SANS Investigative Forensics Toolkit Documentation

Release 3.0

SANS Institute

Nov 07, 2017

Contents

1 User Manual **3**
- 1.1 User Manual . . . 3
  - 1.1.1 Installation . . . 3
  - 1.1.2 Packages . . . 4
  - 1.1.3 Supported Filesystems . . . 7
  - 1.1.4 Evidence Image File Support . . . 8
  - 1.1.5 Partition Table Support . . . 8

2 Tools **9**
- 2.1 License(s) . . . 9
  - 2.1.1 Packages . . . 9
  - 2.1.2 Scripts . . . 11
  - 2.1.3 Volatility Plugins . . . 11
  - 2.1.4 License Info . . . 12
- 2.2 Tools, Commands, Scripts . . . 12
  - 2.2.1 All Tools . . . 12
  - 2.2.2 Registry Analysis . . . 12
  - 2.2.3 Artifact Analysis . . . 12

3 Packages **13**
- 3.1 Packages . . . 13
  - 3.1.1 All Packages . . . 13

4 Cheatsheet **17**
- 4.1 Cheatsheet . . . 17
  - 4.1.1 Mounting DD Images . . . 17
  - 4.1.2 Mounting E01 Images . . . 17
  - 4.1.3 Mounting Split Raw Images . . . 18
  - 4.1.4 Creating Super Timelines . . . 18
  - 4.1.5 String Searches . . . 18
  - 4.1.6 Memory Analysis . . . 18
  - 4.1.7 Recovering Deleted Registry Hives . . . 19
  - 4.1.8 Recovering Data . . . 19
  - 4.1.9 SleuthKit Tools . . . 19

5 About **25**
- 5.1 About . . . 25

SIFT is a collection of various tools to aid you in performing forensics analysis tasks.

SIFT would not be possible without all the open source tools and their authors and the communities behind them. Thank you.

Documentation Status: Work In Progress - ALPHA

The documentation is organized into a few different sections below:

- *User Manual*
- *Tools*
- *Packages*
- *Cheatsheet*
- *About*

CHAPTER 1

User Manual

The User Manaul covers general use of the toolkit along with installation and upgrade instructions.

1.1 User Manual

Welcome to the User's Manual

1.1.1 Installation

We tried to make the installation (and upgrade) of the SIFT workstation as simple as possible, so we create the SIFT Bootstrap project, which is a shell script that can be downloaded and executed to convert your Ubuntu installation into a SIFT workstation.

Check the project out at https://github.com/sans-dfir/sift-bootstrap

Quickstart

Using *wget* to install the latest

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh␣
↪| sudo bash -s -- -i
```

Using *curl* to install the latest

```
curl --silent -L https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh␣
↪| sudo bash -s -- -i
```

Using *wget* to install the latest, configure and use apply the SIFT theme

