Computer Forensic
Evidence Collection and Management

Chapter 10

The Computer and Electronic Forensic Lab

Chapter Objectives

- Understand the functions of a computer and electronic forensic laboratory
- Identify the software, hardware, and personnel requirements for lab examinations
- Determine the infrastructure requirements of an electronic forensic laboratory
- Learn the training and certification requirements for lab examiners
- Look at the processed and tools required to identify and recover electronic evidence
- Understand the importance of documentation and chain-of-custody in the forensic process

Introduction

- Computer and electronic and forensic analysis is often useful in matters that, on the surface , seem unrelated to computer.
- In some cases, personal information containing evidence may have been stored on a laptop computer.
- Computer forensics is the user of specialized techniques for recovery, authentication,
- And analysis of electronic data in corporate, civil, and criminal cases.
- The forensic lab is the facility that provides these examinations.
- Specialized hardware and software products are utilized in investigation of computer system, electronic devices, or any device that contain a processor and memory in order to determine the who, what, where, when and how issues of usage.
- With the proliferation of scams and identity theft over the Internet and e-mail system, investigator are developing forensic techniques for tracking and identifying these criminals.
- The categories for forensic examination that can be conducted in the forensic lab include those involving e-mail, cell phones, hard drives, and any other electronic device that possesses a memory storage capacity.

Computer Forensic Issues

- Computer forensics also known as digital forensics, is concerned with preserving, recovering, and analyzing information stored within a digital medium.
- The purpose is to obtain information or evidence that can be used in a juridical review.
- Forensic experts examine computer systems in order to determine if they have been utilized for any activates that may be illegal or otherwise unauthorized.
- In order to ensure evidence is not destroyed or compromised in any way, forensic experts are careful not to handle the evidence more than necessary, as over handling can possibly change the data.
- Suspects of crimes that were conducted with the aid of digital devices may very well have installed countermeasures against forensic practices.
- Data gathered by a forensic specialist is rarely analyzed on the same machine from which it was obtained.
- Unique measures are also employed when shutting down a computer to not lose data.
- Experts are also on the lookout for traps such as intrusion detection devices and self-destruct mechanism.
- E-mail review is another technique to gather large amounts of digital evidence that could be in the body of the message or in attachments.
- More reviewers employ keyword search programs find relevant data and information.

Forensic Laboratories

- Many corporations, education institutions, and government departments are finding it necessary to establish an in-house electronic forensic laboratory.
- Internal electronic forensics laboratories can be an efficient and cost-effective way of handling routine incidents that are not likely to be referred to law enforcement for prosecution or that will require an expert witness testimony.
- If an organization decides to establish an internal lab, the capabilities should be reviewed by an outside source to validate compliance to industry and federal standards.
- A list of considerations and requirements that can assist in the decision-making process to develop an internal laboratory follows.
  - Personnel must qualify as expert witnesses in computer evidence processing
  - Staff must be properly trained in computer evidence processing procedures
  - Staff must be trained in computer evidence processing procedures
  - Staff must be trained on multiple tool types
  - Examiners must be certified
  - Staff must have sufficient depth to handle multiple cases
  - Multiple sets of tools must be available for investigations
  - Internal forensics capabilities must meet potential legal challenges
  - Computer processing power and media storage must be state-of-the-art
  - Evidence must be protected and accessible to only authorized personnel
  - The chain-of-custody must be maintained and documented.

Examining Computer Evidence

- Physical computer evidence can be represented by physical items.
- Computer evidence, while stored in these physical items, is latent and exists only in an abstract electronic form.
- Computer forensics also requires methods to ensure the integrity of the data and information contained within those physical items.
- Computer forensics examiners must utilize methods and techniques that provides valid, repeatable, and reliable results while protecting the real evidence from destruction or modification.
- The path an examiner takes in each case must be well documented and technologically sound for that particular case.
- The evidence is likely to be significantly different every time the laboratory receives an evidence.

Examining Computer Evidence

Procedures and Practices

- Computer and electronic evidence almost never exits in isolation
- Computer forensic science issues must also be addressed in the context of an emerging and rapidly changing technology environment.
- State, national and international law enforcement agencies recognize the need for common technical approaches.
- Principles of examinations are large-scale concepts that almost always apply to the examination.
- Organizational policy and practices are structural guidance that applies to the forensic examinations.
- Procedures and techniques employ software and hardware solutions to specific forensic problems.
- As an overall example. A laboratory may require that examinations be conducted, if possible and practical, on copies of the original evidence.
- An examiner responsible for duplicating the evidence must first decide on an appropriate level of verification to weigh time constraints against large file types.
- Having decided how vest to ensure the copying process will be complete and accurate, the next step is the actual task, which involves both procedures and techniques.

