# **Chapter 2**

**The Investigator’s Office and Laboratory**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

Chapter 2 describes the investigator’s office and laboratory. Students will review the certification requirements for computer forensics labs. Next, students will learn the physical requirements for a computer forensics lab. This chapter also explains the criteria for selecting a basic forensic workstation. Finally, Chapter 2 describes components used to build a business case for developing a forensics lab.

# **Chapter Objectives**

* Describe certification requirements for digital forensics labs
* List physical requirements for a digital forensics lab
* Explain the criteria for selecting a basic forensic workstation
* Describe components used to build a business case for developing a forensics lab

# **Teaching Tips**

# **Understanding Forensic Lab Accreditation Requirements**

1. Explain that a digital forensics lab is where you conduct investigations, store evidence, and do most of your work.
2. Point out the ANSI-ASQ National Accreditation Board (ANAB) Web site [www.anab.org](http://www.anab.org/) for guidelines for managing a forensics lab and acquiring an official crime lab certification.
3. Mention that for a lab to be accredited, ANAB audits the lab’s tasks and functions to ensure correct and consistent results for all cases.

## **Identifying Duties of the Lab Manager and Staff**

1. Illustrate the tasks of a lab manager, including:
   1. Set up goals, schedules, staff duties, and responsibilities
   2. Assign cases to the lab staff members and know when to expect preliminary and final reports
2. Mention that staff members are responsible for their knowledge and appropriate training to perform their tasks. They should be aware of new technologies and look for training programs that can help them develop on a professional level.

**Lab Budget Planning**

1. Explain that you should break costs down into monthly, quarterly, and annual expenses. Use past investigation expenses to extrapolate expected future costs.
2. Illustrate different expenses that should be considered when planning a lab budget such as:
   1. Purchasing hardware and software
   2. Renting facility space
   3. Training personnel
3. Remind your students that the lab manager is responsible for planning the lab budget.

|  |  |
| --- | --- |
| ***Teaching Tip*** | Use a Uniform Crime Report to illustrate the use of statistics when planning a lab budget. If the report shows that most computers use Microsoft Windows family OSs, you should expect more crimes committed using any of these OSs. Your lab should have sufficient resources to handle these cases. |

1. Mention that you should also identify specialized software used with certain crimes.
2. Describe the requirements for setting up a lab for a private company, including:
   1. Hardware and software inventory
   2. Problems reported last year
   3. Future developments in computing technology
3. Explain some of the storage and network considerations when planning a lab budget.
4. Mention that time management is a major issue when choosing software and hardware to purchase.

**Acquiring Certification and Training**

1. Describe the benefits of having appropriate training and certification.
2. Point out some of the problems you may encounter when getting certification, including:
   1. Certification programs might be expensive
   2. Certification requirements may be hard to meet
3. Describe some of the most well-known certification programs and organizations, including:
   1. International Association of Computer Investigative Specialists (IACIS)
   2. ISC² Certified Cyber Forensics Professional
   3. High Tech Crime Network (HTCN)
   4. EnCase Certified Examiner (EnCE) Certification
   5. AccessData Certified Examiner (ACE) Certification
   6. EC-Council
   7. SysAdmin, Audit, Network, Security (SANS) Institute
   8. Defense Cyber Investigations Training Academy (DCITA)
   9. International Society of Forensic Computer Examiners (ISFCE) for the Certified Computer Examiner (CCE) certification
   10. Computer Technology Investigators Network (CTIN)
   11. Digital Forensics Certification Board (DFCB)
   12. Cloud Security Alliance (CSA)
   13. Federal Law Enforcement Training Center (FLETC)
   14. National White Collar Crime Center (NW3C)
4. Encourage your students to find the certification program that fits their needs.

# **Determining the Physical Requirements for a Digital Forensics Lab**

1. Explain that most of the investigative process is performed at a lab. Therefore, the lab should provide a safe and secure physical environment for you and your evidence.
2. Mention that as with any other lab, you should perform inventory controls of your assets. This will help you know when you need to re-order lab supplies.

