SIFT WORKSTATION 2.0 DISTRO VERSION

DETAILED INFORMATION

SIFT Workstation 2.0 Developed by Rob Lee and distributed as a part of the SANS Institute's Computer Forensic Curriculum. (http://computer-forensics.sans.org)

The SIFT Workstation is released under GPL.

Background

Faculty Fellow Rob Lee created the SANS Investigative Forensic Toolkit(SIFT) Workstation featured in the Computer Forensic Investigations 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.

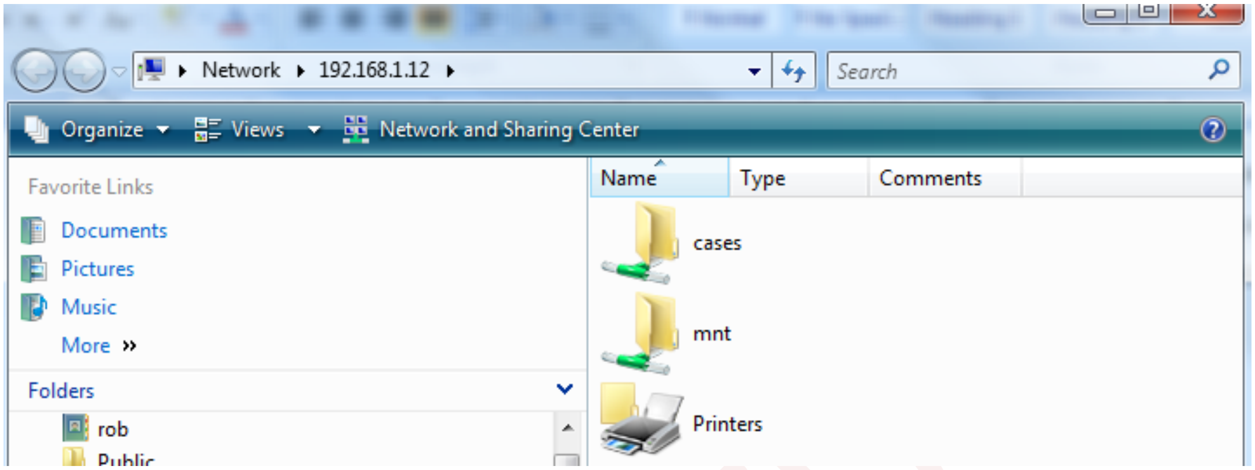
http://computer-forensics.sans.org/course/computer-forensic-investigations-and-incident-response-98-1

The SANS SIFT Workstation is a VMware Appliance that is preconfigured 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 released to the world this week at SANS 2010 has been completely rebuilt on an Ubuntu base with many additional tools and capabilities that can match any modern forensic tool suite.

Basic information:

- After downloading the toolkit, use the credentials below to gain access. Login "sansforensics"
- Password "forensics"
- use **`sudo su -`** to elevate privileges to root while mounting disk images.
- Enable SHARED FOLDERS (VM -> SETTINGS -> OPTIONS -> Shared Folders -> Always Enabled)
  - Access to Host System Found on Desktop **`VMware-Shared-Drive`**
- 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



1. How-Tos -

1.1. How To Mount a Disk Image In Read-Only Mode

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

1.2. How To Create a Filesystem and Registry Timeline

1.2.1. http://blogs.sans.org/computer-forensics/2009/02/24/digital-forensic-sifting-registry-and-filesystem-timeline-creation/

1.3. How To Create a Super Timeline

1.3.1. 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

1.4. How To Acquire and Mount Raw, E01, AFF Disk Images

1.4.1. https://www.sans.org/webcasts/imagine-this-acquisition-and-handling-techniques-of-computer-evidence-92018

1.5. How to use the SIFT Workstation for Basic Memory Image Analysis

1.5.1. https://www.sans.org/webcasts/memory-analysisincident-responders-and-forensic-analysts-92368

2. Filesystem Support

2.1. ntfs (NTFS)

2.2. iso9660 (ISO9660 CD)

2.3. hfs (HFS+)

2.4. raw (Raw Data)

2.5. swap (Swap Space)

2.6. memory (Ram Data)

2.7. fat12 (FAT12)