Procedures and Practices (Cont.)

Documentation and Reporting

- A major function of the forensic lab consists of documentation and reporting.
- There are so many steps required in these forensic examinations and investigations that it is very easy to overlook something important.
- Example of the forms include:
  - Evidence Receipt
  - Windows Examination
  - Windows Examination Checklist
  - Linux Examination
  - Linux Examination Checklist
  - Macintosh Examinations
  - Macintosh Examinations Checklist
  - Disk Imaging Exam
  - Imaging Checklist

Data Recovery versus Forensic Recovery

- Data frequently can be retrieved from a suspect computer.
- Computer forensics technicians employ sophisticated software to view and analyze information that cannot be accessed by the ordinary user.
- In order to determine whether a computer holds information that may serve as evidence, the examiner must first create an exact image of the drive.
- The mirror images are critical because each time someone powers up a computer, changes are automatically made to the files.
- Each agency and examiner must ensure that a copy is true and accurate and must make a decision as to how to implement this principle on a case-by-case basis.
- MD (Message Digest) is a computer algorithm that produces unique mathematical representation of the data.
- The selection of tools must be based on the character of the evidence rather that simply laboratory policy.
- Ensuring chain-of-custody is an important to the specialist who oversees drive imaging and evaluation of the data for its evidentiary value as it is in medical forensics.
- If a file or drive is changes, even in the smallest way, the hash code will also change.

Data Recovery versus Forensic Recovery (Cont.)

- In many cases, even when the user has defragged or reformatted a drive, evidence can still be retrieved.
- A computer forensics specialist with the right software and experience can recover most of what was of the disk before the reformation process took place.
- Particular programs, including Microsoft Word, retain facts about each document that they create, modify or access within the documents themselves.
- Computer forensics professional can retrieve metadata readily and learn all there is to know about the documents' past life.
- Data stored also includes temporary files and cookies.

Forensic Analysis

- The forensic analysis of a computer or electronic system revolves around a cycle of data gathering and processing of material and evidence gathered.
- Ideally the investigator wants an exact copy of the entire system and all its data, but there are roadblocks that prevent this.
- These sorts of problems are the reasons that traditional forensic analysis has focused on data from system that are not running at all.
- Reproducibility of results requires consistent mechanisms for gathering data and a good understanding of any side effect of the same.
- The examiner must also show that the process can be repeated multiple times, using different tools.
- Isolating the computer from other users and the network is the first step.

Forensic Analysis (Cont.)

- The life expectancy of data varies tremendously, going from picoseconds to years.

Table 10.1 Data Life Expectancy.

Registers, peripheral memory, caches, etc.	picoseconds
Main memory	nanoseconds
Network state	milliseconds
Running processes	seconds
Disk	minutes
Floppies, backup media, etc.	years
CD-ROMs, printouts, etc.	tens of years

- What is going on with all the bits stored on the computer system?
- Computer are busy, but most activity accesses the same data, programs, and other resources over and over again.
- Footprints form unusual activity stand out, providing data for forensic evidence.

Collecting Evidence Relating to Electronic Systems

- Suspects often try to avoid persecution by deleting files and data from their computers.
- When a files is deleted, several events take place on the computer.
- New available space is called free or unallocated space.
- It is only when the data is overwritten by new data that part or all of the files are no longer retrievable through normal forensic techniques.
- The usable space on computer hard drives id divided into sectors of equal size.
- When the information being stored will not use up all the space available in the designated sector(s), information that was previously stored on the hard drive remains in the unused part of the designated sector, in what is called *slack space*.
- Critical data contained in slack space is also recoverable using forensic technology.
- Computer system files contain valuable information that allows a forensic examiner to search for additional evidence.
- In many cases transactional evidence is available even if data has not been saved on the computers' hard drive.
- The operating system stores data in temporary locations on the computer.

Collecting Evidence Relating to Electronic Systems (Cont.)

Log Evidence

- Most computer and network devices, if programmed and configured properly, are capable of producing logs.
- Lost must have certain fundamental requisites for computer forensic purposes. These are:
  - Integrity
  - Time-stamping
  - Normalization
  - Data reduction
- The log file can be used n all types of investigation to establish types of transactions and the all-valuable time stamps.

