India Henry
CYSE 407 - 14738
Bryan Bechard
5 December 2025

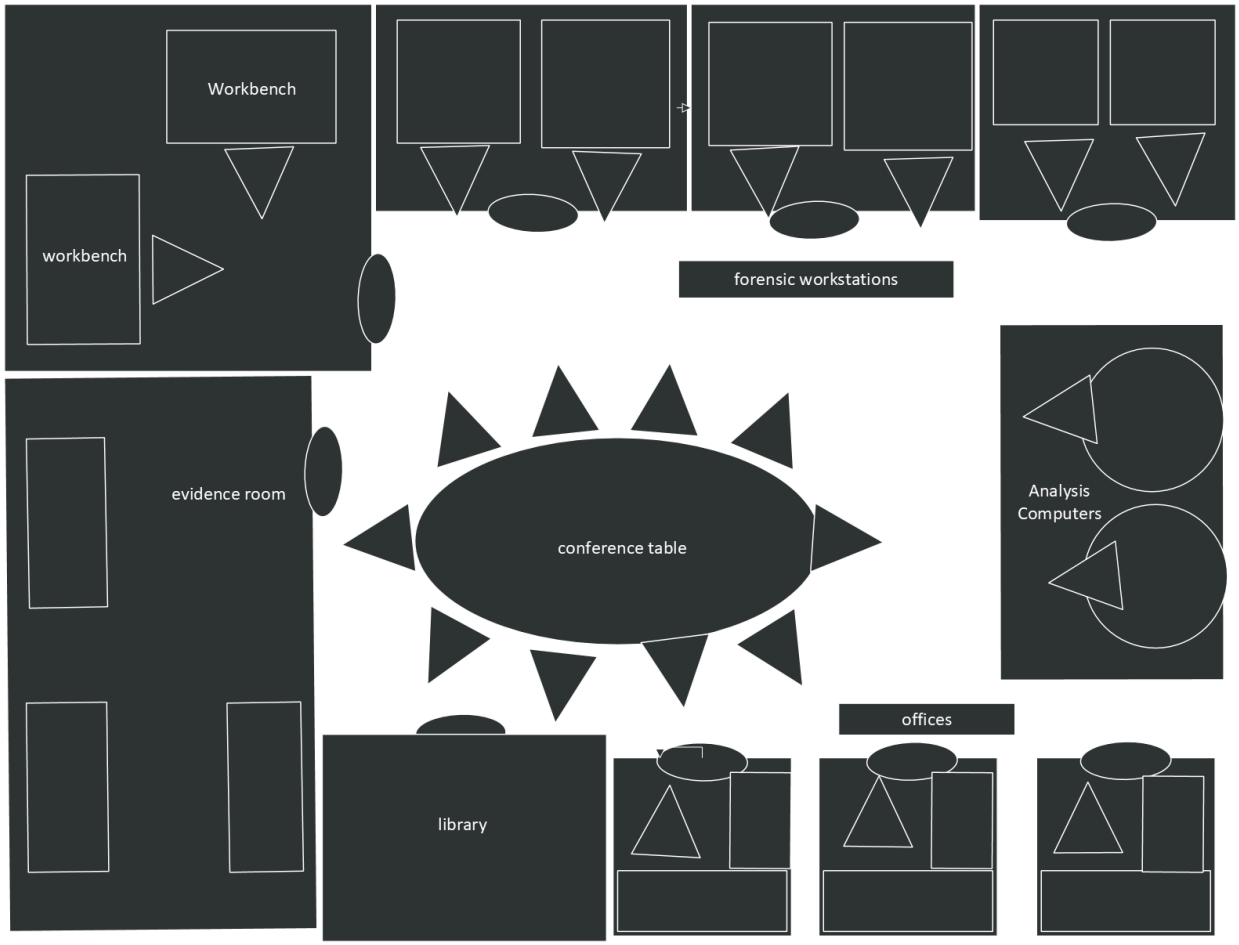
Digital Forensics Midterm

Summary

In order to create and run a digital forensics laboratory for a mid-sized police department, there are various plans that need to be adhered to in order to instate this division. This document gives an overview of what to expect, including the physical layout of the lab, a list of hardware and software inventories that will be helpful when conducting an investigation, a lab accreditation plan, a maintenance plan, and staffing requirements. The physical layout of the lab is an example of what a larger digital forensics lab would entail; a larger lab would be helpful for a mid-sized police department because of the amount of cases they may be handled. The evidence room also needs to be big enough to be able to store evidence for up to twenty cases, which would require a larger room with more cabinets. This room also has multiple forensics workstations and workbenches to allow for a crew of people to work an investigation, and possibly multiple investigations at the same time. Many forensics labs also have libraries to keep information about the hardware, software, and methodology that examiners may need to reference. As well as two analysis computers and a conference room table. A list of inventory items that is required to run a lab is shown in a diagram that separates the hardware needs from the software needs. The accreditation plan stems from the ANSI-ASQ National Accreditation Board and ISO/IEC 17025, which requires a list of certifications that need to be recertified over time. The lab maintenance plan lays out how the lab needs to be budgeted and ways to sustain the hardware upkeep and software updates. Staffing gives definitions and roles for the lab manager and technicians.

Lab Physical Layout

(Nelson et al., 2018, 77)



Inventory

A forensics lab for a mid-sized police department would require more than what a mid-sized digital forensics lab offers, so the following is a list of things that would need to be included in the digital forensics lab:

Hardware	Software

• An evidence room with locks on the door
