Digital Forensics Midterm Paper

Chandler Anderson

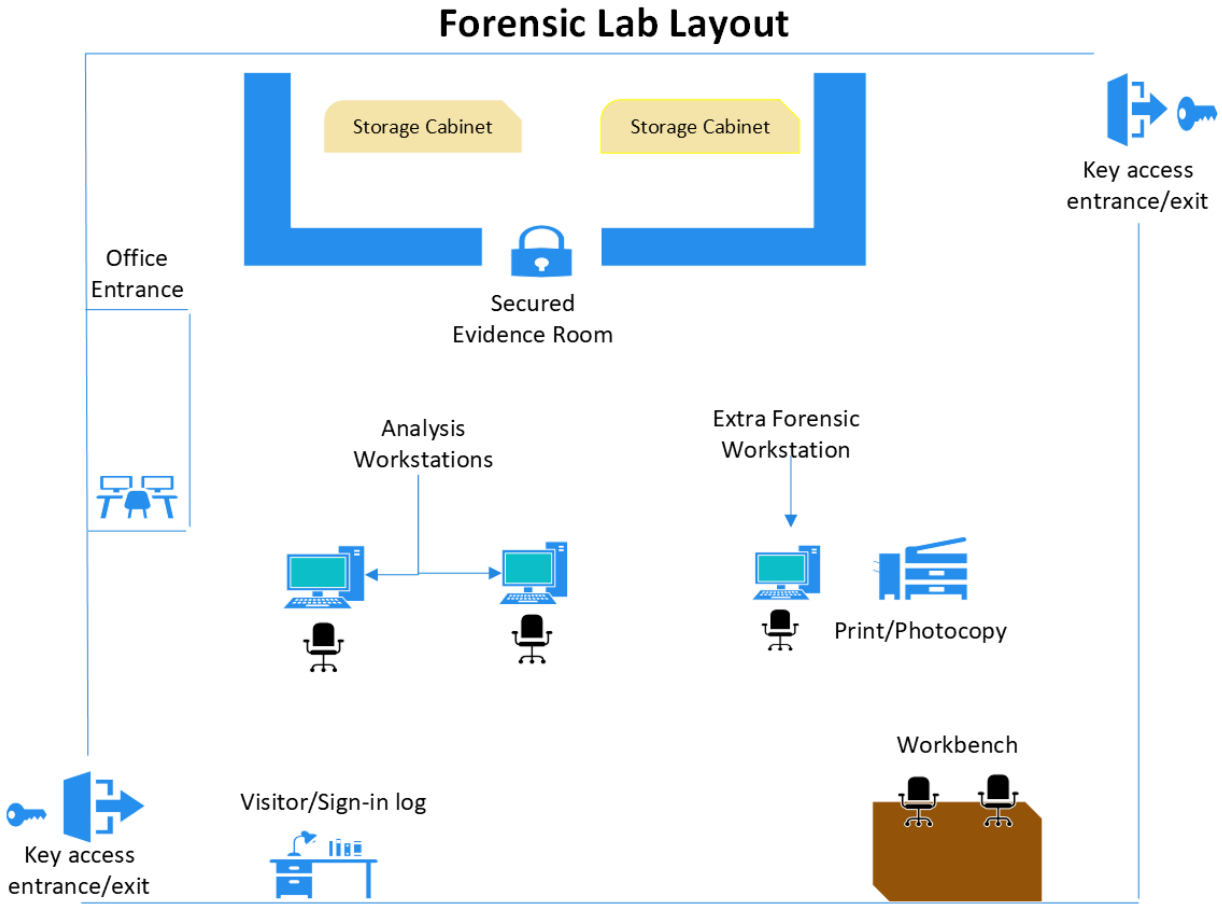
Department of Cybersecurity

CYSE 407: Digital Forensics

Professor Bechard

11/1/2024

Lab Diagram


Forensic Lab Layout
Storage Cabinet
Storage Cabinet
Key access entrance/exit
Office Entrance
Secured Evidence Room
Analysis Workstations
Extra Forensic Workstation
Print/Photocopy
Workbench
Visitor/Sign-in log
Key access entrance/exit

Inventory

- 1 Secure Storage Room: Must be accessed through a badge or key card
- 2 Medium Size Storage Cabinets: File cabinets with 5 drawers, 5-10 cases per drawer, and 20-40 cases between each drawer.
- 2 Physical Key Accessed Entrance/Exit
- 2 CCTV Cameras, one near each entrance and Exit
- 1 Visitors Log Desk: Ensure all visitors are logged in with the date, time in, and time out.
- 1 Office with a forensic workstation, MacOS, and 4 laptops
- Licensed Copies of Legacy Windows and MacOS Systems.

- 1 Workbench for placing and utilizing necessary hardware and other tools
- 1 Windows Analysis Workstation: Workstation equipped with Windows 11 OS, Bitlocker, FTK, and EnCase
- 1 Kali Linux Analysis Workstation: Workstation equipped with Kali Linux OS, Wireshark, Autopsy, and dd
- 4 Write Blockers
- 1 Additional Forensics workstation
- 1 Photocopier/Printer
- 5 External Hard drives
- 10 SATA and USB devices
- 2 Trash Containers- one for sensitive material, one for unrelated investigation items

- 4 Antistatic pads- one for each workstation.

Lab Accreditation Plan

To prepare for accreditation, the following documents should be acquired:

- Copy of the international standard, ISO 12020 for Inspection
- ANAB Accreditation Manual for Forensic Laboratories, Forensic Inspection Bodies, and Property and Evidence Control Units (Document MA 3033)
- Application Documents

Assessment Team: ANAB will appoint a team leader to be the sole assessor and oversee each area of assessment.

Logistics: An assessment Activity Plan will be given which will cover the scope of the assessment, assessment dates, and other important information. All team members will be required to review the plan in order to best prepare for assessment.

Document Review: A document review will ensure that the lab conforms to accreditation standards. All necessary documents should be on hand or available electronically.

Objective Evidence Evaluation: Assessors will evaluate individual ability to perform authorized tasks. This will ensure that all individuals are within standards for Evidence Collecting, Preservation, and quality management procedures.

Interviews will be conducted on document review and procedures on witnessing. The lab manager shall ensure that all staff are fully prepared.

Accreditation Certification: Once accredited, a Certificate of Accreditation will be provided which includes a unique number and date of expiration.

Continuous Improvement: Upon Accreditation, a plan for continuous learning and improvement will be developed, ensuring the necessary standards are upheld.

Lab Maintenance Plan

The safety and health of lab personnel is a main priority, and the lab should be maintained in a way that upholds all safety concerns. Any visible damage to any area of the lab should be reported and cleaned or repaired immediately. All maintenance personnel are to be escorted in and out of the digital forensics lab. Maintenance crews will be required to sign in and out of the visitor log and should always have at least one authorized member around. To avoid static electricity from computers and other electronics, antistatic pads shall be placed at all workstations. Any carpeted area should be cleaned once a week to ensure that no dust is built up near workstations.

Disaster Recovery Plan: A disaster recovery plan should outline how to recover workstations in case of any data loss or contamination from a virus or other form of malware. System backups should be easily accessible, and duplicate backups should be stored off-site

Configuration Management and Backups: Ensure all patches and OSs are up to date to ensure security and efficiency. Log all updates in a configuration management database to ensure compliance with lab policy. Workstations should be backed up at least once a week to ensure restoration in case of disaster.

Staffing

The ANAB website holds guidelines and requirements for managing a digital forensics lab, handling and analyzing digital evidence, standards for lab personnel, and other lab management guidelines.

Roles of the Lab Manager: The lab manager will perform regular managerial tasks, such as assuming responsibility for all lab needs, upholding ethical standards, creating lab plans, and ensuring the necessary hardware and software are accessible. The manager creates and enforces lab policies to ensure safety and efficiency for all staff in the workplace. The manager is also responsible for developing a quality assurance plan, including but not limited to what to do when a case arrives, guidelines for filing reports, who is and is not authorized to enter the lab,

Roles and Requirements of Staff: Bachelor's degree in digital forensics, cybersecurity, computer science, or related technology field required. Though certifications are not required for entry-level roles, the IACIS Certified Forensic Examiner (CFCE) is preferred, and all staff are expected to continue learning and pursuing certifications.

Staff within the workplace are expected to have the necessary knowledge of computer hardware, software, digital forensic practices, and procedures. This includes knowledge of collecting and assessing evidence, storage of evidence, copying and viewing drives, and experience with

imaging software. maintaining chain of custody and preparing required reports. Staff should also be expected to participate in continuous learning and should be encouraged to pursue vendor certification and training.

Staff Certification/Continued Learning Requirements: Other certifications that are encouraged for all staff include: Certified Computer Crime Investigator, Basic, and Advanced, Certified Computer Forensic Technician, Basic, and Advanced, Encase Certified Examiner Certification, ECCouncil, etc.

Bibliography

ACCREDITATION MANUAL FOR FORENSIC SERVICE PROVIDERS. (202.). https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=7183

Guide to Computer Forensics and Investigations, 6th Edition - 9781337568944 - Cengage. (2020). Cengage.com. https://www.cengage.com/c/guide-to-computer-forensics-and investigations-6e-nelson/9781337568944/

Popular Computer Forensics Top 21 Tools [Updated for 2019]. (2019, February 17). Infosec Resources. https://resources.infosecinstitute.com/computer-forensics-tools/