Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Digital Forensics Laboratory Plan (Three- Year Operational Plan)

Summary

This report provides a comprehensive three-year plan for establishing a functional digital forensics laboratory for a mid-sized police department. The proposed laboratory is designed to support the acquisition, preservation, analysis and reporting of digital evidence while adhering to industry standard, legal expectations, and accreditation requirements. The plan describes the physical layout of the lab to include secure evidence storage for up to twenty active cases, two dedicated forensic analysis workstation, and controlled access to ensure the integrity and confidentially of investigative materials. The design also incorporates essential physical security measures such as CCTV monitoring, badge-restricted entry, and isolated forensic workstations aligning with national recommendations for digital evidence environments.

This plan also includes a detailed inventory lists in the specialized hardware, software, and security controls required for modern forensic operations. Including forensic imaging equipment, write blockers, analysis workstations, mobile forensic tools, isolation device, and validated software suites such as EnCase, FTK, Autopsy, Cellebrite UFED, and Magnet AXIOM. These tools reflect best practices outlined in national and international guidelines, including those published by NIST, which emphasize validated tools, reproducible processes, and defensible documentation.

Crucial to the lab's long-term success is its accreditation strategy. This plan aligns the laboratory with ISO/IEC 17025:2017 standard, recognized as the benchmark for the competence of testing and calibration laboratories. Accreditation will be pursued through the ANSI National Accreditation Board (ANAB), who oversees forensic accreditation in the United States and established requirements for quality management systems, staff competency, documentation controls, and proficiency testing. The report outlines a structured accreditation timeline consisting of preparation, implementation, internal audits, proficiency testing, and final assessments.

The maintenance plan provides standardized procedures for equipment calibration, software verification, security reviews, and preventative maintenance, reflecting NIST recommendations for digital forensic reliability. Lastly, the staffing plan outlines roles for a Digital Forensics Lab Manager and a Digital Forensics Technician, including responsibilities, qualifications, and expected contributions to quality assurance, case workflow and laboratory compliance.

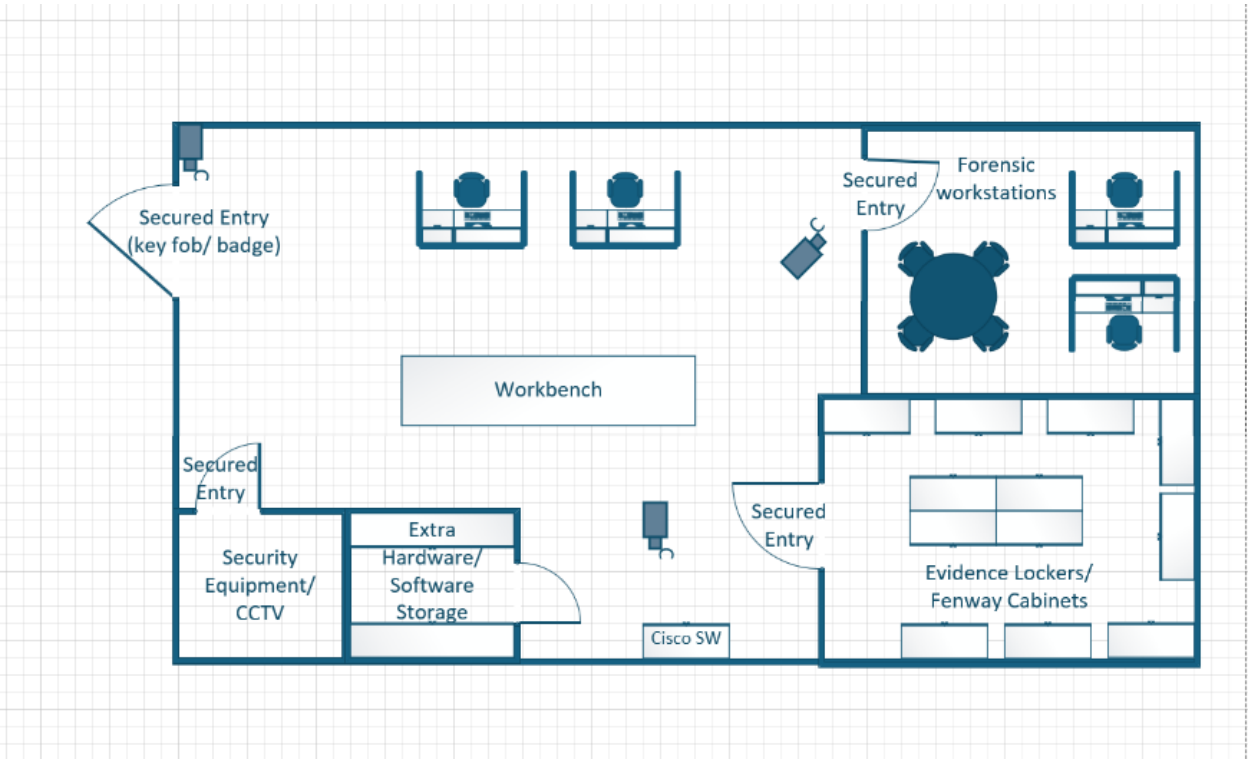
Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

