CYSE 407 Midterm: Police Department Digital Forensic Lab Proposal

Hans Peterson

School of Cybersecurity, Old Dominion University

CYSE 407: Digital Forensics

Professor Bryan Bechard

December 5, 2025

Accreditation Plan

For a digital forensic laboratory to be capable of maintaining technical competence and reproducing reliable results, it must be certified by an accreditation body. This lab will conform to the standards set by ISO/IEC 17025:2017, and the ANSI National Crediting Board (ANAB) will be the accreditation body. For clarification, accreditation is "the procedure by which an authoritative body gives formal recognition that a lab is competent to carry out specified tasks," and an accreditation body is "an organization conducting and administering an accreditation system" (Scientific Working Group On Digital Evidence, 2017).

Self-assessment (of the laboratory) for conformity to ISO/IEC 17025:2017 should be conducted before seeking out the ANSI National Crediting Board for accreditation. Afterwards, evaluation of the level of current conformity to ISO/IEC 17025:2017 should be conducted. The ISO/IEC 17025:2017 is known as the *General Requirement for the Competence of Testing and Calibration Laboratories*; it is the international standard for all forensic laboratories, including digital forensic laboratories.

The ANSI National Crediting Board provides several steps for accreditation:

1. Quote
2. Application
3. Document Review
4. Accreditation Assessment
5. Corrective Action
6. Accreditation Decision
7. Surveillance and Reassessment

As part of the preparation of the assessment, this laboratory must ensure that it has met all accreditation requirements prior to the assessment. Additionally, three items must be in possession:

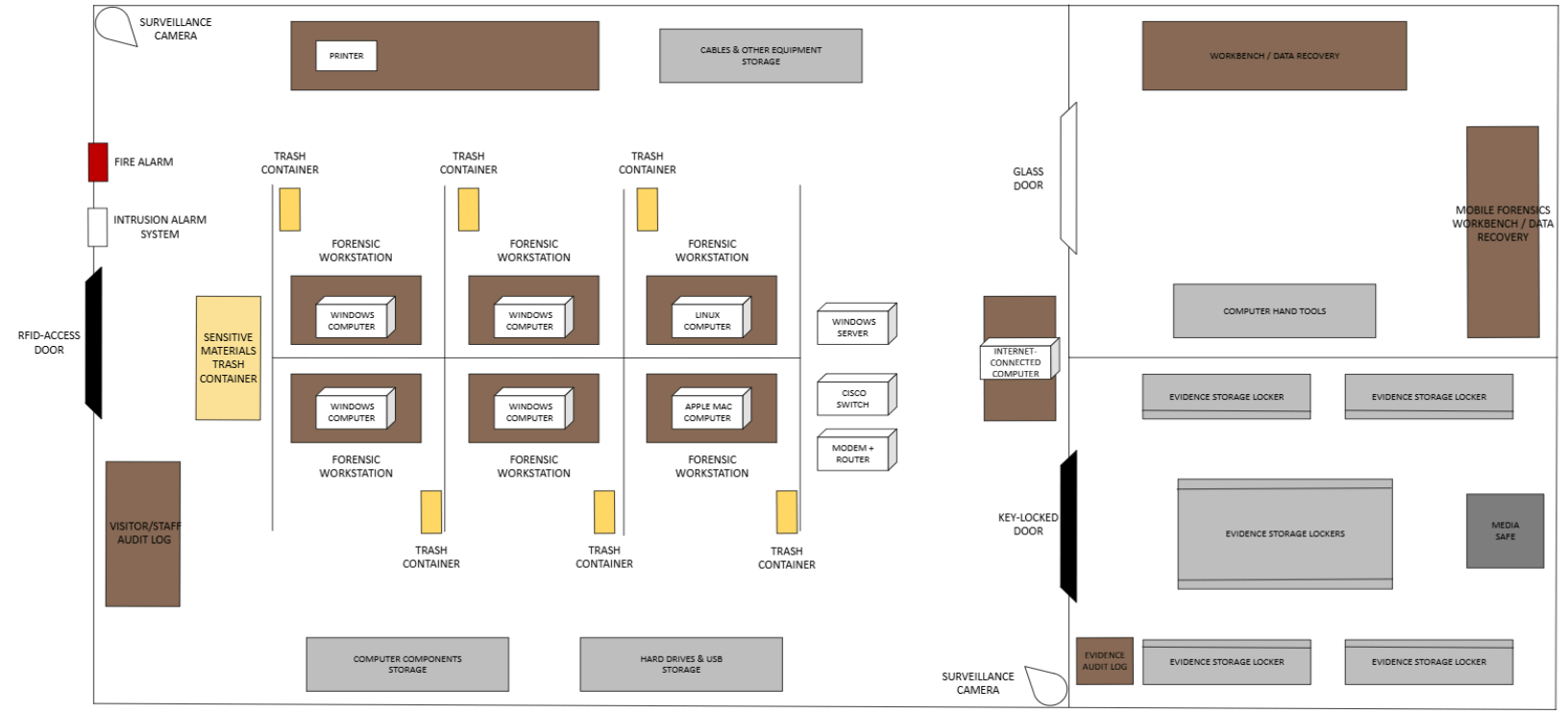
- Licensed Copy of ISO/IEC 17025:2017
- MA 3033 Accreditation Manual
- AR 3125

