Guide to Computer Forensics and Investigations Sixth Edition

Chapter 2

The Investigator's Office and Laboratory

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**

Digital Forensic lab

- Ideally…

- In real life…

Understanding Forensics Lab Certification Requirements

- **Digital forensics lab**
  - Where you conduct your investigation
  - Store evidence
  - House your equipment, hardware, and software

- **American Society of Crime Laboratory Directors (ASCLD)** offers guidelines for:
  - Managing a lab
  - Acquiring an official certification
  - Auditing lab functions and procedures

Ref : www.tn.gov/

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

- **Lab Manager** duties:
  - Set up **processes** for managing cases - ***Processes*** *should be review regularly*
  - 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 *– Ensure that staff know what to do when a case arrive*
  - Set reasonable production schedules – *based on existing resources*
  - Estimate how many cases an investigator can handle *– Certain case can longer due to nature of case*

Identifying Duties of the Lab Manager and Staff

- 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:
  - Have **Knowledge** and **Training**:
    - Hardware and software
    - OS and file types
    - Deductive reasoning
    - Work is reviewed regularly by the lab manager – *to ensure that quality of work is maintained*

Identifying Duties of the Lab Manager and Staff

- Check the ASCLD Web site for online manual and information

AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORS

"Excellence through leadership in forensic science management"

Lab Budget Planning

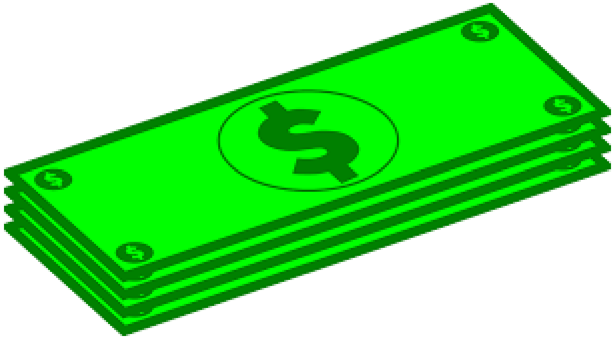
- Break costs down into daily, quarterly, and annual expenses – *The better you understand these expenses, the better you can delegate resources for each investigation.*

- Use past investigation expenses to extrapolate (*extract*) expected future costs – *similar to any budget estimation*

- Expenses for a lab include:
  - Hardware
  - Software
  - Facility space
  - Training personnel

Lab Budget Planning (cont)

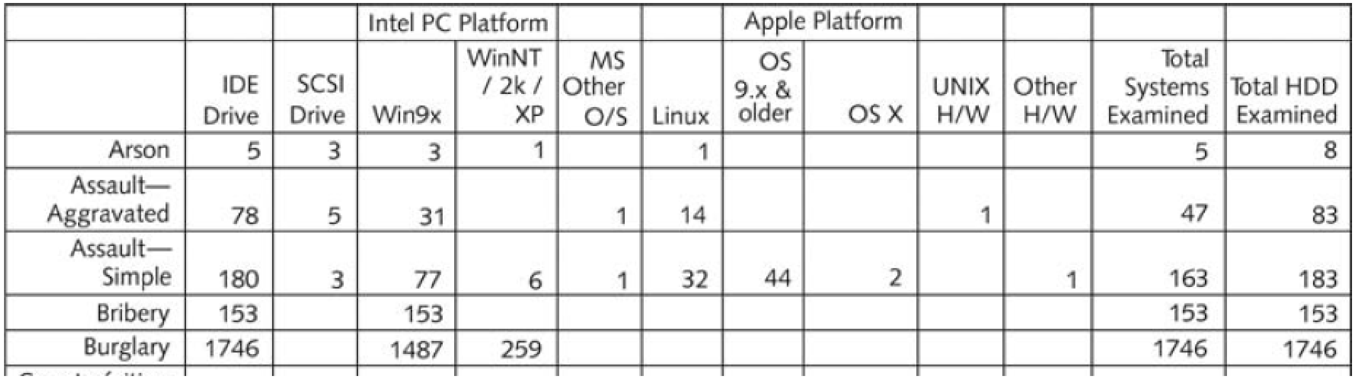
- Estimate the number of computer cases your lab expects to examine
  - Identify types of computers you're likely to examine
- Take into account changes in technology – *s/w n h/w upgrade*
- Use statistics to determine what kind of computer crimes are more likely to occur – *so you can better estimate the resource you need!*
- Use this information to plan ahead your lab requirements and costs



Lab Budget Planning (cont)

- 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** *(for better resource utilization)* is a major issue when choosing software and hardware to purchase



			Intel PC Platform				Apple Platform					
	IDE Drive	SCSI Drive	Win9x	WinNT / 2k / XP	MS Other O/S	Linux	OS 9.x & older	OS X	UNIX H/W	Other H/W	Total Systems Examined	Total HDD Examined
Arson	5	3	3	1		1					5	8
Assault—Aggravated	78	5	31		1	14			1		47	83
Assault—Simple	180	3	77	6	1	32	44	2		1	163	183
Bribery	153		153								153	153
Burglary	1746		1487	259							1746	1746

Acquiring Certification and Training

- Update your skills through appropriate training
  - Thoroughly research the requirements, cost, and acceptability in your area of employment
  - *Address the minimum skills for conducting computing investigations at various levels.*

- International Association of Computer Investigative Specialists (IACIS)
  - **Created by police officers** who wanted to formalize credentials in computing investigations
  - Candidates who complete the IACIS test are designated as a **Certified Forensic Computer Examiner (CFCE)**

Acquiring Certification and Training (cont)

- AccessData Certified Examiner (**ACE**) Certification
  - Open to the public and private sectors
  - Is specific to use and mastery of AccessData Ultimate Toolkit
  - The exam has a knowledge base assessment (KBA) and a practical skills assessment (PSA)

- Other Training and Certifications
  - EC-Council
  - SysAdmin, Audit, Network, Security (SANS) Institute – *can be expensive*
  - Defense Cyber Investigations Training Academy (DCITA)

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 what you have and what you don't have*
  - 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 – *leaking signal can be used to reconstruct information*
    - *Such facilities can stop information systems from leaking through emanations, including unintentional radio or electrical signals, sounds, and vibrations.*

https://www.ramayes.com/_images/USC/Universal_DNB_Shielded_Room.jpg

  - TEMPEST facilities are very expensive
    - You can use **low-emanation workstations** instead

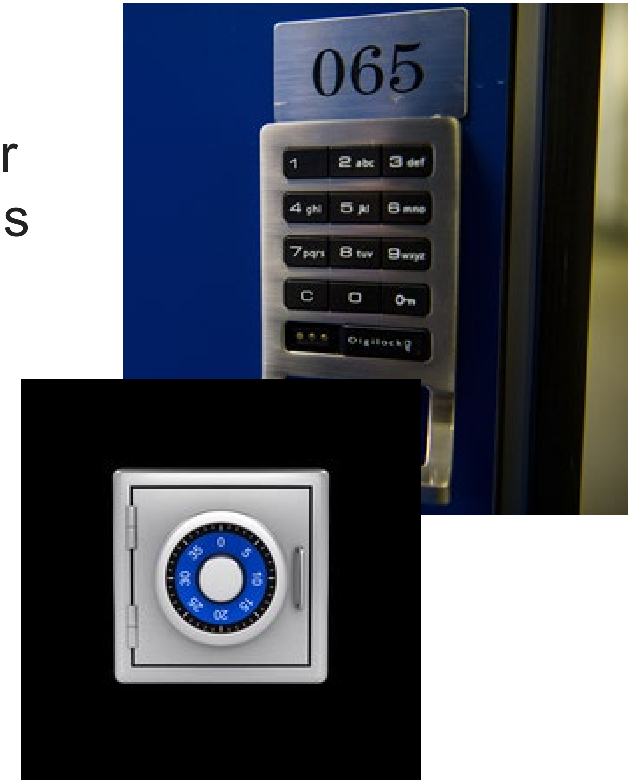
Using Evidence Containers

- Known as evidence lockers
  - Must be secure so that no unauthorized person can easily access your evidence

