

Tool	Use	
<a href="#">Active@ KillDisk</a>	Software that allows you to destroy all data on hard and floppy drives	
<a href="#">Active@ Partition Recovery Enterprise</a>	Ultimate data recovery tool set. In addition to DOS and Windows versions of the software, it contains downloadable Bootable Windows ISO Image	
<a href="#">Active@ UNDELETE - Data Recovery</a>	File undelete and data recovery program for NTFS & FAT32 / FAT volumes.	
<a href="#">Active@ UNERASER</a>	Hard drive recovery software for DOS and Windows (Console) that can recover deleted files and folders on FAT12, FAT16, FAT32 and NTFS file systems. It can even restore files from deleted and reformatted partitions.	
<a href="#">Advanced Access Password Recovery (ACPR)</a>	Recovers passwords for Microsoft Access files.	
<a href="#">Advanced ACE Password Recovery (ACEPR)</a>	Recovers passwords for most ACE & WinACE files.	
<a href="#">Advanced ACT Password Recovery (ACTPR)</a>	Recovers passwords for most ACT files.	
<a href="#">Advanced ARJ Password Recovery (AAPR)</a>	Recovers passwords for most ARJ & WinARJ files.	
<a href="#">Advanced Backup Password Recovery (ABPR)</a>	Recovers passwords for Microsoft Backup files	
<a href="#">Advanced CATaloguer</a>	Searches target media & organizes results.	
<a href="#">Advanced Disk Catalog (ADC)</a>	Creates a catalog of files & folders.	
<a href="#">Advanced Excel 2000 Password Recovery (AE2000PR)</a>	Recovers passwords for Microsoft Excel 2000 files.	
<a href="#">Advanced Instant Messengers Password Recovery (AIMPR)</a>	Recovers passwords for most widely used instant messenger applications.	
<a href="#">Advanced Internet Explorer Password Recovery (AIEPR)</a>	Recovers passwords for Microsoft Internet Explorer sites.	
<a href="#">Advanced Intuit Password Recovery (AINPR)</a>	Recovers passwords for files generated by Quicken, Quicken Lawyer, & QuickBooks applications.	
<a href="#">Advanced Lotus Password Recovery (ALPR)</a>	Recovers passwords for most files generated by Lotus, Organizer, WordPro, & 1-2-3 applications.	
<a href="#">Advanced Mailbox Password Recovery (AMBPR)</a>	Recovers passwords for most widely used e-mail client applications.	

<a href="#">Advanced Money Password Recovery (AMPR)</a>	Recovers passwords for Microsoft Money databases.	
<a href="#">Advanced Office XP Password Recovery (AOXPPR)</a>	Recovers passwords for most commonly used Microsoft software packages.	
<a href="#">Advanced Outlook Express Password Recovery (AOEPR)</a>	Recovers passwords for Microsoft Outlook Express Mail & newsgroups accounts.	
<a href="#">Advanced Outlook Password Recovery (AOLPR)</a>	Recovers passwords for Microsoft Outlook mail & newsgroups accounts.	
<a href="#">Advanced PDF Password Recovery (APDFPR)</a>	Recovers passwords for most PDF files.	
<a href="#">Advanced Project Password Recovery (APPR)</a>	Recovers passwords for Microsoft MSPROJECT files.	
<a href="#">Advanced RAR Password Recovery (ARPR)</a>	Recovers passwords for most RAR & WinRAR files.	
<a href="#">Advanced SQL Password Reco</a>	The password recovery tool accesses the master.mdf file directly, whether or not SQL Server is running or installed.	
<a href="#">Advanced VBA Password Recovery (AVPR)</a>	Recovers passwords for Microsoft Visual Basic files.	
<a href="#">Advanced Word 2000 Password Recovery (AW2000PR)</a>	Recovers passwords for Microsoft Word 2000 files.	
<a href="#">Advanced WordPerfect Office Password Recovery (AWOPR)</a>	Recovers passwords for most files generated by WordPerfect Office suite applications.	
<a href="#">AIDE</a>	Hashes files to ensure file integrity.	
<a href="#">Analyst's Notebook</a>	Presents data & correlations in a visual format.	
<a href="#">ANASIL LAN Analyzer</a>	Analyzes network packets & detects for sniffers.	
<a href="#">AOL Instant Messenger Password</a>	Decryption Tool Decrypts AOL IM passwords.	
<a href="#">Autopsy Forensic Browser</a>	Views & analyzes file systems. Designed to work in conjunction with the @stake Sleuth Kit (TASK).	
<a href="#">AVIPreview</a>	Previews partially downloaded video files.	Not forensically sound
<a href="#">Bates_No</a>	Applies the BATES number system to computer evidence.	Not forensically sound
<a href="#">BCWipe</a>	Disk Wiper (DoD – 7 pass wipe tool)	
<a href="#">BIEW</a>	Examines & views binary & hexadecimal code of files.	Not forensically sound
<a href="#">BinText</a>	Searches & extracts text from files.	