```
wget --quiet -O - https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh␣
↪| sudo bash -s -- -i -s -y
```

1.1.2 Packages

SIFT is built on a collection of various tools that are available for Ubuntu Linux or that have been packaged up by members of the community and hosted on launchpad.net.

Name	Version	Docs and Links
4n6time-static	1.0.1-1ubuntu1	
aeskeyfind	1:1.0-1	
afflib-tools	3.6.6-1.1	/tools/afflib
afterglow	1.6.4-ubuntu1	
aircrack-ng	1.2-beta2-sift1	
arp-scan	1.8.1-1	
autopsy	2.24-1	
bcrypt	1.1-6	
binplist	0.1.4-0ubuntu1	
bitpim	1.0.7+dfsg1-2build1	
bitpim-lib	1.0.7+dfsg1-2build1	
bkhive	1.1.1-1	
bless	0.6.0-3	
blt	2.4z-4.2ubuntu1	
build-essential	11.5ubuntu2.1	
bulk-extractor	1.4.0-beta5-ubuntu5	
cabextract	1.4-1	
ccrypt	1.9-4	
clamav	0.97.8+dfsg-1ubuntu1.12.04.1	
cmospwd	5.0	
cryptcat	20031202-4	
cryptsetup	2:1.4.1-2ubuntu4	
curl	7.22.0-3ubuntu4.7	
dc3dd	7.1.614-1	
dcfldd	1.3.4.1-2	
dconf-tools	0.12.0-0ubuntu1.1	
dff	1.2.0+dfsg.1-1	
driftnet	0.1.6-9ubuntu1	
dumbpig	0.10-ubuntu1	
e2fslibs-dev	1.42-1ubuntu2	
ent	1.1debian-1.1	
epic5	1.1.2-2build1	
etherape	0.9.12-1	
ettercap-graphical	1:0.7.4.2-1	
ettercap-text-only	1:0.7.4.2-1	
exif	0.6.20-1	
extundelete	0.2.0-2 precise	
f-spot	0.8.2-4	
fdupes	1.50-PR2-3	
flare	0.15.1-1	
flasm	1.62-6	
flex	2.5.35-10ubuntu3	
foremost	1.5.7-1	
fuse-utils	2.8.6-2ubuntu2	
g++	4:4.6.3-1ubuntu5	

Continued on next page

Table 1.1 – continued from previous page

Name	Version	Docs and Links
gcc	4:4.6.3-1ubuntu5	
gdb	7.4-2012.04-0ubuntu2.1	
gddrescue	1.14-1	
ghex	3.4.0-0ubuntu1	
gthumb	3:2.14.3-0ubuntu1	
gzrt	0.5-2ubuntu1	
hal	0.5.14-8	
hal-info	20091130-1	
hexedit	1.2.12-4	
honeyd	1.5c-8ubuntu1	
htop	1.0.1	
hydra	7.1-1build1	
hydra-gtk	7.1-1build1	
ipython	0.12.1+dfsg-0ubuntu1	
jdgui	0.3.5	
kdiff3	0.9.96-2	
knocker	0.7.1-3.1	
kpartx	0.4.9-3ubuntu5	
libafflib0	3.6.6-1.1	/tools/afflib
libbde	20130908-1ubuntu2	/tools/libbde
libbde-tools	20130908-1ubuntu2	/tools/libbde
libesedb	20120102-1ubuntu1	/tools/libesedb
libesedb-tools	20120102-1ubuntu1	/tools/libesedb
libevt	20131013-1ubuntu1	/tools/libevt
libevt-tools	20131013-1ubuntu1	/tools/libevt
libevtx	20131013-1ubuntu1	/tools/libevtx
libevtx-tools	20131013-1ubuntu1	/tools/libevtx
libewf	20131210-1ubuntu2	/tools/libewf
libewf-dev	20131210-1ubuntu2	/tools/libewf
libewf-python	20131210-1ubuntu2	/tools/libewf
libewf-tools	20131210-1ubuntu2	/tools/libewf
libfuse-dev	2.8.6-2ubuntu2	
libfvde	20130305-1ubuntu3	/tools/libfvde
libfvde-tools	20130305-1ubuntu3	/tools/libfvde
liblightgrep	1.2.1-ubuntu2	
libmsiecf	20131015-1ubuntu1	
libnet1	1.1.4-2.1	
libolecf	20131108-1ubuntu1	
libparse-win32registry-perl	0.60-1	
libplist1	1.8-1	
libplist-dev	1.8-1	
libregf	20130922-1ubuntu2	
libregf-dev	20130922-1ubuntu2	
libregf-python	20130922-1ubuntu2	
libregf-tools	20130922-1ubuntu2	
libssl-dev	1.0.1-4ubuntu5.10	
libtext-csv-perl	1.21-1	
libvshadow	20131209-1ubuntu2	/tools/libvshadow
libvshadow-dev	20131209-1ubuntu2	/tools/libvshadow

Continued on next page

Table 1.1 – continued from previous page

Name	Version	Docs and Links
libvshadow-python	20131209-1ubuntu2	/tools/libvshadow
libvshadow-tools	20131209-1ubuntu2	/tools/libvshadow
libxml2-dev	2.7.8.dfsg-5.1ubuntu4.6	
lft	2.2-4	
mac-robber	1.02-sift1	
maltegoce	3.4.0.5004-ubuntu1	
md5deep	3.9.2-1	
myunity	3.1.3-0ubuntu1	
nbd-client	2.9.25-2ubuntu1	
nbtscan	1.5.1-6	
netcat	1.10-39	
netpbm	2:10.0-15	
netsed	1.00b-2	
netwox	5.36.0-1.2	
nfdump	1.6.11-sift1	
ngrep	1.45.ds2-11	
nikto	1:2.1.4-2	
ntopng	1.1	
okular	4:4.8.5-0ubuntu0.1	
openjdk-6-jdk	6b27-1.12.6-1ubuntu0.12.04.4	
ophcrack	3.3.0-1build1	
ophcrack-cli	3.3.0-1build1	
outguess	1:0.2-7	
perl-log2timeline	UNKNOWN	/tools/log2timeline
p7zip-full	9.20.1~dfsg.1-4	
phonon	4:4.7.0really4.6.0-0ubuntu1	
p0f	2.0.8-2	
pv	1.2.0	
pyew	2.0-3	
python	2.7.3-0ubuntu2.2	
python-analyzemft	2.0.11-ubuntu2	
python-flowgrep	0.9-ubuntu2	
python-nids	0.6.1-1build1	
python-ntdsxtract	1.2-beta-ubuntu6	
python-pefile	1.2.9.1-1	
python-plaso	1.0.2-3	/tools/plaso
python-qt4	4.9.1-2ubuntu1	
python-tk	2.7.3-1ubuntu1	
python-yara	1.7-1ubuntu1~ppa1~p	
pytsk3	4.1.2-1ubuntu2	
qemu	1.0+noroms-0ubuntu14.12	/tools/qemu
qemu-utils	1.0+noroms-0ubuntu14.12	/tools/qemu
readpst	0.6.54-0ubuntu1	
rsakeyfind	1:1.0-2build1	
safecopy	1.6-1build1	
scalpel	1.60-1build1	
samdump2	1.1.1-1	
socat	1.7.1.3-1.2	
sleuthkit	4.1.3-1ubuntu5	/tools/sleuthkit

Continued on next page

Table 1.1 – continued from previous page

Name	Version	Docs and Links
ssdeep	2.7-1	
ssldump	0.9b3-4.1	
stegdetect	1.0-precise1	
