Guide to Computer Forensics and Investigations Fourth Edition

Chapter 3

The Investigator's Office and Laboratory

Objectives

- 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

Understanding Forensics Lab Certification Requirements

Understanding Forensics Lab Certification Requirements

- **Computer 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

Identifying Duties of the Lab Manager and Staff

- 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 (continued)

- Lab manager duties (continued):
  - 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

Identifying Duties of the Lab Manager and Staff (continued)

- Staff member duties (continued):
  - Knowledge and training (continued):
    - Technical training
    - Investigative skills
    - Deductive reasoning
  - Work is reviewed regularly by the lab manager
- Check the ASCLD Web site for online manual and information (but it's not free, as far as I can tell)

Lab Budget Planning

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

Lab Budget Planning (continued)

- 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
- 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 (continued)

- Check statistics from the **Uniform Crime Report**
  - For federal reports, see *www.fbi.gov/ucr/ucr.htm*
- 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

Lab Budget Planning (continued)

			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
Counterfeiting & Forgery	1390	4	543	331		309	21	186			1390	1394
Destruction, Damage, & Vandalism	976	48	142	45	29	127	325	90	217	1	976	1024
Drug, Narcotic	1939	24	1345	213		158	213	10			1939	1963
Embezzlement	1023		320	549		23	87	41		3	1023	1023
Extortion & Blackmail	77		2	61		10	3	1			77	77
Fraud	2002		638	932	9	173	55	190		5	2002	2002
Gambling	4910	5	1509	2634		136	138	498			4915	4915
Homicide	36		5	11	9	1	3	7			36	36
Kidnapping & Abduction	2		1	1							2	2
Larceny Theft	7342	56	2134	3093	5	935	127	982	1	21	7298	7398
Motor Vehicle Theft	1747		231	1508		5	1	2			1747	1747
Child Porn	593	2	98	162		68	105	160	2		595	595
Robbery	33		23	7			2	1			33	33
Sex Offense—Forcible	80		21	45		1	5	8			80	80
Sex Offense—Non-Forcible	900		324	437		6	90	43			900	900
Stolen Property Offenses	2711	10	800	1634	3	169	53	37	1	9	2706	2721
Weapons Violations	203	1	43	89	2	11	28	31			204	204
Totals Per System	28126	161	9930	12018	59	2179	1300	2289	222	40	28037	28287
			HDD FAT/NTFS	22007				HDD Mac O/S X/Linux/ UNIX	2511			

Figure 3-1 Uniform Crime Report statistics

Acquiring Certification and Training

- Update your skills through appropriate training
- International Association of Computer Investigative Specialists (IACIS)
  - Created by police officers who wanted to formalize credentials in computing investigations
  - Only open to law enforcement officers or full-time civilian employees of law enforcement agencies
  - Certified Electronic Evidence Collection Specialist (CEECS)
  - Certified Forensic Computer Examiners (CFCEs)

Acquiring Certification and Training (continued)

- High-Tech Crime Network (HTCN)
  - Certified Computer Crime Investigator, Basic and Advanced Level
    - Basic requires 3 years of experience and 10 cases
  - Certified Computer Forensic Technician, Basic and Advanced Level

Acquiring Certification and Training (continued)

Certifications that are available without police experience

- EnCase Certified Examiner (EnCE) Certification
  - Link Ch 3d
- AccessData Certified Examiner (ACE) Certification
  - Link Ch 3e
- Other Training and Certifications
  - High Technology Crime Investigation Association (HTCIA)

Acquiring Certification and Training (continued)

- Other training and certifications
  - SysAdmin, Audit, Network, Security (SANS) Institute
  - Computer Technology Investigators Network (CTIN)
  - NewTechnologies, Inc. (NTI)
  - Southeast Cybercrime Institute at Kennesaw State University
  - Federal Law Enforcement Training Center (FLETC)
  - National White Collar Crime Center (NW3C)