Forensic Lab Function

- The cost to develop a forensic laboratory can be considerable.
- Most small law enforcement departments, consultants, and security departments cannot afford this expense.
- The FBI has published a document entitle Handbook of Forensic Services.
  - Computer examination could include the following activities:
  - Determine the type of data files in a computer
  - Compare data files to known documents and data files
  - Determine the time and sequence that data files were created
  - Extract data files from the computer or computer storage media
  - Recover deleted data files from the computer or computer storage media
  - Convert data files from one format to another
  - Search data files for a word or phrase and record all occurrences
  - Recover passwords and decrypt encoded files
  - Analyze and computer source computer code.
- Examinations can be conducted on commercial electronic devices, interception of communication devices, and miscellanies electronic devices and circuits.

Forensic Lab Function (Cont.)

Cyber-Intelligence

- There are new methodologies and goals relative to the new science of cyber-intelligence and how this discipline is being utilized to foster enhancements within the computer forensic community.
- Computer forensic is also increasingly being utilized to support not only traditional law enforcements functions, but also counter-intelligence, counter-terrorism programs as well.
- The following procedures are necessary:
  - Establish common baselines and definitions
  - Identify sources and means, as well as, develop capabilities that perform intelligence analysis
  - Provide and increased capacity to conduct cyber-forensic examinations
  - Ensure the greatest amount of the most relevant information possible is discovered during that same forensic examination process.
- Hardware and software technology that is contained in the computer forensic lab can be used to provide cyber-intelligence support to law enforcement.

Lab Design and Components

- Forensic laboratories can be designed for specific functions or can be generic in nature.
- There are a number of issues that relate to the overall design, physical construction, and security of the lab.
- If any evidence can be discredited, an attempt to do so will be made by opposing counsel.
- Negotiations with contractors can determine areas of responsibility.
- These include the following:

Environmental

- Protection of any evidence present in the forensic laboratory must have a high priority.
- A number of natural and man-made impediments can have a negative impact on this evidence if attention is not focused on the physical environmental components.

Lighting

- Using forensic workstation can result in a considerable amount of eyestrain.
- It is essential that proper lighting be installed in the forensic lab.
- The type of lighting is also an issue. As incandescent and fluorescent lights produce a different type of illumination.

Lab Design and Components (Cont.)

Electrical and Cabling

- Sufficient electrical power is required to run the forensic workstation and other equipment in the lab.
  - Separate 30-ampare circuit breaker
  - UPS
  - Surge Protector
  - Generator
- The physical construction of the lab examination areas must be according to specifications that lend themselves to electronic devices.
- A critical issue concerns electrostatic discharges.
- There are number of solutions available to prevent these problems and all are expensive.
- Examiners could become involved with electronic evidence that is based on *Tempest* standard.
- Tempest is a US government code word for a et of standards for limiting electro or electromagnetic rations emanations from electronic equipment.
- All cabling and wring can be run under a raised computer floor.

Lab Design and Components (Cont.)

Communications

- The lab must have both telephone and data communications capabilities.
- Consideration should be given to the security of these communication facilities.
- Firewalls and routers might be required to isolate the lab from the insecure Internet.

Fire Suppression

- A fire in the lab would certainly be a disaster.
- Fire suppression systems using chemicals can be installed instead of sprinklers.

Security and Safety

- Security policies must be in place for the lab and the personnel.
- Access control, login, and monitoring must be a high priority to ensure integrity of the evidence.
- A sign-in log must be maintained fro all visitors, maintenance personnel, contractors, and law enforcement.
- Visitors must not be allowed to be in a position to observe or touch any forensic evidence.

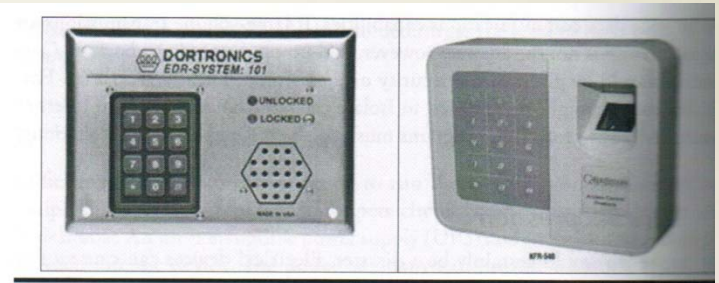


Figure 10.1 Entrance control devices.

