After reading this chapter and completing the exercises, you will be able to:

- Describe certification requirements for computer forensics labs
- List physical requirements for a computer forensics lab
- Explain the criteria for selecting a basic forensic workstation
- Describe components used to build a business case for developing a forensics lab
This chapter details some options for setting up an effective computer forensics laboratory. Each computer forensics investigator in a lab should also have a private office where he or she can manage cases, conduct interviews, and communicate without eavesdropping concerns. Whether you are new to computer forensics or are an experienced examiner, your goal is to make your office and lab work smoothly and efficiently for all casework.

Computer forensics investigators must remember to consider budget and time when updating their labs to keep pace with computer technology changes. The workflow and processes you establish directly affect the quality of evidence you discover. You must balance cost, quality, and reliability when determining the kind of equipment, software, and other items you need to add to your lab. This chapter provides a foundation for organizing, controlling, and managing a safe, efficient computer forensics laboratory.

### Understanding Forensics Lab Certification Requirements

A **computer forensics lab** is where you conduct investigations, store evidence, and do most of your work. You use the lab to house your instruments, current and legacy software, and forensic workstations. In general, you need a variety of computer forensics hardware and software to do your work.

You also need to make sure you have defined policies, processes, and prescribed procedures before beginning any casework to ensure the integrity of an analysis and its results. A number of organizations have created guidelines for devising your own processes and procedures. What’s most important is that you follow the policies and procedures you have created to ensure consistency in your output.

Be sure to research certifying bodies thoroughly before pursuing any certifications. Many certifications are offered by software vendors; others are specific for law enforcement or started by local groups.

The **American Society of Crime Laboratory Directors (ASCLD; [www.ascld.org](http://www.ascld.org))** provides guidelines to members for managing a forensics lab and acquiring crime and forensics lab certification. ASCLD also certifies computer forensics labs that analyze digital evidence as they do other criminal evidence, such as fingerprints and DNA samples. This certification is based on the original crime lab certification, ASCLD/LAB ([www.ascld-lab.org](http://www.ascld-lab.org)), which regulates how crime labs are organized and managed. The ASCLD/LAB program includes specific audits on all functions to ensure that lab procedures are being performed correctly and consistently for all casework. These audits should be performed in computer forensics labs to maintain the quality and integrity of analysis. The following sections discuss several key guidelines from the ASCLD/LAB program that you can apply to managing, configuring, and auditing your computer forensics lab.

### Identifying Duties of the Lab Manager and Staff

The ASCLD states that each lab should have a specific set of objectives that a parent organization and the lab’s director or manager determine. The lab manager sets up processes for managing cases and reviews them regularly. Besides performing general management tasks,
such as promoting group consensus in decision making, maintaining fiscal responsibility for lab needs, and enforcing ethical standards (covered in Chapters 15 and 16) among staff members, the lab manager plans updates for the lab, such as new hardware and software purchases.

The lab manager also establishes and promotes quality assurance processes for the lab’s staff to follow, such as outlining what to do when a case arrives, logging evidence, specifying who can enter the lab, and establishing guidelines for filing reports. To ensure the lab’s efficiency, the lab manager also sets reasonable production schedules for processing work.

A typical case for an internal corporate investigation involves seizing a hard disk, making forensic copies of it, evaluating evidence, and filing a report. A forensics analysis of a 200 GB disk, for example, can take several days and often involves running imaging software overnight and on weekends. This means one of the forensic workstations in the lab is occupied for that time, which can be 20 hours or more. Based on past experience, the lab manager can estimate how many cases each investigator can handle and when to expect a preliminary and final report for each case.

The lab manager creates and monitors lab policies for staff and provides a safe and secure workplace for staff and evidence. Above all, the lab manager accounts for all activities the lab’s staff conducts to complete its work. Tracking cases such as e-mail abuse, Internet misuse, and illicit activities can justify the funds spent on a lab.

Staff members in a computer forensics lab should have sufficient training to perform their tasks. Necessary skills include hardware and software knowledge, including OS and file types, and deductive reasoning. Their work is reviewed regularly by the lab manager and their peers to ensure quality. Staff members are also responsible for continuing technical training to update their investigative and computer skills and maintaining a record of the training they have completed. Many vendors and organizations hold annual or quarterly training seminars that offer certification exams.

The ASCLD Web site summarizes the requirements of managing a computer forensics lab, handling and preserving evidence, performing laboratory procedures, setting personnel requirements, and encouraging professional development. The site also provides a user license for printed and online manuals of lab management guidelines. ASCLD stresses that each lab should maintain an up-to-date library of resources in its field. For computer forensics, these resources include software, hardware information, and technical journals.

### Lab Budget Planning

To conduct a professional computing investigation, you need to understand the cost of your lab operation. Lab costs can be broken down into daily, quarterly, and annual expenses. The better you understand these expenses, the better you can delegate resources for each investigation. Using a spreadsheet program helps you keep track of past investigation expenses so that you can extrapolate expected future costs. Remember, expenses include computer hardware and software, facility space, and trained personnel.

When creating a budget, start by estimating the number of computer cases your lab expects to examine and identifying the types of computers you’re likely to examine, such as Windows PCs or Linux workstations. For example, suppose you work for a state police agency that’s planning to provide computing investigation services for the entire state. You could start by...
collecting state crime statistics for the current year and several previous years to determine how many computers were used to commit a crime and the types of computers used in these crimes. Criminal behavior often reflects sales trends for certain computing systems. Because more than 90% of consumers use Intel and AMD PCs, and 90% of these computers run Microsoft Windows, the same statistics are likely true of computers used in crimes. Verify this trend by determining how often each type of system is used in a crime. List the number of crimes committed using DOS/Windows, Linux/UNIX, and Macintosh computers.

If you can’t find detailed information on the types of computers and OSs used in computer crimes, gather enough information to make an educated guess. Your goal is to build a baseline for the types and numbers of systems you can expect to investigate. In addition to the historical data you compile, identify any future trends that could affect your lab, such as a new version of an OS or an increase in the number of computers involved in crime.

Next, estimate how many investigations you might conduct involving computer systems used less frequently to help determine how many tools you need to examine these systems. For example, if you learn that on average, one Macintosh computer running OS 9 or earlier is involved in a criminal investigation each month, you probably need only one or two software tools to conduct a forensic analysis on Macintosh file systems.

