Brandon Harris
CYSE407
5/25/20205

Smallville Police Department Computer Forensics Lab Plan

Summary

Establishing a fully operational and certified computer forensics lab for the Smallville police department will involve a comprehensive three-year accreditation plan that will achieve and maintain accreditation in accordance with nationally recognized forensic laboratory standards, ensuring the lab meets the highest levels of integrity and reliability. For the next three years, the Smallville police department's computer forensics lab will follow the guidelines and procedures set by the American Society of Crime Laboratory Directors (ASCLD) and the ANSI National Accreditation Board (ANAB). This also includes making sure the lab operations follow ISO/IEC 17025 standards for testing and calibration, which is the international standard for forensic lab competence. Year 1 will focus on creating a strong foundation for the lab by developing Standard Operating Procedures (SOP), hiring and training staff, creating chain-of-custody protocols for the collection and analysis of digital evidence, and creating quality assurance protocols so that evidence is checked for bias or if the evidence has followed standard operating procedures and has not been tampered with. In Year 2, the lab will undergo internal audits and do mock assessments to identify issues with operations, training, and violations of national and international standards. During this time, the necessary adjustments will be made to address any issues with policies and procedures that were found during the mock assessments. In Year 3, the lab will apply for accreditation and will undergo the required external audits, assessments, and address any problems found to receive full accreditation status. This plan will allow the lab to produce digital evidence that can be used in court, uphold public trust by ensuring a fair trial when digital evidence is presented, and support Smallville police department efforts when it comes to cases that require the need digital forensics expertise and skills.

Accreditation Plan

The purpose of this accreditation plan is to establish a structured timeline and standards based roadmap for achieving ISO/IEC 17025:2017 accreditation for the computer forensics laboratory within the Smallville department. Accreditation is what will allow the lab to operate and certify that the lab's techniques and personnel meet internationally and nationally recognized standards for handling of digital evidence. To make this multi-year process easier to understand and execute, the accreditation plan has been divided into three phases based on the year. Year 1 will be the foundation phase, Year 2 is the internal audit and analysis phase, and Year 3 is the accreditation phase. Each of these phases is laid out in a table format to provide a breakdown of what needs to be achieved, what actions are required within each year, and documentation that can work as a guide when completing the assigned task. Incorporating tables allows each year's milestones to be mapped directly to accreditation standards and resource planning, making the process understandable for both technical personnel and law enforcement leadership. This format can serve as a checklist in case the Smallville police department wants to fund an expansion of the lab or assist and provide expertise to another police department building a computer forensics lab once accreditation is achieved.

Year 1 Foundation Phase

Goal	Task	Job Responsible	Documentation	Result
Create SOPs	Create SOPs for collecting, analyzing, and handling digital evidence	Lab Manager and Forensics Quality Assurance Officer	ISO/IEC 17025 and ASCLD Guidelines ISO/IEC 27042	Established the first SOPs and set the standard for quality in the lab
Create Chain of Custody Procedures	Create evidence collection forms, create chain of custody protocols, and determine how nonrepudiation can be established for systems analyzing evidence	Lab Manager and Digital Forensics Analysts	DOJ Digital Evidence Guidelines ISO/IEC 27042	Creation of a secure evidence tracking system
Staff training and hiring Program	Hire and then train staff about ISO/IEC 17025, digital forensics in relation to law enforcement, tools, and ethics	Lab Manager and Human Resources	SANs Institute, EC-Council, internal digital forensics, and policy training	Staff will be qualified to collect and analyze digital evidence and produce a product that can be presented in court
Buy equipment and set up security	Buy evidence lockers and software, and Hardware tools for digital forensics, install PIN and card access readers and security cameras, and workstations	IT team, Lab Manager, Department's Physical Security Team	ISO/IEC 17025, access control policy, and the Police department's physical security requirements	The lab is established and physically secured, and analysts have a place to work
Create a quality assurance and maintenance program	Create a maintenance plan for the tools so they can be calibrated, and establish policies for consistent evidence report quality	Forensics quality assurance officer	ISO/IEC 17025 ANAB AR 3125 ISO 19011:2018 ISO/IEC 27042	A quality assurance plan is created so that tools and final evidence reports are of the best and consistent quality

Year 2 Internal Audit and Analysis phase

Goal	Task	Job Responsible	Documentation	Result
Do internal audits	Review SOPs, ISO standards that relate to digital forensics, and documentation	Forensic quality assurance officer	ISO/IEC 17025 ISO 19011:2018 ISO/IEC 27042	An internal Audit report that can be reviewed
Determine what requirements need to be met	Identify gaps in policies, and if any standards still need to be met	Lab Manger Forensic quality assurance officer	ISO/IEC 17025 ANAB AR 3125 ASCLD Guidelines ISO 19011:2018	A plan that addresses the gaps in policy and procedures
Update SOPs and the Quality Assurance program	Look over the operating procedures based on the results of the audit	Forensic quality assurance officer	ISO/IEC 17025 ANAB AR 3125 ASCLD Guidelines ISO 19011:2018	New standard operating procedures that follow recognized standards
Conduct Mock Audit	Find a consultant to do a mock audit or simulate an ANAB audit	External consultant and Lab manager	ISO/IEC 17025 ANAB AR 3125	Provides a checklist of what is being done correctly and if the lab is ready for the real audit
Test Analyst in proficiency in digital forensics	Test your analyst's knowledge to determine if they are prepared to analyze evidence or need more training	Digital Forensics analysts	SANs, EC-Council, IACIS	Determine the skill level of the Digital Forensics Analyst and identify any gaps in training that can be addressed.
Review Infrastructure and software/Hardware	Find out if the lab has all the necessary hardware and software to complete their jobs, and if physical security measures are installed	Lab Manager, IT team, Department's physical security team	Inventory documents	Determined if any equipment is needed and reviewed the inventory list and documents

Year 3 Accreditation Phase

Goal	Task	Job Responsible	Documentation	Result
Finalize policies	Review all Documents, SOPs, chain of custody policies, etc	Lab Manager, Forensic Quality Assurance Officer	ANAB Application Package	Have all necessary documents ready, such as employee certifications and the ANAB application package
Submit Application to ANAB	Fill out the application packet, and provide information that includes the lab type, scope capabilities, and contact information	Lab Manager	Forensics Draft scope of accreditation	The packet was submitted to ANAB
Audit done by ANAB	Assist the auditor with necessary access to hardware/software and rooms where evidence will be held	ANAB Auditors, Lab Manager	ISO/IEC 17025 Clauses 7 and 8	The Audit Report was generated
Fix any Issues found during the audit	Take corrective action to fix any issues found from the audit, and submit what actions have been taken to fix the issues, if necessary	Lab Manager, Forensics quality assurance officer	A report that details corrective actions needed, if determined by the auditor.	Corrective actions were implemented to ANAB standards
Achieve Accreditation	Receive the Accreditation from ANAB	ANAB	Accreditation Certificate	The lab is now ready to collect and analyze digital evidence
Notify the public and partner agencies	Post the certification on your website, social media platforms, and notify partner agencies of your accreditation	Lab Manager, Department of Public Relations team	Announcement created by the public relations team	Made the public aware that if a crime involves digital evidence, Smallville PD will solve it.

Inventory

Software

Forensic Imaging Tools	EnCase, FTK Imager, Autopsy
Mobile Forensics	Magnet AXIOM, Cellebrite UFED
Network Analysis	Wireshark, Zeek/BRO
Memory Analysis	Volatility
Malware Analysis tools	IDA PRO, Ghidra, PE-Check, Floss, Capa, PEStudio
Virtualization Tools	VMware Workstation, VirtualBox
Log Analysis Tools	Splunk, Elastic
Operating systems	Windows, Kali Linux, Linux, Red Hat, SIFT Workstation
Other	Eric Zimmerman Tool Kit, Hashcat

Hardware

Forensic Workstations (x4)	Windows OS i9/Intel Core processor,128GB RAM, 2TB SSD
Write Blockers	T7u Tableau Forensic
Memory Card Readers(x24)	UltraBlock Card Reader
Printer (x4)	Epson WorkForce WF-2950
Evidence Storage locker(x24)	Spacesaver evidence storage locker
Camera(x4)	CCTV cameras
Solder Kit(x4)	120 v Soldering Station
USBs(x48)	Seagate Expansion USB 2TB storage
External Hard drives(x48)	Seagate Expansion 20TB HHDs
Chairs(x4)	Office Chair
Digital Camers(x8)	Cannon Mirroless Camera
Work phones(x8)	Iphone 14 Pro Max
Laptops	Windows OS i9/Intel Core processor, 64GB RAM, 1TB SSD

Supplies

Evidence Tape
Evidence Bags and Boxes
Label
Gloves
CDs

Expo Markers, pen, pencil, paper
Notebooks
cleaning wipes and blood cleaning chemical
Binders
Masks

Maintenance Plan

Maintaining an accredited computer forensics lab involves more than just analyzing and collecting digital evidence. It requires a well documented maintenance plan to ensure technical accuracy and compliance with both legal and industry laws and regulations. The maintenance plan will include forensic hardware and software upkeep, environmental and physical security controls, restocking supplies, and fixing equipment. The plan will outline the lab's maintenance activities across weekly, monthly, quarterly, and annual periods.

Weekly maintenance begins with the digital forensics analyst physically inspecting and cleaning all forensic workstations and digital devices. This will get rid of any dust or dirt that accumulates over time and damage the hardware, and prevent stable connections for devices such as write blockers and evidence acquisition tools. The analyst will also check each system for abnormal behavior, such as system errors or hardware alerts, and fix it if possible by working with the IT team. Logs from the systems that host the forensic applications, for example, EnCase and FTK Imager, are required to be reviewed for anomalies or signs of misuse. This will be done in conjunction with the IT team and the digital forensic analyst. Security camera footage covering the evidence storage area and workstation areas must be reviewed for any signs of tampering or unauthorized access. This will be handled by the physical security team of the Smallville police department. The lab manager and the Digital forensics analyst will review the Chain-of-custody logs for any incoming or outgoing evidence for accuracy and to maintain legal admissibility.

Monthly tasks will require the IT team of the Smallville police department to apply critical and non-critical software updates and patches to forensic software and operating systems so digital forensic analysts can use any new features or tools that come with updates and keep their system protected from vulnerabilities that can be compromised by hackers. The lab manager and the IT team will also test licensing to make sure that the digital forensics analysts have the right access to the tools necessary for their jobs. Hardware that is damaged will be replaced or sent to the IT team to be repaired. Lab equipment such as gloves, evidence labels, chain of custody forms, portable hard drives, and USBs will be inventoried and replenished as needed. The lab manager will also be required to work with the IT team to back up all case-related data onto a secure system. System backups will preserve critical data in the event of malware infection, system failure, or natural disaster. All backups will be checked for integrity by using hashing to confirm that the data remains unchanged.

Quarterly maintenance involves an in-depth technical and procedural review. The lab manager and the Forensics Quality Assurance Officer will perform a thorough audit of the chain-of-custody documentation to confirm that all entries match physical evidence and inventory. Any issues found must be investigated and resolved immediately, and all staff will be required to attend a lesson learned meeting if procedural failures are found and undergo additional training to prevent similar incidents. The lab's physical security system, which includes door sensors, card and PIN access pads, and CCTV cameras, will be tested to verify that they’re working and that CCTV camera footage has been saved for the last 720 days. The Forensics Quality Assurance Officer and the Lab manager will conduct mock scenarios meant to test how the Digital Forensics Analysts perform imaging, analysis, reporting, and storing of digital evidence, to make sure that the staff remain proficient in tool usage and are following the proper procedures.

Annually, the lab will undergo a comprehensive review. Forensic hardware tools will be sent for calibration or tested against manufacturer standards to ensure they are not modifying data during evidence acquisition. This will be coordinated by the Lab manager and the Forensic Quality Assurance Officer. Forensic imaging software will be validated using test images to confirm its integrity, and this will be the responsibility of the Digital Forensic Analysts. The lab’s Standard Operating Procedures will be reviewed and updated by the Lab Manager to align with evolving best practices and legal precedents. A full risk assessment will also be conducted by the Forensics Quality Assurance Officer to identify any problems within the infrastructure, supply chain, and personnel management. To maintain accreditation, the Forencis Quality Assurance Officer will schedule an external auditor for inspection per the guidelines of ISO/IEC 17025. Staff qualifications and documentation will be prepared and reviewed in advance by the Lab manager in order for the lab to pass inspection. This maintenance plan is required for the lab to remain operational and have the ability to handle sensitive and time-critical investigations. Following this plan will keep the lab in line with national and international digital forensic standards.

Job Roles

Lab Manager

The Lab Manager will be responsible for the computer forensics lab operations, which include personnel, budgeting, case management, and compliance with national and international accreditation standards. The Lab manager will oversee all evidence handling and security procedures to align with legal requirements.

Responsibilities

- Supervise and assign forensics cases to analysts
- Document chain of custody procedures and manage evidence collection and analysis
- Keep the lab ISO/IEC 17025 certified and in compliance with the DOJ Digital Evidence Guidelines, and ISO/IEC 27042
- Provide training and assist in career development for lab personnel
- Track forensics hardware and software inventory
- Create standard operating procedures
- Serve as the point of contact between law enforcement and different legal teams

Qualifications

- Bachelor's degree in computer science, digital forensics, or related field
- 7+ years of experience in a computer forensics lab or similar environment
- 3+ years of managing a team of 4 or more in a supervisor role
- In-depth knowledge of forensic tools such as FTK-Imager, write blockers, Wireshark, Volatility, SIFT workstation, and Cellebrite UFED.
- Certified Information Systems Security Professional (CISSP)

Preferred qualifications

- GIAC Certified Forensic Analyst (GCFA)
- GIAC Battlefield Forensics and Acquisitions (GBFA)

Salary $110,000 to $170,000 based on years of experience and certifications

Digital Forensics Analyst

The digital forensics analyst will be responsible for the collection and analysis of digital evidence to support a wide range of criminal investigations that include data breaches, terrorism, murders, and abuse. The digital forensics analysts will use a variety of forensics tools to analyze cell phones, computer systems, and storage devices.

Responsibilities

- Acquire forensics images from Windows, Linux, MAC, and mobile devices
- Analyze systems for criminal activity
- Create detailed forensic reports that can be used in court
- Document all evidence in chain of custody forms
- Act as an expert witness and be able to explain findings and the steps you took to collect and discover the evidence if necessary
- Maintain all software and hardware, and clean forensics workstations

Qualifications

- Bachelor's degree in computer science, digital forensics, or related field
- 1 to 3+ years of digital forensics experience
- Experience with forensics tools such as FTK-Imager, Autopsy, Magnet AXIOM, Volatility, Tableau write blocker, Encase, Cellebrite, IDA PRO, Ghidra, Wireshark, Splunk, or Elastic.
- Experience with Windows, Linux, and MAC operating systems
- In-depth knowledge of registry hives, system memory, and file systems(FAT32, NTFS), and Indicators of compromise (IOCs)
- Experience with Hardware analysis and External storage devices

Preferred qualifications

- Tool-specific certifications(EnCE, Cellebrite Certified Operator(CCO), FTK-Imager)
- GIAC IOS and MAC OS Examier (GIME)
- GIAC Advanced smartphone Forensics Certification (GASF)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Battlefield Forensics and Acquisitions (GBFA)
- GIAC Certified Forensic Analyst (GCFA)

Salary $70,000 to $130,000 based on years of experience and certifications

Forensics Quality Assurance Officer

The Forensic Quality Assurance Officer will be responsible for making sure that the lab's standard operating procedures, tools, and documentation comply with international and national laws, regulations, and standards. This role will also be responsible for assisting the lab manager in improving the standard operating procedure, and that all evidence collected is of consistent quality and presentable in court.

Responsibilities

- Establish and maintain a lab quality management system
- Ensure the Lab complies with ISO/IEC 17025, ASCLD, ISO 19011:2018, and DOJ Digital Evidence standards
- Conduct internal audits of all documentation, standard operating procedures, and the collection and analysis of evidence
- Implement corrective actions from external audits and inspections
- Prepare the Lab for accreditation assessments and accreditation renewal

Qualifications

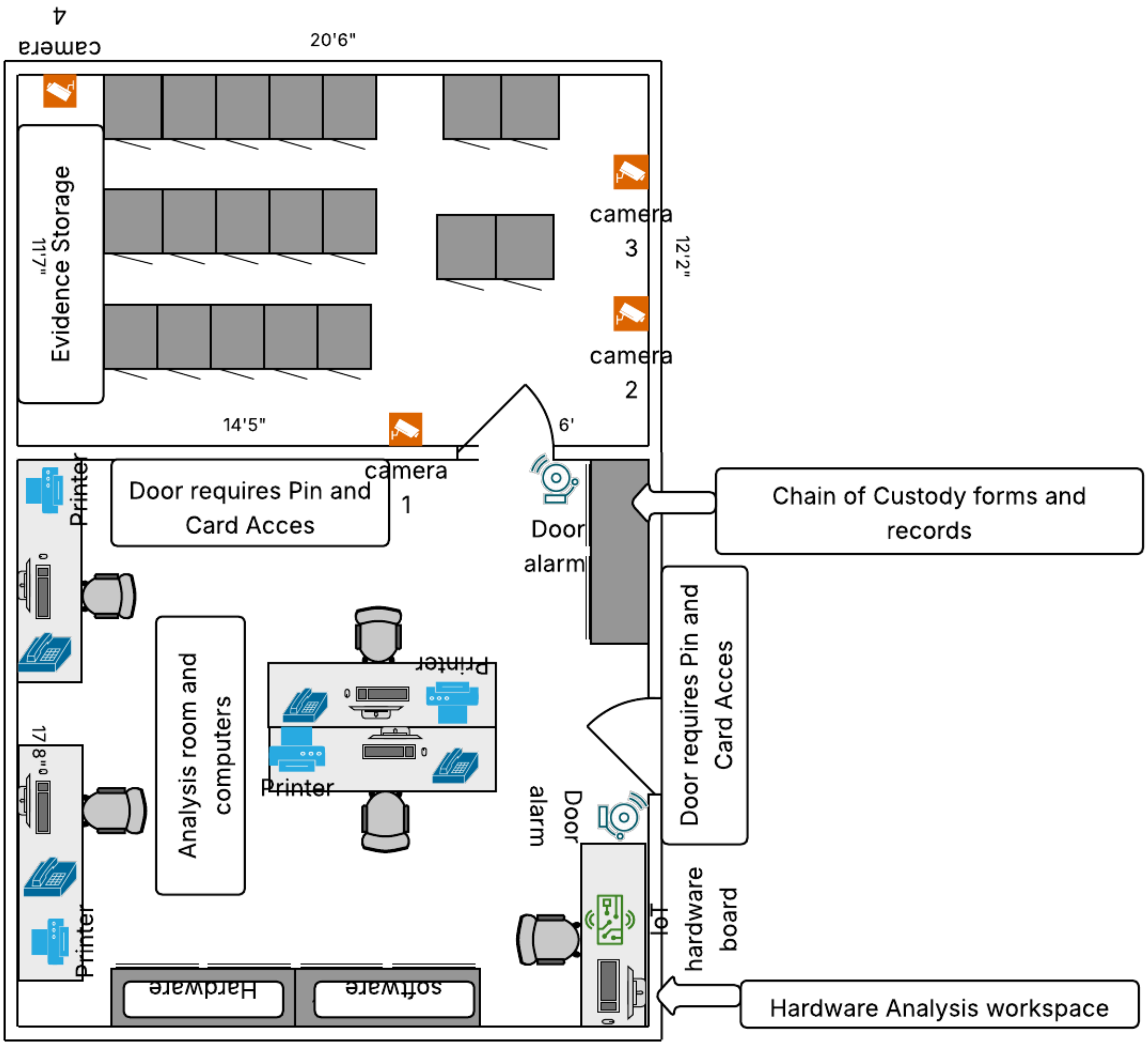
- Bachelor's degree in computer science, digital forensics, or related field
- 3+ years of experience in quality or information assurance
- Understanding of ISO/IEC 17025, ISO/IEC 27042, ISO/IEC 27040, and computer forensic laboratory standards.
- Knowledge how chain of custody procedures
- Experience in documentation and creation of standard operating procedures
- Ability to review evidence reports, if necessary to ensure quality

Preferred qualifications

- ISO/IEC 17025 Internal Auditor
- GIAC Certification Critical Controls Certification
- Certified Quality Auditor (CQA)
- Experience as a direct Foresnics lab auditor or quality assurance officer

Salary $66,000 to $144,000 based on years of experience and certifications

Floor Plan


camera 4
20'6"
Evidence Storage
11'7"
camera 3
12'2"
camera 2
14'5"
6'
camera 1
Door requires Pin and Card Acces
Printer
Door alarm
Chain of Custody forms and records
Analysis room and computers
Printer
Printer
Door alarm
Door requires Pin and Card Acces
17'8"
IoT
hardware board
Printer
Hardware
software
Hardware Analysis workspace

References

Alshebel, A. K. S. (2020). Standardization Requirements for Digital Forensic Laboratories: A Document Analysis and Guideline. *Auckland University of Technology* .https://openrepository.aut.ac.nz/server/api/core/bitstreams/7b32b78f-afce-4bb3-bc63-2a36489a226c/content

Bunting, S., & Wei, W. (2006). *EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide*. John Wiley & Sons.https://books.google.com/books?hl=en&lr=&id=V_XPRmaOH60C&oi=fnd&pg=PR8&dq=computer+forensics+lab+requirements&ots=1VfVx89Hd5&sig=1o65oaNJOrApjT2gpXzQOttlxpM

Cummins Flory, T. A. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law*, *11*(1), 4.https://commons.erau.edu/jdfsl/vol11/iss1/4/

Erbacher, R. F., & Swart, R. S. (2006). Computer forensics: training and education. In *Proceedings of the 5th Security Conference*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b5aeaf0dc731acf1a7b3a97e24374b3b85a27ea7

Grobler, M. (2010). *Digital forensic standards: International progress*. https://books.google.com/books?hl=en&lr=&id=RnzIAgAAQBAJ&oi=fnd&pg=PA261&dq=sans+digital+forensics+certification&ots=LDccGwXwZw&sig=vOOEeyGbRQ2Vr7Fxo-qUrFIAWzM

Jones, A., & Valli, C. (2011). *Building a digital forensic laboratory: Establishing and managing a successful facility*. Butterworth-Heinemann .https://books.google.com/books?hl=en&lr=&id=F5IU7XXKwCQC&oi=fnd&pg=PP1&dq=computer+forensics+lab+requirements&ots=7EXWWCRpJp&sig=gNtBmR0-PP6cz4nzLCdGZcDiMPo

Taylor, S., Rakof, A. M., & Talib, M. Z. A. (2021). Practical Guideline for Digital Forensics Laboratory Accreditation–A Case Study. *OIC-CERT Journal of Cyber Security*, *3*(1), 1-6.https://www.oic-cert.org/en/journal/vol-3-issue-1/practical-guideline-for-digital-forensic.html

Watson, D. L., & Jones, A. (2013). *Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements*. Newnes.https://books.google.com/books?hl=en&lr=&id=P0Hwx4F8Q7cC&oi=fnd&pg=PP1&dq=computer+forensics+lab+requirements&ots=hYvX8nbXEk&sig=FLYEQjCS8oeoa1fsR2CV_0nLO7E

Wolfe, T. (2025, January 13). *Lenny Zeltser*. SANS Institute. https://www.sans.org/blog/digital-forensics-salary-skills-and-career-path/