Appendix I

List of Forensic Equipment and Forensic Software Tools

Introduction

Chapters 7 and 8 provide detailed discussion on the topic of computer forensics. This appendix presents a compiled list of tools/equipment/software used to carry out forensics work. The forensics tool list presented here (Table I.1) is an addendum to the information provided in Table 7.11 in Chapter 7, Tables 8.3 and 8.4 in Chapter 8. Antiforensics tool list is also presented in Table I.2 because antiforensics is explained in Chapter 7 (Section 7.19).

In the tables that follow, we have presented the name of the vendor (where available), product name and the websites. Please note that the links listed in the tables are as they were available at the time of accessing them. There could be subsequent changes or some links may be withdrawn and therefore it is reader's responsibility to obtain the latest or active list, should they be in need of finding information on the tools/software/equipment.

License information is provided where available. We have not provided the price information because prices can be subject to change dynamically. It is best to contact the vendor using the links provided. We do not claim that the tools listed in this appendix are the only tools available. There could be many other tools as well; we have only presented the most dominant ones that are known to exist in the market. We also do not vouch for the features of the tools presented here; the features mentioned about the listed tools are the claims of tool vendors. It is up to the users to contact the vendor to validate those claims. Also readers/users should visit the website provided in the tables to find out the latest/multiple versions of those tools that may exist.

The trade names and company products listed in this appendix are not necessarily intended to imply recommendation or endorsement by authors, nor does it imply that the products are necessarily the best available for the purpose. Users/readers will need to apply their own judgment and/or seek advice from qualified forensics expert depending on their context for the investigation for which any of the tools listed here are to be used. It is important to seek a legal opinion as well depending on your usage circumstances because evidence acceptance in courts is important; some tools are court-approved and some are not.

Computer Forensics Tools (Software Products)

Table I.1 presents the list of software tools that we have compiled for users' easy reference. While going for any of the lists listed in the table, keep in mind the caveats mentioned above.

Table I.1 Forensic Tools (Software Products)

Sr. No.	*Vendor/Creator /Designer*	*Product(s)*	*Remarks*	*Websites*
1.	Guidance Software	EnCase Forensic EnCase Enterprise Forensic Tool Kit	EnCase version 6.17 is a multipurpose forensics tool, widely accepted in court. It is a fully integrated forensics application for Windows. License is commercial and works on Windows Platform.	http://www.guidancesoftware.com/
2.	Decision Group Inc. (Taiwan)	E-Detective	It is a real-time network forensics tool and lawful interception system	http://www.edecision4u.com/E-DETECTIVE.html
		HTTPS/SSL Network Packet Forensics Device	It is a real-time forensics tool and lawful interception system	http://www.edecision4u.com/HTTPS-SSL.html
		VOIP-DETECTIVE	VoIP and real-time forensics tool and lawful interception system	http://www.edecision4u.com/VOIP-DETECTIVE.html http://www.edecision4u.com/NIT.html http://www.digi-forensics.com/Document/VOIP_INTERCEPT_2009.pdf
		Network Investigation Toolkit (NIT)	Network Investigation Toolkit (NIT) is a Wireless and Ethernet real-time packet reconstruction software with the device. The tool is designed for interested groups such as Police, Military, Criminal Investigation Agencies, National Security Agencies, Cybersecurity Agencies, Counter Terrorism Department, Forensics Investigator, etc. to conduct network-based forensics investigation to know whether it is on a wired or wireless LAN networks. NIT is a portable unit (laptop-based) with comprehensive network forensics features which can be carried at any location for network-based investigation task.	http://www.edecision4u.com/data/Network_Investigation_Tool.pdf http://www.decision-groups.com/data/NIT_Brochure_2010.pdf

			NIT can be used to intercept targeted networks or users to collect the necessary evidences and trace out the source of communication.	
3.	DFLabs	PTK Forensics	This is a non-free, open source, commercial GUI for digital forensics tool. The GUI for Sleuth Kit (TSK)	http://ptk.dflabs.com/
4.	Sleuthkit	The Sleuth Kit	A library of tools for both Unix and Windows Licenses – IPL, CPL and GPL Brian Carrier is the Original Author	http://www.sleuthkit.org/
5.	Microsoft	COFEE (Computer Online Forensics Evidence Extractor) – refer to Box 7.1 of Chapter 7	A suite of tools for Windows developed by Microsoft, only available to law enforcement. Available under Microsoft Proprietary license. Developed by Anthony Fung, a former Hong Kong police officer.	http://msforums.ph/forums/t/48034.aspx http://en.wikipedia.org/wiki/Computer_Online_Forensic_Evidence_Extractor
6.	---	Categoriser 4 Pictures	It is a free tool that works on Windows platform. Available for law enforcement.	http://www.cyberagentsinc.com/Forensic%20Accessories%20and%20Software/C4POverview.pdf
7.	National Drug Intelligence Center (NDIC)	HashKeeper	Created by the National Drug Intelligence Center (NDIC), an agency of the United States Department of Justice in 1996. Available free and works on Windows platform. Database application for storing file hash signatures. Available free of charge.	http://tech.groups.yahoo.com/group/hashkeeper/ http://viaforensics.com/computer-forensic-ediscovery-glossary/what-is-hashkeeper.html

8.	SunBlock Systems	BitFlare	BitFlare®, a product of SunBlock Systems, allows anyone comfortable with computers to turn a suspicious computer into a safe and easy-to-use computer forensics and Electronic Discovery (E-Discovery) collections' platform. Freely available on a self-contained CD, BitFlare was designed by computer forensics E-Discovery experts to empower the non-expert. No programs to install and no software licenses to purchase. It allows users to quickly identify suspicious data through metadata file filtering and keyword searches. This electronically stored information (ESI) can be collected *in situ* in response to investigations or litigation. BitFlare's process automates and preserves the chain-of-custody of both the data on the source hard drive at the time of analysis as well as extracted evidence. In addition, BitFlare allows users to create an encrypted, tamper evident forensics copy of a computer drive free of charge. Computers can be safely and cost-effectively imaged within hours of an incident anywhere around the world.	http://www.bitflare.com/ http://www.sunblocksystems.com/
9.	New Technologies	CRCMD5	Mathematically, it creates a unique signature for the contents of one, multiple or all files on a given storage device. Such signatures can be used to identify whether or not the contents of one or more computer files have changed. This forensics tool relies upon 128 bit accuracy and can easily be run from a floppy diskette to benchmark the files on a specific storage device, for example, floppy diskette, hard disk drive and/or zip disk. CRCMd5 can be used as the first step in the implementation of a configuration management policy. Such a policy and related system bench marking can help computer specialists isolate problems and deal with computer incidents after they occur. The program is also used to document that computer evidence has not been altered or modified during computer evidence processing.	http://www.forensics-intl.com/crcmd5.html

10.	DIBS USA, Inc.	DIBS Forensic Workstation	The DIBS® Forensic Workstation provides complete solution to the problems faced by the computer crime investigator. Developed over a number of years by practicing forensics analysts, the dedicated equipment meets the demands imposed by today's advanced enquiries.	http://www.dibsusa.com/
11.	DIBS USA, Inc.	DIBS Mobile Forensic Workstation	The DIBS® Mobile Forensic Workstation provides all the equipment required for onsite analysis of the contents of suspect computers. Contained in a case made of ultra high impact structural polypropylene with a neoprene O-ring seal, the DIBS® Mobile Forensic Workstation is rugged and hard working and provides full protection for the forensics equipment inside. This includes a Pentium-based laptop fully configured with analysis software, an external hard disk housing and three hard disk racks and drives for reconstructions, a black and white/color printer, PCMCIA card, cables, connectors and mouse. The DIBS® Mobile Forensic Workstation allows onsite hard disk restorations and analyses.	http://www.dibsusa.com/
12.	DIBS USA, Inc.	DIBS Portable Evidence Recovery Unit	DIBS® Portable Evidence Recovery Unit is an efficient and easy way to copy the entire content of a computer's hard disk. It was developed after working closely with senior police officers to find a fast, powerful and reliable way to retrieve potential evidence which was admissible in a court of law.	http://www.dibsusa.com/
13.	DIBS USA, Inc.	DIBS Professional Forensic Software	Available as a series of modules, each designed for specific tasks, DIBS® Analyzer is highly effective and productive software. Many time-consuming jobs, such as undeleting files, are automated by the software, and as you work with DIBS® Analyzer you can print out evidence and examination details in a format that will be acceptable in a court of law.	http://www.dibsusa.com/

14.	New Technologies	FileCNVT (File Convert)	Freeware tool that supplements the FileList program from New Technologies. FileList is a forensic tool that is used to quickly catalog the contents of one or more computer hard disk drives. The FileList output is compressed so that the program and related output will normally fit on just one floppy diskette.	http://www.forensics-Intl.com
15.	New Technologies	FileList	Used to quickly document information about files stored on one or more computer hard disk drives and other computer storage devices. This multipurpose tool was designed for covert use, security reviews and forensics laboratory processing of computer evidence. It leaves no trace that it has been used and the output is compressed so that the output will usually fit on just one floppy diskette. It is compatible with DOS, Windows, Windows 95/98 and a special version is available for Windows NT systems.	http://www.forensics-intl.com/
16.	New Technologies	FILTER	Freeware program used to remove binary (non-alphanumeric) characters from computer data. The program has been used by military and law enforcement agencies for years and was donated to the law enforcement community in 1991 by Michael R. Anderson (a New Technologies founder). Once a file has been processed with this program, the contents can be printed and viewed with traditional computer applications, for example, word processors.	http://www.forensics-intl.com/
17.	New Technologies	GetFree	This program is used to capture all of the unallocated file space on DOS/Windows-based computer systems for forensics analysis and review. A special version also exists for use in Windows NT systems. It is sold separately. The use of this program eliminates the need to restore potentially hundreds or thousands of files on a computer hard disk drives and floppy diskettes. It was primarily developed as a computer forensics tool for use	http://www.forensics-intl.com/

			in computer-related investigations and internal audits. However, GetFree is also an ideal tool for computer security risk assessments because it automatically captures the data associated with unallocated space. Such data can be reviewed and analyzed using other NTI forensics tools to identify corporate computer policy violations and evidence in criminal and civil proceedings. From a security standpoint, this tool is also ideal for the validation of computer security scrubbers and related computer security procedures concerning the elimination of sensitive and or classified computer data.	
18.	New Technologies	GetSlack	This program is used to capture all of the file slack on a logical DOS/Windows hard disk drive or floppy diskette for analysis with other NTI forensics tools. A special version also exists for the processing of Windows NT systems. It is sold separately. The software is an ideal tool for use in investigations, internal audits and in computer security reviews. NTI places special importance on the use of this tool in computer security risk assessments because memory dumps in file slack are cause for security concern. Typically, network logons and passwords are found in file slack. It is also possible for file encryption passwords to be stored in memory dumps made to file slack.	http://www.forensics-intl.com/
19.	New Technologies	NTAView	It is a freeware tool used in investigations related to Internet E-Mail, Internet browsing and Internet file downloading. The program is for use with New Technologies Net Threat Analyzer (NTA) software. It can be used to determine E-Mail and Internet browsing frequency and has built-in features that provide for frequency distribution analysis of NTA’s findings.	http://www.forensicsintl.com.ntaview.html

20.	New Technologies	NTI-DOC	This program is used to essentially take an “electronic snapshot” of files and subdirectories that have previously been identified as having evidentiary value. Having the program is like having a camera at the “electronic crime scene.” It is a simple yet effective forensics documentation tool. The program automatically creates documentation that can be printed, viewed or pasted into investigative computer forensics reports. The original program titled DOC has been used for years by military and law enforcement computer specialists and was previously donated for law enforcement use by Michael R. Anderson, an NTI founder. This version contains enhancements that are not found in the original version.	http://www.forensics-intl.com/
21.	New Technologies	ShowFL	Freeware tool for the timeline analysis of computer usage. It is also helpful in the investigation of conspiracies when multiple computers and computer users are involved. It is made available here so that our clients will have easy access to the current version for use in conjunction with the FileList program from New Technologies.	http://www.forensics-intl.com/
22.	Cyber Security Technologies	OnLineDFS^{TM}	OnLine Digital Forensic Suite^{TM} (OnLineDFS^{TM}) enables network-based, real-time investigations of live, running computer systems. It is ideal for rapid incident response, compliance management and eDiscovery in enterprises, and for the needs of law enforcement. OnLineDFS enables the rapid, forensically sound examination of a computer without disrupting the operations of the enterprise. It delivers an extensive suite of functionality for the investigation and capture of volatile and persistent data from the computer under examination.	http://www.cyberstc.com/index.asp

23.	New Technologies	PTable	Hard disk partition table analysis tool. This software tool is used in computer forensics to review and analyze the partition table(s) assigned to a hard disk drive. This tool is essential concerning network forensics and/or when multiple operating systems are stored on one hard disk drive in multiple partitions. This software is also used to identify hidden data potentially stored in the partition gap or "unknown" partitions.	http://www.forensics-intl.com/
24.	New Technologies	Seized	It is an evidence preservation tool. This simple program is designed to limit access to computers that have been seized as evidence. All too often, "resident computer experts" get curious and attempt to operate seized computers in hopes of finding clues or evidence. These individuals many times are not trained in computer forensics and are therefore unfamiliar with proper computer evidence processing procedures. They typically do not know that even the mere running of a computer system can overwrite evidence stored in the Windows swap file and/or in erased file space. This program was written to help prevent these common problems.	http://www.forensics-intl.com/
25.	New Technologies	Filter_I	This enhanced forensics filter utility is used to quickly make sense of nonsense in the analysis of ambient computer data, for example, Windows swap file data, file slack data and data associated with erased files. Filter_I relies upon pre-programmed artificial intelligence to identify fragments of word processing communications, fragments of E-Mail communications, fragments of Internet chatroom communications, fragments of Internet news group posts, encryption passwords, network passwords, network logons, database entries, credit card numbers, social security numbers and the first and last	http://www.forensics-intl.com/

			names of individuals that have been listed in communications involving the subject computer. This software saves days in the processing of computer evidence when compared to traditional methods.	
26.	Fred Cohen & Associates	ForensiX	ForensiX provides a top flight, extensible, forensics examination system for computer evidence, all in a user-friendly graphically managed package. With its broad functionality, easy-to-use interface and built-in foresnics integrity mechanisms, ForensiX meets the need of corporate and law enforcement.	http://www.all.net/ForensiX/index.html
27.	Digital Intelligence	PDBLOCK	A standalone utility designed to prevent unexpected writes to a physical disk drive. When PDBLOCK is executed on a computer its job is to prevent all writes to the physical drives. Handling both the standard, Interrupt 13 and the Interrupt 13 Extensions, PDBLOCK is designed to be the next generation of write blockers providing protection for Large Hard Drives, FAT32(x), DOS 7.1. It also prevents accidental overwriting of computer evidence.	http://www.digitalintel.com/fred.htm
28.	Digital Intelligence	FRED	Forensics Recovery of Evidence Device (FRED) is a highly integrated platform which may be used both for the acquisition and analysis of computer-based evidence. It can operate as a standard PC Platform when not in use for forensics acquisition or processing. It is also available in stationary, mobile or combined configurations.	http://www.digitalintel.com/fred.htm
29.	Digital Intelligence	FREDDIE	Forensics Recovery of Evidence Device Diminutive Interrogation Equipment (FREDDIE) is considered to be little brother of FRED from Digital Intelligence. Like FRED, FREDDIE is a highly integrated platform which may be used both for the acquisition and analysis of computer-based evidence. It is a highly portable solution which meets both imaging and processing requirements. It also uses a standard ATX Motherboard, Power Supply	http://www.digitalintel.com/fred.htm

			and other components to minimize compatibility issues and maximize flexibility. The removable devices in the forensics bays can be interchanged between both FRED and FREDDIE.	
30.	Digital Intelligence	DRIVESPY	A forensics DOS shell, it is designed to emulate and extend the capabilities of DOS to meet forensics needs. Whenever appropriate, DRIVESPY will use familiar DOS commands (CD, DIR, etc.) to navigate the system under investigation. When beneficial, DRIVESPY will extend the capabilities of the associated DOS commands, or add new commands as necessary. DRIVESPY provides a familiar DOS-like prompt during system navigation.	http://www.digitalintel.com/drivespy.htm
31.	CD Dimensions	Evidence Disc Systems	Made by Rimage, it fully automates both burning and direct-to-disk printing of multiple requests for unique CDs, DVDs and Blue Ray Discs with the simplicity of a shared network appliance. No host PC or local operator is required. Archiving and distribution of digital case evidence from authorized users is as easy as printing paper. It is a simple and cost-effective way to generate disks containing the critical evidence to make your case strong. There are fewer errors and downtime, which provides the ability to print professionally on each disk, and also work on multiple cases at once.	http://www.cddimensions.com/
32.	Digital Intelligence	IMAGE	A stand-alone utility to generate physical images of floppy disks. The files which are generated by IMAGE contain complete physical images of the diskette(s) being processed. IMAGE is capable of generating either highly compressed or “flat” images for forensics analysis. IMAGE utilizes internally implemented algorithms which are identical to those used in ZIP compatible archives. If desired, non-compressed (flat) images may also be generated to facilitate examination of the image file itself.	http://www.digitalintel.com/image.htm

33.	KeyGhost	KeyGhost	The KeyGhost® is a hardware key logger that records up to 2 million keystrokes on a flash memory chip. It starts recording immediately and unobtrusively the moment the computer is turned ON. Users can detect file theft and inappropriate use of the computer before it is too late to act. It can be attached externally to the keyboard cable or hardwired inside the keyboard. (*Note:* Be sure to read the legal disclaimer.)	http://www.keyghost.com/products.htm
34.	Digital Intelligence	PART (Partition Manager)	A Partition Manager which will list summary information about all the partitions on a hard disk, switch bootable partitions, and even hide and unhide DOS partitions.	http://www.digitalintelligence.com/software/disoftware/part/ PART documentation can be downloaded from http://www.digitalintelligence.com/software/disoftware/part/part.pdf
35.	Technology Pathways	ProDiscover DFT	A completely integrated Windows™ application for the collection, analysis, management and reporting of computer disk evidence. Designed specifically to meet National Institute of Standards and Technology (NIST) standards. Saves space on forensics workstations by creating compressed image files. Keeps original evidence safe by creating an exact bit-stream copy. Finds data hidden in Windows NT/2000 Alternate Data Streams. Includes powerful search capabilities.	http://www.techpathways.com/DesktopDefault.aspx?tabindex=4&tabid=12
36.	Dan Farmer and Wietse Venema	The Coroner's Toolkit (TCT)	Freeware – The Coroner's Toolkit. A collection of programs that can be used for a post-mortem analysis of a UNIX system after break-in.	http://www.porcupine.org/forensics/tct.html
37.	AccessData Corporation	Password Recovery Registry Viewer	Registry Viewer allows you to view the contents of Windows® operating system registries. Unlike the Windows Registry Editor®, which displays only the current system's registry, Registry Viewer lets you view	http://www.accessdata.com/ http://accessdata.com/support/adownloads

			registry files from any Windows system. Registry Viewer also provides access to a registry's encrypted protected storage, which contains passwords, usernames and other information not accessible in Windows Registry Editor.	http://www.accessdata.com/media/en_us/print/techdocs/Registry%20Viewer.pdf http://www.accessdata.com/forensictoolkit.html
		FTK (Forensics Tool Kit)	Multipurpose tool commonly used to index acquired media. The Forensics Toolkit is the perfect tool for complete and thorough forensics examinations. FTK has full-text indexing, advanced searching, deleted file recovery, data-carving, E-Mail and graphics analysis, etc. FTK includes FTK Imager, the Hash Library-KFF, Registry Viewer and technical phone support with free software subscription service for 12 months.	http://www.accessdata.com/downloads/media/FTK_3_SystemSpecificationsGuide.pdf
38.	ASR Data Acquisition & Analysis	S.M.A.R.T for Linux	The SMART software and methodology have been developed with the intention of integratingtechnical, legal and end-user requirements into a complete package that enables the user to perform their job most effectively and efficiently. SMART is more than a stand-alone data forensics program. The features of SMART allow it to be used in many scenarios.	http://www.asrdata.com/ http://www.asrdata.com/forensic-software/smart-for-linux/
39.	Hot Paper Technology	Email Detective	Email Detective is a software tool that allows investigators to extract the E-Mail contents from America Online's database stores on a user's computer disk drive. A comprehensive report is produced for the forensics investigator detailing all messages and photos retrieved.	http://www.hotpepperinc.com/ http://www.softlist.net/search/email-detective/ http://www.digitalintelligence.com/software/hotpeppertechnology/emaildetective/
40.		Reverse Email Detective	E-Mail addresses can be confusing. Often, E-Mail addresses provide no clue about their owner. This can be the case when you find the E-Mail address in the "cc:" section of a memo, for example. Maybe you found an E-Mail address on a piece of	http://www.squidoo.com/reverseemaildetective

			paper and you may need to find out whom it belongs to. If you are stuck in your search for information about a Yahoo! E-Mail address, this tool may help you. Reverse Email searches are a lot like search engines, except that they search for any E-Mail address, including those from Yahoo. You only need to enter the address, and you can find out within only a few moments the owner of the address as well as added information. *Note:* There are many sites with free Reverse Email lookups. Although some of these sites do provide free searches, however, they will never be as informative as those that charge a fee. This is because there are a limited number of free E-Mail directories. Most of this information is available only at a premium, which means the sites will charge a fee to assist you in finding the information you would like to obtain.	
41.	IRS-CI Electronic Crimes Pgm	ILook (law enforcement only)	ILook is a powerful multithreaded, unicode compliant, fast and efficient forensics analysis tool designed to examine digital media from seized computer systems and/or other digital media. ILook has robust processing capabilities including advanced E-Mail deconstruction and analysis, thorough and comprehensive indexing capabilities, a wealth of reporting features and advanced unallocated space data salvaging capability. ILook runs on Windows XP/Server platforms, both 32 and 64-bit versions. Available under commercial license.	http://www.ilook-forensics.org/ http://www.associatedcontent.com/article/5725306/top_low_cost_law_enforcement_computer.html
42.	New Technologies	DiskSearch 32	Used to find strings of text in files. Can be used to find strings of text in file slack and unallocated space. Also has the capability of finding similar or words that have been spelled incorrectly. Can also be used to search a storage device at a physical level.	http://www.Forensics-Intl.com

43.	New Technologies	DM	Freeware database analysis tool.	http://www.forensics-intl.com/
44.	New Technologies	TextSearch Plus	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.	http://www.forensics-intl.com/
45.	New Technologies	Password Recovery Kit	Allows access to password-protected files.	http://www.forensics-intl.com/
46.	Paraben Corporation	Email Examiner Device Seizure	With Network Email Examiner, you can now thoroughly examine a variety of network E-Mail archives. No longer will you have to be stuck in a long and painstaking restore process. View one or all individual E-Mail accounts in information store. Supports Microsoft Exchange 5.0, 5.5 and 2000 (.EDB), Lotus Notes 4.0, 5.0, 6.0 (.NSF) and GroupWise up to version 6.5.1. Export E-Mail to PST files, msg and EML format. Recover deleted E-Mail.	http://www.paraben.com/ http://tsm-soft.net/downloads/category/sw.asp?id=1661
47.	Porcupine	The Coroner’s Toolkit	A suite of programs for Unix analysis. IBM Public License.	http://www.porcupine.org/forensics/tct.html
48.	TechPathways	Prodiscover Forensic/IR	ProDiscover is a powerful computer security tool that enables computer professionals to find all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.	http://www.techpathways.com/ http://www.techpathways.com/uploads/ProDiscoverForensicsDataSheet.pdf http://www.techpathways.com/ProDiscoverSuite.htm http://www.techpathways.com/uploads/ProDiscoverFamilyGuide.pdf

49.	Westone	Gargoyle Investigator	Provides investigators with information regarding the contents of a suspect's computer along with essential information about its owner's computer use. Once identified, Gargoyle also maps the detected files to the associated cyberweapons and classifies them into a category of Malware. With the ability to identify potentially hostile or suspicious programs based on the loaded dataset, the classification of those hostile programs, and the ability to view the suspect from a new aspect while ascertaining incriminating behaviors or methods, this becomes a core tool for your investigation.	http://www.westtonetech.com/ http://www.htt.co.in/wetstone/Gargoyle-Investigator-Forensic-Pro-Edition.htm
		Live Wire Investigator	Used for collecting volatile evidence from "Live" running computers and networks.	www.wetstonetech.com http://www.asoto.com/id57.html http://www.forensicswiki.org/wiki/LiveWire_Investigator http://www.scmagazineus.com/wetstone-technologies-livewire-investigator-v-311c/review/1027/ http://www.forensicfocus.com/index.php?name=News&file=article&sid=916
50.	SweetScape Software	Hex Editor	Professional-grade text editor and hex editor are designed to quickly and easily edit any file or drive on your computer.	http://sweetscape.com/ http://www.sweetscape.com/companyinfo/
51.	Paraben	Chat Examiner	This is a toolkit to examine chats coming from ICQ, Yahoo, MSN, Trillian or Miranda. Please note, however, that AOL Instant Messanger (AIM) does not have traditional data stores or logs and therefore will not be supported by Chat Examiner.	http://www.digitalintelligence.com/cart/ComputerForensicsProducts/Chat-Examiner.html

Antiforensics Tools (Software Products)

The tools listed in Table I.2 are antiforensics tools. There are situations where use of "antiforensics" tools is permitted. Antiforensics is explained in Chapter 7 (Section 7.19). You may like to refer to Chapter 7 and/or the particular section mentioned to understand what antiforensics is.

Table I.2 Antiforensic tools (software products)

Sr. No.	*Vendor*	*Product(s)*	*Remarks*	*Websites*
1.		DeepFreeze	This is an antiforensics software that claims to delete files.	http://en.wikipedia.org/wiki/Deep_Freeze_(software) http://www.faronics.com/en/Products/DeepFreeze/DeepFreezeEducation.aspx
2.		DECAF	This tool is available for free and works on Windows platform. It is antiforensics software targeting Microsoft's COFEE tool.	http://www.mydigitallife.info/2010/02/13/decaf-free-download-to-detect-computer-forensic-and-auditing-tool-anti-cofee/ There is a discussion on "COFEE vs. DECAF" at: http://isc.sans.edu/diary.html?storyid=7741
3.	Nester	Wipe	This is a tool that effectively degausses the surface of a hard disk, making it virtually impossible to retrieve the data that was stored on the disk. This tool is designed to ensure that the sensitive data is completely erased from the magnetic media. The license is GPL (general-purpose license).	http://wipe.sourceforge.net/
4.	Salvatore Sanfilippo	Overwrite	This is a Unix utility that makes it harder to recover data. It overwrites files using random patterns and deterministic patterns. The license is GPL (general-purpose license).	http://www.kyuzz.org/antirez/overwrite.html

5.	Phil Howard	Diskzapper	Automatically begins erasing all the disks as soon as the booting process is completed. No user action is required. The tool is intended to be used on computers for which it is not convenient to plug-in a keyboard and monitor. Available under commercial license.	http://diskzapper.com/
6.	Dark Horn	DBAN	This is a self-contained boot floppy that securely wipes the hard disks of most computers. It automatically and completely deletes the content of any hard disk that it can detect. It is a freeware.	http://www.dban.org/
7.	Robin Hood Software Ltd.	Evidence Eliminator	Proprietary software commercially available. Works on Windows Platform. Claims to delete files securely. Destroys Windows and SWAP file, Windows Application logs, Windows Temporary files, Windows Recycle Bin, Windows Registry Backups, Windows Clipboard data, Start Menu Recent Documents history, Start Menu Run history, Start Menu Find Files etc. The tool is available under commercial license.	http://www.evidence-eliminator.com http://www.evidence-eliminator.com/product.d2w
8.	Naval Criminal Investigative Service (NCIS)	Track Eraser Pro	Designed to protect you by cleaning up all the tracks of Internet activities on your computer. With a single click, it allows you to erase the cache, cookies, history, typed URLs, autocomplete memory, index.dat, etc. Available under commercial license.	http://www.acesoft.net/features.htm
9.	Neobyte Solutions	Invisible Secrets	In addition to encrypting your data and files for safe-keeping for secure transfer across the net, this tool also hides them in places that appear totally innocent such as picture or sound files or webpages. Available under commercial license.	http://www.invisiblesecrets.com/
10.	BAxBEx Software	CryptoMite	Enables you to encrypt, decrypt, and wipe files and folders of any type. It supports various encryption engines along with zip compression. It also includes E-Mail capabilities and also functions for building self-extracting encrypted zip files. Available under commercial license.	http://www.baxbex.com/products.html

11.	Jetico	bcwipe	Can be run from My Computer as well as from a command-line prompt. Is a powerful set of utilities and complies with US DoD 5200.28-STD standard and Peter Gutmann wiping scheme. You can also create and use your own customized wiping. The tool is available under commercial license.	http://www.jetico.com/
12.	Mares and Company, LLC.	Declasfy	The program is designed to wipe hard disks to meet the Department of Defense (DoD) standards. Available under commercial license.	http://www.dmares.com/maresware/df.htm
13.	Digital Confidence Ltd.	BatchPurifier	Tool to remove hidden data, metadata from multiple files. It is also able to remove more than 50 bytes of hidden data from 20 file types, including Microsoft Office.	http://www.digitalconfidence.com/BatchPurifier.html

Computer Forensics Hardware

There is a variety of forensics hardware equipment available to computer forensics examiners (some of them were depicted in the context of discussion in Chapter 7). This includes hardware specifically designed with forensics in mind, as well as extensively available technical devices put to use in a forensics laboratory. A number of organizations have designed towers, servers, write blocking devices and peripherals for the purpose of forensics. Some individual forensics workstations come bundled with forensics software and cost several thousand dollars. Given these high costs, many forensics examiners prefer to use standard laptops or towers and install their own software, which turns out to be viable solution in most circumstances. This is the reason why the table below does not have too many entries of hardware products used in computer forensics. The links mentioned in Table I.3 can be visited for technical specifications of the hardware products.

Table I.3 Hardware tools

Sr. No.	***Vendor/ Distributor***	***Product(s)***	***Remarks***	***Websites***
1.	SalvationDATA technology	Data Copy King	Data Copy King (DCK) is a newly designed hard drive duplicator from with color touch screen, build-in SATA/IDE support and USB support with additional adapters. DCK is the only hard drive duplicator with “UNIC” disk imaging solutions, which is able to copy data from good drives or drives with severe bad sectors or drives with unstable heads but still detected in the bios.	http://www.salvationdata.com/data-recovery-equipment/data-copy-king.htm http://www.salvationdata.com/data-recovery-equipment/data-copy-king01.htm

2.	InfoAssure Technologies 2 Gujrat Vihar, BMS Complex Vikas Marg New Delhi - 110092, India Sales: +91 9818091173 +91 11 42440997 Fax: Sales@InfoAssure.in Email: www.InfoAssure.in	FRED and FRED DX	**FRED** is **F**orensic **R**ecovery of **E**vidence **D**evice. The FRED family of forensic workstations is highly integrated, flexible and modular forensics platforms. It includes exclusive UltraBay II Write Protected Imaging Bay.	http://www.digitalintelligence.com/products/fredselect/
3.	Same as above	Forensic Network	A Forensic Network is a series of processing and imaging computers connected and integrated directly with a high-speed, high-capacity server to share resources. The file server operates as the core of the Forensic Network and can be used as a central storage facility for Forensic Images as well as applications software for use by the client processing and imaging stations. Workstation clients on the network perform the actual imaging and processing tasks while the central file server stores the images and case work. High-speed scanners and color printers can also be made available as shared resources on the network. Multiple forensics clients can access case and image files simultaneously without duplicating information on several workstations. File and image storage space is centralized at the file server, reducing the localized storage requirements at the workstation clients.	http://www.digitalintelligence.com/products/forensic_network/
4.	Same as above.	Forensic Write Blockers	Write blockers are devices that make it possible to acquire information on a drive without the risk of accidental damage to the contents on the drive. They do this by allowing read commands to pass but by blocking write commands	http://www.asoto.com/id42.html Write Blocker selection chart is available at: http://www.digitalintelligence.com/writeblockers.php

5.	ForensicStore	Super DriveLock eSATA Express Kit	This is claimed to be the only blocker in the market that prevents accidental writes to hard drives.	http://www.forensicstore.com/forensic-hardware/write-blockers/super-drivelock-esata-express-kit.html
6.	ForensicStore	Wiebetech USB Write Blocker	This is a forensics solution to access USB Flash Drives or devices that cannot be removed from a USB enclosure.	http://www.forensicstore.com/forensic-hardware/write-blockers/15-wiebetech-usb-write-blocker.html
7.	ForensicStore	Super DriveLock	Used for preventing accidental writes to hard drives	http://www.forensicstore.com/forensic-hardware/write-blockers/super-drivelock.html
8.	ForensicStore	Analysis Station	The USB interface supports USB 1.1 or USB 2.0 specifications to allow connections to host computer via USB port at maximum data transfer rate 480 Mbps.	http://www.forensicstore.com/forensic-hardware/analysis-station.html
9.	ForensicStore	USB SIM Reader	Omnikey CardMan 6121 USB SIM Reader supports all ISO 7816 microprocessor-based smartcards as well as numerous popular memory cards.	http://www.forensicstore.com/forensic-hardware/omnikey-cardman-6121-usb-sim-reader.html
10.	ForensicStore	Hard Drive Duplicator	The Image MASSter™ 4000 PRO is the next-generation, fast and reliable, IT Duplicator based on the time-proven Image MASSter™ 4000 product line. This new duplication unit comes as the perfect solution for the mid-size IT organization looking for all the benefits of an enterprise level hard drive duplicator in a compact and easy-to-use solution.	http://www.forensicstore.com/forensic-hardware/4000-pro-it-hard-drive-duplicator.html
11.	ForensicStore	Imaging Tool	At SATA-2 speed, the Image MASSter Solo-4 offers investigators the ability to image one “Suspect” to two “Evidence” drives or two separate “Suspect” drives to individual “Evidence” copies simultaneously. The Image MASSter Solo-4 features built-in support for SAS, SATA and USB drives.	http://www.forensicstore.com/forensic-hardware/solo-4.html

Further Reading

Additional Useful Web References

1. An article *An Introduction to Computer Forensics* can be read at: http://www.secureworks.com/assets/uk/ComputerForensics.pdf (26 December 2010).
2. Understand how computer forensics works by visiting:
   http://computer.howstuffworks.com/computer-forensic.htm/printable (23 December 2010).
3. Procedures involved in "seizing a computer" can be read at: http://www.priscilla.com/forensics/ComputerSeizure.html (20 December 2010).
4. Frequently Asked Questions (FAQs) on Computer Forensics are available at: http://www.newyorkcomputerforensics.com/learn/forensics_faq.php (10 December 2010).
5. Forensic Training Courses and Providers are listed at: http://www.forensicswiki.org/wiki/Training_Courses_and_Providers (20 December 2010).
6. To know more about DeepFreeze, visit:
   http://www.ideacts.com/CLINCK-Partner-DeepFreez.html
7. Read the article *Hackers declare war on international forensics tool* at: http://www.theregister.co.uk/2009/12/14/microsoft_cofee_vs_decaf/ (25 December 2010).
8. In the following link , Forensic tools are listed: http://www.timberlinetechnologies.com/products/forensics.html (15 December 2010).
9. In the following link, some antiforensic tools are listed: http://www.securitywizardry.com/index.php/products/forensic-solutions/anti-forensic-tools.html (26 December 2010).
10. The "whatis" list of forensics tools is available at:
    http://cainelive.aforumfree.com/forensic-tools-f14/forensic-tools-whatis-list-t101.htm (26 December 2010).
11. Alphabetical list of links to manufacturers, suppliers and products (sponsored by Mares and Company) is available at: http://www.dmares.com/maresware/linksto_forensic_tools.htm (25 December 2010).
12. Computer Forensic Software Tools Downloads are also available at:
    http://www.forensic-computing.ltd.uk/tools.htm (23 December 2010).
13. You can also visit computer forensics resources at: http://www.evestigate.com/COMPUTER%20FORENSIC%20RESOURCES.htm (25 December 2010). There is a lot of useful guidance provided the link.
14. To know more aobut wiping scheme, visit:
    Peter Gutmann Method: http://en.wikipedia.org/wiki/Gutmann_method (20 December 2010).
    Wiping Schemes: http://www.deletefilespermanently.com/help/Using/WipingSchemes.html (20 December 2010).
    Free Gutmann Erase download: http://3d2f.com/tags/gutmann/erase/ (20 December 2010).
    Best Free Gutmann Downloads: http://www.freedownloadmanager.org/downloads/peter_gutmann_software/ (20 December 2010).

15. An informative article on hiding data, forensics and antiforensics is available at:
http://www.berghel.net/col-edit/digital_village/apr-07/dv_4-07.php (24 December 2010).

16. The official release version of ACPO Guidance on Computer-based Electronic Evidence can be obtained from: http://www.asianlaws.org/library/cci/acpo-guidelines-computer-evidence.pdf (24 December 2010).

17. Read article *Computer Forensics Standards and Controls* at:
http://www.forensicmag.com/article/computer-forensics-standards-and-controls (31 January 2011).
http://www.forensicmag.com/article/computer-forensics-standards-and-controls-0 (31 January 2011).