DIGITAL FORENSICS LABORATORY OPERATIONS PLAN

Three-Year Establishment Plan for a Municipal Police Department

CYSE 407 – Computer Forensics
Midterm Assignment

April 21, 2026

Section 1: Laboratory Physical Layout

The digital forensics laboratory that will be constructed is to accommodate the information technology needs of a mid-sized police department for a minimum period of three years. The layout of the digital forensics laboratory is constructed according to best practices in the field. The digital forensics laboratory will be divided into eight different areas according to their purpose within the laboratory.

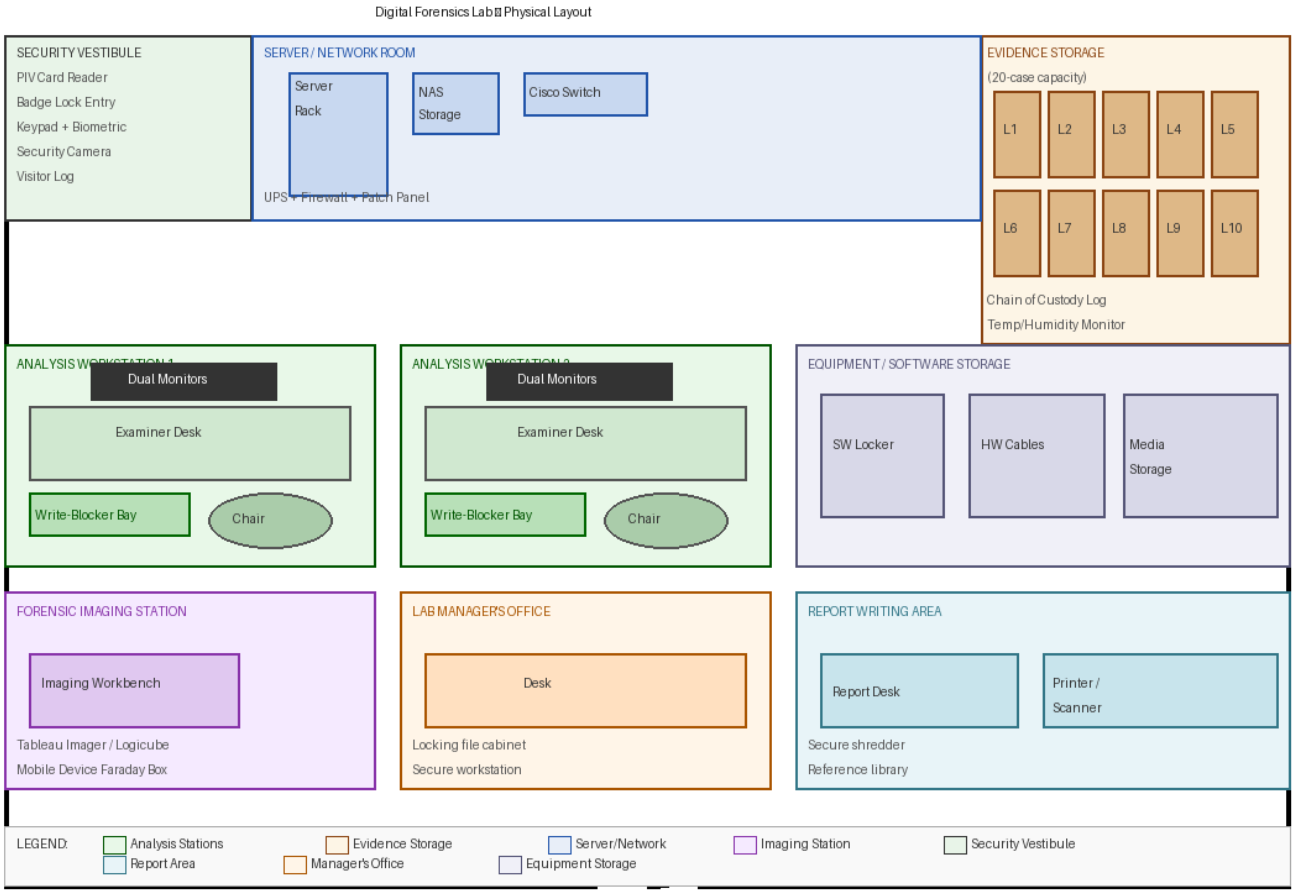


Figure 1: Digital Forensics Lab Floor Plan

Zone Descriptions

Security Vestibule (top-left): Features the facility's only entry point and utilizes PIV-activated smart cards and PINs to control who enters the facility. All visitors must sign in at the desk and be escorted by staff members with access to the facility. A security camera provides 24 hour coverage of the vestibule with recordings kept for 90 days.

Server / Network Room (top-center): Contains the forensic server, NAS drives, switch, UPS battery, and firewall. This room is climate-controlled and accessible only to the Lab Manager and IT personnel.

Evidence Storage Room (top-right): A locked room with climate control and ten physical lockers containing slots for up to 20 crime scene cases (two slots per locker for the drives containing the digital evidence). Access to the room is logged electronically with climate control monitored around the clock to ensure that the digital evidence does not degrade.

Analysis Workstation 1 & 2 (center-left and center): Features two separate workstations with dual monitors and hardware write blockers connected to air-gapped forensic workstations. The workstations are located in separate areas in the lab to prevent the transfer of digital evidence between analysts and potential contamination.

Forensic Imaging Station (bottom-left): Bench area dedicated to drive and mobile device imaging. Software included Tableau forensic imager and mobile device software (Logicube Falcon). Faraday enclosure for mobile device imaging.
Lab Manager's Office (bottom-center): Private office for the Lab Manager. Includes workstation, file cabinet, and area for tracking reports related to the management of the lab.
Report Writing Area (bottom-right): Area for writing reports on cases that have been completed. Workstation is not a case workstation, but a business class machine. Scanner, printer, and shredder are also present in this area.
Equipment / Software Storage (center-right): Area for storing software licensing discs, hardware accessories, cables, drives, and Faraday bags.

Section 2: Equipment Inventory

The following inventory lists all hardware and software required to equip the digital forensics lab at initial operational capacity. Items are organized by category.

Hardware

Item	Qty	Est. Unit Cost	Purpose / Notes
Dell Precision 7960 Tower Workstation (64GB RAM, 2TB NVMe)	2	$3,800	Primary analysis workstations – air-gapped, Windows 10 LTSC
Forensic Examination Server (128GB RAM, RAID-6)	1	$8,500	Central case file storage and processing server
Synology NAS – DS1823xs+ (48TB usable)	1	$3,200	Redundant case image and evidence backup storage
Tableau TX1 Forensic Imager	2	$2,100	Hardware-level write-blocked disk imaging
Logicube Falcon-NEO Drive Duplicator	1	$4,500	High-speed forensic disk duplication and verification
Cellebrite UFED Touch 2	1	$9,000	Mobile device acquisition and extraction
Faraday Bag Set (phone, tablet, laptop sizes)	10	$60	Signal-isolated mobile evidence containment
Faraday Shielded Enclosure (large)	1	$1,800	Bench-top mobile device examination enclosure
Cisco Catalyst 2960-X Switch (24-port)	1	$2,200	Managed network switch for lab segment
Fortinet FortiGate 60F Firewall/UTM	1	$1,100	Perimeter security for lab network segment
APC Smart-UPS 3000VA	2	$900	Battery backup for workstations and server
SpaceSaver High-Capacity Evidence Locker (10-unit)	1	$3,500	Primary evidence storage, 20-case capacity
27" 4K IPS Monitors	4	$450	Dual-monitor per workstation setup
Spectrum Analyzer (portable RF)	1	$800	Network/wireless investigation
HID Global PIV Card Reader + Controller	2	$600	Controlled access points – vestibule + evidence room
IP Security Camera System (4-camera NVR)	1	$1,200	Surveillance: entry, evidence room, lab floor
HP Color LaserJet Enterprise MFP	1	$650	Report printing and document scanning
Write Blocker Kit (USB 3.0, SATA, IDE, PCIe adapters)	2	$380	Hardware write-blocking for all drive interfaces
Miscellaneous Cables & Adapters (IDE, SATA, USB)	Lot	$350	Drive connection and evidence extraction
Ergonomic Examiner Chairs	3	$400	Examiner workstations and manager's office

Item	Qty	Est. Unit Cost	Purpose / Notes
Locking Evidence Bags (anti-static, various sizes)	200	$1.50	Evidence packaging and chain of custody sealing

Software

Software	License Type	Purpose
Magnet AXIOM (w/ Cyber Module)	Annual	Primary forensic examination and artifact analysis platform
AccessData FTK (Forensic Toolkit)	Annual	Disk imaging, indexing, password cracking, reporting
EnCase Forensic	Annual	Enterprise-grade investigation, timeline, and e-discovery
Cellebrite Physical Analyzer	Annual	Mobile device data analysis and reporting
Autopsy (The Sleuth Kit)	Free/Open-Source	Supplementary disk and file system forensics
Kali Linux	Free/Open-Source	Network forensics, penetration testing support, tools
Wireshark	Free/Open-Source	Network packet capture and protocol analysis
Volatility Framework	Free/Open-Source	Memory forensics and RAM artifact extraction
HashCalc / HashMyFiles	Free	File and evidence hash verification
Passware Kit Forensic	Annual	Password and encryption key recovery
Oxygen Forensic Detective	Annual	Cloud and mobile data extraction and analysis
CAINE Linux (Live Forensic OS)	Free/Open-Source	Bootable forensic environment for field acquisitions
Windows 10 LTSC (Enterprise)	Perpetual	Workstation OS – long-term support, no forced updates
Microsoft 365 (restricted admin workstations)	Annual	Report drafting and administrative tasks only

Section 3: Laboratory Accreditation Plan

Within the first 18 months of operation, the laboratory will work towards achieving formal accreditation. The laboratory intends to seek accreditation through the ANSI-ASQ National Accreditation Board (ANAB) according to the ISO/IEC 17025:2017 - General Requirements for the Competence of Testing and Calibration Laboratories standard, as well as according to OSAC (Organization of Scientific Area Committees) standards regarding digital and multimedia evidence. These accreditations are recognized by the courts, and indicate that the techniques and methodologies utilized by the laboratory are validated and auditable.

Accreditation Body

Primary Body: ANSI-ASQ National Accreditation Board (ANAB) – Forensic Science Testing and Calibration (https://www.anab.org/forensic-accreditation)

Standard: ISO/IEC 17025:2017

Secondary Reference: ASCLD (American Society of Crime Laboratory Directors) best practices and the DOJ Uniform Language for Testimony and Reports (ULTR) for Digital Evidence.

Timeline and Milestones

Timeframe	Milestone	Key Activities
Months 1–3	Foundation & Documentation	Procure ISO/IEC 17025:2017 standard. Establish Quality Management System (QMS). Draw organizational chart and authority matrix. Begin writing Standard Operating Procedures (SOPs) for examination methods.
Months 4–6	SOP Development & Training	Standard Operating Procedures (SOPs) and Training Complete SOPs for disk imaging, mobile device extraction, network forensics and reporting. Ensure all staff members have completed ISO 17025 training. Ensure lab manager has completed ANAB pre-accreditation workshop.
Months 7–9	Internal Audit & Gap Analysis	Internal Audit Conduct initial internal audit according to the ISO/IEC 17025:2017 standard (Sections 4-8). Address any non-conformances in the report. Perform Measurement Uncertainty analyses for each test method in the lab.
Months 10–12	Application Submission	Application to ANAB Complete and submit application to ANAB including scope of accreditation and all required documentation (6A.1-6A.16). Pay the registration fees to ANAB. Schedule on-site assessment by ANAB.
Months 13–15	On-Site Assessment	Allow assessors to review competency tests (proficiency tests). Address any findings from assessment report.
Months 16–18	Accreditation Granted	Accreditation Granted Receive certificate of accreditation from ANAB. Post the certificate of accreditation in the forensic lab. Begin surveillance cycle for quality (internal audits every year, re-accreditation every 2 years).

Required Documentation (ISO/IEC 17025:2017 Attachment Set)

The following documentation packages are required for the ANAB application submission:

- 6A.1 – Quality Management System manual
- 6A.2 – Site assessment checklist
- 6A.3 – Organizational chart with reporting relationships

- 6A.4 & 6A.5 – Document control policy and procedure
- 6A.6 – Corrective action procedure with sample records
- 6A.7 – Preventive action procedure
- 6A.8 – Internal audit procedure and results
- 6A.9 – Management review records
- 6A.10 – Quality assurance (QA) report examples
- 6A.11 – Facility floor plan (see Section 1)
- 6A.12 – Validated test methods list
- 6A.13 – Traceability policy and calibration records
- 6A.14 – Measurement uncertainty procedure
- 6A.15 – Final report template examples
- 6A.16 – Proficiency testing schedule and results

Ongoing Compliance

Once accredited, the laboratory will be required to complete internal quality audits every year, participate in external proficiency testing programs (such as the NIST OSAC PT programs or Collaborative Testing Services digital forensics tests), take any corrective actions required as a result of any audit findings, and have a re-accreditation assessment every two years. The Manager of the laboratory will be the Quality Assurance Liaison responsible for maintaining the QMS.

Section 4: Laboratory Maintenance Plan

The maintenance plan ensures that all hardware and software is maintained in an operational state as required by both ISO/IEC 17025:2017 Section 6.4 (Equipment) and to ensure the integrity of the chain of custody of the digital evidence.

Hardware Maintenance

All hardware assets are tracked in the Lab Equipment Register. The Lab Manager maintains this register and it includes information about the manufacturer of the equipment, the manufacturer's model number for that piece of equipment, the serial number for that model, the date of when the equipment was acquired by the laboratory, and the calibration and maintenance history for that equipment.

Preventive Maintenance Schedule:

Equipment	Frequency	Maintenance Actions
Forensic Workstations	Monthly	Dust interior, verify hardware integrity, run diagnostics, confirm write-blocker function with test disk
Write Blockers (Tableau, hardware)	Quarterly	Validate with known-good test disk; verify hash output matches expected values; calibration certificate renewed annually
Forensic Imagers (Logicube, Tableau TX1)	Quarterly	Test imaging with reference media; verify MDS/SHA-1 hash match; firmware updates per manufacturer guidance
Evidence Storage Lockers	Monthly	Inspect locking mechanisms; verify chain-of-custody seal integrity; check temperature/humidity logs
NAS Storage Array	Monthly	RAID health check; review disk SMART data; verify backup integrity and restore test quarterly
PIV Card Readers / Access Control	Quarterly	Test all credentials; audit access logs; replace batteries in backup systems
UPS Battery Backup	Semi-annually	Self-test cycle; battery replacement per manufacturer schedule (typically 3–5 years)
Cellebrite UFED Hardware	Per manufacturer	Firmware and software updates; test with known device images; calibration per UFED documentation
Security Cameras / NVR	Quarterly	Verify recording function and retention; clean lenses; confirm timestamps are accurate

Software Maintenance

All forensic software licenses are tracked in the Software License Register. Software is maintained on air-gapped workstations. All updates are tested on non-case evaluation systems before being deployed to production systems.

- Commercial tools (AXIOM, FTK, EnCase, Cellebrite): Updates are installed within 30 days of vendor release date following validation testing. Vendor license renewals are tracked 60 days in advance of license expiration dates.
- All software updates and additions must be tested for functionality using the validation images prior to being permitted to support any forensic investigations. The results of such tests are logged in the Tool Validation Log.

- Open-source software (Autopsy, Volatility, Wireshark): These tools are reviewed on a monthly basis. The version of these tools installed on the forensic lab workstations will remain the same until the next release of the open-source software is validated.
- Operating Systems: The Windows 10 LTSC operating system receives security patches every month through the WSUS server in an isolated network update environment. Upgrading to a newer version of the operating system requires a full system validation process.
- Anti-malware software (non-casework machines only): Installed daily on non-casework machines through the enterprise anti-malware solution. The forensic analysis workstations do not have anti-malware software installed to avoid the modification of evidence artifacts.

Calibration

All instruments that can have a direct effect upon the validity of the examinations (write-blockers, forensic imagers) will be calibrated to NIST standards. The calibration records will be maintained for a minimum of five years. Calibration of all primary forensic examination instruments will occur every 12 months, unless the manufacturer specifies otherwise.

Malfunctioning Equipment Protocol

Equipment that produces suspect results, fails a calibration check, or has been mishandled must be immediately removed from service and labeled 'OUT OF SERVICE – DO NOT USE.' All cases examined on the affected equipment during the potentially compromised period must be reviewed. The incident is documented in the Equipment Incident Log and the Quality Assurance Liaison is notified within 24 hours.

Three-Year Technology Refresh

To maintain technical currency, the lab will conduct a formal technology review at the 36-month mark. Analysis workstations will be evaluated for replacement or RAM/storage upgrades. Forensic imaging hardware has a typical lifecycle of 5–7 years; software licensing will be renegotiated based on caseload data.

Section 5: Staffing Plan

The Digital Forensics Laboratory will initially be staffed with two (2) positions: a Lab Manager and a Digital Forensics Examiner (Technician). Furthermore, should the caseload justify the additional staffing, a second Examiner position will be requested for Year 2 of the budget cycle. Each of the following job descriptions were developed according to the NICE Cybersecurity Workforce Framework and the ANAB requirements for staff competencies.

Position 1: Digital Forensics Lab Manager

Category	Details
Job Title	Digital Forensics Lab Manager
Classification	Civilian Law Enforcement – Forensic Science Specialist, Grade FS-III
Salary Range	$85,000 – $110,000 (commensurate with certifications and experience)
Reports To	Chief of Police / Criminal Investigations Commander
Primary Responsibilities	Oversee the Digital Forensics Laboratory and all of its operations. Ensure that the Laboratory meets its accreditation requirements. Assign and review the caseload for each technician in the Laboratory. Ensure the chain of custody of all digital evidence. Serve as the expert witness for digital investigations in court. Maintain a register of all Digital Forensics Laboratory equipment and software licenses. Prepare an annual budget for the Digital Forensics Laboratory. Work with the ANAB assessors and other law enforcement agencies regarding Digital Forensics Laboratory operations.
Required Education	Bachelor's degree in Computer Science, Digital Forensics, Cybersecurity, Information Technology, or related field. Master's degree preferred.
Required Experience	Five (5) years of experience in digital forensics investigations; two (2) years in a supervisory role is required.
Required Certifications	At least two of the following: EnCE, GCFE, GCFA, CFCE, CCE. ISO 17025 Lead Auditor certification is preferred.
Technical Skills	Proficiency with FTK, EnCase, Magnet AXIOM, Autopsy, Cellebrite UFED devices. Knowledge of Windows, Linux, macOS, iOS, and Android devices is required.
Other Requirements	Must pass background investigation; must be eligible for a Secret-level security clearance. Must possess a valid driver’s license; must be willing to serve as an expert witness in court.

Position 2: Digital Forensics Examiner (Technician)

Category	Details
Job Title	Digital Forensics Examiner
Classification	Civilian Law Enforcement – Forensic Science Specialist, Grade FS-II
Salary Range	$58,000 – $80,000 (commensurate with certifications and experience)
Reports To	Digital Forensics Lab Manager
Primary Responsibilities	Perform digital forensic acquisitions of digital devices under the supervision of the Lab Manager. Image the hard drives of computers, mobile devices, and removable media. Perform digital forensic analyses using approved digital

Category	Details
	forensic analysis software. Document digital investigations and prepare reports of the investigations. Ensure the chain of custody of digital devices assigned to the Examiner. Participate in proficiency testing and training to improve digital investigation techniques.
Required Education	Associate's degree minimum in Computer Science, Cybersecurity, or Digital Forensics. Bachelor's degree preferred.
Required Experience	Minimum two (2) years of experience in digital forensics, information security, or related field; law enforcement experience is preferred. Experience with digital evidence and chain of custody is required.
Required Certifications	At least one of the following: CFCE, CCE, A+ or Security+ certifications from CompTIA, the CHFI from EC-Council, or the MCFE from Magnet Forensics. The Cellebrite Certified Operator certification is preferred for mobile device investigations.
Technical Skills	Must have a working knowledge of digital forensic investigations software platforms, such as FTK, EnCase, or AXIOM. Experience with write-blocking and forensic imaging standards (NIST SP 800-86) is required. Some knowledge of digital devices, operating systems and file systems is required (Windows, macOS, Linux, iOS, Android; FAT32, NTFS, ext4, APFS; Registry and browser artifact analysis).
Other Requirements	Must pass background investigation; no felony convictions; must have a valid driver's license; must be able to lift and transport digital devices up to 50 lbs; must complete sensitivity training for sworn law enforcement officials within the first six (6) months of employment.

Year 2 Staffing Expansion

According to projections of the growth of the digital investigations caseload for the Police Department, a second examiner is to be requested for Year 2 of the budget cycle. The second examiner will specialize in mobile device and cloud-based digital forensic investigations.

Training & Professional Development

All personnel in the Digital Forensics Laboratory are required to complete at minimum 40 hours of continuing education each year. Approved courses include those offered by SANS FOR, Cellebrite Training Academy, HTCIA, IACIS, and various vendors that offer certification courses for digital forensic investigations software platforms. The training records for each digital forensic investigator will be maintained in the files of the Lab Manager and reviewed during the annual ANAB surveillance of the Police Department.

Bibliography

ANSI-ASQ National Accreditation Board (ANAB). (2024). Forensic science testing and calibration laboratories accreditation. https://www.anab.org/forensic-accreditation

American Society of Crime Laboratory Directors (ASCLD). (2024). Accreditation initiative. https://www.ascld.org/about-us/accreditation-initiative/

Cellebrite. (2024). UFED Touch 2 product overview. https://www.cellebrite.com/en/ufed/

International Organization for Standardization. (2017). ISO/IEC 17025:2017 – General requirements for the competence of testing and calibration laboratories. https://www.iso.org/standard/66912.html

Magnet Forensics. (2024). Magnet AXIOM product overview. https://www.magnetforensics.com/products/magnet-axiom/

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

National Commission on Forensic Science. (2016). Uniform language for testimony and reports for the forensic document examination discipline. U.S. Department of Justice. https://www.justice.gov/archives/ncfs/file/839701/download

Organization of Scientific Area Committees for Forensic Science (OSAC). (2024). Digital evidence subcommittee. National Institute of Standards and Technology. https://www.nist.gov/osac/digital-evidence

Sammons, J. (2012). The basics of digital forensics: The primer for getting started in digital forensics. Syngress/Elsevier.

Tableau Forensic. (2024). TX1 forensic imager product overview. https://www.opentext.com/products/tableau-forensic-imagers