Midterm Paper: Computer Forensics Lab

Raneem Alarian

Department of Cybersecurity, Old Dominion University

CYSE 407: Digital Forensics

Professor Bryan Bechard

June 9, 2025

Summary

This is a three-year plan for the development of a computer forensics lab for a medium-sized police agency. The lab will have digital evidence analysis as its sole mission, offering secure, dependable, and forensically sound forensic lab services in support of investigations. Major goals include maintaining evidence integrity, following industry standards, and obtaining formal accreditation. The plan includes the physical lab layout with secure evidence storage and analyst workstations, an inventory of hardware and software tools required, a structured accreditation roadmap, a maintenance plan for ensuring all equipment and software are up to date, and a staffing plan with defined roles and qualifications. With this detailed plan, the department will be able to process digital evidence in a way that is efficient while ensuring adherence to legal standards and forensic quality assurance.

Lab Accreditation Plan

Accreditation Standards

This forensic lab will pursue formal accreditation with the ANSI National Accreditation Board (ANAB) to the ISO/IEC 17025:2017 standard. This international standard states the general requirements for competence in testing and calibration laboratories. The ISO/IEC 17025:2017 edition is stronger than the former (2005) with an emphasis on risk-based thinking, process approach, and alignment to modern digital systems.

The Lab Requirements

For the laboratory to be compliant with ISO/IEC 17025:2017, it shall prove its competency in a number of areas: impartiality, confidentiality, competence of staff, maintenance and calibration

of equipment, validated test methods, traceability of samples, quality assurance programs, and consistent records. Top priority will be given to the establishment of a system that guarantees digital evidence integrity and reproducibility and reliability of forensic results.

☐ **Step 1: Gap Analysis and Internal Planning**

The lab will begin by appointing an Accreditation Coordinator who will be responsible for documentation, audit, and application process progress. A complete gap analysis will be performed, comparing the lab's current capabilities to the requirements under ISO/IEC 17025:2017.

☐ **Step 2: Documentation Development**

A Quality Manual documenting all the clauses of the ISO/IEC 17025:2017 standard will be prepared. Standard Operating Procedures (SOPs) for handling evidence, forensic imaging, hash verification, documentation practices, and audit will be prepared.

☐ **Step 3: Competency and Training**

All lab staff will be trained in ISO 17025:2017 requirements and forensic-specific standard operating procedures. Competence will be determined by practical proficiency testing. Staff will also participate in annual external proficiency testing programs. This guarantees credibility and objectivity in forensic analysis.

☐ **Step 4: Equipment Calibration and Software Validation**

All forensic hardware will be calibrated against the manufacturer's instructions or national standards. All software, including FTK, EnCase, Autopsy, and OSForensics, will

be validation tested to produce consistent output in a range of test circumstances. These will be documented and revised annually.

☐ **Step 5: Application Submission**

The lab will then submit an application via the ANAB portal, providing all required documentation: Quality Manual, SOPs, staff CVs, method listings, and organizational charts. A preliminary fee will be paid to initiate the process.

☐ **Step 6: ANAB On-Site Assessment**

Upon submission, there is a pre-assessment that can be performed by ANAB to identify any existing deficiencies. Subsequently, an on-site evaluation will be conducted formally, where ANAB auditors will evaluate compliance to ISO/IEC 17025:2017, investigate staff performance, and investigate facilities and documents. If nonconformities are found, the laboratory must present a corrective action plan.

☐ **Step 7: Accreditation and Certificate Issuance**

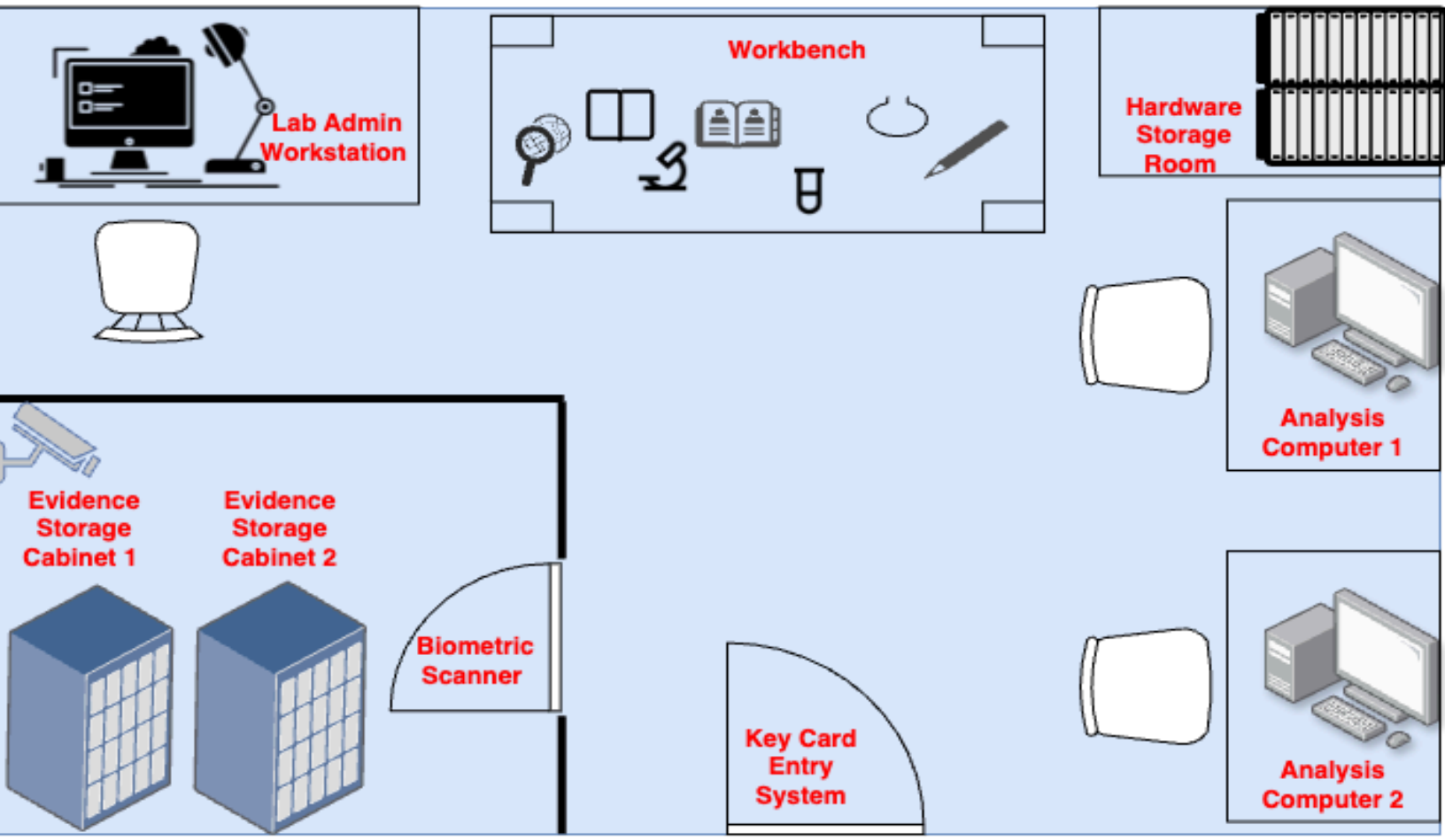
Once the corrective actions are accepted, ANAB will grant the certificate of accreditation. The laboratory will then be listed on ANAB's official registry as an accredited forensic laboratory.

☐ **Step 8: Ongoing Compliance**

To maintain accreditation, the laboratory shall: (a) Undergo annual surveillance audits by ANAB, (b) Perform internal audits and management reviews, (c) Perform annual

proficiency testing for each discipline, (d) Have hardware and software systems upgraded and validated, (e) Document and close all nonconformities.

Forensic Laboratory Floor Plan



Inventory

Hardware & Equipment

High-Performance Forensic Workstation (2)

Anti-static Workbench Station (1)

Two Monitors Per Forensic Workstation (4)

Lab Manager Desktop PC (1)

High-Quality Multifunctional Printer/Scanner/Copier (1)

Shredder (1)

Office/Lab Chair (3)

Tableau TX1 Forensic Imager (2)

Tableau USB Write Blocker (2)

Disk Duplicator (2)

Digital Camera For Documenting Evidence (1)

Lockable Evidence Storage Cabinet (2)

Surveillance Camera (5)

Key Card Entry System (1)

Biometric Entry System For Evidence Storage Room (1)

Alarm System (1)

Basic Computer Repair Tool Kit (1)

Network Switch (1)

Software

Kali Linux

Wireshark

Forensic Toolkit (FTK)

EnCase Forensic

Autopsy (open-source)

OSForensics

Cellebrite UFED (Mobile Forensics)

CaseGuard Studio

Tableau Write Blocker Drivers

Hex Editor (HxD)

Microsoft Windows Operating System

Microsoft Word

Microsoft Excel

Microsoft PowerPoint

Google Workspace

Secure Email and Encrypted File Sharing Platform (Microsoft OneDrive With AIP)

Windows Defender Antivirus

Secure Backup Software

Maintenance Plan

Hardware Maintenance

(a) **Routine Inspection:** Staff will inspect all hardware on a monthly basis to detect any problems

(b) **Environmental Monitoring:** There are temperature and humidity probes in the hardware storage. The probes will be checked monthly to ensure they are in good condition. They will notify staff immediately should levels change

(c) **Security Controls:** Staff will verify and test physical controls on a weekly basis. Staff will also review access logs to determine if there are any unauthorized attempts

(d) **Inventory Audits:** Staff will conduct physical inventory audits every quarter to identify missing or damaged equipment

(e) **Power Management:** All equipment that must operate periodically will be powered up no less than quarterly to prevent battery and/or component deterioration

Software Maintenance

(a) **Automatic Software Updates:** Where possible, software updates, especially major security fixes, are automatically applied during non-busy hours to reduce disruption and secure system

(b) **Backup Plans:** The staff perform system backups before updating software. This allows for rapid restoration to the previous state in the event of problems arising, keeping ongoing forensic investigations intact

(c) **License Compliance Monitoring:** Lab manager tracks all software licenses, their expiration dates, and users to be able to stay in compliance with the law and have access to the lab's critical forensic tools at all times.

(d) **Change Management:** There is a defined process before any significant software change or upgrade in the lab to make sure it will not create problems. This consists of:

(i) **Documenting the Update:** Record what the update is and what it

(ii) changes, and why it is needed

(iii) **Reviewing the Change:** The change will be reviewed by the lab manager

(iv) make sure it is okay and safe to install

(v) **Testing Before Full Use:** The update is first put on a test system to ensure it functions properly and does not have any mistakes

(vi) **Getting Approval:** Once the test is successful, permission by the lab manager is given to apply the update to the rest of the lab computers

Documentation and Reporting

All maintenance procedures, including hardware inspections, software upgrades, environmental monitoring, and security scans, are recorded in a digital maintenance tracker. The lab manager

checks these records on a monthly basis and summarizes them on a quarterly basis to help support accreditation audits and continual improvement.

Staff Training and Awareness

Laboratory staff are trained initially and periodically on how to maintain equipment, safely handle hardware, revise processes, and report accidents. Annual refresher training and review of standard operating procedures allow employees to stay current with emerging technologies and standards.

Staffing

For the digital forensics lab to run effectively and within the bounds of ethics, two main positions of staff are suggested: Lab Manager and Digital Forensics Technician. Both are important in upholding high levels of evidence handling, case examination, compliance with accreditation standards, and laboratory security. Both positions demand signed confidentiality agreements, background screening, and ongoing training on legal parameters, ethical standards, and best ways of evidence preservation.

Lab Manager

The lab manager is responsible for the daily activity of the digital forensics lab. They make certain that any work is of high quality, compliant with regulations, properly managed so as not to damage evidence, and manages all staff members. Planning, policy development, and being the point of contact for external audits and legal issues are also part of this role.

Key Responsibilities:

(a) Coordinate laboratory processes and work

(b) Approve software and system updates (according to change management)

(c) Manage evidence intake, chain of custody, and case assignments

(d) Maintain compliance with ISO/IEC 17025 and ANAB accreditation standards

(e) Maintain maintenance records, revise documents, and get ready for audits

(f) Train and oversee laboratory technicians

(g) Act as liaison with police, legal practitioners, and accrediting bodies

Required Qualifications:

(a) Education & Certifications: The lab manager must have a Bachelor's or Master's in Digital Forensics, Computer Science, Cybersecurity, or Criminal Justice. Furthermore, the manager of this position must have one of the following certifications:

(i) Certified Forensic Computer Examiner (CFCE)

(ii) GIAC Certified Forensic Analyst (GCFA)

(iii) Certified Information Systems Security Professional (CISSP) – this is the preferred certification for this position

Experience: The lab manager's experience should not be fewer than 5 years of experience in digital forensics or cybercrime investigation. The lab manager should not have fewer than 2 years of experience as a supervisor or lab manager.

Other Requirements: The lab manager of this role must be thoroughly familiar with legal proceedings, acquainted with chain of custody, and thoroughly knowledgeable about accreditation standards (ISO/IEC 17025:2017).

Digital Forensics Technician

The job of the Digital Forensics Technician is to collect digital evidence, analyze it, catalog what they have, and help with investigations. The job takes hands-on technical expertise, attention to detail, and following strict guidelines for evidence handling.

Key Responsibilities:

(a) Create copies (forensic imaging) of digital devices with software such as FTK Imager or EnCase

(b) Check hard drives, phones, USBs, cloud storage, and network logs to find some digital evidence

(c) Prepare detailed forensic reports to aid investigators and court proceedings

(d) Keep equipment in working order and support routine maintenance and software updates

(e) Maintain proper chain of custody and documentation at all times

Required Qualifications:

(a) **Education & Certifications:** The lab technician is required to have an Associate's or Bachelor's degree in Digital Forensics, Cybersecurity, Information Technology, or Criminal Justice. It is also recommended to have least one of the following certifications:

(i) CompTIA Security+

(ii) GIAC Certified Forensic Examiner (GCFE)

(iii) EnCase Certified Examiner (EnCE)

(iv) Cellebrite Certified Mobile Examiner (CCME)

Experience: The technician is required to have 1–3 years of direct digital forensic experience or equivalent internship in a law enforcement or accredited forensic laboratory setting.

Other Requirements: For this position, the technician must be familiar with forensic tools such as Autopsy, Wireshark, and FTK. And they also need to be able to write clear and professional forensic reports.

References

ANAB ANSI National Accreditation Board. (n.d.). Forensic calibration accreditation: ISO/IEC 17025. ANAB. https://anab.ansi.org/accreditation/iso-iec-17025-forensic-calibration/

Bl@ckC!pH3r. (2025, May 8). *Top 50 digital forensics tools*. Medium. https://medium.com/infosec-ninja/top-50-digital-forensics-tools-5f83d6000411

Certification - ISFCE. (2024, August 22). ISFCE. https://isfce.com/certification.html

Club, T. C. (n.d.). *Top 24 Digital Forensics Software Of 2024*. The CTO Club. https://thectoclub.com/tools/best-digital-forensics-software/

Critical steps to accreditation. (n.d.). https://www.justice.gov/ncfs/file/795111/dl

EclipseForensics. (2021, April 19). *The Best Hardware and Software Tools for Computer Forensics*. Eclipse Forensics. https://eclipseforensics.com/the-best-hardware-and-software-tools-for-computer-forensics/

GIAC Certifications. (n.d.). www.giac.org. https://www.giac.org/certifications/

IACIS - Home. (n.d.). IACIS. https://www.iacis.com/

International Organization for Standardization. (2017, November). ISO/IEC 17025:2017. ISO.org. https://www.iso.org/standard/66912.html

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology*. NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Mcdonald, J. P. (n.d.). *Building a Basic Computer Forensics Laboratory*. https://www.oas.org/juridico/spanish/cyber/cyb32_forensics_lab_en.pdf

NIST. (2024). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020, November 16). *Workforce Framework for Cybersecurity (NICE Framework*). Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

Taylor, S., Rakof, A., Zabri, M., & Talib, A. (2021). *Practical Guideline for Digital Forensics Laboratory Accreditation -A Case Study. Journal of Cyber Security, 3*(1), 1–6. https://www.oic-cert.org/en/journal/pdf/3/1/311.pdf

U.S. Bureau of Labor Statistics. (2023, September 6). *Forensic Science Technicians: Occupational Outlook Handbook: U.S. Bureau of Labor Statistics*. Bls.gov; U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm

U.S. Bureau of Labor Statistics. (2024, August 29). *Information Security Analysts: Occupational Outlook Handbook: U.S. Bureau of Labor Statistics.* Bls.gov; U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm