



Useful Computer Forensics Tools
Updated: Jun 10, 2003

ProDiscover™

<http://www.techpathways.com>

Platforms: (Windows NT/2000)

ProDiscover™ is a disk forensics tool with the capabilities of many utilities into one simple to use, yet powerful product with an intuitive user interface. ProDiscover™ allows forensics examiners to collect, analyze, manage and report on computer disk evidence.

SafeBack

<http://www.forensics-intl.com>

Platforms: (DOS)

foensics-intl offers various command-line computer forensics tools. **NTI limits their sale** to government agencies, Fortune 1000 corporations, large law firms, large accounting firms, financial institutions, hospitals and law enforcement agencies.

SnapBack DatArrest

<http://www.cdp.com>

Platforms: (DOS)

The developers of the snapback software, Columbia Data Products, specifically state in their documentation that SnapBack DatArrest is a "data seizure" product and they actively advertise it to law enforcement officers as a forensics tool. Does not support disk-to-disk imaging

EnCase

<http://www.encase.com>

Platforms: (DOS, Windows NT, 2000)

Full featured windows based computer forensics analysis.

Byte Back

<http://www.toolsthatwork.com>

Platforms: (DOS)

This is a DOS based computer forensics and disk editor application.

Ilook

<http://www.ilook-forensics.org/>

Platforms: (Windows NT/2000)

Developed by a UK engineer in 1998-99. This application is very similar to ProDiscover. And EnCase. The application was sold to the US IRS Criminal Investigations Division and now only available to law enforcement agencies.

Forensics Tool Kit – System Analysis Tool

<http://www.accessdata.com/>

Platforms: (Windows)

Based on dtSearch FTK offers extensive search capabilities with a Forensics Spin.

The Coroners Toolkit (TCT)

<http://www.porcupine.org/forensics/tct.html>

Platforms: (Solaris, FreeBSD, RedHat, BSD/OS, OpenBSD, SunOS)

TCT is a collection of programs by Dan Farmer and Wietse Venema for a post-mortem analysis of a UNIX system after break-in.

MaresWare Suite

<http://www.maresware.com/maresware/forensic1.htm>

Platforms (DOS, UNIX)

A large group of command line forensics utilities.

PDA Seizure by Paraben

<http://www.paraben-forensics.com/>

Good Palm OS forensics tool

pdd

<http://www.atstake.com/research/tools/>

Platforms: Win 95/98/NT/2K (tested with Palm OS v1.0 to v3.5.2)

pdd allows forensic analysis of Palm OS platform devices. Source code is available for research and legal verification purposes.

TCTUTILs

<http://www.atstake.com/research/tools/>

Platforms: OpenBSD, Linux, Solaris

TCTUTILs is a package of tools that builds upon the popular forensics package, The Coroners Toolkit (TCT).

Autopsy Forensic Browser

<http://www.atstake.com/research/tools/>

Platforms: OpenBSD, Linux, Solaris

WinHex

<http://www.sf-soft.de/winhex/>

Platforms: (Windows NT/2000)

Disk editor for hard disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash memory cards, and more. FAT12, FAT16, FAT32, NTFS, CDFS

NDIC HashKeeper Database

<http://www.hashkeeper.org/>

HashKeeper is a database application of value primarily to those conducting forensic examinations of computers on a somewhat regular basis. The application uses the MD5 file signature algorithm to establish unique numeric identifiers (hash values) for known files and compares those known hash values against the hash values of unknown files on a seized computer system. Where those values match, the examiner can say, with statistical certainty, that the unknown files on the seized system have been authenticated and therefore do not need to be examined.

NIST Special Database 28

National Software Reference Library (NSRL)

<http://www.nist.gov/srd/nistsd28.htm>

Much the same as NDIC's hashkeeper database this is a more complete and subscription service (90.00 yr) for quarterly updates.

System Internals (various must-have utilities)

<http://www.sysinternals.com>

A large assortment of low-level Windows utilities including:

Filemon - This monitoring tool lets you see all file system activity in real-time. It works on all versions of WinNT/2K, Windows 9x/Me, Windows XP 64-bit Edition, and Linux.

Regmon - This monitoring tool lets you see all Registry activity in real-time. It works on all versions of WinNT/2K as well as Windows 9x/Me and full source is included.

Foundstone (Free command-line forensics tools)

<http://www.foundstone.com/rdlabs/tools.php?category=Forensic>

Link contains must-have command-line forensics including tool for viewing Windows NT/2000 Alternate Data Streams and a very useful application to TCP port mapper.

These tools were purchased from NTObjectives.

Frank Heyne Software

<http://www.heysoft.de/index.htm>

Produces a few useful windows NT/2000 event log and registry utilities.

Elcom Software – Password Recovery Software

<http://www.elcomsoft.com/prs.html>

Elcom Software provides a large array of password utility programs.

L0PhtCrack – Windows NT Password Cracker

<http://www.atstake.com/research/lc3/>

The most widely used Windows NT password cracker.

Word List

<http://www.outpost9.com/files/WordLists.html>

A good source for dictionary attack password cracking.

Man Hunt & Man Trap (Network forensics tools form Recourse Technologies)

<http://www.recourse.com/products/products.html>

A couple of good applications for network forensics.

dtSearch Desktop

<http://www.dtsearch.com/>

dtSearch Desktop is a powerful text searching tool.

OrionMagic

<http://www.orionsci.com/>

ORIONMagic enables the investigator to organize multiple search parameters into a matrix format resembling a spreadsheet, and perform massively parallel searches from a single command. This product as well as most computer forensic tools with advanced search capabilities is powered by dtSearch.

TRINIX

<http://trinix.sourceforge.net/>

Platforms: Linux

Trinix is a ramdisk-based Linux distribution that boots from a single floppy or CD-ROM, loads its packages from an HTTP/FTP server, a FAT/NTFS/ISO filesystem, or additional floppies. Trinix contains the latest versions of popular Open Source network security tools.

PLAC - Portable Linux Auditing CD

<http://sourceforge.net/projects/plac/>

Platforms: Linux

PLAC is a business card sized bootable cdrom running linux. It has network auditing, disk recovery, and forensic analysis tools. ISO will be available and scripts to roll your own CD.

F.I.R.E. (originally named Biatchux) – Bootable Forensics System on CD

<http://fire.dmzs.com/>

This is a very nice bootable forensics package and well worth the time to take a look.

Detective – Investigation Utility for System Events

<http://www.toolsthatwork.com/>

A software tool designed to allow for rapid investigation of the contents and activities of a Windows PC.

PowerControl Tools – MS Exchange Server Email Recovery/Forensics

<http://www.ontrack.com>

Power Control Tools allows the user to extract MS Exchange Server EDB/STM files from some(BackupExec, Native NT) backup tapes as well as live server. Additionally users can restore individual mailboxes or messages resulting from search to individual PST files.

ForMorph Message Converter by Fkeeps.com

<http://www.fkeeps.com>

Converts AOL Email. Creates nice html indexes

Email Examiner by Paraben Forensics Tools

<http://www.paraben-forensics.com/>

Good email extraction and examination tool

DBXtract – Extract Outlook Express files for analysis

<http://chattanooga.net/~scochran/DBXtract.htm>

DBXtract.exe extracts all mail and news messages from individual dbx files. After extracting the messages one can drag them from a Windows Explorer folder into an Outlook Express mail folder.

WM MailKeeper - Extract Outlook PST files for analysis

<http://www.wickett.net/>

Extracts Outlook mail from *.pst file to individual *.msg files.

UniAccess by ComAxis – Convert Mailbox formats from one to another

<http://www.comaxis.com/>

Cost effective and good export and conversion utility.

Metadata Assistant – Recover Microsoft Metadata from files

<http://www.payneconsulting.com/public/products/ProductDetail.asp?nProductID=21>

Allows the user to recover the large amount of metadata Microsoft places in office documents.

Windows Secret Explorer

<http://lastbit.com/wse/default.asp>

This system inspection/maintenance tool allows exploring Windows Protected Storage. Protected Storage includes form auto-fill data offered by Internet Explorer every time you enter something into a form on a web page; passwords to websites with limited access; MS Outlook account and identity passwords, dial-up passwords and other data stored by Microsoft in Protected Storage.

Office Recovery – File recovery

<http://www.officerecovery.com/>

Recover corrupted MS files

Conversions Plus

<http://www.dataviz.com>

Convert Mac file formats

Quick View Plus

<http://www.jasc.com/>

All purpose file format viewer.

PhotoRescue

<http://www.wildlifephoto.net/howto/photorescue.html>

Inexpensive, but basic digital camera photo recovery

DIT Data's PhotoRecovery

http://www.dtidata.com/photo_recovery.asp

Expensive, but comprehensive digital camera photo recovery

HTML2CD

<http://www.cd2html.de/>

Nice package to create indexes of CDs for discovery. Will index a set of files for CD and create graphic indexes.

Intelligent Computer Solutions, Inc. - Forensics Hardware

<http://www.ics-iq.com/>

This company sells many models of drive imaging solutions specifically for computer forensics.

Solitaire Forensics by Logicube – Forensics Hardware

<http://www.logicube.com/>

Hand held disk imaging hardware.

Portable Drive Service/Test/Dup by Corporate Systems – Forensics Hardware

<http://www.corpsys.com/>

Good low-cost SCSI/IDE duplication system with forensics mode.

DIBS, Inc.

<http://www.dibsusa.com/home.html?about/about>

Several hardware and software forensics products.

NoWrite IDE Write Blocker

<http://www.techpathways.com>

Very good IDE write blocker designed by long time industry insiders. Works with ProDiscover to allow non-destructive analysis of ATA disk using the Hardware Protected Area.

ACARD SCSI-to-IDE Write Blocking Bridge (AEC7720WP)

<http://www.microlandusa.com/>

Platforms: PC

ACARD AEC-7720UW Ultra Wide SCSI-to-IDE Bridge, Supports IDE devices attached to SCSI bus, with write blocked function.

Centurion Guard – Hardware Write Blocker (almost)

<http://www.centuriontech.com/centurionguard.htm>

The Centurion Guard® Hard Drive Protection Device protects your system by write protecting the hard drive at the physical level, similar to the way you write protect your floppy disks by setting the write protect tab. This system is not suitable for forensics work because it allows temporary writing to the disk for user changes, and then flushes the change area after reboot. Additionally this device requires software drivers to be installed on the target system.

CS Electronics – Drive Adapters

<http://www.scsi-cables.com/index.htm>

Good site for the many drive adapters you may need.

KeyGhost

<http://www.keyghost.com/products.htm>

KeyGhost is a hardware key stroke logging device.

F.R.E.D. (Forensic Recovery Evidence Device)

<http://www.digitalintel.com/fred.htm>

FRED is a highly integrated hardware/software platform which may be used both for the acquisition and analysis of computer based evidence.

ZERT by Netherlands Forensic Institute

<http://www.forensischinstituut.nl/>

ZERT is a hardware tool developed by NFI for recovery of passwords in PDA's

CGM Security Solutions – Tamper Proof Evidence Bags

<http://www.tamper.com/>

Good source for tamper proof evidence bags. (expensive)

Chief Supply – Tamper Proof Evidence Bags, Tape, Labels and more

<http://www.chiefsupply.com/fingerprint.phtml>

Better source for tamper proof evidence bags and tape (best prices)