CyberSecurity Forensic Analyst (CSFA)

- Steve Hailey's company in Washington State
- 70% of grade based on practical exam
- Three days to complete a case
  - Link Ch 3f

Recommended Certifications

- First get ACE Certification
- Then get CSFA
- We expect a local opportunity to get the CSFA within the next few months
- Doug Spindler from PacITPros is working on it
  - pacitpros.org
  - Meetings on the first Tuesday each month
  - Extra credit for attending

Determining the Physical Requirements for a Computer Forensics Lab

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 (national security or murder) demand more security to prevent computer eavesdropping
  - TEMPEST facilities
    - Electromagnetic Radiation (EMR) proofed
    - *http://nsi.org/Library/Govt/Nispom.html*
  - 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:
  - 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 (continued)

- 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 (continued)

- 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
  - Don't use a master key for several locks

Using Evidence Containers (continued)

- Container should be made of steel with an internal cabinet or external padlock
- If possible, acquire a media safe
  - Protects evidence from fire damage
- 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

- Create a security policy
- Enforce your policy
  - 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 Computer Forensics Lab

- Auditing ensures proper enforcing of policies
- Audits should include inspecting:
  - 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 Computer Forensics Labs

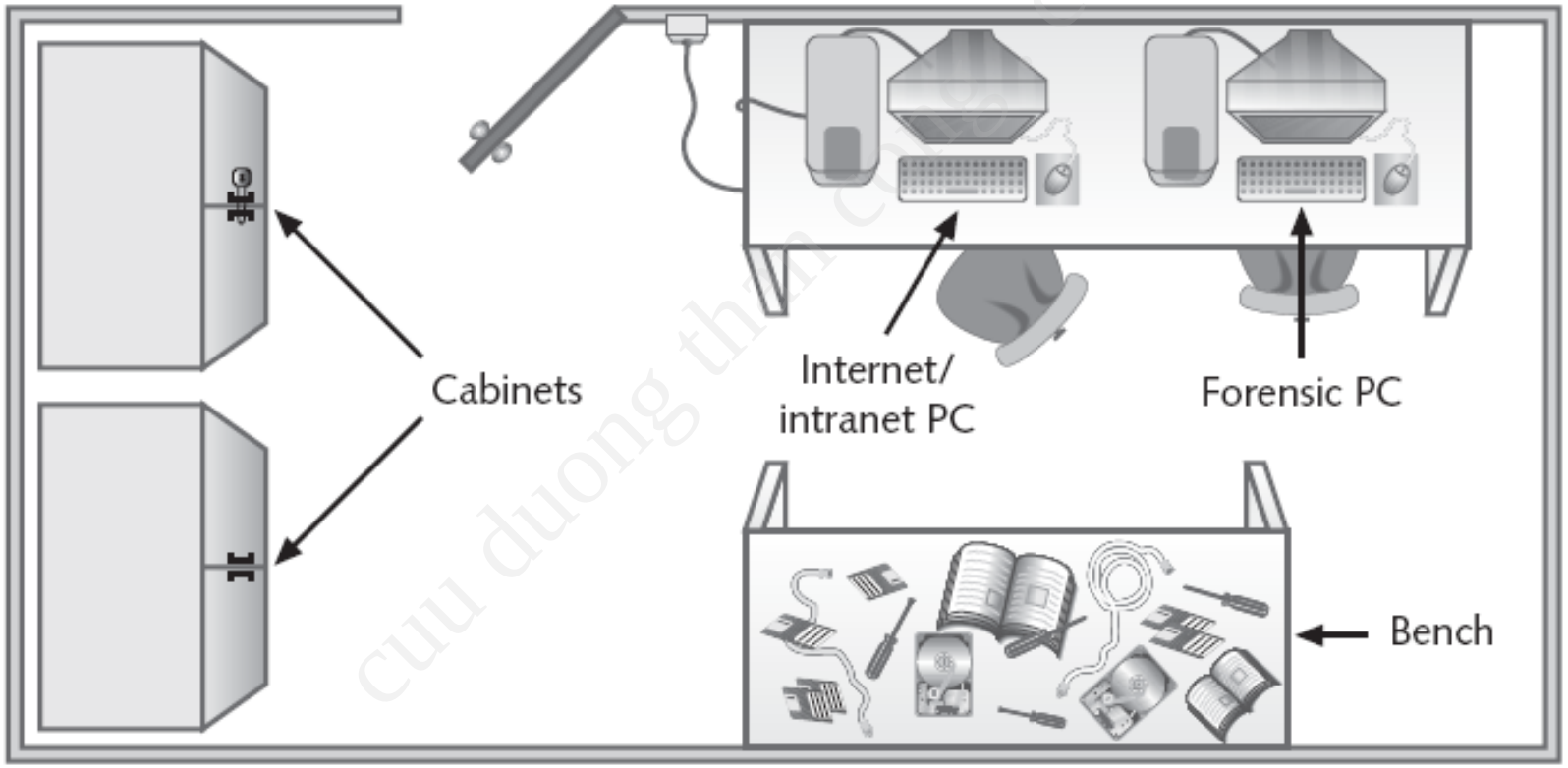

Figure 3-2 Small or home-based lab

Determining Floor Plans for Computer Forensics Labs (continued)