Lab Design and Components (Cont.)

Storage

- Storage areas must be provided for supplies, forms, evidence, and tools.
- A storage room that can be locked would also be required for computer and electronic evidence.
- It is essential that lab management determine the characteristics of a safe storage container, cabinet, or room.
- Logs must be maintained on any movement or examination of evidence.
- The common storage area is also a good place to maintain a supply of forms for the department.
- All evidence must be secured in some type of cabinet, cage, or vault.
- Figured 10.2 depicts and evidence receipt that would be completed by the lab examiner and provided to the investigator handling the case.

Computer Evidence Receipt

Case Number:	Receipt Number:
Items Relinquished By / Title:	Date / Time:
Organization / Company:	Location / Address:

Computer(s):

Desktop	Laptop	Server	Hard Drive	Serial Number
☐	☐	☐	☐	
☐	☐	☐	☐	
☐	☐	☐	☐	

Storage Media:

CD-ROM	USB Media	Floppy / Zip	Tape	Subject
☐	☐	☐	☐	
☐	☐	☐	☐	
☐	☐	☐	☐	

Other Materials:

Items Received By / Title:	Signature:
Organization / Company:	Location / Address:

Page ___ of ___

Figure 10.2 Evidence receipt.

Lab Design and Components (Cont.)

Work Areas

- The configuration of the work area will depend upon the space available and the department's budget.
- Forensic workstation should have their won individual workspaces to avoid cross-contamination of evidence.
- Workstations for creating reports and accessing the Internet would require a separate workspace.
- Workbenches must be sturdy enough to support desktop computers and server devices.
- Network jacks would be required at the workbench for connectivity to the Internet and other private network.
- Additional measures include:
  - Appropriate packing materials
  - Wrist straps and foot-straps
  - Antistatic mats

Devices, Tools, and Supplies

- The primary investigative components include:

Forensic Workstation

- A decision must be made concerning the types(s) of forensic workstations(s) required in the lab.
- Requirements vary; however, a generic configuration is possible.
- Three majors types of computers could be the subject of forensic examinations: Windows/DOS, Macintosh, and UNIX.
- An easier approach is to purchase a turnkey solution. The digital recovery of evidence device (FRED) provides an example solution.

Turnkey Forensic Workstation

- FRED systems re optimized for stationary laboratory acquisition and analysis.
- FRED will acquire data directly from any hard drives and storage devices and save forensic images to DVD, CD,, or hard drives.
- FRED systems come with two high-capacity hard drives.
- With multiple boot menu options, FRED can be booted into data acquisition mode and PDBlock loaded automatically, write protecting the suspect hard drive.
- ALL FRED system can be connected directly to a network for use as standard workstation or file server why not processing or acquiring data;

Devices, Tools, and Supplies

- Software loaded on the FRED system includes the following:
  - MS DOS 6.223 (preinstalled and configured)
  - Microsoft Windows 98SE Standalone DOS (preinstalled and configured)
  - Microsoft Windows XP Pro (preinstalled and configured)
  - Suse Linux 9.1 Professional (preconfigured)
  - SystemWorks Pro 2003 (GHOST 2003 and DiskEdit)
  - DVD/CD Authoring Software
  - DriveSpy, Image, PDWipe, PDBlock, PART
- A list of generic specifications can be provided to a forensic-workstation provider if the design is to be outsourced.
- Costs will depend on the number of investigators and forensic examiners will be working in the lab.
- A model has been developed for a staff complement of four:
  - 15 Terabytes of raw storage in a SAN, fiber, Ethernet environment
  - Ability to handle any forensic format and OS
  - Imaging Systems
  - Forensic workstations
  - Physical storage areas
  - Mobile imaging and analysis kit
  - External hard drive inventory
  - Etc.

Devices, Tools, and Supplies

Supplies

- A variety of forms, crime scene materials, and packaging supplies must be available for the forensic investigation.
  - Supply of forms
  - Tamper-resistant bags – multiple sized
  - Evidence tape
  - Evidence tags
  - Evidence scales-6 inches
  - Multiple colors
  - Storage containers – multiple sizes
  - Credit card scale
  - Photo micrographic scales
  - Photo evidence markers

Devices, Tools, and Supplies

Toolbox and Tools

- the toolbox includes the components normally required when performing a forensic examination.
  - A startup kit would include the following:
  - Adapters, terminators, and cables.
  - Custom imaging work shelf
  - Security screwdrivers set

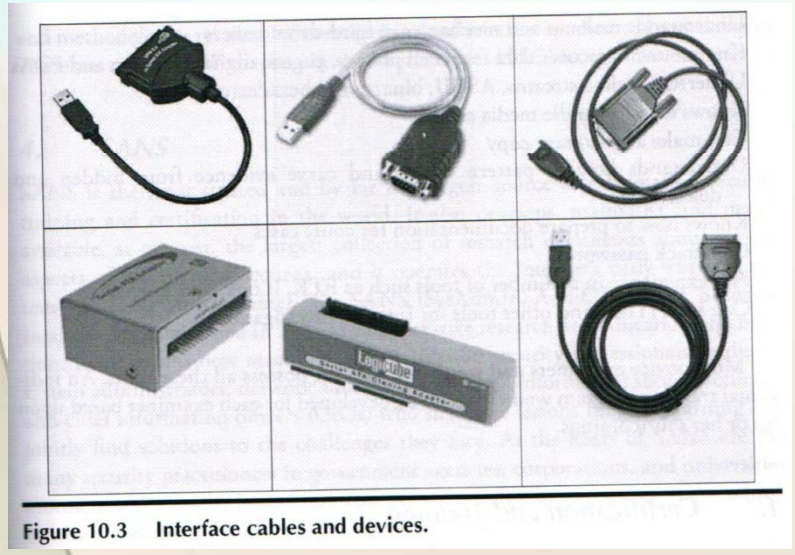


Figure 10.3 Interface cables and devices.

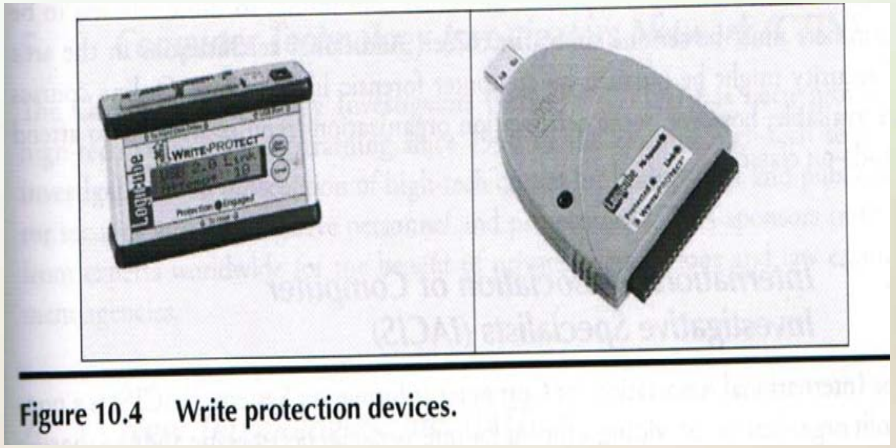


Figure 10.4 Write protection devices.

Training Forensic Lab Examiners

- Examiners must understand the chain-of-custody process and how their work might determine the outcome of a criminal proceeding.
- When looking at prospective examiners, a short list has been developed to assist in that identification process.
  - Works with Microsoft Windows, DOS, and Apple devices
  - Has experience in Linux, UNIX, or Perl
  - Understand makeup and mechanics of hard-drive devices
  - Knows how to recover data from cell phones, pagers, digital cameras, and PDAs
  - Understand data streams, ASCII, binary, ,and hexadecimal
  - Knows how to handle media safely
  - Can make a bit-stream copy
  - Understand how to pattern match and carve evidence from hidden and deleted files
  - Knows how to prepare documentation for court cases
  - Can crack passwords
  - Has experience in a number of tools such as FTK, iLook, and Encase
  - Can use HTML and other tools for the Internet investigation

Training Forensic Lab Examiners (Cont.)

Certification and Training

- A number of certifications offer certifications and training in the area of computer forensics.
- Additional certifications in the area of security might be pursued by computer forensic investigators.

International Association of Computer Investigative Specialist (IACIS)

- The IACIS is a non-profit organization providing a forum of interpersonal networking and the sharing of research, teaching, and technical information through an annual international conference and the quarterly scholarly publication, *Journal of Computer Information*.

High Technology Crime Investigation Association (HTCIA)

- The HTCIA is deigned to encourage, promote, and facilitate the interchange of data, experience, ideas and methodologies relating to investigations and security in advanced technologies.