stunnel4	3:4.42-1	
tcl	8.5.0-2 precise	
tcpflow	0.21.ds1-6	
tcpreplay	3.4.3-2ubuntu2	
tcpstat	1.5-7	
tcptrace	6.6.7-4	
tcptrack	1.4.2-1build1	
tcpxtract	1.0.1-8	
testdisk	6.13-1	
tofrodos	1.7.9.debian.1-1	
torsocks	1.2-1	
transmission	2.51-0ubuntu1.3	
unrar	1:4.0.3-1	
upx-ucl	3.08-2ubuntu1	
vbindiff	3.0-beta3-1	
virtuoso-minimal	6.1.4+dfsg1-0ubuntu1	
winbind	2:3.6.3-2ubuntu2.9	
wine	1.4-0ubuntu4.1	
wireshark	1.6.7-1	
xmount	0.4.5-1	
zenity	3.4.0-0ubuntu4	

1.1.3 Supported Filesystems

1. ntfs (NTFS)
2. iso9660 (ISO9660 CD)
3. hfs (HFS+)
4. raw (Raw Data)
5. swap (Swap Space)
6. memory (RAM Data)
7. fat12 (FAT12)
8. fat16 (FAT16)
9. fat32 (FAT32)
10. ext2 (EXT2)
11. ext3 (EXT3)
12. ext4 (EXT4)
13. ufs1 (UFS1)
14. ufs2 (UFS2)
15. vmdk

1.1.4 Evidence Image File Support

1. raw (Single raw file (dd))
2. aff (Advanced Forensic Format)
3. afd (AFF Multiple File)
4. afm (AFF with external metadata)
5. afflib (All AFFLIB image formats (including beta ones))
6. ewf (Expert Witness format (encase))
7. split raw (Split raw files) via affuse

1. affuse mount 001 image/split images to view single raw file and metadata

8. split ewf (Split E01 files) via mount_ewf.py

1. mount_ewf.py mount E01 image/split images to view single raw file and metadata
2. ewfmount – mount E01 images/split images to view single rawfile and metadata

1.1.5 Partition Table Support

1. dos (DOS Partition Table)
2. mac (MAC Partition Map)
3. bsd (BSD Disk Label)
4. sun (Sun Volume Table of Contents (Solaris))
5. gpt (GUID Partition Table (EFI))

CHAPTER 2

Tools

2.1 License(s)

The SANS Investigative Forensic Tookit is a linux distribution, a collection of many applications and scripts, all with various licenses. Most tools and scripts are installed via debian packages that are presumably built by their authors, however some packages are not built by the original authors.

Below is an attempt to identify some of the tools that are known to not be built by the original author but by someone in the community. While these tools exist on SIFT, they have their own project website and associated licenses. Not all tools will be listed here.

2.1.1 Packages

Name	License	Install Method	Website
afterglow	GNU GPL v2	.deb (SIFT REPO)	https://github.com/zrlram/afterglow
binplist	Apache License, Version 2.0	.deb (SIFT REPO)	http://code.google.com/p/binplist/
bulk_extractor	Public Domain Software	.deb (SIFT REPO)	http://digitalcorpora.org/downloads/bulk_extractor
dumppig	GNU GPL v2	.deb (SIFT REPO)	https://code.google.com/p/dumbpig/
flowgrep	BSD 3-clause	.deb (SIFT REPO)	http://www.monkey.org/~jose/software/flowgrep/
libbde	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libbde
libdata-hexify-perl	Perl 5 License / GNU GPL	.deb (SIFT REPO)	http://search.cpan.org/~jv/Data-Hexify/lib/Data/He
libesedb	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libesedb
libevt	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libevt
libevtx	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libevtx
libewf	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libewf
libfile-mork-perl	MIT	.deb (SIFT REPO)	http://search.cpan.org/~simonw/File-Mork-0.3/lib/F
libfvde	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libfvde
libfwsi	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libfwsi
liblightgrep	GNU GPL	.deb (SIFT REPO)	https://github.com/jonstewart/liblightgrep

Table 2.1 – continued from previous page

Name	License	Install Method	Website
liblnk	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/liblnk
libmac-propertylist-perl	Perl 5 License / GNU GPL	.deb (SIFT REPO)	http://search.cpan.org/~bdfoy/Mac-PropertyList-1.4
libmsiecf	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libmsiecf
libolecf	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libolecf
libpff	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libpff
libqcow	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libqcow
libregf	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libregf
libsmdev	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libsmdev
libsmraw	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libsmraw
libvhdi	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libvhdi
libvmdk	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libvmdk
libvshadow	LGPLv3+	.deb (SIFT REPO)	https://github.com/libyal/libvshadow
libxml-entities-perl	Not Specified	.deb (SIFT REPO)	http://search.cpan.org/~msergeant/XML-LibXML-
log2timeline-perl	GNU GPL v3	.deb (SIFT REPO)	http://log2timeline.net/
mac-robber	GNU GPL v3	.deb (SIFT REPO)	
maltegoce	Free for Non-Commercial Use	.deb (SIFT REPO)	https://www.paterva.com/web6/products/download2
mantaray	GNU GPL v3	.deb (SIFT REPO)	http://mantarayforensics.com/
ntdsxtract	GNU GPL v3	.deb (SIFT REPO)	https://github.com/csababarta/ntdsxtract
ntopng	GNU GPL v3	.deb (SIFT REPO)	http://www.ntop.org/products/traffic-analysis/ntop/
pdf-tools	Not Specified	.deb (SIFT REPO)	http://blog.didierstevens.com/programs/pdf-tools/
pyelftools	Unlicensed - Public Domain	.deb (SIFT REPO)	https://github.com/eliben/pyelftools
python-bencode	BitTorrent Open Source Lic	.deb (SIFT REPO)	http://www.bittorrent.com/
python-construct	MIT	.deb (SIFT REPO)	http://construct.readthedocs.org/en/latest/
python-dfvfs	Apache License, Version 2.0	.deb (SIFT REPO)	https://github.com/log2timeline/dfvfs
python-dpkt	BSD 3-clause	.deb (SIFT REPO)	
python-plaso	Apache License, Version 2.0	.deb (SIFT REPO)	https://github.com/log2timeline/plaso
python-pyparsing	MIT	.deb (SIFT REPO)	http://pyparsing.wikispaces.com/
pytsk	Apache License, Version 2.0	.deb (SIFT REPO)	https://github.com/py4n6/pytsk
re2	BSD-style	.deb (SIFT REPO)	https://github.com/google/re2
regripper	GNU GPL v3	.deb (SIFT REPO)	
sleuthkit	Multiple	.deb (SIFT REPO)	http://www.sleuthkit.org/sleuthkit/licenses.php
volatility	GNU GPL v2	.deb (SIFT REPO)	https://code.google.com/p/volatility/
windows-perl	GNU GPL v2	.deb (SIFT REPO)	https://github.com/keydet89/RegRipper2.8
xmount	GNU GPL v3	.deb (SIFT REPO)	

2.1.2 Scripts

Name	License	Install Method	Website
densityscout	MIT	git repo	https://github.com/sans-dfir/sift-files
extract_mft_record_slack.py	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
ga-parser.py	GNU GPL	git repo	https://github.com/sans-dfir/sift-files
java_idx_parser	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
jobparser.py	GNU GPL	git repo	https://github.com/sans-dfir/sift-files
page_brute	Not Specified	git repo	https://github.com/matonis/page_brute
pe_carver	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
pescanner.py	GNU GPL v3	git repo	https://github.com/sans-dfir/sift-files
shellbags.py	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
shimcacheparser.py	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
sqlparser.py	GNU GPL	git repo	https://github.com/sans-dfir/sift-files

2.1.3 Volatility Plugins

Name	License	Install Method	Website
apihooksdeep.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
autoruns.py	Not Specified	git repo	https://github.com/sans-dfir/sift-files
baseline.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
chromehistory.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
editbox.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
firefoxhistory.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
idxparser.py	Apache License, Version 2.0	git repo	https://github.com/sans-dfir/sift-files
malfinddeep.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
malprocfind.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
malsysproc.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
mimikatz.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
prefetch.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
pstotal.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
sqlite_help.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
ssdeepscan.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
trustrecords.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
uninstallinfo.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files
usnparser.py	GNU GPLv2+	git repo	https://github.com/sans-dfir/sift-files

2.1.4 License Info

License	URL
Apache License, Version 2	http://opensource.org/licenses/Apache-2.0
BSD 3-Clause	http://opensource.org/licenses/BSD-3-Clause
GNU GPL	http://opensource.org/licenses/gpl-license
LGPLv3	http://opensource.org/licenses/lgpl-license
MIT	http://opensource.org/licenses/MIT

2.2 Tools, Commands, Scripts

SIFT is a collection of tools, scripts, libraries and utilities that help facilitate your computer and mobile forensics needs.

2.2.1 All Tools

ewfacquire

- **Package:** libewf-tools

2.2.2 Registry Analysis

2.2.3 Artifact Analysis

CHAPTER 3

Packages

3.1 Packages

SIFT is a collection of tools, scripts, libraries and utilities that help facilitate your computer and mobile forensics needs.

3.1.1 All Packages

afflib

