Erik C. Sorto

CYSE 407

Spring 2025

Midterm - Digital Forensics Lab Proposal

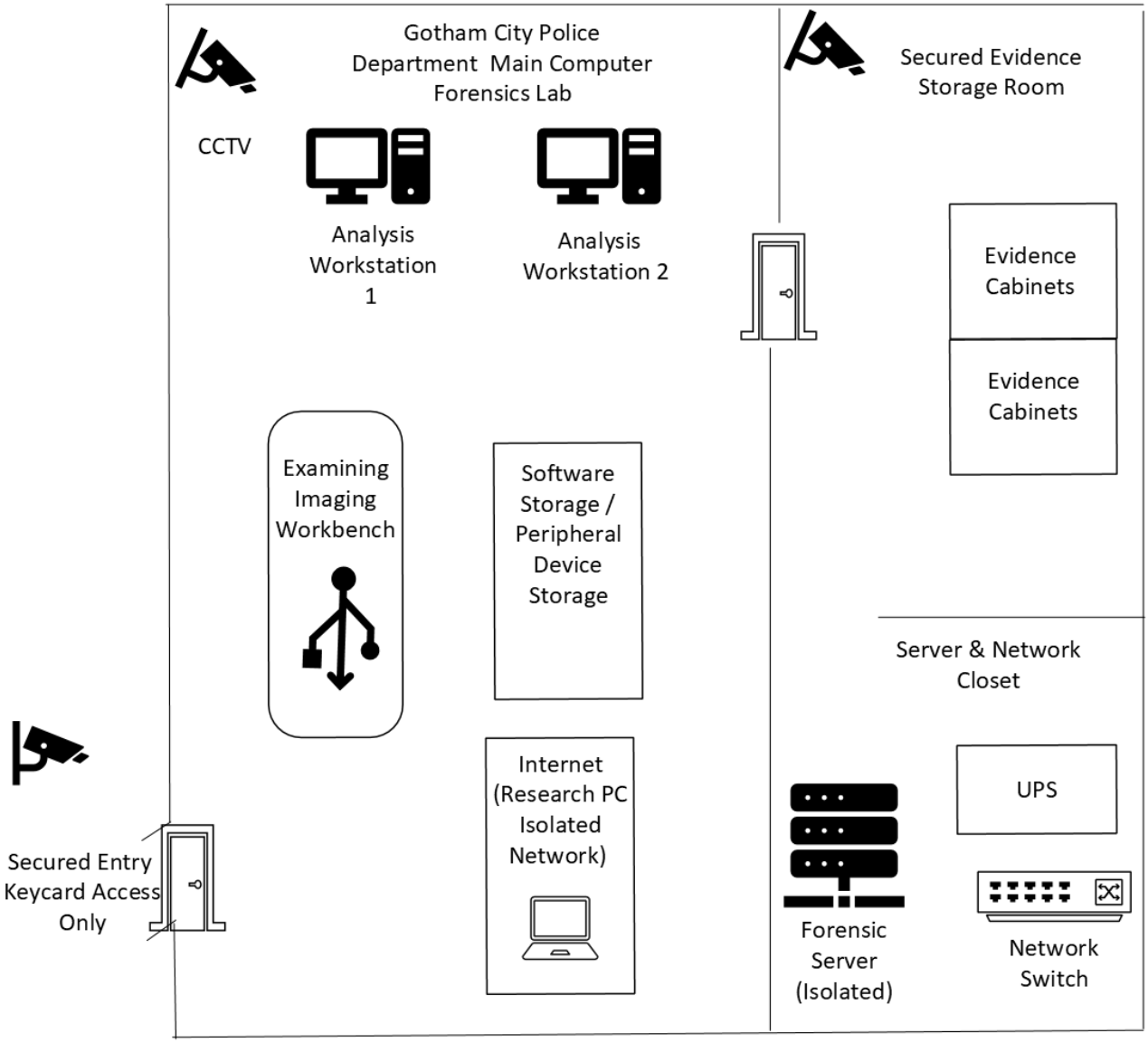
Introduction

In this modern digital world, the use of technology continues to be a necessity in our everyday lives as more devices are connected through the internet of Things. Investigators rely heavily on the importance of digital evidence to solve cases and having a properly structured computer forensics lab to process and analyze evidence is paramount. It is an honor to be granted this opportunity to create a proposal for the Gotham City Police Department (GPD). This proposal exclusively focuses on digital forensics and physical and DNA-related divisions fall outside of the scope of this project. The Computer Forensics lab will primarily support evidence intake, examination, secure storage, and reporting, while meeting the standards that a modern digital forensics lab should have. My proposal outlines a 3-year plan that includes the following:

- A professional floor diagram of the laboratory
- Complete equipment and software inventory
- An accreditation plan aligned with ISO/IEC 17025 and ANAB guidelines
- A maintenance plan to maintain hardware, software, and evidence systems.

The goal ultimately is to design a lab that is secure, compliant, and aligned with industry standards.

1. Laboratory Floor Plan



2. Equipment Inventory

This inventory lists the specific hardware, software, and specialized tools needed to operate GPD's Computer Forensics lab. Every item listed supports industry standards and the lab's core functions: evidence acquisition, forensic acquisition, forensic analysis, secure storage and reporting.

A. Hardware:

Analysis Workstations (2 Units):

High-performing modern forensic workstations that are designed for imaging, processing, and analysis must be equipped with the necessary specifications:

- Intel i9 or Ryzen Class CPU
- 64GB RAM (128GB May be needed with current events involving AI Models and automation)
- Dual NVMe SSDs (Windows OS Dual Boot and Linux)
- USB 3.2 and USB-C Ports
- Dual-monitor capable
- Keyboard & Mouse

Write Blockers – Required to ensure the hardware's use of the data cannot be altered during acquisition

- SATA Write Blocker
- USB Write Blocker
  NVMe Write Blocker
- IDE/SAS Adapters

B. Evidence Handling and Storage Equipment

- Locking evidence storage cabinets (ensuring 20-case capacity)
- Barcade label printer and scanner
- Chain-of-custody logging system
- Anti-Static mats
- Faraday bags and ESD protective tools

C. Networking and Server Equipment

Ensuring secure networks for internal forensic tasks.

- Forensic Storage Server (isolated intranet)
- RAID 5 or 6 configuration

- Redundant power supplies
- Encrypted storage volumes
- Internal network switch (ensuring no external internet access)
- UPS System (Power back up)

D. Software Toolkits

Forensic Suites

- Encase Forensic
- FTK
- Autopsy
- Magnet AXIOM

Imaging Tools

- FTK Imager
- Guymager
- dd / dcedd

Password Recovery Tools

- Hashcat
- Password Kit Forensic

Network and Memory Forensics

- Wireshark
- Volatility
- Cyberchef

Administrative Software

- Microsoft Office
- Adobe Acrobat
- CaseGuard or similar (case-management system)

E. Security Equipment

- Keycard access control
- CCTV cameras (Primarily at lab entrance and evidence room)
- Secured doors with alarms
- Fire Extinguisher

3. Accreditation Plan

Accreditation will help establish the Gotham City Police Department Computer Forensics Laboratory as a reliable, defensible and professionally recognized digital evidence facility. So that all laboratory operations are compliant with National standards for forensic quality, GPD will apply for Accreditation through the ANSI national accreditation Board (ANAB) under ISO/IEC 17025, the international standard for testing and calibration laboratories. Accreditation is a methodical process requiring constant operational readiness / documentation / internal audits / validation studies and an external assessment. Based on national expectations and ANAB assessment procedures, this proposal proposes a three-year accreditation plan to achieve full compliance when the lab goes live.

Year 1 – Set Up the Lab and Create Procedures

The first year focuses on building the foundation the lab needs before applying for accreditation.

- Develop all Standard Operating Procedures (SOPs)
- Create chain-of-custody protocols
- Establish the Quality Management System (QMS)
- Train staff on proper evidence handling
- Begin validating forensic tools and documenting results
- Start basic casework following the written procedures

By the end of Year 1, the lab will be operating with formal procedures and documentation in place.

Year 2 – Quality Assurance and Internal Review

During the second year, the lab improves its consistency and prepares for outside review.

- Conduct internal audits
- Fix any gaps or issues in procedures

- Complete full validation of all forensic tools
- Participate in proficiency testing
- Update SOPs and documentation as needed
- Prepare all paperwork required for accreditation

By the end of Year 2, the lab will be ready to submit its application.

Year 3 – Apply and Complete Accreditation

The third year focuses on the official accreditation process.

- Submit the formal application to ANAB
- Undergo documentation review
- Host on-site assessors who inspect the lab
- Correct any issues they identify
- Receive accreditation once everything meets the standard

Accreditation confirms that the Gotham City Police Department's Computer Forensics Lab follows reliable, repeatable, and defendable forensic practices.

4. Lab Maintenance Plan

To keep the Gotham City Police Department's Computer Forensics Lab running securely and reliably, the lab will follow a regular maintenance schedule for hardware, software, and security systems. The goal is to ensure tools remain accurate, up-to-date, and defensible in court.

Hardware Maintenance

- Inspect forensic workstations every 6 months
- Replace failing hard drives, cables, and adapters as needed
- Test write blockers regularly to confirm they function correctly

- Keep the server and UPS system in good working condition
- Clean equipment, remove dust, and check airflow inside computers

---

Software Maintenance

- Install updates for EnCase, FTK, Autopsy, and other tools when released
- Validate major software updates before using them in real cases
- Apply operating system security patches monthly
- Maintain licenses and renewal records for all forensic software

---

Security Maintenance

- Review keycard access logs weekly
- Ensure CCTV cameras are functioning and recording properly
- Check that evidence cabinets remain locked and sealed
- Test alarms and access control systems regularly

Evidence & Documentation Maintenance

- Conduct weekly evidence inventory checks
- Make sure chain-of-custody logs are complete and accurate
- Verify evidence storage room temperature and environment
- Shred or archive old administrative documents following policy

---

Network & Server Maintenance

- Monitor the forensic server for errors
- Check RAID storage health and backup integrity
- Update internal network configurations if needed
- Ensure the network remains isolated from the internet

Maintaining the lab is an ongoing job that aims to keep everything running as it should be while keeping everything organized and up to date. The Lab manager is tasks to keep inventory of equipment including model, serial number and location. Each device needs regular maintenance so problems can be caught early. Equipment that needs calibration should be checked as needed and documented as to meet the standards. After the

scheduled maintenance is completed, there must be records that must be kept and recorded of what was done, documenting who performed it with their signature. Anything that cannot be fixed or unreliable should be removed from service immediately. The lab also needs a plan to upgrade older hardware since computer components typically have a limited life cycle. Staying on top of updates and replacing equipment, when necessary, keeps the lab up and running to handle digital evidence without putting data or accuracy at risk.

5. Staffing

GPD's Computer Forensics lab requires two Positions to run the lab effectively: One is the lab manager, and the other is the Digital Forensics lab technician. These roles include day-to-day work, evidence handling, documentation and following procedure.

Lab Manager

This Lab Manager keeps the entire forensics Lab organized, secure and in compliance with department policies. This person is responsible for the quality of work done and for handling reports, evidence and procedures properly. A Lab Manager also will maintain SOPs, equipment inventory, case reports and accreditation. They will supervise staff, maintain chain of custody records, schedule and make final decisions regarding lab operations.

- Main responsibilities include:
- Overseeing evidence intake and storage
- Approving forensic reports
- Managing SOP updates and documentation
- Training and supervising the technician
- Keeping the lab ready for audits or accreditation reviews
- Making sure all tools are validated and functioning properly

---

Digital Forensics Lab Technician

The technician performs most of the hands-on work in the lab. This includes imaging drives, collecting and examining digital evidence, and helping prepare case

files for investigators. The technician follows the procedures set by the Lab Manager and documents every step to make sure evidence stays admissible in court. They also help maintain lab equipment, update software tools, and report any issues right away.

- Main responsibilities include:
- Performing forensic imaging and using write blockers
- Analyzing digital evidence following lab procedures
- Preparing notes and documentation for reports
- Keeping the equipment clean, updated, and working properly
- Supporting evidence storage and organizing case materials
- Following chain-of-custody rules for every item they handle

---

Staffing Summary

These two positions work together to keep the lab efficient, secure, and compliant. The Lab Manager focuses on oversight, quality, and documentation, while the Digital Forensics Technician handles the technical and day-to-day forensic tasks. Both roles are necessary for the Gotham City Police Department to run a dependable and professional digital forensics lab.

Conclusion

A digital forensics lab for the Gotham City Police department is one step toward improving how the Department processes and investigates digital evidence. It proposes a realistic lab layout with secure equipment and staffing. By following organized procedures and working towards accreditation the lab will be able to work at a professional standard and support reliable casework. The goal is to have a secure, efficient space that can produce accurate results that stand in court. With the proper systems, tools and staff in place, GPD will have a modern forensics lab to meet the demands of digital investigations for years to come.

References

Steuart, B. N., Phillips, A., & Chapple, C. (2018). *Guide to Computer Forensics and Investigations: Processing Digital Evidence.* Cengage Learning.

NIST. (2023, March 20). *Personal identity verification (PIV).* https://www.nist.gov/identity-access-management/personal-identity-verification-piv

North Carolina State Crime Laboratory. (2017, December 18). *Procedure for equipment calibration and maintenance.* https://forensicresources.org/wp-content/uploads/2019/07/Equipment-Calibration-and-Maintenance-12-18-2017.pdf

ANSI National Accreditation Board. (2023, January 18). *ISO/IEC 17025 forensic — documents and resources.* https://anab.ansi.org/resource/iso-iec-17025-forensic-documents-resources/

Dutton, G. (2021, August 23). *Lab security tips for cyber and physical threats.* Lab Manager. https://www.labmanager.com/lab-security-tips-for-cyber-and-physical-threats-26570

Crime Scene Investigator EDU. (2021, October 20). *Forensic lab technician jobs, education and salary information.* https://www.crimesceneinvestigatoredu.org/forensic-lab-technician/

Infosec Institute. (2021, January 8). *Popular computer forensics tools (Top 19).* https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-tools/

U.S. Bureau of Labor Statistics. (2023, April 25). *Forensic science technicians.* https://www.bls.gov/oes/current/oes194092.htm

National Institute of Standards and Technology. (n.d.). *Computer Forensics Tool Testing Program (CFTT).* https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program

CSI Education. (2021). *How to become a forensic laboratory technician.* https://www.crimesceneinvestigatoredu.org

FBI Laboratory Services. (n.d.). *Digital evidence handling and chain of custody guidelines.* https://www.fbi.gov/services/laboratory