Training Forensic Lab Examiners (Cont.)

SANS

- SysAdin, Audit, Network, Security (SANS) is the most trusted and by far the largest source of information security training and certification in the world.
- It develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning systems – Internet Storm Center.

Compute Technology Investigators Network (CTIN)

- SysAdin, Audit, Network, Security (SANS) is the most trusted and by far the largest source of information security training and certification in the world.
- It develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning systems – Internet Storm Center.

New Technologies, Inc. (NTI)

- NTI supports more than 8,000 law enforcement, military, government and business clients.
- This information has been posted to provide a ready source of information on various topics that are related to computer evidence, computer forensics, document discovery, ,computer incident response, and computer security risk management issues.

Training Forensic Lab Examiners (Cont.)

National White Collar Crime Center (NW3C)

- The mission of NW3C is to provide a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high tech crimes.
- Also to support and partner with other appropriate entities in addressing homeland security initiatives, as they relate to economic and high-tech crimes.

Certified Electronic Evidence Collection Specialist (CEESC)

- The CEECS certification is granted to those who successfully complete the CEECS regional certification course.
- This level of certification is also granted to those students in the Certified Forensic Computer Examiner course who successfully pass the written test.

Certified Forensics Computer Examiners (CFCE)

- The IACIS provides training for the external CFCE. This process is open to active law enforcement officers and others who qualify for memberships in IACIS.
- The process consists of the examination of six specially prepared examinations diskettes and a specially prepared hard disk drive.

Training Forensic Lab Examiners (Cont.)

Certified Computer Forensic Technician (CCFT) – Basic and Advanced

- The CCFT is one of four computer forensic certifications aimed at law enforcement and private IT professionals seeking to specialized in the investigative side of the field.
- Basic requirements include three years of experience, 18months for forensics experience, 40 hours of computer forensics training, and documented experience from at least 10 investigated cases.

EnCase Certified Examiner (EnCE)

- The EnCE program certifies both public – and private-sector professionals in the use of Guidance Software's EnCase computer forensic software.
- EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of ECASE during complex computer examinations.

Training Forensic Lab Examiners (Cont.)

Commercial Forensic Labs

- A number of commercial forensic labs provide services for digital forensics and digital data recovery.
- Digital forensic techniques can be performed on the following:
  - Blackberries
  - Cell phones
  - Computers
  - E-mails
  - Intrusion
  - Networks
  - PDAs
- Digital data recovery techniques can be performed on the following:
  - Computers
  - Cell phones
  - Deleted files
  - iPods
  - Flash cards
  - Passwords
  - USB drives
  - E-mails
- These companies provide information collection, extraction, and recovery functions.
- The types of cased worked on in both the commercial and criminal arenas include:
  - Theft of intellectual property
  - Employment deputes
  - Destruction/misappropriation of data
  - Alteration of data, alteration/misuse of programs
  - User of unlicensed software
  - Unauthorized access to a computer system
  - Unauthorized use of a company's computer for private gain
  - Etc.

Forensic Lab Tools

- The computer forensic lab should be equipped with imaging software, acquisition and seizure tools, hashing software, e-mail tracers, password recovery kits, and latent data recovery tools.

Software Tools:

- The Sleuth Kit: A collection of UNIX-based command line file and volume system forensic analysis tool. The tools allow for the recovery and analysis of deleted content, hash database lookups sorting by file type, and timelines of file activity.
- Autopsy: A graphical interface to the command line tools in the Sleuth Kit and allows to view deleted files, perform keyword searches and creates timelines of file activity.
- Netcat: It is a simple UNIX utility that reads and writes data across network connections using TCP and UDP
- dd: A common UNIX tool that copies data from one file to another.
- dcfl-dd: A modified version of the GNU binutils version of dd.
- Memdump: A memory dumper of UNIX-like systems
- Ethereal: it is used by network professionals round the world for troubleshooting, analysis, software and protocol development, and education. It has all of the standard features expected in a protocol analyzer, and several features not seeing any other product.

Forensic Lab Tools (Cont.)

- The Ilook Investigator Forensic Software: A comprehensive suite of computer forensic tools used to acquire and analyze digital media. Ilook investigator is provided free of charge only to qualifying person. Users must meet one of the criteria below:
  - Law enforcement
  - Government, state, or other regulatory agency
  - Military agencies
  - Government intelligence agencies
- Mac-Daddy: A Mac collector for forensic incident response. This toolset is a modified version of the two programs tree.pl and Mactime .

