3 Year Forensic Lab Plan for a Mid-Sized Police Department

Vincent Rechkemer

Old Dominion University

CYSE 407

December 5, 2025

Summary

This report will map out a three-year plan to create a computer forensic lab for a mid-sized police department. It includes an accreditation plan that will follow the general standards of ISO/IEC 17025:2017. A diagram containing physical security measures as well as a proper layout will be proposed, as well as its inventory including software and hardware. Also, a maintenance plan for maintaining the operations of this forensic lab will be given. Finally, staffing descriptions as well as the requirements and preferences of the employees' qualifications will also be listed.

Accreditation Plan

It is absolutely imperative to have an accreditation plan in order to start a successful digital forensics lab. Applying for accreditation is a process and requirements must be met before the process should begin. Accreditation provides forensic labs a competitive edge over other labs and can lead to more potential opportunities for collaboration.

Year 1

In the first year, the digital forensics lab must follow and adhere to the general and structural requirements provided for ISO/IEC 17205 accreditation. The main principles of the general requirements are impartiality and confidentiality ("ISO/IEC 17025 Accreditation", 2024). Labs must be impartial and maintain confidentially. A few ways a digital forensic lab can show they meet the general requirements would be having a chain of custody, proper training, and effective policies. The structural requirements in ISO/IEC 17205 include documenting procedures, legal setup up, and management oversight (Evans, 2024). Both general and structural

requirements are the baseline for building a successful digital forensics lab and should be enforced firmly.

Year 2

By year two, resource requirements must be met. Resource requirements include competence requirements on personnel, suitable facilities, and validated equipment (Evans, 2024). Having competence requirements on personnel with ensure the employees have the skills and knowledge to perform their job efficiently. The importance of having a suitable facility is critical to ensure tasks are completed properly. Not having a suitable facility will open the digital forensic lab to extreme risks. Having validated equipment is imperative to ensure the evidence integrity.

Process requirements also ensure the evidence integrity. Having evidence integrity will ensure evidence gathered by the digital forensics lab will be admissible in court. The ISO/IEC 17025 process requirements include (ISO/IEC 17025 Accreditation, 2024):