  ○ Cabinets (3)
(Nelson et al., 2018, 77)
 	
• Workbenches (2)
  ○ Desks (2)
  ○ Chairs (2)
  ○ JBC Precision Soldering Station (2)
  ○ Sentry Air (2)
  ○ Ultrasonic Cleaner (2)
	• Licensed copies of as many legacy OSs as possible
	  ○ Microsoft OSs should include
	  ■ Current OS
	  ■ Windows 10
	  ■ Windows 8.0
	  ■ Windows 8.1
	  ■ Windows 7
	  ■ Windows Vista
	  ■ Windows XP
	  ■ Windows 2000
	  ■ Windows NR 3.5

- Polishers (2)
- iFixit Kit (2)
- BGA ReWork Station

(Teel Technologies, 2020)

- Stationary Workstations (3)
  - Forensic Workstations (2)
  - Non-forensic, Internet access workstation (1)
  - Desks (3)
  - Chairs (3)
  - PCs (3)
  - Mice (3)
  - Keyboards (3)

(Nelson et al., 2018, 77)

- Analysis computers (2)
  - PCs (2)
  - Mice (2)
  - Keyboards (2)
  - Desks (2)
  - Chairs (2)

(Nelson et al., 2018, 77)

- Library for field resources (Nelson et al., 2018, 77)
- Conference table
  - Table (1)
  - Chairs (10)

(Nelson et al., 2018, 77)

- Digital camera capable of still and motion recording
- Assorted antistatic bags
- An external CD/DVD drive
- 40-pin 18-in and 36-in IDE cables, both ATA-33 and ATA-100 or faster
- Ribbon cables for floppy disks
- Extra USB 3.0 or newer cables and SATA cards and associated cables
- Extra SCSI cards (preferably ultrawide)
- Graphics cards, both peripheral component interconnect (PCI) and Accelerate Graphic Port (AGP)
- Assorted FireWire and USB adapters
- A variety of hard drives and USB drives (as many as possible)
- At least two 2.5-in adapters from notebook IDE hard drives to standard
    - Windows 3.11
    - Windows DOS 6.22
  - Macintosh OSs
    - macOS
    - Mac OS X
    - 9.x
    - 8
  - Linux OS
    - Linux Mint
    - DeftZ
    - Ubuntu
    - Slackware
    - Bebian
- Some programs to include:
  - Microsoft office (current and older versions)
  - Hexadecimal editor
    - WinHex or Hex Workshop
  - Programming Languages
    - Visual Studio
    - Perl
    - Python
  - Specialized image viewers
    - Quick View
    - ACDSee
    - ThumbsPlus
    - IrfanView
  - WPS Office
  - WordPerfect
  - A third-party or open source office suite
  - Accounting applications
    - Quicken
    - QuickBooks

(Nelson et al., 2018, 81)

IDE/ADA drives, SATA drives, etc. • Phillips head and flathead screwdrivers, socket wrench, vendor-specific tools, flashlight, and an antistatic wrist strap (Nelson et al., 2018, 81)	

Lab Accreditation Plan

ANAB-ASQ National Accreditation Board gives an overview of the process of obtaining accreditation. To obtain this accreditation, "the conformity assessment body (CAB) demonstrates competence for all requested services on the draft scope of accreditation" (ANAB-ANSI National Accreditation Board, 2024, 6). This can be done by submitting "records and reports of completed work, mock work, research, publication, monitoring activities (proficiency testing, or other interlaboratory comparisons, intralaboratory comparisons or observation-based performance monitoring) or a combination of these" (ANAB-ANSI National Accreditation Board, 2024, 6). There are also several actions prior to accreditation that an applicant has to complete including obtaining "the most current version of the following:

- A licensed copy of the international standard, if applicable to the Program for accreditation (ISO/IEC 17025 for testing/calibration, ISO/IEC 17020 for inspection
- A MA 3033 accreditation manual
- Accreditation scheme requirements (AR_3125 for testing/calibration, AR_3120 for inspection, AR_3181 for property and evidence control units
- Application and draft scope documents
- If applicable, additional requirements (FBI quality assurance standards, ABFT forensic toxicology laboratory accreditation checklist, MD OHCQ)" (ANAB-ANSI National Accreditation Board, 2024, 6).

Following certification, "ANAB stresses that each lab should maintain an up-to-date library of resources in its field," so for digital forensics, it is required to keep information on software, hardware, and any methodologies that are applied in the field (Nelson et al., 2018, 65).

"ISO/IEC 17025 is the international standard for testing and calibration laboratories" that provides the requirements for "competence, impartiality, and consistent operation of laboratories" to help ensure "accuracy and reliability of their testing and calibration results" (International Organization for Standardization, 2023). It is important that this standard is upheld and re-evaluated during maintenance in case the standards are expanded when they are re-evaluated. This is where the standards for a lab manager and staff are located.

Accreditation also concerns getting various certifications and ensuring that certifications remain viable. The International Association of Computer Investigative Specialists (IACIS) is an association created by police officers to "formalize credentials in digital investigations," and requires recertification every three years to ensure examiners are "continuing their education and are still active in the field of digital forensics" (Nelson et al., 2018, 70). This association designates members as Certified Forensic Computer Examiners (CFCE). The certifications required from IACIS would be helpful, if not completely necessary, for staff to have. Similarly, the High Tech Crime Network (HTCN) is an association that also requires various certifications

for becoming a computer crime investigator and certified computer forensics technicians, requirements vary for basic and advanced members for both certifications. It may be necessary for the lab manager to carry the expert versions of these certifications.

Lab Maintenance Plan

A part of the lab's maintenance plan is budgeting and addressing lab security needs. In this case, the lab needs to have two analysis computers and room for twenty cases of evidence. Part of the budgeting plan is also being able to estimate the type of operating system the police department is most likely to come in contact with, or "creating a baseline for the types and numbers of systems you can expect to investigate"; while there is a chance that the forensics unit may come in contact with Linux users, it is most likely that they will come in contact with Windows and Apple users (Nelson et al., 2018, 66). It is also important to estimate how many investigations may take place; in this case, we are handling a mid-sized police department and need room for a maximum of twenty cases. This estimate is where we find which software tools are used the most during an investigation as well as any specialized software that may be worth investing in (Nelson et al., 2018, 66). The budget should also leave room for any hardware upkeep or upgrades needed; this also goes for software upgrades or switches that may need to be made in order to keep up with technological innovations (Nelson et al., 2018, 66).

Maintenance for a digital forensics lab also includes ensuring the physical room data is being investigated and stored in is able "to preserve the integrity of evidence, function as an evidence locker or safe, and ensure it is a secure facility" (Nelson et al., 2018, 72). Securing the physical area would mean having "a small room with true floor-to-ceiling walls, door access with a locking mechanism, a secure container for physical evidence, and a visitors log" (Nelson et al., 2018, 72). The room itself should be preserved, so "any damage to the floor walls, ceilings, or furniture would need to immediately be repaired" (Nelson et al., 2018, 74). Repairs need to be done securely, so "cleaning crews need to be escorted and monitored" (Nelson et al., 2018, 74). It is encouraged to take precautions to reduce static electricity that tends to accumulate while working with technology; this can be done by "placing antistatic pads around electronic workbenches and cleaning floors and carpets once a week" (Nelson et al., 2018, 74). It is also encouraged to maintain two separate trash cans to store items related to an investigation and items not related to an investigation; this helps to maintain the integrity of an investigation (Nelson et al., 2018, 74).

It is the *lab manager's* role to ensure that all hardware and software is updated and maintained from investigation-to-investigation. Maintaining hardware would planning for hardware needs: "hardware manufacturers have designed most computer components to last about eighteen months between failures", so it is the responsibility of the lab manager to keep track the amount of time between when the software was initially installed and how soon it needs to be replaced (Nelson et al., 2018, 284). This also means that the lab manager needs to keep track of any hardware innovations that have occurred since the last installation to ensure that the hardware stays up to date. Keeping hardware up to date also involves maintaining the workstations; for a mid-sized forensics lab there would be about four stationary workstations, one workbench, and two analysis computers. Once again, maintenance in these areas would mean ensuring that the PCs are well preserved and up to date, many police departments tend to use vendors, so this would mean ensuring the workstations are up to date by the provider's

standards. Ensuring software tools are up to date, as well as finding new software tools to aid in investigations, is also a requirement for the *lab manager*. This would involve ensuring PCs have integrated any software updates to help ensure the security of any investigations.

Staffing

ANAB requires each lab to have specific objectives for staff; the objectives are usually created by the lab's parent organization or the lab director. The role of the *lab manager* is "to set up processes for managing cases and [to] review them regularly" (Nelson et al., 2018, 65). This role performs a variety of tasks, like "promoting group consensus in decision making, maintaining fiscal responsibility for lab needs, enforcing ethical standards among staff members, and planning updates for the lab" (Nelson et al., 2018, 65). Essentially, the role is to oversee other staff members to maintain lab integrity and efficiency while also ensuring the lab's hardware and software are up to standard. The lab manager is also responsible for "quality assurance expectations" by "outlining what to do when a case arrives, logging evidence, specifying who can enter the lab, establishing guidelines for filing reports, and setting reasonable production schedules for processing work" (Nelson et al., 2018, 65).

Technicians are required to have enough training to perform their tasks: "necessary skills include hardware knowledge, software knowledge, and deductive reasoning skills" (Nelson et al., 2018, 65). The lab manager oversees their work to ensure they are performing their tasks on par and to "ensure quality" of their work (Nelson et al., 2018, 65). Technicians are also required to maintain their training and keep their skills up to date, "many vendors and organizations hold annual or quarterly training seminars that offer certification exams" to help technicians maintain and improve their investigative and computer skills (Nelson et al., 2018, 65).

References

ANAB-ANSI National Accreditation Board. (2024, November 21). *Accreditation Manual for Forensic Laboratories, Forensic Inspection Bodies, and Property and Evidence Control Units*. ANAB. https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=7183

International Organization for Standardization (ISO). (2023). *IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories*. ISO. https://www.iso.org/standard/66912.html

Nelson, B., Phillips, A., & Steuart, C. (2018). *Guide to Computer Forensics and Investigations*. Cengage Learning.

Teel Technologies. (2020). *Workbench Equipment*. TeelTech. https://teeltech.com/chip-off-isp-jtag/workbench-gear/workbench-equipment/