CRCMd5 Data Validation

- This program mathematically creates a unique signature for the contents of one, multiple, or all files on a given storage device.
- Such signatures can be used to identify whether the content of one or more computer files have changed.
- This program is also used to document that computer evidence has not been altered or modified during computer evidence processing.

Forensic Lab Tools (Cont.)

Forensic Tool Testing

- The National Institute of Standards and Technology (NIST) has developed a computer forensic tool testing methodology directed at digital data acquisition tools.
- There are tow critical measureable attributes of the digital source acquisition process.
  - Accuracy
  - Completeness
- The digital source may contain visible and hidden sectors.
- The accuracy and the completeness of the acquisition are influenced by several factors.
- To access the digital resource, the physical device containing the digital source needs to be connected to the computer by a physical interface.
- Another factor that influence the completeness of an acquisition is identifying the true size of the digital source.
- The need for these procedures was predicated on the critical need of law enforcement to ensure the reliability of computer forensic tools.

Photography

- Evidence an be identified, photographed, sequenced, and oriented using photo evidence markers and scales. .

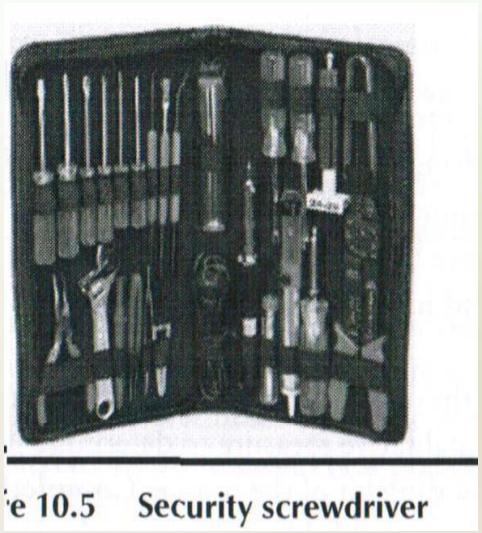
Forensic Lab Tools (Cont.)

Hardware Tools.

- Imaging products for hard drive can be either hardware or software based, or both.
- Logicube and Intelligent Computer Solutions (ICS) offer hardware/software based solution
- Logicube provides a system for hard drive duplication and computer forensics systems.
- ICS offers a number of products that perform hard dirk duplication.

Figure 10.6 Forensic toolkits.

Figure 10.7 Portable forensic devices.



e 10.5 Security screwdriver

Computer Forensic Lab Issues and Concerns

- There are a number of common elements and items that should be part of a computer forensics lab environment.
- A major concern of the forensic lab is security and integrity of the facility
- Written policies and procedures for lab controls, evidence control, forensic examinations, and validation of tools and equipment must be in place and available for personnel access.
- There should be a separate network connection for Internet access.
- There should be an central place to store documents
- Contingency planning and disaster recover planning must also be considered when operating a laboratory.
- Both the primary lab and the backup lab must ensure availability of hardware and/or software tools for:
  - Write protection
  - Acquisition
  - Data recovery/discovery
  - Internet history, images, e-mail
  - Password cracking
  - Mobile devices (PDA/cell phone)
  - Malware/virus detection
  - Binary analysis
  - Large storage analysis
  - Multifunction user

Computer Forensic Lab Issues and Concerns (Cont.)

Portable Flyaway kit

- A portable computer forensic flyaway kit would be an added enhancement to the lab if forensic investigations were to be conducted in the field.
- Items that might be included are as follows:
  - Policy and procedure documentation
  - Supplies of investigation forms
  - Evidence bags and packaging
  - Manual for tools utilized
  - Camera equipment with various lenses
  - Assorted hand tools
  - Storage media for capturing data
  - Hardware and software tools.
- Hardware and software tools need to provide the following functions:
  - Write protection
  - Acquisition
  - Data recovery/discovery
  - Internet history, images, e-mail
  - Etc.

Computer Forensic Lab Issues and Concerns (Cont.)

Lab Work Flow

- The flow of forensic evidence examinations and investigations must proceed in a predictable and orderly manner. The steps include the following:
  - Case initiation
  - Evidence processing
  - Forensic imaging
  - Preprocessing analysis
  - Forensic analysis
  - Report writing/briefing
  - Peer Review
  - Case archiving

Examinations

- Efforts have been made to collect a compendium of forms that are currently in use by a number of agencies in support of forensic investigations and examinations.
- Descriptions of these forms and checklists for documenting forensic processes follow:

Computer Forensic Lab Issues and Concerns (Cont.)