## **Identifying Lab Security Needs**

1. Explain that a forensics lab is a secure facility with special security requirements oriented to preserve the integrity of the evidence data and the work done there.
2. Present a list with the minimum requirements for a lab:
   1. Small room with true floor-to-ceiling walls
   2. Door access with a locking mechanism
   3. Secure container, such as a safe or heavy-duty file cabinet with a quality padlock
   4. Visitor’s log listing all people who have accessed your lab

|  |  |
| --- | --- |
| ***Teaching Tip*** | Having a security policy that nobody knows is the same as not having a policy at all. Your lab staff members should be briefed about the lab’s security policy and any changes to the policy. |

**Conducting High-Risk Investigations**

1. Mention that high-risk investigations cannot be conducted in regular forensics lab facilities. They demand more security than the minimum lab requirements provide.
2. Describe some of the characteristics of a TEMPEST lab. Start by mentioning that the computer emanates electromagnetic radiation that can be picked up by specialized devices up to half-a-mile away, allowing attackers to know exactly what you are doing with your workstation.
3. Illustrate the use of low-emanation workstations as a less expensive alternative to a TEMPEST lab.

|  |  |
| --- | --- |
| ***Teaching Tip*** | Read more about TEMPEST at: <https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981>. |

**Using Evidence Containers**

1. Explain to your students that an evidence container must be secure to prevent unauthorized access to the evidence. Security recommendations include:
   1. Restricted area
   2. Minimum number of authorized people to access the container
   3. Always lock the container when not in use
2. Describe some of the practices to follow if a combination locking system is used, including:
   1. Provide the same level of security for the combination as for the container’s contents
   2. Destroy any previous combinations after setting up a new combination
   3. Allow only authorized personnel to change lock combinations
   4. Change the combination every six months or when required, such as when any authorized personnel leave the organization
3. Describe some of the recommendations if you’re using a keyed padlock, including:
   1. Appoint a key custodian
   2. Stamp sequential numbers on each duplicate key
   3. Maintain a registry listing which key is assigned to which authorized person
   4. Conduct a monthly audit
   5. Take an inventory of all keys
   6. Place keys in a lockable container
   7. Maintain the same level of security for keys as for evidence containers
   8. Change locks and keys annually
   9. Do not use a master key for several locks
4. Mention that an evidence container should be made of steel with an internal cabinet or external padlock.
5. Explain the convenience of having a built-in evidence storage room in your lab and the security measures you should follow building and managing it.
6. Finally, mention other recommendations like buying a media safe and keeping an updated evidence log.

**Overseeing Facility Maintenance**

1. Describe the importance of a well-maintained lab to ensure the safety and health of the lab staff members.
2. Explain some of the considerations for appropriate facility maintenance. You should mention:
   1. Immediately repair damages to walls, ceilings, and floors
   2. Escort cleaning crews into the facility and monitor them as they work
   3. Implement measures to protect equipment from static electricity
   4. Proper disposal of materials; maintain two separate trash containers

|  |  |
| --- | --- |
| ***Security tips*** | Dumpster diving is a technique used especially by social engineers to obtain information from materials wrongly disposed as garbage. Information may include Social Security numbers, credit card numbers, and old passwords lists. |

**Considering Physical Security Needs**

1. Explain the importance of a good physical security policy.
2. Illustrate some of the mechanisms you have to enforce your policy:
   1. Sign-in logs for visitors
   2. Escort all visitors while inside your lab
   3. Alert others of the presence of a visitor
   4. Install an alarm system
   5. Hire guards to protect your premises, especially at night

**Auditing a Computer Forensics Lab**

1. Illustrate how regular auditing processes can help you to better enforce security policies.
2. Describe some of the items your audits should include:
   1. Ceiling, floor, roof, and exterior walls of the lab
   2. Doors and doors locks
   3. Visitor logs
   4. Evidence containers logs
   5. At the end of every workday, secure any evidence that’s not being processed on a forensic workstation

**Determining Floor Plans for Digital Forensics Labs**

1. Computer forensics labs come in a variety of setups and arrangements. Use Figures 2-2 through 2-4 to illustrate different computer forensics lab setups based on their sizes. You should mention characteristics such as:
   1. Number of workstations
   2. Number of workbenches
   3. Working area size
   4. Number of exit doors
   5. Evidence room description
   6. Communications options (phone, Internet, LAN, WAN)

**Quick Quiz 1**

1. The \_\_\_\_\_ provides accreditation of crime and forensics labs worldwide.

Answer: ANSI-ASQ National Accreditation Board (ANAB)

1. The \_\_\_\_ identifies the number of hard disk types, such as SATA or SCSI, and the OS used to commit crimes.

Answer: Uniform Crime Report

1. True or False: To ensure a forensics lab’s efficiency, the lab manager sets reasonable production schedules for processing work.

Answer: True

1. To preserve the integrity of evidence, your lab should function as an evidence locker or safe, making it a(n) \_\_\_\_ or a secure storage safe.

Answer: secure facility

1. Certain kinds of equipment can intercept \_\_\_\_\_, which can be used to determine the data the device is transmitting or displaying.

Answer: EMR (electromagnetic radiation)

**Selecting a Basic Forensic Workstation**

1. Explain to your students that workstations should be selected according to your budget and need. Their use also depends on the tasks you have to do.

**Selecting Workstations for a Lab**

1. Describe the different technological problems police labs have to face dealing with a community.
2. Describe how to create a lightweight, mobile forensic workstation, which can be helpful in creating images of suspect drives in the field.

**Selecting Workstations for Private-Sector Labs**

1. Explain that this process is usually easier than for police labs since you deal with a more homogenous environment where you know exactly what kind of hardware and software platform are being used so you can plan your lab accordingly.

**Stocking Hardware Peripherals**

1. Explain what other items you should have in your lab besides workstations and software, including:
   1. Digital camera capable of still and motion recording
   2. Assorted antistatic bags
   3. An external CD/DVD drive
   4. 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
   5. Ribbon cables for floppy disks
   6. Extra USB 3.0 or newer cables and SATA cards and associated cables
   7. Extra SCSI cards, preferably ultrawide
   8. Graphics cards, both PCI and AGP types
   9. Assorted FireWire and USB adapters
   10. A variety of hard drives and USB drives
   11. At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
   12. Computer hand tools

|  |  |
| --- | --- |
| ***Teaching tips*** | Read more about the SATA interface at: [www.serialata.org/](http://www.serialata.org/). |

**Maintaining Operating Systems and Software Inventories**

1. Present your students with a list of operating systems and application software to keep licensed copies of in a forensics lab, including:
   1. Microsoft Office (current and older versions)
   2. Hexadecimal editor
   3. Programming languages
   4. Specialized image viewers
   5. WPS Office, WordPerfect, and a third-party or open-source office suite
   6. Accounting applications, such as Quicken and QuickBooks

**Using a Disaster Recovery Plan**

1. Outline a good disaster recovery plan that includes:
   1. Recovering from catastrophic situations
   2. Severe virus infection
   3. Workstation reconfigurations
   4. Backup policies and tools for single disks and RAID servers
   5. Configuration management tools to keep track of software updates

|  |  |
| --- | --- |
| ***Teaching tips*** | Read more about configuration management at: <http://searchdatacenter.techtarget.com/definition/configuration-management-CM> |

**Planning for Equipment Upgrades**

1. Explain that risk management involves determining how much risk is acceptable for any process or operation.
2. Explain how to identify equipment you depend on so it can be periodically replaced.
3. Explain how to identify equipment you can replace when it fails.
4. Remember that computing equipment is meant to last 18 to 36 months under normal conditions, so you should schedule upgrades accordingly.

|  |  |
| --- | --- |
| ***Teaching tips*** | Read more about risk management at: <http://www.theirm.org/about/risk-management/> |

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

1. Explain to your class that the best way to get approval for purchases is by showing that at the end, the innovation will reduce costs and increase profits.
2. Show your students good arguments to include when preparing a business case for developing a forensics lab. For example, forensic investigations can help the organization in reducing its litigation costs and establishing a better protection level for intellectual property, trade secrets, and future business plans.
3. Share some examples in which a forensics investigation will help reduce costs.