Advanced Forensics Format (AFF) is an extensible open format for the storage of disk images and related forensic metadata. It was developed by Simson Garfinkel and Basis Technology Corp.

- **Website:** http://afflib.sourceforge.net/

afflib-tools

- aimage - ewfacquire to acquire data from a file or device and store it in th AFF format
- afcat - output contents of an image file to stdout
- afconvert - convert AFF images to Raw or Raw to AFF image
- afuse - mount AFF format images/split images to view single raw file and metadata

libbde

Library and tools to access the BitLocker Drive Encryption (BDE) format. The BDE format is used by Windows, as of Vista, to encrypt data on a storage media volume.

- Author: Joachim Metz
- Website: https://github.com/libyal/libbde/

Full documentation located at https://github.com/libyal/libbde/wiki/

libesedb

Library and tools to access the Extensible Storage Engine (ESE) Database File (EDB) format. ESEDB is used in may different applications like Windows Search, Windows Mail, Exchange, Active Directory, etc.

- Author: Joachim Metz
- Website: https://github.com/libyal/libesedb/

Full documentation located at https://github.com/libyal/libesedb/wiki/

libevt

Library and tooling to access the Windows Event Log (EVT) format.

- Author: Joachim Metz
- Website: https://github.com/libyal/libevt/

Full documentation located at https://github.com/libyal/libevt/wiki/

libevtx

Library and tooling to access the Windows XML Event Log (EVTX) format.

- Author: Joachim Metz
- Website: https://github.com/libyal/libevtx/

Full documentation located at https://github.com/libyal/libevtx/wiki/

libewf

Library for the Expert Witness File Format

- Author: Joachim Metz
- Website: https://github.com/libyal/libewf/

Full documentation located at https://github.com/libyal/libewf/wiki/

libewf-tools

Tools for working with the Expert Witness File format.

Include the following command line tools.

- ewfacquire; which writes storage media data from devices and files to EWF files.
- ewfacquirestream; which writes data from stdin to EWF files.
- ewfdebug; experimental tool does nothing at the moment.
- ewfexport; which exports storage media data in EWF files to (split) RAW format or a specific version of EWF files.
- ewfinfo; which shows the metadata in EWF files.

- ewfmount; which FUSE mounts EWF files.
- ewfrecover; special variant of ewfexport to create a new set of EWF files from a corrupt set.
- ewfverify; which verifies the storage media data in EWF files.

libewf-python

Python bindings for libewf

libfvde

Library and tools to access FileVault Drive Encryption (FVDE) (or FileVault2) encrypted volumes. The FVDE format is used by Mac OS X, as of Lion, to encrypt data on a storage media volume.

Note that this project has an experimental status

- Author: Omar Choudary, Joachim Metz
- Website: https://github.com/libyal/libfvde/

Full documentation located at https://github.com/libyal/libfvde/wiki/

libvshadow

Library and tools to access the Volume Shadow Snapshot (VSS) format. The VSS format is used by Windows, as of Vista, to maintain copies of data on a storage media volume.

- Author: Joachim Metz
- Website: https://github.com/libyal/libvshadow/

Full documentation located at https://github.com/libyal/libvshadow/wiki/

log2timeline

This small little project site is dedicated to the tool log2timeline, a framework for automatic creation of a super timeline. The main purpose is to provide a single tool to parse various log files and artifacts found on suspect systems (and supporting systems, such as network equipment) and produce a timeline that can be analysed by forensic investigators/analysts

- **Author:** Kristinn Gudjonsson
- **Website:** https://code.google.com/p/log2timeline/

Command: log2timeline OR log2timeline_legacy

Note: This tool is being deprecated in favor of /tools/plaso

http://forensicscontest.com/contest01/Finalists/Kristinn_Guojonsson/oftcat

Pcapcat is a perl scrip that reads a pcap file and prints out all the connections in the file and gives the user the option of dumping the content of the TCP stream.

Plaso

A tool designed to extract timestamps from various files found on a typical computer system(s) and aggregate them.

- **Author(s):** Kristinn Gudjonsson and others
- **Website:** https://github.com/log2timeline/plaso/

Command: log2timeline.py

Full documentation available at: http://plaso.kiddaland.net/

qemu

QEMU is a generic and open source machine emulator and virtualizer.

- **Website:** http://wiki.qemu.org/Main_Page

Raw Image to VMDK