2.8. fat16 (FAT16)

2.9. fat32 (FAT32)

2.10. ext2 (Ext2)

2.11. ext3 (Ext3)

2.12. ufs1 (UFS1)

2.13. ufs2 (UFS2)

3. Evidence Image File Support

3.1. raw (Single raw file (dd))

3.2. aff (Advanced Forensic Format)

3.3. afd (AFF Multiple File)

3.4. afm (AFF with external metadata)

3.5. afflib (All AFFLIB image formats (including beta ones))

3.6. ewf (Expert Witness format (encase))

3.7. split raw (Split raw files)

3.8. split ewf (Split E01 files)

3.8.1. mount_ewf.py - mount E01 image/split images to view single raw file and metadata

4. Partition Table Support

4.1. dos (DOS Partition Table)

4.2. mac (MAC Partition Map)

4.3. bsd (BSD Disk Label)
4.4. sun (Sun Volume Table of Contents (Solaris))
4.5. gpt (GUID Partition Table (EFI))
5. Digital Evidence Acquisition
5.1. guymager - GUI Imager
5.1.1. http://guymager.sourceforge.net/
5.2. linen - Guidance Image
5.2.1. http://www.forensicswiki.org/wiki/LinEn
5.3. dd - dd, sometimes called GNU dd, is the oldest imaging tool still used.
5.4. 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.
5.4.1. http://www.gnu.org/software/ddrescue/ddrescue.html
5.5. dc3dd - dc3dd is a patched version of GNU dd with added features for computer forensics.
5.5.1. http://dc3dd.sourceforge.net/
5.6. dcfldd - dcfldd is an enhanced version of dd developed by the U.S. Department of Defense Computer Forensics Lab.
5.6.1. http://dcfldd.sourceforge.net/
5.7. sdd
5.7.1. http://linux.maruhn.com/sec/sdd.html
5.8. ewfacquire - create EWF (E01) file format images
5.8.1. http://linux.die.net/man/1/ewfacquire
5.8.2. http://www.forensicswiki.org/wiki/Libewf
5.9. 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.
5.9.1. http://www.afflib.org/aimage.php
6. Media Management
6.1. ewflib
6.1.1. http://sourceforge.net/projects/libewf/
6.1.2. ewfacquire - ewfacquire to acquire data from a file or device and store it in the EWF format
6.1.3. ewfexport - ewfexport to export data from the EWF format (Expert Witness Compression Format) to raw data or another EWF format.
6.1.4. ewfverify - ewfverify to verify data stored in the EWF format (Expert Witness Compression Format).
6.1.5. ewfinfo - wfinfo to determine information about the EWF format
6.1.6. mount_ewf.pl - mount EWF format images/split images to view single raw file and metadata
6.2. afflib
6.2.1. http://www.afflib.org/aimage.php
6.2.2. aimage- ewfacquire to acquire data from a file or device and store it in the AFF format
6.2.3. afcat - Output contents of an image file to stdout
6.2.4. afconvert - Convert AFF images to Raw or Raw to AFF image
6.2.5. afuse - mount AFF format images/split images to view single raw file and metadata
7. Mounting Disk Images -
7.1. ntfs3g - http://www.tuxera.com/community/ntfs-3g-download/
7.2. http://blogs.sans.org/computer-forensics/2009/02/19/digital-forensic-sifting-how-to-perform-a-read-only-mount-of-evidence/

8. Hashing Tools

8.1. http://md5deep.sourceforge.net/

8.2. md5deep - Compute and compare MD5 message digests

8.3. sha1deep - Compute and compare SHA-1 message digests

8.4. sha256deep - Compute and compare SHA-256 message digests

8.5. tigerdeep - Compute and compare Tiger message digests

8.6. whirlpooldeep - Compute and compare Whirlpool message digests

8.7. hashdeep - Compute, compare, or audit multiple message digests

8.8. Fuzzy Hashing

8.8.1. ssdeep - Computes context triggered piecewise hashes

9. Disk Analysis - Sleuthkit Tools

9.1. http://www.sleuthkit.org/

9.2. Media Management Layer

9.2.1. mmls - Display the partition layout of a volume system (partition tables)

9.2.2. mmstat - Display details about the volume system (partition tables)

9.2.3. disk_stat - Check for Host Protected Area (HPA)

9.2.4. disk_sreset - remove HPA

9.3. Data Layer

9.3.1. blkls - List or output file system data units.

9.3.2. blkstat - Display details of a file system data unit (i.e. block or sector)

9.3.3. blkcat - Display the contents of file system data unit in a disk image.

9.3.4. blkcalc - Converts between unallocated disk unit numbers and regular disk unit numbers

9.3.5. srch_strings - print out ascii or unicode strings from a raw file

9.3.6. grep - search for strings from a dirty_words list or a file

9.4. Metadata Layer

9.4.1. istat - Display details of a meta-data structure (i.e. inode)

9.4.2. ils - List inode information

9.4.3. icat - Output the contents of a file based on its inode number

9.4.4. ifind - Find the meta-data structure that has allocated a given disk unit or file name

9.4.5. analyszeMFT.py - parse MFT structure pulling out all metadata into csv file

9.4.5.1. http://integriography.wordpress.com/2010/01/20/analyzemft-a-python-tool-to-deconstruct-the-windows-ntfs-mft-file/

9.5. Filename Layer

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

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

9.6. 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

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

9.6.2. mac-robber

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

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

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

9.6.5.1. Log2timeline/Timescanner output formats

9.6.5.1.1. cef	Output timeline using the ArcSight Commen Event Format (CEF)

9.6.5.1.2. cftl	Output timeline in a XML format that can be read by CFTL
9.6.5.1.3. csv	Output timeline using CSV (Comma Separated Value) file
9.6.5.1.4. mactime	Output timeline using mactime format
9.6.5.1.5. mactime_l	Output timeline using this particular output method
9.6.5.1.6. simile	Output timeline in a XML format that can be read by a SIMILE widget
9.6.5.1.7. sqlite	Output timeline into a SQLite database
9.6.5.1.8. tln	Output timeline using H. Carvey's TLN format

9.6.5.2. Log2timeline/Timescanner Parsing Formats

9.6.5.2.1. chrome	Parse the content of a Chrome history file
9.6.5.2.2. evt	Parse the content of a Windows 2k/XP/2k3 Event Log
9.6.5.2.3. evtx	Parse the content of a Windows Event Log File (EVTX)
9.6.5.2.4. exif	Extract metadata information from files using ExifTool
9.6.5.2.5. ff_bookmark	Parse the content of a Firefox bookmark file
9.6.5.2.6. firefox3 0.7	Parse the content of a Firefox 3 history file
9.6.5.2.7. iehistory	Parse the content of an index.dat file containg IE history
9.6.5.2.8. iis	Parse the content of a IIS W3C log file
9.6.5.2.9. isatxt	Parse the content of a ISA text export log file
9.6.5.2.10. mactime	Parse the content of a body file in the mactime format
9.6.5.2.11. mcafee	Parse the content of a log file
9.6.5.2.12. opera	Parse the content of an Opera's global history file
9.6.5.2.13. oxml	Parse the content of an OpenXML document (Office 2007 documents)
9.6.5.2.14. pcap	Parse the content of a PCAP file
9.6.5.2.15. pdf	Parse some of the available PDF document metadata
9.6.5.2.16. prefetch	Parse the content of the Prefetch directory
9.6.5.2.17. recycler	Parse the content of the recycle bin directory
9.6.5.2.18. restore	Parse the content of the restore point directory
9.6.5.2.19. setupapi	Parse the content of the SetupAPI log file in Windows XP
9.6.5.2.20. sol	Parse the content of a .sol (LSO) or a Flash cookie file
9.6.5.2.21. squid	Parse the content of a Squid access log (http_emulate off)
9.6.5.2.22. tln	Parse the content of a body file in the TLN format
9.6.5.2.23. userassist	Parses the UserAssist Active Desktop key (part of NTUSER.DAT file)
9.6.5.2.24. win_link	Parse the content of a Windows shortcut file (or a link file)
9.6.5.2.25. xpfirewall	Parse the content of a XP Firewall log