Chain-of-Custody Checklist

- Maintaining the chain-of-custody is one of the most important activities conducted in the investigation.
- Tasks to be competed include:
  - Crate unique case and evidence number
  - Document some assert tag or serial number that uniquely identifies the evidence
  - Document the make and model of system where the data was retrieved
  - Document BIOS time
  - Document location the evidence was found
  - Document physical description of evidence
  - Annotate notes for any accessed to the evidence before arriving
  - Annotate notes for any step that occurs outside of the normal process
  - Fill in history annotating when evidence was received and from whom
  - Update chain-of-custody for each action taken with the original evidence.

Computer Forensic Lab Issues and Concerns (Cont.)

Evidence Receipt

- An important document in the chain-of-custody process is the forensic evidence receipt.
- This form must be completed for each case and filed where it can be retrieved later for case support.
- Care must be made to ensure all information entered on this form is accurate

Hard Drive Examination

- One of the major activities in investigations involving computers in the imaging of the hard drive.
- Items of information concerning the hard drive that need to be identified and documented are as follows:
  - Make and Model
  - Serial number
  - Capacity and size
  - Cylinders and heads
  - Sectors
  - Jumper settings
  - Volume label
  - Number of partitions and names
- Imaging process information must also be identified.

Computer Forensic Lab Issues and Concerns (Cont.)

Imaging Checklist

- When performing the imaging operation on the hard drive, it is essential that all steps be successfully completed. Steps required are as follows:
  - Computer is powered off
  - Drive is removed and serial number recorder
  - System is booted with drive removed and BIOS time recorded
  - Chain-of-custody form filled out
  - Drive is imaged with forensically sound method
  - Chain-of-Custody updated
  - Drive either given back or taken with evidence receipt

Computer Forensic Lab Issues and Concerns (Cont.)

Windows Examination Checklist

- There are a number of steps to be employed when examining a computer with the windows operating system.
- Those steps that apply include the following:
  - Document the Windows version
  - Document the last boot time and last shutdown time
  - Identify and resolve the delta of “local” versus “real” date and time
  - Search the drive for remnants of file system partitions
  - Recover and examine log files
  - Search the drive for mail spools and Internet mail
  - Recover INF02 record and Internet history records
  - Carve documents from unallocated areas
  - Check the drive for wiping
  - Recover deleted files and printer spools
  - Recover SP-UserAssist records
  - Conduct keyword searches as appropriate
  - Decompress and examine archives

Computer Forensic Lab Issues and Concerns (Cont.)

Linux Examination Checklist

- Most steps for examining a Linux system are the same for those for the Windows system.
- Those steps that apply include the following:
  - Document Linux distribution and version
  - Document the last boot time and last shutdown time
  - Identify and resolve the delta of “local” versus “real” date and time
  - Check user shell history files
  - Recover and examine log files
  - Search the drive for mail spools and Internet mail
  - Recover Internet history records
  - Recover documents from unallocated areas
  - Check the drive for wiping
  - Recover deleted files and printer spools
  - Conduct keyword searches as appropriate
  - Decompress and examine archives
  - Examine swap space

Computer Forensic Lab Issues and Concerns (Cont.)

Macintosh Examination Checklist

- Most steps for examining the Mac are the same for those for the Windows system.
- Those steps that apply include the following:
  - Document the operating system version
  - Document the last boot time and last shutdown time
  - Identify and resolve the delta of “local” versus “real” date and time
  - Search the partition waste space for file system artifacts
  - Recover and examine log files
  - Search the drive for mail spools and Internet mail
  - Examine large files and image files
  - Recover Internet history
  - Carve documents from unallocated areas
  - Check the drive for wiping
  - Recover deleted files
  - Preprocess cache files and mbox files
  - Conduct keyword searches as appropriate
  - Decompress and examine archives

Auditing the Forensic Lab

- An audit function is required to ensure the forensic lab maintains a level of certification consistent with the courts requiems.
- Routine inspections should be conducted relating to the various policies and procedures of the lab.
- The audit should also include the following activities:
  - Check working orders of locks and entry devices
  - Review visitor logs and evidence storage logs
  - Inspect doors to ensure they close properly
  - Check the facility perimeter
  - Look at the general cleanliness and order the lab.