To certify ownership of a copy of the ISO/IEC standard, an FM 3058 form shall be completed and sent to QualityMatters@anab.org. Afterwards, there shall be an internal audit to ensure that the laboratory conforms to ISO/IEC 17025:2017. Corrective actions shall be applied to nonconformities identified in the audit. Once completed, a meeting with an assessment team may be scheduled.

There are specific requirements outlined by the ISO/IEC 17025:2017 that the laboratory must follow:

- General Requirements
- Structural Requirements
- Resource Requirements
- Process Requirements
- Management System Requirements

Floor Plan


SURVEILLANCE CAMERA
PRINTER
CABLES & OTHER EQUIPMENT STORAGE
WORKBENCH / DATA RECOVERY
FIRE ALARM
INTRUSION ALARM SYSTEM
TRASH CONTAINER
TRASH CONTAINER
TRASH CONTAINER
GLASS DOOR
MOBILE FORENSICS WORKBENCH / DATA RECOVERY
FORENSIC WORKSTATION
FORENSIC WORKSTATION
FORENSIC WORKSTATION
WINDOWS COMPUTER
WINDOWS COMPUTER
LINUX COMPUTER
WINDOWS SERVER
COMPUTER HAND TOOLS
RFID-ACCESS DOOR
SENSITIVE MATERIALS TRASH CONTAINER
INTERNET-CONNECTED COMPUTER
WINDOWS COMPUTER
WINDOWS COMPUTER
APPLE MAC COMPUTER
CISCO SWITCH
EVIDENCE STORAGE LOCKER
EVIDENCE STORAGE LOCKER
MODEM + ROUTER
FORENSIC WORKSTATION
FORENSIC WORKSTATION
FORENSIC WORKSTATION
VISITOR/STAFF AUDIT LOG
KEY-LOCKED DOOR
EVIDENCE STORAGE LOCKERS
MEDIA SAFE
TRASH CONTAINER
TRASH CONTAINER
TRASH CONTAINER
COMPUTER COMPONENTS STORAGE
HARD DRIVES & USB STORAGE
EVIDENCE AUDIT LOG
EVIDENCE STORAGE LOCKER
EVIDENCE STORAGE LOCKER
SURVEILLANCE CAMERA

Inventory

Hardware

ETEKJOY Electronic Door Lock (1) + RFID Keycards

BG-12 Series Fire Alarm Pull Station (1)

Amerex 322 Carbon Dioxide Fire Extinguisher (1)

ADT Burglar Intrusion System (1)

Ubiquiti G5 Dome Ultra Surveillance Cameras (2)

Ergonomic Chairs (9)

Work Desks (8)

Electronic Workbenches (2)

Small Table (1)

United Solutions Wastebaskets (6)

Trashcan With Soft-Foot Pedal (1)

Greenvelly Metal Storage Cabinets (4)

VitalValt Non-Pass-Thru Evidence Lockers With 10 Openings (6)

Sentry Fireproof and Waterproof Safe (1)

HP LaserJet Pro Printer (1)

Workstation Computers, Including Computer Components (GPU, CPU, RAM, Motherboard, Power Supply, NIC) (8)

Mice and Keyboard (8)

Cisco MS130-8X Switch (1)

SURFboard Cable Modem & Router Combo (1)

SATA Cables (15)

IDE Ribbon Cables (15)

USB-C Cables (5)

CAT6 Cables (15)

Logicube WriteProtect USB (1)

Logicube WriteProtect DESKTOP (1)

Logicube EchoPlus-NG Disk Duplicator (1)

HDMI Cables (5)

JTAG Cables (5)

Anti-Static Mats (5)

Anti-Static Gloves (2)

Milwaukee Screwdriver Set (1)

Tweezer Set (1)

Micro Wire Cutters (2)

Software

Windows 10/11

Windows Server 2019

macOS 15 Sequioa

Kali Linux

VMware

Oracle VirtualBox

Wireshark

Network Miner

Maltego

FTK Imager

Sleuth kit/Autopsy

ProDiscover Pro

EnCase Forensic Suite

MAGNET Ram Capture

Maintenance Plan

Policy/Documentation Audits

To maintain technical competency, internal audits, external audits, or inspections should be conducted every year or six months. More specifically, laboratory policies (e.g., safety procedures) and documentation management should be reviewed to ensure they are up to date and efficient. Furthermore, an accrediting body, such as ANAB, should perform external audits on the laboratory every six months if possible to ensure the laboratory is complying with ISO/IEC 17025:2017. Individual case files should be reviewed to ensure that SOPs are being followed, reporting is accurate, and evidence was properly handled (e.g., maintaining chain-of-custody).

Hardware and Software Equipment Audits

In addition to scheduled auditing, hardware and software should be maintained and, if necessary, updated to ensure they are reliable and accurate. Hardware and software should be regularly inspected and documented every week. The workstation computers within the laboratory should undergo hardware checks (e.g., benchmarking performance). Physical write-blockers and disk duplicators should be tested before usage. All forensic software should

be tested using a dummy/test hard drive before any case work. Upon updates to both hardware and software, their functionality should be validated and documented. If the updates to forensic software impact their performance, roll back to a previous version. If necessary, hardware, such as hand tools, printers, and computer components, should be replaced and documented every three to four years to maintain efficient performance. Additionally, every two or three months, schedule a cleaning crew to inspect, sanitize, and clean the laboratory. Ensure that they sign in on the visitor/staff audit log before allowing them to clean.

Security Audits

The manager of the secure evidence room should inspect the room to ensure lack of damage to the lockers and vault. Ensure that the lockers and vault close properly. Ensure that the RFID entrance door for the laboratory is locked and functions properly; test the RFID cards and document whoever holds them. Additionally, the functionality of the surveillance cameras should be verified to ensure that image/audio quality has not deteriorated. Ensure that blind spots have been minimized, firmware updates have been installed, and there are timestamps for all footage. Recordings/footage should be saved and kept for 30 to 90 days on cloud storage outside of access from the laboratory's physical space.

Lab Roles/Responsibilities

Digital Forensic Lab Manager

Description: Manages and oversees daily operations of the digital forensic laboratory while providing technical direction to technicians (ESSAE, 2023). Responsible for staff oversight, maintenance of accreditation (ISO/IEC 17025:2017), coordinating and scheduling

internal and external audits, ensuring SOPs comply with legal standards, and enforcing safety protocols.

Responsibilities/Tasks/Skills:

- Budget and manage fiscal needs of the laboratory to continue daily operations.
- Lead a team of digital forensic technicians and provide guidance/support while promoting cooperation and group consensus during major decision making.
- Schedule internal and external audits to assess/mitigate safety risks and to comply with ISO/IEC standards.
- Perform daily inspections on workstations, peripherals, and devices throughout the laboratory.
- Creates outlines of case management, evidence logging, and reporting guidelines for technicians.
- Creates safety policies for lab technicians, staff, and visitors.
- Monitors and documents staff performance/conduct for performance and any misuse of equipment.
- Train new technicians to perform their tasks and regularly review technician work.

Qualifications:

- Strong verbal and written communication skills.
- Strong interpersonal skills.
- Bachelor's or higher degree in the field of Computer Science, Cybersecurity, Criminal Justice, or Forensic Science.
- Minimum 3-6 years of experience within a laboratory setting.

- Minimum 2-4 years of experience in digital forensics as a lead/manager role.
- Knowledgeable and able to use Office 365 Suite (e.g., Word, Excel, Powerpoint).
- Knowledgeable on laboratory safety protocols and procedures.
- Experience coordinating with accrediting bodies such as ANAB
- Familiar with forensic tools such as EnCase, FTK, Autopsy, and ProDiscover.
- Knowledgeable in networks and network protocols.

Notable Certifications:

- CFCE (Certified Computer Forensic Examiner).
- CCFP (Certified Cyber Forensics Professional).
- CompTIA Security+, Network+, A+.
- CISSP (Certified Information Systems Security Professional)

Digital Forensic Lab Technician/Analyst

Description: Responsible for handling/working on digital forensic casework and ensuring proper evidence intake, imaging, storage, and tracking while complying with standards (ISO/IEC 17025:2017). Assists in peer casework preparation and calibrates/maintains digital forensic software when necessary. Analyzes digital forensic casework and reports/documents results to the lab manager. Can work both on-the-field and in a laboratory setting.

Responsibilities/Tasks/Skills:

- Receive, analyze, and extensively report digital evidence (e.g. computers, laptops, mobile devices, and legacy devices) while adhering to ISO/IEC 17025:2017 standards.

- Comply with Federal Rules of Evidence or state rules of evidence while performing digital forensic analysis.
- Ensure chain of custody for evidence is documented.
- Collaborate with other peers/technicians on large casework.
- Verify the integrity of copied digital evidence (e.g., SSDs, HDDs).
- Maintain cleanliness of workstation and other equipment.
- Properly transport, store, and retrieve digital evidence.
- Identify and report non-comformities with ISO/IEC 17025:2016.

Qualifications:

- Strong interpersonal and communication (verbal and written) skills.
- Able to work with groups, possesses a strong work ethic, and is open to collaborate.
- Bachelor's or higher degree in the field of Computer Science, Cybersecurity, Criminal Justice, or Forensic Science.
- Minimum 1-2 years of experience within a laboratory setting.
- Minimum 2-4 of experience with digital forensics, including data analysis and extensive reporting.
- Knowledgeable on chain of custody documentation, Federal Rules of Evidence or other equivalent rules of evidence, and ISO/IEC 17025:2017 standards.
- Possess strong analytical skills and is meticulous in their work.
- Strong reporting/documentation skills on digital forensic casework.
- High familiarity with forensic tools (e.g., EnCase, FTK, Autopsy, and ProDiscover).

- High familiarity with networking tools (e.g., Wireshark, Nmap) and understands networks/networking protocols.
- Comfortable with hex-editors.
- Possess strong coding and scripting background in Python, C#, C++, Java, or Javascript.
- Knowledgeable on mobile forensics.

Notable Certifications:

- CFCE (Certified Computer Forensic Examiner).
- CCFP (Certified Cyber Forensics Professional).
- CompTIA Security+, Network+, A+.
- EnCE (EnCase Certified Examiner).
- ACE (AccessData Certified Examiner)
- CCO (Cellebrite Certified Operator)

Bibliography

ANAB. (November 21, 2024). *ACCREDITATION MANUAL FOR FORENSIC LABORATORIES, FORENSIC INSPECTION BODIES, AND PROPERTY AND EVIDENCE CONTROL UNITS*. https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=7183

ANAB. (February 1, 2023). *ACCREDITATION REQUIREMENTS FOR FORENSIC TESTING AND CALIBRATION (2023)*. https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=12371

ANAB. (n.d.). *Forensic Laboratory Accreditation | ISO/IEC 17025 | ANAB*. Https://Anab.ansi.org/. https://anab.ansi.org/accreditation/iso-iec-17025-forensic-testing-laboratory/

ESSAE. (2023). *Lab Manager (Laboratory Manager) Job Description (Updated 2023 With Example)*. Empire State Society of Association Executives. https://careers.essae.org/career/lab-manager-laboratory-manager/job-descriptions

General requirements for the competence of testing and calibration laboratories. (November, 2017). Retrieved September 28, 2025, from https://calibrationworld.net/wp-content/uploads/2024/04/ISO_IEC_17025_2017_.pdf

Scientific Working Group on Digital Evidence. (February 21, 2017). *Scientific Working Group on Digital Evidence SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs*. Retrieved September 28, 2025, from https://www.swgde.org/wp-content/uploads/2023/11/2017-02-21-SWGDE-Overview-of-the-Accreditation-Process-for-Digital-and-Multimedia-Forensic-Labs.pdf

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/B5%201-6%20%20Paper%201%20Practical%20Guideline%20for%20Digital%20Forensics%20Laboratory%20Accreditation%20(with%20author).pdf