Figure 3-1 shows a table of statistics from a Uniform Crime Report that identifies the number of hard disk types, such as IDE or SCSI, and the OS used to commit crimes. Annual Uniform Crime Reports are generated at the federal, state, and local levels to show the types and frequency of crimes committed. For federal reports, see www.fbi.gov/ucr/ucr.htm, and for a summary of crimes committed at various levels, see www.ojp.usdoj.gov/bjs/dtd.htm.

You can also identify specialized software used with certain crimes. For example, if you find a check-writing software tool used in a large number of counterfeiting cases, you should consider adding this specialized software to your inventory.

If you’re preparing to set up a computer forensics lab for a private company, you can determine your needs more easily because you’re working in a contained environment. Start by obtaining an inventory of all known computing systems and applications used in the business. For example, an insurance company often has a network of Intel PCs and servers and specialized insurance software using a database for data storage. A large manufacturing company might use Intel PCs, UNIX workstations running a computer-aided design (CAD) system, super minicomputers, and mainframes. A publishing company might have a combination of Intel PCs and Apple Macintosh systems and a variety of word processing, imaging, and composition packages.

Next, check with your Management, Human Resource, and Security departments to determine the types of complaints and problems reported in the past year. Most companies using Internet connections, for example, receive complaints about employees accessing the Web excessively or for personal use, which generate investigations of Web misuse. Be sure to distinguish investigations of excessive Web use from inappropriate Web site access and e-mail harassment.

Your budget should also take future developments in computing technology into account because drive storage capabilities improve constantly. When examining a disk, you need a target disk to which you copy evidence data. This disk should be at least one and a half
times the size of the evidence (suspect) disk. For example, a lab equipped with 100 GB disks can effectively analyze disks up to 66 GB. If your company upgrades its computers to 200 GB disks, however, you need disks that are 300 GB or larger or a central secure server with at least 1 TB of storage. (Several forensic servers on the market are in the 20 TB and higher range.) Many businesses replace their desktop computer systems every 18 months to three years. You must be informed of computer upgrades and other changes in the computing environment so that you can prepare and submit your budget for needed resources.

Figure 3-1 Uniform Crime Report statistics
Like computer hardware, OSs change periodically. If your current computer forensics tool doesn’t work with the next release of a Microsoft OS or file system, you must upgrade your software tools. You should also monitor vendor product developments to learn about upgrades. File systems change, too. Forensics tools had their birth in DOS, and over the years, Windows hard disks evolved into a variety of file systems, including FAT16, FAT32, New Technology File System (NTFS), and Windows File System. Most DOS-based tools can’t read NTFS disks. Now investigators must also address Vista, which has caused problems even with Windows forensics tools. In addition, the popularity and prevalence of the Xbox requires that investigators be familiar with the FATX file system.

Time management is a major issue when choosing software and hardware to purchase. For example, you’ve decided to purchase eight machines for your lab. Many commercial forensics software packages require a USB dongle to operate or have a site license of five concurrent users. You or the budget manager must decide whether you’re using all the machines or need only two licensed copies of each software package. As another example, you can have a command-line tool running overnight for drive imaging; while it’s running; investigators can use a commercial or freeware package to evaluate a drive. You choices depend on what tools you have verified and what’s needed for your casework.

Another option is to use Helix (a Linux Live CD, discussed in Chapter 4) to view file systems, as it doesn’t mount the hard drive automatically and, therefore, doesn’t write to the drive. (A hardware write-blocker is still recommended to prevent errors caused by the forensics technician, if nothing else.) Examining PDAs, USB drives, and cell phones is routine now in cases from criminal investigations to civil litigation discovery demands. Computer investigators must be prepared to deal with constant change in these devices and know what tools are available to safely extract data from them for an investigation. In Chapter 13, you learn how to acquire data from these devices.

**Acquiring Certification and Training**

To continue a career in computing investigations and forensic analysis, you need to upgrade your skills through training. Several organizations have developed or are currently developing certification programs for computer forensics that usually test you after you have completed one or more training sessions successfully. Certifying organizations range from nonprofit associations to vendor-sponsored groups. All these programs charge fees for certification, and some require candidates to take vendor- or organization-sponsored training to qualify for the certification. More recently, some state and federal government agencies have been looking into establishing their own certification programs that address the minimum skills for conducting computing investigations at various levels.

Before enlisting in a certification program, thoroughly research the requirements, cost, and acceptability in your chosen area of employment. Most certification programs require continuing education credits or reexamination of candidates’ skills, which can become costly.

**International Association of Computer Investigative Specialists (IACIS)**

Created by police officers who wanted to formalize credentials in computing investigations, IACIS is one of the oldest professional computer forensics organizations. It restricts membership to sworn law enforcement personnel or government employees working as computer forensics examiners. This restriction might change, so visit the IACIS Web site (www.iacis.com) to verify the requirements.
IACIS conducts an annual two-week training course for qualified members. Students must interpret and trace e-mail, acquire evidence properly, identify OSs, recover data, and understand encryption theory and other topics. Students must pass a written exam before continuing to the next level. Passing the exam earns the status of Certified Electronic Evidence Collection Specialist (CEECS). The next level of training is completed through a correspondence course lasting up to one year. The IACIS certification process for this level consists of examining a variety of media and completing a written test. Some media must be examined by using a command-line tool. The testing agency plants files on these media that you must find, including easy-to-find items, data in unallocated space, RAM slack, file slack, and deleted files. Cell phones, PDAs, and other digital devices are being added as the field broadens.

Other topics include data hiding, determining file types of disguised files, and accessing password-protected files. You might also be asked to draw conclusions on a case based on evidence found on the media. Proficiency in technical tools and deductive reasoning is necessary. A detailed report demonstrating accepted procedures and evidence control must be submitted with each disk before proceeding to the next. The most basic test is the CEECS exam. Other candidates who complete all parts of the IACIS test successfully are designated as a Certified Forensic Computer Examiner (CFCE). The CFCE process changes as technology changes. The description here is current as of this writing. IACIS requires recertification every three years to demonstrate continuing work in the field of computer forensics. Recertification is less intense than the original certification but does test examiners to make sure they’re continuing their education and are still active in the field of computer forensics. For the latest information about IACIS and applying for CFCE certification or membership in IACIS, visit the IACIS Web site.

**High-Tech Crime Network (HTCN)** The High-Tech Crime Network (HTCN) also offers several levels of certification. Unlike IACIS, however, HTCN requires a review of all related training, including training in one of its approved courses, a written test for the specific certification, and a review of the candidate’s work history. HTCN certification is open to anyone meeting the criteria in the profession of computing investigations. At the time of this writing, the HTCN Web site (www.htcn.org) specifies requirements for the certification levels discussed in the following paragraphs. Requirements are updated without notice, so make sure you check the site periodically.

