DIGITAL FORENSIC LABORATORY/INVESTIGATION TOOLS

OPENSOURCE, FREEWARE

Backtrack (generally for security purposes including penetration testing)

Safeback/snapback

MD5/SHA-3

Tripwire (for academic use visit tripwire.org)

syslogd for UNIX

dd from \*nix

NTsyslog for Windows

Sleuth Kit (sleuthkit.org)

Stegdetect (outguess.org)

Pixelab’s xxcopy, Windows’ Robocopy (collecting live data from Windows platform)

Glimpse (webglimpse.org) (free full text indexing program)

libPST/libDBX package (well-known tool for reading Outlook files, UniAccess to convert UNIX mail back into PST and other formats) (extract the contents of a DBX file into a RFC-compliant UNIX mail format)

Red Cliff Web Historian (extract the history data and put it into plaintext or HTML with Firefox)

NetAnalysis (Firefox forensically work out history file, performs searching)

PROPRIETARY/COMMERCIAL, FEEAWARE

Forensic computers: http://www.forensiccomputers.com/educational-program.html

E-fence/Helix (collect volatile information in Windows platform)

Encase (file system recovery – FAT, NTFS, deleted files and file fragments, INFO record (data from Recycle Bin), sectors analyzer, indexing, well-known tool for reading Outlook files, open and search the contents of PST directly, newer version have support for Outlook Compressible Encryption, past filenames and has built support for reading and searching the Unicode into the latest version, Palm-OS device data acquisition)

Pasco/Galleta (Foundstone) (Internet browsing investigation) (history file, cookie)

Superscan (Foundstone) (Probe the test system and determine which ports are open)

OnTrack (PowerControls, access, search and extract emails from an .edb, written by Veritas NetBackup, Veritas Backup Exec, Computer Associates BrightStor ARCserve, Legato NetWorker, IBM Tivoli and NTBackup, though not automated)

ASRData's SMART (file system recovery – FAT, NTFS, deleted files and file fragments, INFO record(has great tools for performing analysis of the ext2/3 file system)(user friendly program that runs natively on Windows, Linux and Macintosh))

AccessData’s Forensic Tool Kit (FTK) (HFS and HFSX support) (parse unallocated space, take entire image, can be used to determine symmetric keys, its component PRTK can be used to brute force asymmetric, cryptosystem, however, files with stronger keys may take years to crack, data carving and conversion i.e. import whole image from EnCase and SMART, can access text of MIME, RFC822, well-known tool for reading Outlook files, review large amount of of email and will now identify and segregate webmail from other email, excellent all-around tool for investigating e-mail files, fastest tool for searching through e-mail files) (Windows registry)

NetworkMiner (netresec.com)

The Coroner’s Toolkit (TCT) (unallocated space, Lazarus—data carving, searches unallocated space in Linux—it will then attempt to break the data into file types and blocks))

Belkasoft Evidence Center Portable (with forgery detection plugin, IM analyzer)

Stego Suite (wetstonetech.com)

MTX (mtx.opensource-sw.net) (control attached tape manually)

MediaMerge (eMag Solution) (accessing tape)

Verity (especially for enterprise indexing system)

Recovery Manager for Exchange/Notes (offers functionality that other tools in the market do not offer, act as virtual Exchange server—run in emulation mode, extract NSF files from tape to PST)

Network Email Examiner (access, search and extract messages from an NSF and GroupWise, if NGWGUARD.DLL and the three directories OFMSG, OFUSER, OFFILES—it can recover deleted messages)

Transend Migrator Forensic Edition (allow the conversion of Novell GroupWise data to a number of different formats, GroupWise server must exist first, great tool for performing a number of email tasks include converting EML, text, mbox and many other e-mail formats (e-discovery and compliance) to Outlook PST format)

Nucleus Data Recovery (allows to convert OST files to PST)

DBX Examination Tools (Outlook Express)

Hot Pepper Technology’s Email Detective (for AOL email)

Rdhtool.exe (strips MS Office 2003 documents of all its metadata)

XEmacs (for non-forensics work, look for information that may have been deleted but not removed from the file)

Strings.exe (past filenames—stored in Unicode instead of straight ASCII, extracts files)

SQLite Manager (Firefox, also check MORK format, uses SQLite to store cookies as well as other information, result can be exported as CSV)

UserAssist Utility (Windows 2000, XP, Vista, can be immensely valuable in the timeline creation process, didierstevens.com—free and can decrypt ROT13—Caesar’s cipher)