10. Artifact Analysis

10.1. missidentify - Find executable files without an executable extensionq
10.2. Galetta - a ms-windows cookies analyzer
10.3. Pasco - a ms-windows IExplorer cache analyzer
10.4. Rifiuti - a ms-windows trashcan analyzer
10.5. mdbtools - playing with MS mdb access databases
10.6. antiword - show the text and images of MS Word documents
10.7. exiftool - metadata extractor (over 400 file types)
10.8. extract - keyword extractor
10.9. lslnk - list link file metadata information
10.10. pref.pl - list prefetch directory information
10.11. reglookup
10.12. vinetto - parse thumbs.db files

10.13. Windows Event Log Analysis

10.13.1. GrokEVT - parse windows event logs

10.13.1.1. http://projects.sentinelchicken.org/grokevt/

10.13.2. Evtxtools - Parse EVTX event logs

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

11. Registry Analysis

11.1. recover_deleted_registry_keys.pl - recover unallocated keys and key slack from a registry hive

11.2. ripxp.pl - Windows XP Restore Point Parser

11.2.1. 1.1.1. www.regripper.net

11.3. rip.pl - regripper

11.3.1. www.regripper.net

11.3.2. Regripper Plugins

11.3.2.1. appinitdlls [Software] - Gets contents of AppInit_DLLs value

11.3.2.2. cmd_shell [Software] - Gets shell open cmds for various file types

11.3.2.3. mspaper [NTUSER.DAT - Gets images listed in user's MSPaper key

11.3.2.4. usb [System] - Get USB subkeys info; csv output

11.3.2.5. acmru [NTUSER.DAT] - Gets contents of user's ACMru key

11.3.2.6. logonusername [NTUSER.DAT] - Get user's Logon User Name value

11.3.2.7. winzip [NTUSER.DAT] - Get WinZip extract and filemenu values

11.3.2.8. controlpanel [NTUSER.DAT] - Look for RecentTask* values in ControlPanel key (Vista)

11.3.2.9. mountdev2 [System] - Return contents of System hive MountedDevices key

11.3.2.10. recentdocs [NTUSER.DAT] - Gets contents of user's RecentDocs key

11.3.2.11. adoberdr [NTUSER.DAT] - Gets user's Adobe Reader cRecentFiles values

11.3.2.12. usbstor2 [System] - Get USBStor key info; csv output

11.3.2.13. bitbucket [Software] - Get HKLM\..\BitBucket keys\values

11.3.2.14. muicache [NTUSER.DAT] - Gets EXEs from user's MUICache key

11.3.2.15. bho [Software] - Gets Browser Helper Objects from Software hive

11.3.2.16. listsoft [NTUSER.DAT] - Lists contents of user's Software key

11.3.2.17. user_win [NTUSER.DAT] - --

11.3.2.18. applets [NTUSER.DAT] - Gets contents of user's Applets key

11.3.2.19. mmc [NTUSER.DAT] - Get contents of user's MMC\Recent File List key

11.3.2.20. tsclient [NTUSER.DAT] - Displays contents of user's Terminal Server Client\Default key

11.3.2.21. apppaths [Software] - Gets content of App Paths key

11.3.2.22. timezone [System] - Get TimeZoneInformation key contents

11.3.2.23. logon_xp_run [NTUSER.DAT] - Autostart - Get XP user logon Run key contents from NTUSER.DAT hive

11.3.2.24. auditpol [Security] - Get audit policy from the Security hive file

11.3.2.25. devclass [System] - Get USB device info from the DeviceClasses keys in the System hive

11.3.2.26. winlogon [Software] - Get values from the WinLogon key

11.3.2.27. shutdown [System] - Gets ShutdownTime value from System hive

11.3.2.28. typedurls [NTUSER.DAT] - Returns contents of user's TypedURLs key.

11.3.2.29. comdlg32 [NTUSER.DAT] - Gets contents of user's ComDlg32 key

11.3.2.30. winnt_cv v.20080609 [Software]- Get and display the contents of the Windows\CurrentVersion key

11.3.2.31. network [System] - Gets info from System\Control\Network GUIDs

11.3.2.32. vista_bitbucket [NTUSER.DAT] - Get BitBucket settings from Vista via NTUSER.DAT

11.3.2.33. mountdev [System] - Return contents of System hive MountedDevices key

11.3.2.34. ssid [Software] - Get WZCSVC SSID Info

11.3.2.35. regtime [All] - Dumps entire hive, all keys sorted by LastWrite time

11.3.2.36. usbstor [System] - Get USBStor key info

11.3.2.37. aim [NTUSER.DAT] - Gets info from the AOL Instant Messenger (not AIM) instal

11.3.2.38. compdesc [NTUSER.DAT] - Gets contents of user's ComputerDescriptions key

11.3.2.39. fileexts [NTUSER.DAT] - Get user FileExts values

11.3.2.40. mp2 [NTUSER.DAT] - Gets user's MountPoints2 key contents

11.3.2.41. shares [System] - Get list of shares from System hive file

11.3.2.42. realplayer6 [NTUSER.DAT] - Gets user's RealPlayer v6 MostRecentClips(Default) values

11.3.2.43. services [System] - Lists services/drivers in Services key by LastWrite times

11.3.2.44. uninstall [Software] - Gets contents of Uninstall key from Software hive

11.3.2.45. ide [System] - Get IDE device info from the System hive file

11.3.2.46. mndmru [NTUSER.DAT] - Get contents of user's Map Network Drive MRU

11.3.2.47. user_run [NTUSER.DAT] - Autostart - get Run key contents from NTUSER.DAT hive

11.3.2.48. userassist [NTUSER.DAT] - Displays contents of UserAssist Active Desktop key

11.3.2.49. imagedev [System] - --

11.3.2.50. networkcards [Software] - Get NetworkCards

11.3.2.51. wallpaper [NTUSER.DAT] - Parses Wallpaper MRU Entries

11.3.2.52. profilelist [Software] - Get content of ProfileList key

11.3.2.53. compname [System] - Gets ComputerName value from System hive

11.3.2.54. fw_config [System] - Gets the Windows Firewall config from the System hive

11.3.2.55. vncviewer [NTUSER.DAT] - Get VNCViewer system list

11.3.2.56. assoc [Software] - Get list of file ext associations

11.3.2.57. shutdowncount [System] - Retrieves ShutDownCount value

11.3.2.58. userinit [Software] - Gets UserInit value

11.3.2.59. svc [System] - Lists services/drivers in Services key by LastWrite times, short format

11.3.2.60. imagefile [Software] - Gets Image File Execution Options subkeys w/ Debugger value

11.3.2.61. removdev [Software] - Parses Windows Portable Devices key (Vista)

11.3.2.62. mrt [Software] - Check to see if Malicious Software Removal Tool has been run

11.3.2.63. samparse [SAM] - Parse SAM file for user/group mbrshp info

11.3.2.64. snapshot [Software] - Check ActiveX comp kill bit; Access Snapshot

11.3.2.65. termserv [System] - Gets fDenyTSConnections value from System hive

11.3.2.66. nic_mst2 [System] - Gets NICs from System hive; looks for MediaType = 2

11.3.2.67. mpmru [NTUSER.DAT] - Gets user's Media Player RecentFileList values

11.3.2.68. officedocs [NTUSER.DAT] - Gets contents of user's Office doc MRU keys

11.3.2.69. winrar [NTUSER.DAT] - Get WinRAR\ArcHistory entries

11.3.2.70. runmru [NTUSER.DAT] - Gets contents of user's RunMRU key

11.3.2.71. soft_run [Software] - Autostart - get Run key contents from Software hive

12. RAM Analysis

12.1. pdfbook - extract facebook chats from ram

12.1.1. http://blogs.sans.org/computer-forensics/2009/11/20/facebook-memory-forensics/

12.2. pdgmail - extract gmail from ram

12.2.1. http://blogs.sans.org/computer-forensics/2008/10/20/pdgmail-new-tool-for-gmail-memory-forensics/

12.3. pdymail - extrat yahoo mail from ram

12.3.1. http://blogs.sans.org/computer-forensics/2009/01/12/pdymail-yahoo-mail-in-memory/

12.4. skypeex - recover skype chat from ram

12.4.1. http://nickfurneaux.blogspot.com/2010/03/skype-chat-carver-from-ram-skypeex.html

12.5. volatility - https://www.volatilesystems.com/default/volatility

12.5.1.	connections	Print list of open connections
12.5.2.	connscan	Scan for connection objects
12.5.3.	connscan2	Scan for connection objects (New)
12.5.4.	datetime	Get date/time information for image
12.5.5.	dlllist	Print list of loaded dlls for each process
12.5.6.	dmp2raw	Convert a crash dump to a raw dump
12.5.7.	dmpchk	Dump crash dump information
12.5.8.	files	Print list of open files for each process
12.5.9.	hibinfo	Convert hibernation file to linear raw image
12.5.10.	ident	Identify image properties
12.5.11.	memdmp	Dump the addressable memory for a process
12.5.12.	memmap	Print the memory map
12.5.13.	modscan	Scan for modules
12.5.14.	modscan2	Scan for module objects (New)
12.5.15.	modules	Print list of loaded modules
12.5.16.	procdump	Dump a process to an executable sample
12.5.17.	pslist	Print list of running processes
12.5.18.	psscan	Scan for EPROCESS objects
12.5.19.	psscan2	Scan for process objects (New)
12.5.20.	raw2dmp	Convert a raw dump to a crash dump
12.5.21.	regobjkeys	Print list of open regkeys for each process
12.5.22.	sockets	Print list of open sockets
12.5.23.	sockscan	Scan for socket objects
12.5.24.	sockscan2	Scan for socket objects (New)
12.5.25.	strings	Match physical offsets to virtual addresses (may take a while, VERY verbose)
12.5.26.	thrdscan	Scan for ETHREAD objects
12.5.27.	thrdscan2	Scan for thread objects (New)
12.5.28.	vaddump	Dump the Vad sections to files
12.5.29.	vadinfo	Dump the VAD info
12.5.30.	vadwalk	Walk the vad tree

12.6. volatility plugins

12.6.1.	apihooks	[VAP] Detect API hooks in user and/or kernel space
12.6.2.	cachedump	Dump (decrypted) domain hashes from the registry
12.6.3.	cryptoscan	Find TrueCrypt passphrases
12.6.4.	driverscan	Scan for driver objects
12.6.5.	fileobjscan	Scan for file objects
12.6.6.	getsids	Print the SIDs owning each process
12.6.7.	hashdump	Dump (decrypted) LM and NT hashes from the registry
12.6.8.	hivedump	Dump registry hives to CSV
12.6.9.	hivelist	Print list of registry hives
12.6.10.	hivescan	Scan for _CMHIVE objects (registry hives)
12.6.11.	idt	[VAP] Print Interrupt Descriptor Table (IDT) entries

12.6.12.	keyboardbuffer	Print BIOS keyboard buffer
12.6.13.	ldr_modules	[VAP] Detect unlinked LDR_MODULE using mapped file names
12.6.14.	lsadump	Dump (decrypted) LSA secrets from the registry
12.6.15.	malfind	Dump and rebuild executables
12.6.16.	malfind2	[VAP] Detect hidden and injected code
12.6.17.	moddump	Dump loaded kernel modules to disk.
12.6.18.	mutantscan	Scan for mutant (mutex) objects
12.6.19.	orphan_threads	[VAP] Find kernel threads that don't map back to loaded modules
12.6.20.	printkey	Print a registry key, and its subkeys and values
12.6.21.	pstree	
12.6.22.	ssdt	Display SSDT entries
12.6.23.	suspicious	Find suspicious command lines and display them
12.6.24.	symlinkobjscan	Scan for symbolic link objects
12.6.25.	thread_queues	Print message queues for each thread
12.6.26.	volshell	Shell in the memory image

