



TOOLS FOUND ON SIFT WORKSTATION

2.14

Contents

SIFT 2.1 Development and Thanks	3
Background	3
Basic Configuration Information	3
SIFT Workstation Recommended Software Requirements	5
SIFT Workstation 2.14 Capabilities	6
Tools, Locations, and Descriptions.....	8





TOOLS FOUND ON SIFT WORKSTATION

2.14

SANS INSTITUTE



2.14

SIFT 2.1 Development and Thanks

Lead – Rob Lee

Community Contributors/Testers

- Hal Pomeranz
- Doug Koster
- Lenny Zeltser
- Kristinn Gudjonsson
- Lee Whitfield
- Eric Huber
- Chad Tilbury
- Jess Garcia
- Josh More
- Mark Mckinnon
- Ramon Garo
- Mark Hallman
- Jonathan Bridbord
- Brad Garnett
- Frank McClain
- Glyn Gowing
- Tim Mughnerini

Background

[Faculty Fellow Rob Lee](#) created the SANS Investigative Forensic Toolkit(SIFT) Workstation featured in the [Advanced Computer Forensics and Incident Response course \(FOR 508\)](#) in order to show that advanced investigations and investigating hackers can be accomplished using freely available open-source tools.

The SANS SIFT Workstation is a VMware Appliance that is pre-configured with all the necessary tools to perform a detailed digital forensic examination. It is compatible with Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many additional tools and capabilities that can match any modern forensic tool suite.

Basic Configuration Information

Recommend to increase VMware Options for

- [Download VMworkstation](#), Player, or Fusion



TOOLS FOUND ON SIFT WORKSTATION

2.14

- Memory (Currently 1024K, increase to add more RAM as needed)
- CPUs (Currently 1, increase as needed for more power)

SIFT Login/Password

After downloading the toolkit, use the credentials below to gain access.

- Login "sansforensics"
- Password "forensics"
- \$ sudo su -
 - Use to elevate privileges to root while mounting disk images.

PTK login

- Login "admin"
- Password "forensics"

Host Machine Connectivity

Enable SHARED FOLDERS

- VM -> SETTINGS -> OPTIONS -> Shared Folders -> Always Enabled (Check)
- Access to Host System Found on Desktop
- VMware-Shared-Drive

Automatic Mounting

- SIFT 2.14 is intended to be used with evidence that is already acquired. It is an analysis platform. To facilitate use for many who have challenges having their hardware recognized, SIFT 2.14 out of the box is configured with automount turned on.
- Typically individuals are examining file images so attaching a hard drive with a image file on the drive should not matter.
- The point of SIFT is to facilitate analysis and this is just a preference option to help out those who are new to linux

Access from a Windows Machine

- Filesystem Shares \\SIFTWORKSTATION
 - or use ifconfig and connect to eth0 IP Address listed (e.g. \\192.168.1.12)
 - /mnt - Mount point for read-only examination of digital forensic evidence
 - /cases - Directory to store evidence



2.14

SIFT Workstation Recommended Software Requirements

- VMware Player, Workstation, or Fusion (Free From www.vmware.com)
- SANS SIFT Workstation Capabilities



TOOLS FOUND ON SIFT WORKSTATION

2.14

SIFT Workstation 2.14 Capabilities

Ability to securely examine raw disks, multiple file systems, evidence formats. Places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed

File system support

- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS+)
- Solaris (UFS)
- Linux (EXT2/3/4)

Evidence Image Support

- Expert Witness (E01)
- RAW (dd)
- Advanced Forensic Format (AFF)

Software Includes

- The Sleuth Kit (File system Analysis Tools)
- log2timeline (Timeline Generation Tool)
- ssdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)
- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)
- DFF (Digital Forensic Framework)

Key Directories in SANS SIFT Workstation

- /usr/local/src
 - Source files for Autopsy, The Sleuth Kit, and other tools
- /usr/local/bin
 - Location of the forensic pre-compiled binaries
- /cases
 - Location of your collected evidence
- /mnt/ewf
 - Location to mount E01 images



TOOLS FOUND ON SIFT WORKSTATION

2.14

- /mnt/aff
 - Location to mount AFF images
- /mnt/windows_mount
 - Location to mount NTFS or FAT file systems

What I like the best about SIFT is that my forensic analysis is not limited because of only being able to run a forensic tool on a specific host operating system. With the SIFT VM Appliance, I can create snapshots to avoid cross-contamination of evidence from case to case, and easily manage system and AV updates to the host OS on my forensic workstation. Not to mention, being able to mount forensic images and share them as read-only with my host OS, where I can run other forensic tools to parse data, stream-lining the forensic examination process.

Brad Garnett

www.digitalforensicsource.com



TOOLS FOUND ON SIFT WORKSTATION

2.14

Tools, Locations, and Descriptions

- A. Tools and Locations
 - A.1. Command Line Utilization - Most Tools will be found in /usr/local/bin
 - A.2. GUI Tools should execute from the Forensics Menu GUI in the Upper Left Corner or the Magnifying Glass Dropdown
- B. How-Tos -
 - B.1. How To Mount a Disk Image In Read-Only Mode
 - B.1.1. <http://blogs.sans.org/computer-forensics/2009/02/19/digital-forensic-sifting-how-to-perform-a-read-only-mount-of-evidence/>
 - B.2. How To Create a Filesystem and Registry Timeline
 - B.2.1. <http://blogs.sans.org/computer-forensics/2009/02/24/digital-forensic-sifting-registry-and-filesystem-timeline-creation/>
 - B.3. How To Create a Super Timeline
 - B.3.1. http://blogs.sans.org/computer-forensics/2010/03/19/digital-forensic-sifting-super-timeline-analysis-and-creation/?utm_source=rss&utm_medium=rss&utm_campaign=digital-forensic-sifting-super-timeline-analysis-and-creation
 - B.4. How To Acquire and Mount Raw, E01, AFF Disk Images
 - B.4.1. <https://www.sans.org/webcasts/imagine-this-acquisition-and-handling-techniques-of-computer-evidence-92018>
 - B.5. How to use the SIFT Workstation for Basic Memory Image Analysis
 - B.5.1. <https://www.sans.org/webcasts/memory-analysisincident-responders-and-forensic-analysts-92368>
- C. Filesystem Support
 - C.1. ntfs (NTFS)
 - C.2. iso9660 (ISO9660 CD)
 - C.3. hfs (HFS+)
 - C.4. raw (Raw Data)
 - C.5. swap (Swap Space)
 - C.6. memory (Ram Data)
 - C.7. fat12 (FAT12)
 - C.8. fat16 (FAT16)
 - C.9. fat32 (FAT32)
 - C.10. ext2 (Ext2)
 - C.11. ext3 (Ext3)
 - C.12. ufs1 (UFS1)
 - C.13. ufs2 (UFS2)
 - C.14. vmdk



TOOLS FOUND ON SIFT WORKSTATION

2.14

- D. Evidence Image File Support
 - D.1. raw (Single raw file (dd))
 - D.2. aff (Advanced Forensic Format)
 - D.3. afd (AFF Multiple File)
 - D.4. afm (AFF with external metadata)
 - D.5. afflib (All AFFLIB image formats (including beta ones))
 - D.6. ewf (Expert Witness format (encase))
 - D.7. split raw (Split raw files) via affuse
 - D.7.1. affuse - mount 001 image/split images to view single raw file and metadata
 - D.8. split ewf (Split E01 files) via mount_ewf.py
 - D.8.1. mount_ewf.py - mount E01 image/split images to view single raw file and metadata
 - D.8.2. ewfmount - mount E01 images/split images to view single rawfile and metadata
- E. Partition Table Support
 - E.1. dos (DOS Partition Table)
 - E.2. mac (MAC Partition Map)
 - E.3. bsd (BSD Disk Label)
 - E.4. sun (Sun Volume Table of Contents (Solaris))
 - E.5. gpt (GUID Partition Table (EFI))
- F. Digital Evidence Acquisition
 - F.1. dd - dd, sometimes called GNU dd, is the oldest imaging tool still used.
 - F.2. ddrescue - ddrescue is a raw disk imaging tool that "copies data from one file or block device to another, trying hard to rescue data in case of read errors." The application is developed as part of the GNU project and has written with UNIX/Linux in mind.
 - F.2.1. <http://www.gnu.org/software/ddrescue/ddrescue.html>
 - F.3. dc3dd - dc3dd is a patched version of GNU dd with added features for computer forensics.
 - F.3.1. <http://dc3dd.sourceforge.net/>
 - F.4. dcfldd - dcfldd is an enhanced version of dd developed by the U.S. Department of Defense Computer Forensics Lab.
 - F.4.1. <http://dcfldd.sourceforge.net/>
 - F.5. sdd
 - F.5.1. <http://linux.maruhn.com/sec/sdd.html>
 - F.6. ewfacquire - create EWF (E01) file format images
 - F.6.1. <http://linux.die.net/man/1/ewfacquire>
 - F.6.2. <http://www.forensicswiki.org/wiki/Libewf>
 - F.7. aimage - aimage can create files in raw, AFF, AFD, or AFM formats. AFF and AFD formats can be compressed or uncompressed. aimage can optionally compress and calculate MD5 or SHA-1 hash residues while the data is being copied.
 - F.7.1. <http://www.afflib.org/aimage.php>
- G. Media Management



