Special Feature

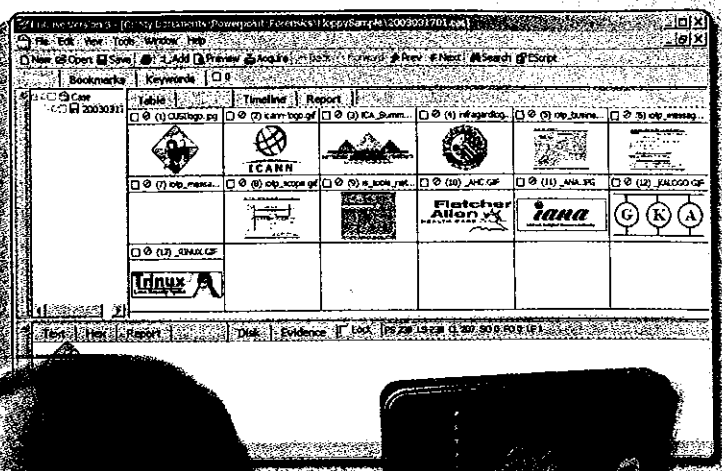
COMPUTER FORENSICS

Forensics is the use of science to investigate and establish facts in criminal or civil courts. Forensic scientists are able to examine a set of clues and rebuild a sequence of events. Computer forensics is the newest and fastest growing discipline in this field. As described earlier in Chapter 11, computer forensics — also called digital forensics, network forensics, or cyber-forensics — is the discovery, collection, and analysis of evidence found on computers and networks. Computer forensics techniques include analyzing log files, analyzing storage media (including deleted files), analyzing chat logs, and tracking the routes of packets on a data network (Figure 1). This field of study integrates aspects of criminal justice, computer science, and computer and network investigative techniques.

(a) Analyze Log Files

```
1) Mar 13 03:11:55 watson ipop3d[16319]: pop3
   service init from 192.168.187.35
2) Mar 13 03:11:55 watson ipop3d[16319]: Login
   user=kumquat host=holmes.example.net
   [192.168.187.35] nmsgs=0/0
3) Mar 13 03:12:16 watson ipop3d[16319]: Logout
   user=kumquat host=holmes.example.net
   [192.168.187.35] nmsgs=0 ndele=0
```

(b) Analyze Deleted Files



Computer Forensics Examiner

(c) Analyze Chat Logs

```
Session Start: Tue Mar 23 15:50:33 2008
Session Ident: #Strong&40
* Now talking in #Strong&40
* Topic is 'Welcome to the BEST little channel on the net!   www.40plus.com.html
* Set by Bunni on Tue Mar 23 10:31:01
<BettyF> It sure beats the 20's we've been having, Cary
<BettyF> Hi, billy
<billy89> Hi
<abc_m> hi Cary:)
<abc_m> hi billy89
<`Cary> hey cd  how  be?
<billy89> Hi
<abc_m> not bad a bit cold but doing okay
<BettyF> How ya doing, billy?
<billy89> So... I'm just lookin' around irc...
<BettyF> and lo and behold you found us
<billy89> Doin' ok... also cold where I am... Minnesota... Where're you?
<BettyF> Maine here
<billy89> Yep... here I am ... :-)
<abc_m> ottawa canada here
<billy89> Sunny Ontario! :-)
<BettyF> You had some really nasty spells in January, billy
<`Cary> I gotta go again.. laters  yawl.. play safe
* `Cary has left #Strong&40
<billy89> Bitter cold in Jan. dumped on by TWO bad snow storms in December
<BettyF> I talked with my old Ottawa friend a few days ago, cdn -- but only for
about a minute -- I think he had a date. lol
<abc_m> ohhhhhhhhhhhh
<abc_m> they have those out here?
<BettyF> I have a friend in St. Paul, billy -- she was in her house with her jacket
on in January.
```

(d) Track Packet Routes

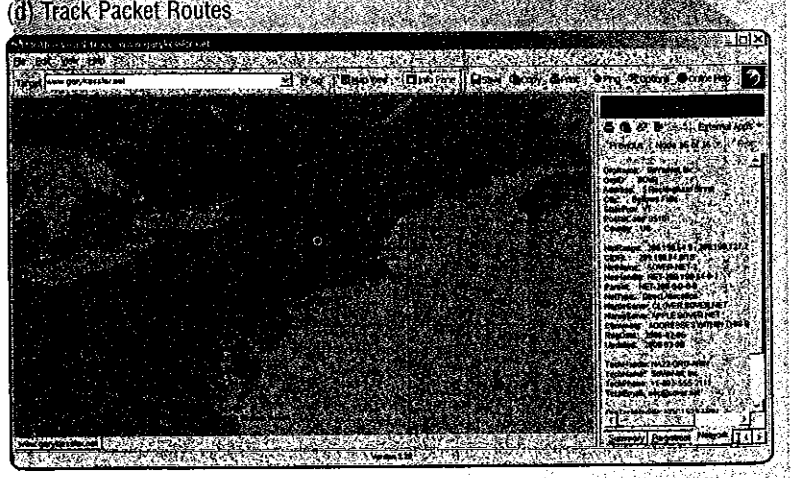


FIGURE 1 Computer forensics is the discovery, collection, and analysis of evidence found on computers and networks.

THE SCOPE OF COMPUTER FORENSICS

Computer forensics focuses on computers and networks. The forensic analysis of computers specifically involves the examination of computer media, programs, and data and log files to reconstruct the activity in which a computer was engaged, such as instant messaging conversations, Internet chats, e-mail messages, Web sites visited, documents and spreadsheets opened, and image and audio files viewed. The forensics analysis of networks focuses more on the activity of a network and includes the analysis of server contents, server and router log files, packet traffic, and information obtained from Internet service providers.

The science of computer forensics covers several overlapping areas (Figure 2). It is critical for law enforcement as an evidence gathering and criminal investigation tool. It is an increasingly important tool used for civilian and military intelligence gathering — including activities related to homeland security. It is becoming widely employed by businesses and other private sector organizations for combating information security attacks. The core tools and skills are the same regardless of the application.

A computer forensics specialist also must have knowledge of the law regardless of whether the investigation is for law enforcement or civilian purposes. Additional complexity in this area exists because computer crime statutes and users' legitimate expectation of privacy vary widely from state to state and nation to nation. With the Internet and World Wide Web, jurisdictional boundaries are blurred, and an individual in one country can commit crimes almost anywhere in the world without ever leaving his or her keyboard.

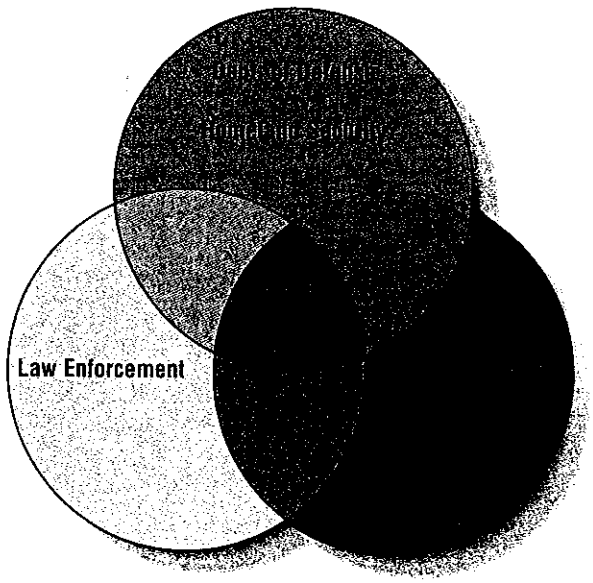


FIGURE 2 The domain of computer forensics is multidisciplinary, spanning the needs of the military and homeland security, law enforcement, and the private sector.

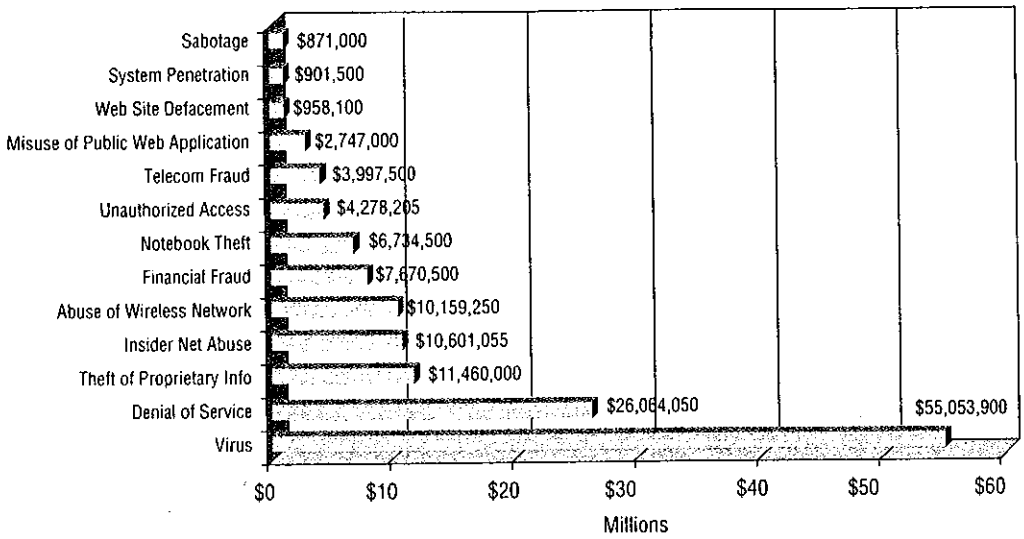
Although most computer forensic specialists today are engaged in law enforcement investigations, the field is not by any means limited to finding evidence of criminal guilt. Computer forensics also is a rapidly growing subspecialty for information security professionals. The traditional information security manager is responsible for proactively protecting the information technology assets within an organization. Security intrusions and other events are inevitable, however, and the computer forensics specialist often leads the incident response function to learn how an event occurred, who was behind it, and how to prevent a recurrence. Computer forensics techniques increasingly are being used by third-party firms for policy auditing and compliance enforcement for issues ranging from an organization's Appropriate User Policies (AUPs) to regulations such as Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

Computer forensics also is part of the toolkit of today's computer scientist. Many information security researchers purposely place a honeypot (vulnerable computer) on their networks for the specific purpose of analyzing the attacks that eventually will be perpetrated on those systems. Carefully examining the way in which a honeypot has been attacked can provide significant insight into new forms of attack, which then can be translated into new defensive tools and strategies.

THE IMPORTANCE OF COMPUTER FORENSICS

Computer forensics is a rapidly growing field for the simple reason that computers and the Internet are the fastest growing technology used for criminal activity. As computers become smaller, lighter, cheaper, and easier to use, they appear at nearly every crime scene that police investigate. Some activities, such as illegal gambling and the distribution of worms and viruses, have been given new life because of the pervasiveness of computers and the Internet.

Cybercrimes are growing rapidly in both the number of incidents as well as the cost in dollars, largely because these crimes are safer and more lucrative than crimes in the "real" world. The average bank robber, for example, nets only a few thousand dollars, and most are caught and sent to jail. Conversely, white collar computer crimes such as auction fraud, credit card theft, identity theft, and other financial scams tend to net a much larger sum of money, and the perpetrators are more difficult to catch and convict. In addition, computer criminals tend to generate more sympathy with judges, juries, and the public than violent offenders. Compounding the problem is the fact that access to corporate network resources makes insider jobs by employees easier and easier. Figure 3 shows the dollar loss reported by 269 large companies in a recent year due to telecom and financial fraud, insider abuse, unauthorized network access, theft of proprietary information, and other computer-related crimes.



Source: Computer Security Institute

FIGURE 3 Total computer security losses of $141,496,560 reported by 269 respondents in a recent year.

Computer forensics is being used not just to combat cybercrime. Terrorists around the world are known to use computers and other digital devices, so computer forensics analysis is important as an antiterrorism tool for both criminal prosecution and intelligence gathering. All organizations that employ computers, ranging from nonprofit agencies and major corporations to government agencies and utility companies, are at risk. As more information is stored digitally and more aspects of our society are under computer control, we all face increased exposure and vulnerability. Computer forensics is an important tool in understanding our digital information systems and keeping them safe, as well as tracking down the people who abuse those systems.

THE COMPUTER FORENSICS PROCESS

The computer forensics process can be simple or complex, depending upon the circumstances causing the investigation in the first place. The computer forensics specialist may be part of an investigative team, and the analysis of digital evidence may be just one part of the investigation as a whole. The specialist will look for information pertinent to the incident or event being investigated, which may be limited by a search warrant, time, and/or other circumstances.

The first step in the process is to gather the materials to analyze. This may not be quite as easy as it sounds. Law enforcement personnel will be guided by a search warrant in the seizure of materials while a corporate forensics specialist may be guided by what equipment is owned by the company. Even with clear guidelines, many items need to be considered for collection and examination as described in the following sections.

Computer Media

Computer media can be found in many places these days (Figure 4). This includes the obvious hard disk, Zip disk, floppy disk, and optical disc (CDs and DVDs). Also included are physically small, high-capacity memory devices such as USB flash drives (including the versions where the device is embedded in a watch, pen, or Swiss Army knife) and flash memory cards.

FIGURE 4 Computer forensics experts analyze the data stored on various types of media.

Computers and Peripherals

Every part of the computer needs to be considered for examination, and it is generally important to take possession of all of the equipment. The specialist cannot assume that the spare keyboard back in the lab will fit the computer being seized. The computer shown in Figure 5 has the basic hardware one might expect to see at a crime scene.

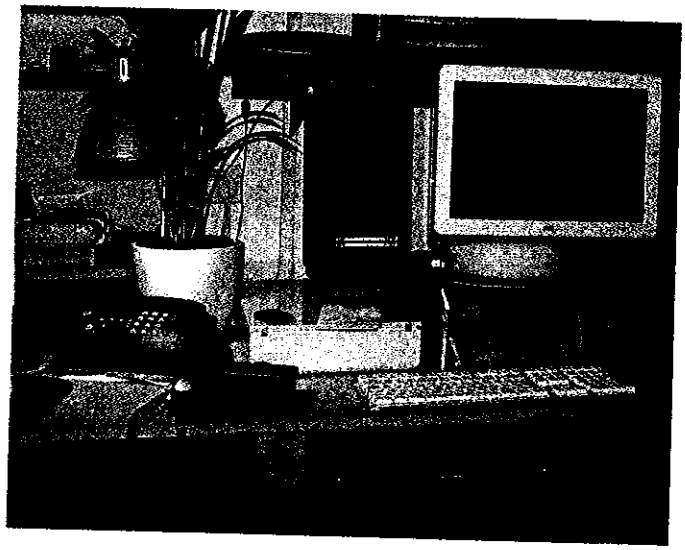


FIGURE 5 A typical scene a computer forensics specialist encounters.

Other Computer and Network Hardware

The word computer should be interpreted broadly in computer forensics to include not only traditional desktop, notebook, and server systems, but any digital device, including routers, digital cameras, mobile phones, and PDAs (Figure 6). Homes with broadband network connections increasingly have networks and, therefore, multiple computers and a router. Wireless networks make it relatively easy to hide a networked computer; a computer using a home's wireless network could be as far as 100 yards or so from the wireless access point, and thus be situated far outside of the immediate structure.

Computer Software

Although the computer forensics specialist generally will not run software directly from the suspect drive, it may be impossible to examine files without the proper application software. In some cases, the user of a suspect computer might have installed specialized, custom, or very old software to which the specialist generally will not have access; in that case, the specialist may have to install software found at the suspect site on a forensics lab computer. This is one reason to look around the site where the computer is found and consider seizing distribution media and manuals of any software with which the specialist is not familiar. The papers and books found near the computer also will give the specialist a clue as to the sophistication of the user and the possible types of applications to be found on the system.

FIGURE 6 Common digital hardware devices examined by a computer investigator.

In the Computer Forensics Lab

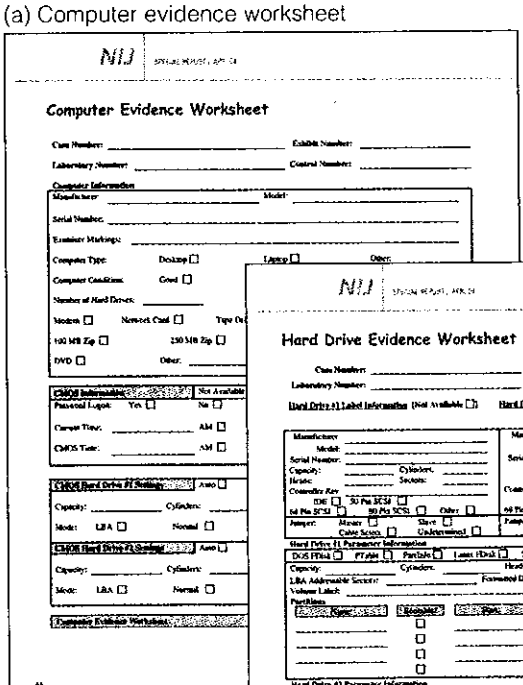
Once the materials are in the computer forensics lab, the investigation can begin. The basic steps of a computer forensics analysis are:

1. **Preserve the media** — Computer forensics analysis never should be performed on the original media except under the most extraordinary circumstances because of the potential of accidentally making a change to the original evidence. The copy also needs to be made in such a way that the original information is not altered in any way and that it can be authenticated as containing the same information as the original. This process is known as **imaging a drive**.
2. **Extract evidence** — Based upon the guidelines of the investigation, the specialist needs to determine what kind of information on the computer is pertinent to the case. Clues as to what to search for will depend upon the type of case. Spreadsheets, for example, would be highly relevant to a business fraud case, while images are important for a case of suspected child pornography, and chat and e-mail logs are of use in a case of cyberstalking. Keywords, such as pertinent phrases, slang words, names, locations, etc., must be provided to the computer forensics specialist on the case.
3. **Analyze computer media** — The actual analysis of evidence and/or the root cause of the event is the most time-consuming aspect of the process. It is important to note that the information retrieved from the computer either can be incriminating (indicating guilt) or exculpatory (indicating innocence). In addition, the specialist has to look at the entire capacity of the medium because information can be hidden anywhere. Figure 7 summarizes the common items examined during a computer forensics investigation.
4. **Document results** — The results of a computer forensics exam must be documented thoroughly, particularly if the examination is being performed for legal purposes. Everything must be written down, from the configuration of the computer and BIOS settings to each and every step taken by the computer forensic specialist and any pertinent evidence that is found. All computer equipment, media, peripherals, or other items seized must be logged, and photographs should be taken of external and internal connections, if possible. The handling of the evidence also has to be logged carefully to demonstrate that no tampering occurred. Sample computer forensics evidence worksheets are shown in Figure 8. Figure 8a is an evidence worksheet used with a computer. Figure 8b is an evidence worksheet used with a hard drive.

1. Visited Web sites
2. Downloaded files
3. Dates when files were last accessed and modified
4. Attempts to conceal, destroy, or fabricate evidence
5. Deleted or overwritten files
6. Data from RAM
7. Use of cryptography or steganography
8. File directory structure
9. Image, movie, and sound files
10. Keyword search hits
11. Contents of system files, such as the print spool and swap files
12. Installed programs
13. E-mail, chat logs, instant messaging logs
14. Registry entries
15. Contents of the Recycle Bin and unallocated space
16. Antivirus, personal firewall, and spyware detection software, as well as the presence of viruses, Trojan horses, and spyware

FIGURE 7 Common items examined during a computer forensics investigation.

(a) Computer evidence worksheet



(b) Hard drive evidence worksheet

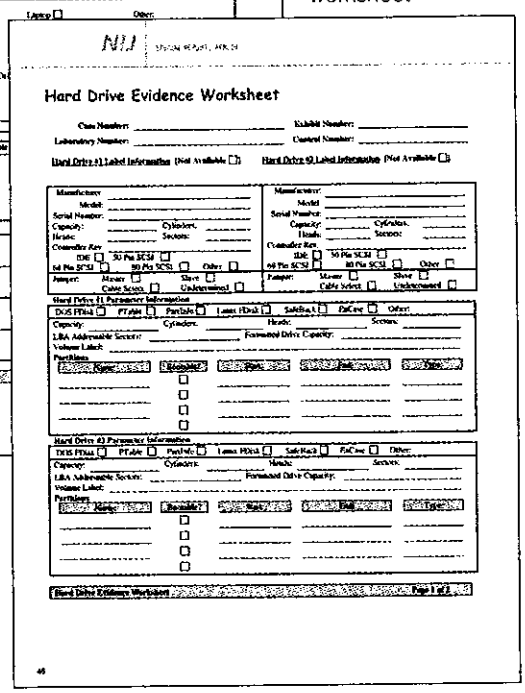


FIGURE 8 Computer Evidence and Hard Drive Evidence Worksheets (from *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, National Institute of Justice).

In general, specialized computer forensics tools are used to perform an analysis to ensure that no information is modified on the target media and that the examination is thorough. Booting a computer changes hundreds of registry, log, and/or data files; therefore, the original hard disk never should be used to boot a computer. In addition, many operating systems, such as Linux and Windows, maintain a number of time stamps associated with every file, including the creation, last access, and last modified dates; using ordinary operating system tools to examine the contents of files usually will cause at least the last-access date to be altered. Use of specialized analysis tools maintains the integrity of the original data so that the specialist can be sure that the results of the analysis are legally and technically valid. It is important that no harm be done to the original evidence.

In some cases, specialists prefer to image hard disks in the field rather than transporting entire computers to the lab; this often is the preferable approach when the device to be imaged is a company's critical server where seizing the computer might cause undue economic hardship to the owner. Devices such as Intelligent Computer Solutions' Road MASSter-II (Figure 10) is such a device; note that it fits in a small carrying case.

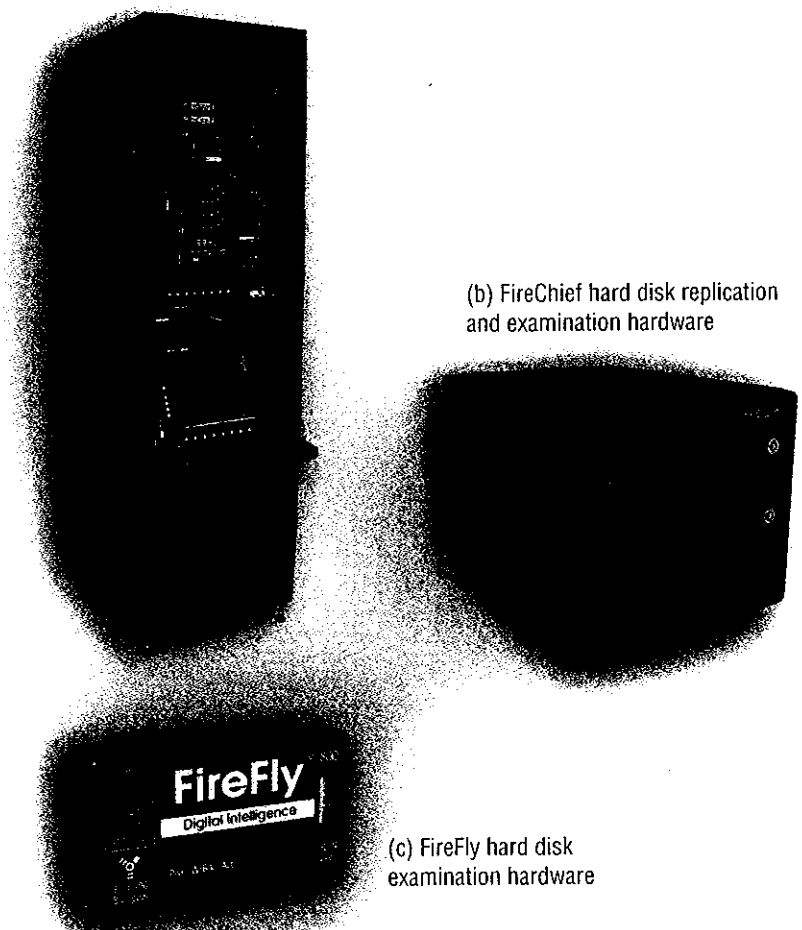
Notebook computers represent a particular challenge for forensic analysis because many notebook computer hard disks have proprietary or specialty interfaces; additional hardware is available specifically for imaging drives from various models of Dell, Gateway, HP, IBM, NEC, Toshiba, and other brands of notebook computers. Other specialized hardware allows for the imaging of PDAs, smart phones, and other digital devices.

COMPUTER FORENSICS TOOLS

A wide variety of computer forensics tools are available, each with its own applications, strengths, and weaknesses. Several companies make computer forensics hardware, primarily for purposes of disk imaging. Digital Intelligence, for example, makes several forensics hardware devices, including:

- The Forensic Recovery of Digital Evidence (FRED) hardware (Figure 9a) is a standalone forensics workstation that can acquire data from all types of hard disk media, including IDE, ATA, SATA, and SCSI hard disks as well as floppy and Zip disks. This system includes fixed hard disks for the workstation's operating system and analysis tools plus a number of bays for other drives to be inserted and removed. For imaging applications, the contents of the suspect disk are copied to a blank disk; the analysis then is performed on the newly copied disk.
- The FireChief hardware (Figure 9b) has two removable hard disk bays, one of which is write-protected (for the original disk). This device can be used to copy the contents of one disk to another. It is connected to a computer via a FireWire connection and is ideal for building a low-cost forensics workstation.
- The FireFly hardware (Figure 9c) can plug directly into an IDE or SATA hard disk and attach to the forensics computer via a FireWire connection.

(a) Forensic Recovery of Digital Evidence (FRED) forensics workstation



(b) FireChief hard disk replication and examination hardware

(c) FireFly hard disk examination hardware

FIGURE 9 Three computer forensics devices manufactured by Digital Intelligence, Inc.

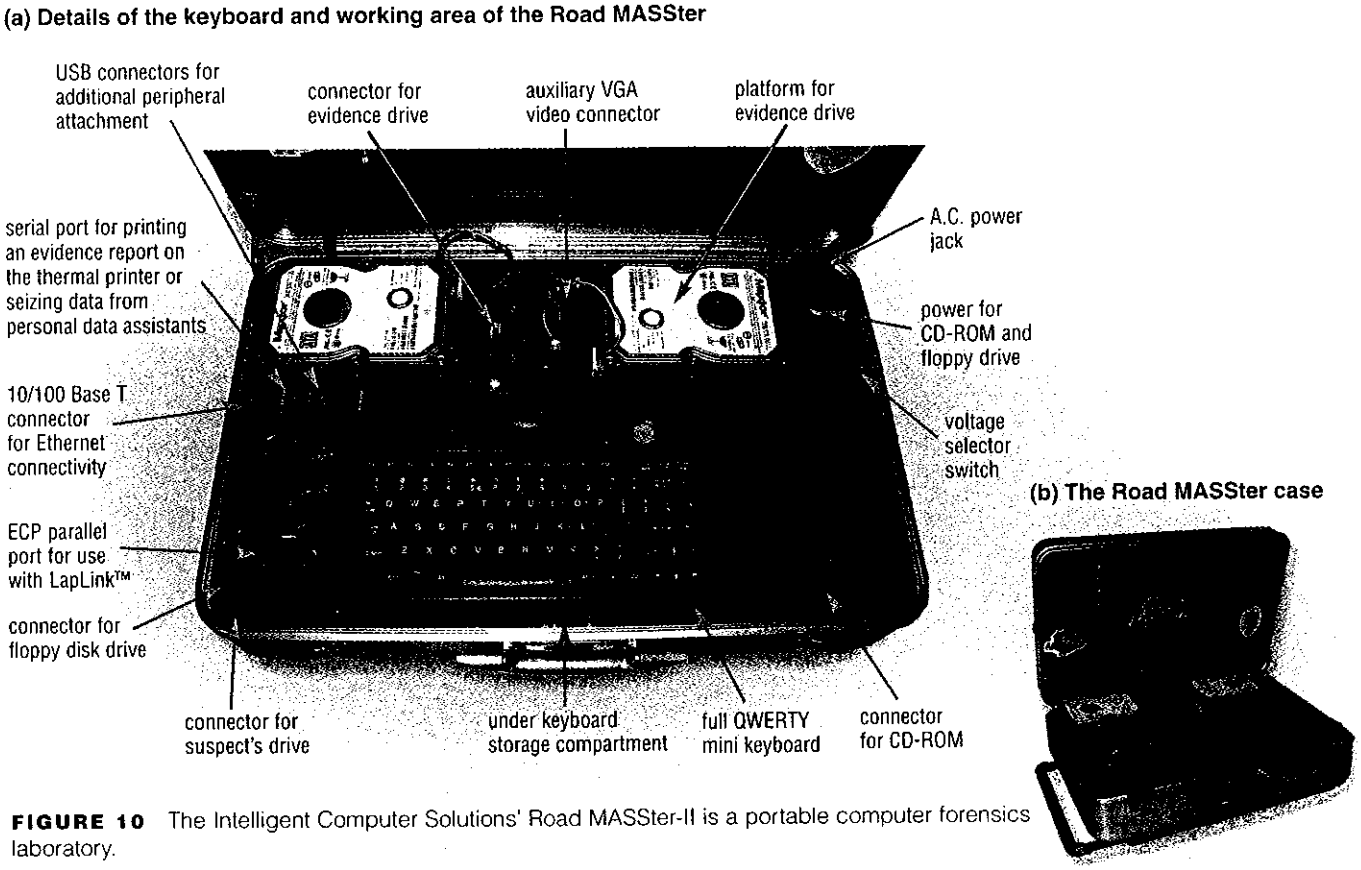


FIGURE 10 The Intelligent Computer Solutions' Road MASSter-II is a portable computer forensics laboratory.

The primary computer forensics analysis tool is software. The most widely-used specialty forensics programs today are Guidance Software's EnCase and AccessData's Ultimate Toolkit (Figure 11). No single program can perform all aspects of a computer forensics analysis, although several come close. These programs provide a broad range of forensics functions (Figure 12).

(a) Guidance Software's EnCase

(b) AccessData's Ultimate Toolkit

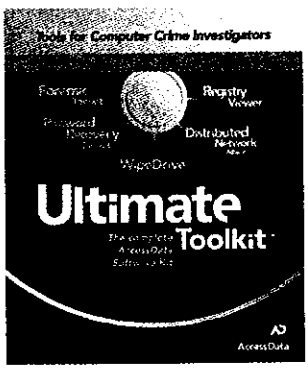


FIGURE 11 Popular computer forensics software.

1. Create disk images
2. Recover passwords
3. Perform file access, modification, and creation time analysis
4. Create file catalogs
5. View system and application logs
6. Determine the activity of users and/or applications on a system
7. Recover "deleted" files and examine unallocated file space
8. Obtain network information such as IP addresses and host names, network routes, and Web site information
9. Track forensics activity and aid in documentation and report writing

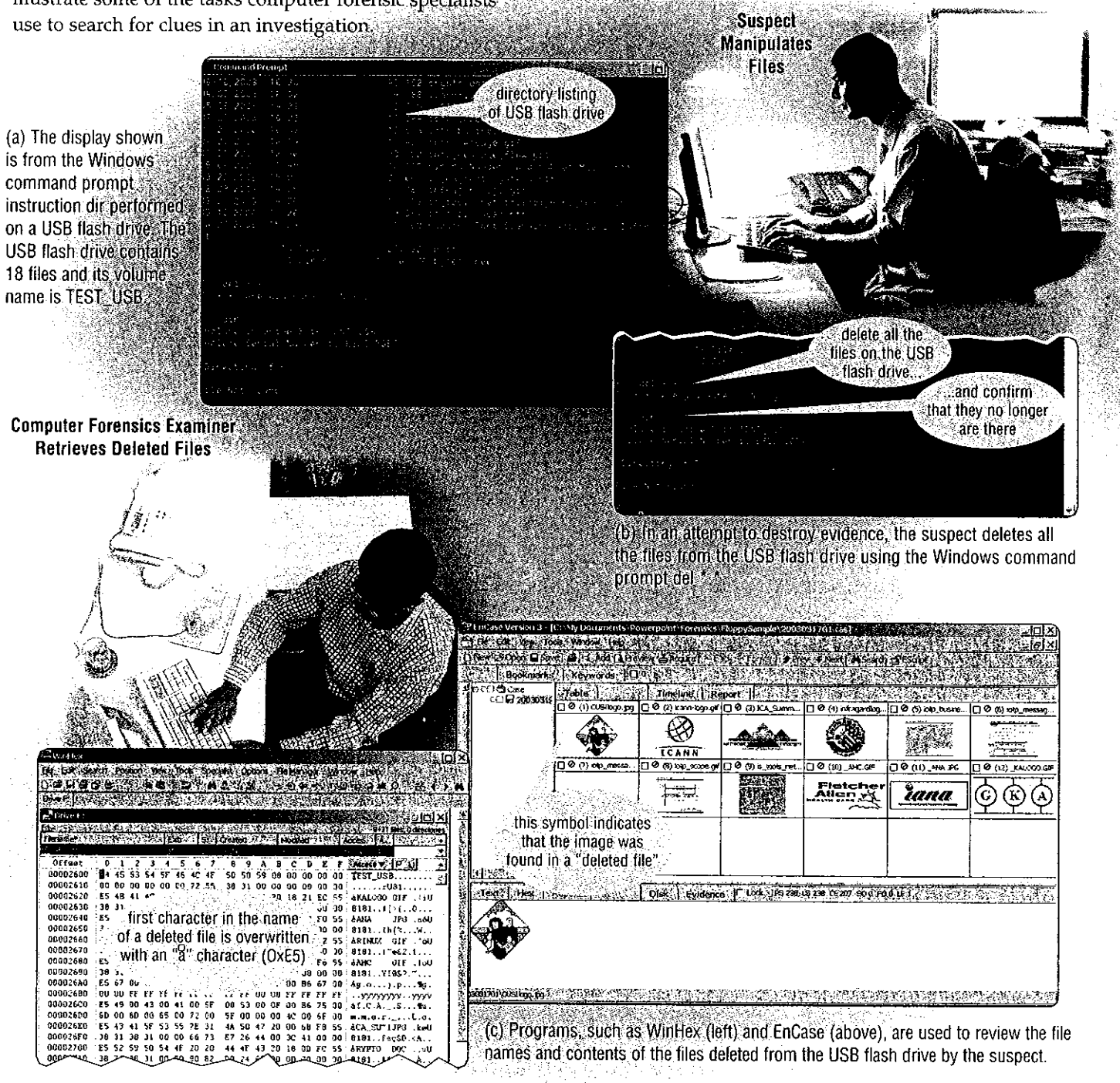
FIGURE 12 Common tasks handled by computer forensics software.

COMPUTER FORENSICS AT WORK

A computer forensics specialist needs to have a working knowledge of a wide range of topics related to computers and networks. The most essential bit of knowledge concerns how files are stored on storage media and the various file systems that will be found. The following sections illustrate some of the tasks computer forensic specialists use to search for clues in an investigation.

Analyzing Deleted Files

Consider the scenario shown in Figure 13. Figure 13a shows the suspect displaying the names of the files involved in the criminal activity. Figure 13b shows the suspect deleting the files. Figure 13c shows the computer forensics specialist using special programs to retrieve the deleted files.



(a) The display shown is from the Windows command prompt instruction dir performed on a USB flash drive. The USB flash drive contains 18 files and its volume name is TEST_USB.

(b) In an attempt to destroy evidence, the suspect deletes all the files from the USB flash drive using the Windows command prompt del *.*

(c) Programs, such as WinHex (left) and EnCase (above), are used to review the file names and contents of the files deleted from the USB flash drive by the suspect.

FIGURE 13 The top portion of this figure shows the suspect (a) listing the files involved in criminal activity, (b) later deleting the files in an attempt to cover-up the illegal activity, and then the lower portion of the figure shows (c) the computer forensics specialist retrieving the deleted files using special programs.

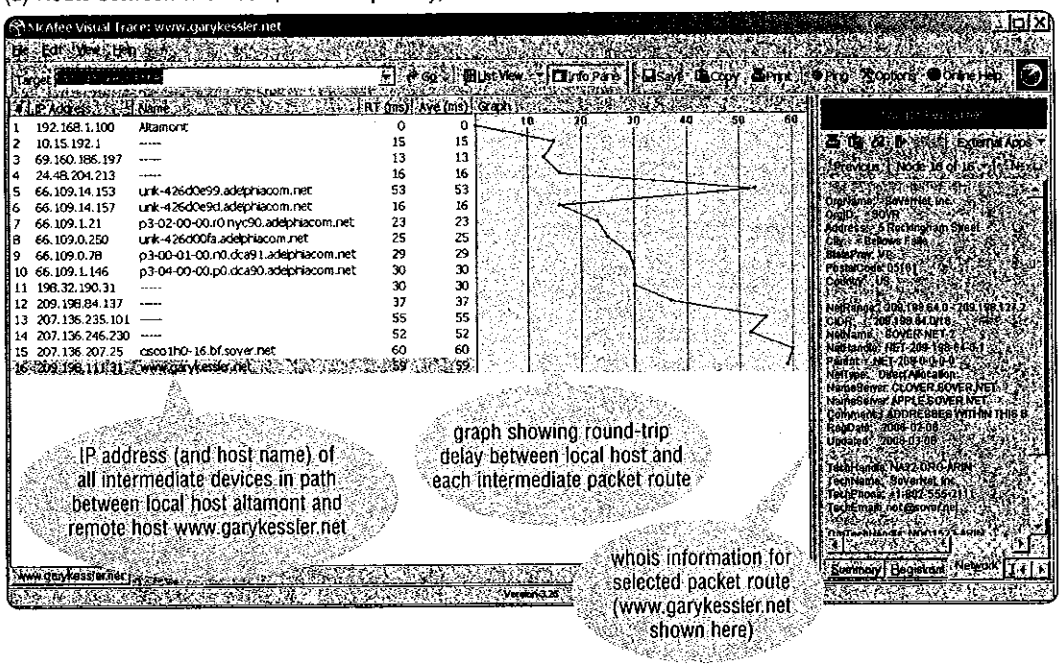
Tracking Packet Routes

Knowledge of the Internet is another essential skill. Figure 14a shows the output from McAfee's Visual Trace, listing the intermediate packet routes between a local host computer (altamont) and a Web server (www.garykessler.net). Visual Trace is a graphical version of the tracert (DOS) and traceroute (Linux) command line utilities and lists the IP address of all hops along the path between the two computers. This display also shows the round-trip delay and can be used to show whois information about each packet route in the path. Visual Trace also can show a geographical map of the path (Figure 14b).

Analyzing Network Traffic

The ability to analyze network traffic also is an essential skill for a computer forensics specialist. E-mail headers are particularly important, as they provide many clues as to the origin and authenticity of e-mail messages. By now you should be familiar with the standard e-mail headers, such as To:, From:, and Subject:. But e-mail headers contain more information than what you see at the top of an e-mail; e-mail headers also can reveal the name and version of the e-mail program you use, the operating system, the name and version of your mail server, internal IP addresses, and the mail server path taken by this message.

(a) Route between two hosts, round-trip delay, and whois information.



(b) Geographic map display of the route between two hosts.

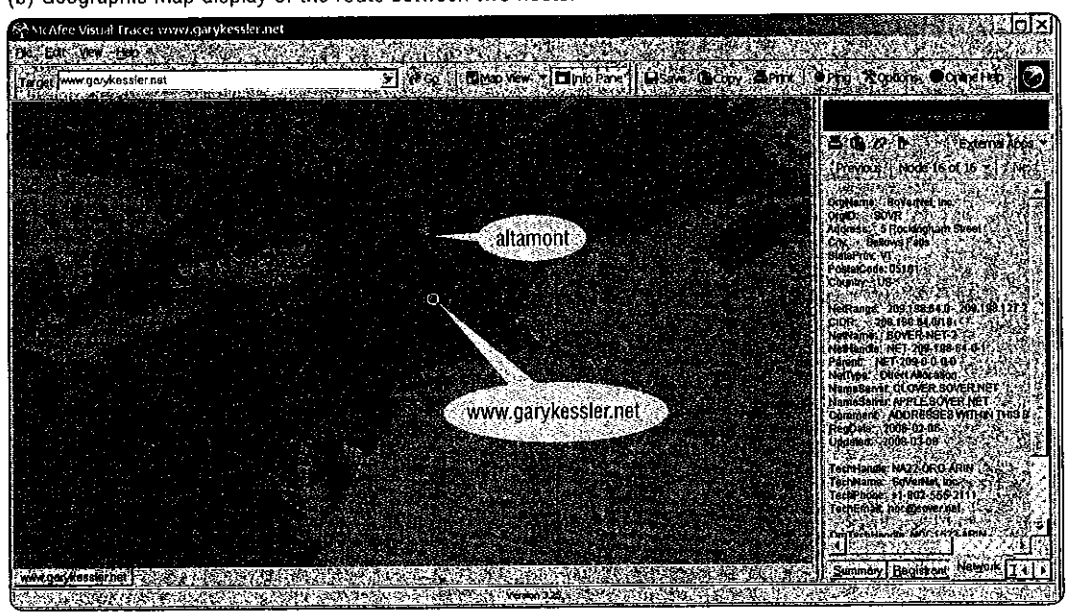


FIGURE 14 Tracing nodes between a local host computer (altamont) and a Web server using McAfee's Visual Trace.

Analyzing ISP Logs

During a computer forensics investigation, the specialist might request logs from an Internet service provider. The Internet service provider will deliver the logs, but they will be in the raw format in which they are saved.

While SMTP is used to forward e-mail across the Internet, other protocols are used to download e-mail by the client. One such protocol is the Post Office Protocol version 3 (POP3). Figure 1a on page 607 shows a set of three records from a POP3 server log showing a user logging on to check and download e-mail messages. All records show a date (March 13) and time stamp on a host named watson running the POP service (ipop3d) and access by a user on the host with IP address 192.168.187.35.

Analyzing Chat Logs

Analysis of chat logs is another important aspect of network analysis. The log shown in Figure 1c on page 607 is a conversation between BettyF, billy89, and other members of the Internet Relay Chat (IRC) Strong&40 channel. Although this conversation is relatively innocuous, analysis of logs such as these can turn up evidence of cyberstalking, criminal conspiracy, economic espionage, harassment, or other items of interest.

Analyzing a Packet Trace

Packet sniffers are an important software tool in the understanding of network traffic. A **packet sniffer** monitors all of the traffic seen on the network port of a computer and keeps a copy for later analysis. One of the most commonly used packet sniffers is tcpdump, a command line utility for UNIX/Linux; WinDump is the Windows version.

Analyzing Mobile Devices

Mobile phones, PDAs, and digital cameras increasingly are the focus of forensics examinations. Analysis of these devices is a growing subspecialty of computer forensics. In some ways, analysis of mobile devices is more problematic than analysis of traditional computers, because mobile devices have a large variety of physical connectors, operating environments, file structures, data formats, features, user interfaces, and operating modes. Mobile devices also can contain a variety of expansion cards ranging from flash memory to Subscriber Identity Module (SIM) cards.

LEARNING MORE ABOUT COMPUTER FORENSICS

Every action a user takes on a computer leaves a trail. Deleting files really does not erase information. Evidence of computer activity is stored in many places on the hard disk, some obvious and some very obscure. Information about network access potentially is logged on many computers throughout the local network and global Internet. Digital tracks are everywhere.

Computer forensics specialists must be technically knowledgeable and enjoy troubleshooting and solving puzzles. They must be aware of the legal constraints and organizational polices that guide what they can and cannot do.

Many sources for news and information about computer forensics are available online. Using the popular Web portals such as Google, Yahoo!, and others, you will find links to hundreds of computer forensics sites. Figure 15 lists sources for information about computer forensics and their Web addresses.

	WEB SITE	WEB ADDRESS
Computer Forensics Hardware Companies	Digital Intelligence, Inc.	digitalintelligence.com
	Intelligent Computer Solutions, Inc.	www.ics-iq.com
	WiebeTech	wiebetech.com
Computer Forensics Software	AccessData Corp. Ultimate Toolkit	accessdata.com
	Guidance Software EnCase	guidancesoftware.com
	STD — Security Tools Distribution	s-t-d.org
	SleuthKit & Autopsy	sleuthkit.org
	Technology Pathways ProDiscover	www.techpathways.com
	X-Ways Software Technology AG	winhex.com
Network Analysis Software	McAfee Personal Firewall Plus	us.mcafee.com
	tcpdump/libpcap	http://www.tcpdump.org
Additional Information	GCK Cybercrime and Cyberforensics-related URLs	www.garykessler.net/library/forensicsurl.html
	High Technology Crime Investigation Association (HTCIA)	htcia.org
	International Association of Computer Investigative Specialists (IACIS)	cops.org
	National White Collar Crime Center (NW3C)	nw3c.org

For an updated list, visit scsite.com/dc2008/ch11/computerforensics.

FIGURE 15 Online sources for information about computer forensics.