

Midterm Paper

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE407: Digital Forensics

Professor Bryan Bechard

May 5, 2026

Summary

This paper will outline a three-year roadmap for building a new digital forensics lab within a mid-sized police department. The lab will be able to handle digital evidence from various different cybercrime investigations. To run effectively, the lab needs the correct tools, the right people, a path to accreditation, and a maintenance strategy that would keep everything working in the long run. This report will cover those areas and will include the physical layout of the space, an equipment and software inventory, an accreditation plan with ISO/IEC 17025 standards, a full maintenance and calibration program, and staffing requirements.

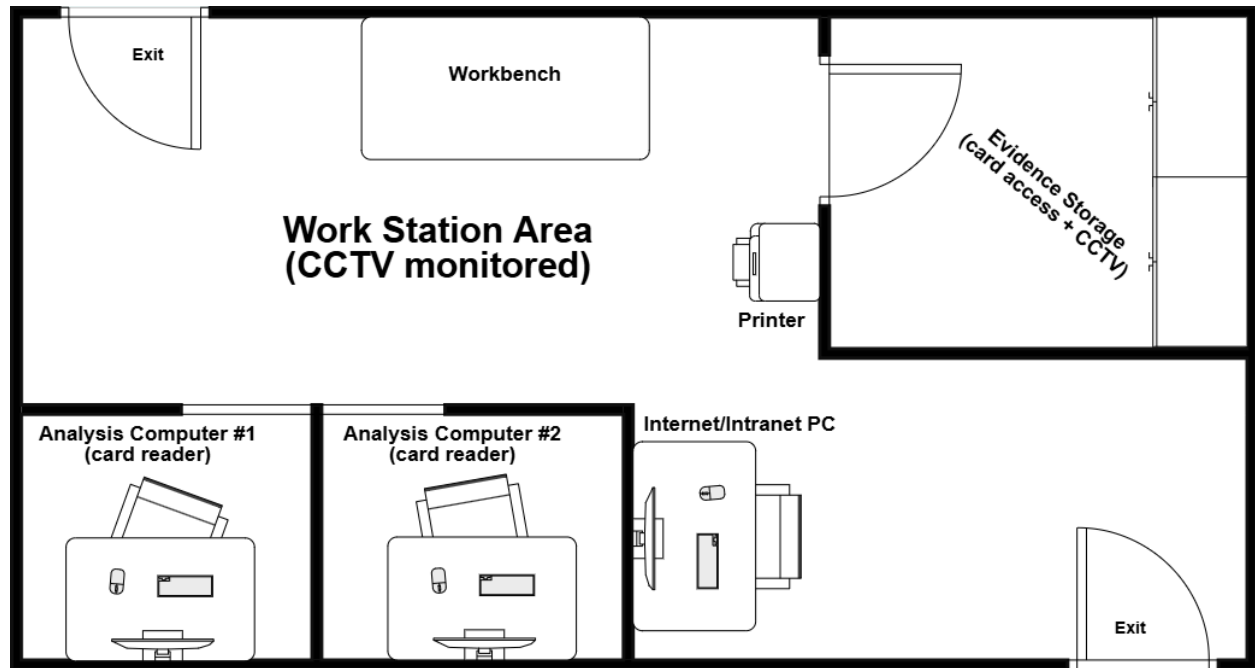
Accreditation Plan

The digital forensic lab will follow accreditation under ISO/IEC 17025, the international standard for the competence, impartiality, and consistent operation of testing and calibration laboratories. It is recognized by law enforcement agencies and provides a framework that guarantees valid lab results. The accreditation process will be carried out over the course of three years. Below are the following phases:

- **Year 1:** The first year is dedicated to preparation. In this period the lab will obtain the ISO/IEC 17025 standard and start a gap analysis to identify flaws in the current state. Qualified staff members will be hired early in this phase in order to allow time for training in later phases. An internal audit will also be carried out to catch any remaining gaps. By the end of the first year, the lab should have all policies and procedures in place and ready for submission.
- **Year 2:** In year two, the focus will shift towards application. The policies and records will be submitted to ANAB with the accreditation application (ANAB, 2024). Then,

ANAB will perform an on-site assessment where they will evaluate the lab and verify that daily operations match what was submitted to them. Any inadequacies will be fixed so we can ensure we obtain the official accreditation certificate.

- **Year 3:** The third year will focus on maintaining accreditation. ANAB requires annual inspections to confirm that the lab meets the standards and requirements. Additionally, the lab will also undergo proficiency testing. This means we'd have to submit lab results on a regular basis to verify accurate and reliable findings (ANAB, 2024). By the end of year three, the lab will complete its first accreditation and prepare for re-accreditation.

Forensic Lab Floor Plan

kjg

- This is the floor plan of a digital forensic lab for a mid-size police department. It contains a work station area with two cubicles, each having their own analysis computer, an internet/intranet PC, a work bench, and an office printer. There is also a separate, secure evidence storage room for up to twenty cases. Physical security measures include 24/7 CCTV, card access into evidence storage, and card readers for both analysis computers. For safety reasons, the lab has two exits (Nelson et al., 2019).

Inventory

Hardware:

- Monitors (x3, one per analysis computer and one for the internet/intranet PC)
- Keyboards and mice (x3 sets)
- Analysis computers (x2)
- Internet/Intranet PC (x1)
- Office printer
- Workbench
- Write blockers
- Evidence storage rack & shelving unit (holds up to 20 cases)
- Ergonomic chairs (x3)
- Cables (Ethernet, USB, PC power)

Software:

- FTK (Forensic Toolkit)
- EnCase Forensic
- Autopsy
- Wireshark
- Helix Pro
- Antivirus software
- Kali Linux
- Cellebrite

- Volatility

Maintenance Plan

The maintenance plan for the lab will focus on keeping the equipment reliable, accurate, and available at all times for all call casework. According to ISO/IEC17025 Section 5.5, This will apply to all hardware and software used in the forensic process. In addition to equipment, staff maintenance will also be a requirement. Each examiner shall complete annual training in order to stay up to date on forensic standards. Calira, a SaaS-based laboratory management and equipment company, states that “investing in training can help equip laboratory staff with the knowledge and skills needed to perform tasks and understand calibration procedures”. Employee certifications must also be renewed when needed. The lab manager is responsible for verifying that training and renewals are completed on time.

All equipment should be maintained according to the manufacturer specifications. It is important if a piece of equipment is overdue for calibration. In that case, it will be taken out of service until it is fixed. All maintenance activity has to be logged and documented. This is to verify accountability during inspections. All computers in the lab receive monthly operating system updates, regular antivirus scanning, and hardware checks. If any piece of equipment fails a maintenance check, or isn't working at all, the lab manager must be notified.

Equipment Security

All hardware and software needs to be protected from unauthorized access. Access to the lab and all equipment is restricted to authorized employees only. When not in use, digital forensic tools should be stored in the locked evidence storage room.

Staffing

Lab manager: Responsible for overseeing all operations of the digital forensics lab. This includes reviewing digital forensic cases, managing accreditation, supervising staff, and communicating to other departments.

- Minimum qualifications for this position:
 - Bachelor's degree in digital forensics or an IT related field (Cybersecurity, Computer Science, etc.)
 - At least 4 years of hands-on digital forensic experience at an intermediate to expert level
 - Possession of at least one certification is required: CFCE, EnCE, GCFA; multiple is desirable; CFCE preferred
 - Proficient with digital forensic tools (FTK, EnCase, Autopsy, and Wireshark)

Forensic Technician: Responsible for handling the analysis portion of digital evidence, while also working closely with the lab manager. Duties include the documentation of digital evidence, maintaining chain of custody, forensic imaging, examining digital evidence, and the writing of reports.

- Minimum qualifications for this position:
 - Associate's degree in digital forensics or an IT related field (Cybersecurity, Computer Science, etc.). Bachelor's degree preferred
 - At least a year of hands-on digital forensic experience, or a closely related technical field

- Possession of at least one certification is required within 6 months of hire: CFCE, EnCE, GCFA. CFCE preferred.
- Intermediate knowledge of digital forensic tools (FTK, EnCase, Autopsy, and Wireshark)

References

ACCREDITATION MANUAL FOR FORENSIC SERVICE PROVIDERS. (2024).

<https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=7183>

Best practices for lab equipment maintenance and calibration | *The Calira blog*. (2026).

Calira.co.

<https://calira.co/blog/best-practices-for-lab-equipment-maintenance-and-calibration>

Building a Digital Forensics Lab. (2025, December 9). ACE Computers.

https://acecomputers.com/building-a-digital-forensics-lab/#Storage_Solutions

ISO. (2017). *ISO/IEC 17025 testing and calibration laboratories*. ISO.

<https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html>

Job Bulletin. (2023). Governmentjobs.com.

<https://www.governmentjobs.com/careers/northcarolina/jobs/newprint/3772355>

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* (6th ed.). Cengage.