Ruth Abeselom

Professor Bechard

CYSE 407

8 December 2023

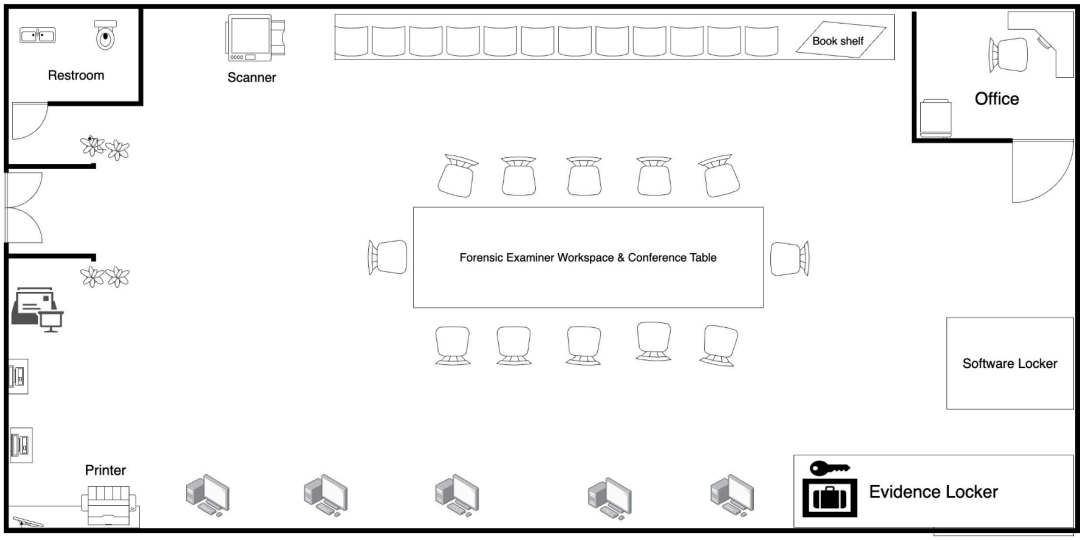
Plan Outline for a Computer Forensics Lab

Summary: ISO/IEC 17025:2005 is an international standard that specifies the general requirements for the competence of testing and calibration laboratories. The standard emphasizes the importance of quality assurance and control in laboratory operations. It requires laboratories to establish and maintain procedures for the identification, collection, and handling of samples, as well as for the execution of tests and calibrations. It sets out criteria for laboratories to demonstrate their ability to produce accurate and reliable results. To function, a digital forensics laboratory must execute operations such as measuring, sampling and assessing outcomes. The purpose of the lab is to critically assess data and evidence that are subject to specific policies and procedures. This covers a wide range of items such as calibration methods, staffing and duties, floor plans, maintenance plans, definitions, and accreditation plans.

Accreditation Plan: This plan involves conducting a comprehensive gap analysis to identify areas of compliance and areas requiring improvement. Policies and procedures will be developed or revised to align with the accreditation standards, covering aspects like evidence handling, data acquisition, analysis, and quality control. Training programs will be implemented to enhance personnel competencies, and equipment and facilities will be evaluated to meet the required standards. A robust Quality Management System will be established, encompassing document control, risk management, audits, and continual improvement. The plan includes validation and

proficiency testing procedures, compliance monitoring, and a clear timeline with allocated resources. Regular reviews and communication with stakeholders will ensure progress and engagement throughout the accreditation process. Ultimately, achieving accreditation will demonstrate the lab's competence and reliability in the field of digital forensics.

Forensic Laboratory Floor Plan:



Inventory:

Hardware equipment will include

- ➔ Flat-panel monitors
- ➔ CRT panel monitors
- ➔ Keyboards
- ➔ Mouses
- ➔ Headphones
- ➔ Projector

- ➔ Printer
- ➔ Scanner
- ➔ LCD projection panels
- ➔ Surround sound speakers
- ➔ Graphic and sound cards
- ➔ Serial attached SCSI
- ➔ Audio cables
- ➔ USB cables
- ➔ Fiber cables
- ➔ VGA split cables
- ➔ Ribbon cables
- ➔ Modular adapters
- ➔ Ethernet cables
- ➔ RAM hard disk drives
- ➔ Chips
- ➔ Multiple processor motherboard
- ➔ Multiple core processor

Software equipment will include:

- ➢ Helix Pro
- ➢ Chainlinx
- ➢ Kali Linux
- ➢ Pro discover forensic
- ➢ Wireshark

- ➢ Autopsy
- ➢ SPEKTOR Forensics intelligence
- ➢ The Sleuth kit

Maintenance Plan: Includes creating an asset inventory, developing a maintenance schedule, defining specific tasks, allocating necessary resources, and establishing detailed procedures. Training and competency development for maintenance personnel are crucial, along with proper documentation and record-keeping of all maintenance activities. Performance monitoring, continuous improvement, and vendor management are important aspects of maintaining asset reliability. Emergency response protocols, budgeting, stakeholder communication, and periodic reviews or audits complete the plan.

Definitions:

- Computer Forensics: The process of collecting, analyzing, and preserving electronic evidence from computers, networks, and digital devices in a manner that maintains its integrity and admissibility in a legal context.
- Digital Evidence: Any information or data stored or transmitted in digital form that is relevant to an investigation or legal proceeding. It can include files, emails, chat logs, network traffic, metadata, and other digital artifacts.

- Chain of Custody: The documentation and procedures that establish the chronological history of the handling, control, and location of evidence. It ensures that the integrity of the evidence is maintained and can be presented as reliable in court.
- Imaging: Creating a bit-for-bit copy or snapshot of a storage media or device, including hard drives, USB drives, or mobile devices. It captures all data, including deleted files and hidden information, without modifying the original evidence.
- Risk management: Monitors and finalizes how much risk can be accounted for, and the most reliable equipment
- Data Acquisition: The process of gathering digital evidence from various sources, such as computers, servers, mobile devices, and cloud storage. It involves identifying, collecting, and preserving the data in a forensically sound manner.
- File System: The structure and organization of files and directories on a storage device. Common file systems include FAT, NTFS, HFS+, and Ext4. Understanding file systems is crucial for data recovery and analysis.

Scope:

- ❖ Types of Cases: Determine the specific types of cases or investigations that the lab will handle.
- ❖ Digital Devices and Media: Specify the range of digital devices and media that the lab will analyze.
- ❖ Operating Systems and Platforms: Identify the operating systems and platforms that the lab will support, such as Windows, macOS, Linux, Android, iOS, etc

- ❖ Forensic Techniques: Outline the forensic techniques and methodologies that the lab will employ.

Roles & Responsibilities: The roles and responsibilities of the Laboratory Manager, Quality Assurance Liaison, and Designee can be defined as follows:

1. Laboratory Manager: Oversee the overall operations of the Computer Forensics Lab and ensure its smooth functioning. Develop and implement policies, procedures, and protocols for evidence handling, data acquisition, analysis, and reporting. Manage and allocate resources, including personnel, equipment, and budgets.
2. Quality Assurance Liaison: Serve as the primary point of contact for quality assurance activities within the Computer Forensics Lab. Develop and implement a Quality Management System (QMS) in accordance with applicable standards and accreditation requirements. Provide training and guidance to lab personnel on quality assurance principles and practices.
3. Designee (Deputy or Assistant): Assist the Laboratory Manager in overseeing daily operations and managing resources. Support the development and implementation of lab policies, procedures, and protocols. Assist in monitoring and evaluating lab performance and implementing improvement measures.

Maintenance Practices: These practices include preventive maintenance to prevent failures, regular software updates and patches for security and performance improvements, backup and disaster recovery measures to protect critical data, implementation of security measures to safeguard infrastructure and data, equipment calibration for accurate measurements, inventory

management for tracking equipment, documentation of maintenance activities, monitoring and performance analysis, training and skill development for lab personnel, and a focus on continuous improvement.

Calibration Procedures: Procedures involve the systematic and controlled process of verifying and adjusting the accuracy and precision of measurement tools and equipment. These procedures typically include a series of steps, such as selecting appropriate calibration standards, performing measurements using the equipment, comparing the results to known reference values, and making necessary adjustments to ensure accuracy. Calibration may involve adjusting settings, calibrating sensors, or verifying the accuracy of digital scales, oscilloscopes, or temperature sensors. The procedures also encompass documenting calibration activities, including dates, equipment details, calibration standards used, and results obtained.

Calibration Interval: The recommended frequency at which measurement tools and equipment should undergo calibration. The specific calibration intervals may vary based on factors such as manufacturer recommendations, industry standards, regulatory requirements, and the criticality of the measurements being performed. Calibration intervals are typically determined based on factors such as the stability and drift characteristics of the equipment, the level of accuracy required for the specific measurements, and the historical performance data.

Maintenance: This involves a range of activities aimed at ensuring the proper functioning and reliability of equipment and systems. Security measures, including antivirus software, firewalls, and access controls, are employed to safeguard the lab's infrastructure and data. Documentation, monitoring, and performance analysis are integral to tracking maintenance activities, identifying

issues, and optimizing workflows. Continuous training and skill development ensure personnel stay updated with the latest forensic techniques and best practices.

Preventive Maintenance: This includes preventive maintenance, such as regular cleaning, calibration, lubrication, and inspection of hardware components to prevent failures and minimize downtime. Software updates and patches are applied to address security vulnerabilities, improve performance, and maintain compatibility. Backup and disaster recovery measures are implemented to protect critical data and enable quick restoration in case of hardware failures or data loss.

Corrective Maintenance: Includes troubleshooting, diagnosing the root cause of the problem, repairing or replacing faulty components, and restoring the equipment to its normal operating condition. The primary goal of corrective maintenance is to minimize downtime and ensure that equipment and systems are back up and running as quickly as possible.

Performance Checks: This involves assessing the operational efficiency and effectiveness of equipment, systems, and processes. These checks are conducted to ensure that the lab is functioning optimally and meeting the required performance standards. Performance checks may include monitoring metrics such as network bandwidth, server utilization, storage capacity, and response times to identify potential bottlenecks or areas of improvement.

Malfunctioning Equipment: This can include hardware failures, software glitches, compatibility problems, or other issues that impede the normal operation of the equipment. Prompt action is required to diagnose and rectify the problem, which may involve

troubleshooting, repair, replacement of faulty components, or software updates. It is crucial to address malfunctioning equipment swiftly to minimize downtime, maintain the lab's efficiency, and ensure the accuracy and reliability of the forensic processes conducted within the lab.

Equipment Security: The measures implemented to protect the lab's hardware, software, and associated data from unauthorized access, tampering, theft, or damage. This includes physical security measures such as controlled access to the lab, secure storage for equipment, and surveillance systems. It also involves implementing appropriate cybersecurity measures like firewalls, encryption, and intrusion detection systems to safeguard against cyber threats.