Objectives

• Understand computer forensics lab certification requirements
• Determine the physical layout of a computer forensics lab
• Select a basic forensic workstation
• Build a business case for developing a forensics lab

Understanding Forensic Lab Certification Requirements

• Computer forensics lab
  – 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 for 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
  – Encouraging honesty among lab staff members
  – Plan updates for the lab

Identifying Duties for the Lab Manager and Staff (continued)

• Lab manager duties (continued):
  – Establish and promote quality-assurance processes
  – Set reasonable production schedules
  – Estimate how many cases an investigator can handle
  – Estimate when to expect preliminary and final results

Identifying Duties for the Lab Manager and Staff (continued)

• Staff knowledge and training:
  • Hardware and software
  • OS and file types
  • Deductive reasoning
  • Technical training
  • Investigative skills
Identifying Duties for the Lab Manager and Staff (continued)

- Work is reviewed regularly by the lab manager
- Check the ASCLD website for online manual and information

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)

- 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 your lab requirements and costs
- Check statistics from the Uniform Crime Report
  - For federal reports, see www.fbi.gov/ucr/ucr.htm
Lab Budget Planning (continued)

• Identify crimes committed with specialized software
• When setting up a lab for a private company, check:
  – Hardware and software inventory
  – Problems reported last year

Acquiring Certification and Training

• Update your skills through appropriate training
• International Association of Computer Investigative Specialists (IACIS)
  – Certified Electronic Evidence Collection Specialist (CEECS)
  – Certified Forensic Computer Examiners (CFCEs)

(continued)

• 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
Determining the Physical Layout of 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

- 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
    - [http://nsi.org/Library/Govt/Nispom.html](http://nsi.org/Library/Govt/Nispom.html)
    - Are very expensive; can use low-emanation workstations instead
Considering Office Ergonomics

• Ergonomics designs
  – Provide comfort
  – Improve productivity
• Involves:
  – Psychology
  – Anatomy
  – Physiology

Considering Office Ergonomics (continued)

• Furniture ergonomics consider:
  – Desk or workstation table
  – Chair
  – Workbench
• Hardware ergonomics consider:
  – Keyboard
  – Mouse

Figure 3-2. Proper ergonomics at a desk
Considering Office Ergonomics (continued)

![Figure 3-3: Hand and wrist positioning with a wrist pad](image)

Considering Environmental Conditions

- Ventilation and temperature
- HVAC system:
  - How large is the room, and how much air moves through it per minute?
  - Can the room handle the heat?
  - Maximum number of workstations the room can handle
  - How many computers will be located in this room immediately?

Considering Environmental Conditions (continued)

- Lighting:
  - Too many lights at the wrong illumination can cause headaches or eyestrain
  - Natural or full-spectrum lighting is less fatiguing
- For information on how to deal with eyestrain
  - [www.apple.com/about/ergonomics/vision.html](http://www.apple.com/about/ergonomics/vision.html)
Considering Structural Design Factors

- Consider the physical construction of the lab
- Lab should be a safe, secure, lockable room
- Use resistant materials with walls, ceilings, and floors
- Reinforce false ceiling and raised floors with material to seal the openings

Considering Structural Design Factors (continued)

- Resistant materials:
  - Plaster
  - Gypsum wallboard
  - Metal and wire mesh
  - Hardboard
  - Wood and plywood
  - Grass
- Avoid windows on your lab exterior and doors
- Use secure door’s locking devices

Determining Electrical Needs

- You need enough power to run workstations and other equipments
  - 15 and 20 amp are preferred
- Protect your equipment from power fluctuations
- Uninterruptible power supply (UPS) units are a must
  - Protect your workstations
  - Give you time for a safe shutdown
  - Block or filter electrical fluctuations
Planning for Communications

- Telephone service
  - ISDN phone system
- Internet connection
  - Dial-up or broadband access
  - Disconnect it while conducting your analysis
- LAN access
- WAN access
  - Use separate computer to connect to your WAN

Installing Fire-Suppression Systems

- Computers can cause fire
  - Over-voltage on a cable
  - Malfunctioning hard drive
- Countermeasures
  - Fire sprinklers
  - Dry chemical fire extinguishers (B rated) for lab with raised floors
- Contact your fire marshal for more information

Using Evidence Containers

- Recommendations for securing a storage container:
  - Locate it in a restricted area
  - Limit 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)

- 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 on 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 a burglar alarm system
  - Hire a guard force for your lab
**Auditing a Computer Forensics Lab**

- Auditing ensures proper enforcing of policies
- Audits should include (but are not limited to):
  - Ceiling, floor, roof, and exterior walls of the lab
  - Doors and door locks
  - Visitor logs
  - Evidence containers logs
  - 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**

*Figure 3-4 Small or home-based lab*

**Determining Floor Plans for Computer Forensics Labs (continued)**

*Figure 3-5 Mid-size computer forensics lab*
Determining Floor Plans for Computer Forensics Labs (continued)

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 (SIGs)
- 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 easier to determine
- Identify the environment you deal with
  - Hardware platform
  - OS
- Gather tools to work on the specified environment

Stocking Hardware Peripherals

- Any lab should have in stock:
  - IDE cables
  - Small Computer System Interface (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 adapter
  - Computer hand tools

Maintaining Operating Systems and Application Software Inventories

- Maintain licensed copies of software, like:
  - Microsoft Office XP, 2003, 2000, 97, and 95
  - A variety of Linux systems
  - Quicken
  - Programming languages
  - Specialized viewers
  - Corel Office Suite
  - StarOffice/OpenOffice
  - Peachtree accounting applications
Using a Disaster Recovery Plan

- Restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- Includes backup tools for single disks and RAID servers
- Configuration management
  - To keep track of software updates on your workstation

Planning for Equipment Upgrades

- Risk management
  - 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 24 months on normal conditions
  - Schedule upgrades based on this fact

Using Laptop Forensic Workstations

- Create a 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 are improving
Building a Business Case for Developing a Forensics Lab

• Can be a problem because of budget problems
• Demonstrate how the lab will help your organization to save money and increment profits
  – Compare the cost of an investigation with the 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

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

• Steps (continued):
  – Approval and acquisition
  – Implementation
  – Acceptance testing
  – Correction for acceptance
  – Production
Summary

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

Summary (continued)

- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab

Questions & Discussion