# Guide to Computer Forensics and Investigations Sixth Edition

## *Chapter 2*

*The Investigator's Office and Laboratory*

CENGAGE

# 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

# Understanding Forensics Lab Certification Requirements

- **Digital forensics lab**
  - Where you conduct your investigation
  - Store evidence
  - House your equipment, hardware, and software
- **ANSI-ASQ National Accreditation Board (ANAB)**
  - Provides accreditation of crime and forensics labs worldwide
  - Accreditation includes forensics labs that analyze digital evidence
  - Audits lab functions and procedures

# Identifying Duties of the Lab Manager and Staff (1 of 2)

- Lab manager duties:
  - Set up processes for managing cases
  - Promote group consensus in decision making
  - Maintain fiscal responsibility for lab needs
  - Enforce ethical standards among lab staff members
  - Plan updates for the lab
  - Establish and promote quality-assurance processes
  - Set reasonable production schedules
  - Estimate how many cases an investigator can handle

# Identifying Duties of the Lab Manager and Staff (2 of 2)

- Lab manager duties (cont'd):
  - Estimate when to expect preliminary and final results
  - Create and monitor lab policies for staff
  - Provide a safe and secure workplace for staff and evidence
- Staff member duties:
  - Knowledge and training:
    - Hardware and software
    - OS and file types
    - Deductive reasoning
  - Work is reviewed regularly by the lab manager
- Check the ANAB Web site for online manual and information

# Lab Budget Planning (1 of 3)

- Break costs down into monthly, quarterly, and annual expenses
- Use past investigation expenses to extrapolate expected future costs
- Expenses for a lab include:
  - Hardware
  - Software
  - Facility space
  - Training personnel

# Lab Budget Planning (2 of 3)

- Estimate the number of cases your lab expects to examine
  - Identify types of computers you’re likely to examine
- Take into account changes in technology
- Use statistics to determine what kind of computer crimes are more likely to occur
- Use this information to plan ahead your lab requirements and costs

# Lab Budget Planning (3 of 3)

- Check statistics from the **Uniform Crime Report**
  - For federal reports
- Identify crimes committed with specialized software
- When setting up a lab for a private company, check:
  - Hardware and software inventory
  - Problems reported last year
  - Future developments in computing technology
- Time management is a major issue when choosing software and hardware to purchase

# Acquiring Certification and Training (1 of 5)

- Update your skills through appropriate training
  - Thoroughly research the requirements, cost, and acceptability in your area of employment
- International Association of Computer Investigative Specialists (IACIS)
  - Created by police officers who wanted to formalize credentials in digital investigations
  - Candidates who complete the IACIS test are designated as a **Certified Forensic Computer Examiner (CFCE)**

# Acquiring Certification and Training (2 of 5)

- **ISC$^2$ Certified Cyber Forensics Professional (CCFP)**
  - Requires knowledge of
    - Digital forensics
    - Malware analysis
    - Incident response
    - E-discovery
    - Other disciplines related to cyber investigations

# Acquiring Certification and Training (3 of 5)

- **High-Tech Crime Network (HTCN)**
    - Certified Computer Crime Investigator, Basic and Advanced Level
    - Certified Computer Forensic Technician, Basic and Advanced Level
- **EnCase Certified Examiner (EnCE) Certification**
    - Open to the public and private sectors
    - Specific to use and mastery of EnCase forensics analysis
    - Candidates are required to have a licensed copy of EnCase

# Acquiring Certification and Training (4 of 5)

- AccessData Certified Examiner (ACE) Certification
  - Open to the public and private sectors
  - Specific to use and mastery of AccessData Ultimate Toolkit
  - The exam has a knowledge base component and a practical skills component
- Other Training and Certifications
  - EC-Council
  - SysAdmin, Audit, Network, Security (SANS) Institute
  - Defense Cyber Investigations Training Academy (DCITA)

# Acquiring Certification and Training (5 of 5)

- Other training and certifications (cont’d)
  - International Society of Forensic Computer Examiners (ISFCE)
  - Computer Technology Investigators Network (CTIN)
  - Digital Forensics Certification Board (DFCB)
  - Cloud Security Alliance (CSA)
  - Federal Law Enforcement Training Center (FLETC)
  - National White Collar Crime Center (NW3C)