```
$ qemu-img convert imagefile.dd -O vmdk vmdkname.vmdk
```

VMDK to Raw Image

http://zhigang.org/2008/07/01/convet-vmdk-to-raw.html

SleuthKit

CHAPTER 4

Cheatsheet

4.1 Cheatsheet

4.1.1 Mounting DD Images

```
mount -t fstype [options] image mountpoint
```

image can be a disk partition or dd image file

Useful Options

Option	Description
ro	mount as read only
loop	mount on a loop device
noexec	do not execute files
offset=<BYTES>	offset
show_sys_files	system files
streams_interface=windows	streams

4.1.2 Mounting E01 Images

```
mount_ewf.py image.E01 mountpoint
```

1. mount_ewf.py image.E01 /mnt/ewf
2. mount –o loop,ro,show_sys_files

/mnt/ewf/<RAWFILE> /mnt/mount_location

4.1.3 Mounting Split Raw Images

```
affuse image.001 mountpoint
```

1. affuse image.001 /mnt/aff
2. mount –o loop,ro,show_sys_files

4.1.4 Creating Super Timelines

1. Step 1 – Find Partition Starting Sector

   ```
   mmls image.dd - calculate offset ##### (sector *512)
   ```

2. Step 2 – Mount image for processing

   ```
   mount -o ro, noexec,show_sys_files,loop,offset=##### image.dd /mnt/
   windows_mount
   ```

3. Step 3 – Create Comprehensive Timeline

   ```
   log2timeline -p -r -f winxp -z CST6CDT /mnt/windows_mount -w
   timeline.csv
   ```

4. Step 4 – Filter Timeline

   ```
   l2t_process -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY
   ```

4.1.5 String Searches

ASCII string search and list the byte offset

```
srch_strings -t d imagefile.dd > imagefile.ascii.str
```

uNICODE string search and list byte offset

```
srch_strings -e l -t d imagefile.dd > imagefile.uni.str
```

Search for a specific string using grep

GREP useful Options

Option	Description
-i	ignore case
-f	dirty word list filename

```
grep -i password -f dirty_words.txt imagefile.ascii.str
```

4.1.6 Memory Analysis

```
vol.py [plugin] -f [image] --profile [PROFILE]
```

Supported Commands

Commands	Description
connscan	Scan for connection objects
files	List of open files process
hibinfo	Convert hibernation file
procdump	Dump process
pslist	List of running processes
sockscan	Scan for socket objects

Profiles

Profile	Operating System
VistaSP0x86	Windows Vista SP0 x86
VistaSP1x86	Windows Vista SP1 x86
VistaSP2x86	Windows Vista SP2 x86
Win2K8SP1x86	Windows 2008 SP1 x86
Win2K8SP2x86	Windows 2008 SP2 x86
Win7SP0x86	Windows 7 SP0 x86
WinXPSP2x86	Windows XP SP2
WinXPSP3x86	Windows XP SP3

4.1.7 Recovering Deleted Registry Hives

```
deleted.pl <HIVEFILE>
```

```
deleted.pl /mnt/windows_mount/Windows/System32/config/SAM > /cases/
windowsforensics/SAM_DELETED.txt
```

4.1.8 Recovering Data

Create unallocated Image (deleted data) using blkls `blkls imagefile.dd > unallocated_imagefile.blkls`

Create Slack Image Using dls (for FAT and NTFS) `blkls -s imagefile.dd > imagefile.slack`

Foremost Carves out files based on headers and footers `foremost -o outputdir -c /path/to/foremost.conf data_file.img`

Sigfind - search for a binary value at a given offset (-o) `sigfind <hexvalue> -o <offset> data_file.img`

4.1.9 SleuthKit Tools

File System Layer Tools (Partition Information)

Tool Name	Description	Example
fsstat	Displays details about the file system	`fsstat imagefile.dd`

Data Layer Tools (Block or Cluster)

Tool Name	Description	Example
blkcat	Displays the contents of a disk block	`blkcat imagefile.dd block_num`
blkls	Lists contents of deleted disk blocks	`blkls imagefile.dd > imagefile.blkls`
blkcalc	Maps between dd images and blkls results	`blkcalc imagefile.dd -u blkls_num`
blkstat	Display allocation status of block	`blkstat imagefile.dd cluster_number`

MetaData Layer Tools (inode, MFT, or Directory Entry)

Tool Name	Description	Example
ils	Displays inode details	`ils imagefile.dd`
istat	Displays information about a specific inode	`istat imagefile.dd inode_num`
icat	Displays contents of blocks allocated to an inode	`icat imagefile.dd inode_num`
ifind	Determine which inode contains a specific block	`ifind imagefile.dd -d block_num`

Filename Layer Tools

Tool Name	Description	Example
fls	Displays deleted file entries in a directory inode	
ffind	Find the filename that using the inode	

log2timeline (aka plaso)

Plaso is the successor to log2timeline. Plaso is written in python and is available on SIFT 3.0 along side of log2timeline.

log2timeline commands are `log2timeline` and `log2timline_legacy`.

The plaso command is `log2timeline.py`

Mounting DD Images

```
mount -t fstype [options] image mountpoint
```

image can be a disk partition or dd image file

Useful Options

Option	Description
ro	mount as read only
loop	mount on a loop device
noexec	do not execute files
offset=<BYTES>	offset
show_sys_files	system files
streams_interface=windows	streams

Mounting E01 Images

```
mount_ewf.py image.E01 mountpoint
```

1. mount_ewf.py image.E01 /mnt/ewf
2. mount –o loop,ro,show_sys_files

/mnt/ewf/<RAWFILE> /mnt/mount_location

Mounting Split Raw Images

```
affuse image.001 mountpoint
```

1. affuse image.001 /mnt/aff

2. mount –o loop,ro,show_sys_files

Creating Super Timelines

1. Step 1 – Find Partition Starting Sector

   ```
   mmls image.dd - calculate offset ##### (sector *512)
   ```

2. Step 2 – Mount image for processing

   ```
   mount -o ro, noexec,show_sys_files,loop,offset=##### image.dd /mnt/
   windows_mount
   ```

3. Step 3 – Create Comprehensive Timeline

   ```
   log2timeline -p -r -f winxp -z CST6CDT /mnt/windows_mount -w
   timeline.csv
   ```

4. Step 4 – Filter Timeline

   ```
   l2t_process -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY
   ```

String Searches

ASCII string search and list the byte offset

```
srch_strings -t d imagefile.dd > imagefile.ascii.str
```

uNICODE string search and list byte offset

```
srch_strings -e l -t d imagefile.dd > imagefile.uni.str
```

Search for a specific string using grep

GREP useful Options

Option	Description
-i	ignore case
-f	dirty word list filename

```
grep -i password -f dirty_words.txt imagefile.ascii.str
```

Memory Analysis

```
vol.py [plugin] -f [image] --profile [PROFILE]
```

Supported Commands

Commands	Description
connscan	Scan for connection objects
files	List of open files process
hibinfo	Convert hibernation file
procdump	Dump process
pslist	List of running processes
sockscan	Scan for socket objects

Profiles

Profile	Operating System
VistaSP0x86	Windows Vista SP0 x86
VistaSP1x86	Windows Vista SP1 x86
VistaSP2x86	Windows Vista SP2 x86
Win2K8SP1x86	Windows 2008 SP1 x86
Win2K8SP2x86	Windows 2008 SP2 x86
Win7SP0x86	Windows 7 SP0 x86
WinXPSP2x86	Windows XP SP2
WinXPSP3x86	Windows XP SP3

Recovering Deleted Registry Hives

```
deleted.pl <HIVEFILE>
```

```
deleted.pl /mnt/windows_mount/Windows/System32/config/SAM > /cases/
windowsforensics/SAM_DELETED.txt
```

Recovering Data

Create unallocated Image (deleted data) using blkls `blkls imagefile.dd > unallocated_imagefile.blkls`

Create Slack Image Using dls (for FAT and NTFS) `blkls -s imagefile.dd > imagefile.slack`

Foremost Carves out files based on headers and footers `foremost -o outputdir -c /path/to/foremost.conf data_file.img`

Sigfind - search for a binary value at a given offset (-o) `sigfind <hexvalue> -o <offset> data_file.img`

SleuthKit Tools

File System Layer Tools (Partition Information)

Tool Name	Description	Example
fsstat	Displays details about the file system	`fsstat imagefile.dd`

Data Layer Tools (Block or Cluster)

Tool Name	Description	Example
blkcat	Displays the contents of a disk block	`blkcat imagefile.dd block_num`
blkls	Lists contents of deleted disk blocks	`blkls imagefile.dd > imagefile.blkls`
blkcalc	Maps between dd images and blkls results	`blkcalc imagefile.dd -u blkls_num`
blkstat	Display allocation status of block	`blkstat imagefile.dd cluster_number`

MetaData Layer Tools (inode, MFT, or Directory Entry)

Tool Name	Description	Example
ils	Displays inode details	`ils imagefile.dd`
istat	Displays information about a specific inode	`istat imagefile.dd inode_num`
icat	Displays contents of blocks allocated to an inode	`icat imagefile.dd inode_num`
ifind	Determine which inode contains a specific block	`ifind imagefile.dd -d block_num`

Filename Layer Tools

Tool Name	Description	Example
fls	Displays deleted file entries in a directory inode	
ffind	Find the filename that using the inode	

CHAPTER 5

About

5.1 About

An international team of forensics experts, led by SANS Faculty Fellow Rob Lee, created the SANS Investigative Forensic Toolkit (SIFT) Workstation and made it available to the whole community as a public service. The free SIFT toolkit, that can match any modern forensic tool suite, is also featured in SANS' Advanced Computer Forensic Analysis and Incident Response course (FOR 508). It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Offered free of charge, the SIFT 3.0 Workstation will debut during SANS' Advanced Computer Forensic Analysis and Incident Response course (FOR508) at DFIRCON. SIFT 3.0 demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

"Even if SIFT were to cost tens of thousands of dollars, it would still be a very competitive product," says, Alan Paller, director of research at SANS. "At no cost, there is no reason it should not be part of the portfolio in every organization that has skilled forensics analysts."

Developed and continually updated by an international team of forensic experts, the SIFT is a group of free open-source forensic tools designed to perform detailed digital forensic examinations in a variety of settings. With over 100,000 downloads to date, the SIFT continues to be the most popular open-source forensic offering next to commercial source solutions.

"The SIFT Workstation has quickly become my "go to" tool when conducting an exam. The powerful open source forensic tools in the kit on top of the versatile and stable Linux operating system make for quick access to most everything I need to conduct a thorough analysis of a computer system," said Ken Pryor, GCFA Robinson, IL Police Department