<a href="#">BlackBag MacQuisition Boot Dis</a>	A forensic acquisition tool used to safely and easily image Mac source drives using the source system.	
<a href="#">BlackBag Macintosh Forensic S</a>	Set of 19 tools that provide forensic examiners with a flexible, open environment within which to perform their analysis. The Suite is specifically designed for Mac OS X (version 10.1 & higher).	
<a href="#">BlackBag Technologies FireBox</a>	Ability to preview, analyze or image a suspect hard drive without compromising data.	
<a href="#">BOping</a>	Scans for Back Orifice.	Not forensically sound
<a href="#">BXDR</a>	Displays full sector count including "protected" areas.	
<a href="#">BringBack</a>	Data recovery for Windows™ & Linux (ext2) operating systems and digital images stored on memory cards, etc.	
<a href="#">Can Opener</a>	For browsing all types of files, including foreign files and files your PC can't open, and it's indispensable for recovering text from damaged files	Not forensically sound
<a href="#">Can Opener (Mac)</a>	For browsing all types of files, including foreign files and files your PC can't open, and it's indispensable for recovering text from damaged files	Not forensically sound
<a href="#">Carbonite</a>	Detects rootkits.	
<a href="#">CD-R Diagnostic</a>	Recovers data from corrupted CD storage media.	CD-R Diagnostic has been replaced by CD/DVD Diagnostic
<a href="#">CD-R Inspector</a>	Recovers, searches, & examines CD storage media.	
<a href="#">CDRoller</a>	Recovers data from damaged CD's.	Not forensically sound
<a href="#">CellIDEK</a>	Allows investigators with little knowledge or training in wireless technologies to immediately extract, review and utilize cell phone and PDA data on-scene.	
<a href="#">CellIDEK® TEK</a>		
<a href="#">CmosPwd</a>	Decrypts password stored in cmos used to access BIOS SETUP.	
<a href="#">Clone Card</a>		
<a href="#">CompuPic Pro</a>	Can help you manage, view and use all the multimedia content on your computer.	

<a href="#"><u>Computer COP Forensic</u></a>	Searches & examines a suspect's computer & restores deleted files.	Can search computers running all Windows operating systems since Windows 95 and including Windows XP. However, currently, the examiner's machine must be running Windows 95 or 98.
<a href="#"><u>Computer COP Professional</u></a>	Searches for data, recovers deleted files, & reports results.	
<a href="#"><u>Conversions Plus</u></a>	Converts, opens, & views a file regardless of file format.	
<a href="#"><u>Cookie View</u></a>	Decodes Internet cookie files.	
<a href="#"><u>CopyQM</u></a>	Makes duplicate copies of floppy diskettes.	Not forensically sound
<a href="#"><u>CRCMD5</u></a>	Performs file to file comparisons.	
<a href="#"><u>CSC Dup-It</u></a>	Creates a precise duplicate of a CD-ROM.	Copy entire IDE hard disk images on SCSI drives or vice-versa.
<a href="#"><u>CSC Pro Drive</u></a>	Creates a precise duplicate of a hard drive.	
<a href="#"><u>CSC Ultra Performance 8 Drive IDE Duplicator</u></a>	Creates a precise duplicate of a hard drive.	
<a href="#"><u>Dateconv</u></a>	In many forensic and operating system applications there is a long number used to express a date/time in seconds elapsed since a given reference date(ex., 9123456789). <b>Dateconv</b> converts it to the conventional format for writing a date, i.e., 00-00-0000.	
<a href="#"><u>DataLifter</u></a>	Recovers data, extracts files, & reports results.	
<a href="#"><u>Davory</u></a>	Recovers data from formatted or damaged drives.	
<a href="#"><u>DBXtend</u></a>	Extracts e-mails from dbx files for viewing in Outlook Express.	DBXtend has been superseded by the new program OEX
<a href="#"><u>DBXtract</u></a>	Extracts e-mails from dbx files for viewing in Outlook Express.	DBXtend has been superseded by DBXpress
<a href="#"><u>DDoSPing</u></a>	Scans & detects common DDoS programs.	Not forensically sound

<a href="#">DecExt</a>	Decode Internet email attachments simply by right-clicking on a saved message file from Explorer and selecting Decode from the menu. Decode Shell Extension is for 32 bit Windows. It will not work on x64 platforms.	
<a href="#">Decoder</a>	Converts time values stored in decimal or hexadecimal values into date & time values.	Not forensically sound
<a href="#">Decode - Forensic Date/Time De</a>	Decode the various date/time values found embedded within binary and other file types.	
<a href="#">Decryption Collection</a>	Advanced password recovery suite.	
<a href="#">Detective</a>	Searches content, extracts data, views images, displays actions, & creates reports.	Not forensically sound
<a href="#">DETS</a>	Ensures evidence integrity through hashing & secure time stamping of evidence.	*
<a href="#">DIBS Analyzer</a>		
<a href="#">DIBS Forensic Workstation</a>	Computer workstation designed for forensic analysis.	Replaced with DIBS Advanced Forensic Workstation
<a href="#">DIBS Mobile Forensic Workstation</a>	Computer laptop designed for forensic analysis on site.	
<a href="#">DIBS Mycroft V3</a>	Searches suspect computers for forensic evidence.	
<a href="#">DIBS PERU</a>	Creates forensic images of hard drives.	
<a href="#">DIBS PIU</a>	Used in conjunction with "optical cartridges" to work with forensic evidence.	
<a href="#">DIBS RAID</a>	Images suspect hard drive.	
<a href="#">DirectorySnoop</a>	Searches, retrieves, & recovers data from hard drives & other storage media.	Not forensically sound
<a href="#">Disk_crc</a>	Reads the contents of a disk, floppy or hard disk and produces a 32 bit CRC, 128 bit MD5, or 160 bit SHA representing the hash of that disk. This value can be used later as a reference to verify that the contents of the disk have/have not been changed.	

<a href="#">Disk image</a>	Designed to make a copy or copies of suspect floppy disks onto a hard drive for analysis. It can also be used to make a copy of a disk onto a hard drive which can later be restored to as many floppies as necessary.	
<a href="#">Diskcat</a>	"Disk cataloguer.' It creates a listing (catalog) of all files and/or directories on a hard or floppy disk.	
<a href="#">Disk Search 32</a>	Note: DiskSearch 32 has been replaced by TextSearch NT which deals with all Microsoft operating systems.	
<a href="#">Disk Search Pro</a>	DiskSearch Pro has been replaced with NTI's TextSearch NT which has been enhanced for speed and it deals with all MicroSoft operating system searches. All DiskSearch Pro users can easily upgrade to this new forensic search utility.	
<a href="#">Diskjockey2000</a>	View over 50 popular file types-- including graphics, spreadsheet, word processing, database, audio, video, HTML, ASCII, and RTF formats.	
<a href="#">DiskSig</a>	DiskSig Pro replaces and upgrades NTI's popular DiskSig forensic utility.	
<a href="#">Distributed Network Attack DNA</a>	Recovering password protected files	
<a href="#">DRAC 1000</a>	User specified unit designed to extract & analyze evidence from suspect machines & storage media.	
<a href="#">DRAC 3000</a>	Fully configured unit designed to extract & analyze evidence from suspect machines & storage media.	
<a href="#">DriveLook</a>	riveLook scans a drive or a partition of a drive for text strings and stores these in a table.	
<a href="#">DriveSpy</a>	Extracts, examines, images, & protects data.	
<a href="#">DT Search</a>	The dtSearch product line can instantly search terabytes of text across a desktop, network, Internet or Intranet site.	

<a href="#">Dual Drive External Drive Imaging Station</a>	Performs imaging of hard drives.	
<a href="#">DumpAutoComplete v0.7</a>	This application will search for the default Firefox profile of the user who runs the tool and dump the AutoComplete cache in XML format to standard output.	
<a href="#">EasyRecovery DataRecovery</a>	Recovers damaged or deleted data.	Not forensically sound
<a href="#">Echo Plus</a>	Single-target, drive-to-drive duplicator for IDE, UDMA, & SATA drives. (2.5", 1.8", and compact flash drives - optional.)	
<a href="#">ElcomSoft Distributed Password</a>	Recover the most complex passwords and strong encryption keys in realistic timeframes.	
<a href="#">ElcomSoft Password Recovery</a>	unprotect disks and systems and decrypt files and documents protected with popular applications.	
<a href="#">Email Examiner</a>	Recovers active or deleted e-mails	
<a href="#">EnCase</a>	Acquire data in a forensically sound manner	
<a href="#">Evidor</a>	Searches data via keywords, examines all files, & recovers deleted data.	
<a href="#">Expert Witness for Macintosh</a>	Images, analyzes, & acquires data on a Macintosh system.	
<a href="#">F.I.R.E.</a>	Performs data recovery & analysis.	
<a href="#">F.R.E.D.</a>	Examines & acquires digital evidence.	
<a href="#">F.R.E.D. Sr</a>	Examines & acquires digital evidence.	
<a href="#">F.R.E.D.C.</a>	Examine, acquire, & store digital evidence.	
<a href="#">F.R.E.D.D.I.E.</a>	Examines & acquires digital evidence.	
<a href="#">FacTracker</a>	Searches, images, recovers data & reports results.	
<a href="#">FastBloc</a>	Allows the investigator to conduct previews and acquisitions for desktop and laptop IDE hard drives, quickly, in Windows, without altering data on the suspect hard drive.	
<a href="#">FCCU GNU/Linux boot CD 10.0</a>	This CD is based on KNOPPIX. It is a remaster made for the computer forensic investigator. Its main purpose is to create images copies of devices before analysis.	

<a href="#">Favourite File *.URL Viewer</a>	Decodes *.url "favorites" files.	
<a href="#">FCrackZip</a>	Fast zip password cracker	
<a href="#">FileList Pro</a>	Documents file information from hard drive & storage media.	
<a href="#">Filerecovery for Windows</a>	Searches for & recovers deleted files.	Not forensically sound
<a href="#">Filewatch</a>	Detects changes made to critical files.	
<a href="#">Filter_I</a>	Seeks & filters out specific information from masses of computer data.	
<a href="#">FINALeMAIL</a>	Recover the email database file and locates lost emails that do not have data location information associated with them.	
<a href="#">FIREBLOCK</a>	Blocks write access to IDE drive & provides access to Firewire bus.	
<a href="#">FIRECHIEF</a>	Allows imaging of an IDE drive to another IDE drive over a Firewire bus.	
<a href="#">FireFly (available in IDE and SA</a>	Hardware based write blocker which will allow an IDE or SATA hard drive to be connected to a IEEE 1394a or 1394b compliant FireWire device chain.	
<a href="#">Firewire Card IDE Drive Bay</a>	Firewire 1394 based Read-only IDE drive bay.	
<a href="#">Firewire Card Second Generation</a>	Hardware component to incorporate Firewire 1394 technology.	
<a href="#">Foremost</a>	A linux tool for conducting forensic examinations. Reads through a file, such as a dd image file or a disk partition and extracts file	
<a href="#">Forensic Air-Lite</a>	Portable computer forensic workstation.	
<a href="#">Forensic Dossier</a>	Hand held. Captures data from one or two sources drives (SATA/IDE) to one or two estination drives.	
<a href="#">Forensic Duplicator</a>	Provides forensic (write-protected source drive) disk-to-file or disk-to-disk duplication for IDE to IDE, IDE to SATA, SATA to SATA and SATA to IDE hard disk drives.	
<a href="#">Forensic Replicator</a>	Images & encrypts digital data from hard drives & floppy diskettes.	

<a href="#">The Forensic Server Project (FSP)</a>	Proof of concept tool for retrieving volatile (and some non-volatile) data from potentially compromised systems. The FSP consists of several Perl scripts and third-party utilities.	
<a href="#">Forensic SF-5000u</a>	Images suspect hard drive bit-by-bit.	Replaced with the Forensic Talon
<a href="#">Forensic Steel Towers</a>	Hardware designed specifically for digital forensic investigations.	
<a href="#">Forensic Tool Kit</a>	Stand-alone forensic investigations.	
<a href="#">Forensic Toolkit v. 2.0</a>	Lists file information & locates hidden files & data.	
<a href="#">Forensic Tower</a>	Hardware designed specifically for digital forensic investigations.	
<a href="#">Forensic Quest</a>	Hand-held forensic data acquisition device featuring MD5 authentication, DD imaging, native write-protect and localized multi-language user interface.	
<a href="#">Forensic Utility Suite</a>	Recover & restore deleted data including digital images.	
<a href="#">FPipe</a>	Source port forwarder/redirector. It can create a TCP or UDP stream with a source port of your choice.	
<a href="#">fport</a>	Examines open TCP & UDP ports.	
<a href="#">FSCrack</a>	Graphical user interface (GUI) for access to most of JtR's functions.	
<a href="#">Galleta v1.0</a>	Will parse the information in a Cookie file and output the results in a field delimited manner so that it may be imported into your favorite spreadsheet program.	
<a href="#">GetDataBack</a>	Do-it-yourself Data Recovery Software	
<a href="#">GetFree</a>	Used to capture all of the unallocated file space on DOS, Windows, Windows 95 and Windows 98-based computer systems.	
<a href="#">GetSlack</a>	Is used to capture all of the file slack contained on a logical hard disk drive or floppy diskette on a DOS, Windows, Windows 95 and/or Windows 98 computer system.	
<a href="#">GetTime</a>	Documents system data & time information from suspect machine.	

<a href="#">Graphics Image File Extractor</a>	Locate & extract graphic image files.	
<a href="#">GPStamp</a>	Produces a verified fix on the location, time, and date of the data capture.	
<a href="#">Grok-NTFS</a>	Grok-NTFS will accept all types of "forensic" images (Expert Witness / EnCase E01, FTK Imager, SMART, SAW, etc.) as well as dd images and VMWare disk images.	
<a href="#">GSpot</a>	Identifies the codec used on a video/audio file.	
<a href="#">HardCopy 3</a>	Duplicates the source at up to 7.5 GB/min., makes a 2nd copy, and computes SHA256 verify, all simultaneously, with no slow down in imaging speed.	
<a href="#">Helix3</a>	Fast and powerful live CD for your live forensics, incident response and e-discovery requirements. <a href="http://www.e-fense.com/products.php">www.e-fense.com/products.php</a>	
<a href="#">Helix3 Enterprise</a>	Software solution integrated into your network giving you visibility across your entire infrastructure revealing malicious activities such as Internet abuse, data sharing and harassment. <a href="http://www.e-fense.com/h3-enterprise.php">www.e-fense.com/h3-enterprise.php</a>	
<a href="#">HashKeeper</a>	Used to expedite the analysis of electronic media. HashKeeper is a software application that quickly eliminates known operating system files and focuses on electronic files created by the user/subject of the investigation.	
<a href="#">Hex Workshop</a>	Hex Workshop combines advanced binary editing and data interpretation with the ease and flexibility of a modern word processor.	
<a href="#">IDA Pro</a>	Disassembler and Debugger is an interactive, programmable, extendible, multi-processor disassembler hosted on the Windows platform.	
<a href="#">iLook</a>	Forensic analysis tool designed to examine digital media from seized computer systems and/or other digital media.	
<a href="#">Image</a>	Images floppy disks.	

<a href="#">NTI's Image Buster Suite</a>		
<a href="#">Image MASter Solo 2 Forensic Systems</a>	Images hard drives & disk media.	ImageMASter Solo-3 Forensic Kit replaced Solo 2
<a href="#">ImageCast</a>	Hard drive duplication tool.	
<a href="#">ImageMasster</a>	ImageMASter Solo-3 Forensic Kit replaced ImageMasster	
<a href="#">InCtrl5</a>	Monitors your system files when new applications are installed.	
<a href="#">IsoBuster</a>	Rescue lost files from a bad or trashed CD or DVD or a Blu Ray disc (e.g. BD or HD DVD)	
<a href="#">ISPGP</a>	Intended to search an entire disk, or just specified directories, for files that are PGP related files.	
<a href="#">Live Response</a>	USB key for First Responders, Investigators and IT Security Professionals to collect the live volatile data which will be lost once the computer system is shutdown	
<a href="#">LADS</a>	Lists all alternate data streams of an NTFS directory.	
<a href="#">LIMS-plus</a>	Performs case management.	
<a href="#">Lockdown v2</a>	Write-blocker that combines speed and portability to allow IDE and SATA media to be acquired quickly and safely.	
<a href="#">Mac Marshal</a>	Macintosh Evidence Gathering and Analysis tool suite for investigators to assess and collect data on dual-boot Apple Mac OS X systems	
<a href="#">Mailbag Assistant</a>	This program provides tools for searching, organizing, analyzing and archiving your e-mail messages.	
<a href="#">Maresware: Computer Forensics</a>	Images, examines, searches, & protects digital data.	
<a href="#">Maresware: Linux Forensics</a>	Examines, searches, & protects digital data.	
<a href="#">Maresware: The Suite</a>	Compilation of tools for analysis, examination, imaging, & data protection.	
<a href="#">MBXtract</a>	Extracts all mail & news messages from individual mbx files.	
<a href="#">MD5 Hash</a>	Generates a MD5 hash value for files.	

<a href="#">MD5Sum</a>	Win 95/98/NT program that generates and checks MD5 checksums.	
<a href="#">MediaMerge for PC</a>	Retrieves data files from backup tapes.	
<a href="#">MediaMerge for UNIX</a>	Retrieves data files from backup tapes.	
<a href="#">Microsoft Access Password Decoder</a>	Retrieves master password for Microsoft Access files.	
<a href="#">MicroSATA Adapter</a>	Used to adapt a SATA interface to a Micro SATA drive.	
<a href="#">MIL-CAS</a>	Indexes, scans, & analyzes telephone communications.	
<a href="#">MOBILedit!</a>	Extracts all content and generates a forensic report ready for courtroom presentation.	
<a href="#">M-Sweep Pro</a>	Erases data completely from unallocated & free space on a hard drive.	
<a href="#">MultiDrive Adapter</a>	Allows 2.5 inch, 1.8 inch PIN connector and 1.8 inch ZIF connector IDE hard drives to be connected to a write blocker or standard 40 pin IDE connector.	
<a href="#">Net Analysis</a>	Searches, filters, rebuilds, & extracts evidence from Internet history data.	
<a href="#">Net Threat Analyzer</a>	Analyzes Internet activity.	
<a href="#">Net Witness</a>	Records network traffic & checks for attacks based on the normal activity of the network.	
<a href="#">NetDetector</a>	Sorts & records network traffic.	
<a href="#">Netstat Logger</a>	Logs current TCP connections.	
<a href="#">Network Flight Recorder</a>	Monitors network usage for both internal & external attacks.	
<a href="#">No Write</a>	Protect digital evidence from unintentional writes.	
<a href="#">Norton Disk Edit</a>	Norton Diskedit is a hexeditor for logical and physical disk drives on all Windows filesystems.	
<a href="#">Norton Ghost</a>	Creates full system and file backups	
<a href="#">Norton Ghost 2003</a>	Images hard drives.	
<a href="#">NTLast</a>	Examines network activity.	
<a href="#">NT SAMs</a>	Linux Boot Disk, that accesses the Windows Partition then Resets Account Passwords by exploiting that SAM File	
<a href="#">Office Recovery</a>	Restores files for several Microsoft Office applications.	Now Office Recovery 2009

<a href="#">Omniquad Detective</a>	Can reconstruct the usage history of the analyzed workstation, presenting you with a log of past actions for inspection	
<a href="#">OmniClone 2 Xi</a>	Supports UDMA-5 transfer speeds for cloning IDE, EIDE, UDMA, & SATA drives at up to 3.5 GB/min.	
<a href="#">OmniClone 5Xi</a>	5 target, IDE, EIDE, UDMA, SATA hard drive to hard drive duplication.	
<a href="#">OmniClone 10Xi</a>	10 target, IDE, EIDE, UDMA, SATA hard drive to hard drive duplication.	
<a href="#">OmniSAS</a>	OmniSAS is Windows Vista compatible and features advanced software that provides a variety of cloning modes.	
<a href="#">OmniSCSI</a>	Duplicating a SCSI master drive to one SCSI target at speeds exceeding 2.3 GB/min.	
<a href="#">OmniSCSI 4</a>	Self-contained IDE/SCSI duplication system capable of duplicating an IDE or SCSI master drive to 2 or 4 SCSI target drives at speeds that may exceed 1.2 GB/min.	
<a href="#">OmniWipe</a>	Quickly wipe drives prior to using them for data capturing purposes.	
<a href="#">OnLineDFS</a>	OnLine Digital Forensic Suite- aids investigators and administrators with the forensic task of system assessment following a suspected intrusion and the potential compromise of a host.	
<a href="#">OrionMagic</a>	Search, analyze, & organize through mass amounts of information.	
<a href="#">Oxygen Forensic Suite 2</a>	mobile forensic software	
<a href="#">Pasco v1.0</a>	Pasco will parse the information in an index.dat file and output the results in a field delimited manner so that it may be imported into your favorite spreadsheet program.	
<a href="#">PatchIt v2.0</a>	A file byte-patching utility.	
<a href="#">P2 Commander</a>	Digital forensic tool designed to handle more data, more efficiently.	
<a href="#">P2 eXplorer v1.0</a>	Mount your forensic image and explore it as though it were a drive on your machine while preserving the forensic nature of your evidence.	

<a href="#">P2P Marshal</a>	Automatically gather, in a forensically sound way, all the files related to P2P usage on a target computer.	
<a href="#">PART</a>	Allows viewing & management of partition information.	
<a href="#">Passware Kit</a>	Can recover passwords for opening applications, for write reservations, and for workbooks, worksheets, templates, documents, personal folders and files, form designs, databases, and user accounts.	
<a href="#">Password Recovery Toolkit</a>		
<a href="#">Password Recovery Toolkit Professional</a>	Recovers passwords from various Windows applications & provides utilities to bypass Novell & NT system passwords.	
<a href="#">PDA Seizure</a>	Replaced with Paraben's Device Seizure	
<a href="#">PDBLOCK</a>	Protects digital evidence by preventing unintentional writes to the hard drive.	
<a href="#">PhoneBase 2</a>	Mobile phone analysis system with the capability to deliver a full report on the contents of SIM cards and phone memories, typically lists of phone numbers and associated names, recently made calls and text messages	
<a href="#">PhotoRecovery</a>	Retrieves & restores erased digital images.	
<a href="#">PhotoRescue</a>	Able to recover after other recovery methods have further corrupted the cards.	
<a href="#">Pilot-Link</a>	Used to get contents of ROM and RAM from Palms. Additionally <i>pilot-xfer</i> allows acquisition	
<a href="#">PkCrack</a>	Breaks PKZip encryption.	
<a href="#">PLAC</a>	Images & recovers data & provides network analysis mechanisms.	
<a href="#">Portable Forensic Lab® (PFL)</a>	portable computer forensic field lab. The PFL (in its fully bundled package).	
<a href="#">ProDiscover™ DFT</a>	Image hard drives, search data, generate reports, & verify evidence integrity.	
<a href="#">QuickView Plus</a>	Access & view e-mails & documents.	

<a href="#">RAID I/O Adapter</a>	Enables the Forensic Talon® to capture a Suspect RAID drive pair directly to 1 Destination drive*, and 1 Suspect drive to 2 Destination drives.	
<a href="#">Rainbow Table</a>	Allow an examiner to crack the files quickly compared to a standalone computer or even a standard twenty five machine Distributed Network Attack (DNA) system.	
<a href="#">Rack-A-TACC</a>	Is a rack mounted network appliance that leverages multiple Tableau TACC1441 accelerators to recover passwords from encrypted files using dictionary and brute-force attack methods.	
<a href="#">Recover It All</a>	Recovers data from damaged or formatted hard drives.	
<a href="#">ReviveR</a>	Recover deleted files even if the files were deleted from the recycle bin, or if applications (which normally bypass the recycle bin) deleted the files.	
<a href="#">Rifiuti v1.0</a>	Rifiuti will parse the information in an INFO2 file and output the results in a field delimited manner so that it may be imported into your favorite spreadsheet program.	
<a href="#">R-Mail</a>	Recovers accidentally deleted Outlook e-mail messages, contacts, notes, tasks and other items, and repairs damaged Outlook data files (*.pst) files where Outlook stores folders with the data.	
<a href="#">Robocopy</a>	Copies files & folders.	
<a href="#">R-Undelete</a>	Recovers files on any local disks recognized by the software.	
<a href="#">SafeBack</a>	Images hard drives & verifies evidence integrity.	
<a href="#">SATA to IDE Adapter</a>	Can be used to adapt a SATA host interface to an IDE drive.	
<a href="#">SAW</a>	Smart Acquisition Workshop (SAW), is a Data Acquisition and case management framework optimized to deliver outstanding performance and benefits in large, complex data forensic investigations.	

<a href="#">ScanLine</a>	Scans TCP & UDP ports.	
<a href="#">SCSIBLOCK</a>	Blocks write access to IDE drive.	
<a href="#">Seized</a>	Used to aid in the preservation of computer evidence.	
<a href="#">Serial ATA (SATA)</a>	Instead of the traditional 40 pin connectors and ribbon cables, the new serial ATA drives utilize a thin round cable and a very small connector (somewhat resembling a USB cable).	
<a href="#">Shadow 2</a>	Enables an investigator to boot and view a suspect's system on site, without threat of altering the evidence on the boot drive.	
<a href="#">ShoWin</a>	Displays Windows passwords.	
<a href="#">Silent Runner</a>	Monitors & analyzes network traffic.	
<a href="#">SIMCon</a>	Forensic imaging and analysis of SIM cards, including recovery of deleted items. Free to Law Enforcement	
<a href="#">SIM Manager</a>	Recovers phone numbers, SMS messages from a range of phones	
<a href="#">SIM Scan</a>	Tool that allows investigation of SIM cards – freeware.	
<a href="#">Single Read-only Drive Imaging Station</a>	Protects digital evidence against writes to an imaged drive.	
<a href="#">SMART</a>	Images media, extracts, & analyzes data.	
<a href="#">SMART Linux</a>	A live CD distribution of Linux designed for Data Forensics and Incident Response.	
<a href="#">Smart Mount</a>	Allows you to mount filesystems contained in logical and physical disk image files. It automatically detects the partitions and filesystems in your images.	
<a href="#">Snap View</a>	Enables quick viewing & examination of various file formats.	
<a href="#">Snapback</a>	Server-based backup and restore program for Windows servers that features full open file management, remote administration and backup scheduling.	Now called SnapBack Exact
<a href="#">SnapBack DatArrest</a>	Images server or PC hard drives.	Now called SnapBack Exact
<a href="#">Snort</a>	Sorts & records network traffic. Performs IDS functions.	

<a href="#">Solitaire Forensic Unit</a>	Clone from target to master or master to target through an IDE interface or the parallel port connection.	
<a href="#">stegdetect</a>	Detects steganography in JPEG images.	
<a href="#">Stego Detect</a>	Detects steganography programs installed on a computer.	Now part of Stego Suite
<a href="#">Steghide</a>	Steganography program that is able to hide data in various kinds of image- and audio-files. The color-respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests.	
<a href="#">Stego Watch</a>	Detects steganography in images including JPEG, GIF, & BMP files.	Now part of Stego Suite
<a href="#">STRSRCH</a>	The program is designed to do multiple string searches of files contained on a disk	
<a href="#">SuperSonix</a>	Hard disk drive duplicator, the second generation of Logicube's popular Sonix is a compact and portable cloning solution with blazing cloning speeds approaching 6GB/min	
<a href="#">Suspect Presenter</a>	Creates a web page to view suspect information visually.	
<a href="#">TADILdecoder</a>	Software application that allows network administrators to configure, monitor, manage and debug one or more Joint Tactical Information Distribution System (JTIDS) networks (also known as Link-16 networks).	
<a href="#">Task</a>	Performs extraction & analysis of Microsoft & UNIX files & data.	Now called "Slueth Kit"
<a href="#">TASK / Autopsy</a>	Now called "Slueth Kit"	
<a href="#">Tcpflow</a>	Program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging.	

<a href="#">Tcpttrace</a>	Tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including Tcptdump, snoop, etherpeek, HP Net Metrix, and WinDump.	
<a href="#">TeleDisk</a>	Creates images of floppy diskettes.	TeleDisk is no longer made available for sale. NTI recommends the use of either CopyQM or AnaDisk when disks need to be copied, shared or duplicated.
<a href="#">Text Search Plus</a>	This software is used to quickly search hard disk drives, zip disks and floppy diskettes for key words or specific patterns of text. It operates at either a logical or physical level at the option of the user	
<a href="#">Text2Hex</a>	Converts ASCII text to hexadecimal values.	
<a href="#">The Coroner's Toolkit (TCT)</a>	Collects & examines data.	
<a href="#">ThumbsPlus</a>	Is a highly customizable image database with thumbnails and batch editing. It makes it easy to catalog, organize, locate and maintain all of your graphics, multimedia and font files.	
<a href="#">Time Lock</a>	Incorporates secure digital time stamps into Microsoft Word Documents.	
<a href="#">Time Lock Biometric</a>	Incorporates biometrics & secure digital time stamps into Microsoft Word Documents.	
<a href="#">Trinux</a>	A collection of open source network security tools.	
<a href="#">Trout</a>	Performs Traceroute & Whois searches.	
<a href="#">TULP2G</a>	A .NET based forensic software framework for extracting and decoding data stored in electronic devices.	
<a href="#">UltraBlock eSATA IDE-SATA Kit</a>	Is used to acquire data from an IDE or SATA hard drive in a forensically sound write-protected environment.	
<a href="#">UltraBlock SCSI</a>	Used to acquire data from a SCSI hard drive in a forensically sound write-protected environment.	

<a href="#">UltraBlock Forensic USB Write E</a>	Works with USB thumb drives, external USB disk drives, even USB-based cameras with card-reader capability.	
<a href="#">UltraBlock Forensic Card Reader</a>	The UltraBlock FCR can work either as a write blocker (Read Only mode) or as a read writable device. This function is set by a switch on the side of the Ultra Block.	
<a href="#">UndeleteSMS</a>	Recover deleted SMS messages from a GSM SIM card.	
<a href="#">Uni Access</a>	E-mail conversion utility.	Now called Transend Migrator
<a href="#">USB Adapters</a>	The USB Adapter is the ideal option for the Solitaire Turbo or Solitaire Turbo with integrated keypad. The USB adapter allows for cloning and drive management directly through the USB (1.1 or 2.0) port on a PC or laptop. Capable of cloning at speeds between 500 and 700 MB/min. through USB 2.0 port, the USB Adapter features a 20 pin connector that attaches to the Solitaire Turbo or Solitaire Turbo with integrated keypad.	
<a href="#">USB Omniport</a>	Two versions are available; Write Protected (ideal for Forensic work) and Non-Write Protected (for IT applications). Capture and deploy data to or from most USB Flash drives	
<a href="#">VEDIT</a>	Edits, translates and sorts any text, data, binary (hex) or EBCDIC file	
<a href="#">Vision</a>	Examines open TCP & UDP ports.	
<a href="#">Vital Data FoRK v1.0.0</a>	For use as a forensic imaging and previewing tool. <b>forensicIT.com.au</b>	
<a href="#">WipeDrive Pro</a>	Completely erase a damaged operating system with possible hidden viruses.	
<a href="#">WinHex</a>	Inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems	
<a href="#">WN MailKeeper</a>	Creates a readable e-mail archive on CD or other external media.	

<a href="#">WritePROtect</a>	Supports IDE hard drive protection from alteration (either inadvertent or malicious), either through a direct cable connection, or through a USB connection.	
<a href="#">YServer Parse</a>	Translates cryptic Yahoo Messenger session logged data.	
<a href="#">ZAR 8.3</a>	Digital Image Recovery	
<a href="#">ZDelete</a>	Is a cleanup and internet eraser utility that completely erases selected files, drives, folders, Internet Cache, Internet History, Internet Cookies, temporary files, etc. without any possibility of data recovery.	