

Computer Investigations in the UC System

February 7, 2005

Albert Barsocchini, Director of Professional Services, is an attorney and recognized expert in computer law, electronic discovery and computer forensics. Over the past 4 years, he has consulted with law firms and corporate clients on computer forensics, electronic data productions, electronic records retention policies, incident response, and electronic risk control. He has written and lectured on Sarbanes Oxley, Graham Leach Bliley, H.I.P.A.A., F.E.R.P.A., Patriot Act, California SB 1386, and new S.E.C. and N.A.S.D. rules affecting data management. He served as Chairperson of the California State Bar's Law Practice Management & Technology Section in 2000, was a founding member of the California State Bar Cyberspace Law committee, and is an Editorial advisor to Law Technology News, and currently serves as a special master for the State Bar of California in search and seizure of privileged and confidential matters.

Brent Botta, Senior Computer Forensic Investigator. Upon achieving a Bachelor of Science degree in Computer Science in 1997, he was immediately hired by the Georgia Secretary of State's office as a Special Agent for a Major Fraud and Telemarketing White Collar Crime Unit as a computer forensic investigator. In 1999, Brent was employed by the Federal Bureau of Investigations (FBI) CART as a full time computer forensic examiner in which he was the forensic lead on more than 100 state and federal search warrants.

© 2004 Guidance Software, Inc. All Rights Reserved.

Taking Your Pulse

February 7, 2005

- How many of you are familiar with computer investigations?
- How many of you have specialized training in Computer forensic investigations?
- What percentage of your cases require a computer forensic response– 10%, 25%, 50% ?
- Of the cases that do trigger a computer forensics response, how important was the examination to the case – very little, somewhat or significant?

© 2004 Guidance Software, Inc. All Rights Reserved.

Computer Forensic Triggers

February 7, 2005

- Cyber stalking
- Financial Fraud
- Rogue Servers
- Identity Theft / phishing
- Sexual harassment
- Possession of Child Pornography
- Computer File Deletion / Destruction
- Unauthorized users/ intruders
- Vandalism & Viruses
- DoS attacks
- IP piracy
- SB 1386

© 2004 Guidance Software, Inc. All Rights Reserved.

2004 CSI/FBI Study

February 7, 2005

Conclusions from CSI/FBI Study:

- If you have a network, you will likely have an attack from outside
- Only 30% of respondents report incidents to law enforcement
- If you have employees, you will likely have a problem of internal abuse or attack
- Effective response and investigation over networks is needed to minimize losses
- Over \$70 million lost in the theft of proprietary information
- Over \$65 million lost in denial of service attacks
- Over \$27 million lost as the result of viruses

Since networks are now the tie that binds computers, network forensics is critical to any corporate investigation!

© 2004 Guidance Software, Inc. All Rights Reserved.

Why use Forensic Tools?

February 7, 2005



Your data “iceberg”

**The data found by common tools
(such as Explorer)**

**The additional data found by
EnCase Enterprise
(Deleted, renamed, hidden, difficult
to locate.)**

© 2004 Guidance Software, Inc. All Rights Reserved.

Goal of Forensic Investigations

February 7, 2005

- Conduct structured investigation
- Preserve and secure electronic data using methods that withstood judicial scrutiny
- Obtain all data potentially relevant to a matter
- Minimize cost and business disruption
- Obtain relevant information
- Document
- Integrate into litigation function

© 2004 Guidance Software, Inc. All Rights Reserved.

Goals of Incident Response

February 7, 2005

- Confirm whether an incident occurred
- Provide accurate, relevant, and timely information
- Implement controls to secure the crime scene
- Protect individual rights established by policy and law
- Minimize downtime and effect to business and network services
- Enable legal and law enforcement to prosecute malicious entities
- Provide recommendations to Sr. Management
- Understand, correct and protect from future compromise

© 2004 Guidance Software, Inc. All Rights Reserved.

Business Requirements of IR

February 7, 2005

- Business continues un-interrupted
- Evidence preserved quickly
- Reach well-informed decisions sooner
- Reach geographically dispersed systems
- Investigate on a need-to-know basis
- Follow a repeatable forensic methodology

© 2004 Guidance Software, Inc. All Rights Reserved.

Computer Forensics

February 7, 2005

The Two Methods For Conducting Computer Forensic Investigations

1. Stand Alone Static Forensics using EnCase: Remove the hard drive and image with EnCase utilizing a hardware write blocking device
2. Network Based Forensics using EnCase Enterprise: Image hard drive from remote without disrupting the user.

© 2004 Guidance Software, Inc. All Rights Reserved.

Limitations of Static Forensics

February 7, 2005

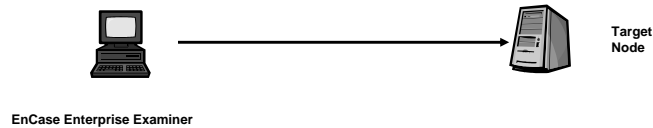
- Unable to avoid power down encryption lock of the entire drive, folders, removable media, etc.
- Unable to perform covert operations when physical access is not possible i.e. web cam, someone always home, etc.
- Difficult to isolate individual computers from a large network and only image those with a high target value
- Unable to preserve volatile data during an unauthorized access i.e. logs, temporary swap files, etc.

© 2004 Guidance Software, Inc. All Rights Reserved.

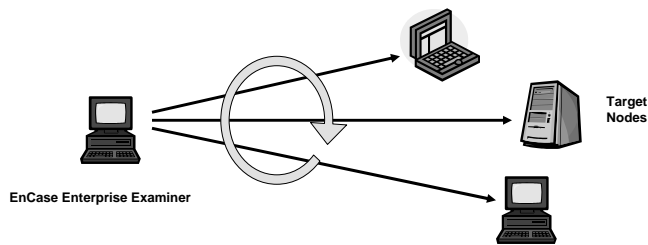
Network Enabled Forensics

February 7, 2005

Local analysis = 1 analyst : 1 target computer



Network-enabled analysis = "N" analysts : "N" target computers



© 2004 Guidance Software, Inc. All Rights Reserved.

Network Forensic Access

February 7, 2005

Accessing the target computer(s) across a network:

- Covertly load the small program called a "Servlet" onto the target computer(s) that can be easily removed with little or no footprints
- Install the hidden Servlet on the subject's computer so each time it boots it will allow access by the authorized forensics examiner

Experienced forensic investigators are necessary to properly deal with technical issues related to network architecture, speed and firewalls among other things.

© 2004 Guidance Software, Inc. All Rights Reserved.

Network Forensics

February 7, 2005

- Allow access to data without physical entry into a location
- Computer can remain on and in use
- Preserve and record volatile data
- Easily conduct covert operations
- Avoid power down encryption lock of the entire drive, folders, removable media, etc.
- Quickly preview and acquire a computer over the network from any location.
- Easily isolate individual computers from a large network and remotely image computers with a high target value
- Can use scripts to automate the investigation process
- Ability to trace linked events
- Establish a time line of events

© 2004 Guidance Software, Inc. All Rights Reserved.

Case Study - Hacking

February 7, 2005

The most common problem in a hack attack is preserving data in order to identify the intruder. EnCase Enterprise will perform a “SNAPSHOT” of the target computer.

This process records the following volatile data:

- Open Ports
- Running Processes
- Open Files
- Logged in Network Users

© 2004 Guidance Software, Inc. All Rights Reserved.

February 7, 2005

Questions?

Albert Barsocchini
Director of Professional Services
Guidance Software Inc.
2100 Powell Street, Suite 100
Emeryville CA 94608
415.760.0154

Brent Botta
Professional Services
Senior Forensic Consultant
Guidance Software Inc.

© 2004 Guidance Software, Inc. All Rights Reserved.

**A Guide for First Responders
National Institute of Justice
Annotated For Corporate Investigations By Gsi**

Albert Barsocchini, Esq.
Director of Professional Services
Guidance Software
2100 Powell Street, Suite 100
Emeryville CA 94608-1803
Phone: 415.760.0154
Fax: 510.652.5018

Overview

Each responder must understand the fragile nature of electronic evidence and the principles and procedures associated with its collection and preservation. Actions that have the potential to alter, damage, or destroy original evidence may be closely scrutinized by the courts.

The Latent Nature of Electronic Evidence

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence are latent. In its natural state, we cannot "see" what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations.

Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. This guide suggests methods that will help preserve the integrity of such evidence.

The Forensic Process

The nature of electronic evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, follow proper forensic procedures. These procedures include, but are not limited to, four phases: collection, examination, analysis, and reporting. Although this guide concentrates on the collection phase, the nature of the other three phases and what happens in each are also important to understand.

