Jesse Chin

CYSE 407

12/11/2022

Mid-Term: Computer Forensics Lab Set-Up

**Case** **Scenario**: You have been hired to create and run a brand-new digital forensics lab for a mid-sized police department. Your assignment is to come up with a plan for the lab for the next 3 years.

**Summary**: The following will summarize a general plan for the requirements needed for the creation, accreditation, physical set-up, hardware and software needs, for the computer forensics lab, which will specialize with digital and technological assistance as opposed to the police department’s forensics lab. The purpose of this report will not only specify the requirements that will be needed for the functionality of this lab but will serve as a frame of reference in comparison for the specific needs of this police department and its services.

**Accreditation**: Referencing the ANSI-ASQ National Accreditation Board (ANAB) website will assist in providing a framework for the steps needed towards accreditation of the lab. ISO 17025 is the accreditation needed for the foundational standard for forensics labs as its requirements are international standards as well states the technical competences. ISO 17025 can be compartmentalized into 5 categories: scope, normative references, terms and definitions, management requirements, technical terms. Each subsection will need to be considered and referred to as accreditation is being applied for and managed.

MA 3033, Accreditation Manual for Forensic Service Providers will be the reference guide in use during the accreditation process. Prior to the application process and assessment, a licensed copy of the ISO 17025 standard must be purchased, and an ISO/ IEC Document Ownership Certification Form (form ID FM 3058) must be submitted to the ANAB to notify ownership of certified copy of ISO. They are required to internally notate ownership in their systems. Once notified, the ANAB will provide an updated checklist needed for the ISO 17025 accreditation which will be used for reference going forward in conjunction with the MA 3033 manual. Scope of Accreditation will have needed to already be determined by this point as accreditation will be within specific fields of forensic standards. Forensic Draft Scope of Accreditation (document ID FA 3068) can be referred to for disciplines regarding scope; however, disciplines identified for the purpose of the digital forensic lab will fall within digital audio and imaging and first responders. FA 3068 can be used as a reference for internal use to identify generalized requirements for basic functionalities the lab will be expected to perform, although initial decision on scope of accreditation can be subject to change, allowed by the ANAB. A completed FA 3068 will be required to be submitted with the initial application as well as any re-assessments. Prior to submission of application, the ANAB should be contacted for a quote and breakdown of all expected fees. Once the checklist for the lab requirements have been verified by the forensics team and completed, all documents will be submitted for review. The ANAB will verify the completed documents. If approved, an on-site assessment will be scheduled with a designated ANAB assessment team based per the required needs of our lab. The lab director must be present with confirmed team members during on-site review.

The lab team members can be expected to explain their duties, the scope of their allowed responsibilities, knowledge: based on designated tasks, software, hardware, physical lab layout, and perform sample assessments designated by the ANAB team. Assessment will also include review of record documentation and organization, calibration and testing of all equipment, interviews, etc. The assessment leader will review results and provide a closing meeting report providing any assessment of non-conformance. In the event, a potential reassessment may be needed. Accreditation will pend on results and review of on-site assessment to assure compliance with ISO standards.

**\*Optional:** An on-site meeting can be requested with the ANAB, if needed, during the initial application process to ensure all required documents are notated, as well as to answer any pre-application questions. However, consultation of actual lab will NOT be allowed.



Figure : Process-flow for ANAB accreditation process.

Refer to: <https://anab.ansi.org/en/forensic-accreditation/iso-iec-17025-ar-3125-docs> for checklist pertaining to required and assistance documents for accreditation process.

**Sample Floor Plan:**



Figure : Sample Floor Plan

The above sample floor plan is a rough layout of the basic physical requirements the digital forensics lab will need to have in order to support the police department.

* A secure room with no windows and 2 exits located at the west and east walls.
* The main entrance on the bottom right will have a check-in desk for all authorized members (i.e., digital forensic team members) to scan in and out of or for outside members (i.e., officers, janitorial staff, etc.) to sign in and out of while entering.
* The circles by the exits represent security camera placement to ID faces when entering and exiting.
* The upper right corner will be the evidence locker room with a security door, containing at minimum 9-10 lock and key cabinets divided into sections per case allowing at least 2 cases to be entered for storage per locker and a security camera in the back wall.
* 2 work benches are located on the bottom left corner fitted with tools for hardware needs
* The bottom 2 desks will be internet/ intranet accessible PCs.
* 6 forensic work-stations cubicles are located along the west and north walls with dividers between each station to allow for privacy.
* A larger table located in the middle of the room for any important team meetings or department discussions.

The floor plan and physical layout will be subject to change depending on the capacity and growth of the police department over time.

**Inventory Requirements:**

|  |  |
| --- | --- |
| **Hardware**: | **Software**: |
| * Computer Chairs (8)
* Desk chairs (6-8)
* 2 work benches
* 9 computer desks
* 1 communal meeting table
* 9-10 combination or lock-key lockers
* Digital camera
* Anti-static mats
* Vinyl gloves (for antistatic use)
* Antistatic bags (varying sizes)
* External disk drive (depending on type of terminal used)
* 40-pin 18 in. and 36 in IDE cables, both ATA-33 and ATA- 100
* Ribbon cables
* Extra USB 3.0 cables (USB A/B/C adapters)
* Additional hard-drives and SSD
* Hand-tools for hardware (Phillips/ flat-head screwdriver, socket wrench, tweezers, plyers, screws
* Cable tester
* PCs with at least an intel I7 processor and accompanying monitors
* Various types of mobile devices (smartphones, tablets, etc.) on hand for reference and for spare parts.
 | * Copies of various operating systems (Windows 7, 8, 10, MacOS, X, Linux, Ubuntu, etc.)
* Wireshark, Nagios
* Kali Linux
* Autopsy, NetworkMiner
* Winhex
* VLC
* Virtual machine
* Anti-malware (ex: Norton 360)
* Quickbooks
* Microsoft Office
* Programming language for python, C++, etc.
* FTK Imager
* EnCase
* VPN (ex: pulse secure)
* ProDiscover
 |

* The above inventory is a rough suggestion based on the general needs of a forensics lab. Supporting a mid-size police department may require more hardware and software to better accommodate the specific needs of the department. Set-up of the hardware will be a collaborative endeavor between the forensics and IT teams of the police department and/or contracted 3rd parties per the discretion of the law enforcement agency.

**Maintenance**

Maintenance of the computer forensics lab will be a split responsibility between multiple parties depending on the need. However, forensics lab director will take full responsibility for quality and maintenance communication as per the facility’s needs. Should the director feel the need to delegate the responsibility of maintenance, they may appoint a quality assurance liaison at their discretion. The janitorial needs of the lab will be managed by the police departments janitorial staff (either hired in-house or contracted). They will use anti-static bags for disposal and utilize vinyl gloves while performing duties. Cleaning should take place, at minimum, 1 to 2 times per week to prevent and dust/dirt build up and prevent static. The calibration of equipment will depend on the policy allowed by the law enforcement agency as to whether they permit 3rd party vendors/contractors. ISO 17025 states that all equipment calibration procedures must be documented and available on-site of the facility. A record will be kept logging the date, time, and name of the individual completing the calibration per piece of equipment; however, calibrations are not to take place or occur outside of the recommended timeframe by the manufacturer. Handling of all equipment will require the use of gloves as well. All personnel will receive training on calibration procedures regarding the equipment per their specific function in the event the police department does not authorize a 3rd-party vendor; however, the lab director and quality assurance liaison will be responsible for understanding the procedures for all hardware and equipment. Software, operating system, and licensing updates will be managed by the police department’s IT team (or vendor permitted contractor), with all updates being logged for reference. Any and all issues with either hardware or software must be logged for auditing purposes. Any offsite requirements for repairs or consultation need to be notified and approved. Human resources will assist in communicating to employees of specific credentials/ certifications required for their continued employment under the forensics lab. The lab director and/or quality liaison will be responsible for managing the employees in their renewal or completion. Continued maintenance upgraded equipment, and proper upkeep of facilities will heavily depend on the funding made available for the department. Proper budget allocation and utilization will be reviewed by the lab director for continued maintenance.

**Staffing:**

Lab manager: The lab manager, or lab director, will have a number of responsibilities pertaining to the digital forensics team. While majority of the duties listed will fall under the lab managers responsibility, as previously stated, it will be up to their discretion on their need to delegate certain tasks (such as a quality insurance liaison for the lab). The lab manager will be responsible for creating, enforcing, and monitoring lab policies and procedures such as logging inventory, auditing, managing needs for calibration and updates on equipment/ software, etc. Per ISO standards, they must be written and accessible for all employees to view as needed. They will also be responsible for assigning cases to the staff and monitoring progress of all analysts and technicians by setting realistic expectations. In short, a lab manager will be responsible for the proper functionality of the digital forensics team.

Digital Forensics Analyst: An analyst can be responsible for analyzing log files, web traffic reports, etc. It is within their duties to run forensic software and collect information on devices that involve, encryption, malware, security configuration, intrusion, and so on. They will research what they can in terms of data collection and generate a report in an effort to contribute evidence to a case. Part of their skillset would include software knowledge, malware knowledge, data carving, forensic analysis, etc. It will not be uncommon for the analysts to work in teams, normally with 1 analyst taking charge as a lead investigator. The roll can also be referred to as a digital forensic technician; however, many technicians are referred to those who specialize in hardware. However, all members should have knowledge interchangeable between hardware and software.

First Responder: A first responder is usually one of the first few people allowed at the scene of a crime. This position can be filled with a digital forensics analyst or filled separately. The first responder will be responsible in coordinating with the officers on site to make sure the scene is not tampered with by unauthorized personnel. They will be responsible for gathering evidence in a safe and timely manner that does further jeopardize the equipment on site or potential digital evidence. They will be required to understand the importance of keeping a device alive or confirming/ preventing active remote sessions are taking place in order to prevent tampering of evidence. They will also be responsible for properly documenting the scene with as much detail as possible and determining all aspects pertaining to potential evidence. And most importantly, they will need to be able to demonstrate knowledge of how to organize, package, and transport all digital devices properly back to the lab for further analysis.

Citations:

*ANSI National Accreditation Board: ANAB*. ANAB/ANSI ISO Accreditation Solutions. (n.d.). Retrieved December 11, 2022, from https://anab.ansi.org/

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. (n.d.). *CISA CYBER DEFENSE FORENSIC ANAYLST*. CYBER DEFENSE FORENSICS ANAYLST. Retrieved December 11, 2022, from <https://www.cisa.gov/cyber-defense-forensics-analyst>

JACOBIA, J. A. C. K. (2004, April). *COMPUTER FORENSICS: DUTIES OF THE FIRST RESPONDER*. U.S. DEPARTMENT OF JUSTICE: OFFICE OF JUSTICE PROGRAMS. Retrieved December 11, 2022, from https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-forensics-duties-first-responder

Johnson, L. (2014). *Computer Incident Response and Forensics Team Management Conducting a Successful Incident Response*.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations: Processing digital evidence* (6th). CENGAGE LEARNING.

Watson, D., & Jones, A. (2013). *Digital Forensics Processing and Procedures [e-book] Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*.