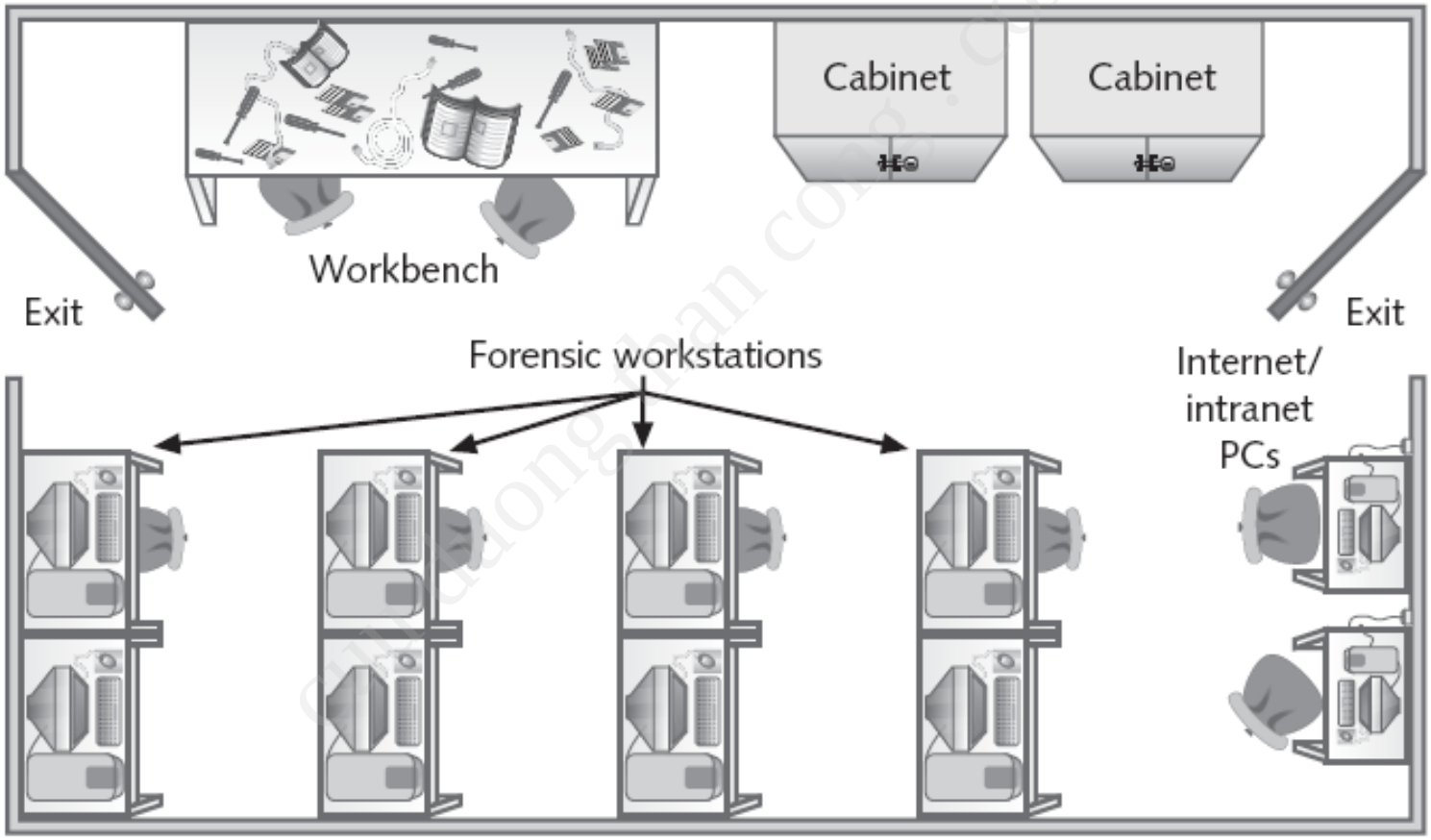

Figure 3-3 Mid-size computer forensics lab

Determining Floor Plans for Computer Forensics Labs (continued)

