Marcus Sowers

Digital Forensics

Midterm

2/23/21

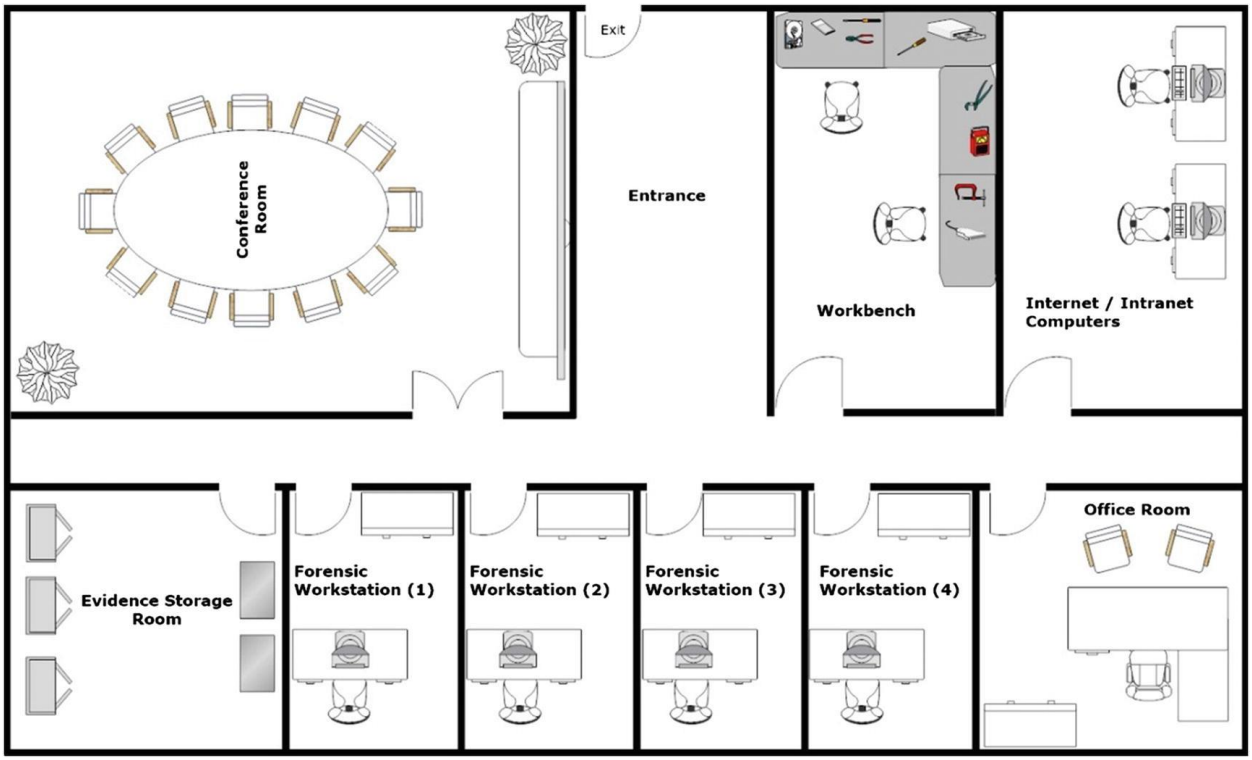
Summary:

- I have been hired to create and run a brand-new digital forensics lab for a mid-sized police department. My assignment is to come up with a plan for the lab for the next 3 years that will run as efficient as possible. Too maintain a digital forensics laboratory, I must make sure that my staff has the necessary training, resources, and qualifications to perform each task at the best efficiency level. The goal of this lab is to evaluate certain information and evidence monitored by procedures and policies. The function is to identify, seize, acquire, and analyze all electronic devices related to all cyber-enabled offences reported to collect digital evidence which is presented in a court of law for prosecution purposes. This goal includes maintenance plans, calibration procedures, an accreditation plan, calibration procedures and more.

Accreditation Plan:

- The accreditation plan for the laboratory will be to make sure everyone follows protocols while keeping a safe and well running environment. The requirements that will be enforced is checked through the international standard.

Forensic Laboratory Floor Plan:



Inventory:

- *Hardware Equipment*:
  - Mouses
  - Keyboards
  - Desks/Tables
  - Computer Chairs
  - Monitors (Flat and CRT panel)
  - Speakers
  - Printers
  - Headphones
  - Projector

  - Scanners
  - Serial attached SCSI
  - Cables (Audio, USB, Fiber, VGA, Ribbons, and Ethernet)
  - Motherboard and Core Processors
  - RAM Hard Disk Drives
  - Modular Adapters
  - Power Cables
  - Rite Blockers
  - Graphic Cards
  - Sound Cards
- *Software Equipment:*
  - Helix Pro
  - Chainlinx
  - Kali Linux
  - Wire Shark
  - VMWare
  - Virus Protection
  - Forensic Suites (Encase, FTK, Ilook, and Black Bag)
  - Ubuntu

Maintenance Plan:

- The maintenance plan for the laboratory includes a plan of tasks to maintain and fulfill the needed requirements to support and monitor the lab. The level of maintenance will be high, as it will help maintain and keep the performance level high and the best quality as possible.

Scope:

- The scope defines the specific tests and calibrations for which your organization will be accredited, and it helps us to determine the number of days needed for your on-site assessment. This includes a safe environment for every worker, training that will be required and proper consequences for potential misuse of equipment within the laboratory.

Roles/Responsibilities:

- *Digital Investigators*: The role and responsibilities of the digital investigators is to investigate all evidence possible.
- *Security Officer*: The role and responsibility of the security officer is check visitors and staff members in and out the laboratory.
- *Lab Manager*: The role and responsibility of the lab manager is to look over operations, security, scheduling, and procedures done within the lab.
- *Lab Safety Director*: The role and responsibility of the lab safety director is to maintain and enforce safety procedures and policies, keeping the environment as safe as possible.
- *Facility Manager*: The role and responsibility of the facility manager is to manage maintenance within the facility.
- *Analysist/Examiners*: The role and responsibility of the examiners is self-explanatory, which is to examine, analyze, recover, file, and collect ESI.
- *Forensics Engineer*: The role and responsibility of forensic engineers is to inspect evidence drawn from the site of the failure to piece together the sequence of events that led up to it.

Maintenance Policies:

- The maintenance policies for my digital forensics lab will be daily cleanings, constant repairs and upgrades, and renovation and calibrations if needed. Keeping the equipment clean and updated prevents the possibility of expensive damage and repairs. This policy helps reduce the risk of possible damage and exposure.

Calibration Procedures:

- The calibration procedure will be quick and efficient as just checking if a machine is calibrated or non-calibrated, could lead to a easy fix from an employee.

Reference Standards, Certified Reference Materials, and Reference Material:

- These references will include filed paperwork and documents that will highlight the specific use of each equipment in the laboratory.

Calibration Interval:

- This allows the company to be certain everything is working and functioning.

Maintenance:

- Maintenance for every equipment will be cleaned and locked up in the equipment room daily.

Preventive Maintenance:

- Calibrations and performance checklist will be done daily to make sure the equipment is properly working.

Performance Checks:

- I decided the performance checks will be completed with a biweekly checklist. This will allow us to locate any errors and malfunctions, while being able to find the best solution immediately.

Equipment Security:

- Each equipment will be barcoded so we can indicate which equipment is being used at a certain time. Every equipment owned by the laboratory will be stored in a locked room. To retrieve the equipment, you will have to check it out so everything and everyone is accounted for just incase of any problems. Only employees and verified selected individuals can access the equipment.

Bibliography:

"DIGITAL FORENSIC LABORATORY(DFL)." Directorate of Criminal Investigations, cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html#:~:text=FUNCTIONS%20&%20ROLES%20The%20DCI%E2%80%99S%20Digital%20Forensic%20Lab,in%20a%20court%20of%20law%20for%20prosecution%20purposes.

Hassan N.A. (2019) Computer Forensics Lab Requirements. In: Digital Forensics Basics. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-3838-7_3

"ISO/IEC 17025 Forensic Lab Accreditation Process." ANAB/ANSI ISO Accreditation Solutions, anab.ansi.org/forensic-accreditation/iso-iec-17025-forensic-labs-process-0.