- Recommendations for securing storage containers:
  1. Locate them in a restricted area
  2. Limited number of authorized people to access the container
  3. Maintain records on who is authorized to access each container
  4. Containers should remain locked when not in use

Using Evidence Containers (Cont)

- If a combination locking system is used:
  1. Provide the same level of security for the combination as for the container's contents – *Need to protect the combination!*
  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



Using Evidence Containers (Cont)

- If you’re using a keyed padlock:
  1. Appoint a key custodian – *Someone responsible for distributing keys*
  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

Using Evidence Containers (Cont)

- Container should be made of **steel** with an internal cabinet or **external padlock**
- If possible, acquire a **media safe**
    - *Designed to protect electronic media*
- 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
  - ***Is it feasible?***
- Minimize the risk of **static electricity**
  - Antistatic pads
  - Clean floor and carpets – *minimize dust!*
- 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

VISITOR / VISITEUR
APR 2007
No 2-277532
VALID ONLY FOR DATE SHOWN / VALIDE POUR LA DATE INDIQUÉE SEULEMENT
RETURN TO SECURITY / RETOURNEZ À LA SÉCURITÉ

Auditing a Digital Forensics Lab

- Auditing ensures **proper enforcing of policies**
- Audits should include inspecting the following facility components and practices:
  1. Ceiling, floor, roof, and exterior walls of the lab
  2. Doors and doors locks
  3. Visitor **logs**
  4. Evidence container **logs**
  5. 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

- 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 work station for 2 to 3 cases a month*
  - One non-forensic workstation with Internet access

Determining Floor Plans for Digital Forensics Labs (Cont)

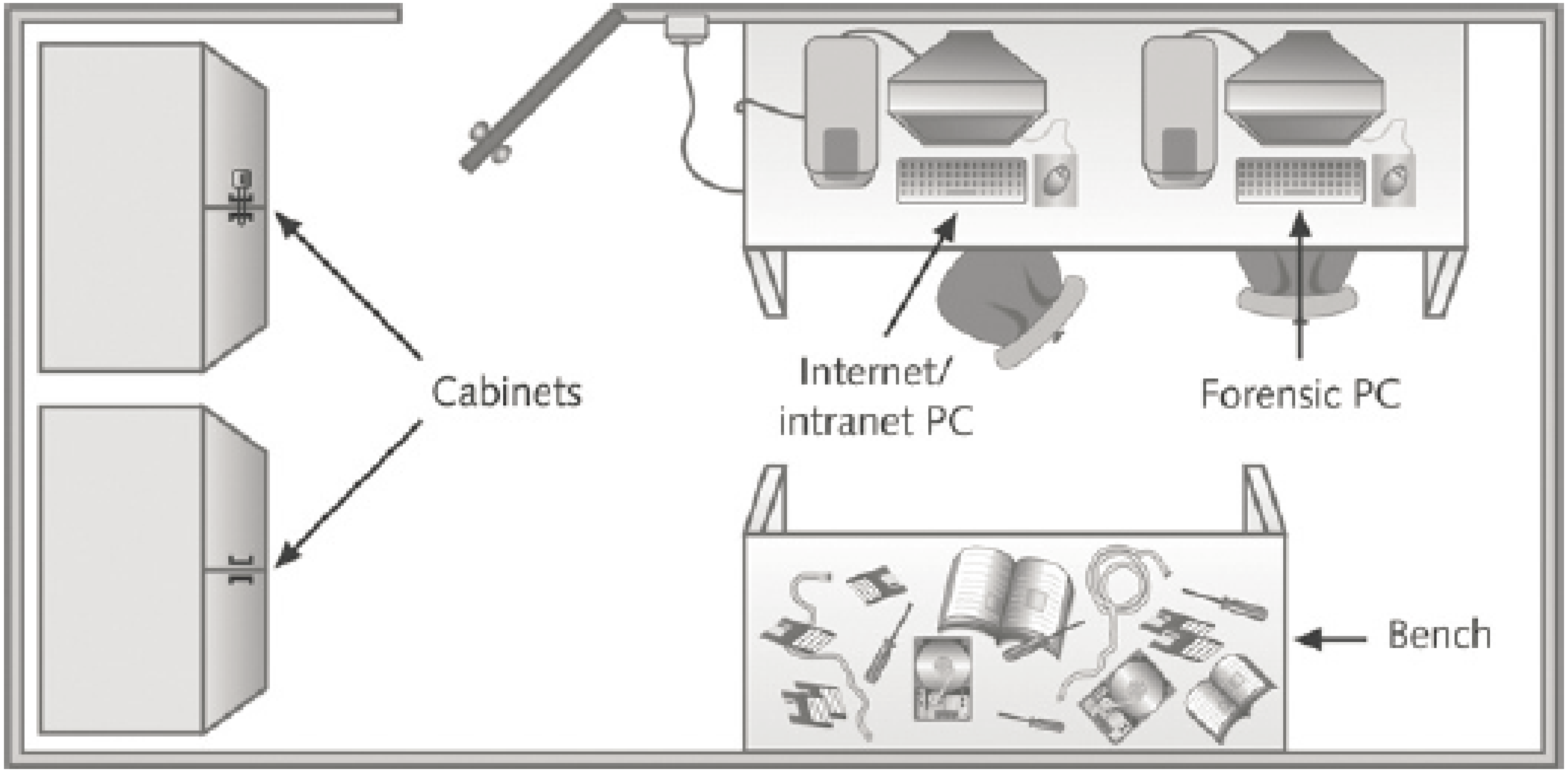


Figure 2-2 Small or home-based lab
©Cengage Learning®

Determining Floor Plans for Digital Forensics Labs (Cont)