**Certified Computer Crime Investigator, Basic Level**
- Candidates must have three years of experience directly related to investigating computer-related incidents or crimes.
- Candidates have successfully completed 40 hours of training from an approved agency, organization, or training company.
- Candidates must provide documentation of at least 10 cases in which they participated.

**Certified Computer Crime Investigator, Advanced Level**
- Candidates must have five years of experience directly related to investigating computer-related incidents or crimes.
- Candidates have successfully completed 80 hours of training from an approved agency, organization, or company.
Candidates have served as lead investigator in at least 20 cases during the past three years and were involved in at least 40 other cases as a lead investigator or supervisor or in a supportive capacity. Candidates have at least 60 hours of involvement in cases in the past three years.

Certified Computer Forensic Technician, Basic

- Candidates must have three years of experience in computing investigations for law enforcement or corporate cases.
- Candidates must have completed 40 hours of computer forensics training from an approved organization.
- Candidates must provide documentation of at least 10 computing investigations.

Certified Computer Forensic Technician, Advanced

- Candidates must have five years of hands-on experience in computer forensics investigations for law enforcement or corporate cases.
- Candidates must have completed 80 hours of computer forensics training from an approved organization.
- Candidates must have been the lead computer forensics investigator in 20 or more investigations in the past three years and in 40 or more additional computing investigations as lead computer forensics technician, supervisor, or contributor. The candidate must have completed at least 60 investigations in the past three years.

EnCase Certified Examiner (EnCE) Certification

Guidance Software, the creator of EnCase, sponsors the EnCE certification program. EnCE certification is open to the public and private sectors and is specific to use and mastery of EnCase computer forensics analysis.

Requirements for taking the EnCE certification exam don’t depend on taking the Guidance Software EnCase training courses. Candidates for this certificate are required to have a licensed copy of EnCase. For more information on EnCE certification requirements, visit www.encase.com or www.guidancesoftware.com.

AccessData Certified Examiner (ACE)

AccessData, the creator of Ultimate Toolkit, sponsors the ACE certification program. ACE certification is open to the public and private sectors and is specific to use and mastery of AccessData Ultimate Toolkit.

Requirements for taking the ACE exam include completing the AccessData BootCamp and Windows forensic courses. The exam has a knowledge base assessment (KBA) and a practical skills assessment (PSA), which is optional. For more information on this certification, visit www.accessdata.com/acepreparation.html.

Other Training and Certifications

Other organizations are considering certifications or have related training programs. Nonprofit high-technology organizations for public- and private-sector investigations that offer certification and training include the following:

- High Technology Crime Investigation Association (HTCIA), www.htcia.org
- SysAdmin, Audit, Network, Security (SANS) Institute, www.sans.org
Determining the Physical Requirements for a Computer Forensics Lab

After you have the training to become a computer forensics investigator, you conduct most of your investigations in a lab. This section discusses the physical requirements for a computer forensics lab. Addressing these requirements can make a lab safer, more secure, and more productive.

Your lab facility must be physically secure so that evidence isn’t lost, corrupted, or destroyed. As with hardware and software costs, you must consider what’s needed to maintain a safe and secure environment when determining physical lab expenses. You must also use inventory control methods to track your computing assets, which means you should maintain a complete and up-to-date inventory of all major hardware and software items in the lab. For consumable items, such as cables and storage media, maintain an inventory so that you know when to order more supplies.

Identifying Lab Security Needs

All computer forensics labs need an enclosed room where a forensic workstation can be set up. You shouldn’t use an open cubicle because it allows easy access to your evidence. You need a room you can lock to control your evidence and attest to its integrity. In particular, your lab should be secure during data analysis, even if it takes several weeks to analyze a disk drive. To preserve the integrity of evidence, your lab should function as an evidence locker or safe, making it a secure facility or a secure storage safe.

The following are the minimum requirements for a computer forensics lab of any size:

- Small room with true floor-to-ceiling walls
- Door access with a locking mechanism, which can be a regular key lock or combination lock; the key or combination must be limited to authorized users
- Secure container, such as a safe or heavy-duty file cabinet with a quality padlock that prevents drawers from opening
- Visitor’s log listing all people who have accessed the lab

For daily work production, several examiners can work together in a large open area, as long as they all have the same level of authority and access need. This area should also have floor-to-ceiling walls and a locking door. In many public and private organizations, several investigators share a door to the lab that requires an ID card and entry code.

Copyright 2009 Cengage Learning, Inc. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part.
Computing investigators and forensics examiners must be briefed on the lab’s security policy. Share information about a case investigation only with other examiners and personnel who need to know about the investigation.

**Conducting High-Risk Investigations**

High-risk investigations, such as those involving national security or murder, for example, demand more security than the minimum lab requirements provide. As technology improves and information circulates among computer attackers, keeping an investigation secure can be more difficult. For example, detecting computer eavesdropping is difficult and expensive, but sophisticated criminals and intelligence services in foreign countries can use equipment that detects network transmissions, wireless devices, phone conversations, and the use of computer equipment. Instructions for building a sniffing device that can collect computer emissions illegally can be found online and, therefore, are available to anyone. These devices can pick up anything you type on your computer.

Most electronic devices emit electromagnetic radiation (EMR). Certain kinds of equipment can intercept EMR, which can be used to determine the data the device is transmitting or displaying. The EMR from a computer monitor can be picked up as far away as a half mile.

During the Cold War, defense contractors were required to shield sensitive computing systems and prevent electronic eavesdropping of any computer emissions. The U.S. Department of Defense calls this special computer-emission shielding TEMPEST. (For a brief description of TEMPEST, see the National Industrial Security Program Operating Manual [NISPOM]. DoD 5220.22-M, Chapter 11, Section 1, Tempest, http://nsi.org/Library/Govt/Nispom.html. Another site listing reliable sources is www.eskimo.com/~joelm/tempestintro.html.)

To protect your investigations, you might consider constructing a TEMPEST-qualified lab, which requires lining the walls, ceiling, floor, and doors with specially grounded conductive metal sheets. Typically, copper sheeting is used because it conducts electricity well. TEMPEST facilities must include special filters for electrical power that prevent power cables from transmitting computer emanations. All heating and ventilation ducts must have special baffles to trap emanations. Likewise, telephones inside the TEMPEST facility must have special line filters. A TEMPEST facility usually has two doors separated by dead space. The first exterior door must be shut before opening the interior door. Each door also has special copper molding to enhance electricity conduction.

Because a TEMPEST-qualified lab facility is expensive and requires routine inspection and testing, it should be considered only for large regional computer forensics labs that demand absolute security from illegal eavesdropping. To avoid these costs, some vendors have built low-emanating workstations instead of TEMPEST facilities. These workstations are more expensive than average workstations but less expensive than a TEMPEST lab.

**Using Evidence Containers**

Evidence storage containers, also known as evidence lockers, must be secure so that no unauthorized person can access your evidence easily. You must use high-quality locks, such as padlocks, with limited duplicate-key distribution. Also, routinely inspect the contents of evidence storage containers to make sure only current evidence is stored. The evidence custody forms should indicate what’s still in the locker. Evidence for closed cases should be moved to a secure off-site facility.
NISPOM Chapter 5, Section 3 ([http://nsi.org/Library/Govt/Nispom.html](http://nsi.org/Library/Govt/Nispom.html)) describes the characteristics of a safe storage container. Consult with your facility management or legal counsel, such as corporate or prosecuting attorneys, to determine what your lab should do to maintain evidence integrity. The following are recommendations for securing storage containers:

- The evidence container should be located in a restricted area that’s accessible only to lab personnel.
- The number of people authorized to open the evidence container should be kept to a minimum. Maintain records on who’s authorized to access each container.
- All evidence containers should remain locked when they aren’t under the direct supervision of an authorized person.

If a combination locking system is used for your evidence container, follow these practices:

- Provide the same level of security for the combination as for the container’s contents. Store the combination in another equally secure container.
- Destroy any previous combinations after setting up a new combination.
- Allow only authorized personnel to change lock combinations.
- Change the combination every six months, when any authorized personnel leave the organization, and immediately after finding an unsecured container—that is, one that’s open and unattended.

If you’re using a keyed padlock, follow these practices:

- Appoint a key custodian who’s responsible for distributing keys.
- Stamp sequential numbers on each duplicate key.
- Maintain a registry listing which key is assigned to which authorized person.
- Conduct a monthly audit to ensure that no authorized person has lost a key.
- Take an inventory of all keys when the custodian changes.
- Place keys in a lockable container accessible only to the lab manager and designated key custodian.
- Maintain the same level of security for keys as for evidence containers.
- Change locks and keys annually; if a key is missing, replace all associated locks and the key.
- Do not use a master key for several locks.

The storage container or cabinet should be made of steel and include an internal cabinet lock or external padlock. If possible, purchase a safe, which provides superior security and protects your evidence from fire damage. Look for specialized safes, called media safes, designed to protect electronic media. Media safes are rated by the number of hours it takes before fire damages the contents. The higher the rating, the better the safe protects evidence.

An evidence storage room is also convenient, especially if it’s part of your computer forensics lab. Security for an evidence room must integrate the same construction and securing devices as the general lab does. Large computer forensics operations also need an evidence custodian
and a service counter with a securable metal roll-up window to control evidence. With a secure evidence room, you can store large computer components, such as computers, monitors, and other peripheral devices.

Be sure to maintain a log listing every time an evidence container is opened and closed. Each time the container is accessed, the log should indicate the date it was opened and the initials of the authorized person. These records should be maintained for at least three years or longer, as prescribed by your prosecuting or corporate attorneys. Logs are discussed in more detail in Chapter 5.

**Overseeding Facility Maintenance**

Your lab should be maintained properly at all times to ensure the safety and health of lab personnel. Any damage to the floor, walls, ceilings, or furniture should be repaired immediately. Also, be sure to escort cleaning crews into the facility and monitor them as they work.

Because static electricity is a major problem when handling computer parts, consider placing antistatic pads around electronic workbenches and workstations. In addition, floors and carpets should be cleaned at least once a week to help minimize dust that can cause static electricity.

Maintain two separate trash containers, one to store items unrelated to an investigation, such as discarded CDs or magnetic tapes, and the other for sensitive material that requires special handling to make sure it’s destroyed. Using separate trash containers maintains the integrity of criminal investigation processes and protects trade secrets and attorney-client privileged communications in a private corporation. Several commercially bonded firms specialize in disposing of sensitive materials, and you should hire one to help maintain the integrity of your investigations.

**Considering Physical Security Needs**

In addition to your lab’s physical design and construction, you need to enhance security by setting security policies. How much physical security you implement depends on the nature of your lab. A regional computer crime lab has high physical security needs because of the risks of losing, corrupting, or damaging evidence. The physical security needs of a large corporation are probably not as high because the risk of evidence loss or compromise is much lower. Determining the risk for your organization dictates how much security you integrate into your computer forensics lab.

Regardless of the security risk to your lab, maintain a paper or electronic sign-in log for all visitors. The log should list the visitor’s name, date and time of arrival and departure, employer’s name, purpose of the visit, and name of the lab member receiving the visitor. Consider anyone who’s not assigned to the lab to be a visitor, including cleaning crews, facility maintenance personnel, friends, and family. All visitors should be escorted by an assigned
authorized staff member throughout their visit to the lab to ensure that they don’t accident-
tally or intentionally tamper with an investigation or evidence. As an added precaution, use a visible or audible alarm, such as a visitor badge, to let all investigators know that a visitor is in the area. If possible, hire a security guard or have an intrusion alarm system with a guard to ensure your lab’s security. Alarm systems with guards can also be used after business hours to monitor your lab.

**Auditing a Computer Forensics Lab**

To make sure security policies and practices are followed, conduct routine inspections to audit your lab and evidence storage containers. Audits should include, but aren’t limited to, the following facility components and practices:

- Inspect the lab’s ceiling, floor, roof, and exterior walls at least once a month, looking for anything unusual or new.
- Inspect doors to make sure they close and lock correctly.
- Check locks to see whether they need to be replaced or changed.
- Review visitor logs to see whether they’re being used properly.
- Review log sheets for evidence containers to determine when they have been opened and closed.
- At the end of every workday, secure any evidence that’s not being processed on a forensic workstation.

**Determining Floor Plans for Computer Forensics Labs**

How you configure the work area for your computer forensics lab depends on your budget, the amount of available floor space, and the number of computers you assign to each computing investigator. For a small operation handling two or three cases a month, one forensic workstation should be enough to handle the workload. One workstation requires only the space an average desk takes up. If you’re handling many more cases per month, you can probably process two or three investigations at a time, which requires more than one workstation. The ideal configuration for multiple workstations is to have two forensic workstations plus one nonforensic workstation with Internet access.

Because you need plenty of room around each workstation, a work area containing three workstations requires approximately 150 square feet of space, meaning the work area should be about 10 feet by 15 feet. This amount of space allows for two chairs so that the computing investigator can brief another investigator, paralegal, or attorney on the case.

Small labs usually consist of one or two forensic workstations, a research computer with Internet access, a workbench (if space allows), and storage cabinets, as shown in Figure 3-2.

Mid-size computer forensics labs, such as those in a private business, have more workstations. For safety reasons, the lab should have at least two exits, as shown in Figure 3-3. If possible, cubicles or even separate offices should be part of the layout to reinforce the need-to-know policy. These labs usually have more library space for software and hardware storage.
State law enforcement or the FBI usually runs most large or regional computer forensics labs. As shown in Figure 3-4, these labs have a separate evidence room, which is typical in police investigations, except this room is limited to digital evidence. One or more custodians might be assigned to manage and control traffic in and out of the evidence room.

As discussed earlier, the evidence room needs to be secure. The lab should have at least two controlled exits and no windows. Separate offices for supervisors and cubicles for investigators are more practical in this configuration. Remember that forensic workstations are connected to an isolated LAN, and only a few machines are connected to an outside WAN or metropolitan area network (MAN).
Selecting a Basic Forensic Workstation

The computer workstation you use as a forensics analysis system depends on your budget and specific needs. Many well-designed forensic workstations are available that can handle most computing investigation needs. However, when you start processing a case, you use a workstation for the duration of the examination. Use less powerful workstations for mundane tasks and multipurpose workstations for higher-end analysis tasks.

Selecting Workstations for Police Labs

Police departments in major cities probably have the most diverse needs for computing investigation tools because the communities they serve use a wide assortment of computing systems. Not all computer users have the latest technology, so police departments usually need older machines and software, such as a Commodore 64, an Osborne I, or a Kaypro running CP/M or Minix, to match what’s used in their community. For small, local police departments, however, the majority of work involves Windows PCs and Apple Macintosh systems. A small police department’s computer forensics lab could be limited to one multipurpose forensic workstation with one or two basic workstations.

One way to investigate older and unusual computing systems is to keep track of special-interest groups (SIGs) that still use these systems. SIGs, which you can find through an Internet search, can be a valuable source of support for recovering and analyzing uncommon systems. You can also coordinate with or subcontract to larger computer forensics labs. Like
large police departments, a regional computer forensics lab must have diverse systems to serve its community and often receives work from smaller labs involving unusual computers or OSs.

Computing systems in a lab should be able to process typical cases in a timely manner. The time it takes to process a case usually depends on the size and type of industries in the region. For example, suppose your lab is located in a region with a large manufacturing firm that employs 50,000 people. Based on crime reports you’ve consulted, 10% of those employees might be involved in criminal behavior, meaning 5000 employees will commit crimes such as fraud, embezzlement, and so on. These statistics can help you estimate how much time is involved in processing these types of cases.

Until recently, the general rule was at least one law enforcement computer investigator for every 250,000 people in a geographic region. For example, if your community has 1,000,000 people, the regional computer forensics lab should have at least four computer investigators, each with at least one multipurpose forensic workstation and one general-purpose workstation. This rule is quickly changing, however, as the amount of data stored on digital devices increases.

**Selecting Workstations for Private and Corporate Labs**

For the private sector, such as a business conducting internal investigations or a commercial business providing computer forensics services to private parties, equipment resources are generally easy to determine.

Commercial businesses providing computer forensics analysis for other companies can tailor their services to specific markets. They can specialize in one or two platforms, such as an Intel PC running a Microsoft OS. They can also gather a variety of tools to meet a wider market. The type of equipment they need depends on their specialty, if any. For general computer forensics facilities, a multipurpose forensic workstation is sufficient.

Private companies conducting their own internal computing investigations can determine the type of forensic workstation they need based on the types of computers they use. If a company uses only Windows PCs, internal investigators don’t need a wide variety of specialized equipment. If a company uses many kinds of computers, the Internal Computing Investigation Department needs systems and equipment that support the same types of computers. With some computer forensics programs, you can work from a Windows PC and examine both Windows and Macintosh disk drives.

**Stocking Hardware Peripherals**

In addition to workstations and software, all labs should have a wide assortment of cables and spare expansion slot cards. Consider stocking your computer forensics lab with the following peripheral devices:

- 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
- Ribbon cables for floppy disks
- Extra SCSI cards, preferably ultra-wide
- Graphics cards, both Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP)
• Extra power cords
• A variety of hard drives (as many as you can afford and in as wide a variety as possible)
• At least two 2.5-inch adapters from notebook IDE hard drives to standard IDE/ATA drives, SATA drives, and so on
• Computer hand tools, such as Phillips and flathead screwdrivers, a socket wrench, and a small flashlight

Maintaining Operating Systems and Software Inventories
Operating systems are an essential part of your lab’s inventory. You should maintain licensed copies of as many legacy OSs as possible to handle cases involving unusual systems. Microsoft OSs should include Windows XP, 2000, NT 4.0, NT 3.5, 9x, 3.11, and DOS 6.22. Macintosh OSs should include Mac OS X, 9.x, and 8 or older. Linux OSs can include Fedora, Caldera Open Linux, Slackware, and Debian. The most recent OSs, such as Windows Vista, should also be included.

Although most high-end computer forensics tools can open or display data files created with popular programs, they don’t support all programs. Your software inventory should include current and older versions of the following programs. If you deal with both Windows PCs and Macintosh systems, you should have programs for both.

• Microsoft Office (including current and older versions)
• Quicken (if you handle a lot of financial investigations)
• Programming languages, such as Visual Basic and Visual C++
• Specialized viewers, such as QuickView, ACDSee, ThumbsPlus, and IrfanView
• Corel Office Suite
• StarOffice/OpenOffice
• Peachtree accounting applications

Using a Disaster Recovery Plan
Besides planning for equipment needs, you need to plan for disasters, such as hard disk crashes, lightning strikes, and power outages. A disaster recovery plan ensures that you can restore your workstations and file servers to their original condition if a catastrophic failure occurs.

A disaster recovery plan also specifies how to rebuild a forensic workstation after it has been severely contaminated by a virus from a drive you’re analyzing. Central to any disaster recovery plan is a system for backing up investigation computers. Tools such as Norton Ghost are useful for restoring files directly. As a general precaution, consider backing up your workstation once a week. You can restore programs from the original disks or CDs, but recovering lost data without up-to-date backups is difficult.

Store your system backups where they are easily accessible. You should have at least one copy of backups on site and a duplicate copy or a previous copy of backups stored in a safe off-site facility. Off-site backups are usually rotated on a schedule that varies according to your needs, such as every day, week, or month.
In addition, record all updates you make to your workstation by using a process called configuration management. Some companies record updates in a configuration management database to maintain compliance with lab policy. Every time you add or update software on your workstation, enter the change in the database or in a simple notebook with handwritten entries to document the change.

A disaster recovery plan can also address how to restore a workstation you reconfigured for a specific investigation. For example, if you install a suite of applications, you might not have enough disk space for normal processing needs, so you could encounter problems during reconfigurations or even simple upgrades. The disaster recovery plan should outline how to uninstall software and delete any files the uninstall program hasn’t removed so that you can restore your system to its original configuration.

For labs using high-end RAID servers (such as Digital Intelligence F.R.E.D.C. or F.R.E.D.M.), you must consider methods for restoring large data sets. These large-end servers must have adequate data backup systems available in the event of a major failure of more than one drive. When planning a recovery procedure for RAID servers, consider whether the amount of downtime it takes to restore backup data is acceptable to the lab operation.

**Planning for Equipment Upgrades**

Risk management involves determining how much risk is acceptable for any process or operation, such as replacing equipment. Identify the equipment your lab depends on, and create a schedule to replace that equipment. Also, identify equipment that you can replace when it fails.

Computing components are designed to last 18 to 36 months in normal business operations, and new versions of OSs and applications that take up more disk space are released frequently. Therefore, systems periodically need more RAM, disk space, and processing speed. To keep your lab current with updates in hardware technology, schedule hardware replacements at least every 18 months and preferably every 12 months.

**Using Laptop Forensic Workstations**

Recent important advances in hardware technology offer more flexibility in computer forensics. You can now use a laptop PC with FireWire (IEEE 1394B standard), USB 2.0, or PCMCIA SATA hard disks to create a lightweight, mobile forensic workstation. Improved throughput speeds of data transfer on laptops also make it easier to create images of suspect drives.

However, laptops are still limited as forensic workstations. Even with improved data transfer rates, acquiring data with a data compression imaging tool, such as EnCase or SafeBack, creates a bottleneck. The processor speed determines how quickly you can acquire an image of a hard disk. The faster the processor on your laptop (or other PC), the faster an image is created in a compressed mode.

**Building a Business Case for Developing a Forensics Lab**

Before you can set up a computer forensics lab, you must enlist the support of managers and other team members. To do so, you build a business case, a plan you can use to sell your
services to management or clients. In the business case, you justify acquiring newer and better resources to investigate computer forensics cases.

How you develop a business case depends on the organization you support. If you’re the sole proprietor, creating a business case is fairly simple. If you need money to buy tools, you can save your money for the purchase or negotiate with your bank for a loan. For a public entity such as a police department, business requirements can change drastically because budgets are planned a year or more in advance. Public agency department managers present their budget proposals to upper management. If the proposal is approved, upper management makes money available to acquire resources outlined in the budget. Some public organizations might have other funds available that can be spent immediately for special needs. Managers can divert these funds for emergency or unforeseen needs.

Keep in mind that a private-sector business, especially a large corporation, is motivated by the need to make money. A business case should demonstrate how computing investigations could save money and avoid risks that can damage profits, such as by preventing litigation involving the company. For example, recent court decisions have defined viewing pornographic images in the workplace as creating a hostile environment for other employees, which is related to employee harassment and computer misuse. An employer is responsible for preventing and investigating harassment of employees and non-employees associated with the workplace. A company is also liable if it doesn’t actively prevent the creation of a hostile workplace by providing employee training and investigating allegations of computer misuse. A lawsuit, regardless of who wins, can cost an employer several hundred thousand dollars. In your business case, compare the cost of training and conducting computing investigations with the cost of a lawsuit.

The Internet makes it difficult for employers to provide a safe and secure environment for employees. In particular, employees can misuse free Web-based e-mail services. These free services give senders anonymity, making it possible for employees to send inappropriate e-mails, often in the form of sexual harassment. Because training rarely prevents this type of behavior, an employer needs to institute an investigation program that involves collecting network logs, such as proxy server logs, and examining computer disks to locate traces of message evidence. Chapter 12 discusses e-mail abuse and using e-mail server and network logs.

Your business case should also show how computing investigations can improve profits, such as by protecting intellectual property, trade secrets, and future business plans. For example, when employees leave one company for a competing company, they can reveal vital competitive information to their new employers. Suppose a company called Skateboard International (SI) has invested research and development funds into a new product that improves the stability of skateboards. Its main competitor is Better Skateboard; this company contacts Gwen Smith, a disgruntled SI employee, via e-mail and offers her a job. When Gwen leaves SI, she takes with her the plans for the new product. A few months later, Better Skateboard introduces a product similar to the skateboard Gwen had been researching at SI. SI recognizes that the new, improved skateboard is similar to the one Gwen had been developing and consults the noncompete agreement Gwen signed when she was hired. SI thinks the new technology Gwen might have given Better Skateboards belongs to its company. It suspects that Better Skateboard stole its trade secret and intellectual property.

SI could sue Better Skateboard and demand discovery on internal documents. Because Gwen and Better Skateboard corresponded via e-mail, a computing investigator needs to find data
related to hiring and research engineering at Better Skateboard. Better Skateboard can also demand discovery on SI’s research records to determine whether any discrepancies in product design could disprove the lawsuit. In this example, computing investigations can allow one company to generate revenue from a new product and prevent the other company from doing so. Information related to profit and loss makes a persuasive argument in a business case.

Preparing a Business Case for a Computer Forensics Lab

It’s important to understand the need for planning in the creation and continued maintenance of a computer forensics lab. The reason for this demand is the constant cost-cutting efforts of upper management. Because of organizations’ tendencies to constantly reduce costs, you must plan ahead to ensure that money is available for facilities, tools, supplies, and training for your computer forensics lab. The following sections describe some key elements for creating a computer forensics business case. It’s a good idea to maintain a business case with annual updates.

Justification  Before you can start, you need to justify to the person controlling the budget the reason a lab is needed. This justification step requires asking the following questions:

- What type of computing investigation service is needed for your organization?
- Who are the potential customers for this service, and how will it be budgeted—as an internal operation (police department or company security department, for instance) or an external operation (a for-profit business venture)?
- How will you advertise your services to customers?
- What time-management techniques will you use?
- Where will the initial and sustaining budget for business operations come from?

No matter what type of organization you work for—a public agency or a private business—operating a computer forensics lab successfully requires constant efforts to communicate, or advertise, the lab’s services to previous, current, and future customers and clients. By using marketing to attract new customers or clients, you can justify future budgets for the lab’s operation and staff.

Budget Development  The budget needs to include all items described in the following sections. You must be as exact as possible when determining the true cost of these items. Making a mistake could cause delays and possible loss of the opportunity to start or improve your lab.

Facility Cost  For a new computer forensics lab, startup costs might take most of the budget. Depending on how large the lab is, you must determine first how much floor space is needed. As mentioned, a good rule of thumb is 150 square feet per person. This amount of space might seem a bit larger than necessary, but consider how much storage space is needed to preserve evidence and to have enough supplies in stock. Check with your organization’s facility manager on per-square-foot costs for your area or building. Here are some sample questions to answer to get started on calculating a budget:

- How many computer forensics examiners will you need?
- How much training will each examiner require per year?
- Will you need more than one lab?
• How many computer forensics examiners will use each lab? Will there be a need to accommodate other nonexaminers temporarily to inspect recovered evidence?
• What are the costs to construct a secure lab?
• Is there a suitable room that can be converted into a lab?
• Does the designated room have enough electrical power and heating, ventilation, and air-conditioning (HVAC) systems?
• Does the designated room have existing telephone lines and network cables? If not, how much will it cost to install these additional items?
• Is there an adequate door lock on the designated room’s door?
• What will the furniture costs be?
• Will you need to install an alarm system?
• Are there any other facility costs, such as fees for janitorial services and facility maintenance services?

Computer Hardware Requirements Determining the types of investigations and data that will be analyzed in your computer forensics lab dictates what hardware equipment you need. If your organization is using Intel-based PCs with Windows XP, for instance, your forensic workstation should be a high-end Intel-based PC, too. For a small police department, determining the types of computers the public uses is more difficult. The diversity of a community’s computer systems requires a police department to be more versatile in the tools needed to conduct investigations. To determine computer hardware budget needs, here are some questions to consider in your planning:

• What types of investigations and data recovery will be performed in the lab?
• How many investigations can be expected per month of operation?
• Will there be any time-sensitive investigations that demand rapid analysis of disk data?
• What sizes and how many drives will be needed to support a typical investigation?
• Will you need a high-speed backup system, such as tape backup or DVD burners?
• What is the predominant type of computer system you will investigate?
• What will you use to store digital evidence? How long do you need to store it?

Software Requirements In the past few years, many more computer forensics tools have become available. For the private sector, the cost for these tools ranges from about $300 and up. For the public sector, many computer forensics software vendors offer discounts. However, just as you select hardware for your computer forensics lab to fit specific needs, you must first determine what type of OSs and applications will be investigated and then make purchases that fit. Keep in mind that the more you spend on a computer forensics software package, the more function and flexibility will be available. To determine computer software budget needs, here are some questions to consider in your planning:

• What types of OSs will be examined?
• For less popular, uncommon, or older OSs (such as Mac OS 9.x, OS/2, and CP/M), how often will there be a need to investigate them?
What are the minimum needs for forensics software tools? For example, how many copies of each tool will be needed? How often will each tool be used in an average week?

What types of OSs will be needed to conduct routine examinations?

Will there be a need for specialized software, such as QuickBooks or Peachtree?

Is there a budget to purchase more than one forensics software tool, such as EnCase, FTK, or ProDiscover?

Which disk-editing tool should be selected for general data analysis?

**Miscellaneous Cost Needs** For this section of the budget, you need to brainstorm on other items, tools, and supplies to consider purchasing for the lab, from general office supplies to specific needs for daily operations. To determine miscellaneous budget needs, here are some questions to consider in your planning:

- Will there be a need for errors and omission insurance for the lab’s operation and staff?
- Will you need a budget for office supplies?

**Approval and Acquisition** The approval and acquisition phase for a computer forensics lab is a management function. It’s your responsibility to create a business case with a budget to present to upper management for approval. As part of the approval process, you should include a risk analysis describing how the lab will minimize the risk of litigation, which is a persuasive argument for supporting the lab. You also need to make an educated guess of how many investigations are anticipated and how long they will take to complete on average. Remember, part of the approval process requires using negotiation skills to justify the business case. You might need to revise your case as needed to get approval.

As part of the business case, acquisition planning requires researching different products to determine which one is the best and most cost effective. You need to contact several vendors’ sales staff and design engineers to learn more about each product and service. Another factor to investigate is annual maintenance costs. You need to budget for this expense, too, so that you can get support if you run into problems during an investigation. An additional item to research from others in the profession is the vendor’s maintenance history. Do other computer forensics labs use the same product, and have they had any problems getting support for problems they encounter?

Another consideration is vendors’ pricing structures. Vendor pricing isn’t based on the cost of creating CDs and DVDs and packaging them. Product prices are based on cost for development, testing, documentation support, shipping, and research and development for future improvements. In addition, vendors are for-profit organizations; they have investors to pay, too. Keep in mind that for vendors to be around next year to provide products and services for you, they need to make money.

**Implementation** After approval and acquisition, you need to plan the implementation of facilities and tools. As part of your business case, describe how implementation of all approved items will be processed. A timeline showing expected delivery or installation dates and expected completion dates must be included. You should also have a coordination plan for delivery dates and times for materials and tools. Inspection of facility construction,
equipment (including furniture and benches), and software tools should be included in the schedule. Make sure you schedule inspection dates, too, to ensure that what you ordered arrived and is functional.

**Acceptance Testing** Following the implementation scheduling and inspection, you need to develop an acceptance test plan for the computer forensics lab to make sure everything works correctly. When writing the acceptance test plan, consider the following items:

- Inspect the facility to see whether it meets the security criteria to contain and control digital evidence.
- Test all communications, such as phone and network connections, to make sure they work as expected.
- Test all hardware to verify that it operates correctly; for example, test a computer to make sure it boots to Windows.
- Install and start all software tools; make sure all software can run on the computers and OSs you have in the lab.

**Correction for Acceptance** The better you plan for your lab, the less likely you’ll have problems. However, any lab operation has some problems during startup. Your business case must anticipate problems that can cause delays in lab production. In the business case, you need to develop contingencies to deal with system or facility failures. For example, devise workarounds for problems such as the wrong locks being installed on lab doors or electrical power needing additional filtering.

**Production** After all essential corrections have been made, your computer forensics lab can then go into production. At this time, you implement the lab operations procedures that have been described in this chapter.

For additional information on how to write a business case, see [www.sba.gov/smallbusinessplanner/plan/writeabusinessplan/index.html](http://www.sba.gov/smallbusinessplanner/plan/writeabusinessplan/index.html).

---

**Chapter Summary**

- A computer forensics lab is where you conduct investigations, store evidence, and do most of your work. You use the lab to house your instruments, current and legacy software, and forensic workstations. In general, you need a variety of computer forensics hardware and software.
- To continue a career in computing investigations and forensic analysis, you need to upgrade your skills through training. Several organizations offer training and certification programs for computer forensics that test you after you have successfully completed training. Some state and federal government agencies are also considering establishing certification programs that address minimum skills needed to conduct computing investigations at different levels.
- Your lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed.
Police departments in major cities need a wide assortment of computing systems, including older, outdated technology. Most computer investigations in small, local police departments involve Windows PCs and Macintosh systems. As a general rule, there should be at least one law enforcement computer investigator for every 250,000 people in a geographic region. Commercial services providing computer forensics analysis for other businesses can tailor their services to specific markets.

A forensic workstation needs to have adequate memory, storage, and ports to deal with the common types of cases that come through your lab.

Before you can set up a computer forensics lab, you must enlist the support of your managers and other team members by building a business case, a plan you can use to sell your services to management or clients. In the business case, you justify acquiring newer and better resources to investigate computer forensics cases.

Key Terms

**American Society of Crime Laboratory Directors (ASCLD)** A national society that sets the standards, management, and audit procedures for labs used in crime analysis, including computer forensics labs used by the police, FBI, and similar organizations.

**business case** A document that provides justification to upper management or a lender for purchasing new equipment, software, or other tools when upgrading your facility. In many instances, a business case shows how upgrades will benefit the company.

**Certified Electronic Evidence Collection Specialist (CEECS)** A certificate awarded by IACIS at completion of the written exam.

**Certified Forensic Computer Examiner (CFCE)** A certificate awarded by IACIS at completion of all portions of the exam.

**computer forensics lab** A computer lab dedicated to computing investigations; typically, it has a variety of computers, OSs, and forensics software.

**configuration management** The process of keeping track of all upgrades and patches you apply to your computer’s OS and applications.

**High Tech Crime Network (HTCN)** A national organization that provides certification for computer crime investigators and computer forensics technicians.

**risk management** The process of determining how much risk is acceptable for any process or operation, such as replacing equipment.

**secure facility** A facility that can be locked and allows limited access to the room’s contents.

**special-interest groups (SIGs)** Associated with various operating systems, these groups maintain electronic mailing lists and might hold meetings to exchange information about current and legacy operating systems.

**TEMPEST** A term referring to facilities that have been hardened so that electrical signals from computers, the computer network, and telephone systems can’t be monitored or accessed easily by someone outside the facility.

**Uniform Crime Report** Information collected at the federal, state, and local levels to determine the types and frequencies of crimes committed.
Review Questions

1. An employer can be held liable for e-mail harassment. True or False?

2. Building a business case can involve which of the following?
   a. Procedures for gathering evidence
   b. Testing software
   c. Protecting trade secrets
   d. All of the above

3. The ASCLD mandates the procedures established for a computer forensics lab. True or False?

4. The manager of a computer forensics lab is responsible for which of the following? (Choose all that apply.)
   a. Necessary changes in lab procedures and software
   b. Ensuring that staff members have sufficient training to do the job
   c. Knowing the lab objectives
   d. None of the above

5. To determine the types of operating systems needed in your lab, list two sources of information you could use.

6. What items should your business plan include?

7. List two popular certification systems for computer forensics.

8. The National Cybercrime Training Partnership is available only to law enforcement. True or False?

9. Why is physical security so critical for computer forensics labs?

10. If a visitor to your computer forensics lab is a personal friend, it’s not necessary to have him or her sign the visitor’s log. True or False?

11. What three items should you research before enlisting in a certification program?

12. Large computer forensics labs should have at least _____ exits.

13. Typically, a(n) _____ lab has a separate storage area or room for evidence.

14. Computer forensics facilities always have windows. True or False?

15. The chief custodian of evidence storage containers should keep several master keys. True or False?

16. Putting out fires in a computer lab usually requires a _____ rated fire extinguisher.

17. A forensic workstation should always have a direct broadband connection to the Internet. True or False?

18. Which organization provides good information on safe storage containers?
19. Which organization has guidelines on how to operate a computer forensics lab?

20. What term refers to labs constructed to shield EMR emissions?

**Hands-On Projects**

**Hands-On Project 3-1**

You have just been hired to perform digital investigations and forensics analysis for a company. You find that no policies, processes, or procedures are currently in place. Do an Internet search to find information, and then create a policy and processes document to provide the structure necessary for your lab environment. Be sure to cite your online sources.

**Hands-On Project 3-2**

As mentioned previously, new forensics certifications are constantly being offered. Research certifications online and find one not discussed in this chapter. Write a short paper stating what organization offers the certification, who endorses the certification, how long the organization has been in business, and so forth.

**Hands-On Project 3-3**

Physical security of a lab must always be maintained. In your classroom lab, get permission to make observations at different times of the day when classes are and aren’t in session. Record how many people go in and out during a period. Do you know all the people or can you identify them? Are they all students or faculty? Who monitors the lab when classes aren’t in session? Are the rooms locked? How often are things stolen from the labs? Write one to two pages about your observations. If it were a computer forensics lab, what changes would you have to make?

**Hands-On Project 3-4**

Write a disaster recovery plan of not more than three pages for a fictitious company’s computer forensics lab. Include backup schedules, note the programs and OS installed on each machine, and list other information you would have to recover after a disaster. You should also note where the original disks and backups are located.

**Hands-On Project 3-5**

A law firm has hired you to assist with digital evidence cases involving divorces. The main evidence consists of e-mail, spreadsheets, and documents. Before hiring you, the firm used an outside group to conduct investigations. You have to decide what equipment and software to purchase. What would you do to build a business plan that would be approved?
Case Projects

Case Project 3-1
Based on your evaluation of the arson case in Case Project 2-1, build a business case for the resources you think you’ll need to investigate it for the insurance company. Write a brief paper outlining the resources you’ll need, and make sure to justify your needs.

Case Project 3-2
A new version of Windows has been released. What do you need to do to be ready in 6 to 10 months when you encounter cases involving the new OS? Include research, user groups, and others you need to contact. Write a one-page paper on the procedures you should use.