CYSE 407 Midterm Case Scenario

Antonio Shields

School of Cybersecurity, Old Dominion University

CYSE 407: Digital Forensics

Prof. Bryan Bechard

December 2, 2023

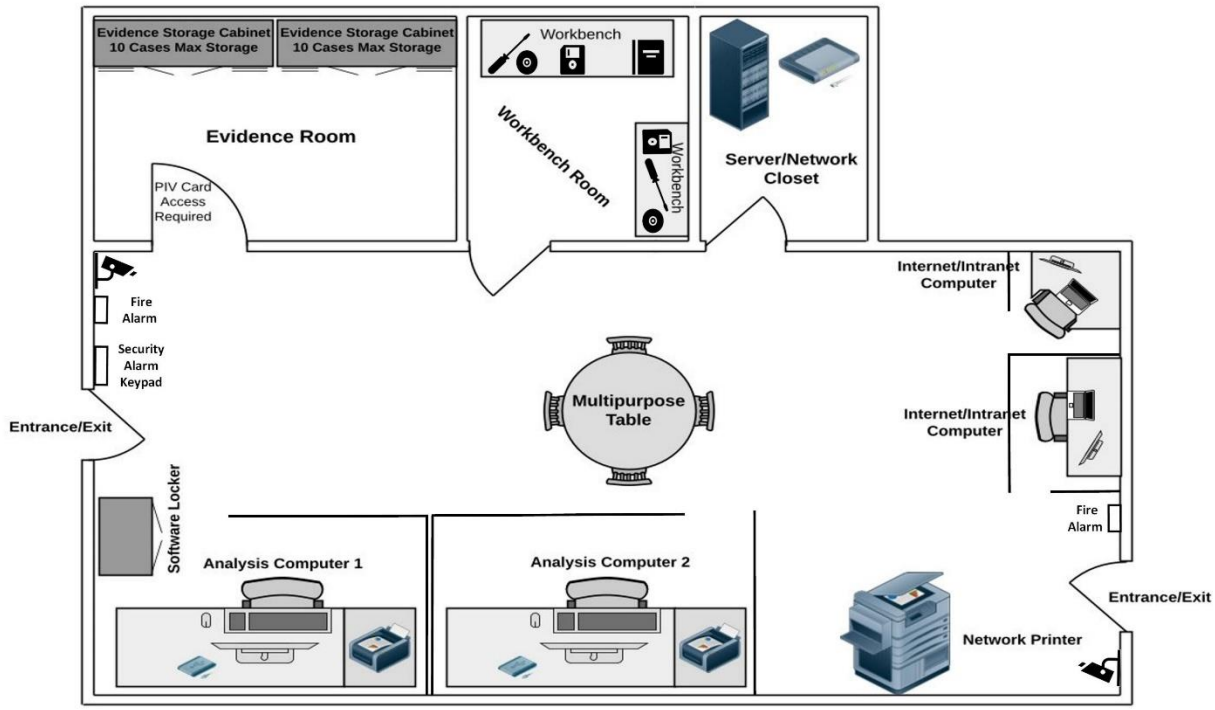
Summary

ISO/IEC 17025 specifies the general requirement for the competence, impartiality, and consistent operation of laboratories. ISO/IEC 17025:2005 was the previous version used from 2005 to 2017 when ISO/IEC 17025:2017 was implemented. The 2005 version included scope, normative references, terms and definitions, management requirements, and technical requirements, while the 2017 version includes scope, normative references, terms and definitions, general requirements, structural requirements, resource requirements, process requirements, and management system requirements. The 2017 version focuses more on risk-based standards and less on procedure-based standards than the 2005 version did. ISO/IEC 17025:2017 is the main ISO standard used by testing and calibration laboratories for which most labs must hold accreditation to be considered technically viable. In many cases, suppliers and regulatory authorities will not accept test or calibration results from a laboratory that is not accredited. ISO/IEC 17025:2017 applies to all organizations performing laboratory activities, regardless of the number of personnel. Maintaining ISO 17025:2017 accreditation ensures that daily laboratory practices are being conducted and continuously improved, which makes the digital forensic evidence obtained from the lab highly accepted and validated.

Accreditation Plan

For this lab's work to be accepted as evidence in digital forensic investigations, accreditation is important to obtain and maintain. To ensure that the lab meets industry standards and is recognized as a trusted, accurate, and reliable digital forensics retrieval facility, accreditation will be sought through an accreditation body, such as ANAB. The ANSI-ASQ National Accreditation Board (ANAB) provides accreditation for crime and forensics labs worldwide including digital evidence analysis forensics labs. To achieve accreditation, ANAB audits the lab's tasks and functions to ensure correct and consistent results for all cases in addition to the lab's work quality and integrity using ISO/IEC 17025 standards as their guide. The steps to achieving ISO/IEC 17025 Forensic Testing Laboratory Accreditation are Quote, Application Submittal, Documentation Review, Accreditation Assessment, Corrective Action and/or Follow-up Visit, Accreditation Decision, and once Accreditation is granted, Continued Surveillance and Reassessment. These steps will be followed to achieve accreditation standards. https://anab.ansi.org/accreditation/iso-iec-17025-forensic-testing-laboratory/ will provide more information on accreditation requirements.

Forensic Laboratory Floor Plan



The Forensic Laboratory Floor Plan for the mid-size police department consists of four rooms: Forensics Lab Main Room, Evidence Room, Workbench Room, and the Server/Network Closet. The Forensic Laboratory has two entrances/exits that require a Common Access Card to enter to provide physical security to the laboratory, the forensic lab with have its own security system separate from the building, so it will have its own security keypad to activate/deactivate the alarm, there are also two security cameras placed at opposite corners of the main room to provide 24/7 monitoring throughout. Inside of the main room will be where the Analysis computers and Internet/Intranet computers are located, surrounded by cubicle panels to provide need-to-know privacy. The main room also has a software locker for any software storage, a network printer, a multipurpose table for meetings, etc., and room available for a small information library of books if needed. There are also fire alarms placed at each entrance/exit in case of fire. The evidence room contains two evidence storage lockers that can hold up to 10 cases of evidence each for a max total of 20 evidence cases stored at one time. This room will also be card-accessed due to chain-of-custody requirements and the ability to monitor access logs to the room in conjunction with the logs for the lab for any issues or irregularities that may arise. The workbench room has two tables for any physical work that needs to be done during the evidence

retrieval process. The network/server room will consist of the network server, router, and switches needed for the lab and any spare network or computer equipment needing to be stored.

Inventory

Some of the equipment that is needed to get this Digital Forensic up and running are as follows:

Physical Lab equipment requirements:

- 1 evidence storage room
- 1 workbench room
- 1 server/network room
- 9 cubicle privacy panels
- 1 round multipurpose table with four chairs
- 2 security cameras
- 3 common access card entry panels
- 2 evidence storage cabinets that can hold 10 cases of evidence each
- 1 security system with alarm keypad and motion sensors
- 2 long desk for analysis computers
- 1 short desk for internet/intranet laptop
- 1 corner desk for internet/intranet laptop
- 2 small desks for analysis computer printers
- 1 software locker
- 4 computer desk chairs
- Trash cans

Hardware needed to conduct Digital Forensics functions:

- 2 high-quality analysis computers with capabilities of running modern digital forensics software
- 2 external hard drives minimum
- 2 laptops for Internet/Intranet functions
- 2 printers for analysis computers
- 1 network printer
- 2 monitors for internet/intranet laptops
- 2 monitors for the analysis computers
- digital camera with record capabilities
- HDMI cords
- USB cords
- Ethernet Cables
- Switch
- 1 network server
- 1 router
- Sound speakers
- Headphones

- USB-C cords
- iPhone cords

Software needed to conduct Digital Forensics functions:

- EnCase
- Autopsy
- Wireshark
- Kali Linux
- FTK (Forensic Toolkit) Imager
- The Sleuth Kit
- OS Forensics
- Splunk
- Bulk Extractor
- Digital Forensics Framework
- Helix3 Pro

Maintenance Plan

With most equipment, maintenance is a requirement to prevent breakdowns and irreparable damage to a system. Technology and software also need to be updated and upgraded occasionally to maintain functionality, security, and to make use of the latest advances. Having a regular maintenance plan in place will minimize the unexpected from occurring, but will not eliminate it entirely. This not only goes for the computer systems, but for the security systems as well. The physical aspects of the laboratory and the furniture will also need to be maintained on an occasional basis as well, but not as frequently as the digital forensics equipment, technology, and software. In addition, those efforts should be coordinated with the facility maintenance personnel to maintain optimal sustainability throughout.

The maintenance plan will include:

- the schedule for regular hardware and software updates
- maintenance costs
- contingency plan for equipment downtime
- trusted vendors to utilize for maintenance repairs
- regular audits of security measures and policies
- routine backups of data stored in the lab
- regular testing of forensic tools and processes for accuracy and reliability

Staffing

With the digital forensics lab being a part of a mid-size police department, the number of staff needed to run the lab will only consist of a lab manager and a single technician at this time. Depending on the budget and workload during these 3 years, personnel issues can be reevaluated at a later time. All staff will possess the appropriate certifications and credentials needed to sustain and maintain ISO/IEC 17025:2017 accreditation.

Lab manager - Responsible for overseeing the operations of the lab, including supervising the lab technician, providing a safe and secure workplace for the staff and the evidence, coordinating with law enforcement agencies, and managing relationships with external stakeholders. Lab manager duties will also include, but are not limited to: setting up the process for managing cases, implementing policies and procedures and ensuring adherence by all staff members including yourself, implementing the protocol for handling and storing evidence and maintaining logs, and conducting yearly audits to ensure accreditation requirements are being meet and address any deficiencies promptly.

Lab Technician - Responsible for performing forensic examinations of digital media, preparing reports, and testifying those findings in court when called upon. The technician should be proficient in working digital forensic cases and be knowledgeable in the hardware and software available to analyze the evidence efficiently. Because you may be called upon to testify your analysis results, must be familiar with the questioning process and have the ability to explain the results clearly and understandably.

Both the lab manager and technician will participate in and receive regular training on the use of digital forensics software and hardware in addition to the policies and procedures of the lab. This training will be provided by either the lab manager themselves for the Lab technician or an outside experienced professional brought in to instruct. The lab manager and technician both will receive annual evaluations to show their respective progress and sustainment and improvement areas to aim for before the next evaluation.

References

Accreditation Requirements for Forensic Testing and Calibration. ANAB. (2023, February 1). https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=12371

ANAB ANSI National Accreditation Board. (n.d.). Forensic laboratory accreditation: ISO/IEC 17025. ANAB. https://anab.ansi.org/accreditation/iso-iec-17025-forensic-testing-laboratory/

Honsa, J. D., & McIntyre, D. A. (2003). ISO 17025: Practical benefits of implementing a quality system. Journal of AOAC INTERNATIONAL, 86(5), 1038–1044. https://doi.org/10.1093/jaoac/86.5.1038

ISO 17025 accreditation: Overview & Benefits. Excedr. (n.d.). https://www.excedr.com/resources/iso-17025-accreditation-the-benefits-and-how-to-obtain

Patrick, B. (2019, June 12). ISO 17025 standards. ISO 17025 Store. https://17025store.com/iso-17025-standards/