Forensics Lab Certification Summary

LECTURE 3: THE INVESTIGATOR’S OFFICE AND LABORATORY

Dr. Zunera Jalil

📧 *zunera.jalil@au.edu.pk*

📅 *Date: 04/03/2025*

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** is where:
  - You conduct your investigation
  - Store evidence
  - House equipment, hardware, and software
- **ANSI-ASQ National Accreditation Board (ANAB)**:
  - Provides accreditation to crime and forensics labs worldwide
  - Includes digital forensics labs
  - 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
- 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)

Additional Lab Manager Duties:

- Estimate when to expect preliminary & final results
- Create and monitor lab policies

Staff Member Duties:

- Have knowledge and training in:
  - Hardware and software
  - OS and file types
  - Deductive reasoning
- Provide a safe and secure workplace
- Have their work regularly reviewed by the lab manager

ACTIVITY #1 [5 Minutes]

- Make a group of two
- Visit ANAB website: https://anab.ansi.org/
- Find 3 key points and write down
- Be ready to explain

LAB BUDGET PLANNING

(1 of 3)

- Break costs into monthly, quarterly, and annual expenses
- Use past expenses to forecast future costs
- Include costs for:
  - Hardware
  - Software
  - Facility space
  - Personnel training
- Estimate number and types of cases
- Consider technology changes

(2 of 3)

- Use statistics to identify common computer crimes
- Plan your lab needs and costs accordingly

(3 of 3)

- For federal reports, check:
  - Uniform Crime Report stats
  - Crimes with specialized software

  - Hardware/software inventory
  - Last year’s problems
  - Future tech developments
- For private labs, time management affects software/hardware purchases

---

ACQUIRING CERTIFICATION AND TRAINING

(1 of 5)

- Update skills regularly
- Research requirements and costs
- **IACIS**:
  - Created by police
  - Certification: **Certified Forensic Computer Examiner (CFCE)**

(2 of 5)

- **ISC² CCFP**:
  - Knowledge of:
    - Digital forensics
    - Malware analysis
    - Incident response
    - E-discovery

(3 of 5)

- **HTCN Certifications**:
  - Certified Computer Crime Investigator (Basic & Advanced)
  - Certified Computer Forensic Technician (Basic & Advanced)
  - Focus on EnCase forensics
- **EnCE Certification** requires a licensed EnCase copy

(4 of 5)

- **AccessData Certified Examiner (ACE)**:
  - Requires AccessData Ultimate Toolkit
  - Includes theory + practical
- Other certification providers:
  - EC-Council
  - SANS Institute
  - DCITA

(5 of 5)

- Additional certifiers:
  - ISFCE
  - CTIN
  - DFCB
  - CSA
  - FLETC
  - NW3C

DETERMINING THE PHYSICAL REQUIREMENTS FOR A COMPUTER FORENSICS LAB

- Secure lab to protect evidence
- Provide safe, secure environment
- Keep inventory
- Monitor supplies

IDENTIFYING LAB SECURITY NEEDS

- Secure facility:
  - Floor-to-ceiling walls
  - Locking doors
  - Secure containers
  - Visitor log
- Staff should share access levels
- Brief staff on security policy

ACTIVITY #2 [5 Minutes]

- Make a group of two
- Research TEMPEST facilities
- Be ready to explain

CONDUCTING HIGH-RISK INVESTIGATIONS

- Requires advanced security
- **TEMPEST Facilities**:
  - EMR proofed
  - Expensive
  - Use low-emanation workstations instead

USING EVIDENCE CONTAINERS

(1 of 4)

- Also called **evidence lockers**

- Must be secure and in restricted areas
- Only authorized access
- Keep access records
- Keep containers locked

(2 of 4)

- If using **combination locks**:
  - Treat combo security same as contents
  - Destroy old combos
  - Change combos every 6 months

(3 of 4)

- If using **keyed padlocks**:
  - Assign a key custodian
  - Stamp keys with serial numbers
  - Maintain a key registry
  - Conduct monthly key audits
  - Change keys/locks yearly
  - No master keys
- Use steel containers with internal cabinet/padlock

(4 of 4)