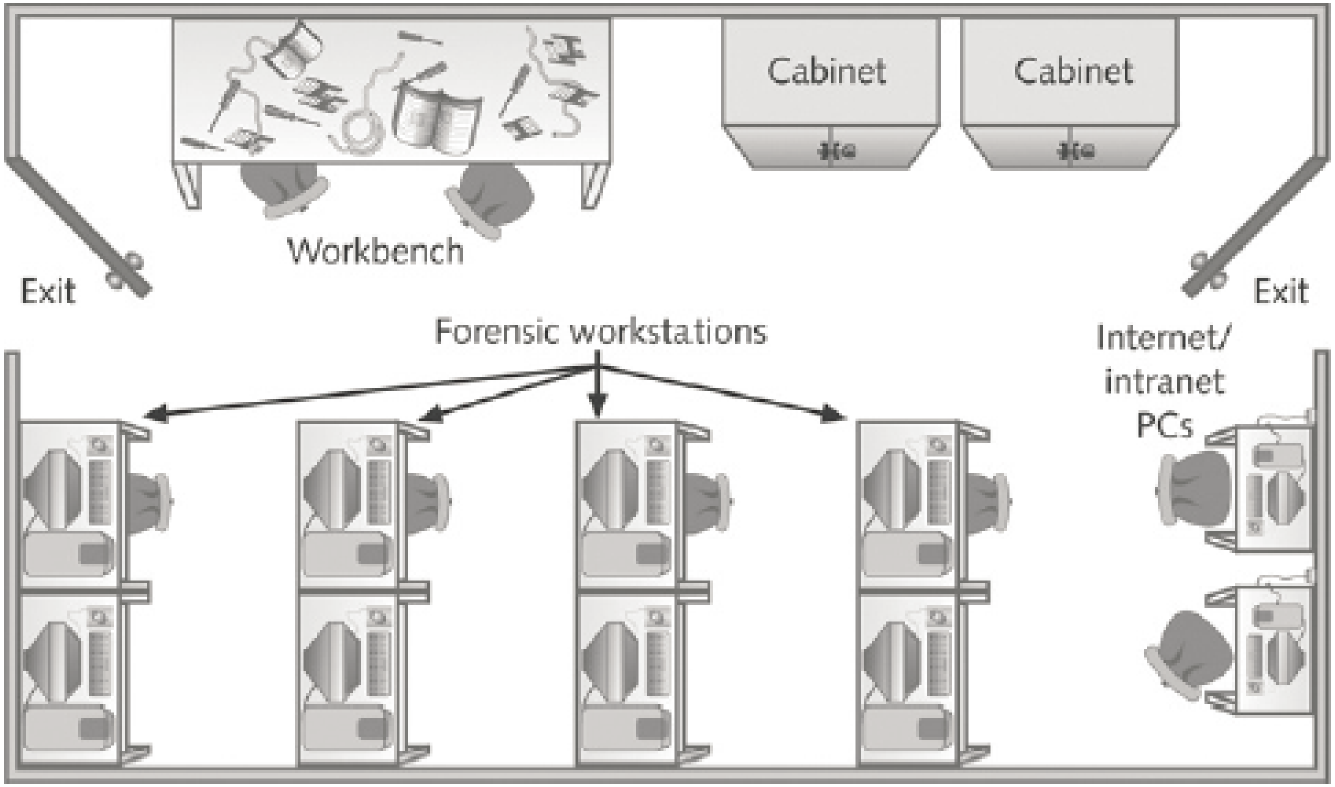


Figure 2-3 Mid-size digital forensics lab

©Cengage Learning®

Determining Floor Plans for Digital Forensics Labs (Cont)