# Determining the Physical Requirements for a Computer Forensics Lab

- Most of your investigation is conducted in a lab
- Lab should be secure so evidence is not lost, corrupted, or destroyed
- Provide a safe and secure physical environment
- Keep inventory control of your assets
    - Know when to order more supplies

# Identifying Lab Security Needs

- **Secure facility**
  - Should preserve integrity of evidence data
- Minimum requirements
  - Small room with true floor-to-ceiling walls
  - Door access with a locking mechanism
  - Secure container
  - Visitor’s log
- People working together should have same access level
- Brief your staff about security policy

# Conducting High-Risk Investigations

- High-risk investigations demand more security than the minimum lab requirements
  - **TEMPEST** facilities
    - Electromagnetic Radiation (EMR) proofed
  - TEMPEST facilities are very expensive
    - You can use low-emanation workstations instead

# Using Evidence Containers (1 of 4)

- Known as evidence lockers
  - Must be secure so that no unauthorized person can easily access your evidence
- Recommendations for securing storage containers:
  - Locate them in a restricted area
  - Limited number of authorized people to access the container
  - Maintain records on who is authorized to access each container
  - Containers should remain locked when not in use

# Using Evidence Containers (2 of 4)

- If a combination locking system is used:
  - Provide the same level of security for the combination as for the container’s contents
  - Destroy any previous combinations after setting up a new combination
  - Allow only authorized personnel to change lock combinations
  - Change the combination every six months or when required

# Using Evidence Containers (3 of 4)

- If you’re using a keyed padlock:
  - Appoint a key custodian
  - Stamp sequential numbers on each duplicate key
  - Maintain a registry listing which key is assigned to which authorized person
  - Conduct a monthly audit
  - Take an inventory of all keys
  - Place keys in a lockable container
  - Maintain the same level of security for keys as for evidence containers
  - Change locks and keys annually
  - Do not use a master key for several locks

# Using Evidence Containers (4 of 4)

- Container should be made of steel with an internal cabinet or external padlock
- If possible, acquire a media safe
- When possible, build an evidence storage room in your lab
- Keep an evidence log
  - Update it every time an evidence container is opened and closed

# Overseeing Facility Maintenance

- Immediately repair physical damages
- Escort cleaning crews as they work
- Minimize the risk of static electricity
  - Antistatic pads
  - Clean floor and carpets
- Maintain two separate trash containers
  - Materials unrelated to an investigation
  - Sensitive materials
- When possible, hire specialized companies for disposing sensitive materials

# Considering Physical Security Needs

- Enhance security by setting security policies
- Enforce your policy
  - Maintain a sign-in log for visitors
    - Anyone that is not assigned to the lab is a visitor
    - Escort all visitors all the time
  - Use visible or audible indicators that a visitor is inside your premises
    - Visitor badge
  - Install an intrusion alarm system
  - Hire a guard force for your lab

# Auditing a Digital Forensics Lab

- Auditing ensures proper enforcing of policies
- Audits should include inspecting the following facility components and practices:
  - Ceiling, floor, roof, and exterior walls of the lab
  - Doors and doors locks
  - Visitor logs
  - Evidence container logs
  - At the end of every workday, secure any evidence that’s not being processed in a forensic workstation

# Determining Floor Plans for Digital Forensics Labs (1 of 7)

- How you configure the work area will depend on:
  - Your budget
  - Amount of available floor space
  - Number of computers you assign to each computing investigator
- Ideal configuration is to have:
  - Two forensic workstations
  - One non-forensic workstation with Internet access

# Determining Floor Plans for Digital Forensics Labs (2 of 7)

- Small labs usually consist of:
  - One or two forensic workstations
  - A research computer with Internet access
  - A workbench (if space allows)
  - Storage cabinets

