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

ISO/IEC JTC 1 or joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission is the standard for developing and maintaining the lab. ISO IEC 17025 are specific standards laying out all requirements when conducting laboratory testing/calibrations.

Lab Accreditation Plan

A series of requirements and steps are required to get officially ISO IEC 17025 accredited for a digital forensics lab. Taking into consideration what technical requirements American Association For Laboratory Accreditation (A2LA) asks for. (See below for required martial)

A2LA accreditation steps

Step 1:

Conduct research and check the criteria regarding required martial needed for application eg. documents, financial statements, etc. For more information view A2LA's accreditation requirements at *https://www.a2la.org/accreditation/forensics*

Step 2:

Contact A2LA and inform them that the mid-sized police department wants to get accredited for a digital forensics lab. Contact information provided in link *https://www.a2la.org/form/contact-us*.

Step 3:

Review current martial and check to see if any documentations or procedures are missing within the system. Check for deficiencies and go over them with the current management team.

Step 4:

Submit required documentations/system's needed to A2LA including application.

Step 5:

Wait for approval. Once approved the lab will be ISO IEC 17025 accredited be officially A2LA and internationally recognized.

Inventory

Hardware

- swivel chairs
- desks
- Tables
- Private secured storage room
- USB's/Hard drives (TBD)
- Printers (3)
- PC monitors/CPU's & required hardware eg. wires, adaptors, keyboards, mouse (5)
- Scanner (3)
- Laptops
- Speakers
- Projector/projection panel
- DSLR Camera/camcorder & required hardware eg. charger, memory card, tripod
- VGA Split cable
- Ethernet cable
- HDMI Cables
- Optical fiber cable
- UniPRO GbE Multistream Bidirectional transmission tester
- TP-Link AC1750 Smart WiFi Router
- TP-Link N300 WiFi Extender
- TP-Link AC750 WiFi Extender

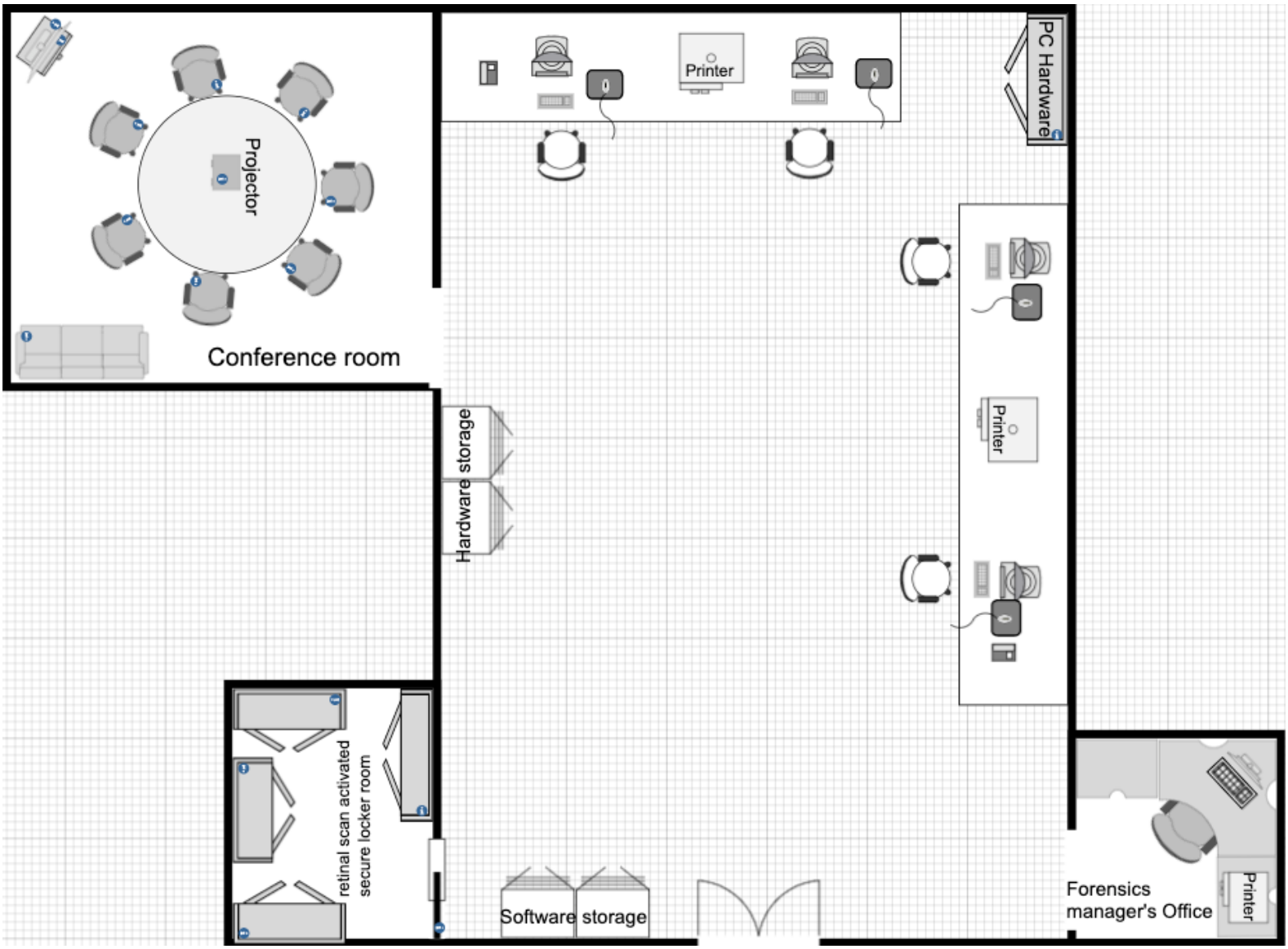
Operating System Software

- Windows OS
- Kali Linux
- MacOS

Software Applications

- SIFT Workstation
- FTK imager
- Autopsy
- OphCrack

Forensics Laboratory Floor Plan



Maintenance plan

A maintenance plan is key when ensuring the relatability of the equipment within the lab. It is required that both the lab and staff are prepared to recalibrate and assess equipment on a regular basis. In preparation for any anomalies within the digital forensics lab, it is required to understand the 4 different maintenance strategies.

See below for provided link and terms.

Corrective maintenance

- Preparing to maintain and restore any missing data within the lab. Having resources to continue normal operations.

Preventive maintenance

- Maintaining equipment at all costs to ensure and prevent failure before it even occurs.

Risk-based maintenance

- Review assess and analyze equipment's conditions, acknowledge risk failure and define appropriate maintenance program.

Condition-based maintenance

- The condition of all equipment in the lab is constantly assessed on the condition and performance. Maintenance is performed on equipment once signs of deterioration begins to show.

Staffing

Forensics/lab manager

Tasks

- Provides and assists with overseeing the hands-on work of the digital examination team within the lab.
- Acting liaison between the laboratory staff and police department. Providing quality and accuracy, his/her job is key when providing information to the police department on both a local and federal level on what digital evidence is discovered within an investigation.
- Reviews and assess all hardware and software within the lab to make sure it is up to date.

Minimum requirements

- Must have bachelor's degree in either biology chemistry, Forensics science, Criminalistics
- 3 years experience in digital casework
- 2 years experience in both digital and physical analysis of evidence
- 2 years of managerial experience

Digital Examination Team

Tasks

- Assess and analyze digital devices recovered from investigations
- Photograph and copy evidence
- Determine the outcome of evaluated evidence

Minimum requirements

- Must have a bachelor's degree in computer forensics or a similar degree
- CFCE certified or related certification
- Minimum 1-year experience in digital analysis

Courtroom team

Tasks

- Provide legal counseling to the laboratory team
- Help determine what is and isn't allowed when conducting a digital investigation
- Monitoring and assessing whether obtained evidence is constitutionally valid
- Must be able to provide legal assistance when needed

Minimum requirements

- Have law a law degree
- State and federal board certified
- 1-2 years experience working criminal cases

Bibliography

Forensic Examination Accreditation Program: A2LA. American Association for Laboratory Accreditation. (n.d.). https://www.a2la.org/accreditation/forensics.

Forensicsware. (n.d.). *Customized Setup for Dedicated Cyber Investigation*. Cyber Lab Setup ~ Digital Forensic Lab Experts for Hardware, Software & Training. https://www.forensicsware.com/lab-setup.html.

Says, K., Says, N., says, S., says, D., Says, H. K., says, P., Says, S., says, D., & says, M. (2017, October 3). *Top 10 Password Cracking Tools for all Platforms*. TECHNIG. https://www.technig.com/password-cracking-tools/.

4 types of maintenance strategy, which one to choose. Medium Voltage Products. (n.d.). https://new.abb.com/medium-voltage/service/maintenance/feature-articles/4-types-of-maintenance-strategy-which-one-to-choose#:~:text=Four%20general%20types%20of%20maintenance,based%20and%20condition%2Dbased%20maintenance.