net_image.dd
```

Extracting partition images from full disk image:

```
# dd if=image.dd of=image.part1.dd bs=512 skip=57
count=10203
```

bs, skip and count from sfdisk output

Integrity Checking

```
# sha1sum /dev/sdb > image.sha1
```
Calculate SHA1 Cheksum
```
# find .  -type f -exec sha1sum {} \; >
/evidence/image.filelist.sha1
```
List all files with SHA1 Checksum (run in mounted Image root)
```
# sha1sum -c /evidence/image.sha1
```
Checks if image matches original partition
```
# sha1sum -c /evidence/image.filelist.sha1 ¦grep
failed
```
Checks if all files match originals (run in mounted Image root)
All checks can be done with md5sum instead of sha1sum

Search for hidden files

Gather information about the image:
```
# img_stat image.dd
# mmls image.dd
# mmls -i raw -t dos
03:   00:01   0000010260   0000112859   0000102600   Linux
(0x83)
```
Gather information about filesystem(s):
```
# fsstat -o 10260 image.dd
```
Show root directory:
```
# fls -o 10260 image.dd
d/d 11105:   .001
```
Show directory content
```
# fls -o 10260 image.dd 11105
```
Show all deleted files with inodes:
```
# fls -o 10260 -Frd image.dd
```
Show all filenames for an inode:
```
# ffind -o 10260 image.dd 1239
```
Get information and content for an inode: `# istat -o 10260 image.dd 2139`
```
# icat -o 10260 image.dd 2139 ¦file -
```
Recover deleted file:
```
# icat -o 10260 image.dd 2139 > filename.2139
```

String Searches & some Calculations

String searches on Image:
```
# strings -radix=d image.dd
# cat image.dd  strings  grep -i -f wordlist -A 2
-B 2
# grep -abi password image.dd
```
treat as text, byte offset, not casesensitive
```
10561603:  *   password for root...
```
Hexeditor view of the line by File offset:
```
xxd -s 10561603 image.dd ¦head -n 5
```
Find out Sectornumber:
```
# echo "10561603/512" ¦bc
20628
```
Find out Partition offset in blocks:
```
# mmls image.dd
03:   00:01   0000010260   0000112859   0000102600   Linux
(0x83)
```
Change Partition offset to blocks and subtract from File offset:
```
# echo "10561603-(10260*512)" ¦bc
5308483
```
Retrieve Block or Clustersize:
```
# fsstat -o 10260 -f ext image.dd
```
Calculate Blocknumbber in the partition:
```
# echo "5308483/1024 ¦bc
5184
```
Find out if block is allocated:
```
# blkstat -o 10260 -f ext image.dd 5184
```
Find inode vor blocknumber:
```
# ifind -o 10260 -f ext -d 5184 image.dd
10090
```
Get fileinformation and file:
```
# istat -o 10260 -f ext image.dd 10090
# icat -r -o 10260 -f ext image.dd 10090 >
filename.10090
```
Maybe do a search before:
```
ffind -o 10260 image.dd 10090
```

Handling Unallocated Space

Extract unallocated space from disk or partition:
```
# blkls image.part1.dd or -o 10260 image.dd
# blkls image.part1.dd > image.blkls
```
Discover evidence:
```
# blkls image.part1.dd ¦strings ¦less
# grep -abi word image.blkls
1631299:looking for the word...
```
Find in original image:
```
# echo "1631299/1024" ¦bc
1593
# blkcalc -o 10260 -u 1593 image.dd
5184
```
Retrieve information:
```
# blkstat -o 10260 image.dd 5184
# blkcat -o 10260 image.dd 5184 ¦xxd ¦less
```
Followed by `ifind, istat, icat`

NTFS Alternate Data Streams (ADS)

Find ADS suspects in image:
```
# fls -Fr -f ntfs image.part1.dd¦grep -v \\$¦grep
:.*: r/r 137-128-3:   normal.doc
r/r 137-128-4:   normal.doc:badhack.txt
```
View ADS:
```
# icat -f ntfs image.part1.dd 137-128-4
```

Sorting

First preview:
```
# sorter -l -o 59 -f ntfs image.dd
```
Full overview in subdirectory with index.html:
```
««««< .mine sorter -d ./sort_ dir -md5 -h -s -o 59 -f
ntfs image.dd
=======   sorter -d ./sort_dir -md5 -h -s -o 59 -f
ntfs image.dd
»»»» .r48 Preparing NIST NSRLFile:
# hfind -i nsrl-md5 NSRLFile.txt
```
Leaving out known files by hash:
```
««««    .mine    # sorter -s -d ./sort_ dir -o 59 -n
NSRLFile.txt -f ntfs image.dd   =======   # sorter
-s -d ./sort_dir -o 59 -n NSRLFile.txt -f ntfs
image.dd
»»»» .r48
```