# Determining Floor Plans for Digital Forensics Labs (3 of 7)

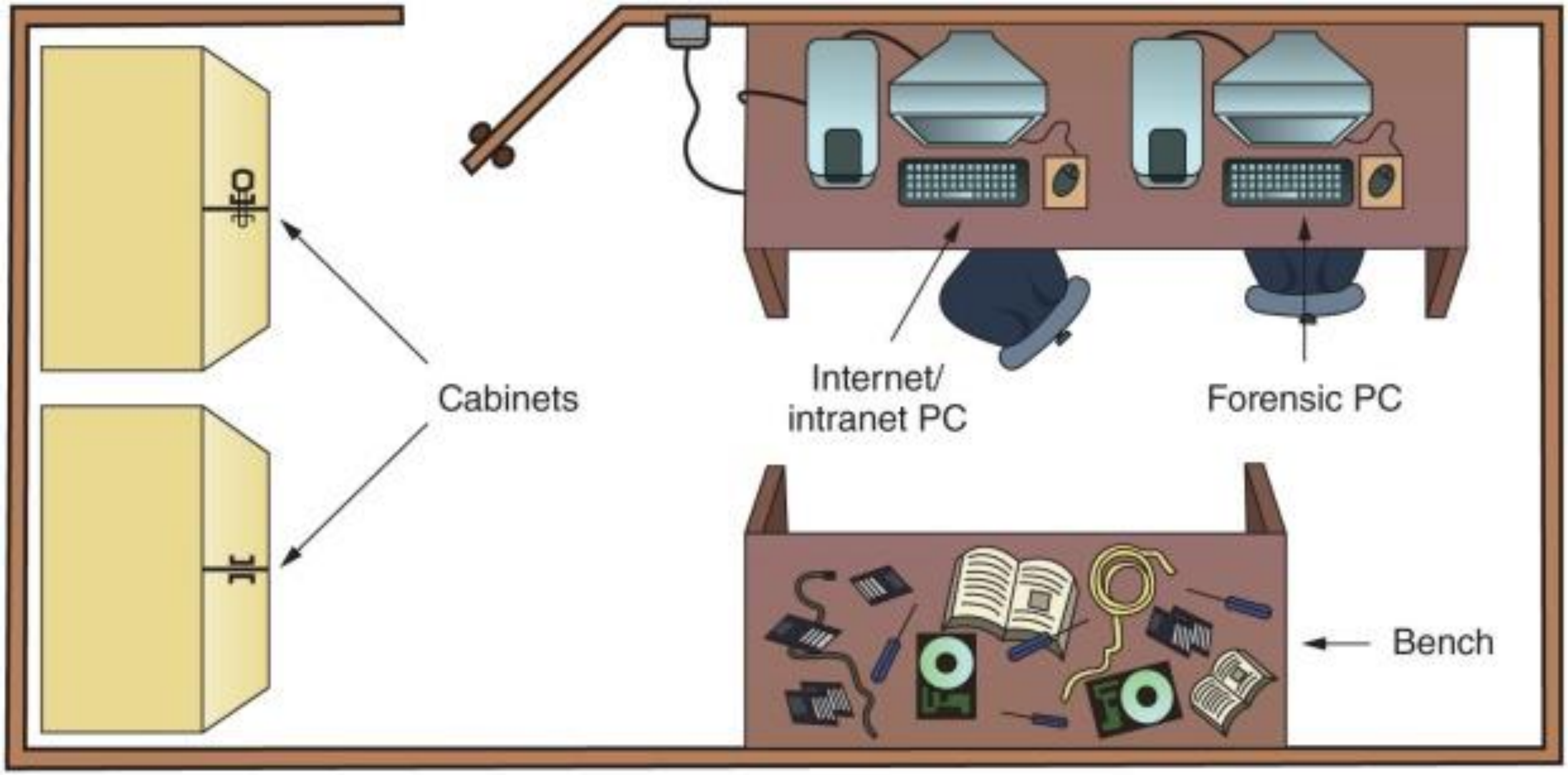

Figure 2-2 Small or home-based lab

# Determining Floor Plans for Digital Forensics Labs (4 of 7)

- Mid-size labs are typically those in a private business
  - Have more workstations
  - Should have at least two exits, for safety reasons
  - Cubicles or separate offices should be part of the layout to reinforce need-to-know policy
  - More library space for software and hardware storage

# Determining Floor Plans for Digital Forensics Labs (5 of 7)

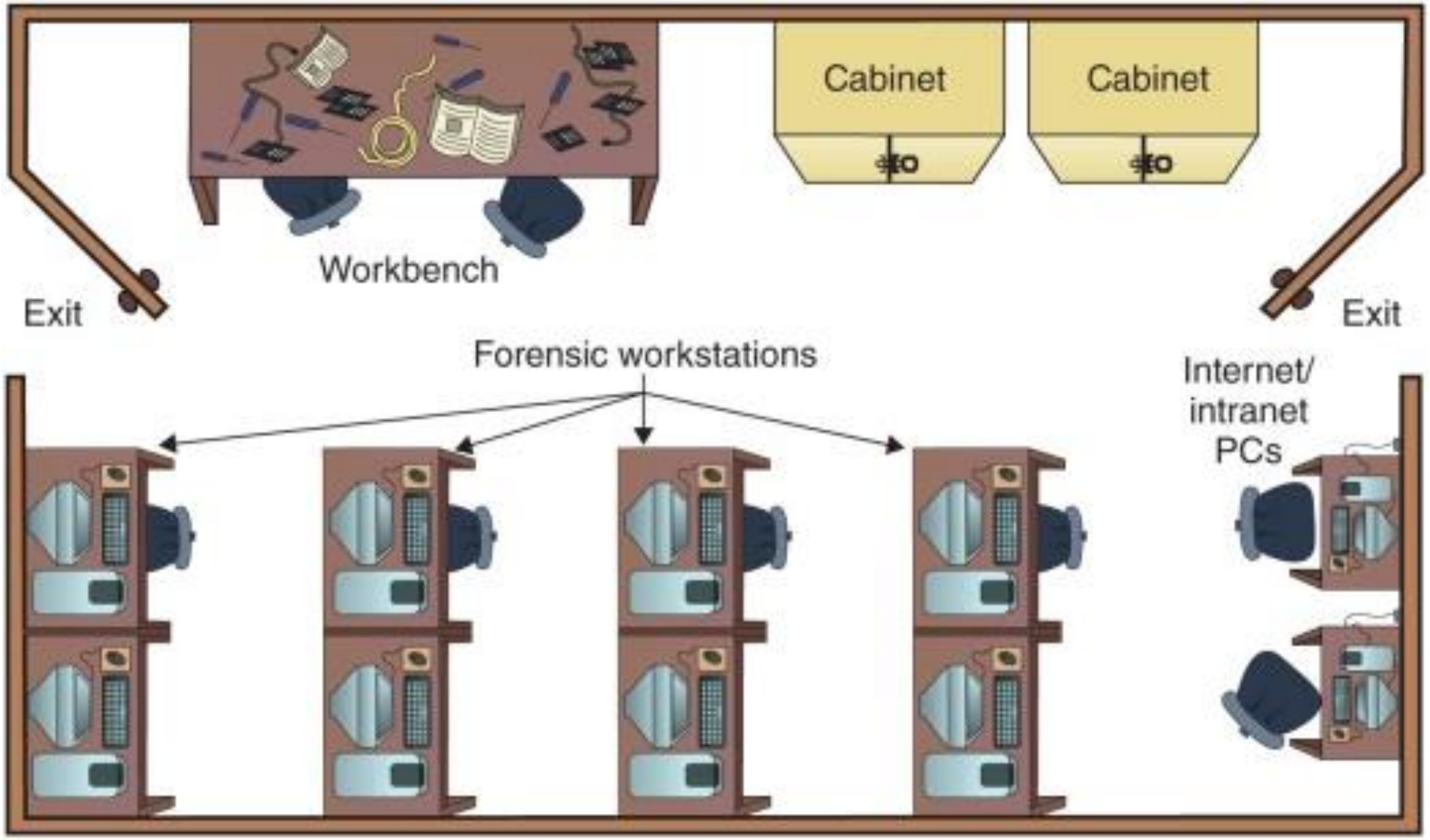

**Figure 2-3** Mid-size digital forensics lab

# Determining Floor Plans for Digital Forensics Labs (6 of 7)

- State law enforcement or the FBI usually runs most large or regional digital forensics labs
  - Have a separate evidence room
  - One or more custodians might be assigned to manage and control traffic in and out of the evidence room
  - Should have at least two controlled exits and no windows