The collection phase involves the search for, recognition of, collection of, and documentation of electronic evidence. The collection phase can involve real-time and stored information that may be lost unless precautions are taken at the scene.

The examination process helps to make the evidence visible and explain its origin and significance. This process should accomplish several things. First, it should document the content and state of the evidence in its totality. Such documentation allows all parties to discover what is contained in the evidence. Included in this process is the search for information that may be hidden or obscured. Once all the information is visible, the process of data reduction can begin, thereby separating the "wheat" from the "chaff." Given the tremendous amount of information that can be stored on computer storage media, this part of the examination is critical.

Analysis differs from examination in that it looks at the product of the examination for its significance and probative value to the case. Examination is a technical review that is the province of the forensic practitioner, while analysis is performed by the investigative team. In some agencies, the same person or group will perform both these roles.

A written report that outlines the examination process and the pertinent data recovered completes an examination. Examination notes must be preserved for discovery or testimony purposes. An examiner may need to testify about not only the conduct of the examination but also the validity of the procedure and his or her qualifications to conduct the examination.

Introduction

When dealing with electronic evidence, general forensic and procedural principles should be applied:

- Actions taken to secure and collect electronic evidence should not change that evidence.
- Persons conducting examination of electronic evidence should be trained for the purpose.
- Activity relating to the seizure, examination, storage, or --transfer of electronic evidence should be fully documented, --preserved, and available for review.

What Is Electronic Evidence?

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. Such evidence is acquired when data or physical items are collected and stored for examination purposes.

Electronic evidence:

- Is often latent in the same sense as fingerprints or DNA evidence.
- Can transcend borders with ease and speed.
- Is fragile and can be easily altered, damaged, or destroyed.
- Is sometimes time-sensitive.

How Is Electronic Evidence Handled?

Precautions must be taken in the collection, preservation, and examination of electronic evidence.

Handling electronic evidence consists of the following steps:

- Identification of the evidence.
- Documentation.
- Collection and preservation of the evidence.
- Packaging and transportation of the evidence.

The information in this document assumes that the necessary legal authority to search for and seize the suspected evidence has been obtained.

Note: First responders should use caution when seizing electronic devices. The improper access of data stored in electronic devices may violate provisions of certain Federal laws, including the Electronic Communications Privacy Act. Additional legal process may be necessary. Because of the fragile nature of electronic evidence, examination should be done by appropriate personnel.

Electronic Devices: Types and Potential Evidence

Electronic evidence can be found in many of the new types of electronic devices available to today's consumers. This chapter displays a wide variety of the types of electronic devices commonly encountered, provides a general description of each type of device, and describes its common uses. In addition, it presents the potential evidence that may be found in each type of equipment.

Many electronic devices contain memory that requires continuous power to maintain the information, such as a battery or AC power. Data can be easily lost by unplugging the power source or allowing the battery to discharge. (Note: After determining the mode of collection, collect and store the power supply adaptor or cable, if present, with the recovered device.)

Computer Systems

Description: A computer system typically consists of a main base unit, sometimes called a central processing unit (CPU), data storage devices, a monitor, keyboard, and mouse. It may be a standalone or it may be connected to a network. There are many types of computer systems such as laptops, desktops, tower systems, modular rack-mounted systems, minicomputers, and mainframe computers. Additional components include modems, printers, scanners, docking stations, and external data storage devices. For example, a desktop is a computer system consisting of a case, motherboard, CPU, and data storage, with an external keyboard and mouse.

Primary Uses: For all types of computing functions and information storage, including word processing, calculations, communications, and graphics.

Potential Evidence: Evidence is most commonly found in files that are stored on hard drives and storage devices and media. Examples are:

User-Created Files

User-created files may contain important evidence of criminal activity such as address books and database files that may prove criminal association, still or moving pictures that may be evidence of pedophile activity, and communications between criminals such as by e-mail or letters. Also, drug deal lists may often be found in spreadsheets.

- Address books.
- Audio/video files.
- Calendars.
- Database files.
- Documents or text files.
- E-mail files.
- Image/graphics files.
- Internet bookmarks/favorites.
- Spreadsheet files.

User-Protected Files

Users have the opportunity to hide evidence in a variety of forms. For example, they may encrypt or password-protect data that are important to them. They may also hide files on a hard disk or within other files or deliberately hide incriminating evidence files under an innocuous name.

- Compressed files.
- Encrypted files.
- Hidden files.
- Misnamed files.
- Password-protected files.
- Steganography.

Evidence can also be found in files and other data areas created as a routine function of the computer's operating system. In many cases, the user is not aware that data are being written to these areas. Passwords, Internet activity, and temporary backup files are examples of data that can often be recovered and examined.

Note: There are components of files that may have evidentiary value including the date and time of creation, modification, deletion, access, user name or identification, and file attributes. Even turning the system on can modify some of this information.

Computer-Created Files

- Backup files.
- Configuration files.
- Cookies.
- Hidden files.
- History files.
- Log files.
- Printer spool files.
- Swap files.
- System files.
- Temporary files.

Other Data Areas

- Bad clusters.
- Computer date, time, and password.
- Deleted files.
- Free space.
- Hidden partitions.
- Lost clusters.
- Metadata.
- Other partitions.
- Reserved areas.
- Slack space.
- Software registration information.
- System areas.
- Unallocated space.

Components

Central Processing Units (CPUs)

Description: Often called the "chip," it is a microprocessor located inside the computer. The microprocessor is located in the main computer box on a printed circuit board with other electronic components.

Primary Uses: Performs all arithmetic and logical functions in the computer. Controls the operation of the computer.

Potential Evidence: The device itself may be evidence of component theft, counterfeiting, or remarking.

Memory

Description: Removable circuit board(s) inside the computer. Information stored here is usually not retained when the computer is powered down.

Primary Uses: Stores user's programs and data while computer is in operation.

Potential Evidence: The device itself may be evidence of component theft, counterfeiting, or remarking.

Access Control Devices

Smart Cards, Dongles, Biometric Scanners

Description: A smart card is a small handheld device that contains a microprocessor that is capable of storing a monetary value, encryption key or authentication information (password), digital certificate, or other information. A dongle is a small device that plugs into a computer port that contains types of information similar to information on a smart card. A biometric scanner is a device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, retina).

Primary Uses: Provides access control to computers or programs or functions as an encryption key.

Potential Evidence: Identification/authentication information of the card and the user, level of access, configurations, permissions, and the device itself.

Digital Cameras

Description: Camera, digital recording device for images and video, with related storage media and conversion hardware capable of transferring images and video to computer media.

Primary Uses: Digital cameras capture images and/or video in a digital format that is easily transferred to computer storage media for viewing and/or editing.

Potential Evidence:

- Images.
- Removable cartridges.
- Sound.
- Time and date stamp.
- Video.

Handheld Devices (Personal Digital Assistants [PDAs], Electronic Organizers)

Description: A personal digital assistant (PDA) is a small device that can include computing, telephone/fax, paging, networking, and other features. It is typically used as a personal organizer. A handheld computer approaches the full functionality of a desktop computer system. Some do not contain disk drives, but may contain PC card slots that can hold a modem, hard drive, or other device. They usually include the ability to synchronize their data with other computer systems, most commonly by a connection in a cradle (see photo). If a cradle is present, attempt to locate the associated handheld device.

Primary Uses: Handheld computing, storage, and communication devices capable of storage of information.

Note: Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (e.g., evidence custodian, lab chief, forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

Potential Evidence:

- Address book.
- Appointment calendars/information.
- Documents.
- E-mail.
- Handwriting.
- Password.
- Phone book.

- Text messages.
- Voice messages.

Hard Drives

Description: A sealed box containing rigid platters (disks) coated with a substance capable of storing data magnetically. Can be encountered in the case of a PC as well as externally in a standalone case.

Primary Uses: Storage of information such as computer programs, text, pictures, video, multimedia files, etc.

Potential Evidence: See potential evidence under computer systems.

Memory Cards

Description: Removable electronic storage devices, which do not lose the information when power is removed from the card. It may even be possible to recover erased images from memory cards. Memory cards can store hundreds of images in a credit card-size module. Used in a variety of devices, including computers, digital cameras, and PDAs. Examples are memory sticks, smart cards, flash memory, and flash cards.

Primary Uses: Provides additional, removable methods of storing and transporting information.

Potential Evidence: See potential evidence under computer systems.

Modems

Description: Modems, internal and external (analog, DSL, ISDN, cable), wireless modems, PC cards.

Primary Uses: A modem is used to facilitate electronic communication by allowing the computer to access other computers and/or networks via a telephone line, wireless, or other communications medium.

Network Components

Local Area Network (LAN) Card or Network Interface Card (NIC)

Note: These components are indicative of a computer network. See discussion on network system evidence in chapter 5 before handling the computer system or any connected devices.

Description: Network cards, associated cables. Network cards also can be wireless.

Primary Uses: A LAN/NIC card is used to connect computers. Cards allow for the exchange of information and resource sharing.

Potential Evidence: The device itself, MAC (media access control) access address.

Routers, Hubs, and Switches

Description: These electronic devices are used in networked computer systems. Routers, switches, and hubs provide a means of connecting different computers or networks. They can frequently be recognized by the presence of multiple cable connections.

Primary Uses: Equipment used to distribute and facilitate the distribution of data through networks.

Potential Evidence: The devices themselves. Also, for routers, configuration files.

Servers

Description: A server is a computer that provides some service for other computers connected to it via a network. Any computer, including a laptop, can be configured as a server.

Primary Uses: Provides shared resources such as e-mail, file storage, Web page services, and print services for a network.

Potential Evidence: See potential evidence under computer systems.

Network Cables and Connectors

Description: Network cables can be different colors, thicknesses, and shapes and have different connectors, depending on the components they are connected to.

Primary Uses: Connects components of a computer network.

Potential Evidence: The devices themselves.

Pagers

Description: A handheld, portable electronic device that can contain volatile evidence (telephone numbers, voice mail, e-mail). Cell phones and personal digital assistants also can be used as paging devices.

Primary Uses: For sending and receiving electronic messages, numeric (phone numbers, etc.) and alphanumeric (text, often including e-mail).

Note: Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (e.g., evidence custodian, lab chief, forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

Potential Evidence:

- Address information.
- E-mail.
- Phone numbers.
- Text messages.
- Voice messages.

Printers

Description: One of a variety of printing systems, including thermal, laser, inkjet, and impact, connected to the computer via a cable (serial, parallel, universal serial bus (USB), firewire) or accessed via an infrared port. Some printers contain a memory buffer, allowing them to receive and store multiple page documents while they are printing. Some models may also contain a hard drive.

Primary Uses: Print text, images, etc., from the computer to paper.

Potential Evidence: Printers may maintain usage logs, time and date information, and, if attached to a network, they may store network identity information. In addition, unique characteristics may allow for identification of a printer.

- Documents.
- Hard drive.
- Ink cartridges.
- Network identity/information.
- Superimposed images on the roller.

- Time and date stamp.
- User usage log.

Removable Storage Devices and Media

Description: Media used to store electrical, magnetic, or digital information (e.g., floppy disks, CDs, DVDs, cartridges, tape).

Primary Uses: Portable devices that can store computer programs, text, pictures, video, multimedia files, etc.

New types of storage devices and media come on the market frequently; these are a few examples of how they appear.

Potential Evidence: See potential evidence under computer systems.

Scanners

Description: An optical device connected to a computer, which passes a document past a scanning device (or vice versa) and sends it to the computer as a file.

Primary Uses: Converts documents, pictures, etc., to electronic files, which can then be viewed, manipulated, or transmitted on a computer.

Potential Evidence: The device itself may be evidence. Having the capability to scan may help prove illegal activity (e.g., child pornography, check fraud, counterfeiting, identity theft). In addition, imperfections such as marks on the glass may allow for unique identification of a scanner used to process documents.

Copiers

Some copiers maintain user access records and history of copies made. Copiers with the scan once/print many feature allow documents to be scanned once into memory, and then printed later.

Potential Evidence:

- Documents.
- Time and date stamp.
- User usage log.

Credit Card Skimmers

Credit card skimmers are used to read information contained on the magnetic stripe on plastic cards.

Potential Evidence: Cardholder information contained on the tracks of the magnetic stripe includes:

- Card expiration date.
- Credit card numbers.
- User's address.
- User's name.

Digital Watches

There are several types of digital watches available that can function as pagers that store digital messages. They may store additional information such as address books, appointment calendars, e-mail, and notes. Some also have the capability of synchronizing information with computers.

Potential Evidence:

- Address book.
- Appointment calendars.
- E-mail.
- Notes.
- Phone numbers.

Facsimile Machines

Facsimile (fax) machines can store preprogrammed phone numbers and a history of transmitted and received documents. In addition, some contain memory allowing multiple-page faxes to be scanned in and sent at a later time as well as allowing incoming faxes to be held in memory and printed later. Some may store hundreds of pages of incoming and/or outgoing faxes.

Potential Evidence:

- Documents.
- Film cartridge.
- Phone numbers.
- Send/receive log.

Global Positioning Systems (GPS)

Global Positioning Systems can provide information on previous travel via destination information, way points, and routes. Some automatically store the previous destinations and include travel logs.

Potential Evidence:

- Home.
- Previous destinations.
- Travel logs.
- Way point coordinates.
- Way point name.

Securing and Evaluating the Scene

Principle: The first responder should take steps to protect the integrity of all evidence, both traditional and electronic.

Policy: All activities should be in compliance with departmental policy and Federal, State, and local laws. (Additional resources are referenced in appendix B.)

Procedure: The first responder should visually identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. The first responder should evaluate the scene and formulate a search plan.

Conduct preliminary interviews:

Consistent with departmental policy and applicable law, obtain from potential witnesses:

- Owners and/or users of electronic devices found at the scene, as well as passwords (see below), user names, and Internet service provider.

- Passwords. Any passwords required to access the system, software, or data. (An individual may have multiple passwords, e.g., BIOS, system login, network or ISP, application files, encryption pass phrase, e-mail, access token, scheduler, or contact list.)
- Purpose of the system.
- Any unique security schemes or destructive devices.
- Any offsite data storage.
- Any documentation explaining the hardware or software installed on the system.

Evidence Collection

Principle: Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains.

Certain types of computer evidence, therefore, require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.

Policy: Electronic evidence should be collected according to departmental guidelines. In the absence of departmental guidelines outlining procedures for electronic evidence collection, the following procedures are suggested.

Stand-Alone and Laptop Computer Evidence

CAUTION: Multiple computers may indicate a computer network. Likewise, computers located at businesses are often networked. In these situations, specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. When a computer network is encountered, contact the forensic computer expert in your department or outside consultant identified by your department for assistance. Computer

systems in a complex environment are addressed later in this chapter.

A "stand-alone" personal computer is a computer not connected to a network or other computer. Stand-alones may be desktop machines or laptops.

Laptops incorporate a computer, monitor, keyboard, and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source. Therefore, they require the removal of the battery in addition to stand-alone power-down procedures.

If the computer is on, document existing conditions and call your expert or consultant. If an expert or consultant is not available, continue with the following procedure:

Procedure:

- a. Record in notes all actions you take and any changes that you observe in the monitor, computer, printer, or other peripherals that result from your actions.
- b. Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

Situation 1: Monitor is on and work product and/or desktop is visible.

1. Proceed to step c.

Situation 2: Monitor is on and screen is blank (sleep mode) or screen saver (picture) is visible.

1. Move the mouse slightly (without pushing buttons). The screen should change and show work product or request a password.
2. If mouse movement does not cause a change in the screen, DO NOT perform any other keystrokes or mouse operations.
4. Proceed to step c.

Situation 3: Monitor is off.

1. Make a note of "off" status.
2. Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.
 - c. Regardless of the power state of the computer (on, off, or sleep mode), remove the power source cable from the computer-NOT from the wall outlet. If dealing with a laptop, in addition to removing the power cord, remove the battery pack. The battery is removed to prevent any power to the system. Some laptops have a second battery in the multipurpose bay instead of a floppy drive or CD drive. Check for this possibility and remove that battery as well.
 - d. Check for outside connectivity (e.g., telephone modem, cable, ISDN, DSL). If a telephone connection is present, attempt to identify the telephone number.
 - e. To avoid damage to potential evidence, remove any floppy disks that are present, package the disk separately, and label the package. If available, insert either a seizure disk or a blank floppy disk. Do NOT remove CDs or touch the CD drive.
 - f. Place tape over all the drive slots and over the power connector.
 - g. Record make, model, and serial numbers.
 - h. Photograph and diagram the connections of the computer and the corresponding cables.

Computers in a Complex Environment

Business environments frequently have multiple computers connected to each other, to a central server, or both. Securing and processing a crime scene where the computer systems are networked poses special problems, as improper shutdown may destroy data. This can result in loss of evidence and potential severe civil liability. When investigating criminal activity in a known business environment, the presence of a computer network should be planned

for in advance, if possible, and appropriate expert assistance obtained. It should be noted that computer networks can also be found in a home environment and the same concerns exist.

The possibility of various operating systems and complex hardware configurations requiring different shutdown procedures make the processing of a network crime scene beyond the scope of this guide. However, it is important that computer networks be recognized and identified, so that expert assistance can be obtained if one is encountered. Appendix C provides a list of technical resources that can be contacted for assistance.

Indications that a computer network may be present include:

- The presence of multiple computer systems.
- The presence of cables and connectors, such as those depicted in the pictures at left, running between computers or central devices such as hubs.
- Information provided by informants or individuals at the scene.
- The presence of network components as depicted in chapter 1.

Other Electronic Devices and Peripheral Evidence

The electronic devices such as the ones in the list below may contain potential evidence associated with criminal activity. Unless an emergency exists, the device should not be operated. Should it be necessary to access information from the device, all actions associated with the manipulation of the device should be documented to preserve the authenticity of the information. Many of the items listed below may contain data that could be lost if not handled

properly. For more detailed information on these devices, see chapter 1.

Examples of other electronic devices (including computer peripherals):

- Audio recorders.
- Answering machines.
- Cables.
- Caller ID devices.
- Cellular telephones.
- Chips. (When components such as chips are found in quantity, it may be indicative of chip theft.)
- Copy machines.
- Databank/Organizer digital.
- Digital cameras (still and video).
- Dongle or other hardware protection devices (keys) for software.
- Drive duplicators.
- External drives.
- Fax machines.
- Flash memory cards.
- Floppies, diskettes, CD-ROMs.
- GPS devices.
- Pagers.
- Palm Pilots/electronic organizers.
- PCMCIA cards.
- Printers (if active, allow to complete printing).
- Removable media.
- Scanners (film, flatbed, watches, etc.).
- Smart cards/secure ID tokens.
- Telephones (including speed dialers, etc.).
- VCRs.
- Wireless access point.

Note: When seizing removable media, ensure that you take the associated device that created the media (e.g., tape drive, cartridge drives such as Zip(r), Jaz(r), ORB, Klik!(tm), Syquest, LS-120).

Packaging, Transportation, and Storage

Principle: Actions taken should not add, modify, or destroy data stored on a computer or other media. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and

magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, document its packaging, transportation, and storage.

Policy: Ensure that proper procedures are followed for packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

Packaging procedure:

- a. Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packaging.
- b. Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags.
- c. Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, and tapes.
- d. Ensure that all containers used to hold evidence are properly labeled.

Transportation procedure:

- a. Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- b. Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- c. Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt.
- d. Maintain the chain of custody on all evidence transported.

Storage procedure:

- a. Ensure that evidence is inventoried in accordance with departmental policies.
- b. Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.

Note: Be aware that potential evidence such as dates, times, and systems configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (e.g., evidence custodian, lab chief, forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

Forensic Examination by Category

The following outline should help identify the common findings of a forensic examination as they relate to specific crime categories. This outline will also help define the scope of the examination to be performed. (This information is also presented as a matrix at the end of this chapter.)

Computer Intrusion

- Address books.
- Configuration files.

- E-mail/notes/letters.
- Executable programs.
- Internet activity logs.
- Internet protocol (IP) address and user name.
- Internet relay chat (IRC) logs.
- Source code.
- Text files (user names and passwords).

Economic Fraud (Including Online Fraud, Counterfeiting)

- Address books.
- Calendar.
- Check, currency, and money order images.
- Credit card skimmers.
- Customer information/credit card data.
- Databases.
- E-mail/notes/letters.
- False financial transaction forms.
- False identification.
- Financial/asset records.
- Images of signatures.
- Internet activity logs.
- Online financial institution access software.

E-Mail Threats/Harassment/Stalking

- Address books.
- Diaries.
- E-mail/notes/letters.
- Financial/asset records.
- Images.
- Internet activity logs.
- Legal documents.
- Telephone records.
- Victim background research.

Extortion

- Date and time stamps.
- E-mail/notes/letters.
- History log.
- Internet activity logs.
- Temporary Internet files.
- User names.

Identity Theft

Hardware and software tools.

- Backdrops.
- Credit card generators.
- Credit card reader/writer.
- Digital cameras.
- Scanners.

Identification templates.

- Birth certificates.
- Check cashing cards.
- Digital photo images for photo identification.
- Driver's license.
- Electronic signatures.

- Fictitious vehicle registrations.
- Proof of auto insurance documents.
- Scanned signatures.
- Social security cards.

Internet activity related to ID theft.

- E-mails and newsgroup postings.
- Erased documents.
- Online orders.
- Online trading information.
- System files and file slack.
- World Wide Web activity at forgery sites.

Negotiable instruments.

- Business checks.
- Cashiers checks.
- Counterfeit money.
- Credit card numbers.
- Fictitious court documents.
- Fictitious gift certificates.
- Fictitious loan documents.
- Fictitious sales receipts.
- Money orders.
- Personal checks.
- Stock transfer documents.
- Travelers checks.
- Vehicle transfer documentation.

Software Piracy

- Chat logs.
- E-mail/notes/letters.
- Image files of software certificates.
- Internet activity logs.
- Serial numbers.
- Software cracking information and utilities.
- User-created directory and file names that classify copyrighted software.

At a physical scene, look for duplication and packaging material.

Telecommunications Fraud

- Cloning software.
- Customer database/records.
- Electronic Serial Number (ESN)/Mobile Identification Number (MIN) pair records.
- E-mail/notes/letters.
- Financial/asset records.

- "How to" manuals.
- Internet activity.
- Telephone records.

The following information, when available, should be documented to assist in the forensic examination:

- Case summary.
- Internet protocol address(es).
- Keyword lists.
- Nicknames.
- Passwords.
- Points of contact.
- Supporting documents.
- Type of crime.

END

COMPUTER SYSTEM WORKSHEET

--	--

		GSI File #:
Date:	Agency:	Agency Case #:
Site #:	Site Address: Room/Location ID:	
Examiner:		
Notes:		

Computer Description (Fill-in or Check all that apply)

Make: <input type="checkbox"/> None	Case Type	<input type="checkbox"/> Mini Tower <input type="checkbox"/> Mid Tower <input type="checkbox"/> Full Tower <input type="checkbox"/> Laptop <input type="checkbox"/> Desktop <input type="checkbox"/> All-In-One <input type="checkbox"/> Rack Mount <input type="checkbox"/> Other:
Model: <input type="checkbox"/> None	System Date	<input type="checkbox"/> Unk
Serial # <input type="checkbox"/> None	System Time	<input type="checkbox"/> Unk
OAN: <input type="checkbox"/> None	System Status	<input type="checkbox"/> On <input type="checkbox"/> Active <input type="checkbox"/> Suspended/Stand-by <input type="checkbox"/> Screen Saver Active <input type="checkbox"/> Off <input type="checkbox"/> No Power/Not Connected <input type="checkbox"/> Other:
Apparent OS <input type="checkbox"/> Unk	Active/Open Programs: (List all active and/or open programs – from taskbar) <input type="checkbox"/> None <input type="checkbox"/> N/A	
FROM <input type="checkbox"/> N/A <input type="checkbox"/> Start Button <input type="checkbox"/> Screen <input type="checkbox"/> Other:	1.	
Shutdown Method <input type="checkbox"/> Hard <input type="checkbox"/> Soft <input type="checkbox"/> Unknown <input type="checkbox"/> N/A <input type="checkbox"/> Other:	2.	
Shutdown Date & Time <input type="checkbox"/> N/A	Date:	3.
	Time:	4.

Peripherals & Connections (Check & Complete entries for all that apply. Fill in additional information, as appropriate)

☑	INTERFACE	DESCRIPTION	NOTES
<input type="checkbox"/>	RJ-45	NIC Interface	Note if Active
<input type="checkbox"/>	RJ-11	Telephone Modem	Note Phone Number, if Known
<input type="checkbox"/>	<input type="checkbox"/> EGA <input type="checkbox"/> VGA	Monitor	Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>	<input type="checkbox"/> PS/2 <input type="checkbox"/> AT	Keyboard	Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>	<input type="checkbox"/> PS/2 <input type="checkbox"/> AT	Mouse	Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>	<input type="checkbox"/> LPT <input type="checkbox"/> USB	Printer	Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>	<input type="checkbox"/> A/V	Speakers	Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>			Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>			Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>			Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>			Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>			Make/Model: _____ Serial No: _____ <input type="checkbox"/> NA
<input type="checkbox"/>	PASSWORD INFO:		

Additional Info – Continued on next page

CONFIDENTIAL

This document and its contents are property of the Guidance Software, Inc.
Distribution of this document or information contained herein is strictly prohibited without the express permission of GSI.
© 2003 GUIDANCE SOFTWARE, INC.



EVIDENCE CUSTODY CONTROL

Professional Services Division

CHAIN OF CUSTODY Cont.

GSI File #: _____

Page#: _____

Package #'s	Date/Time	Released By	Received By	Reason
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	