13. Data Carving

    13.1. foremost - carve files based on headers/footers/max length

    13.2. magicresuce

    13.3. safecopy

    13.4. testdisk

    13.5. rapier -

14. Compression Tools

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

    14.2. rar - archive files with compression

    14.3. unrar - extract files from rar archives

    14.4. gzrecover

    14.5. bzip/bzip2

15. Malware Analysis

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

16. PDF Tools

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

        16.1.1. http://blog.didierstevens.com/2009/03/31/pdfid/

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

        16.2.1. http://blog.didierstevens.com/programs/pdf-tools/

        16.2.2. http://blog.didierstevens.com/2008/10/20/analyzing-a-malicious-pdf-file/

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

        16.3.1. http://blog.didierstevens.com/programs/pdf-tools/

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

    16.5. pdfinfo - Portable Document Format (PDF) document information extractor

    16.6. pdfimages - Portable Document Format (PDF) image extractor

    16.7. pdftotext - Portable Document Format (PDF) to text converter

17. F-Response Compatibility

    17.1. iSCSI

18. GUI Forensic Analysis

18.1. Autopsy

18.1.1. http://www.sleuthkit.org/autopsy/

18.2. PTK

18.2.1. http://ptk.dflabs.com/

18.3. PyFLAG

18.3.1. http://www.pyflag.net/cgi-bin/moin.cgi

19. Anti-Virus

19.1. ClamAV - Anti-Virus

19.1.1. http://www.clamav.net/lang/en/

19.2. rkhunter - Rootkit Hunter

19.2.1. http://www.rootkit.nl/

19.3. chkrootkit

19.3.1. http://www.chkrootkit.org/

20. Password Crackers

20.1. CmosPwd - BIOS Cracker 5.0

20.2. john the ripper (john - a tool to find weak passwords of your users)

20.3. samdump : a tool to extract password hashes from MS Windows registry files

20.4. bkhive -- dumps the syskey bootkey from a Windows NT/2K/XP/Vista system hive

20.5. fcrackzip - a Free/Fast Zip Password Cracker

20.6. ophcrack - Cracks Windows passwords with Rainbow tables

20.6.1. http://ophcrack.sourceforge.net/

21. Stego

21.1. outguess - universal steganographic tool

21.1.1. stegbreak

21.1.2. stegcompare

21.1.3. stegdeimage

21.1.4. stegdetect

22. Crypto

22.1. cryptcat - twofish encryption enabled version of nc

22.2. outguess - universal steganographic tool

22.3. bcrypt - blowfish file encryption

22.4. ccrypt - encrypt and decrypt files and streams

23. Mail

23.1. readpst - convert PST (MS Outlook Personal Folders) files to mbox and other formats

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

24. Network Forensics

24.1. Snort - open source network intrusion detection system

24.2. tcpdump - dump traffic on a network

24.3. wireshark - Interactively dump and analyze network traffic

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

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

24.6. tcpreplay - Replay network traffic stored in pcap files

24.7. tcpxtract - extract files from captured network packets

24.8. tcptrack - Monitor TCP connections on the network

24.9. tcpflow - TCP flow recorder

24.10. p0f - identify remote systems passively
24.11. arping - send ARP REQUEST to a neighbour host
24.12. ngrep - network grep
24.13. netwox - examples/tools of the network library netwib
24.14. lft - display the route packets take to a network host/socket; optionally show heuristic network information in transit
24.15. netsed - network packet stream editor
24.16. socat - Multipurpose relay (SOcket CAT)
24.17. oftcat - OFT package, which is a package created by AIM when sending files over the network
24.18. 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
24.19. 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

25. Network Scanning
25.1. knocker - An easy to use network security port scanner
25.2. nikto - web security scanner
25.3. nbtscan - program for scanning networks for NetBIOS name information

26. Utilities
26.1. winexe - psexec for linux
26.1.1. http://eol.ovh.org/winexe/
26.2. ent - entropy calculator
26.3. rdesktop - Remote Desktop Protocol client
26.4. seahorse - manage and examine key files
26.5. uni2ascii - convert UTF-8 Unicode to various 7-bit ASCII representations
26.6. sqlite - A command line interface for SQLite
26.7. bless - hex editor
26.8. ghex2 - hex editor

If you have any questions about the SIFT Workstation, please email the creator and author Rob Lee rlee@sans.org with upgrade requests and questions.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

* a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

* b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

* c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

* d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

* a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

* b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

* c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

* d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

* e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

* a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

* b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

* c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

  * d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

  * e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

  * f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
    <program>  Copyright (C) <year>  <name of author>

    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

    This is free software, and you are welcome to redistribute it

    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.