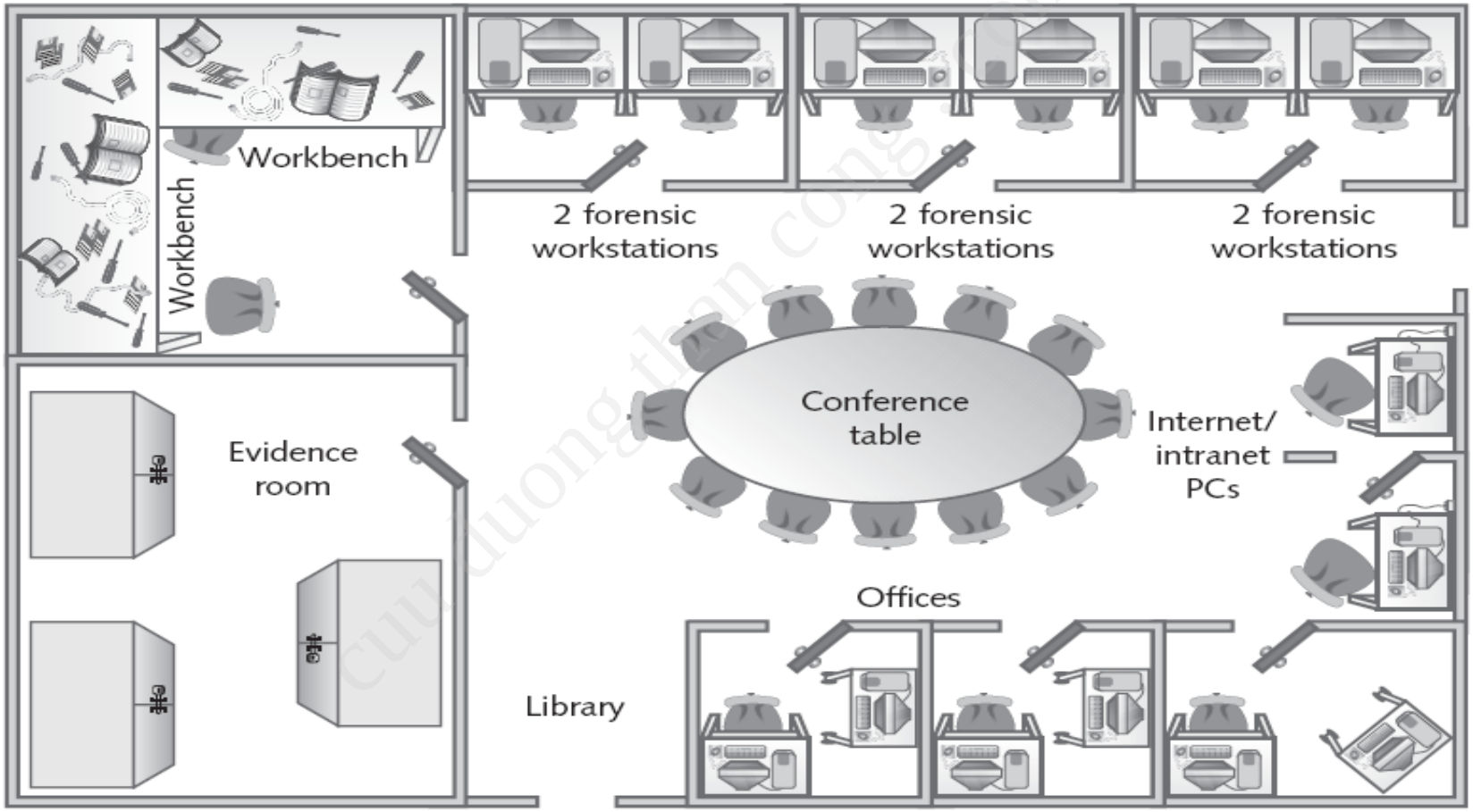

Figure 3-4 Regional computer forensics lab

Selecting a Basic Forensic Workstation

Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for high-end analysis tasks

Selecting Workstations for Police Labs

- Police labs have the most diverse needs for computing investigation tools
  - Special-interest groups (SIG) are helpful to investigate old systems, like CP/M, Commodore 64, etc.
- General rule
  - One computer investigator for every 250,000 people in a region
  - One multipurpose forensic workstation and one general-purpose workstation

Selecting Workstations for Private and Corporate Labs

- Requirements are easy to determine, because you can specialize
- Identify the environment you deal with
  - Hardware platform
  - Operating system
- Gather tools to work on the specified environment

Stocking Hardware Peripherals

- Any lab should have in stock:
  - IDE cables
  - Ribbon cables for floppy disks
  - SCSI cards, preferably ultra-wide
  - Graphics cards, both PCI and AGP types
  - Power cords
  - Hard disk 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 like:
  - Microsoft Office 2007, XP, 2003, 2000, 97, and 95
  - Quicken
  - Programming languages
  - Specialized viewers
  - Corel Office Suite
  - StarOffice/OpenOffice
  - Peachtree accounting applications

Using a Disaster Recovery Plan

- Keep regular backups, using Ghost or other utilities
  - Win 7 has *Windows Image Backup*
- Store backups off-site but securely
- Be able to restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- **Configuration management**
  - Keep track of software updates to your workstation

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

Using Laptop Forensic Workstations

- Create a lightweight, mobile forensic workstation using a laptop PC
  - FireWire port
  - USB 2.0 port
  - PCMCIA SATA hard disk
- Laptops are still limited as forensic workstations
  - But improving

Building a Business Case for Developing a Forensics Lab

Building a Business Case for Developing a Forensics Lab

- Can be a problem because of budget problems
- **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 Computer Forensics Lab

- When preparing your case, follow these steps:
  - Justification
  - Budget development
    - Facility cost
    - Computer hardware requirements
    - Software requirements
    - Miscellaneous costs
      - Errors and Omissions Insurance!
  - Approval and acquisition
  - Implementation

Preparing a Business Case for a Computer Forensics Lab (continued)

- Steps:
  - Acceptance testing
  - Correction for acceptance
  - Production