# Determining Floor Plans for Digital Forensics Labs (7 of 7)

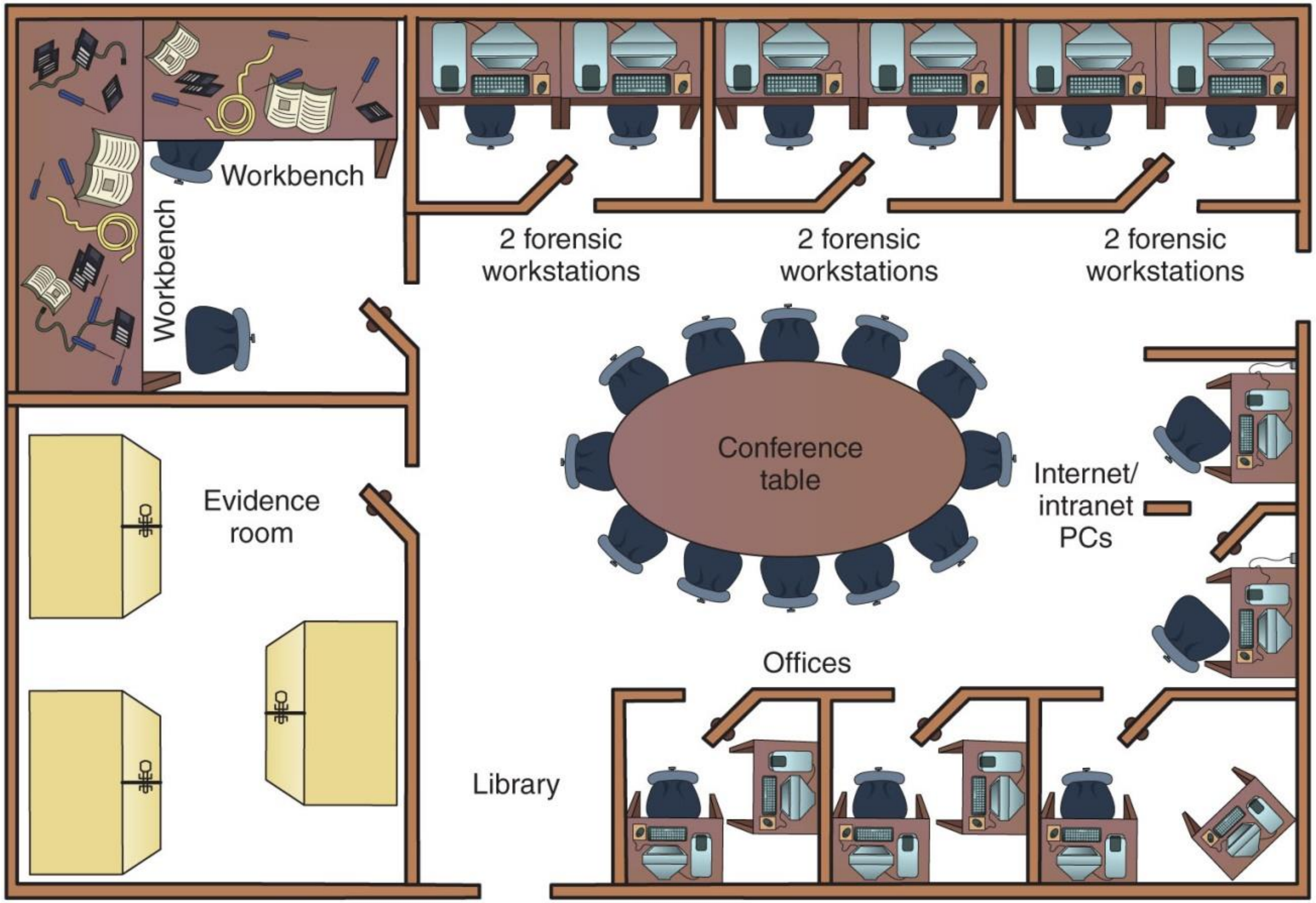

**Figure 2-4** Regional digital forensics lab

# Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for resource-heavy analysis tasks