These components together form a cohesive, scalable plan that equips the police department with a secure, efficient, and accreditation-ready digital forensics laboratory capable of supporting high-quality investigative work.

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Lab Layout

The diagram below illustrates the proposed digital forensics lab layout.



Security Controls

- Badge access system
- 24/7 CCTV monitoring
- Air-gapped forensic workstations
- Faraday shielding for wireless isolation
- Locked, restricted-access evidence storage room

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Inventory

Hardware	
Description	**Items**
Forensic Workstations	2 high-performance forensic PCs (12-core CPU, 64GB RAM, NVMe SSD, GPU support)
Write Blockers	Tableau Universal Write Blockers (USB/SATA/IDE)
Network Forensics Tools	Managed isolated switch, packet capture appliance, Wi-Fi analyzer
Mobile Forensics	Cellebrite UFED
Isolation Equipment	Faraday cabinet, Faraday bags
Storage Systems	20TB RAID NAS for forensic images, backup server
Adapters & Cables	STA/IDE adapters, drive docks, USB cables, network cables
Evidence Storage	20 metal evidence lockers with barcode system
Security Infrastructure	IP cameras, NVR, badge reader

Software	
Software	**Reason**
EnCase Forensic	File system analysis, imaging
FTK	Evidence indexing, carving, registry analysis
Autopsy/ Sleuth Kit	Open-source forensic analysis
Magnet AXIOM	Cloud, computer and mobile forensics
Cellebrite UFED	Mobile acquisition and analysis
ProDiscover	Disk imaging and examination
Kali Linux	Network analysis and incident response
Wireshark	Packet capture and protocol analysis
Bulk Extractor	Artifact and keyword extraction

These tools align with NIST recommendations for forensic software which must be validated, maintained, and reproducible to ensure scientific defensibility.

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Accreditation Plan (ISO/IEC 17025)

Accredited Organization	Accreditation Standard	Purpose/Scope	Application Requirements	Steps to Achieve Accreditation
ANAB (ANSI National Accreditation Board)	ISO/IEC 17025:2017	Primary US accreditation for forensic testing and calibration laboratories. Required for most government forensic labs.	• Completed application • Quality Management System (QMS) • Documented SOPs • Organizational Chart • Staff training records • Evidence handling and chain-of-custody procedures • Internal audit records.	1. Obtain ISO/IEC 17025 documentation 2. Develop QMS and SOPs 3. Conduct internal audits & corrective actions 4. Submit ANAB application 5. On-site pre-assessment 6. Resolve findings 7. Full assessment and proficiency testing review 8. Receive accreditation; maintain through annual surveillance audits
A2LA (American Association for Laboratory Accreditation)	ISO/IEC 17025: 2017	Alternative international accreditation body accepted for forensic science labs. Similar scope to ANAB, it is less commonly used for digital forensics.	• QMS documentation • Scope of testing • Method validation records • Equipment calibration records • Staff competency documentation	1. Submit request for quote 2. Prepare QMS and documentation 3. Participate in assessor interview 4. Undergo full assessment 5. Complete corrective actions 6. Accreditation awarded upon approval
ASCLD/LAB (Legacy Program)	International Program (ISO/IEC-based) *Has been merged into ANAB, but is still referenced historically*	Former primary accreditation body for US forensic labs prior to ANAB consolidation. Listed here for completeness and context	• Evidence of compliance with legacy ASClD/LAB requirements • Document control and chain-of-	No longer accepting new labs; transitioned under ANAB (historical frameworks continue to influence ANAB's digital forensics assessment criteria).

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

			custody procedures.	
SWGDE Compliance (Not a formal accreditation)	SWGDE Best Practices & Guidelines	Ensures lab procedures align with widely recognized digital forensic standards	• Adoption of SWGDE-approved methods • Internal documentation validating method reliability	1. Review SWGDE best practices 2. Validate lab methods according to guidance 3. Incorporate into QMS 4. Conduct internal reviews and annual updates
NIST OSAC Registry Alignment (Voluntary)	OSAC-recommended standards and practices	Provides recognition that lab processes algin with nationally accepted forensic standards.	• Method documentation aligning with OSAC-approved standards • Participation in proficiency testing	1. Identify OSAC-listed standards applicable to digital forensics 2. Update SOPs accordingly 3. Document compliance mapping

---

Lab Maintenance Plan

A lab maintenance plan ensures reliability, security, and compliance across all equipment and processes.

<u>Calibration</u>

- The lab should conduct annual calibration of all write blockers
- Conduct regular verification of imagining tools
- Maintain logs containing calibration dates, results and the next maintenance date.

<u>Software Maintenance</u>

- The lab should conduct quarterly update cycles for forensic tools
- Conduct validation testing after major updates
- Documentation stored in QMS

<u>Hardware Maintenance</u>

- The lab should conduct an annual inspection of workstations and storage arrays
- Replace aging drives
- Conduct continuous health monitoring of RAID systems

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Security Reviews

- The lab should conduct access control audits on a quarterly basis
- Evidence room inventory reconciliation
- Annual CCTV system validation

Corrective Actions

- Equipment failures trigger immediate removal from service
- Document in corrective action log
- Revalidate before returning to operational use

These guidelines align with the NIST recommendations for lab reliability and defensibility.

Staffing Plan

Digital Forensics Lab Manager

Responsibilities:

- Oversee daily lab operations
- Maintain accreditation documentation
- Review all forensic reports
- Manage chain-of-custody integrity
- Conduct internal audit
- Coordinate with detectives and legal teams

Qualifications

- Bachelors in Cybersecurity or Digital Forensics
- 5+ years of forensics experience
- Certifications in EnCE, CFCE, GCFA, or similar
- Familiarity with ISO/IEC 17025

Digital Forensics Technician

Responsibilities:

- Perform forensic imagining and evidence intake
- Maintain hardware/ software inventory
- Document chain-of-custody
- Prepare systems for forensic analysis
- Assist with mobile and cloud evidence acquisition

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

Qualifications:

- Associate or Bachelor's in IT or Cybersecurity
- Experience with forensic tools (FTK, EnCase, Cellebrite)
- Strong documentation skills
- Knowledge of Linux, Windows, MacOS

Name: Emma Humphreys
Date: December 5, 2025
Course: Digital Forensics
Assignment: Mid-Term

References:

Aguilar, J., Barnes, T., Browne, J., Burney, Y., Byrd, J., Carver, B., Denmark, A., Halla, S., Hartman, L., Kennedy, A., Leben, D., Matheson, G., McClaren, J., McElroy, R., Miranda, R., Mohr, K., Mount, M., Sigel, S., Smither, J., ... Williams, S. (2013, June). NISTIR 7941: Forensic Science Laboratories: Handbook for Facility Planning, Design, Construction, and Relocation. National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913987

ANAB ANSI National Accreditation Board. (n.d.). Accreditation for forensic inspection bodies: ISO/IEC 17020. ANAB. https://anab.ansi.org/accreditation/iso-iec-17020-forensic-inspection-bodies/

Best Practices for Digital Evidence Collection: SWGDE 18-F-002-2.0. SWGDE. (2025, July 8). https://www.swgde.org/wp-content/uploads/2025/07/2025-06-30-Best-Practices-for-Digital-Evidence-Collection-18-F-002-2.0.pdf

National Institute of Standards and Technology. (2006). Guide to integrating forensic techniques into Incident response (NIST SP 800-86). https://csrc.nist.gov/publications/detail/sp/800-86/final

National Institute of Standards and Technology. (2014). Guidelines on mobile device forensics (NIST SP 800-101r1). https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final

U.S. Department of Justice. (2008). Electronic crime scene investigation: A guide for first responders. https://www.ojp.gov/pdffiles1/nij/219941.pdf