TOOLS FOUND ON SIFT WORKSTATION

2.14

G.1. ewflib

G.1.1. <http://sourceforge.net/projects/libewf/>

- G.1.1.1. ewfacquire - ewfacquire to acquire data from a file or device and store it in the EWF format
- G.1.1.2. ewfexport - ewfexport to export data from the EWF format (Expert Witness Compression Format) to raw data or another EWF format.
- G.1.1.3. ewfverify - ewfverify to verify data stored in the EWF format (Expert Witness Compression Format).
- G.1.1.4. ewfinfo - winfo to determine information about the EWF format
- G.1.1.5. ewfmount – mount E01 Images
- G.1.1.6. mount_ewf.py - mount EWF format images/split images to view single raw file and metadata

G.2. afflib

G.2.1. <http://www.afflib.org/aimage.php>

- G.2.1.1. aimage- ewfacquire to acquire data from a file or device and store it in the AFF format
- G.2.1.2. afcat - Output contents of an image file to stdout
- G.2.1.3. afconvert - Convert AFF images to Raw or Raw to AFF image
- G.2.1.4. afuse - mount AFF format images/split images to view single raw file and metadata

G.3. qemu

G.3.1. Convert images to another formation (such as raw image -> vmdk or vmdk -> raw image)

G.3.1.1. Raw Image to VMDK How To

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

G.3.1.2. VMDK to RAW IMAGE How To

- <http://zhigang.org/blog/convet-vmdk-to-raw/>

G.4. Raw2vmdk

G.4.1. Convert images to another formation (such as raw image -> vmdk)

G.4.1.1. Found in /usr/local/src/raw2vmdk

G.4.1.2. `# java -jar raw2vmdk.jar data001.dd data001.vmdk`

H. Mounting Disk Images -

H.1. ntfs3g - <http://www.tuxera.com/community/ntfs-3g-download/>

H.2. <http://blogs.sans.org/computer-forensics/2009/02/19/digital-forensic-sifting-how-to-perform-a-read-only-mount-of-evidence/>

I. Hashing Tools

I.1. <http://md5deep.sourceforge.net/>

- I.1.1. md5deep - Compute and compare MD5 message digests
- I.1.2. sha1deep - Compute and compare SHA-1 message digests
- I.1.3. sha256deep - Compute and compare SHA-256 message digests



TOOLS FOUND ON SIFT WORKSTATION

2.14

- I.1.4. tigerdeep - Compute and compare Tiger message digests
- I.1.5. whirlpooldeep - Compute and compare Whirlpool message digests
- I.1.6. hashdeep - Compute, compare, or audit multiple message digests
- I.2. Fuzzy Hashing
 - I.2.1. ssdeep - Computes context triggered piecewise hashes
- J. Disk Analysis - Sleuthkit Tools
 - J.1. <http://www.sleuthkit.org/>
 - J.2. Media Management Layer
 - J.2.1. mmls - Display the partition layout of a volume system (partition tables)
 - J.2.2. mmstat - Display details about the volume system (partition tables)
 - J.2.3. disk_stat - Check for Host Protected Area (HPA)
 - J.2.4. disk_sreset - remove HPA
 - J.3. Data Layer
 - J.3.1. blkls - List or output file system data units.
 - J.3.2. blkstat - Display details of a file system data unit (i.e. block or sector)
 - J.3.3. blkcat - Display the contents of file system data unit in a disk image.
 - J.3.4. blkcalc - Converts between unallocated disk unit numbers and regular disk unit numbers
 - J.3.5. srch_strings - print out ascii or unicode strings from a raw file
 - J.3.6. grep - search for strings from a dirty_words list or a file
 - J.4. Metadata Layer
 - J.4.1. istat - Display details of a meta-data structure (i.e. inode)
 - J.4.2. ils - List inode information
 - J.4.3. icat - Output the contents of a file based on its inode number
 - J.4.4. ifind - Find the meta-data structure that has allocated a given disk unit or file name
 - J.4.5. fib - Find Indirect Blocks
 - J.4.5.1. <https://blog.mandiant.com/archives/1593>
 - J.4.6. frib - File Recovery via Indirect Blocks
 - J.4.6.1. <https://blog.mandiant.com/archives/1593>
 - J.4.7. analyzeMFT.py - parse MFT structure pulling out all metadata into csv file
 - J.4.7.1. <http://integriography.wordpress.com>
 - J.4.7.2. <http://integriography.wordpress.com/2010/01/20/analyzemft-a-python-tool-to-deconstruct-the-windows-ntfs-mft-file/>
 - J.4.8. MFT_Parser_cl and GUI by Mark Mckinnon
 - J.4.9. body-outliers.py
 - J.4.9.1. <http://computer-forensics.sans.org/blog/2011/11/07/outlier-analysis-in-digital-forensics>
 - J.4.10. meta-outliers.py
 - J.4.10.1. <http://trustedsignal.com/code/meta-outliers.py>



TOOLS FOUND ON SIFT WORKSTATION

2.14

J.5. Filename Layer

J.5.1. fls - List file and directory names in a disk image

J.5.2. ffind - Finds the name of the file or directory using a given inode

J.6. Timeline Analysis - http://blogs.sans.org/computer-forensics/2010/03/19/digital-forensic-sifting-super-timeline-analysis-and-creation/?utm_source=rss&utm_medium=rss&utm_campaign=digital-forensic-sifting-super-timeline-analysis-and-creation

J.6.1. fls - List file and directory names in a disk image

J.6.2. mac-robber

J.6.3. regtime.pl - list registry key last write times in a hive file

J.6.4. timescanner - A recursive scanner to produce timeline data extracted from file artifacts

J.6.5. log2timeline - a log file parser that produces a body file used to create timelines (for forensic investigations)Artifact Analysis

J.6.5.1. <http://log2timeline.net/>

J.6.5.2. SIFT Timeline Creation

J.6.5.3. Partition image (not a whole disk image)

- `# log2timeline-sift -z EST5EDT -p 0 log_partition.dd`

J.6.5.4. Disk image:

- `# log2timeline-sift -z EST5EDT phys_disk_image.dd`

J.6.5.5. Log2timeline/Timescanner output formats

- `cef` Output timeline using the ArcSight Common Event Format (CEF)
- `cftl` Output timeline in a XML format that can be read by CFTL
- `csv` Output timeline using CSV (Comma Separated Value) file
- `mactime` Output timeline using mactime format
- `mactime_l` Output timeline using this particular output method
- `simile` Output timeline in a XML format that can be read by a SIMILE widget
- `sqlite` Output timeline into a SQLite database
- `tlm` Output timeline using H. Carvey's TLN format

J.6.5.6. Log2timeline/Timescanner Parsing Formats

- `apache2_access` 0.3 Parse the content of a Apache2 access log file
- `apache2_error` 0.2 Parse the content of a Apache2 error log file
- `chrome` 0.3 Parse the content of a Chrome history file
- `encase_dirlisting` 0.2 Parse the content of a CSV file that is exported from FTK Imager
- `evt` 0.2 Parse the content of a Windows 2k/XP/2k3 Event Log
- `evtx` 0.5 Parse the content of a Windows Event Log File (EVTX)
- `exif` 0.4 Extract metadata information from files using ExifTool
- `ff_bookmark` 0.3 Parse the content of a Firefox bookmark file
- `firefox2` 0.3 Parse the content of a Firefox 2 browser history



TOOLS FOUND ON SIFT WORKSTATION

2.14

•	firefox3	0.8	Parse the content of a Firefox 3 history file
•	ftk_dirlisting (dirlisting)	0.2	Parse the content of a CSV file that is exported from FTK Imager
•	generic_linux HH:MM:SS	0.3	Parse content of Generic Linux logs that start with MMM DD
•	iehistory	0.7	Parse the content of an index.dat file containing IE history
•	iis	0.5	Parse the content of a IIS W3C log file
•	isatxt	0.4	Parse the content of a ISA text export log file
•	jp_ntfs_change	0.1	Parse the content of a CSV output file from JP (NTFS Change log)
•	mactime	0.6	Parse the content of a body file in the mactime format
•	mcafee	0.3	Parse the content of a log file
•	mft	0.1	Parse the content of a NTFS MFT file
•	mssql_errlog	0.2	Parse the content of an ERRORLOG file produced by MS SQL server
•	ntuser	1.0	Parses the NTUSER.DAT registry file
•	opera	0.2	Parse the content of an Opera's global history file
•	oxml	0.4	Parse the content of an OpenXML document
			pcap 0.5
			Parse the content of a PCAP file
•	pdf	0.3	Parse some of the available PDF document metadata
•	prefetch	0.7	Parse the content of the Prefetch directory
•	recycler	0.6	Parse the content of the recycle bin directory
•	restore	0.9	Parse the content of the restore point directory
•	safari	0.3	Parse the contents of a Safari History.plist file
•	sam	0.1	Parses the SAM registry file
•	security	0.1	Parses the SECURITY registry file
•	setupapi	0.5	Parse the content of the SetupAPI log file in Windows XP
•	skype_sql	0.1	Parse the content of a Skype database
•	software	0.1	Parses the SOFTWARE registry file
•	sol	0.5	Parse the content of a .sol (LSO) or a Flash cookie file
•	squid	0.5	Parse the content of a Squid access log (http_emulate off)
•	syslog	0.2	Parse the content of a Linux Syslog log file
•	system	0.1	Parses the SYSTEM registry file
•	tlh	0.5	Parse the content of a body file in the TLN format
•	volatility	0.2	Parse the content of a Volatility output files (psscan2, sockscan2, ...)
•	win_link	0.7	Parse the content of a Windows shortcut file (or a link file)
•	wmipro	0.2	Parse the content of the wmipro log file
•	xpfirewall	0.4	Parse the content of a XP Firewall log

J.6.5.7. Timeline Filtering l2t_process

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

K. Artifact Analysis

K.1. shellbags.py

K.1.1. accepts the path to a raw Registry hive acquired forensically as a command line argument.