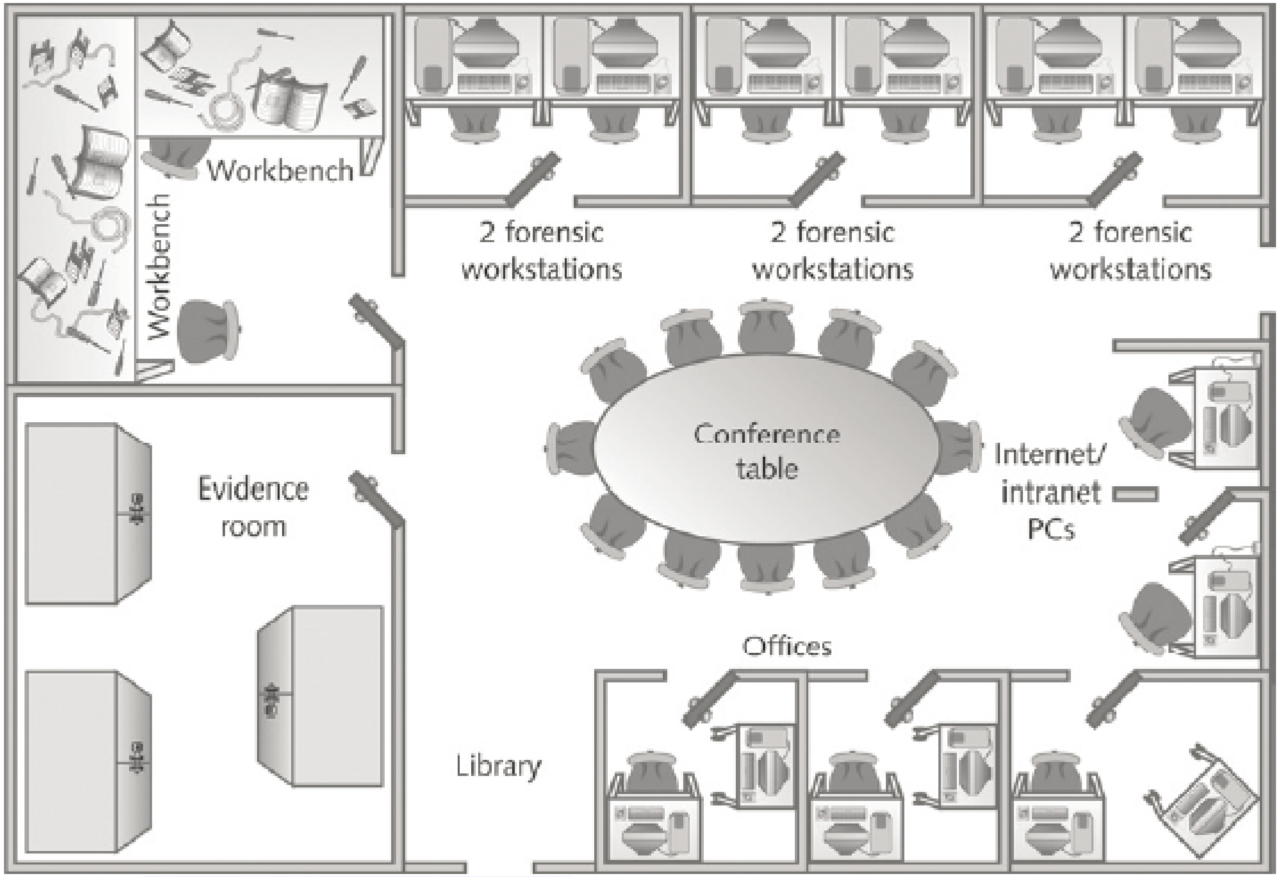


Figure 2-4 Regional digital forensics lab
©Cengage Learning®

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

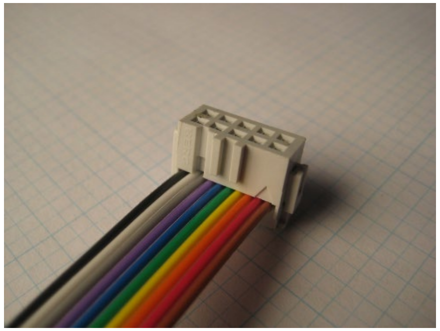
Ref : http://verity.com.sg

Selecting Workstations for a Lab

- Identify the environment you deal with
  - Hardware platform
  - Operating system – *Windows / Mac*
- 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 and one or two general-purpose workstations
- You can now use a laptop PC with FireWire, USB 3.0, or SATA hard disks to create a lightweight, mobile forensic workstation

Stocking **Hardware Peripherals**

- Any lab should have in stock:
  1. IDE cables
  2. Ribbon cables for floppy disks
  3. Extra USB 3.0 or newer cables and SATA cards
  4. SCSI cards, preferably ultrawide
  5. Graphics cards, both PCI and AGP types
  6. Assorted FireWire and USB adapters
  7. Hard disk drives
  8. At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
  9. Computer hand tools



Maintaining Operating Systems and Software Inventories

- Maintain **licensed copies of software** like:
  1. Microsoft Office (current and older version)
  2. Quicken - *personal finance management tool*
  3. Programming languages (Visual Basic and Visual C++)
  4. Specialized viewers (Quick View- *Viewer can be used to view practically any file*)
  5. LibreOffice, OpenOffice, or Apache OpenOffice
  6. Peachtree and QuickBooks accounting applications

Summary

- A digital forensics lab is where you conduct investigations, store evidence, and do most of your work
- Seek to upgrade your skills through training/certifcation
- 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

- 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 – Justification!!