# Selecting Workstations for a Lab

- Police labs have the most diverse needs for computing investigation tools
  - A lab might need legacy systems and software to match what’s used in the community
- A small, local police department might have one multipurpose forensic workstation with one or two basic workstations or high-end laptops
- You can now use a laptop PC with USB 3.0 or SATA hard disks to create a lightweight, mobile forensic workstation

# Selecting Workstations for Private-Sector Labs

- Requirements are easy to determine
  - Businesses can conduct internal investigations
- Identify the environment you deal with
  - Hardware platform
  - Operating system
- With some digital forensics programs
  - You can work from a Windows PC and examine both Windows and Macintosh disk drives

# Stocking Hardware Peripherals

- Any lab should have in stock:
  - Digital camera
  - Assorted antistatic bags
  - External CD/DVD drive
  - IDE cables
  - Ribbon cables for floppy disks
  - Extra USB 3.0 or newer cables and SATA cards
  - SCSI cards, preferably ultrawide
  - Graphics cards, both PCI and AGP types
  - Assorted FireWire and USB adapters
  - Hard disk drives and USB drives
  - At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
  - Computer hand tools

# Maintaining Operating Systems and Software Inventories

- Maintain licensed copies of software such as:
  - Microsoft Office (current and older version)
  - Hexadecimal editor
  - Programming languages (Visual Studio, Perl, or Python)
  - Specialized viewers (Quick View)
  - Third-party or open-source office suite
  - Quicken and QuickBooks accounting applications

# Using a Disaster Recovery Plan

- A disaster recovery plan ensures that you can restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- Includes backup tools such as Norton Ghost
- **Configuration management**
  - Keep track of software updates to your workstation
- For labs using high-end RAID servers:
  - You must consider methods for restoring large data sets
  - Large-end servers must have adequate data backup systems in case of a major failure or more than one drive

# Planning for Equipment Upgrades

- **Risk management**
  - Involves determining how much risk is acceptable for any process or operation
  - Identify equipment your lab depends on so it can be periodically replaced
  - Identify equipment you can replace when it fails
- Computing components last 18 to 36 months under normal conditions
  - Schedule upgrades at least every 18 months
    - Preferably every 12 months

# Building a Business Case for Developing a Forensics Lab

- Enlist the support of managers and other team members
- **Business case**
  - Plan you can use to sell your services to management or clients
- Demonstrate how the lab will help your organization to save money and increase profits
  - Compare cost of an investigation with cost of a lawsuit
  - Protect intellectual property, trade secrets, and future business plans

# Preparing a Business Case for a Digital Forensics Lab (1 of 3)

- Investigators must plan ahead to ensure that money is available for facilities, tools, supplies, and training for your forensics lab
- **Justification**
  - You need to justify to the person controlling the budget the reason a lab is needed
  - Requires constant efforts to market the lab’s services to previous, current, and future customers and clients
- **Budget development** - needs to include:
  - Facility cost
  - Hardware requirements
  - Software requirements
  - Miscellaneous budget needs

# Preparing a Business Case for a Digital Forensics Lab (2 of 3)

- **Approval and acquisition**
  - You must present a business case with a budget to upper management for approval
- **Implementation**
  - 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
  - Schedule inspection dates

# Preparing a Business Case for a Digital Forensics Lab (3 of 3)

- **Acceptance testing** - consider the following items:
  - Inspect the facility to make sure it meets security criteria for containing and controlling digital evidence
  - Test all communications
  - Test all hardware to verify it is operational
  - Install and start all software tools
- **Correction for Acceptance**
  - Your business case must anticipate problems that can cause delays in lab production
- **Production**
  - After all essential corrections have been made the lab can go into production
  - Implement lab operations procedures

# Summary (1 of 2)

- A digital forensics lab is where you conduct investigations, store evidence, and do most of your work
- Seek to upgrade your skills through training
- A lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed
- It is harder to plan a computer forensics lab for a police department than for a private organization or corporation

# Summary (2 of 2)

- A forensic workstation needs to have adequate memory, storage, and ports to deal with common types of cases that come through the lab
- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab