Kobe Coleman

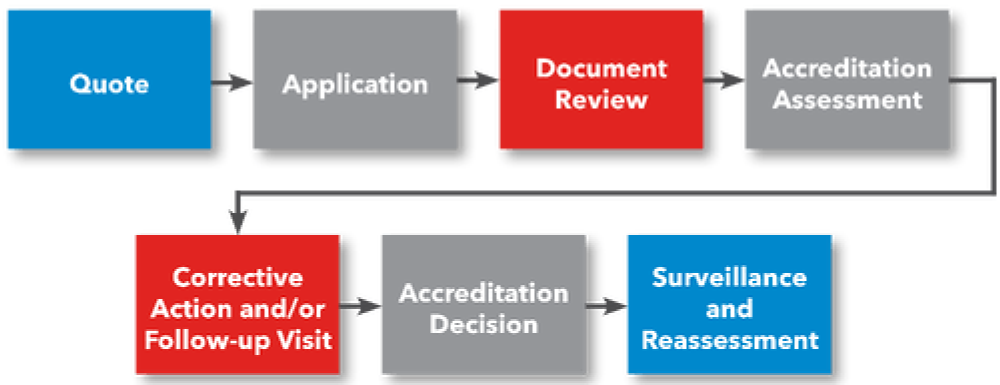
Midterm Paper

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.

Lab Accreditation Plan

"ISO/IEC 17025 enables laboratories to demonstrate that they operate competently and generate valid results, thereby promoting confidence in their work both nationally and around the world." (ISO)



Step 1: A laboratory applies for accreditation by visiting the A2LA website and completing the required application forms, paperwork, and checklist.

Step 2: After submitting financial papers to government officials, applicants must wait for approval.

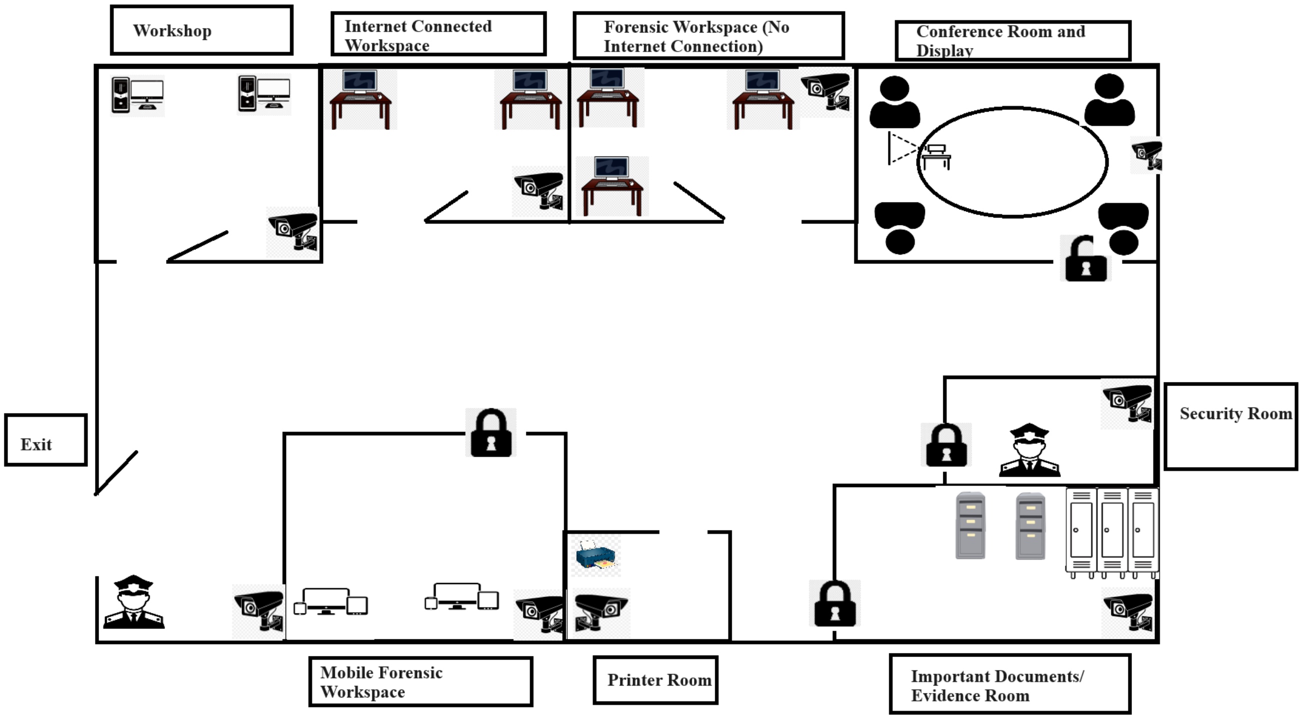
Step 3: Once approved, the laboratory must identify a suitable place to begin operations.

Step 4: The laboratory then has to hire people who are experienced and qualified to operate in its facilities.

Step 5: Next, find the required equipment that has been approved on the A2LA website. Make sure that the equipment is available at a reasonable cost to avoid paying too much.

Step 6: After submitting all required paperwork and receiving approval from the ISO IEC 17025 accreditation organization, along with payment of the required fees, proceed with setting up the investigation laboratory. As a result, the laboratory will become well-known worldwide.

Forensic Lab Floor Plan



Floor Plan Features

- Floor Plan includes a conference room and display monitors so meetings can be held.
- Floor Plan also includes security room so we can monitor suspicious activities.
- Has an Evidence Room/Storage/Important Documents rooms to hold all the files documents and equipment needed.
- Plan includes a Mobile Forensic, Forensic Workplace (No Internet Connection), A Workshop, and an Internet Connected Workspace.
- Printer Room for printing documents needed for cases

Hardware

- Random Access Memory (RAM)
- Solid State Drives (SSDs)
- Hard Disk Drives (HDDs)
- Graphics Processing Units (GPUs)
- Central Processing Units (CPUs)
- Network Interface Cards (NICs)
- Power Supply Units (PSUs)
- Cooling Systems (e.g., fans, liquid cooling)

- Forensic Hardware Write-Blockers
- Hardware-based Encryption Devices
- Workstations
- Write Blockers
- Forensic Imaging Tools
- Storage Arrays
- Network Forensic Appliances
- Mobile Device Forensic Tools
- Forensic Write-Once Read-Many (WORM) Drives
- Portable Forensic Kits

Software

- EnCase Forensic
- AccessData Forensic Toolkit (FTK)
- X-Ways Forensics
- Autopsy
- Magnet AXIOM
- Sleuth Kit
- Volatility
- Cellebrite UFED (Universal Forensic Extraction Device)
- Oxygen Forensic Detective
- Digital Forensics Framework (DFF)
- Forensic Explorer
- BlackLight
- OSForensics
- Registry Recon
- Wireshark

Operating Systems

- Linux
- Windows
- iOS
- Android
- LAMP

Maintenance Plan

1. Computers should be cleaned and system information deleted once a week. This method ensures that no unneeded data from earlier cases is preserved on computer storage.
2. Every six months, staff will engage in a fire exercise to practice evacuating the building in the event of an emergency and familiarizing themselves with the fire exits.
3. Security camera footage must be monitored and, at the end of each shift, sent to a data storage center.
4. To maintain sanitary requirements, the area should be cleaned every night by professional cleaning personnel who are supervised by a guard.

5. Electrical wiring should be checked every six months to ensure there are no short circuts that could cause a fire.

Lab Maintenance Plan

1. Backups of newly extracted information and data should be performed daily to ensure that collected data is preserved.
2. Every month, the IT team will come in and perform a system diagnosis.
3. Implement patch management to keep software up to date and optimized for use.
4. An incident response team should be present and operational in the lab.

Staff

1. Senior Digital Forensics Analyst (Team Lead)
2. Cyber forensic analysts
3. Legal Consultants
4. Security Guards
5. IT Specialists

Senior Digital Forensics Analyst (Team Lead)

- As a Senior Digital Forensics Analyst (Team Lead), you will serve as the digital forensics team's primary point of contact and leader, overseeing all aspects of forensic investigations and operations. With your significant experience in digital forensics, you will lead and train a team of analysts, directing them through detailed examinations of digital devices and networks to unearth evidence of cybercrime and security breaches. You will also be responsible for managing the team's workload, prioritizing assignments, and ensuring that forensic services are delivered on time and accurately. Working collaboratively with management, you will help design strategic objectives, policies, and processes to improve the effectiveness and efficiency of the digital forensics team.
    - Qualifications:
        - A bachelor's or master's degree in computer science, digital forensics, cyber security, or a related profession.
        - A minimum of 10 years of experience in digital forensics, including demonstrated leadership skills.
        - Experience with forensic analysis tools such as EnCase, FTK, X-Ways, and open-source forensic tools.
        - Strong knowledge of file systems, operating systems, and network protocols.
        - Certifications including CISSP or CASP

<u>Cyber forensic analysts</u>

- As a Cyber Forensic Analyst, you will be responsible for examining and evaluating digital evidence relating to cybercrime and security issues. Using your knowledge of digital forensics and cybersecurity, you will conduct detailed inspections of digital devices, networks, and systems to identify and mitigate security concerns. Your duties will include gathering, conserving, and evaluating digital evidence, documenting results, and giving expert testimony in judicial processes. You will also work with cross-functional teams to support incident response operations, conduct threat intelligence analysis, and create plans to improve cybersecurity posture. Your analytical abilities, technological proficiency, and commitment to maintaining the highest levels of integrity will be critical in protecting digital assets and managing cyber risks.
  - Qualifications
    - A bachelor's or master's degree in computer science, digital forensics, cyber security, or a related profession.
    - A minimum of 2 years of experience in digital forensics, including demonstrated leadership skills.
    - Experience with forensic analysis tools such as EnCase, FTK, X-Ways, and open-source forensic tools.
    - Strong knowledge of file systems, operating systems, and network protocols.
    - Certifications including CFCE, EnCE, or CCE

<u>Legal Consultants</u>

- As a Legal Consultant for the Forensic Lab, you will give expert legal advice and support to ensure that all forensic activities and procedures are in accordance with applicable laws, regulations, and standards. You will provide advice on evidence collection, preservation, analysis, and presentation in legal processes, drawing on your knowledge of digital forensics, cybersecurity, and legal requirements. Your responsibilities will include examining forensic techniques, protocols, and reports to assure legal compliance, advising on complicated legal matters, and representing the lab in legal actions as needed. You will also stay up to date on evolving legal developments and industry best practices, making recommendations to improve compliance and reduce legal risks. Your contributions will be crucial in maintaining the integrity, admissibility, and legality of forensic activities.
  - Qualifications
    - A Juris Doctor (JD) degree from an authorized law school and admission to the bar in the applicable jurisdiction.
    - A minimum of 1 years of legal experience, preferably in digital forensics, cybersecurity, or a similar field.
    - Knowledge of rules, regulations, and standards governing digital forensics, cybersecurity, and electronic evidence.
    - Excellent analytical, problem-solving, and communication abilities, as well as the ability to analyze complicated legal issues and deliver clear, practical advice.

Security Guards

- As a Security Guard, you will be in charge of ensuring the forensic lab facility's premises, personnel, and assets are safe and secure. Your primary responsibility will be to maintain a vigilant presence, prevent unwanted access, and respond quickly to security events or crises. In addition, you will conduct routine patrols, monitor surveillance systems, and implement access control measures to prevent security breaches. Your responsibilities will also include dealing with visitors, staff, and external stakeholders in a professional and courteous manner. Maintaining a safe environment helps to preserve sensitive information, evidence, and equipment located in the lab facility.
    - Qualifications
        - High school diploma or equivalent; extra training in security or law enforcement is recommended.
        - Proven background in security, law enforcement, or a related profession. Strong observation and surveillance abilities, with a sharp eye for detail.
        - Excellent communication and interpersonal skills, as well as the ability to work professionally with a varied range of people.
        - Physical fit and has the capacity to stand, move, and patrol for long periods of time.
        - Knowledge of security processes, protocols, and emergency response methods.

IT Specialists

- As an IT Specialist at the forensic lab, your responsibilities will include administering and maintaining the lab's IT infrastructure, systems, and software applications. Your major goal will be to guarantee that all IT resources run efficiently and securely, hence helping the forensic analysis and investigation procedures. You will work with forensic analysts, security specialists, and management to determine IT requirements, develop solutions, and resolve technical issues. In addition, you will be responsible for maintaining compliance with industry standards, legislation, and best practices for IT security and data protection.
    - Qualifications
        - Bachelor’s degree in Computer Science, Information Technology, or a related field; relevant certifications (e.g., CompTIA, Cisco, Microsoft) preferred.
        - Minimum of 2 years of experience in IT support, administration, or a related role, with a focus on cybersecurity or digital forensics preferred.
        - Proficiency in administering Windows, Linux, and/or macOS operating systems, as well as virtualization technologies.
        - Experience with network administration, including TCP/IP, DNS, DHCP, VLANs, and VPNs.
        - Strong knowledge of cybersecurity principles, practices, and technologies, including firewalls, intrusion detection/prevention systems, and encryption.

Reference

Computer Forensics: Operating System Forensics [updated 2019]. Infosec. (n.d.). https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-operating-system-forensics/

ISO/IEC 17025 - testing and Calibration Laboratories. ISO. (2020, March 11). https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html

Steps to obtain a DOD 8570 baseline certification. DoD Cyber Exchange. (n.d.). https://public.cyber.mil/wid/dod8140/dod-approved-8570-baseline-certifications/

Written by Steven Bowcut – Last updated: January 16. (2024, January 16). *In-demand Digital Forensics Certifications*. Cybersecurity Guide. https://cybersecurityguide.org/programs/cybersecurity-certifications/digital-forensics/