Midterm Paper

CYSE 407 – Digital Forensics

Natalie Hardwicke

Summary

The forthcoming Accreditation and Lab Maintenance Plan stands as the definitive strategic roadmap for the digital forensics' laboratory within the police department, charting a comprehensive course for the next three years. This multifaceted plan encompasses a detailed outline of imperative steps essential for accreditation, meticulous lab maintenance, and the unwavering adherence to established standards by all lab personnel. This plan should be reviewed and updated as necessary.

Accreditation Plan

To initiate the accreditation process for a digital forensic lab in accordance with the International Standard ISO/IEC 17025:2005, the lab must first submit an application for "General Requirements for the Competence of Testing and Calibration Laboratories." Additionally, they must furnish evidence of possessing this document before proceeding with the accreditation application. This plan will align with both the ANSI National Accreditation Board (ANAB) and ISO 17025:2005 standards for the accreditation process. The following steps outline the initial stages of the accreditation process and can be found on the ANAb site at https://anab.ansi.org/accreditation/iso-iec-17025-testing-laboratory-accreditation/:

1. Request a quote. Fees are associated with becoming a certified body.
2. File an application. This will need to be filed on ANAB's EQM database at https://anab.jadian.com/.
3. Prepare for the accreditation assessment.
4. Submit any necessary documents for review.
5. Accreditation assessment performed.
6. Corrective action if required.
7. ANAB makes accreditation decision.
8. Receive the accreditation certificate.

To ensure the lab is ready to be ANAB certified, lab staff should be familiar with any requirements associated with the certification process. One way that staff can become familiar with requirements is to participate in training found at: https://anab.ansi.org/accreditation/iso-iec-17025-testing-laboratory-accreditation/.

This certification will need to be upheld annually at a minimum with an annual office and witness assessment/s with a complete reassessment required at the end of the accreditation cycle.

Necessary documentation that the lab will need to provide is as followed:

- Document and Record Control Procedure
- Quality Policy
- Training and Awareness Procedures
- Externally Provided Products and Services Procedures
- Equipment and Calibration Procedure
- Customer Service Procedure
- Test and Calibration Method Procedure
- Sampling Procedure
- Quality Assurance Procedure
- Handling of Laboratory Test or Calibration Items Procedure
- Corrective Action Procedure
- Testing Report Procedure
- Calibration Report and Certificate Requirements Procedure

Staffing

Digital Forensics Lab Manager: The Digital Forensics Lab Manager holds a range of vital responsibilities in maintaining and overseeing the operations of the digital forensics' lab within the Police Department. These responsibilities encompass establishing and managing processes to effectively handle cases, conducting thorough reviews of cases and the work performed by lab technicians, and facilitating group discussions to reach consensus in the event of disputed findings. Lab technicians are expected to seek the lab manager's expertise for quality assurance and to guarantee adherence to proper procedures for evidence handling. Additionally, the lab manager is accountable for meticulous budget management for the fiscal year, ensuring that the lab technicians have access to the requisite hardware and software resources. The lab manager is also responsible for keeping both hardware and software up to date. Of paramount importance, the lab manager ensures that all lab work is completed promptly and with the utmost care, guaranteeing that all digital evidence is handled securely and in accordance with established protocols.

Requirements:

- Bachelor's Degree: A bachelor's degree in Computer Science, Digital Forensics, Cybersecurity, or a related field is typically required. Prefer candidates with a master's degree or higher in relevant fields.
- Certifications: Industry-recognized certifications in digital forensics, such as Certified Information Systems Security Professional (CISSP) or Certified Forensic Computer Examiner (CFCE).
- Experience: 5+ years of experience in digital forensics with at least 1 year of management experience.
- Digital Forensics Tools: Proficiency in the use of digital forensics tools and software, such as EnCase, FTK (Forensic Toolkit), X-Ways Forensics, and other industry-standard tools.

- Evidence Handling: A deep understanding of evidence handling procedures and maintaining the chain of custody to ensure the integrity of digital evidence.
- Computer and Network Knowledge: Comprehensive knowledge of computer hardware and software, operating systems, and network infrastructure to oversee forensic investigations effectively.
- Legal Expertise: Familiarity with legal procedures, regulations, and requirements related to digital evidence collection and presentation in court.
- Communication: Must have excellent written and verbal communication skills to documents findings, create and maintain procedures, and communicate to the team.

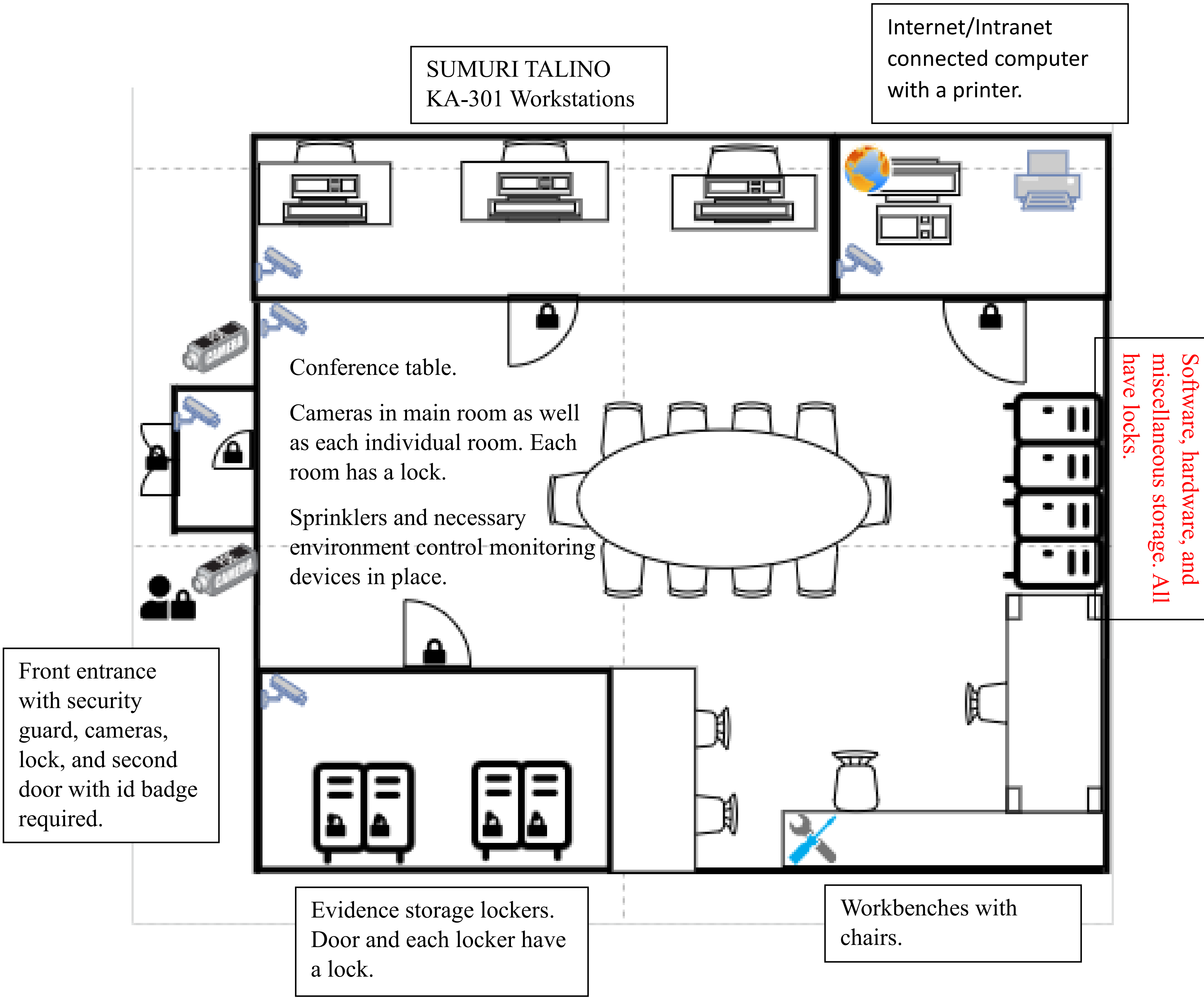
Digital Forensics Lab Technician: As a Digital Forensics Lab Technician at the Police Department, this role carries significant weight. The primary function revolves around the collection, scrutiny, and upkeep of digital evidence, alongside the meticulous management of technological tools. The primary duty of this role entails the acquisition, safeguarding, and thorough documentation of digital evidence, all conducted in strict compliance with established protocols and legal mandates. Furthermore, the Lab Technician will engage in comprehensive examinations of various digital devices, encompassing computers, smartphones, and storage media, with the objective of extracting, analyzing, and methodically cataloging digital data. In cases where data has been deleted or compromised, the Lab Technician's expertise will be leveraged to deploy specialized software and techniques to recover and reconstruct the information. The stringent maintenance of an impeccable chain of custody for all evidence remains an indispensable aspect of the Lab Technician's responsibilities. This involves vigilant record-keeping for every transfer and handling process, ensuring the utmost integrity of the evidence. Collaboration with fellow Lab Technicians is encouraged, with an active participation in group deliberations aimed at achieving a consensus when disputes arise. Staying attuned to the latest developments in digital forensic tools, software, and hardware is a crucial facet of the role. The Lab Technician's assistance will be sought in implementing these innovations as directed by the Lab Manager.

Requirements:

- Bachelor's Degree: A bachelor's degree in Computer Science, Digital Forensics, Cybersecurity, or a related field is typically required. May accept an associate degree with relevant experience.
- Certifications: Industry-recognized certifications are often preferred and can enhance your qualifications. Consider obtaining certifications like Certified Digital Forensics Examiner (CDFE), Certified Computer Examiner (CCE), or Certified Forensic Computer Examiner (CFCE).
- Digital Forensics Tools: Proficiency in using digital forensics tools and software such as EnCase, FTK (Forensic Toolkit), X-Ways Forensics, Autopsy, and open-source forensic tools.

- Data Recovery: Skill in data recovery techniques and tools to retrieve deleted or damaged files.
- Chain of Custody: Knowledge of maintaining and documenting the chain of custody to preserve the integrity of evidence.
- Computer and Network Knowledge: A deep understanding of computer hardware and software, operating systems, and network architecture is essential.
- Operating Systems: Proficiency in Windows, macOS, and Linux operating systems to conduct investigations on various platforms.
- Cybersecurity: Awareness of cybersecurity principles and an understanding of common attack vectors and security measures.
- Programming and Scripting: Familiarity with scripting languages like Python for automating tasks and analyzing data.

Forensic Laboratory Floor Plan



SUMURI TALINO KA-301 Workstations

Internet/Intranet connected computer with a printer.

Conference table.

Cameras in main room as well as each individual room. Each room has a lock.

Sprinklers and necessary environment control monitoring devices in place.

Software, hardware, and miscellaneous storage. All have locks.

Front entrance with security guard, cameras, lock, and second door with id badge required.

Evidence storage lockers. Door and each locker have a lock.

Workbenches with chairs.

Inventory

Hardware

Digital Camera for still and motion recording

Antistatic Bags

External CD/DVD Drive

External Hard Drives

40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster

Ribbon Cables for Floppy Disks

USB 3.0 or newer cables and SATA cards and associated cables

SCSI cards, some ultrawide

Graphic Cards (Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP))

FireWire and USB Adapters

Variety of USB Drives

Variety of Hard Drives

(2) 2.5-inch adapters from notebook IDE hard drives to standard IDE/ATA drives, SATA drives, etc.

IDE Cables

SATA Cables

CAT 6E Cables

Cable Tester

Hardware Tools: Phillips and Flathead Screwdriver, Hammer, Socket Wrench, etc.

Flashlight

Antistatic Wrist Wrap

Secure Storage Room

Spectrum Analyzer

Write Blockers

Computer Power Cables

(3) Industry Best Switches

(7) Computer Chairs

(2) Printers

(2) Workbenches

(3) SUMURI TALINO KA-301 Workstations

(1) Personal Computer with Internet/Intranet Access

Padlocks

(4) Evidence Containers

Software

Current and Legacy Versions of Microsoft OSs (At least Windows 10, 8.0 and 8.1, 7, Vista, XP, 2000, NT 4.0, NT 3.5, 9x, 3.11, and DOS 6.22)

Current and Legacy Versions of Macintosh OSs (MacOS, Mac OS X, 9.x, and 8 or older.)

Current and Legacy Versions of Linux Oss (Kali Linux, Linux Mint, DeftZ, Fedora, Ubuntu, Slackware, and Debian.)

Current and Older Versions of Microsoft Office

Hexadecimal Editor (Hex Workshop)

Programming Languages (Python, C, C++, Visual Studio, Perl)

Specialized Image Viewers (Quick View, ACDSee, ThumbsPlus, and IrfanView)

Accounting Application (QuickBooks)

Mobile Device Forensic Software (Oxygen Forensic Detective)

Video Conferencing Solution (Zoom)

Forensic Tools for Examination and Analysis (The Sleuth Kit, CAINE Linux, Maltego, and SIFT.)

Password Recovery and Data Decryption Tool (Passware Kit Ultimate and Paladin)

Antivirus Program (McAfee)

Open-Source File Viewers (Evince and Okular)

Memory Forensic Tools (Volatility)

Network Analysis Tool (Wireshark and Xplico)

Registry Analysis Tool (Registry Recon)

Maintenance Plan

The practices and guidelines described below ensure that the necessary maintenance routines are followed. This Maintenance Plan is an integral part of the digital forensics lab's operation. By adhering to these practices and guidelines, the lab ensures that evidence and data extracted from investigations maintain their accuracy, reliability, and repeatability, thereby upholding the highest standards of integrity and professionalism in the field of digital forensics.

Maintenance Practice Summary

The lab manager or individuals assigned by the lab manager will maintain a comprehensive record of all hardware, software, and other equipment that necessitates regular maintenance. Each piece of equipment must be appropriately labeled, and a record should be maintained, including information such as the equipment/software name, manufacturer's name, identification number, make/model, and any other pertinent details. The lab manager and the lab manager’s supervisor should conduct an annual review of lab maintenance practices to ensure adherence to the required protocols.

Hardware Maintenance

Regular inspections must be carried out on all hardware components, including but not limited to servers, forensic workstations, internet-connected devices, and storage devices. These devices should be scrutinized for any signs of wear and tear, loose connections, damage, or other issues that may impact test results.

To ensure the security and optimal performance of hardware devices, it is imperative that they have the latest firmware or updates. Daily checks for updates should be conducted, and a weekly review by the lab manager or a designated person is essential to guarantee that all hardware remains up to date.

Additionally, it is crucial to verify the compatibility of these devices with the forensic software used in the lab for testing purposes. This compatibility check should be a routine part of the maintenance process to ensure seamless integration and functionality during forensic examinations.

Regular performance assessments must be carried out to verify that the equipment is functioning as anticipated and to corroborate the accuracy of testing results and the handling of any evidence.

Software Maintenance

Any forensic software tools and operating systems should be updated to their latest versions to address security concerns and ensure the validity of tests performed with these tools. Before putting new versions into production, thorough testing in a controlled environment is essential to guarantee the accuracy and reliability of these updates.

Anti-virus and malware software must be employed to safeguard the lab environment from external threats that could compromise the validity of any evidence. Daily scans should be conducted to remove suspicious files and detect any unusual activity, while deep scans should be performed weekly to ensure comprehensive coverage.

The lab manager should hold, monitor, and manage software licenses to ensure compliance with all legal requirements. Regular reviews of licenses, at least monthly, should be conducted to stay current. A detailed record should be maintained, including information on all licenses, associated expenses, and expiration dates.

Confirmation of the operational effectiveness of forensic imaging and analysis tools should be achieved through the execution of test scenarios using known data. It is imperative to validate that these tools demonstrate precision and efficiency in handling diverse file types and storage media to ensure the accuracy of evidence and results.

Corrective Maintenance and Malfunction Equipment

Corrective lab maintenance within the domain of digital forensics encompasses the organized process of identifying and resolving issues that may manifest within the laboratory setting. When irregularities, malfunctions, or discrepancies surface in digital forensics tools, hardware, or software, established corrective maintenance procedures come into play. These procedures encompass the prompt reporting of issues, in-depth troubleshooting to discern the root cause, and the application of suitable solutions such as debugging, updates, or patches. The primary objective is to minimize operational downtime, guarantee the continual functionality of tools, and preserve the accuracy and reliability of forensic analyses. A continual monitoring system, timely interventions, and a comprehensive documentation framework constitute integral elements of an effective corrective lab maintenance, contributing to the overall efficiency and efficacy of the digital forensics investigative process. Regular assessments and refinements to the corrective maintenance protocols further bolster the lab's capability to address challenges promptly and uphold the integrity of digital evidence.

Any lab equipment that does not pass the corrective maintenance checks and cannot be recalibrated or fixed must be disposed of properly. All sensitive information or data must be wiped and disposed of following proper legal and environmental guidelines/laws.

Network Security

The lab should be equipped with a firewall, intrusion detection system (IDS), intrusion prevention system (IPS), and any other necessary network security perimeters. Firewall rules should undergo regular checks and updates, occurring no less than monthly, to fortify the security of the lab’s network. Daily inspections of the IPS and IDS are necessary, with any detected alerts promptly investigated to distinguish between real threats and false positives. In the event of a confirmed threat, appropriate measures should be taken to mitigate and contain the potential damage.

Access controls must be consistently checked, reviewed, and updated, at a minimum quarterly, and particularly when new staff is onboarded. Adherence to the principle of least privilege is imperative to ensure that employees are granted the minimum access required to perform their duties. Regular audits should be conducted to verify compliance with all security policies.

All equipment must be safeguarded against unauthorized changes or adjustments unless approved by the proper authority. This measure ensures the integrity and security of the lab's infrastructure.

Backup Schedule

The backup process should be completed regularly, and these schedules should be reviewed regularly to ensure that the most up to date data are accessible in the case of data loss or other issues. These backups should be tested and validated to ensure the functionality of these backups. The lab manager is responsible for ensuring backups are tested and performed regularly.

Reference Standards, Certified Reference Materials and Reference Materials

Reference standards serve as foundational benchmarks or models in digital forensics, providing a baseline for comparison. These may encompass standardized datasets, recognized signatures, or predefined configurations that act as a reference during investigations. Reference standards play a crucial role in identifying anomalies, assisting forensic analysts in evaluating whether the observed data conforms to established norms. Reference standards should always be used by analysts whenever possible.

Certified Reference Materials (CRMs), acknowledged for their accurately defined characteristics and certified precision by a reputable authority, stand as essential tools in digital forensics. Within this context, CRMs extend to software tools, hardware components, or datasets endowed with meticulously identified attributes. Their role is pivotal in establishing a uniform basis for calibration and quality control, ensuring the consistent and precise output of forensic instruments and methodologies. The lab will utilize the CRMs to help calibrate and ensure the accuracy of all lab equipment.

Reference materials, employed for comparative purposes, involve samples or datasets in digital forensics. Unlike CRMs, they may not carry formal certification attesting to their accuracy. Nonetheless, these materials play a crucial role as supportive tools in forensic analyses. Among them are samples acknowledged for their reliability, exemplars, or datasets used by analysts to validate their methodologies and findings against established standards. Reference materials may be used by lab analysts to help in their digital forensics' investigation.

NIST provides tools designed to assist forensic crime laboratories in validating their analytical methods and ensuring the precision of test results. NIST offers a selection of widely recognized Standard Reference Materials (SRMs), which serve as benchmarks for accuracy and reliability in forensic analyses. These SRMs play a crucial role in supporting laboratories by providing a standardized and reputable foundation for the validation and calibration of analytical methods, contributing to the overall quality and integrity of forensic testing outcomes. When possible, the lab will utilize NIST as a resource as well as any other nationally recognized standard.

Where possible, all findings done by analysts will be traceable unless there are extenuating circumstances. The lab manager or another technician must review the work of the analyst to ensure the quality assurance of all work.

References

https://advisera.com/17025academy/blog/2019/08/30/list-of-mandatory-documents-required-by-iso-170252017/

https://anab.ansi.org/accreditation/iso-iec-17025-testing-laboratory-accreditation/

How to Become an ANAB-Accredited Certification Body

Popular computer forensics top 19 tools [updated 2021] | Infosec

TALINO KA-301 Forensic Workstation : SUMURI

Cyber Lab Setup ~ Digital Forensic Lab Experts for Hardware, Software & Training

https://www.nist.gov/forensic-science/reference-materials-standards-and-guidelines/reference-materials-and-standards