F-Response (Field kit, consultant, enterprise) (live response toolkit, does not write on the target’s harddrive and can be done on remote, collect RAM contents)

Advance registry tracer (Elcomsoft) – (use to monitor Windows registry)

Utilities especially used for REMOTE FORENSICS

Encase Enterprise Edition (iPhone raw disk image) (discover mounted encrypted volume (and data as well?)(Windows registry)(Can be used to locate, parse and analyze Windows event logs))

Paraben Enterprise (P2EE) (Paraben’s registry analyzer, text search,makes use of dtSearch indexing, extract messages .edb, access text of MIME and RFC822, Paraben’s Network E-mail Examiner (offers some rare and valuable features such as the ability to convert mailboxes from Novell GroupWise, Lotus Notes, or EDB databases to Outlook PST, MSG, or EML) is entirely different with Paraben’s Email Examiner (simplifies the complexity of the PST mail store by converting it into a generic mailbox format of Outlook artifacts include .PST, .OST, .PAB, search capabilities are excellent), well-known tool for reading Outlook files, very fast in converting the PSTs, AOL converter also with EnCase and FTK, decrypt ROT13 used by UserAssist) (Paraben StrongHold Bag, blocks all electronic signals from entering or exiting the device) (Device Seizure was designed with the realization that consumers have choices regarding what kind of mobile device and carrier services they can buy, uses several types of plug-ins and data acquisitions, acquires literally hundreds of models of cellphones)

Prodiscover (collect the contents of physical memory as well as system BIOS via remote server applet)

Firefox Forensic (Machor Software) (break out profile data and user setting from these preference files)

Forensic Registry Viewer (useful for malware)

WINDOWS

Registry (if USB has been or being used)

Share.exe (id network/file shares)

Pstoreview.exe (view contents of protected storage)

Nigilant32.exe (collect volatile information)

Wmic.exe (to collect information remotely)

Psexec.exe (unusual or suspicious process in the system)

Svc.exe (collects information about services on the system)

Tlist.exe (process list)

UrlScan (protect IIS from vulnerabilities)

Pd.exe (process dumper of memory contents, available also in Linux, dumps the entire process along with additional metadata and process environment)

Userdump.exe (process memory dumper, available in MS)

Adplus (autodumplus)

Dd in UNIX (dump process memory also with Windows)

KnTDD (collect physical memory and system BIOS even through user level)

KnTTools ( capable of bulk encryption output using X.509 certifications, AES-256 (default) and downgrading to 3DES on Windows 2000, memory acquisition using a KnTDDSvc, remote deployment module that is able to deply the KnTDDSvc by either pushing it to a remote admin share or pulling it from a Web server over SSL with cryptographic verification, the system is still running when contents of memory are retrieved)

MDD.exe (allows dumping the content of physical memory)

Win32dd.exe (dumps RAM content, crash dump—similar to Windows’—which can then be used to analyze it with Microsoft Debugging Tools)

Memoryze (memory collection and analysis)

Winen.exe—Guidance Software (collect contents of physical memory)

Fastdump.exe (collect contents of RAM)

Cain (Windows registry, LSA)

LSAdump.exe (bindview.com) (Windows registry particularly LSA)

Passdump.exe (Windows registry)

Dependency Walker (depends.exe) (Other analysis method without executing the suspect tools is analyzing the softwore on which the tool is dependent)

\*NIX

Unrm – extract only the deleted portions and significantly reduce the work lazarus has to do

iOS

John the Ripper (cracks iOS root and mobile passwords)

Froq (alwintroost.nl) (Viewing the tables of a database and exporting the portions of the database)

OmniOutliner 3 (omnigroup.com)(bundled with OSX 1.4 Tiger)(view plists)

Blackrai1n, Qwkpwn and so (jailbrake software)

Mdhelper (ericasadun.com) (parse data)

Oxygen Forensic Suite (has support to 3GS and iPad)

Cellebrite Universal Forensic Extraction Device (hardware device)

Katana lantern forensic

Susteen secure view

Skype analyser

HxD hex editor

SQLite database browser

iPod robot PlistEditor

iPhone Backup Extractor (supercrazyawesome.com) (works with latest iOS version)

JuicePhone (addpod.de) (tool that converts the backup files to a folder structure that an examiner can then look through and search for the artifacts)

GeoHunter (convert plist into viewable reports)

iXAM (images an entire iPhone, exploit digital rights management, jailbrake use)

hfsdebug (filexray.com) (forensic analysis tool)

MacForensicLab.com (examine HFS and HFSX)

HARDWARE-BASED

Keyloggers