Digital Forensics Laboratory Proposal

John Wilson

Old Dominion University

CYSE 407 Digital Forensics

Professor Bryan Bechard

16 October 2022

Digital Forensics Laboratory Proposal

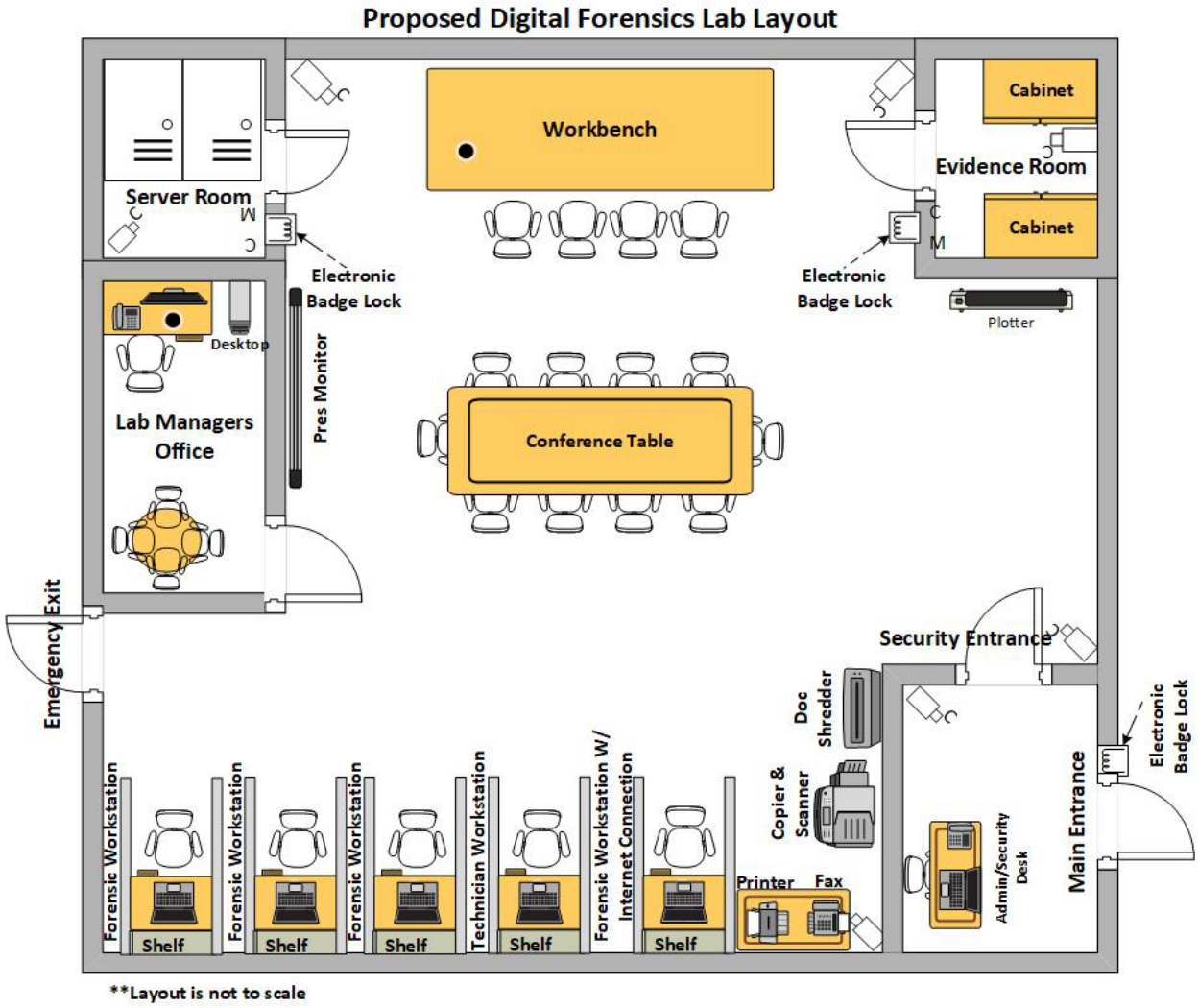
Introduction

This paper is a proposal to build, utilize, and the upkeep of a state-of-the-art digital forensics laboratory that will provide investigative and scientific analysis information from the processing of digital evidence. The digital devices processed in this laboratory include but are not limited to computers, tablets, cell phones, smart phones, personal digital assistants (PDA), external and internal hard drives, digital video and still cameras, and any mechanism deemed to capture, store, or transmit electronic information. The proposal will utilize the document ISO/IEC 17025:2017 as a guideline to assist in standardizing the laboratory setup process. ISO/IEC 17025:2017 is an internationally recognized document used as the standard to set up a forensics laboratory for accreditation and self-assessment purposes so customers will have confidence the laboratory will provide competent and impartial forensics data analysis results.

Accreditation Plan

This lab will follow the accreditation guidelines set forth by the ANSI-ASQ National Accreditation Board (ANAB) and the American Society of Quality (ASQ) for the labs processing of digital evidence to ISO/IEC 17025 laboratory accreditation requirements. The accreditation includes the calibration and testing of the laboratory to be able to certify that the lab equipment and procedures are trustworthy to process evidence from digital media. Without the lab receiving a national qualification standard the evidence produced from this facility would be inadequate and likely contested as illegitimate.

Forensic Laboratory Floor Plan



Inventory

Proposed Lab Inventory			
Software	**Hardware/Equipment**	**Work Bench Tools**	**Supplies**
Operating systems (Windows, Apple, Kali Linux)	Laptop	Hammer	CD-R's/DVD-R's/Blueray-R's

Proposed Lab Inventory			
Forensic Utility software (Disk imager, Network analyzers, Forensic suites, etc.)	Desktop	Screwdrivers	Magnetic Tapes (all sizes)
Write Blocking Software	CPU (latest Intel or AMD)	Drill	Printer paper
Mouse Jiggler (keeps live computer from going to sleep)	Monitors	Drill bits	Badge ID
Anti-virus software (McAfee, Norton, Bit Defender, etc.	USB 1.0 -3.0 Drives	Channel locks	Plastic bags
System ghosting software	CD/DVD/Blue ray-R/RW Drives	Vice	Labels
Microsoft office suite	TEMPEST Shielding	Vice Grips	Printer cartridges
Accounting software	Internal Hard drives (HDD and SSD)	Duckbill pliers	Pens/pencils/highlighters
Programming software (code blocks, visual studio, etc)	External Hard drives (HDD/SSD)	Wire Cutters	Paper
	SATA Cables	Voltage meter	Scotch tape
	Printers	Continuity meter	Staples and stapler
	Fax Machine	Soldering iron	
	Document shredder	Work Bench Magnifying Lamp	
	CD/DVD/Blue ray shredder	Protective Eye Wear	
	Graphics Cards	Gloves	
	Sound Cards	Workbench Apron or Lab coat	
	RAM (Maximize the motherboard will take)		

Proposed Lab Inventory			
	Hardware write blocker		
	Floppy disk drives		
	Magnetic tape drives		
	Hard drive imagers (Ditto x86 SE)		
	HotPlug field kit (transports computers without shutting them down)		
	Hard drive eraser		
	Data Diode (moves data to secure network)		
	Anti-Static storage boxes (for transportation and storage)		
	USB and SATA docks		
	Internal/External Network Servers		
	Electronic storage (SAN/NAS/or RAID)		
	Network Equipment (routers, switches, firewall, Cat 6 ethernet cables)		
	Network cards		
	Misc Data cables (to pull data from latest and old electronic equipment like PDA, generation 1 iPod, etc.)		
	Faraday bags (block cellphone communications)		
	Misc Power cables (for powering up misc electronic equipment new and old)		

Proposed Lab Inventory			
	Misc phone data cables		
	CCTV Security Cameras		
	Badge ID maker		
	Mouse		
	Keyboard		

Maintenance Plan

Integrity of the lab and evidence is paramount therefore the lab will be maintained at all times for cleanliness and safety. If anything is damaged or broken it will be reported immediately to the lab manager for repair as soon as possible. Cleaning of the facility is also vital and will be conducted weekly by a trusted and vetted third party that is an expert in lab cleaning procedures. The cleaning crew will be supervised and escorted into and out of the lab by security. All trash will be empty or destroyed nightly according to lab policies and procedures.

Scope

The below information are the recommended best practices and procedures for the building and maintaining of a medium sized Digital Forensics Laboratory.

Roles and Responsibilities

Laboratory Manager

Is a subject matter expert in digital investigation and laboratory procedures. Is responsible for budgeting; managing resources; staff hiring and performance monitoring; create procedures and policies for evidence chain of custody and inner workings (processes and procedures) of the lab; lab employment descriptions, supervise ongoing cases, liaison with law enforcement or other clients, procurement of all lab equipment, attend internal and external meetings as the digital lab representative, and be an expert witness in court if called upon.

Asst Laboratory Manager/

Is a subject matter expert in digital investigation and laboratory procedures and is the second person in charge of the lab and will administer the duties of the laboratory manger when called upon. The Asst Manager will have expert knowledge of the technology to examine all data evidence collected for analysis through the use of up-to-date forensics software, hardware, tools, and other miscellaneous equipment. The examiner will possess excellent communication skills to effectively explain the technical process of who, how, what, when, and where evidence was collected to the customer through standardized report templates, spreadsheets, and briefings. In addition, the examiner will also be required to know and adhere to the chain of custody requirements, adhere to current laboratory procedures, and be an expert witness in court if called upon. In addition, this position will also work with an intern to help train a future digital forensics examiner.

Forensics Analyst/Examiner

The Forensics Analyst/Examiner will have expert knowledge of the technology to examine all data evidence collected for analysis through the use of up-to-date forensics software, hardware, tools, and other miscellaneous equipment. The examiner will possess excellent communication skills to effectively explain the technical process of who, how, what, when, and where evidence was collected to the customer through standardized report templates, spreadsheets, and briefings. In addition, the examiner will also be required to know and adhere to the chain of custody requirements, adhere to current laboratory procedures, and be an expert witness in court if called upon.

Forensics Analyst/Examiner (intern)

This is an entry level position for learning about the digital examiners process. The position will have introductory knowledge (experience through colleges, universities, or other accredited training programs) of how to examine electronic devices using the most up-to-date forensics software, hardware, tools, and other miscellaneous equipment. The intern will not be allowed to work on cases alone but will assist on active cases with supervision by the asst lab manger. Intern should be able to communicate effectively, work under pressure, meet time sensitive deadlines,

Lab Technical Technician

The lab technical technician is the subject matter expert in the technical side of the lab. The position will keep all lab equipment up to date, patching software as required, assist in calibrating any sensitive equipment, knowledge of networking troubleshooting and solutions, maintain maintenance on lab equipment, fix or replace electronic equipment (computers, monitors, networking equipment), and help assist examiners or other jobs as necessary.

Administrative Assistant

The administrative assistant will perform a variety of general secretarial, clerical, and administrative support functions and processes in support of lab personnel. These processes may include data entry, proofreading/editing lab reports, and processing of lab documents and records. The position should know how to use standard office equipment and software (copier, scanner, phones, fax machine, computer, Microsoft office suite or other office software). In addition, this position will also be responsible for checking badges at the front door as an extra layer of security to validate that only the people who have access are allowed inside the facility.

Maintenance Practices

The lab manger will create a maintenance policy that will spell out the labs maintenance schedule to keep the lab equipment up to date and from falling into disrepair. The policy should list all of the sensitive equipment and a schedule for the equipment to be updated (software), repaired, cleaned, replaced, or recalibrated. In addition, the policy should implement a report that keeps track of date, name of equipment, type of maintenance, and who conducted the maintenance.

Calibration Procedures

The lab manger will create a calibration procedure policy that will spell out the labs calibration procedures to keep the lab equipment in pristine condition. The policy should list all of the sensitive equipment that requires calibration, schedule for the equipment to be updated (software), repaired, cleaned, replaced, or recalibrated, and list of vendors that can execute the calibration process. In addition, the policy should implement a report that keeps track of date, name of equipment, type of maintenance, and who conducted the maintenance.

Reference Standards, Certified Reference Materials, and Reference Materials

The following are accepted certification standards for digital forensics examiners:

- Certified Forensic Computer Examiner (CFCE) -
- Certified Cyber Forensics Professional (CCFP)
- High Tech Crime Network (HTCN)
- Encase Certified Examiner Certification
- AccessData Certified Examiner
- Or other certified training that is accepted.

Preventive Maintenance

The laboratory manger will create a preventive maintenance policy that regularly schedule preventive maintenance practices.

Corrective Maintenance

Any lab equipment that requires corrective maintenance will be completed as soon as possible. Equipment that requires corrective maintenance does not require calibration.

Performance Checks

Performance checked on necessary equipment will be conducted as required by the properly trained personnel.

Malfunctioning Equipment

If any equipment is considered malfunctioning, the equipment will either be replaced or repaired depending on budget and time constraints. If the equipment cannot be repaired or replaced in a timely manner than the case could be pushed out to a vetted and reputable vendor that can process the case.

Equipment Security

The lab will have an electronic badging system with a keypad that will track and allow access to the facility. In addition, once inside the front door, the administrator will check the badge with the individual to make sure the person allowed access to the facility has the proper clearance. Once they have been vetted, the administrator will unlock the second door that will allow access to the facility. Additionally, the evidence rooms and the server rooms will also be secured at all times with access bring granted by eligible personnel through an electronic badging system and keypad.

Security Cameras on a close circuit will also be used inside and outside the facility to monitor the labs activity. The digital camera feed will be saved to the servers inside the facility and also backed up to a cloud system in the case the servers go down. CCTV Cameras will also be located inside the server and evidence rooms and be operational 24 hours a day.

All equipment will be physical touched and counted on a biweekly basis to make sure that all equipment is accounted for. If any equipment is deemed missing, an investigation into the incident will commence immediately by a third-party vendor.

References

Aguilar, J., Barnes, T., Browne, J., Kennedy, A., Miranda, R., Williams, S., Burney, Y., Byrd, J., Carver, B., McClaren, J., McElroy, R., Denmark, A., Mount, M., Halla, S., Hartman, L., Mohr, K., Leben, D., Matheson, G., Sigel, S., & Smither, J. (2013). *Forensic science laboratories : handbook for facility planning, design, construction, and relocation*. https://doi.org/10.6028/nist.ir.7941

Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving. (1998). https://www.ojp.gov/pdffiles/168106.pdf

GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES INTERPOL For official use only. (2019). https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

Guide to Computer Forensics and Investigations Fourth Edition Chapter 3 The Investigator's Office and Laboratory. (n.d.). Retrieved September 24, 2022, from https://www.utc.edu/document/71881

Jones, N., Volzow, V., Bradley, A., & Samenkovic, B. (2016). *Digital Forensics Laboratory Management and Procedures Guide Global Action on Cybercrime From GLACY to GLACY+ GLACY Closing and GLACY+ Launching Conference Bucharest 26 th to 28 th*. https://rm.coe.int/16806b3058

Kaizen, S. (2015, December). *Computer Forensics Lab Requirements | BlueKaizen*. Bluekaizen.org. https://www.bluekaizen.org/computer-forensics-lab-requirements/

Mcdonald, S. (n.d.). *Building a Basic Computer Forensics Laboratory*. https://www.oas.org/juridico/spanish/cyber/cyb32_forensics_lab_en.pdf