Accreditation Plan

To be accredited for the International Standard ISO/IEC 17025:2005, a digital forensic lab must apply for the "General Requirements for the Competence of Testing and Calibration Laboratories" document and provide evidence of ownership of this document prior to applying for accreditation. This plan will use the ANAB and ISO 17025:2005 standards for accreditation. ANAB accredits and assesses organizations (i.e., conformity assessment bodies or "CABs") to certain domestic and international requirements, standards, and programs. A CAB that delivers the covered services has the ability to partake in one or more of the ANAB accreditation programs, which would allow it to demonstrate that its technical operations and overall management system align and conform to the requirements for accreditation that is defined by ANAB.

For CABs seeking or looking to maintain their accreditation, ANAB's accreditation services study the effectiveness and competence of the overall management system within the CABs. For a CAB to achieve and maintain accreditation, it must demonstrate its ability to perform the necessary tasks, have an effective management system, and have conformance with all the applicable requirements in the specific program that it is seeking accreditation for. The requirements also include the CAB's compliance to its own internally documented management system. If ANAB determines that a Program requirement does not apply to the work conducted by the CAB, the requirement will be deemed "not applicable" during the assessment activity.

Access to the ANAB accreditation program documents is provided on ANAB's website at www.anab.org, and it is encouraged that the CAB reviews all documents relevant to the program that it seeks accreditation for. ANAB will also notify accredited and applicant CABs when there are changes to an ISO/IEC standard or ANAB accreditation Program Requirement or Requirements, such as the accreditation manual, requirement documents, and the ANAB's Terms and Conditions for Accreditation. However, the CAB is responsible for reviewing other related forensic accreditation documents posted on www.anab.org to ensure that it is using the most up to date version. Regarding the CAB's preparation for an assessment, a required part of it is the determination and documentation by the CAB that it meets all applicable accreditation requirements. ANAB requires several actions prior to application for accreditation in order to make this determination. Any CAB preparing for ANAB accreditation should possess the most current version of the following documents:

- A licensed copy of the international standard, if applicable to the Program for accreditation (e.g., ISO/IEC 17025 for testing/calibration, ISO/IEC 17020 for inspection)
- Accreditation scheme Requirements (AR 3125 for testing/calibration, AR 3120 for inspection, AR 3181 for property and evidence control units)
- Application and draft scope documents
- The MA 3033 accreditation manual
- If applicable, additional requirements such as the FBI Quality Assurance Standards, ABFT Forensic Toxicology Laboratory Accreditation Checklist, MD OHCQ).

After the results of the assessment activity, the resolution of all nonconformities, reviewing of the supporting records, and any other relevant information provided will be reviewed by an Accreditation Manager, with the accreditation decision will be made by the Vice President or designee. Accreditation will be limited to the disciplines where the CAB was determined to be competent by the assessment team.

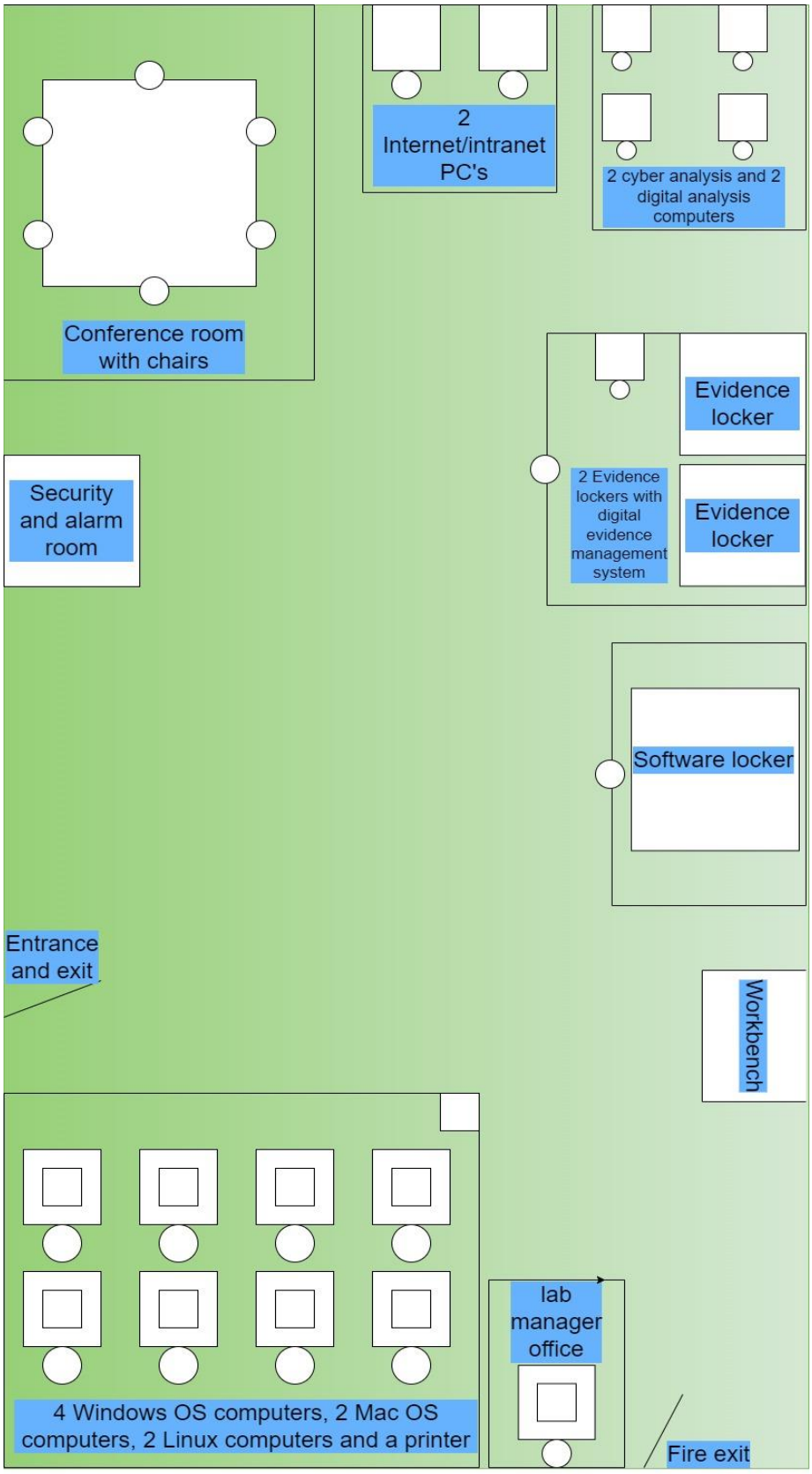
INVENTORY

Hardware, Software, and Materials

- Large Secure storage room with ordinary safe
- 2 large evidence storage containers in the storage room with 5 shelves (1 for media safe)
- 17 Desks and 12 chairs
- Workbenches
- 1 large table
- 11 medium sized tables
- 5 small tables
- 1 workbench
- Fire exits and sprinkler system.
- 4 combination locks
- 20 CAT cables
- 20 SATA cables
- 20 IDE cables
- RAM – 10 GB
- Quad core CPUs
- 2 analysis computers
- 10 computers with at least 2 that have internet access
- 10 mice and keyboards
- PC power chords
- 10 Large monitors or dual monitors
- Digital camera with recording features
- Printers
- Antistatic pads
- Separate trash bins, one for sensitive material, one for items unrelated to the lab.
- IDSN telephone system
- Network equipment (switch, router, etc.)
- Onboard sound and graphics
- Mobile Acquisition Bundles

- USB 1 and 2
- DVD/CD-RW
- Cable tester
- OSForensics
- Kali Linux
- Wireshark
- Helix pro
- AccessData FTK
- XRY
- CAINE
- AidMail
- Autopsy
- PuTTY
- WinSCP
- Microsoft Office (including current and older versions)
- Hexadecimal editor, such as WinHex or Hex Workshop
- Programming languages, such as Visual Studio, Perl, or Python
- Specialized image viewers, such as Quick View, ACDSee, ThumbsPlus, and IrfanView
- WPS Office, WordPerfect, and a third-party or open-source office suite
- Accounting applications, such as Quicken and QuickBooks
- A digital camera capable of still and motion recording
- Assorted antistatic bags.
- 5-10 computer chairs
- Fluke Network Cable Tester
- Spectrum Analyzer
- An external CD/DVD drive
- 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
- Ribbon cables for floppy disks
- Extra USB 3.0 or newer cables and SATA cards and associated cables
- Extra SCSI cards
- Graphics cards, both Peripheral Component Interconnect (PCI) and Accelerated
- Graphics Port (AGP)
- Assorted FireWire and USB adapters
- A variety of 20 hard drives and USB drives
- At least two 2.5-inch adapters from notebook IDE hard drives to standard IDE/
- ATA drives, SATA drives

Floor plan


2 Internet/intranet PC's
2 cyber analysis and 2 digital analysis computers
Conference room with chairs
Evidence locker
Security and alarm room
2 Evidence lockers with digital evidence management system
Evidence locker
Software locker
Entrance and exit
Workbench
lab manager office
4 Windows OS computers, 2 Mac OS computers, 2 Linux computers and a printer
Fire exit

Physical Security measures

- Security Staff and proper training for said staff.
- Visitors log for anytime anyone accessed the lab and when they exited the lab.
- Control Access Systems and limited access to who has authorization to enter the lab and various sections of the lab.
- Locks on every door with high security codes and other methods that require authorization.
- Lockable windows and other passageways in the lab.
- A limited number of windows within the lab and on the section of the building or the building itself where the lab is present.
- Alarm system in place to notify when an attempted unauthorized entry or any other attempted unauthorized access to tools within the lab occurs.
- Hardened doors, frames, and locks.
- Perimeter walls extending from the floor to the ceiling to prevent access from one area to the other over a drop ceiling.
- Surveillance video cameras
- Disabling of the ports within a system when the system is not in use.

Staff Roles and Responsibilities

Lab Manager: The lab manager will be tasked with the responsibilities below:

- Overseeing of the collection, examination, analysis, and reporting of the data and evidence.
- Overseeing of any other events that occur within the digital forensics laboratory and ensuring that they are carried out in an effective and safe manner.
- The creation of a lab policy for the staff
- Overseeing of the scheduling of the lab staff.
- Supervision of the lab staff.
- Maintaining the lab's equipment.
- Ordering supplies when necessary.
- Making sure the lab complies with accreditation standards.
- Overseeing all software and security documentation.
- Ensure that any information and data within the lab is secure.
- Ensuring the lab itself is completely secure.

Lab technician: The lab technician will be tasked with the responsibilities below:

- Performing forensic examinations on digital electronic devices, which can include computers, mobile devices, USB flash drives, hard drives, SSDs, and any other digital data storage media.
- Forensically examine any digital evidence that has been discovered on the associated device.
- Oversee maintaining the network infrastructure, software, and hardware within the lab.
- Notifying the lab manager if there are any security concerns, events, or other issues that are of concern.
- Assisting law enforcement and any other legal entities by providing support in the examination and the digital investigation processes.
- Prepare and distribute comprehensive reports that detail the examination results to law enforcement and any other legal entities.

Forensic Examiner: The Forensic Examiner will be tasked with the responsibilities below:

- Arriving to the crime scene to investigate and gather any relevant digital evidence and devices.
- Forensically collect any other evidence that may be relevant to the crime.
- The preservation of the evidence for it to be returned to the lab for further investigating.
- Recording any observations noticed at the crime scene and any other relevant information that may be of benefit to the lab and law enforcement.
- Use specialized methods and tools to extract evidence from devices.
- Be able to trace the evidence to its origin.
- If necessary, testify in court about what methods and procedures were used to obtain the data for the investigation.

Data Analyst: The Data Analyst will be tasked with the responsibilities below:

- Perform digital forensic analysis of evidence and research and development within the current laboratory requirements.
- Ensure that as little data as possible is lost throughout the analysis and recover data if necessary.
- Provide a summary of findings that align with the labs current reporting procedures.
- Discover trends that may arise within cybercrime and trends that may identify potential sources of forensic information and techniques.
- Assist with the acquiring of digital evidence from onsite crime locations.
- Develop software and hardware solutions to aid the laboratory operations.

Cybersecurity Analyst: The Cybersecurity Analyst will be tasked with the responsibilities below:

- The configuration of tools such as password protectors, vulnerability management software, and virus software.
- Use specialized knowledge to help maintain network and IT infrastructure security.
- Help prevent any vulnerabilities from forming within the network and IT infrastructure.
- Anticipate and prevent any attacks from occurring that could harm the lab and the digital environment.
- Reading and making a report of the network status and evaluate the health of the network.
- Indicate if there is any unusual activity detected in the network.
- Help gather and examine the digital evidence and work with the lab manager and the lab technician.

Forensic Lab Accountant: The Lab Accountant will be tasked with the responsibilities below:

- Collaborate with the lab manager and digital forensics specialists to recognize financial crimes such as fraud, embezzlement, and money laundering.
- Plan and coordinate and work with the lab manager in directing the examination of any financial data or information associated with the investigation.
- Examine any financial transactions and records that are associated with the cybercrime.
- Produce detailed financial investigative exhibits, such as briefings, and financial reports.

Definitions:

These are abbreviations used within the lab.

ANAB - The ANSI National Accreditation Board
CAB – Conformity Assessment Body (a testing and calibration laboratory)
DEMS – Digital Evidence Management System
DFS – Department of Forensic Science

Maintenance Plan

The lab manager will be the main individual responsible for maintenance and upkeep of the lab and the equipment. The lab will need to be maintained at all times in order to ensure the safety and health of lab personnel, and to ensure that all of the tools, devices, and equipment are safe to use and are functioning properly. When our lab equipment has a malfunction, we will attempt to repair or refurbish the equipment or the affected parts before disposing of the equipment. Equipment may also just need to be properly updated, and in this case, we will do so before disposing of the equipment.

The tasks to be carried out to ensure upkeeping of the facility include:

- Reviewing visitor and entrance logs to determine if the logs are being used with the proper information being recorded.
- Reviewing log sheets and the DEMS for evidence containers to determine if or when they have been accessed and when they were locked.
- Any evidence not being processed needs to be locked in a safe and secure container.
- All equipment, tools, software, used by digital forensic lab personnel must be tested and validated each time the equipment, firmware, and software are upgraded, reinstalled, or modified in order to confirm that they are operating as intended to and are producing valid and accurate results.
- If there is a malfunction within a device or equipment, the lab manager is to contact the proper entity or entities for repairing or the ordering of new equipment/devices.
- Floors and carpets are to be cleaned at least once a week if not every 5 days to help minimize dust and other ways that can cause static electricity.
- Machines are to be wiped at least twice a week.
- Antistatic pads are also to be placed around the electronic workstations and workbenches to help combat static electricity.
- Inspection of doors to make sure they close and lock correctly.
- Further inspection of locks on any containers, and if locks on doors or containers are faulty in any way, they will need to be replaced as soon as possible.
- Separate trash containers will be needed and will need to have the material it may contain disposed of in a safe and orderly fashion. We will need one of the bins to store items unrelated to the lab, and the other for sensitive material that requires special handling to make sure it’s destroyed.
- The lab manager and a commercially bonded firm will handle the sensitive material. Routine inspections of the lab will also be a necessity to help ensure that there is proper upkeep within the facility.
- Thorough inspection needs to be conducted of the lab’s ceiling, floor, roof, interior and exterior walls at least once a month.

Calibration Plans

We will regularly calibrate equipment for ongoing preventative maintenance that will help keep our devices, equipment, and lab itself performing in optimal condition. Calibration of the equipment within the lab is to be done at least once a month. However, if an electronic device or equipment appears to be acting abnormally, or has been physically damaged in any capacity, a calibration test is expected to be performed immediately. Furthermore, calibration will be performed before large major projects, and after the major projects. Calibration will help the lab by:

- Saving Money – When we do not properly calibrate, it can be very costly and time consuming, as a machine that has not been calibrated in a recent time period, has a much higher chance of experiencing a malfunction, error, or outright producing inaccurate results.
- Maintaining certification/accreditation – In order to maintain our proper status as an accredited lab, we need our equipment, tools, and devices to be in proper working order and have the ability to display proper information and readings.
- Maintain the life of our equipment and tools – Equipment that is improperly calibrated, especially over an extended period of time, can experience a malfunction or an error, as mentioned under the saving money section. Maintaining and keeping our equipment calibrated is a key part of maintenance as well.

Bibliography

Cannon, Marcus. “Laboratory Equipment Maintenance 101.” *MyNewLab*, InterFocus Ltd, 20 Aug. 2020, https://www.mynewlab.com/blog/laboratory-equipment-maintenance-101/.

“Measure for Measure: What Is Calibration and Why Is It Important for Your Lab?” *SensoScientific*, SensoScientific, 25 Jan. 2019, https://www.sensoscientific.com/blog-whats-calibration-why-important-labs/#:~:text=In%20the%20context%20of%20lab,and%20adjusting%20for%20that%20difference.

“Laboratory Security.” *Environmental Health and Safety*, Stony Brook University, 2023, https://ehs.stonybrook.edu/programs/laboratory-safety/laboratory-security/index.php.

“Digital Forensic Examiner - FBIJOBS.” *FBIjobs.gov*, FBI, May 2022, https://fbijobs.gov/sites/default/files/2022-05/Digital%20Forensic%20Examiner.pdf.

“Job Descriptions.” *Job Descriptions | Career Opportunities*, NEOGOV, 2023, https://www.governmentjobs.com/careers/hillsboro/classspecs/862521#:~:text=Conducts%20forensic%20examination%20of%20electronic,other%20digital%20data%20storage%20media.&text=Uses%20software%20and%20hardware%20forensic,for%20further%20investigations%20or%20testing.

“What Does a Cybersecurity Analyst Do?” *Western Governors University*, 30 Apr. 2022, https://www.wgu.edu/career-guide/information-technology/cybersecurity-analyst-career.html#:~:text=What%20Is%20a%20Cybersecurity%20Analyst,anticipate%20and%20prevent%20these%20attacks.

“Career on the Rise: How to Become a Forensic Accountant.” *Franklin*, https://www.franklin.edu/blog/accounting-mvp/how-to-become-a-forensic-accountant#:~:text=Forensic%20accountants%20act%20as%20financial,in%20civil%20and%20criminal%20investigations.

Nelson, Bill, et al. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. 6th ed., CENGAGE LEARNING, 2018.