K.1.2. <http://www.williballenthin.com/forensics/shellbags/index.html>

K.1.3. # shellbags.py /path/to/NTUSER.DAT

K.2. INDXParse.py



TOOLS FOUND ON SIFT WORKSTATION

2.14

K.2.1. will parse INDX structure slack space if provided the '-d' flag. Entries identified in the slack space will be tagged with a string of the form "(slack at ###)" where ### is the hex offset to the slack entry. Note that slack entries will have separate timestamps from the live entries, and could be used to show the state of the system at a point in time.

K.2.2. <http://www.williballenthin.com/forensics/indx/index.html>

K.3. python-registry

K.3.1. python-registry was originally written by [Willi Ballenthin](http://www.williballenthin.com), a forensicator who wanted to access the contents of the Windows Registry from his Linux laptop. python-registry currently provides read-only access to Windows Registry files, such as NTUSER.DAT, userdiff, and SOFTWARE. The interface is two-fold: a high-level interface suitable for most tasks, and a low level set of parsing objects and methods which may be used for advanced study of the Windows Registry. python-registry is written in pure Python, making it portable across all major platforms.

K.3.2. <http://www.williballenthin.com/registry/>

- K.4. libesedb (Exchange database handling)
- K.5. liblnk (LNK file parsing)
- K.6. libmsiecf (index.dat parsing)
- K.7. libnk2 (Nickfile parsing)
- K.8. libpff (PST/OST parsing)
- K.9. libbfio
- K.10. libqcow (direct qemu image support)
- K.11. missidentfy - Find executable files without an executable extension
- K.12. Galetta - a ms-windows cookies analyzer
- K.13. Pasco - a ms-windows IExplorer cache analyzer
- K.14. Rifiuti - a ms-windows trashcan analyzer
- K.15. mdbtools - playing with MS mdb access databases
- K.16. antiword - show the text and images of MS Word documents
- K.17. exiftool - metadata extractor (over 400 file types)
- K.18. extract - keyword extractor
- K.19. lslnk - list link file metadata information
- K.20. pref.pl - list prefetch directory information
- K.21. reglookup
- K.22. vinetto - parse thumbs.db files
- K.23. Windows 'index.dat' Parser

K.23.1. 'id' is a cmdline version of a Windows index.dat parser. While there are other index.dat parsers freely available, 'id' was developed for research purposes: (a) To help one understand the index.dat internal structure and how it relates to the information on the Windows system and (b) the desire to have the resulting tool to be OS agnostic (eg. use



TOOLS FOUND ON SIFT WORKSTATION

2.14

the tool in a any non-Windows host that could compile c/c++). Currently there are compiled versions for Windows, Linux and MAC OS X.

K.24. Windows Journal Parser (for NTFS change logs)

K.24.1. 'jp' is short for Journal Parser. The notion to write this tool was originally inspired by one of the instructors from a forensic course. Therefore 'jp' is only a command line implementation of a parser that will extract NTFS change log entries.

K.25. Windows LNK Parsing Utility

K.25.1. 'lp' is a prototype version of a lnk file parser. Originally inspired by the forensic class taken from the SAN Institute [1] back in Jan 2010, 'lp' is another tool created for eventual inclusion into a computer forensic toolkit.

K.26. Windows NTFS Metadata Extractor Utility

K.26.1. 'ntfswalk' is a prototype version of a tool that traverses a specified NTFS volume reading all MFT entries and pulling predefined statistics as it runs.

K.27. Windows Prefetch Parser

K.27.1. 'pf' is a prototype version of a prefetch parser.

K.28. sbag

K.28.1. 'sbag' is a prototype version of a ShellBag parser. The ShellBag information is a set of keys in a user registry hive (eg. ntuser.dat file) used by the Windows operating system to track user window viewing preferences. It does this by storing various Windows Explorer settings that relates to dimensions, settings, etc. This allows one to reopen the same folder at a later time with the settings from the previous time. Each user will have separate preferences for folders, and therefore, these settings are stored in the user specific hive.

K.29. Windows USB Storage (USBSTOR) Parser

K.29.1. 'usp' is a prototype version of a tool that finds documented USB storage device artifacts on an NTFS system volume. Sources of artifacts include the registry hives as well as some log files that Windows updates autonomously when a usb device is inserted into a computer.

K.30.

K.31. Windows Event Log Analysis

K.31.1. GrokEVT - parse windows event logs

K.31.1.1. <http://projects.sentinelchicken.org/grokevt/>

K.31.2. Evtxtools - Parse EVTX event logs

K.31.2.1. http://computer.forensikblog.de/en/2010/02/evtx_parser_1_0_3.html#more

K.32. Windows Event Log Viewer

K.32.1. 'evtx_view' is a prototype version of an event log viewer that can parse eventlogs from pre-Vista Windows (eg XP), as well as Vista and Windows 7. The event log format changed with Vista into a binary XML format. Originally inspired by the paper by Andreas Schuster on 'Introducing the Microsoft Vista event log format', evtx_view was an attempt to take the concepts introduced in the paper and implement a Windows API independent parsing



TOOLS FOUND ON SIFT WORKSTATION

2.14

engine. Written entirely in C++, the evtx_view parse engine was easily ported to Linux and MAC OS X.

L. Registry Analysis

L.1. Reglookup 1.0.1 - RegLookup is released under the GNU GPL, and is implemented in ANSI C. RegLookup provides command line tools, a C API, and a Python module for accessing registry data structures. The project has a focus on providing tools for digital forensic examiners (though is useful for many purposes), and includes algorithms for retrieving deleted data structures from registry hives. Browse the project's [goals](#) to read up on the objectives of future releases.

L.1.1. <http://projects.sentinelchicken.org/reglookup/>

L.1.2. *Reglookup* - The reglookup binary is used to list the contents of a registry into a comma separated format. By default it will list all the paths, last write times, and name/value pairs contained within the registry. The `-s` option enables printing of security descriptor information as well

L.1.3. *reglookup-timeline* - This tool is used to create a CSV timeline based on last write times within a hive

L.1.4. *reglookup-recover* - This tool recovers deleted entries within registry hives, and then reports them in a CSV format similar to *reglookup*. The theory used to recover deleted entries is covered in Tim's paper that can be found [here](#). This capability has fairly obvious applications in forensics investigations, and investigators should consider adding *reglookup-recover* usage to their forensics process.

L.2. Registry Viewer (YARU)

L.2.1. *yaru* is a minimal version of a registry viewer compared to the many others that are freely available on the Internet. 'yaru' was designed to try to parse (on a best effort basis) the Windows registry hives and display the results in a tree view GUI. Inspired by the desire to look into the Windows registry metadata so as to better forensically analyze the registry hives, *yaru* was designed with a portable and extensible architecture in mind so that it could be compiled to run on various operating systems.

