Digital Forensics Lab

Clarence V. Kimbrell Jr.

Old Dominion University

CYSE 407 Digital Forensics

Professor Bechard

Summary

We have been hired to create and operate a brand-new digital forensics lab for a mid-sized police department. This plan will be in operation for the next 3 years until upgrades are needed. Digital forensics labs are a crucial element in today's cybercrime, particularly in the use of hacking tools to analyze evidence and potential threats in cases. The use of digital forensics labs has skyrocketed in the past 40 years, and some standards must be considered when creating a brand-new lab. The International Organization for Standardization and the International Electrotechnical Commission have developed guidelines that should be followed worldwide. These guidelines are called ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence (Introduction to Digital Forensics, 2019).

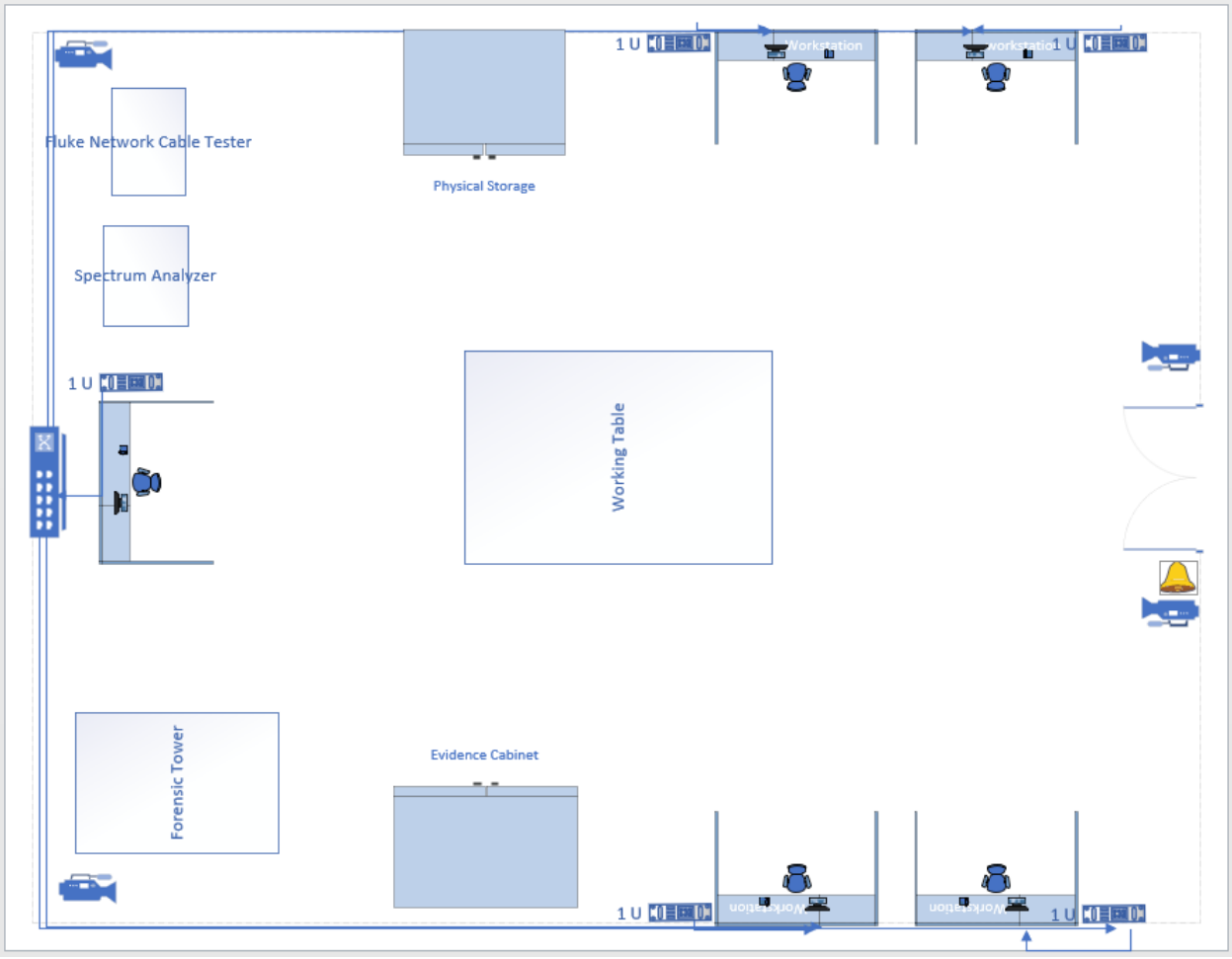
Accreditation Plan

For a digital forensics lab to obtain an accreditation certification it must follow the nine critical steps presented by the National Commission on Forensics Science. It is noted that one key outcome of preparing these steps is the "creation of a quality management system that is aligned with recognized technical and administrative requirements." (NCFS, n.d.). Improving the quality and reliability of forensic work and quality management can be achieved through this approach. These steps do not have to be done in order but all of them need to be implemented.