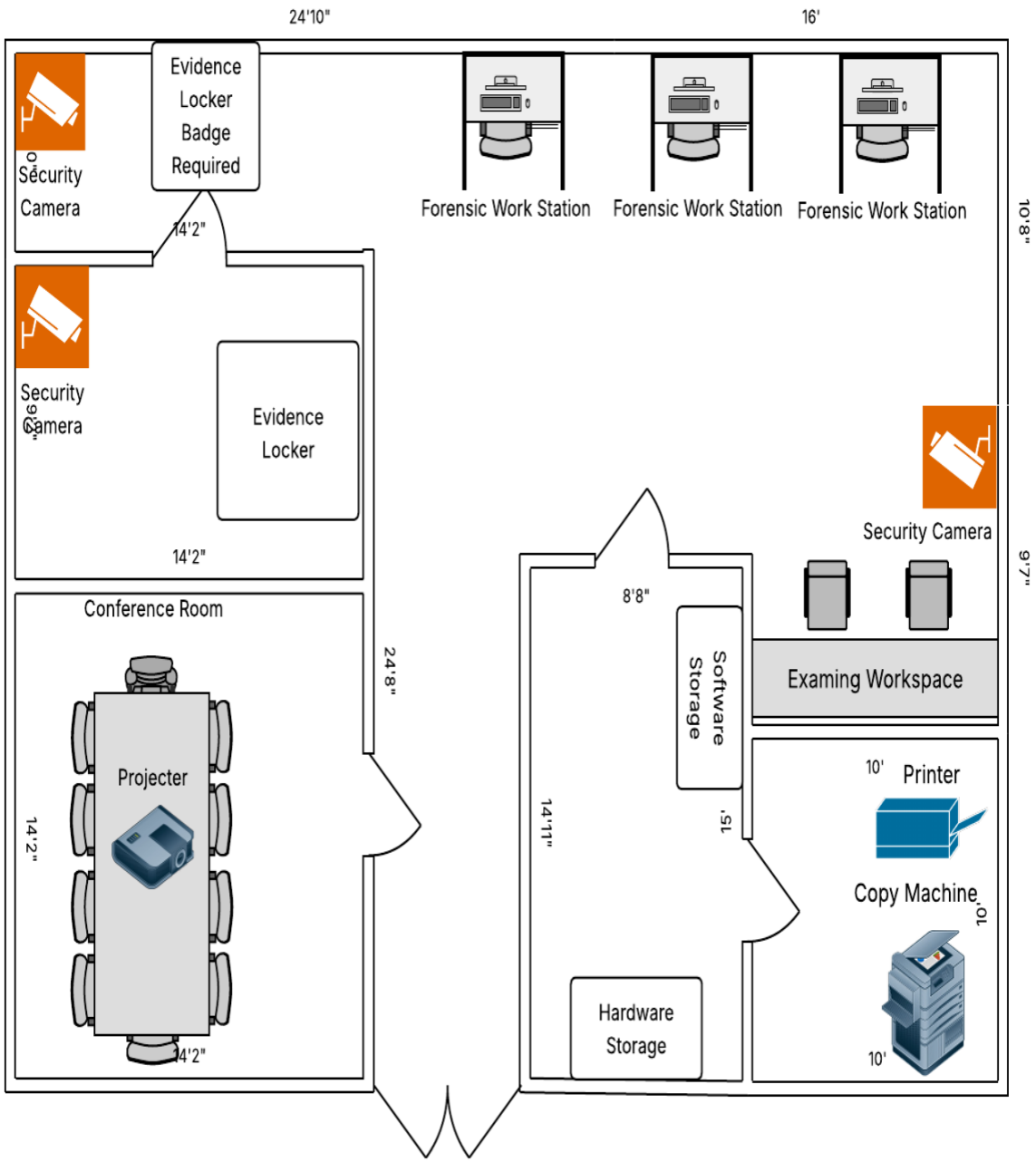
- Contract and Client Communication
- Method Selection and Validation
- Sampling Procedures
- Management of Test Items
- Technical Record Management
- Result Validation
- Evaluation of Measurement Uncertainty
- Result Reporting
- Complaint Handling

- Nonconformity Management
- Control of Data and Information Management

Year 3

After two years of adhering and following the requirements for IEC/IS0 17025 accreditation, the lab should be able to apply for accreditation. By this time, the lab will have built an effective case to why they deserve to be accredited. It will take around eighteen months for the accreditation process to be completed for the lab to achieve accreditation (Zarwell et al., 2024). It is absolutely imperative for the digital forensic lab to keep up with advancements and ensure their requirements are being met at all times.

Diagram for Lab Layout



Inventory

Hardware

- Evidence Storage For 20 Cases
- Three Security Cameras
- Printer
- Printer Paper
- Copy Machine
- Projector
- Three Forensic Workstations (3 Desktops and 3 Small Desks, Sufficient RAM Storage)
- 13 Work Chairs
- Two Long Desks (One for Conference Room, Other for Evidence Examining Workspace)
- Hardware Storage Bin
- Software Storage Bin
- A/C Unit
- Access Badges
- PC Power Cables
- PC Components
- WIFI Adapter
- Write Blocker
- Sim Card Reader

Software

- Wireshark

- Kali Linux
- EnCase
- FTK Imager
- Autopsy
- Helix Pro
- All Microsoft Applications
- Virus Protection

Maintenance Plan

This digital forensics lab needs constant maintenance in order to keep up with professional standards. Forensic software applications must be updated regularly to ensure up to date security improvements and new features. Employees must be informed and kept up to date on these new software updates. Digital forensic applications must be formally tested at least twice a year to ensure their reliability for maintaining accreditation. All of these software updates should be logged. Microsoft applications and virus protection should also be regularly updated. Regular updates to software are imperative for the integrity of the evidence being obtained.

The hardware in the digital forensic lab also must have constant maintenance. The security cameras in this lab must be up and running at all times. Anytime these security cameras have an outage, immediate fixes should be imperative. Monthly checks on these security cameras should occur as a proactive approach. The badges given to the employees to access the secure evidence room must also have maintenance. If an employee experiences issues with their badge, the issue must be solved immediately. If needed, the manufacturer should be involved depending on the severity of the issue.

Anytime there is damage to hardware used in this lab, inspections and/or repairs should be made. If repairs can't be made, replacement may have to be made to maintains operational standards. Since some damage to hardware is hard to diagnose, monthly detailed inspections should occur. Several pieces of hardware that will be inspected monthly include storage bins, forensic workstations, write blockers, and PC components.

Training lab personnel is an absolutely critical part of maintaining a digital forensics lab. Digital forensics is an evolving field that continues to grow. Employees should be given annual refreshers as well as updates on advancements occurring in digital forensics (Building a Digital Forensics Lab, 2025). This will keep employees updated to ensure their methods in handling digital evidence are reliable.

Staffing

Lab Manager

The lab manager will be responsible for overseeing the digital forensics lab operations. Also, the lab manager will deal with budgeting and purchases. In order to qualify for this position, a minimum of a bachelor's degree is required. In particular, a bachelor's degree in digital forensics or a relating field as well as multiple years in a supervisory role is required.

Technicians

The technicians are responsible for receiving and taking care of digital evidence given to them by law enforcement agencies, clients, law firms, or private investigators (Evidence Technician, 2024). While taking care of this evidence, they will maintain a proper chain of custody and follow proper protocols in dealing with the evidence. A bachelor's degree in digital

forensics or a related field is required. Also, obtaining certifications can be beneficial. Some certifications that will help include:

- CompTIA A+
- CompTIA Security+
- IAPE Evidence Specialist
- Cellebrite CCO

Digital Forensic Examiner

The role of a digital forensic examiner include (AU Online, 2024):

- Providing evidence reports
- Recovering and restoring data
- Collecting digital evidence from computer-based crimes
- Extracting data from digital devices

Requirements for becoming a digital forensic examiner would be having a bachelor's degree in digital forensics or any other relating field. Digital forensic examiners must also have multiple years of experience in the field of digital forensics. Also, having certifications such as Certified Forensic Computer Examiner and/or GIAC Certified Forensic Analyst will help enhance their skills and qualifications.

References

Building a Digital Forensics Lab. ACE Computers. (2025, October 31). https://acecomputers.com/forensics/blog/building-a-digital-forensics-lab/

Evans, N. (2024, March 12). *ISO 17025: Everything Labs Need To Know*. QBench Cloud-Based LIMS. https://qbench.com/blog/iso-17025-everything-labs-need-to-know

Evidence technician. Carney Forensics. (2024, June 18). https://www.carneyforensics.com/evidence-technician/

Two types of professionals work to fight cybercrime: Those who focus on preventing cyberattacks, and those who investigate them after they've occurred. Digital Forensic Examiner: Salary and Job Description. (2024, August 27). https://www.augusta.edu/online/blog/digital-forensic-examiner-salary

What is ISO/IEC 17025 accreditation - importance & benefits. CloudLIMS. (2024, November 20). https://cloudlims.com/what-is-iso-iec-17025-accreditation-key-benefits-the-role-of-an-iso-iec-17025-lims-solution/

Zarwell, L., Grassel, J., & Pilkington, M. M. (2024, January 31). *Police crime lab accreditation initiative*. National Institute of Justice. https://nij.ojp.gov/topics/articles/police-crime-lab-accreditation-initiative