**Preparing a Business Case for a Computer Forensics Lab**

1. Outline the different stages you need to follow when preparing a business case:
   1. Justification
   2. Budget development
   3. Facility cost
   4. Hardware requirements
   5. Software requirements
   6. Miscellaneous budget needs
   7. Approval and acquisition
   8. Implementation
   9. Acceptance testing
   10. Correction for acceptance
   11. Production
2. Mention that the better you plan for your case, the more likely it will be accepted and funded.

**Quick Quiz 2**

1. One way to investigate older and unusual computing systems is to keep track of \_\_\_\_ that still use these old systems.

Answer: forums and blogs

1. A(n) \_\_\_\_ ensures that you can restore your workstations and investigation file servers to their original condition in the presence of a catastrophic failure.

Answer: disaster recovery plan

1. \_\_\_\_ involves determining how much risk is acceptable for any process or operation, such as replacing equipment.

Answer: Risk management

1. A(n)\_\_\_\_is a plan you can use to sell your services to your management or clients.

Answer: business case

1. When determining how much floor space is needed for your lab, a good rule of thumb is to plan for \_\_\_\_\_\_square feet per person.

Answer: 150

# **Class Discussion Topics**

1. Discuss some advantages and disadvantages of mobile forensic workstations implemented using laptop PCs.
2. Compare a business case to a Return of Investment (ROI) plan. Are they the same? If not, what are the differences?

# **Additional Projects**

1. Have students perform a risk evaluation of the equipment in the computer lab that they are working in right now and write a report with their findings.
2. Have students investigate several low-emanation workstation brands, and ask them to write a report about the brands’ advantages and disadvantages.

# **Additional Resources**

1. Helix Live CD:

[www.e-fense.com/helix/index.php](http://www.e-fense.com/helix/index.php)

1. International Association of Computer Investigative Specialists (IACIS):

[www.iacis.org/](http://www.iacis.org/)

1. High-Tech Crime Network (HTCN):

[www.htcn.org/](http://www.htcn.org/)

1. Forensic discovery auditing of digital evidence containers:

<http://www.sciencedirect.com/science/article/pii/S1742287607000291>

1. Serial ATA:

<http://www.intel.com/content/www/us/en/io/serial-ata/serial-ata-developer.html>

1. Disaster recovery planning Web sites:
   1. Disaster Recovery Toolkit: [www.ebrp.net/](http://www.ebrp.net/)
   2. Disaster Recovery Resources: <http://labmice.techtarget.com/disaster.htm>
2. Risk Management:

[www.managementhelp.org/risk\_mng/risk\_mng.htm](http://www.managementhelp.org/risk_mng/risk_mng.htm)

**Key Terms**

* **ANSI-ASQ National Accreditation Board (ASCLD)** — A wholly owned subsidiary of ANSI (American National Standards Institute) and ASQ (American Society for Quality), provides accreditation of crime and forensics labs worldwide.
* **business case** — A plan you can use to sell your services to management or clients.
* **Certified Computer Examiner (CCE)** — A certification from the International Society of Forensic Computer Examiners.
* **Certified Cyber Forensic Professional (CCFP)** — A certification from ISC² for completing the education and work experience and passing the exam.
* **Certified Forensic Computer Examiner (CFCE)** — A certificate awarded by IACIS at completion of all portions of the exam.
* **configuration management** — The process of keeping track of all upgrades and patches you apply to your computer’s OS and applications.
* **digital forensics lab** — A computer lab dedicated to investigations; typically, it has a variety of computers, OSs, and forensics software.
* **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.
* **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 easily monitored or accessed 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.