- Use a **media safe** if possible
- Build a dedicated evidence room
- Maintain:
  - Evidence log
  - Visitor log

CONSIDERING PHYSICAL SECURITY NEEDS

- Enforce policies
- Use visual/audio alerts for visitors
- Escort all visitors
- Use:
  - Visitor badges
  - Alarm systems
  - Guard force

OVERSEEING FACILITY MAINTENANCE

1. Immediately repair damage
2. Escort cleaning crews
3. Use:
   - Antistatic pads
   - Clean floors/carpets
4. Two trash containers:
   - One for sensitive materials
   - One for regular waste
5. Use professional services for sensitive material disposal

AUDITING A DIGITAL FORENSICS LAB

- Ensures policy enforcement
- Inspect:
  - Ceilings, floors, walls
  - Doors and locks
  - Visitor and evidence logs

- Secure all unused evidence daily

DETERMINING FLOOR PLANS FOR DIGITAL FORENSICS LABS

(1 of 7)

- Depends on:
  - Budget
  - Space
  - Number of investigators
- Ideal: 2 forensic workstations + 1 non-forensic (Internet)

(2 of 7)

- **Small lab** setup:
  - 1–2 forensic workstations
  - 1 Internet research computer
  - Storage + workbench

(4 of 7)

- **Mid-size labs**:
  - Run by private firms
  - Multiple exits
  - Cubicles or offices
  - Library space

(6 of 7)

- **Large/regional labs (FBI/state)**:
  - Evidence room
  - Evidence custodians

    - 2 controlled exits, no windows

SELECTING A BASIC FORENSIC WORKSTATION

- Based on **budget and needs**
- Use:
    - Less powerful systems for simple tasks
    - Multipurpose systems for complex analysis

SELECTING WORKSTATIONS FOR A LAB

- **Police labs** need:
    - Legacy systems
    - Multipurpose or high-end laptops
    - USB 3.0 / SATA disk support
    - Lightweight mobile setups

SELECTING WORKSTATIONS FOR PRIVATE SECTOR LABS

- Understand business environment
- Investigate internally
- Choose suitable:
    - OS
    - Hardware platform
- Use Windows to examine both Windows & Mac drives

STOCKING HARDWARE PERIPHERALS

- Stock:
    - Digital camera
    - Antistatic bags
    - External drives
    - IDE/SATA/SCSI cables
    - Graphics cards
    - USB/FireWire adapters
    - Various hard drives
    - Hand tools

MAINTAINING OS AND SOFTWARE INVENTORIES

- Maintain licensed copies:
    - Microsoft Office
    - Hex editor
    - Programming tools
    - Viewers
    - Office suites
    - Accounting software

USING A DISASTER RECOVERY PLAN

- Recover workstation/data after failure
- Includes:
    - Backup tools (e.g., Norton Ghost)

    - Config management
- For RAID servers:
    - Ensure large data backup systems

PLANNING FOR EQUIPMENT UPGRADES

- Practice risk management
- Identify:
    - Critical replaceable equipment
    - Non-critical failure-prone equipment
- Upgrade every:
    - 18 months (minimum)
    - 12 months (preferred)

BUILDING A BUSINESS CASE FOR DEVELOPING A FORENSICS LAB

- Gain support from:
    - Managers
    - Team members

Purpose:

- Sell lab services
- Show cost-saving and profit-boosting potential
- Compare investigation vs. lawsuit cost
- Protect IP and business plans

PREPARING A BUSINESS CASE FOR A FORENSICS LAB

(1 of 3)

- Plan for:
  - Tools
  - Facilities
  - Training
- Justify to decision-makers
- Constantly promote lab services

(2 of 3)

- Present budget for approval
- Include:
  - Implementation steps
  - Delivery/install timelines
  - Inspection dates

(3 of 3)

- Include:
  - Acceptance testing
  - Correction plans
  - Test communications and hardware
  - Start software tools
- Begin production phase

SUMMARY

- A forensics lab is where investigations and evidence storage happen
- Keep upgrading skills and training

- Secure your lab physically
- Planning is harder for police than private labs
- Workstations must be well-equipped
- Business cases help secure support for lab development