Kris Vargas

CYSE 407

Midterm – Digital Forensics Lab Proposal

Summary:

As technology continues to advance rapidly, more and more crimes are committed in the digital realm that need to be accounted for. In doing so, assets such as digital forensics laboratories are becoming more and more valuable and important for police departments. Digital forensic labs exist in order to aid in the examining and analyzing of digital evidence for the purpose of collection, evidence preservation, and identification. In the following assignment, I will be detailing my plan for opening and implementing a digital forensics plan for a mid-sized police department. While the benefits of the lab will be immediate once it is set in motion, there is a lot of planning and prerequisites that must be met before the lab can even be built. In my three-year plan, I will cover a lab accreditation plan, an inventory (including both hardware and software), a lab maintenance plan, and staffing requirements/job descriptions of the workers that will be employed at the lab. Additionally, I will be including a diagram that will detail the physical layout of the laboratory, including physical security measures.

Accreditation Plan:

When attempting to start a digital forensics lab, the agency responsible must first undergo the steps required for accreditation. Accreditation serves to ensure that digital forensic labs conduct their activities in accordance with the internationally recognized industry standards and that they abide by the conformity expected of all labs.

Accrediting Body: For this particular lab, we will be abiding by the standards of the ANSI National Accreditation Board (ANAB) in order to gain the ISO/IEC 17025 Forensic Testing Laboratory Accreditation.

Pre-Application: Before we can even submit our application for our lab to be assessed, we must first ensure that our lab meets all of the applicable accreditation requirements. Any lab that is currently vying for ANAB-specific accreditation must first be in possession of the most current versions of these documents:

- A licensed copy of the international standard, which in this case is the ISO/IEC 17025 for testing/calibration
    - ISO standards can be purchased from national standards bodies, including ANSI (American National Standards Institute) or other authorized distributors found through the Internet
- A MA 3033 accreditation manual (which can be found on the ANAB website)
- Accreditation scheme requirements
- Application and draft scope documentation

Since this accreditation program includes an ISO/IEC standard, ANAB requires for the organization to certify that it has ownership of a licensed copy of the required standard by submitting an ISO/IEC Document Ownership Certification form to QualityMatters@anab.org. Once the certification form is verified and on file over at ANAB and the appropriate application fee has been paid, the organization will be given formal access to the accreditation tools offered by ANAB. This includes checklists that will ensure conformance with the application accreditation requirements.

***In addition to confirmed ownership of the required documents, all information regarding the required accreditation fees can be found through contacting ANAB at http://www.anab.org/lab-related-accreditation/request-for-quote.

Formal Application: A formal application for accreditation must be submitted for an initial assessment or reassessment of the organization's request for accreditation. This application and a draft scope of accreditation for the location of interest is to be submitted to QualityMatters@anab.org, and should be in English or Spanish and in an electronic format.

In the case that an organization submits an accreditation application but has not followed up by actively pursuing accreditation for the time period of one year, a new application and new application fees may have to be fulfilled.

Accreditation Decision:

All of the prerequisite actions and the formal application will undergo the scrutiny of a certified Accreditation manager and the actual accreditation decision will fall under the authority of the Vice President or designee. Accreditation will only be awarded to applicants that are found to be competent by the assessment team when considering all relevant information. If accreditation is successfully awarded, the laboratory/client will be provided with a Certificate of Accreditation and a Scope of Accreditation. The certificate itself will contain a unique certificate number and a date of expiration. The expiration date will allow for a formal time to be established for ANAB to perform conformance monitoring and reassessment of the laboratory in the future.

Laboratory Inventory:

To ensure that our digital forensics lab meets international standards and is able to carry out all of its necessary functions, the lab must be properly equipped with all of the assets that it needs to be successful. A multitude of different computer forensics tools must be accounted for, and the lab itself must be outfitted with certain physical components to make sure it can be inhabited as a workplace.

Hardware

Computer desk chairs (4)

Evidence Lockers/Containers (20)

Analysis Computers (4)

Computer Desks (4)

Computer Monitors (4)

HP Printers (2)

High-speed wireless router

Computer Hard Drives (storage unit)

Plastic static bags (storage unit)

Cartridges (for the printers)

PC components (appropriate cables, storage drives, fans)

Storage Room

Bulletin Board

A/C Unit

Software Locker

Printer Paper

File Cabinets (2)

Software

Kali Linux

Helix Pro

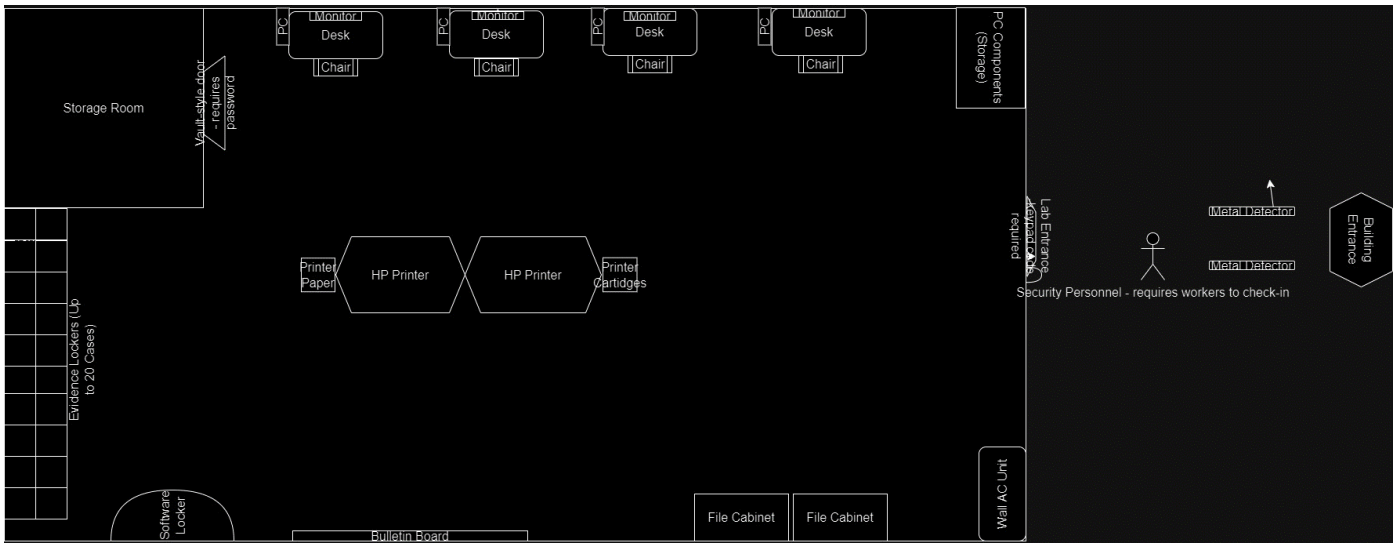
Wireshark

Autopsy/The Sleuth Kit

Volatility

Oxygen Forensic Detective

Laboratory Floor Plan



Lab Maintenance Plan

For a digital forensics lab to be performing at its best, all assets within the lab environment must be kept up to date. Thus, it is extremely important to regularly maintain and calibrate all hardware and software that is being actively utilized in the lab environment. This keeps all of the laboratory's assets running smoothly and can also serve to prevent more costly fees in the future in the forms of repairs or complete replacements. In order to simplify this complex

process, I have created a Lab Maintenance Plan that separates the care for the hardware and software, as they should be approached in different manners.

Hardware:

1) Assessment

   The first step for maintaining the hardware in the lab will be to take a detailed assessment of all of the hardware that is currently being utilized within the laboratory environment. Each relevant component will be accounted for from the all-encompassing inventory list, and then a file for each will be created that states the component's age, current condition, past issues or repairs, and any types of warranties that apply to the device.

2) Frequency of Maintenance Checks

   Maintenance checks on hardware will be routinely carried out once a month, this high frequency will be paramount in ensuring that any and all issues that must be resolved regarding the hardware will be properly addressed as swiftly as possible. This will aid the laboratory in being able to operate year-round and able to handle a heavy workload as far as total cases goes. (This will be applied over the three-year period that this lab is expected to operate, totaling 36 maintenance checks).

3) The Tasks performed (during each check)

   A checklist of tasks will be diligently performed during each maintenance period:

   - Interior cleaning of all of the components
   - Exterior cleaning of all of the components
   - Power supply testing

- Battery checks/replacements (if applicable)
- Cable and connector testing
- Backup cable and connector testing (assets that are in storage will be tested as well)
- Calibration testing (if applicable)
- Diagnostic Testing

4) Post-Check Tasks

   All hardware that was found to be malfunctioning or damaged in a manner that prevents further use or repair will be promptly disposed of. Replacement components shall be ordered as soon as possible, and a maintenance check is to be completed on all new hardware upon arrival at the laboratory to ensure that it is functioning up to lab standards.

Software:

When it comes to software maintenance, a different approach is required compared to hardware maintenance. Software changes and updates tend to occur at a much more rapid pace compared to hardware, which results in a more frequent maintenance schedule being needed in order to accommodate any necessary changes. Staying true to this maintenance schedule is absolutely paramount when it comes to software, as updates from the developers of the software can contain new security features and coding that could address any new cyberthreats that are on the rise.

1) Assessment

A general assessment of all software programs used within the confines of the laboratory is always the first step in the maintenance check. A thorough testing shall be performed in order to account for all software programs and their general information. This will include checking and implementing any new updates or security patches that may have been released for the software since the last scheduled maintenance check. Once this has been completed, the software will be run through diagnostic testing and system checks in order to find any glaring issues regarding security or factors that are impeding functionality. Any and all problems that are found are to be recorded so that feedback can be sent to the parent company of the problematic software for further troubleshooting.

2) Frequency of maintenance checks

   Due to the more frequent updates and patches that occur in the world of digital forensics software, maintenance checks for software will be expected to be carried out twice a month, as opposed to the once-a-month nature of hardware checks.

3) The Tasks performed (during each check)

   - Diagnostic testing
   - Documentation (glaring issues or problems)
   - Optimization testing (for speed and efficiency of software)
   - Adaptation of software towards any relevant new hardware
   - Checks for new available features or improvements that must be implemented
   - Installation of newer versions of software (if available)

4) Post-check Tasks

   Any malfunctioning or compromised software will be done away with and promptly replace with another program serving a similar function. All bugs and vulnerabilities found will be documented by the lab technicians and then reported to the lab manager for further action.

Staffing

For our digital forensics lab, we will be employing a lab manager and two lab technicians to work within the confines of the laboratory. To ensure that these individuals are appropriately trained and qualified for these positions, a very specific type of candidate will be selected. Being as the field of digital forensics is a very lucrative field, there will certainly be a wide range of superb candidates to choose from. In the following section, I will detail the certifications, degrees, and experience that will be expected for the individuals that will be chosen to fill these positions.

Lab Manager

General job description:

The Lab Manager will be expected to handle the daily management tasks of the laboratory in conjunction with the two lab technicians and will also be expected to collaborate with the senior authority of the police department that houses said lab. He/she/they will be in charge of managing the laboratory's various resources, the efficiency of laboratory activities, the team

morale of the employees and any additional staffing that is needed in the future. This individual should have experience in leading a team-environment in a previous workplace and should be capable of both encouragement of employees and strict admonishment. The lab manager will be responsible for ensuring that the lab adheres to all procedures and processes detailed by ISO/IEC 17025 industry standards. The lab manager will be expected to oversee the carrying out of maintenance checks and to take the appropriate actions should any hardware/software in the laboratory need repairs or a replacement.

Certifications:

EnCase Ce EnCase Certified Examiner (EnCE) Certification required

Certified Computer Examiner (CCE) Certification required

GIAC Certified Forensic Analyst (GCFA) Certification required

***Any additional relevant certifications in digital forensics, cybersecurity or IT are desired, but not required

Degrees:

A master's degree in the fields of Digital Forensics, Computer Science, or any other related field.

Experience:

- At least 4 years of experience working in the field of digital forensics

- 3-4 years of experience of conducting digital forensics-related investigations and writing official investigative reports of findings
- 3-4 years of experience using all of the relevant software and hardware that will be used in the laboratory environment
- 3+ years of experience in a managerial role in digital forensics or another closely related field, where the candidate was tasked with overseeing a team
- Familiarity with the common types of OS (operating systems) that will be used in the laboratory environment
- A passion for technology and digital forensics is encouraged

In addition to the previous requirements, the candidate will be required to take and pass both a background check and drug test before being hired.

Lab Technician (2)

General job description:

The lab technicians will be working under the supervision of the lab manager and will be expected to report directly to them. They will be in charge of directly operating all of the equipment within the confines of the laboratory environment. Lab technicians will also be expected to be able to perform under high-stress and super detail-oriented circumstances on a daily basis, with a dynamic range of daily tasks that vary from case to case. The lab technicians will directly carry out maintenance checks on the hardware and software in the laboratory and will report any and all findings directly to the acting lab manager. Lab techs should also keep up

to date with all progressions and technological advancements in the field of digital forensics in their own personal time, in order to best perform at their roles and to help keep the laboratory at international industry standards. Lab technicians are to be familiar with and consciously abide by ISO/IEC 17025 standards without exception when working in the laboratory.

Certifications:

EnCase Certified Examiner (EnCE) Certification required

Certified Computer Examiner (CCE) Certification required

AccessData Certified Examiner (ACE) Certification required

***Any additional relevant certifications in digital forensics, cybersecurity or IT are desired, but not required

Degrees:

A bachelor's degree in the field of digital forensics or any other relevant fields (computer science, criminal justice, information technology, cybersecurity) required.

Experience:

- 2-3 years of experience of working in digital forensics field
- At least 2 years of experience working in a digital forensics' laboratory environment
- General familiarity with all relevant OS (operating systems) used in the lab
- 2+ years of experience using all relevant laboratory technologies
- General troubleshooting experience with hardware and software used in lab

- A passion for technology and digital forensics is encouraged
- Adaptability towards learning new technologies or software that is implemented into the laboratory

In addition to the previous requirements, the candidates will be required to take and pass both a background check and drug test before being hired.