L.3. *recover_deleted_registry_keys.pl* - recover unallocated keys and key slack from a registry hive

L.4. *ripXP.pl* - Windows XP Restore Point Parser

L.4.1. <http://regripper.wordpress.com/>

L.5. *rip.pl* - regripper

L.5.1. <http://regripper.wordpress.com/>

L.5.2. Regripper Plugins

L.5.2.1. <http://code.google.com/p/regripperplugins/>

- *vmplayer* v.20110204 [NTUSER.DAT]
 - Extracts full filepath for recent VMware Player VM images.
- *appinitdls* v.20080324 [Software]
 - Gets contents of *Appinit_DLLs* value
- *winver* v.20081210 [Software]



TOOLS FOUND ON SIFT WORKSTATION

2.14

- Get Windows version
- secctr v.20100310 [Software]
 - Get data from Security Center key
- urlzone v.20090526 [Software]
 - URLZONE detection
- cmd_shell v.20100830 [Software]
 - Gets shell open cmds for various file types
- printers v.20090223 [NTUSER.DAT]
 - Get user's printers
- mspaper v.20080324 [NTUSER.DAT]
 - Gets images listed in user's MSPaper key
- usbstor3 v.20100312 [System]
 - Get USBStor key info
- streammru v.20090205 [NTUSER.DAT]
 - streammru
- usb v.20080825 [System]
 - Get USB subkeys info; csv output
- 12. acmru v.20080324 [NTUSER.DAT]
 - Gets contents of user's ACMru key
- 13. logonusername v.20080324 [NTUSER.DAT]
 - - Get user's Logon User Name value
- 14. notify v.20110309 [Software]
 - - Get Notify subkey entries
- 15. decaf v.20110210 [NTUSER.DAT]
- 16. winzip v.20080325 [NTUSER.DAT]
 - - Get WinZip extract and filemenu values
- 17. schedagent v.20100817 [Software]
 - - Get SchedulingAgent key contents
- 18. productpolicy v.20091116 [System]
 - - Parse ProductPolicy value (Vista & Win2008 ONLY)
- 19. appcompatflags v.20110204 [NTUSER.DAT]
 - - Extracts AppCompatFlags for Windows.
- 20. controlpanel v.20080428 [NTUSER.DAT]
 - - Look for RecentTask* values in ControlPanel key (Vista)
- 21. startmenuinternetapps_lm v.20101219 [NTUSER.DAT]
 - - Start Menu Internet Applications info
- 22. mountdev2 v.20080324 [System]
 - - Return contents of System hive MountedDevices key
- 23. recentdocs v.20080418 [NTUSER.DAT]
 - - Gets contents of user's RecentDocs key
- 24. wordwheelquery v.20100330 [NTUSER.DAT]
 - - Gets contents of user's WordWheelQuery key
- 25. ie_version v.20091016 [Software]
 - - Get IE version and build
- 26. kb950582 v.20081212 [Software]
 - - KB950582 - Gets autorun settings from HKLM hive
- 27. odysseus v.20110202 [NTUSER.DAT]
 - - Extract registry keys for Odysseus by bindshell.net.
- 28. port_dev v.20090118 [Software]
 - - Parses Windows Portable Devices key (Vista)
- 29. adoberdr v.20100218 [NTUSER.DAT]
 - - Gets user's Adobe Reader cRecentFiles values
- 30. shellfolders v.20090115 [NTUSER.DAT]
 - - Retrieve user Shell Folders values
- 31. xpedition v.20090727 [System]
 - Queries System hive for XP Edition info
- 32. wlm_cu v.20110511 [NTUSER.DAT]
 - - Windows Live Messenger parser
- 33. sql_lastconnect v.20090112 [Software]
 - - MDAC cache of successful connections



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 34. userassist2 v.20100308 [NTUSER.DAT]
 - - Displays contents of UserAssist subkeys
- 35. putty v.20110204 [NTUSER.DAT]
 - - Extracts the saved SshHostKeys for PuTTY.
- 36. rootkit_revealer v.20110204 [NTUSER.DAT]
 - - Extracts the EULA value for Sysinternals Rootkit Revealer.
- 37. usbstor2 v.20080825 [System]
 - - Get USBStor key info; csv output
- 38. netassist v.20110427 [NTUSER.DAT]
 - - Check for Firefox Extensions.
- 39. startmenuinternetapps_cu v.20101219 [NTUSER.DAT]
 - - Start Menu Internet Applications info
- 40. proxysettings v.20081224 [NTUSER.DAT]
 - - Gets contents of user's Proxy Settings
- 41. bitbucket v.20080418 [Software]
 - - Get HKLM\...\BitBucket keys\values
- 42. privoxy v.20110204 [NTUSER.DAT]
 - - Extracts the install path for Privoxy.
- 43. autorun v.20081212 [NTUSER.DAT]
 - - Gets autorun settings
- 44. regback v.20100219 [Software]
 - - List all tasks along with logfile name and last written date/time
- 45. muicache v.20080324 [NTUSER.DAT]
 - - Gets EXEs from user's MUICache key
- 46. bho v.20080418 [Software]
 - - Gets Browser Helper Objects from Software hive
- 47. bitbucket_user v.20091020 [NTUSER.DAT]
 - - TEST - Get user BitBucket values
- 48. lsasecrets v.20100219 [Security]
 - - TEST - Get update times for LSA Secrets
- 49. sfc v.20080909 [Software]
 - - --
- 50. listsoft v.20080324 [NTUSER.DAT]
 - - Lists contents of user's Software key
- 51. policies_u v.20091021 [NTUSER.DAT]
 - - Get values from the user's Policies key
- 52. user_win v.20080415 [NTUSER.DAT]
 - - --
- 53. banner v.20081119 [Software]
 - - Get HKLM\SOFTWARE.. Logon Banner Values
- 54. haven_and_hearth v.20110204 [NTUSER.DAT]
 - - Extracts the username and savedtoken for Haven & Hearth.
- 55. applets v.20080324 [NTUSER.DAT]
 - - Gets contents of user's Applets key
- 56. typedpaths v.20100330 [NTUSER.DAT]
 - - Gets contents of user's typedpaths key
- 57. printermru v.20091125 [NTUSER.DAT]
 - - Gets user's Printer Wizard MRU listing
- 58. mmc v.20080324 [NTUSER.DAT]
 - - Get contents of user's MMC\Recent File List key
- 59. tsclient v.20080324 [NTUSER.DAT]
 - - Displays contents of user's Terminal Server Client\Default key
- 60. eventlog v.20090112 [System]
 - - Get EventLog configuration info
- 61. macaddr v.20090118 [Software]
 - - --
- 62. eventlogs v.20081219 [System]
 - - Gets Event Log settings from System hive
- 63. apppaths v.20080404 [Software]
 - - Gets content of App Paths key



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 64. crashdump v.20081219 [System]
 - - Gets crashdump settings from System hive
- 65. msis v.20090911 [Software]
 - - Determine MSI packages installed on the system
- 66. svchost v.20100322 [Software]
 - - Get entries from SvcHost key
- 67. taskman v.20091116 [Software]
 - - Gets Taskman from HKLM\...\Winlogon
- 68. vmware_vsphere_client v.20110204 [NTUSER.DAT]
 - - Extract recent connections list for VMware vSphere Client.
- 69. timezone v.20080324 [System]
 - - Get TimeZoneInformation key contents
- 70. crashcontrol v.20081212 [System]
 - - Get crash control information
- 71. iexplore v.20100308 [NTUSER.DAT]
 - - Get Main Key contents from HKCU\Software\Microsoft\Internet Explorer
- 72. networkuid v.20100312 [Software]
 - - Gets Network key UID value
- 73. gthist v.20100218 [NTUSER.DAT]
 - - Gets Google Toolbar Search History
- 74. yahoo_lm v.20101219 [NTUSER.DAT]
 - - Yahoo Messenger parser
- 75. logon_xp_run v.20080328 [NTUSER.DAT]
 - - Autostart - Get XP user logon Run key contents from NTUSER.DAT hive
- 76. vista_wireless v.20090514 [Software]
 - - Get Vista Wireless Info
- 77. autoendtasks v.20081128 [NTUSER.DAT]
 - - Automatically end a non-responsive task
- 78. installedcomp v.20100116 [Software]
 - - Get info about Installed Components/StubPath
- 79. ie_main v.20091019 [NTUSER.DAT]
 - - Gets values beneath user's Internet Explorer\Main key
- 80. environment v.20110204 [NTUSER.DAT]
 - - Extracts user's Environment paths from NTUSER.DAT
- 81. domains v.20100116 [NTUSER.DAT]
 - - Gets contents Internet Settings\ZoneMap\Domains key
- 82. svcDll v.20091104 [System]
 - - Lists Services keys with ServiceDll values
- 83. dllsearch v.20100824 [System]
 - - Get crash control information
- 84. drwatson v.20081219 [Software]
 - - Gets Dr. Watson settings from Software hive
- 85. auditpol v.20080327 [Security]
 - - Get audit policy from the Security hive file
- 86. indexes v.20090728 [All]
 - - Scans a hive file looking for binary value data that contains MZ
- 87. gtwhitelist v.20100218 [NTUSER.DAT]
 - - Gets Google Toolbar whitelist values
- 88. devclass v.20100901 [System]
 - - Get USB device info from the DeviceClasses keys in the System hive
- 89. shelloverlay v.20100308 [Software]
 - - Gets ShellIconOverlayIdentifiers values
- 90. polacdms v.20100531 [Security]
 - - Get local machine SID from Security hive
- 91. userlocsvc v.20090411 [NTUSER.DAT]
 - - Displays contents of User Location Service\Client key
- 92. dependency_walker v.20110204 [NTUSER.DAT]
 - - Extracts Recent File List for Dependency Walker.
- 93. winlogon v.20080415 [Software]
 - - Get values from the WinLogon key



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 94. shutdown v.20080324 [System]
 - - Gets ShutdownTime value from System hive
- 95. rdpport v.20100713 [System]
 - - Queries System hive for RDP Port
- 96. liveContactsGUID v.20110221 [NTUSER.DAT]
 - - Gets user Windows Live Messenger GUIDs
- 97. ctrlpnl v.20100116 [Software]
 - - Get Control Panel info from Software hive
- 98. hibernate v.20081216 [System]
 - - Check hibernation status
- 99. typedurls v.20080324 [NTUSER.DAT]
 - - Returns contents of user's TypedURLs key.
- 100. nero v.20100218 [NTUSER.DAT]
 - - Gets contents of Ahead\Nero Recent File List subkeys
- 101. streams v.20081124 [NTUSER.DAT]
 - - Parse Streams and StreamsMRU entries
- 102. comdlg32 v.20100402 [NTUSER.DAT]
 - - Gets contents of user's ComDlg32 key
- 103. load v.20100811 [NTUSER.DAT]
 - - Gets load and run values from user hive
- 104. warcraft3 v.20110202 [NTUSER.DAT]
 - - Extract usernames for Warcraft 3.
- 105. comdlg32a v.20100409 [NTUSER.DAT]
 - - Gets contents of user's ComDlg32 key
- 106. startpage v.20100330 [NTUSER.DAT]
 - - Gets contents of user's StartPage key
- 107. skype v.20100713 [NTUSER.DAT]
 - - Gets data user's Skype key
- 108. virut v.20090218 [Software]
 - - Detect Virut artifacts
- 109. winnt_cv v.20080609 [Software]
 - - Get and display the contents of the Windows\CurrentVersion key
- 110. pagefile v.20081212 [System]
 - - Get info on pagefile(s)
- 111. network v.20080324 [System]
 - - Gets info from System\Control\Network GUIDs
- 112. vista_bitbucket v.20080420 [NTUSER.DAT]
 - - Get BitBucket settings from Vista via NTUSER.DAT
- 113. aports v.20110204 [NTUSER.DAT]
 - - Extracts the install path for SmartLine Inc. Active Ports.
- 114. mountdev v.20080324 [System]
 - - Return contents of System hive MountedDevices key
- 115. ssid v.20080327 [Software]
 - - Get WZCSVC SSID Info
- 116. regtime v.20080324 [All]
 - - Dumps entire hive, all keys sorted by LastWrite time
- 117. nic2 v.20100401 [System]
 - - Gets NIC info from System hive
- 118. shellexec v.20081229 [Software]
 - - Gets ShellExecuteHooks from Software hive
- 119. yahoo_cu v.20101219 [NTUSER.DAT]
 - - Yahoo Messenger parser
- 120. usbstor v.20080418 [System]
 - - Get USBStor key info
- 121. aim v.20080325 [NTUSER.DAT]
 - - Gets info from the AOL Instant Messenger (not AIM) install
- 122. compdesc v.20080324 [NTUSER.DAT]
 - - Gets contents of user's ComputerDescriptions key
- 123. win_cv v.20090312 [Software]
 - - Get & display the contents of the Windows\CurrentVersion key



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 124. nolmhash v.20100712 [System]
 - - Gets NoLMHash value
- 125. fileexts v.20080818 [NTUSER.DAT]
 - - Get user FileExt values
- 126. mp2 v.20080324 [NTUSER.DAT]
 - - Gets user's MountPoints2 key contents
- 127. publishingwizard v.20110202 [NTUSER.DAT]
 - - Extract AddNetPlace\LocationMRU for Microsoft Publishing Wizard
- 128. shares v.200800420 [System]
 - - Get list of shares from System hive file
- 129. realplayer6 v.20080324 [NTUSER.DAT]
 - - Gets user's RealPlayer v6 MostRecentClips(Default) values
- 130. clampitm v.20100624 [NTUSER.DAT]
 - - Checks for IOCs for Clampi (per Trend Micro)
- 131. services v.20080507 [System]
 - - Lists services/drivers in Services key by LastWrite times
- 132. realvnc v.20091125 [NTUSER.DAT]
 - - Gets user's RealVNC MRU listing
- 133. renocide v.20110309 [Software]
 - - Check for Renocide malware
- 134. uninstall v.20080331 [Software]
 - - Gets contents of Uninstall key from Software hive
- 135. ide v.20080418 [System]
 - - Get IDE device info from the System hive file
- 136. rdphint v.20090715 [NTUSER]
 - - Gets hosts logged onto via RDP and the Domain\Username
- 137. mndmru v.20080324 [NTUSER.DAT]
 - - Get contents of user's Map Network Drive MRU
- 138. ddm v.20081129 [System]
 - - Get DDM data from Control Subkey
- 139. user_run v.20080328 [NTUSER.DAT]
 - - Autostart - get Run key contents from NTUSER.DAT hive
- 140. stillimage v.20100222 [System]
 - - Get info on StillImage devices
- 141. userassist v.20080726 [NTUSER.DAT]
 - - Displays contents of UserAssist Active Desktop key
- 142. imagedev v.20080730 [System]
 - - --
- 143. networkcards v.20080325 [Software]
 - - Get NetworkCards
- 144. ie_settings v.20091016 [NTUSER.DAT]
 - - Gets IE settings
- 145. disablelastaccess v.20090118 [System]
 - - Get NTFSDisableLastAccessUpdate value
- 146. wallpaper v.200800810 [NTUSER.DAT]
 - - Parses Wallpaper MRU Entries
- 147. product v.20100325 [Software]
 - - Get installed product info
- 148. profilelist v.20080415 [Software]
 - - Get content of ProfileList key
- 149. win7_ua v.20090121 [NTUSER.DAT]
 - - Get Win7 UserAssist data
- 150. compname v.20090727 [System]
 - - Gets ComputerName and Hostname values from System hive
- 151. fw_config v.20080328 [System]
 - - Gets the Windows Firewall config from the System hive
- 152. samparse2 v.20110303 [SAM]
 - - Parse SAM file for user/group mbrshp info
- 153. unreadmail v.20100218 [NTUSER.DAT]
 - - Gets contents of Unreadmail key



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 154. shellex v.20100515 [Software]
 - - Gets Shell Extensions from Software hive
- 155. vncviewer v.20080325 [NTUSER.DAT]
 - - Get VNCViewer system list
- 156. officedocs2010 v.20110329 [NTUSER.DAT]
 - - Gets contents of user's Office doc MRU keys
- 157. routes v.20100817 [System]
 - - Get persistent routes
- 158. svc2 v.20081129 [System]
 - - Lists Services key contents by LastWrite times (CSV)
- 159. landesk v.20090729 [Software]
 - - Get list of programs monitored by LANDESK from Software hive file
- 160. snapshot_viewer v.20110210 [NTUSER.DAT]
 - - Extracts Recent File List for Microsoft Snapshot Viewer.
- 161. assoc v.20080815 [Software]
 - - Get list of file ext associations
- 162. shutdowncount v.20080709 [System]
 - - Retrieves ShutDownCount value
- 163. auditfail v.20081212 [System]
 - - Get CrashOnAuditFail value
- 164. safeboot v.20081216 [System]
 - - Check SafeBoot entries
- 165. usbdevices v.20100219 [System]
 - - Parses Enum\USB key for devices
- 166. specaccts v.20100223 [Software]
 - - Gets contents of SpecialAccounts\UserList key
- 167. clampi v.20091019 [NTUSER.DAT]
 - - TEST - Checks for keys set by Trojan.Clampi PROT module
- 168. userinit v.20080328 [Software]
 - - Gets UserInit value
- 169. svc v.20080610 [System]
 - - Lists services/drivers in Services key by LastWrite times, short format
- 170. imagefile v.20080325 [Software]
 - - Gets Image File Execution Options subkeys w/ Debugger value
- 171. removdev v.200800611 [Software]
 - - Parses Windows Portable Devices key (Vista)
- 172. mrt v.20080804 [Software]
 - - Check to see if Malicious Software Removal Tool has been run
- 173. outlook v.20100218 [NTUSER.DAT]
 - - Gets user's Outlook settings
- 174. networklist v.20090811 [Software]
 - - Collects network info from Vista NetworkList key
- 175. bagtest v.20090828 [NTUSER.DAT]
 - - Test -- BagMRU
- 176. clsid v.20100227 [Software]
 - - Get list of CLSID/registered classes
- 177. nic v.20100401 [System]
 - - Gets NIC info from System hive
- 178. init_dlls v.20110309 [Software]
 - - Check for odd **pInit_DLLs keys
- 179. cain v.20110204 [NTUSER.DAT]
 - - Extracts details for Cain & Abel by oxid.it
- 180. producttype v.20100325 [System]
 - - Queries System hive for Windows Product info
- 181. cpldontload v.20100116 [NTUSER.DAT]
 - - Gets contents of user's Control Panel don't load key
- 182. codeid v.20100608 [Software]
 - - Gets CodeIdentifier DefaultLevel value
- 183. arpcache v.20090413 [NTUSER.DAT]
 - - Retrieves CurrentVersion\App Management\ARPCache entries



TOOLS FOUND ON SIFT WORKSTATION

2.14

- 184. sevenzip v.20100218 [NTUSER.DAT]
 - - Gets records of histories from 7-Zip keys
- 185. bagtest2 v.20090828 [NTUSER.DAT]
 - - Test -- BagMRU
- 186. winvnc v.20110202 [NTUSER.DAT]
 - - Extracts the encrypted password for WinVNC.
- 187. kbdcrash v.20081212 [System]
 - - Checks to see if system is config to crash via keyboard
- 188. winlogon_u v.20091021 [NTUSER.DAT]
 - - Get values from the user's WinLogon key
- 189. legacy v.20090429 [System]
 - - Lists LEGACY_ entries in Enum\Root key
- 190. snapshot v.20080725 [Software]
 - - Check ActiveX comp kill bit; Access Snapshot
- 191. termserv v.20080418 [System]
 - - Gets fDenyTSConnections value from System hive
- 192. oisc v.20091125 [NTUSER.DAT]
 - - Gets contents of user's Office Internet Server Cache
- 193. nic_mst2 v.20080324 [System]
 - - Gets NICs from System hive; looks for MediaType = 2
- 194. mpmru v.20080324 [NTUSER.DAT]
 - - Gets user's Media Player RecentFileList values
- 195. defbrowser v.20091116 [Software]
 - - Gets default browser setting from HKLM
- 196. timezone2 v.20101219 [System]
 - - Get TimezoneInformation key contents
- 197. brisv v.20090210 [NTUSER.DAT]
 - - Detect artifacts of a Troj.Brisv.A infection
- 198. officedocs v.20080324 [NTUSER.DAT]
 - - Gets contents of user's Office doc MRU keys
- 199. winrar v.20080819 [NTUSER.DAT]
 - - Get WinRAR\ArcHistory entries
- 200. regtime_tln v.20080324 [All]
 - - Dumps entire hive - all keys sorted by LastWrite time
- 201. runmru v.20080324 [NTUSER.DAT]
 - - Gets contents of user's RunMRU key
- 202. vista_comdlg32 v.20090821 [NTUSER.DAT]
 - - Gets contents of Vista user's ComDlg32 key
- 203. vnchooksapplicationprefs v.20110208 [NTUSER.DAT]
 - - Get VNCHooks Application Prefs list
- 204. soft_run v.20080328 [Software]
 - - Autostart - get Run key contents from Software hive

M. RAM Analysis

M.1. pdfbook - extract facebook chats from ram

M.1.1. <http://blogs.sans.org/computer-forensics/2009/11/20/facebook-memory-forensics/>

M.2. pdgmail - extract gmail from ram

M.2.1. <http://blogs.sans.org/computer-forensics/2008/10/20/pdgmail-new-tool-for-gmail-memory-forensics/>

M.3. pdymail - extrat yahoo mail from ram

M.3.1. <http://blogs.sans.org/computer-forensics/2009/01/12/pdymail-yahoo-mail-in-memory/>

M.4. skypeex - recover skype chat from ram

M.4.1. <http://nickfurneaux.blogspot.com/2010/03/skype-chat-carver-from-ram-skypeex.html>

M.5. Volatility 1.3

M.6. [volatility](https://www.volatilesystems.com/default/volatility) - <https://www.volatilesystems.com/default/volatility>



TOOLS FOUND ON SIFT WORKSTATION

2.14

M.6.1. Execute commands anywhere in filesystem via command below

M.6.1.1. # volatility [plugin] -f [image]

- connections Print list of open connections
- connscan Scan for connection objects
 - connscan2 Scan for connection objects (New)
 - datetime Get date/time information for image
 - dlllist Print list of loaded dlls for each process
 - dmp2raw Convert a crash dump to a raw dump
 - dmpchk Dump crash dump information
 - files Print list of open files for each process
 - hibinfo Convert hibernation file to linear raw image
 - ident Identify image properties
 - memdmp Dump the addressable memory for a process
 - memmap Print the memory map
 - modscan Scan for modules
 - modscan2 Scan for module objects (New)
 - modules Print list of loaded modules
 - procdump Dump a process to an executable sample
 - pslist Print list of running processes
 - psscan Scan for EPROCESS objects
 - psscan2 Scan for process objects (New)
 - raw2dmp Convert a raw dump to a crash dump
 - regobjkeys Print list of open regkeys for each process
 - sockets Print list of open sockets
 - sockscan Scan for socket objects
 - sockscan2 Scan for socket objects (New)
 - strings Match physical offsets to virtual addresses
 - thrdsan Scan for ETHREAD objects
 - thrdsan2 Scan for thread objects (New)
 - vaddump Dump the Vad sections to files
 - vadinfo Dump the VAD info
 - vadwalk Walk the vad tree

M.7.volatility plugins

- apihooks [VAP] Detect API hooks in user and/or kernel space
- cachedump Dump (decrypted) domain hashes from the registry
- cryptoscan Find TrueCrypt passphrases
- driverscan Scan for driver objects
- fileobjscan Scan for file objects



TOOLS FOUND ON SIFT WORKSTATION

2.14

- getsids Print the SIDs owning each process
- hashdump Dump (decrypted) LM and NT hashes from the registry
- hivedump Dump registry hives to CSV
- hivelist Print list of registry hives
- hivescan Scan for _CMHIVE objects (registry hives)
- idt [VAP] Print Interrupt Descriptor Table (IDT) entries
- keyboardbuffer Print BIOS keyboard buffer
- ldr_modules [VAP] Detect unlinked LDR_MODULE using mapped file names
- lsadump Dump (decrypted) LSA secrets from the registry
- malfind Dump and rebuild executables
- malfind2 [VAP] Detect hidden and injected code
- moddump Dump loaded kernel modules to disk.
- mutantscan Scan for mutant (mutex) objects
- orphan_threads [VAP] Find kernel threads that don't map back to loaded modules
- printkey Print a registry key, and its subkeys and values
- pstree
- ssdt Display SSDT entries
- suspicious Find suspicious command lines and display them
- symlinkobjscan Scan for symbolic link objects
- thread_queues Print message queues for each thread
- volshell Shell in the memory image

M.8. Volatility 2.0 Subversion Checkout

M.8.1. Update: svn update in /usr/local/src/Volatility directory)

M.8.2. Execute commands anywhere in filesystem via command below

M.8.2.1. # vol.py [plugin] -f [image] --profile [PROFILE]

M.8.2.2. Profiles for [PROFILE]

- VistaSP0x86 - A Profile for Windows Vista SP0 x86
- VistaSP1x86 - A Profile for Windows Vista SP1 x86
- VistaSP2x86 - A Profile for Windows Vista SP2 x86
- Win2K3SP0x86 - A Profile for Windows 2003 SP0 x86
- Win2K3SP1x86 - A Profile for Windows 2003 SP1 x86
- Win2K3SP2x86 - A Profile for Windows 2003 SP2 x86
- Win2K8SP1x86 - A Profile for Windows 2008 SP1 x86
- Win2K8SP2x86 - A Profile for Windows 2008 SP2 x86
- Win7SP0x86 - A Profile for Windows 7 SP0 x86
- Win7SP1x86 - A Profile for Windows 7 SP1 x86
- WinXPSP2x86 - A Profile for Windows XP SP2



TOOLS FOUND ON SIFT WORKSTATION

2.14

- WinXPSP3x86 - A Profile for windows XP SP3

M.8.3. PLUGINS for [plugin]

- apihooks [MALWARE] Find API hooks
- bioskbd Reads the keyboard buffer from Real Mode memory
- callbacks [MALWARE] Print system-wide notification routines
- connections Print list of open connections [Windows XP Only]
- connscan2 Scan Physical memory for _TCPT_OBJECT objects (tcp connections)
- crashinfo Dump crash-dump information
- dlldump Dump DLLs from a process address space
- dlllist Print list of loaded dlls for each process
- driverirp [MALWARE] Driver IRP hook detection
- driverscan Scan for driver objects _DRIVER_OBJECT
- files Print list of open files for each process
- filescan Scan Physical memory for _FILE_OBJECT pool allocations
- gdt [MALWARE] Display Global Descriptor Table
- getsids Print the SIDs owning each process
- hashdump Dumps passwords hashes (LM/NTLM) from memory
- hibdump Dumps the hibernation file to a raw file
- hibinfo Dump hibernation file information
- hivedump Prints out a hive
- hivelist Print list of registry hives.
- hivescan Scan Physical memory for _CMHIVE objects (registry hives)
- idt [MALWARE] Display Interrupt Descriptor Table
- imagecopy Copies a physical address space out as a raw DD image
- imageinfo Identify information for the image
- impscan [MALWARE] Scan a module for imports (API calls)
- inspectcache Inspect the contents of a cache
- kdbgscan Search for and dump potential KDBG values
- kpcrscan Search for and dump potential KPCR values
- ldrmodules [MALWARE] Detect unlinked DLLs
- lsadump Dump (decrypted) LSA secrets from the registry
- malfind [MALWARE] Find hidden and injected code
- memdump Dump the addressable memory for a process
- memmap Print the memory map
- moddump Dump a kernel driver to an executable file sample
- modscan2 Scan Physical memory for _LDR_DATA_TABLE_ENTRY objects
- modules Print list of loaded modules



TOOLS FOUND ON SIFT WORKSTATION

2.14

- mutantscan Scan for mutant objects _KMUTANT
- mutantscan db [MALWARE] mutantscan extension for highlighting suspicious mutexes
- netscan Scan a Vista, 2008 or Windows 7 image for connections and sockets
- orphanthreads [MALWARE] Locate hidden threads
- patcher Patches memory based on page scans
- printkey Print a registry key, and its subkeys and values
- procexedump Dump a process to an executable file sample
- procmemdump Dump a process to an executable memory sample
- pslist print all running processes by following the EPROCESS lists
- psscan Scan Physical memory for _EPROCESS objects
- psscan2 Scan Physical memory for _EPROCESS pool allocations
- pstree Print process list as a tree
- psxview [MALWARE] Find hidden processes with various process listings
- regobjkeys Print list of open regkeys for each process
- sockets Print list of open sockets
- sockscan Scan Physical memory for _ADDRESS_OBJECT objects (tcp sockets)
- ssdt Display SSDT entries
- ssdt_by_threads [MALWARE] SSDT hooks by thread
- ssdt_ex [MALWARE] SSDT Hook Explorer for IDA Pro (and SSDT by thread)
- strings Match physical offsets to virtual addresses
- svcscan [MALWARE] Scan for Windows services
- testsuite Run unit test suit using the Cache
- thrdsan2 Scan physical memory for _ETHREAD objects
- userassist Print userassist registry keys and information
- vaddump Dumps out the vad sections to a file
- vadinfo Dump the VAD info
- vadtrees Walk the VAD tree and display in tree format
- vadwalk Walk the VAD tree
- volshell Shell in the memory image

N. Data Carving

N.1. Foremost 1.5.7 - carve files based on headers/footers/max length

N.2. magicrescue

N.3. safecopy

N.4. testdisk



TOOLS FOUND ON SIFT WORKSTATION

2.14

N.5. rapier –

N.6. scalpel 2.0 –

N.6.1. <http://dfsforensics.blogspot.com/2011/04/announcing-scalpel-20.html>

O. Compression Tools

O.1. p7zip - Wrapper on 7zr, a 7-zip file archiver with high compression ratio

O.2. rar - archive files with compression

O.3. unrar - extract files from rar archives

O.4. gzrecover

O.5. bzip/bzip2

P. Malware Analysis

P.1. REMNIX Tools

P.1.1. Analyzing Flash malware: [swftools](#), [flasm](#), [flare](#), [RABCDAsm](#)

P.1.2. Network-monitoring and interactions: [Wireshark](#), [fakedns](#)

P.1.3. JavaScript deobfuscation: Firefox with [Firebug](#), [NoScript](#) and

P.1.4. Interacting with web malware: [TinyHTTPd](#), [Burp Suite Free Edition](#), [stunnel](#), [VirusTotal](#), [VTzilla](#), [User Agent Switcher](#),

P.1.5. Analyzing shellcode: [gdb](#), [objdump](#), [Radare](#) (hex editor+disassembler), [shellcode2exe](#), [libemu](#) with "sctest", [diStorm disassembler](#) library

P.1.6. Dealing with suspicious files: [upx](#), [packerid](#), [bytehlist](#), [xorsearch](#), [TRiD](#), [xortools.py](#), [ssdeep](#), [md5deep](#), [pescanner.py](#)

P.1.7. Malicious document file analysis: [Didier's PDF tools](#), [Origami framework](#), [pdftk](#), [pyOLEScanner.py](#)

P.1.8. Memory forensics: [Volatility Framework](#) with [malware.py](#), [AESKeyFinder](#) and [RSAKeyFinder](#).

P.1.9. Miscellaneous: unzip, strings, [feh](#) image viewer, [SciTE](#) text editor, [OpenSSH](#) server, [VBinDiff](#) file comparison/viewer.

P.2. yara - yara - find files matching patterns and rules written in a special-purpose language

P.3. radare, the reverse engineering framework

P.3.1. <http://radare.nopcode.org/y/>

P.4. PDF Tools

P.4.1. pdfid.py - differentiate between PDF documents that could be malicious and those that are most likely not

P.4.1.1. <http://blog.didierstevens.com/2009/03/31/pdfid/>

P.4.2. pdf-parser.py - parse a PDF document to identify the fundamental elements used in the analyzed file

P.4.2.1. <http://blog.didierstevens.com/programs/pdf-tools/>

P.4.2.2. <http://blog.didierstevens.com/2008/10/20/analyzing-a-malicious-pdf-file/>

P.4.3. make-pdf-javascript.py - create a simple PDF document with embedded JavaScript that will execute upon opening of the PDF document

P.4.3.1. <http://blog.didierstevens.com/programs/pdf-tools/>

P.4.4. pdftohtml - program to convert pdf files into html, xml and png images



TOOLS FOUND ON SIFT WORKSTATION

2.14

- P.4.5.pdfinfo - Portable Document Format (PDF) document information extractor
- P.4.6.pdfimages - Portable Document Format (PDF) image extractor
- P.4.7.pdfotext - Portable Document Format (PDF) to text converter
- Q. Mobile Device Forensics
 - Q.1. Google Android SDK
 - Q.1.1. ipddump (Blackberry backup parser)
 - Q.1.2. iPhone Analyzer
- R. GUI Forensic Analysis
 - R.1. Autopsy
 - R.1.1. <http://www.sleuthkit.org/autopsy/>
 - R.2. PTK 2.0 (SIFT WORKSTATION Exclusive)
 - R.2.1. Login -> admin
 - R.2.2. Password -> forensics
 - R.2.3. <http://ptk.dflabs.com/>
 - R.3. PyFLAG
 - R.3.1. <http://www.pyflag.net/cgi-bin/moin.cgi>
 - R.4. DFF – Digital Forensic Framework
 - R.4.1. <http://www.digital-forensic.org/>
- S. Password Crackers
 - S.1. CmosPwd - BIOS Cracker 5.0
 - S.2. john the ripper (john - a tool to find weak passwords of your users)
 - S.3. samdump : a tool to extract password hashes from MS Windows registry files
 - S.4. bkhive -- dumps the syskey bootkey from a Windows NT/2K/XP/Vista system hive
 - S.5. fcrackzip - a Free/Fast Zip Password Cracker
 - S.6. ophcrack - Cracks Windows passwords with Rainbow tables
 - S.6.1. <http://ophcrack.sourceforge.net/>
- T. Stego
 - T.1. outguess - universal steganographic tool
 - T.1.1.stegbreak
 - T.1.2.stegcompare
 - T.1.3.stegdeimage
 - T.1.4.stegdetect
- U. Crypto
 - U.1. cryptcat - twofish encryption enabled version of nc
 - U.2. outguess - universal steganographic tool
 - U.3. bccrypt - blowfish file encryption
 - U.4. cccrypt - encrypt and decrypt files and streams
- V. Mail
 - V.1. readpst - convert PST (MS Outlook Personal Folders) files to mbox and other formats



TOOLS FOUND ON SIFT WORKSTATION

2.14

V.2. bulk_extractor - create histogram of email addresses on a hard drive

V.2.1. http://afflib.org/software/bulk_extractor

W. Network Forensics

W.1.Snort - open source network intrusion detection system

W.2.tcpdump - dump traffic on a network

W.3.wireshark - Interactively dump and analyze network traffic

W.4.ettercap - A multipurpose sniffer/contet filter for man in the middle attacks

W.5.driftnet - capture images from network traffic and display them in an Xwindow; optionally, capture audio streams and play them.

W.6.tcpreplay - Replay network traffic stored in pcap files

W.7.tcpxtract - extract files from captured network packets

W.8.tcptrack - Monitor TCP connections on the network

W.9.tcpflow - TCP flow recorder

W.10.p0f - identify remote systems passively

W.11.arping - send ARP REQUEST to a neighbour host

W.12.ngrep - network grep

W.13.netwox - examples/tools of the network library netwib

W.14.lft - display the route packets take to a network host/socket; optionally show heuristic network information in transit

W.15.netsed - network packet stream editor

W.16.socat - Multipurpose relay (SOcket CAT)

W.17.oftcap - OFT package, which is a package created by AIM when sending files over the network

W.18.pcapcat - 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

W.19.findsmtpinfo.py - cript creates a report of the SMTP information, stores any emails in msg format, stores any attachments from the emails, decompresses them if they are a compressed format (zip, docx), checks MD5 hashes of all files including the msg files

X. Network Scanning

X.1. knocker - An easy to use network security port scanner

X.2. nikto - web security scanner

X.3. nbtscan - program for scanning networks for NetBIOS name information

Y. Libraries

Y.1. libpff - Library and tools to access the Personal Folder File (PFF) and the Offline Folder File (OFF) format. PFF is used in PAB (Personal Address Book), PST (Personal Storage Table) and OST (Offline Storage Table) files.

Y.1.1. <http://sourceforge.net/projects/libpff>

Y.2. libewf - Libewf is a library for support of the Expert Witness Compression Format (EWF), it support both the SMART (EWF-S01) and EnCase (EWF-E01) format. Libewf allows you to read and write EWF files. Recent versions also support the LEV (EWF-L01) format.



TOOLS FOUND ON SIFT WORKSTATION

2.14

Y.2.1. <http://code.google.com/p/libewf/>

Y.2.1.1. To mount a set of EWF file(s) you can specify the first segment file in the set:

Y. 2. 1. 2. `ewfmount image.E01 /mnt/ewfimage/`

Y.2.1.3. Or specify all segment files:

Y. 2. 1. 4. `ewfmount image.E?? /mnt/ewfimage/`

Y.2.1.5. Note that using a glob of `.E*` can also include files like `.E01.txt`, e.g. for EWF file(s) created by FTKImager. If non-EWF file(s) are passed `ewfmount` will not open the image.

Y.2.1.6. This will create the following device file:

Y. 2. 1. 7. `/mnt/ewfimage/ewf1`

Y.2.1.8. If you get the error:

Y. 2. 1. 9. `No sub system to mount EWF format.`

Y.2.1.10. That means fuse was not detected when building the ewftools, check if you have fuse-dev installed and if `./configure` is able to detect it. The last part of the `./configure` output shows you this in an overview.

Y.2.1.11. To mount a logical evidence file (L01)

Y. 2. 1. 12. `ewfmount -f files image.L01 /mnt/ewfimage/`

Y.2.1.13. This will create directories and files under `/mnt/ewfimage/`. Note that the L01 can also be mounted without the `-f files`, but then it will provide you the raw directory and file data in the L01.

Y.2.2.

Y.3. libnsief - Library and tools to access the Microsoft Internet Explorer (MSIE) Cache File (index.dat) files.

Y.3.1. <http://sourceforge.net/projects/libnsief/>

Y.4. Libbfio - Library to provide basic file input/output abstraction. Libbfio is used in multiple other libraries like libewf, libnsief, libnk2, libolecf and libpff. It is used to chain I/O to support file-in-file access.

Y.4.1. <http://sourceforge.net/projects/libbfio/>

Y.5. liblnk Library and tools to access the Windows Shortcut File (LNK) Format.

Y.5.1. <http://sourceforge.net/projects/liblnk/>

Y.6. Libnk2 - Library and tooling to support the Microsoft Outlook Nickfile (NK2) format. The nickfile is used to store email address aliases.

Y.6.1. <http://sourceforge.net/projects/libnk2/>

Y.7. libolecf - Library and tools to support the OLE 2 Compound File format. The OLE 2 Compound File format is used to store certain versions of Microsoft Office files, thumbs.db and other file formats.

Y.7.1. <http://sourceforge.net/projects/libolecf/>

Y.8. libregf - Library and tools to access the Windows Registry file (regf) format.

Y.8.1. <http://sourceforge.net/projects/libregf/>

Y.9. libvshadow - Library and tools to support 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.

Y.9.1. vshadowmount



TOOLS FOUND ON SIFT WORKSTATION

2.14

Y.9.2.vhshadowinfo

Y.9.3.<http://code.google.com/p/libvshadow/>

Y.9.3.1. You can either mount a VSS volume directly from a device file:

Y.9.3.2. `vshadowmount /dev/sda2 /mnt/vssvolume/`

Y.9.3.3. Or directly out of a RAW image at a certain offset:

Y.9.3.4. `vshadowmount -o $((2048 * 512)) image.raw /mnt/vssvolume/`

Y.9.3.5. Note that vshadowmount takes an offset in bytes if you're copying the output from mmls multiply by the sector size as in the example above:

Y.9.3.6. This will create the volume device file(s) similar to:

Y.9.3.7. `/mnt/vssvolume/vss1`

Y.9.3.8. You can then mount the volume device file as a loopback device:

Y.9.3.9. `mount -o loop,ro /mnt/vssvolume/vss1 /mnt/ntfs_file_system`

Y.10.libbde - Library and tools to support the BitLocker Drive Encryption (BDE) encrypted volumes.

Y.10.1. <http://code.google.com/p/libbde/>

Y.10.1.1. You can either mount a BDE volume directly from a device file:

Y.10.1.2. `bdemount -r 599907-126192-034078-378543-435050-262383-683309-100661 /dev/sda2 /mnt/bdevolume/`

Y.10.1.3. Or directly out of a RAW image at a certain offset:

Y.10.1.4. `bdemount -o 2048 -r 599907-126192-034078-378543-435050-262383-683309-100661 image.raw /mnt/bdevolume/`

Y.10.1.5. Note that bdemount takes an offset in bytes if you're copying the output from mmls multiply by the sector size:

Y.10.1.6. `bdemount -o $((1024 * 512)) -r 599907-126192-034078-378543-435050-262383-683309-100661 image.raw /mnt/bdevolume/`

Y.10.1.7. This will create the following volume device file:

Y.10.1.8. `/mnt/bdevolume/bde1`

Y.10.1.9. If you get the error:

Y.10.1.10. `No sub system to mount BDE volume.`

Y.10.1.11. That means fuse was not detected when building the bde tools, check if you have fuse-dev installed and if ./configure is able to detect it. The last part of the ./configure output shows you this in an overview.

Y.10.1.12. You can then mount the volume device file as a loopback device:

Y.10.1.13. `mount -o loop,ro /mnt/bdevolume/bde1 /mnt/ntfs_file_system`

Y.10.2.

Z. Utilities

Z.1. Maclookup – Look up GEO Location coordinates based off of mac address

Z.2. winexe - psexec for linux

Z.2.1.<http://eol.ovh.org/winexe/>

Z.3. ent - entropy calculator

Z.4. rdesktop - Remote Desktop Protocol client

Z.5. seahorse - manage and examine key files

Z.6. uni2ascii - convert UTF-8 Unicode to various 7-bit ASCII representations

Z.7. sqlite - A command line interface for SQLite

Z.8. bless - hex editor



TOOLS FOUND ON SIFT WORKSTATION

2.14

Z.9. ghex2 - hex editor

Z.10. mbr_parser.py – parse MBR

Z.11. jobparser.py – parse windows .job files

Z.12. jobparse.pl – parse windows .job files

Z.13. shellbags.pl – parse windows shellbags

Z.14. virustotal-search.py – send files to virustotal

Z.15. Maltego - Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.

Z.15.1. <http://www.paterva.com/web5/>

AA. FireFox Plugins

- Passive Cache
 - Passive Cache uses Google's text-only cache service and Archive.org Wayback Machine to display historical versions of a specified web link. This add-on allows for the viewing of a page, or site, while avoiding active connections to the target site.
- Passive Recon
 - PassiveRecon provides information security professionals with the ability to perform "packetless" discovery of target resources utilizing publicly available information.
- SQLite Manager
 - Manage any SQLite database on your computer.
- 1-Click YouTube Downloader
 - v1.5- Supports YouTube's new layout! YouTube download in a single click. Download YouTube videos in FLV, 3GP and MP4 (both High Definition and iPod compatible High-Quality). The simplest YouTube Video Downloader for all YouTube Flash sites, period.
- CookieWatcher
 - Cookie Watcher is a tool to watch selected cookie in a statusbar.
- ExifViewer
 - Displays the Exif and IPTC data in local and remote JPEG images.
- FlagFox
 - Displays a country flag depicting the location of the current website's server and provides a multitude of tools such as site safety checks, whois, translation, similar sites, validation, URL shortening, and more...
- FoxyProxy Standard
 - FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. It offers more features than SwitchProxy, ProxyButton, QuickProxy, xyzproxy, ProxyTex, TorButton, etc.
- Globefish



TOOLS FOUND ON SIFT WORKSTATION

2.14


- Globefish assists users in reading and writing in a foreign language: (1) users can translate any foreign text simply by highlighting it; (2) users can compare usage frequency of different expressions to check errors and find a better expression.
- HostIP.info Geolocation Plugin
 - Displays Geolocation information for a website using hostip.info data. Works with all versions of Firefox...
- Leet Key
 - Transforms typed or static text to L337, ROT13, BASE64, HEX, URL, BIN, DES, AES, Morse code, DVORAK keyboard layout and to lower/to upper case functionality, Leet Font...
- Live HTTP Headers
 - View HTTP headers of a page and while browsing.
- NoScript
 - Allow active content to run only from sites you trust, and protect yourself against XSS and Clickjacking attacks.
- WorldIP
 - REAL location of web server,IP,Datacenter,Ping,Traceroute,RDNS,AS. Often shows different countries from similar add-ons,because it is based on data from core routers worldwide,and not on whois data.Real Google's data centers.Providers looking glasses
- ViewCookies
 - It adds a tab to the Page Info dialog box, which shows the cookies belonging to the current page
- UserAgentSwitcher
 - The User Agent Switcher extension adds a menu and a toolbar button to switch the user agent of a browser.




TOOLS FOUND ON SIFT WORKSTATION


2.14

SANS Digital Forensics Curriculum







Website:
<http://computer-forensics.sans.org>




Blogs:
<http://blogs.sans.org/computer-forensics>




SIFT Workstation:
<http://computer-forensics.sans.org/community/downloads>




Digital Forensics Challenge:
<http://computer-forensics.sans.org/challenges>




Twitter:
www.twitter.com/sansforensics




FOR408
Computer Forensic Investigations – Windows In-Depth
GCFE




FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA



FOR558
Network Forensics




FOR563
Mobile Device Forensics



FOR610
REM: Malware Analysis Tools & Techniques
GREM

Additional Forensics Courses



FOR526
Advanced Filesystem Recovery and Memory Forensics