- Writing procedures for evidence
- Written Reports
- Technical and administrative review of reports and supporting records
- Testimony monitoring
- Note-taking

- Technical procedures
- Training program
- Proficiency testing
- Corrective and Preventive action process

Forensic Laboratory Floor Plan



Inventory

According to Howard Poston, an author for InfoSec, 8 essential tools need to be accounted for in a computer forensics lab.

- Disk and Data Capture tools
- File Viewers
- File Analysis tools
- Registry analysis tools
- Internet analysis tools
- Mobile Devices analysis tools
- Network Forensics tools
- Database forensics tools

Within this tool categories, we need programs such as

- Autopsy
- Sleuth
- X-Ways,
- AcessData FTK
- EnCase
- Mandiant RedLine
- Paraben Suite
- Bulk Extractor
- Registry Recon
- Volatility
- WindowsSCOPE
- Wireshark
- Network Miner

- Xplico
- Oxygen Forensics Detective
- Cellebrite UFED
- XRY
- CAINE
- SANS SIFT
- HELIX3

These are 19 software programs that will be incorporated into the lab. Now we will look at the hardware used.

- 5 computers (4 will be for workstations)
- PC Power Cables
- 20 IDE Cables
- 20 SATA Cables
- Cisco 3560 Switch
- 20 CAT 6E Cables
- Fluke Network Cable Tester
- Spectrum Analyzer
- Spare parts such as (RAM, Network Cards, Hard Disks, and Storage Devices)
- Forensics Tower
- Cameras
- Uninterrupted Power Supplies

Then we can gather other miscellaneous items.

- Computer Chairs
- Intrusion Alarm
- Large Desks
- Physical Storage Units
- Forensic workstation desks

Maintenance Plan

These practices establish calibration and maintenance requirements to ensure the accuracy and reliability of the computer forensics lab. The Laboratory Manager, Quality Assurance Liaison, or Laboratory technician will ensure that each unit maintains a record of instruments and equipment that require calibration. This record will include, at a minimum, the identity of the equipment and its software, the manufacturer's name, and type identification. Other maintenance practices include repairing any physical damage to lab equipment, escorting the cleaning crew to ensure reliability, and minimizing static electricity. Instruments and equipment will be properly maintained, and the Laboratory Manager or their designee will ensure that the maintenance plans are followed extensively.

Definitions

ANAB - ANSI- ASQ National Accreditation Board

ISO – International Standard Organization

IEC – International Electrotechnical Commission

Staffing/Responsibilities

The laboratory manager is responsible for scheduling lab and equipment time for employees. In some cases, laboratory managers have to purchase lab supplies and prepare order lists (Laboratory Manager, 2019). Lastly, laboratory managers handle security documents and 'ensure that all information collected is kept safe (Laboratory, 2019). This includes maintaining a sign-in log for visitors, issuing visitor badges, and hiring guards.

Laboratory technicians are described as individuals who collect, receive, label, or analyze samples and evidence. A critical takeaway for laboratory technicians is to ensure that safety guidelines are followed at all times within the digital forensics laboratory.

Finally, there is the Quality Assurance Liaison, whose job is to 'facilitate communications with scientists on quality assurance issues and requirements, which typically generates greater productivity in investigations' (Bolivar, 1993). It is also their responsibility to help the scientific community implement new regulations and requirements that fit the needs of the laboratories. This is helpful because there may be situations where an investigation is halted due to the lack of policies or regulations on a particular subject matter. The Laboratory Manager, Laboratory Technician, or Quality Assurance Liaison will enforce policies and conduct safe investigations into digital evidence.

Bibliography

Better Team Authors. (2020). *Lab technician job description*. Betterteam. Retrieved March 21, 2023, from https://www.betterteam.com/lab-technician-job-description

Bolivar, S. L., & Day, J. L. (1993, March 16). *The quality assurance liaison: Combined technical and quality assurance support*. NASA/ADS. Retrieved March 21, 2023, from https://ui.adsabs.harvard.edu/

Manu, K. K. (2017). *Cybercrime module 4 key issues: Standards and best practices for digital forensics*. Cybercrime Module 4 Key Issues: Standards and best practices for digital forensics. Retrieved March 21, 2023, from https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html

National Commission on Forensic Science. (2016). Recommendations and key measures for strengthening the practice of forensic science: A report to the Attorney General. U.S. Department of Justice. https://www.justice.gov/archives/ncfs/page/file/795111/download

Poston, H. (2021, May 27). *Popular Computer Forensics Top 19 Tools [updated 2021]*. Infosec Resources. Retrieved March 21, 2023, from https://resources.infosecinstitute.com/topic/computer-forensics-tools/

Purdue University Authors. (2019). *Laboratory manager*. Laboratory Manager - College of Science - Purdue University. Retrieved March 21, 2023, from https://www.purdue.edu/science/careers/what_can_i_do_with_a_major/Career%20Pages/la

boratory_manager.html#:~:text=It's%20a%20lab%20manager's%20job,the%20lab%20is%20kept%20safe.

Whitcomb, C. M. (2002). *A historical perspective of digital evidence*. International Journal of Digital Evidence. Retrieved March 21, 2023, from https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf