SYSTEM FORENSICS INVESTIGATORS HAVE MANY PLATFORMS and tools to turn to in their work, whether strengthening a system against attack or dealing with the consequences of a cyberattack. Add to your knowledge by doing the following:

- Studying for forensic certifications
- Earning a college or university degree in digital forensics
- Networking with professionals in the field
- Joining user groups and online discussion groups
- Attending lectures, conferences, and events
- Reading books, articles, and Web sites

This chapter discusses resources for system forensics. It begins by looking at some of the available system forensics training programs and certifications. It then provides lists of system forensics resources. Finally, it supplies URLs for forensic organizations and information sources, journals related to system forensics, and software and hardware forensic tools.
Chapter 15 Goals

When you complete this chapter, you will be able to:

• Understand what system forensics training programs and certifications are available
• Locate a local chapter of a system forensics user group
• Access online resources for system forensics

System Forensics Certification and Training

Numerous organizations offer certification programs for system forensics. These programs usually test a student after completing one or more training sessions successfully. Certifying organizations range from nonprofit associations to vendor-sponsored groups. All these programs charge fees for certification. Some require candidates to take vendor- or organization-sponsored training to qualify for the certification.

Some state and federal government agencies have established their own certification programs. These programs address the skills needed to conduct computing investigations at various levels. In addition, a number of universities and other organizations offer courses in system forensics.

The following sections describe some of the most prominent system forensics training programs and certifications.

International Association of Computer Investigative Specialists (IACIS)

The International Association of Computer Investigative Specialists (IACIS) is one of the oldest professional system forensics organizations. It was created by police officers who wanted to formalize credentials in computing investigations. Currently, IACIS limits membership. Only law enforcement personnel and government employees working as system forensics examiners may join.

IACIS conducts an annual two-week training course for qualified members. Students learn to interpret and trace e-mail, acquire evidence properly, identify operating systems, recover data, and understand encryption theory and other topics. Students must pass a written exam before continuing to the next level. Passing the exam earns the student Certified Electronic Evidence Collection Specialist (CEECS) status.
Other candidates who complete all parts of the IACIS test successfully receive Certified Forensic Computer Examiner (CFCE) certification. The CFCE process changes as technology changes. Topics include data hiding, determining file types of disguised files, and accessing password-protected files. The program might also ask a student to find evidence and draw conclusions from it. Students must demonstrate proficiency in technical tools and deductive reasoning.

For the latest information about IACIS, visit its Web site, http://www.iacis.info.

IACIS requires recertification every three years to demonstrate continuing work in the field of system forensics. Recertification is less intense than the original certification.

High Tech Crime Network (HTCN)

High Tech Crime Network (HTCN) offers several levels of certification, with different requirements:

- Certified Computer Crime Investigator, Basic
- Certified Computer Crime Investigator, Advanced
- Certified Computer Forensic Technician, Basic
- Certified Computer Forensic Technician, Advanced

HTCN certification is open to anyone in a computing investigations profession.

Unlike IACIS, HTCN requires a review of all related training. This includes training in one of its approved courses, a written test for the specific certification, and a review of the candidate's work history.

The HTCN Web site, http://www.htcn.org, specifies requirements for the various certification levels.

EnCase Certified Examiner (EnCE) Certification

Guidance Software, the creator of the EnCase software, sponsors the EnCase Certified Examiner (EnCE) certification program. EnCE certification is open to the public and private sectors. This certification focuses on the use and mastery of system forensics analysis using EnCase.

For more information on EnCE certification requirements, visit http://www.guidancesoftware.com.

AccessData Certified Examiner (ACE)

AccessData is the creator of Forensic Toolkit (FTK) software. AccessData sponsors the AccessData Certified Examiner (ACE) certification program. ACE certification is open to the public and private sectors. This certification is specific to use and mastery of FTK. Requirements for taking the ACE exam include completing the AccessData boot camp and Windows forensic courses.

For more information on ACE certification, visit http://www.accessdata.com.
Defense Cyber Investigations Training Academy (DCITA)

The Defense Cyber Investigations Training Academy (DCITA) develops and delivers computer investigation training courses for government and law enforcement organizations.

DCITA is accredited through the Council of Occupational Education (COE). DCITA is a government organization dedicated to computer investigations training, development, and delivery. It uses state-of-the-art equipment, classrooms, and technologies to train students in digital forensics techniques. DCITA’s training topics include the following:

- How to perform computer search and seizure
- How to investigate network intrusions
- How to forensically analyze computer media
- How to perform basic and advanced forensic examinations

For more information on DCITA training, see http://www.dc3.mil/dcita.

Other Training Programs and Certifications

Besides those already listed, other organizations offer certification programs and related training programs. The following are some of these other organizations and universities that offer certification and training:

- **Computer Technology Investigators Network (CTIN)**—http://www.ctin.org
- **CyberSecurity Institute**—http://www.cybersecurityinstitute.biz
- **DIBS USA, Inc.**—http://www.dibsusa.com
- **Federal Bureau of Investigation Academy**—http://www.fbi.gov/hq/td/academy/academy.htm
- **Federal Law Enforcement Training Center (FLETC)**—http://www.fletc.gov
- **Florida Association of Computer Crime Investigators, Inc.**—http://www.facci.org
- **Forensic Association of Computer Technologists**—http://www.byteoutofcrime.org
- **Global Digital Forensics**—http://www.evestigate.com/computer%20forensic%20training.htm
- **Henry C. Lee College of Criminal Justice and Forensic Sciences**—http://www.newhaven.edu/9/
- **High Tech Crime Institute**—http://www.hightechcrimeinstitute.com
- **High Technology Crime Investigation Association (HTCIA)**—http://www.htcia.org
- **Indiana Forensic Institute**—http://ifi-indy.org
- **Institute of Police Technology and Management**—http://www.iptm.org
- **International Society of Forensic Computer Examiners**—http://www.certifiedcomputer-examiner.com
- **National Center for Forensic Science**—http://www.ncfs.ucf.edu
- **National White Collar Crime Center (NW3C)**—http://www.nw3c.org
• **New Technologies, Inc. (NTI)**—http://www.forensics-intl.com
• **Paraben**—http://www.paraben-training.com/pcme.html
• **Regional Computer Forensics Laboratories (RCFLs) Program**—http://www.rcfl.gov
• **SANS Institute**—http://www.sans.org
• **Technical Resource Center**—http://trcglobal.com
• **Utica College Economic Crime Institute**—http://www.utica.edu/academic/institutes/ecii/
• **Wisconsin Association of Computer Crime Investigators**—http://www.wacci.org

**User Groups**

A system forensics user group is a good way for you to keep up with the latest tools and trends. Two organizations to consider joining are:

• **High Technology Crime Investigation Association (HTCIA)**—HTCIA enables members to share information, experience, ideas, and knowledge with one another. Members discuss methods, processes, and techniques related to investigations and security in advanced technologies. See http://www.htcia.org for more information.

• **Computer Technology Investigators Network (CTIN)**—CTIN provides instruction, presentations, and monthly meetings. It enables discussions on high-tech crime, investigative strategies, and tools. CTIN includes members of federal, state, and local law enforcement. It also includes members from corporate security, educational institutions, and the computer science community. Web site access is available to members only. Membership is free. See http://www.ctin.org for more information.

**Online Resources**

The following sections provide lists of online system forensics resources. They start with an inventory of forensic organizations and information sources. Then they catalog discussion list servers, journals, and conferences related to system forensics. Finally, they list open source and commercial software tools as well as commercial hardware tools.

**System Forensics Organizations and Information**

• **American Academy of Forensic Sciences**—http://www.aafs.org
• **Computer Forensics, Cybercrime and Steganography Resources**—http://forensix.org
• **Computer Forensics World**—http://www.computerforensicsworld.com
• **Department of Defense Cyber Crime Center (DC3)**—http://www.dc3.mil
• **Department of Justice Computer Crime & Intellectual Property Section**—http://www.cybercrime.gov
• **Digital Forensic Research Workshop**—http://dfrws.org
• Electronic Evidence Information Center—http://www.e-evidence.info
• Federal Bureau of Investigation Cyber Investigations—http://www.fbi.gov/cyberinvest/cyberhome.htm
• Forensics Wiki—http://www.forensicswiki.org
• Global Digital Forensics—http://www.evestigate.com/COMPUTER%20FORENSIC%20RESOURCES.htm
• High Technology Crime Investigation Association (HTCIA)—http://www.htcia.org
• Information Systems Security Association (ISSA)—https://www.issa.org
• International Association of Computer Investigative Specialists (IACIS)—http://www.iacis.com
• International Organization on Computer Evidence—http://ioce.org
• National Center for Forensic Science—http://ncfs.org
• National Criminal Justice Computer Laboratory and Training Center—http://www.search.org/programs/hightech/
• National Institute of Standards and Technology Computer Forensics Tool Testing (CFTT)—http://www.cftt.nist.gov
• National White Collar Crime Center—http://nw3c.org

Discussion List Servers
• Computer Forensic Investigators Digest Listserv (CFID)—For subscription information, see http://www.forensicsweb.com or e-mail jnj@infobin.org
• Computer Forensics Tool Testing (CFTT)—For subscription information, see http://groups.yahoo.com/group/cftt
• SecurityFocus: Binary Analysis—binaryanalysis@securityfocus.com
• SecurityFocus: Forensics—forensics@securityfocus.com
• SecurityFocus: Honeypots—honeypots@securityfocus.com
• SecurityFocus: Incidents—incidents@securityfocus.com
• SecurityFocus: LogAnalysis—loganalysis@securityfocus.com
• SecurityFocus: Phishing and Botnets—phishing@securityfocus.com
• SecurityFocus: Real Cases—realcases@securityfocus.com
Forensic Journals

- **Digital Investigation**—Digital Investigation covers cutting-edge developments in digital forensics and incident response from around the globe. It covers new technologies, useful tools, relevant research, investigative techniques, and methods for handling security breaches. See [http://www.elsevier.com](http://www.elsevier.com).

- **International Journal of Digital Crime and Forensics (IJDCF)**—IJDCF provides state-of-the-art coverage of issues related to digital evidence. IJDCF addresses the use of electronic devices and software for crime prevention and investigation. It contains high-quality theoretical and empirical research articles, research reviews, case studies, book reviews, tutorials, and editorials. See [http://www.igi-global.com/Bookstore/TitleDetails.aspx?TitleId=1112](http://www.igi-global.com/Bookstore/TitleDetails.aspx?TitleId=1112).

- **International Journal of Digital Evidence (IJDE)**—IJDE is a forum for discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence. IJDE is supported by the Economic Crime Institute (ECI) at Utica College. See [http://ijde.org](http://ijde.org).

- **Journal of Digital Forensic Practice**—The Journal of Digital Forensic Practice is a helpful resource for forensic specialists. Articles in the journal target both the public and private sectors. They present useful information, techniques, and unbiased reviews designed to assist forensic specialists in day-to-day practice. See [http://www.tandf.co.uk/journals/titles/15567281.asp](http://www.tandf.co.uk/journals/titles/15567281.asp).

- **Journal of Digital Forensics, Security and Law (JDFSL)**—JDFSL is a unique and innovative publication of the Association of Digital Forensics, Security and Law. The mission of JDFSL is to expand digital forensics research to a wide and eclectic audience. See [http://www.jdfsl.org/index.htm](http://www.jdfsl.org/index.htm).


- **Small Scale Digital Device Forensics Journal (SSDDFJ)**—SSDDFJ is an online journal for academics and practitioners. It publishes articles regarding theory, research, and practice in the rapidly changing field of small-scale digital device forensics. SSDDFJ is supported by the Cyber Forensics Lab (CFL) at Purdue University. See [http://www.ssddfj.org/about.asp](http://www.ssddfj.org/about.asp).

Conferences


• **Black Hat Briefings & Training**—http://www.blackhat.com/html/bh-link/briefings.html
• **ChicagoCon—White Hats Come Together in Defense of the Digital Frontier**—http://www.chicagocon.com
• **Computer and Enterprise Investigations Conference (CEIC)**—http://www.ceicconference.com
• **Department of Defense Cyber Crime Conference**—http://www.dodcybercrime.com
• **DFRWS (Digital Forensics Research Conference)**—http://www.dfrws.org
• **eDiscovery Summit**—http://www.ediscoverysummit.org
• **Forum of Incident Response and Security Teams (FIRST) Conference**—http://www.first.org/conference
• **HTCIA International Training Conference and Expo**—http://www.htcia.org/index.shtml
• **IACIS Computer Forensic Training Event**—http://www.cops.org/training
• **Mobile Forensics World Training Conference**—http://www.MobileForensicsWorld.org
• **Open Source Software for Computer and Network Forensics**—http://conferenze.dei.polimi.it/ossconf/index.php
• **Regional Computer Forensics Group Conference (RCFG)**—http://www.rcfg.org
• **SANS Computer Forensics**—http://computer-forensics.sans.org/events/
• **SANSFIRE (SANS Forensics, Investigations, Response, Education)**—https://www.sans.org/sansfire-2010/
• **Systematic Approaches to Digital Forensic Engineering (SADFE)**—http://conf.ncku.edu.tw/sadfe/
• **Techno Forensics Conference**—http://www.techsec.com
• **Techno Security Conference**—http://www.techsec.com

**Forensic Tools**

Forensic tools can be hardware or software. Software forensics tools can be either open source or commercial. Commercial forensic software ranges in price. Some products cost very little, and others are so costly that only large companies can afford them.

The following sections provide Web addresses for a number of tools. Mares and Company (http://www.dmares.com/maresware/linksto_forensic_tools.htm) lists dozens of system forensics tools, both commercial and open source.

**Open Source Software Tools**

• **Autopsy Forensic Browser**—Autopsy Forensic Browser is a graphical interface to the command-line digital investigation tools in The Sleuth Kit (TSK). Together, these tools enable investigation of the file system and volumes of a computer. See http://www.sleuthkit.org/autopsy.
• **BitPim**—BitPim allows an investigator to view and manipulate data on many mobile phones. See [http://www.bitpim.org](http://www.bitpim.org).

• **The Sleuth Kit (TSK)**—TSK is a tool that runs on Windows and UNIX systems, such as Linux, OS X, Cygwin, FreeBSD, OpenBSD, and Solaris. Use it to analyze NTFS, FAT, HFS+, Ext2, Ext3, UFS1, and UFS2 file systems and several volume system types. See [http://www.sleuthkit.org](http://www.sleuthkit.org).

Open source tools are available online at a number of sites. For more information on open source forensic tools and links to open source tools, see the site Open Source Digital Forensics, at [http://www.opensourceforensics.org/index.html](http://www.opensourceforensics.org/index.html). Also, see the Open Source Computer Forensics Manual, at [http://sourceforge.net/projects/oscfmanual/](http://sourceforge.net/projects/oscfmanual/).

### Commercial Software Tools and Vendors

• **AccuBurn**—R-AccuBurn-R produces exact copies of disks that have been imaged using CD/DVD Inspector. It supports all types and formats of disks. See [http://www.infinadyne.com](http://www.infinadyne.com).

• **ASR Data Acquisition & Analysis**—ASR Data Acquisition & Analysis offers a variety of software: SMART Linux, SMART for Linux, SmartMount (Windows/Linux/Macintosh), Grok-NTFS (Windows/Linux/Macintosh), and Grok-LNK (Windows/Linux/Macintosh). These products are customized for forensic work, integrated acquisition, authentication, and analysis. See [http://asrdata.com](http://asrdata.com).

• **BlackBag Technologies, Inc.**—BlackBag offers several forensic software products, including Mobilyze, SoftBlock, Macintosh Forensic Suite, and MacQuisition CF. Below are some product details (for even more information on Blackbag’s tools, see [http://www.blackbagtech.com](http://www.blackbagtech.com)):

  • **Mobilyze** was designed to forensically analyze iPhone, iPod Touch, and iPad devices. The product is capable of analyzing multiple devices simultaneously, easing the time and effort of consolidating findings into one comprehensive report.

  • **SoftBlock** is kernel-based, write-blocking software for Macs that identifies devices when they connect. It can mount a device in a forensically sound read-only manner. It can also mount a device in a conventional read/write configuration. SoftBlock offers flexibility, security, and speed in previewing and analyzing evidence across a number of devices.

  • **Macintosh Forensic Suite** is a unique set of 19 tools that gives forensic examiners a flexible, open analysis environment. The suite is specifically designed for Mac OS X versions 10.1 and higher. The applications speed an examiner’s analysis time while ensuring a thorough investigation of the drive.

  • **MacQuisition CF** is an external bootable forensic acquisition tool that safely and easily images Mac drives using the suspect system. MacQuisition provides an intuitive user interface. The tool automatically generates hashes.
• **ComputerCOP**—ComputerCOP has developed two unique forensic tools: Professional and Forensic Examiner. For information on both tools, see [http://computercop.com](http://computercop.com):
  - **ComputerCOP Professional** is an automated search tool that allows an examiner to immediately find electronic evidence for trial. Many supervision officers use it to monitor probationers’ and parolees’ computer use.
  - **ComputerCOP Forensic Examiner** is a field forensic solution. It acts as both an automated forensic search software and a simple-to-connect write blocker.

• **Darik’s Boot and Nuke (DBAN)**—DBAN is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN automatically and completely deletes the contents of any hard disk that it can detect. It is a useful utility for bulk or emergency data destruction. See [http://www.dban.sourceforge.net](http://www.dban.sourceforge.net).

• **DataLifter**—DataLifter is a suite of products designed to assist with computer forensics. DataLifter Forensicware Solution package contains investigative tools and comes in two versions: DataLifter and DataLifter.Net Bonus Tools. Two additional packages, DataLifter Digital Companion and DataLifter File Extractor Pro, are add-ons or major updates to tools already included with DataLifter or DataLifter.Net Bonus Tools. See [http://wwwdatalifter.com/products.htm](http://wwwdatalifter.com/products.htm).

• **Digital Detective**—Digital Detective offers Blade, HstEx, and NetAnalysis. For more information on all these tools, see [http://www.digital-detective.co.uk](http://www.digital-detective.co.uk):
  - **Blade** is a Windows-based data recovery solution. It supports plug-ins that give it advanced data recovery and analysis capabilities.
  - **HstEx** is a Windows-based data recovery solution. It is designed to recover browser artifacts and Internet history. HstEx supports all major forensic image formats.
  - **NetAnalysis** is software for the recovery and analysis of Internet browser artifacts.

• **Digital Intelligence**—Digital Intelligence, Inc., offers forensic hardware and software. Its software products include DRIVESPY, IMAGE, PART, PDBlock, and PDWipe. For information on all these products, see [http://www.digitalintelligence.com](http://www.digitalintelligence.com):
  - **DRIVESPY** processes large hard drives, FAT12/16/16x/32/32x partitions, hidden DOS partitions, and non-DOS partitions. It investigates long filenames, file dates, erased files, slack space, and unallocated space.
  - **IMAGE** is a standalone utility that generates physical images of floppy disks. The program is capable of generating highly compressed images for forensic analysis.
  - **PART** is a partition manager. It lists summary information about all the partitions on a hard disk. It also switches bootable partitions and even hides and unhides DOS partitions.
  - **PDBlock** is a write blocker. It provides customary write protection from Interrupt 13 disk access methods.
  - **PDWipe** is a standalone utility capable of quickly wiping large hard drives.
• **Directory Snoop**—This data recovery tool is a cluster-level search tool. It allows Windows users to search FAT and NTFS-formatted disk drives to see what data may be hiding. Directory Snoop can recover deleted files and permanently erase sensitive files. See [http://www.briggsoft.com/dsnoop.htm](http://www.briggsoft.com/dsnoop.htm).

• **dtSearch**—The dtSearch product line can instantly search terabytes of text across a desktop, network, Internet, or intranet site. See [http://dtsearch.com](http://dtsearch.com).

• **e-fense**—e-fense produces both Helix3 and Live Response. For more information on both of these products, see [http://www.e-fense.com](http://www.e-fense.com):

  - **Helix3 Enterprise (H3E)** provides incident response, computer forensics, and e-discovery in one interface. The Helix3 Pro edition software is available to e-fense forum members only.

  - **Live Response** allows a forensic examiner to acquire volatile data, such as Internet history, screen capture, and memory. The examiner can move this data from a suspect system onto a USB thumb drive.

• **Forensic Toolkit (FTK)**—This court-validated digital investigations platform delivers computer forensics analysis, decryption, and password cracking. FTK 3 is fast and provides enterprise-class scalability. See [http://www.accessdata.com/forensictoolkit.html](http://www.accessdata.com/forensictoolkit.html).

• **Foundstone**—Foundstone is a source for a number of free forensic tools. PatchIt is a file byte-patching utility. DumpAutoComplete is an application that searches for the default Firefox profile of the user who runs the tool and dumps the AutoComplete cache in XML format to standard output. Galleta is an Internet Explorer cookie forensic analysis tool. BinText can extract text from any kind of file and includes the ability to find plain ASCII text, Unicode text, and resource strings. Vision shows all open TCP and UDP ports and maps them to the owning process or application. Pasco is an Internet Explorer activity forensic analysis tool. NTLast is a security audit tool for Windows NT. Rifiuti is a Recycle Bin forensic analysis tool. See [http://www.foundstone.com/us/resources-overview.asp](http://www.foundstone.com/us/resources-overview.asp).

• **Guidance Software**—Guidance Software offers a number of EnCase products, including Enterprise, eDiscovery, Forensic, and Portable. For more information on all these products, see [http://www.guidancesoftware.com](http://www.guidancesoftware.com):

  - **EnCase Enterprise** allows the deepest level of visibility into laptops, desktops, file servers, and e-mail servers. Use it to investigate human resources matters or to quickly determine the root cause of suspicious network activity.

  - **EnCase eDiscovery** performs search, collection, preservation, and processing in a forensically sound manner. It collects and processes only potentially relevant data.

  - **EnCase Forensic** gives you the ability to image a drive and preserve it in a forensically sound manner. The EnCase evidence file format is a digital evidence container validated and approved by courts worldwide. EnCase Forensic also contains a full suite of analysis, bookmarking, and reporting features.

  - **EnCase Portable** is a pocket-sized USB data collection and triage solution. Even non-experts can use EnCase Portable so that specialists can focus on case management, processing, detailed analysis, and reporting.
• **ILookPI**—ILookPI is an advanced digital evidence toolset. It includes imaging software and also enables virus/Trojan search and identification. Its analysis features are designed to reduce investigative time while providing focus and clarity. See [http://www.perluckstro.com](http://www.perluckstro.com).

• **L0phtCrack**—L0phtCrack is password auditing and recovery software offered in three versions: L0phtCrack Professional, Administrator, and Consultant. See [http://www.l0phtcrack.com](http://www.l0phtcrack.com).

• **M-Sweep**—This tool can repeatedly overwrite ambient computer data storage areas. See [http://www.forensics-intl.com/msweep.html](http://www.forensics-intl.com/msweep.html).


  • **AnaDisk** software identifies data storage anomalies on floppy diskettes and generic hardware in the form of floppy disk controllers. BIOS are needed when using this software. AnaDisk works at a very low level and makes maximum use of the floppy diskette hardware. The software also has limited search capabilities, and you can use it to copy abnormal diskettes. Apply it as well to write data at a physical sector level and to format diskettes using any number of combinations.

  • **Filter_G** is a forensic English grammar filter utility used to quickly make sense of nonsense in the analysis of ambient data sources, e.g., Windows swap/page files, file slack, and data associated with erased files. Filter_G is a patented fuzzy logic filter that quickly identifies patterns of English language grammar in ambient data files. Use it as a sampling tool. It is particularly useful for evaluating Windows swap/page files.

  • **GFE Stealth**, NTI’s forensic graphics image file extractor, is a computer forensics software tool which was designed to automatically extract exact copies of graphics file images from ambient data sources and from SafeBack bit stream image backup files.

  • **SafeBack** creates mirror-image (bit-stream) backup files of hard disks or makes a mirror-image copy of an entire hard disk drive or partition.

  • **TextSearch Plus** is software that quickly searches hard disk drives, zip disks, and floppy diskettes for keywords or specific patterns of text. It operates at either a logical or physical level at the user’s option.

  • **CopyQM Plus** essentially turns a PC into a disk duplicator. In a single pass, it formats, copies, and verifies a disk. This capability is useful for system forensics specialists who need to preconfigure CDs for specific uses and duplicate them.

• **Norton Ghost**—Norton Ghost creates full system and file backups, including settings, applications, and files. It also restores from system failures and enables convenient, secure offsite backups. See [http://www.symantec.com/norton/ghost](http://www.symantec.com/norton/ghost).

• **Notes the Ripper**—This computer forensic and electronic discovery tool quickly and safely analyzes and extracts data from Lotus Notes NSF files. See [http://www.mykeytech.com](http://www.mykeytech.com).

• **Paraben Forensic Tools**—Paraben Forensic Tools produces a number of tools, including Device Seizure and P2 Commander. For more information on these tools, see [http://paraben.com/catalog/](http://paraben.com/catalog/):
  - **Device Seizure** is a forensic investigation tool for handheld devices.
  - **P2 Commander** is a comprehensive digital forensic tool. It examines e-mail and chat logs. Use it as well for file sorting and Internet file analysis.

• **pdd**—Pdd (Palm dd) is a Windows-based tool for memory imaging and forensic acquisition of data from the Palm OS family of PDAs. Pdd preserves the crime scene by obtaining a bit-by-bit image or snapshot of the Palm device’s memory contents. See [http://www.grandideastudio.com/portfolio/pdd](http://www.grandideastudio.com/portfolio/pdd).


• **SnapBack Exact**—This server-based backup and restore program for Windows servers features full open file management, remote administration, and backup scheduling. It copies an actual byte-by-byte copy of a server hard drive to tape while the backup is running and files are open and being modified. See [http://www.snapback.com](http://www.snapback.com).

• **Tech Assist, Inc. (Tools That Work)**—Tech Assist offers a variety of forensic software products, including BringBack, ByteBack, and Omniquad Detective. For information on all these tools, visit the Web at [http://www.toolsthatwork.com](http://www.toolsthatwork.com).
  - **BringBack** enables easy-to-use and highly successful file recovery for Windows and Linux operating systems. It also works on digital images stored on memory cards and more.
  - **ByteBack Data Recovery Investigative Suite** allows forensic examiners to recover data, repair logical damage, and verify the integrity of an investigation.
  - **Omniquad Detective** is a Windows-driven search-and-report utility. It can make searching for images and keywords simple and fast.

• **Technology Pathways Tools**—Technology Pathways offers the ProDiscover Family of tools, including Forensics and Incident Response. For more information on these tools, see [http://www.techpathways.com](http://www.techpathways.com):
  - **ProDiscover Forensics** is a Windows application for the collection, analysis, management, and reporting of evidence. It supports all Windows-based file systems in addition to file systems such as Sun Solaris UFS and Linux Ext 2/3.
  - **ProDiscover Incident Response** turns the ProDiscover Forensics workstation product into a client/server application. It allows disk preview, imaging, and analysis over any TCP/IP network. It also allows live disk preview, imaging, and analysis. In addition, it includes advanced tools for incident response to cyberattacks.
• **ThumbsDisplay**—This tool examines and reports on the contents of Thumbs.db files used by Windows. ThumbsDisplay prints a full-page version of thumbnail images without any other graphics programs being required. See [http://www.infinadyne.com/forensicsoftware.html](http://www.infinadyne.com/forensicsoftware.html).

• **ThumbsPlus**—This tool provides database and thumbnail organization, image viewing and editing, and folder and file organization. See [http://www.cerious.com/thumbnails.shtml](http://www.cerious.com/thumbnails.shtml).

• **Visual TimeAnalyzer**—Visual TimeAnalyzer automatically tracks all computer use and activities, including working time and pauses. It presents detailed, richly illustrated reports. See [http://www.neuber.com/timeanalyzer/](http://www.neuber.com/timeanalyzer/).

• **X-Ways Software Technology AG**—X-Ways produces a number of products, including Evidor, X-Ways Forensics, and WinHex. For more information on all these products, see [http://www.x-ways.net](http://www.x-ways.net):
  - **Evidor** searches text on hard disks and retrieves the context of keyword occurrences on computer media. It examines the entire allocated space as well as currently unallocated space and slack space. That means it even finds data from files that have been deleted if the files still exist physically.
  - **X-Ways Forensics**—X-Ways Forensics is an advanced work environment for system forensics examiners. It’s integrated with the WinHex hex and disk editor.
  - **WinHex** is a system forensics, data recovery, and IT security tool that includes a hex editor, disk editor, and RAM editor.

• **Zdziarski’s forensic guide for the iPhone**—Jonathan Zdziarski’s forensic technique for iPhones provides a way to make a bit-by-bit copy of the original media. By analyzing the image this method provides, discover a wealth of information that other tools can’t provide. Site access is freely available to full-time, active-duty law enforcement or military personnel tasked with mobile forensic imaging as part of their duties. See [http://www.iphoneinsecurity.com](http://www.iphoneinsecurity.com).

### Commercial Hardware Tools and Vendors

• **DIBS USA, Inc.**—DIBS USA, Inc., produces a range of computer forensics hardware and software. Its products are specifically designed to copy, analyze, and present computer data in a forensically sound manner. DIBS Mobile Forensic Workstation is for on-site collection and analysis of suspect computer data. DIBS Advanced Forensic Workstation is for laboratory-based collection and analysis of suspect computer data. DIBS Rapid Action Imaging Device (RAID) enables fast copying of suspect hard drives. See [http://www.dibsusa.com](http://www.dibsusa.com).

- **ForensicPC.com**—ForensicPC.com sells forensic workstations and forensic computer systems, including laboratory and portable stations. It also offers forensic acquisition devices, drive bays, tools, and kits. In addition, if offers write blockers and forensic software. See [http://www.forensicpc.com](http://www.forensicpc.com).

- **FRED (Forensic Recovery of Evidence Device)**—Digital Intelligence, Inc., produces devices, write blockers, networks, and the FRED family of forensic workstations. FRED workstations are integrated forensic processing platforms available in mobile, stationary, and laboratory configurations. These systems are designed for both the acquisition and examination of computer evidence. Digital Intelligence, Inc., products enable you to easily duplicate evidence directly from hard drives and other media in a forensically sound manner. See [http://www.digitalintelligence.com](http://www.digitalintelligence.com).

- **Intelligent Computer Solutions**—Intelligent Computer Solutions produces a wide variety of forensic products. Image MASSter Solo-4 is a high-speed, handheld hard drive duplication device. RoadMASSter-3 is a portable forensic station. Intelligent Computer Solutions also produces multi-drive duplicators, write protectors, and hard drive encryption products. See [http://www.ics-iq.com](http://www.ics-iq.com).

- **Kazeon**—Kazeon offers both software forensics products and hardware devices. The Information Server product line creates a content and metadata index, applies classification rules and policies, and enables automated or manual searching, reporting, and action on resulting data sets. Information Center allows corporations with distributed information to create groups of clusters to deliver administrators a data management capability across all Information Server installations. Information Center also allows a unified search and unified reporting capability across clusters. See [http://www.kazeon.com](http://www.kazeon.com).

- **Logicube**—Logicube provides hard drive duplication and computer forensics systems. Logicube’s hard drive cloning systems offer high-speed solutions for copying hard drives, drive formatting, data recovery, and disaster recovery. Logicube’s products include Echo Plus, SuperSonix, OmniClone Xi series, OmniSCSI, and OmniSAS hard drive duplicators. See [http://www.logicube.com](http://www.logicube.com).

- **MOBILedit**—MOBILedit! Forensic is a mobile phone investigation tool. It extracts all content from a device and generates a forensic report ready for courtroom presentation. See [http://www.mobiledit.com](http://www.mobiledit.com).

- **MyKey Technology, Inc.**—MyKey Technology, Inc., produces NoWrite FPU, a FireWire write blocker. It also produces NoWrite FlashBlock II, a write-blocker add-on for compact flash and digital media. See [http://www.mykeytech.com](http://www.mykeytech.com).

- **Paraben Forensic Tools**—In addition to forensic software, Paraben provides cell phone cable kits, hard drive lockdown devices, signal blocking bags, and other forensic hardware to support investigations. See [http://paraben.com/catalog/](http://paraben.com/catalog/).
• **Secure Kit for Forensics**—This software and hardware solution provides law enforcement, corporate security, and forensic consultants with logical data extraction of the content stored in a mobile phone. Susteen also provides Secure View Mobile, a standalone mobile forensics solution to extract mobile phone data at the touch of a button. See [http://www.susteen.com](http://www.susteen.com).

• **UFED (Universal Forensic Extraction Device) System**—CelleBrite UFED is a stand-alone device for use in the field as well as in the forensics labs. UFED can extract vital data, such as phonebook, pictures, videos, text messages, and call logs from 2,500 models of handsets sold worldwide. UFED system supports almost all mobile phones on the market today, including smartphones and PDA devices. UFED easily stores hundreds of phonebooks and content items onto an SD card or USB flash drive. Extractions can then be brought back to the forensics lab for review and verification using the reporting/analysis tool. See [http://www.cellebrite.com](http://www.cellebrite.com).

• **WiebeTech**—WiebeTech produces a variety of forensic products. USB WriteBlocker is for in-line USB write-blocking. RTX400-QR is a RAID in a portable enclosure. Forensic UltraDock is a quad-interface, write-blocking imager. Forensic Notebook DriveDock provides write-block access to 2.5-inch notebook drives via FireWire. HotPlug lets a forensic specialist move a computer to battery power and transport it elsewhere without ever shutting it down. WiebeTech also offers forensic field kits. See [http://www.wiebetech.com](http://www.wiebetech.com).
CHAPTER SUMMARY

This chapter discusses a variety of system forensics resources. It begins by discussing training and certifications available in the field of system forensics. It also lists other system forensics resources, such as user groups, conferences, and list servers. It provides URLs for forensic organizations and information sources, journals related to system forensics, and software and hardware forensics tools.

KEY CONCEPTS AND TERMS

Certification

CHAPTER 15 ASSESSMENT

1. A number of free system forensics certification programs are available.
   A. True
   B. False

2. EnCE stands for ________.

3. Which of the following is a government organization dedicated to computer investigations training, development, and delivery?
   A. IACIS
   B. HTCN
   C. EnCE
   D. DCITA

4. Being a member of a ________ is a good way for a forensic specialist to keep up with the latest tools and trends.

5. The field of system forensics is so young that not many resources exist.
   A. True
   B. False